# 排除常见的 L2L 和远程访问 IPsec VPN 问题

## 目录

# 简介

本文档介绍 IPsec VPN 问题最常见的解决方案。

# 背景信息

此处介绍的解决方案直接来自Cisco技术支持解决的服务请求。

其中许多解决方案是在对IPsec VPN连接进行深入故障排除之前实施的。

本文档提供了在开始排除连接故障之前要尝试的常见步骤的摘要。

尽管本文档中的配置示例适用于路由器和安全设备，但几乎所有这些概念也适用于VPN 3000 。

请参阅IP安全故障排除-了解和使用debug命令，了解用于在Cisco IOS®软件和(RADIUS/TACACS/TACACS)上排除IPsec问题的常见debug命令的解释。

注意：ASA不会通过IPsec VPN隧道传递组播流量。

警告：本文档中介绍的许多解决方案可能导致设备上的所有IPsec VPN连接暂时中断。

建议根据更改控制策略小心实施这些解决方案。

# 先决条件

## 要求

思科建议了解以下思科设备上的IPsec VPN配置：

- Cisco PIX 5500 系列安全设备
- 思科IOS®路由器

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco PIX 5500 系列安全设备
- Cisco IOS®

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。

### 规则

有关文档规则的详细信息，请参阅思科技术提示规则。

## IPsec VPN 配置不起作用

### 问题

最近配置或修改的 IPSec VPN 解决方案不起作用。

当前 IPSec VPN 配置不再起作用。

### 解决方案

本部分包含最常见 IPSec VPN 问题的解决方案。

尽管这些解决方案未按任何特定顺序列出，但可以用作项目清单，在您进行深入补救之前进行验证或尝试。

所有这些解决方案都直接来自TAC服务请求，并且已经解决了许多问题。

- 启用 NAT 穿透（RA VPN 问题 1）
- 正确测试连接
- 启用 ISAKMP
- 启用/禁用 PFS
- 清除旧的或现有的安全关联（隧道）
- 验证 ISAKMP 生存时间
- 启用或禁用 ISAKMP Keepalive
- 重新输入或恢复预共享密钥
- 预共享密钥不匹配
- 删除并重新应用加密映射
- 验证sysopt命令是否存在（仅限/ASA）

- 验证 ISAKMP 身份
- 验证空闲/会话是否超时
- 验证 ACL 是否正确且绑定到加密映射
- 验证 ISAKMP 策略
- 验证路由是否正确
- 验证转换集是否正确
- 验证加密映射序列号和名称
- 验证对等体 IP 地址是否正确
- 验证隧道组和组名称
- 禁用 L2L 对等体的 XAUTH
- VPN 池耗尽
- VPN Client 流量的延迟问题

注意：由于空间方面的考虑，这些部分中的某些命令已分成两行。

## 启用 NAT 穿透（RA VPN 问题 1）

NAT穿越（或NAT-T）允许VPN流量通过NAT或PAT设备，例如Linksys SOHO路由器。

如果未启用NAT-T，则VPN客户端用户通常看似可以正常连接到ASA，但他们无法访问安全设备背后的内部网络。

如果您未在NAT/PAT设备中启用NAT-T，则会在ASA中收到错误消息**regular translation creation failed for protocol 50 src inside : 10.0.1.26 dst outside : 10.9.69.4**。

同样，如果无法从同一IP地址同时登录，则会显示**Secure VPN connection terminated locally by client.原因412：**远程对等体不再响应。出现错误消息。

在前端 VPN 设备中启用 NAT-T，以解决此错误。

注意：在Cisco IOS®软件版本12.2(13)T及更高版本中，Cisco IOS®中默认启用NAT-T。

以下是用于在 Cisco 安全设备上启用 NAT-T 的命令。本示例中的二十(20)是保持连接时间（默认值）。

ASA

```
<#root>

securityappliance(config)#
```

```
crypto isakmp nat-traversal 20
```

要使命令正常工作，还需要修改客户端。

在Cisco VPN Client中，导航到Connection Entries，然后单击Modify。此时将打开一个新窗口，您必须在其中选择传输选项卡。

在此选项卡下，单击Enable Transparent Tunnelingand theIPSec over UDP（NAT / PAT）单选按钮。然后单击“保存”并测试连接。

通过配置ACL允许NAT-T、UDP 500和ESP端口的UDP 4500非常重要，因为ASA充当NAT设备。

要了解有关ASA中ACL配置的详细信息，请参阅配置一条通过防火墙（执行NAT）的IPSec隧道。

## 正确测试连接

VPN连接最好通过执行加密的端点设备之后的设备进行测试，然而许多用户在执行加密的设备上使用ping命令测试VPN连接。

虽然ping通常可实现此目的，但使ping命令源自正确的接口非常重要。

如果Ping的来源不正确，则VPN连接可能表现为已发生故障，但实际上它仍在正常工作。以下是一个示例：

路由器 A 加密 ACL

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

路由器 B 加密 ACL

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

在这种情况下，apingmust sourced from the inside network behind either router.这是因为加密 ACL仅配置为加密具有那些源地址的流量。

源自任一路由器的外部接口的添加不会加密。在特权EXEC模式下使用ping命令的扩展选项，可以使ping源自路由器的“内部”接口：

```
<#root>

routerA#

ping
```

```
Protocol [ip]:
Target IP address: 192.168.200.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

假设此图中的路由器已替换为ASA安全设备。用于测试连接的ping也可以源自具有insidekeyword的内部接口：

```
<#root>
securityappliance#
ping inside 192.168.200.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

建议不要使用yourping来定位安全设备的内部接口。

如果必须使用yourping来定位内部接口，则必须在该接口上enablemanagement-accesson，否则设备不会应答。

```
<#root>
securityappliance(config)#
management-access inside
```

当连接存在问题时，即使VPN的第一阶段(1)也不起作用。

在ASA上，如果连接失败，则SA输出与以下示例类似，表明可能存在不正确的加密对等体配置和/或ISAKMP建议配置：

<#root>

```
Router#
show crypto isakmp sa


1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG2
```

状态可以是MM_WAIT_MSG2到MM_WAIT_MSG5，这表示相关状态在主模式(MM)下的交换失败。

当阶段 1 启动时，加密 SA 输出与以下示例类似：

<#root>

```
Router#
show crypto isakmp sa


1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

## 启用 ISAKMP

如果没有指示IPsec VPN隧道正常工作，则可能是因为尚未启用ISAKMP。请确保已在设备上启用了 ISAKMP。

使用以下命令之一可在您的设备上启用 ISAKMP：

Cisco IOS®

<#root>

```
router(config)#
crypto isakmp enable
```

Cisco ASA(用所需接口替换外部)

<#root>

```
securityappliance(config)#
```

**crypto isakmp enable outside**

在外部接口上启用 ISAKMP 时，也可能会出现以下错误：

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

错误的原因可能是，在接口上启用isakmp之前，ASA后面的客户端会获取PAT到udp端口500。删除 PAT 转换 (clear xlate) 之后，就可以启用 isakmp。

验证UDP 500和4500端口号已保留以用于与对等体的ISAKMP连接协商。

如果未在接口上启用 ISAKMP，VPN Client 会显示与以下消息类似的错误消息：

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

为了解决此错误，请在 VPN 网关的加密接口上启用 ISAKMP。

## 启用/禁用 PFS

在 IPsec 协商中，完全转发保密 (PFS) 可确保每个新的加密密钥与任何先前密钥不相关。

启用或禁用两个隧道对等体上的PFS；否则，ASA/Cisco IOS®路由器中不会建立LAN到LAN (L2L) IPsec隧道。

完全转发保密 (PFS) 是 Cisco 专有技术，在第三方设备上不支持。

ASA ：

默认情况下 PFS 处于禁用状态。要启用PFS，请在组策略配置模式下使用带有enable关键字的 thepfscommand。要禁用 PFS，请输入 disable 关键字。

**<#root>**

```
hostname(config-group-policy)#
```

**pfs {enable | disable}**

要从配置中删除PFS属性，请输入此命令的no形式。

一个组策略可以从另一个组策略继承 PFS 的值。请输入此命令的no形式以防止值转移。

<#root>

**hostname(config-group-policy)#**

**no pfs**

Cisco IOS®路由器：

要指定在此加密映射条目请求新的安全关联时IPsec必须要求PFS，请在加密映射配置模式下使用set pfscommand。

要指定IPsec在接收新安全关联请求时需要PFS，请在加密映射配置模式下使用set pfscommand。

要指定 IPsec 不可以请求 PFS，请使用此命令的 no 形式。默认情况下，不会请求 PFS。如果使用此命令时未指定任何组，则 group1 会用作默认值。

```
set pfs [group1 | group2]
no set pfs
```

对于 set pfs 命令：

- group1 -指定在执行新的Diffie-Hellman交换时，IPsec必须使用768位Diffie-Hellman主模数组。
- group2 -指定在执行新的Diffie-Hellman交换时，IPsec必须使用1024位Diffie-Hellman主模数组。

示例：

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
```

**set pfs group2**

## 清除旧的或当前的安全关联（隧道）

如果Cisco IOS®®路由器中出现此错误消息，则问题在于SA已过期或已清除。

远程隧道终端设备不知道它使用了已过期的 SA 来发送数据包（并非 SA 建立数据包）。

建立新的 SA 后，通信将恢复，因此请启动隧道间的相关流量来创建新的 SA 并重新建立隧道。

<#root>

**%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x  has no SA**

如果您清除 ISAKMP（阶段 I）和 IPsec（阶段 II）安全关联 (SA)，这是解决 IPsec VPN 问题的最简单而且通常也是最佳的解决方案。

如果清除 SA，通常可以解决各种错误消息和奇怪行为问题，而无需进行故障排除。

虽然此方法可以在任何情况下轻松使用，但是在更改当前 IPSec VPN 配置或对其进行添加之后，几乎都需要清除 SA。

而且，虽然可以仅清除特定的安全关联，但是在设备上全局清除 SA 时好处最多。

清除安全关联后，可能必须在隧道中发送流量以重新建立安全关联。

警告：除非指定要清除的安全关联，否则此处列出的命令可以清除设备上的所有安全关联。如果其他 IPSec VPN 隧道处于使用中，请小心执行操作。

1. 在清除安全关联之前，请查看它们

    a. 思科Cisco IOS®

    <#root>

    **router#**

    **show crypto isakmp sa**

    **router#**

    **show crypto ipsec sa**

    b. Cisco ASA安全设备

    <#root>

    securityappliance#

    **show crypto isakmp sa**

    securityappliance#

    **show crypto ipsec sa**

2. 清除安全关联。可以如粗体所示输入每个命令或同时输入与命令一起显示的选项。

a. Cisco IOS®

a. ISAKMP（阶段 I）

<#root>

```
router#

clear crypto isakmp

 ?
  <0 - 32766>  connection id of SA
  <cr>
```

b. IPsec（阶段 II）

<#root>

```
router#

clear crypto sa

 ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
  <cr>
```

b. Cisco ASA安全设备

a. ISAKMP（阶段 I）

<#root>

```
securityappliance#

clear crypto isakmp sa
```

b. IPsec（阶段 II）

<#root>

```
security appliance#

clear crypto ipsec sa

 ?

  counters  Clear IPsec SA counters
```

```
entry     Clear IPsec SAs by entry
map       Clear IPsec SAs by map
peer      Clear IPsec SA by peer
<cr>
```

## 验证 ISAKMP 生存时间

如果用户在 L2L 隧道中频繁地断开连接，则问题可能是在 ISAKMP SA 中配置了较短的生存时间。

如果ISAKMP生存时间发生任何差异，您会收到%ASA-5-713092： Group = x.x.x.x， IP = x.x.x.x，Failure during phase 1 rekey attempt due to collisioning错误消息。

默认值为 86,400 秒（24 小时）。通常，较短的生存时间可提供更安全的 ISAKMP 协商（在某种程度上），但是，由于生存时间较短，安全设备建立未来的 IPSec SA 也更快。

当来自两个对等体的两个策略包含相同的加密、散列、身份验证和 Diffie-Hellman 参数值，并且远程对等体的策略指定的生存时间小于或等于对比策略中的生存时间时，即视为策略匹配。

如果生存时间不同，将使用较短的生存时间（来自远程对等体的策略）。如果找不到可接受的匹配，IKE 将拒绝协商，并且无法建立 IKE SA。

指定 SA 生存时间。以下示例设置的生存时间为 4 小时（14400 秒）。默认值为 86400 秒（24 小时）。

ASA

<#root>

```
hostname(config)#
isakmp policy 2 lifetime  14400
```

Cisco IOS®路由器

<#root>

```
R2(config)#
crypto isakmp policy 10
R2(config-isakmp)#
lifetime 86400
```

如果超出配置的最大生存时间，在终止 VPN 连接时您会收到以下错误消息：

**Secure VPN Connection terminated locally by the Client.Reason 426： Maximum Configured Lifetime Exceeded**

。

要解决该错误消息，请将thelifetimevalue设置为零(0)，以将IKE安全关联的生存时间设置为无限。VPN始终处于连接状态，不会终止。

```
hostname(config)#isakmp policy 2 lifetime 0
```

您也可以在组策略中禁用re-xauth以解决此问题。

## 启用或禁用 ISAKMP Keepalive

如果配置 ISAKMP Keepalive，则它有助于防止 LAN 到 LAN 或远程访问 VPN 偶尔被丢弃，这包括 VPN Client、隧道和一段非活动时间之后丢弃的隧道。

此功能使隧道端点可以监控远程对等体的持续存在状态，以及向该对等体报告其自己的存在状态。

如果对等体没有响应，则端点会删除连接。

要使 ISAKMP keepalive 起作用，两个 VPN 端点必须支持它们。

在Cisco IOS®中使用以下命令配置ISAKMP keepalive：

<#root>

```
router(config)#
crypto isakmp keepalive 15
```

使用以下命令在ASA安全设备上配置ISAKMP keepalive：

用于名为10.165.205.222的隧道组的Cisco ASA

<#root>

```
securityappliance(config)#
tunnel-group 10.165.205.222
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#
isakmp keepalive
   threshold 15 retry 10
```

在某些情况下，必须禁用此功能以便解决问题，例如，如果 VPN Client 位于阻止 DPD 数据包的防火墙之后。

Cisco ASA，用于名为10.165.205.222的隧道组

禁用IKE保活处理，默认情况下启用。

<#root>

```
securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive


disable
```

禁用 Cisco VPN Client 4.x 的 Keepalive

在发生问题的客户端PC上，导航到%System Root% > Program Files > Cisco Systems >VPN Client > Profiles以禁用IKE keepalive，并在适用的情况下编辑连接的PCF文件。

将theForceKeepAlives=0（默认值）更改为ForceKeepAlives=1。

Keepalive 是 Cisco 专有技术，在第三方设备上不支持。

## 重新输入或恢复预共享密钥

在许多情况下，当IPsec VPN隧道不起作用时，可能会将简单排版错误归咎于它。例如，在安全设备上，预共享密钥在输入后即变为隐藏状态。

这种模糊方法使得无法了解密钥是否正确。请确保已在每个 VPN 端点上正确输入了任何预共享密钥。

重新输入密钥以确保其正确；这是一个简单的解决方案，有助于避免深入故障排除。

在远程访问 VPN 中，请检查 Cisco VPN Client 中是否输入了有效的组名称和预共享密钥。

如果VPN客户端和头端设备之间的组名或预共享密钥不匹配，可能会出现此错误。

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
```

```
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

警告：如果删除与加密相关的命令，则可能会关闭一个或所有VPN隧道。在删除与加密相关的命令之前，请谨慎使用这些命令，并参阅组织的更改控制策略。

使用以下命令，以删除和重新输入对等体10.0.0.1或grouppngroupn Cisco IOS®的预共享密钥：

Cisco LAN 到 LAN VPN

```
<#root>

router(config)#

no crypto isakmp key secretkey
   address 10.0.0.1

router(config)#

crypto isakmp key secretkey
   address 10.0.0.1
```

Cisco 远程访问 VPN

```
<#root>

router(config)#

crypto isakmp client configuration
   group vpngroup

router(config-isakmp-group)#

no key secretkey

router(config-isakmp-group)#

key secretkey
```

使用以下命令，以删除和重新输入/ASA安全设备上对等体10.0.0.1的预共享密钥密钥：

思科6.x

```
<#root>

(config)#

no isakmp key secretkey address 10.0.0.1

(config)#

isakmp key secretkey address 10.0.0.1
```

Cisco /ASA 7.x及更高版本

```
<#root>

securityappliance(config)#

tunnel-group 10.0.0.1
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#

no ikev1 pre-shared-key

securityappliance(config-tunnel-ipsec)#

ikev1


pre-shared-key
   secretkey
```

## 预共享密钥不匹配

启动 VPN 隧道操作的连接断开。出现此问题的原因是在阶段I协商期间，预共享密钥不匹配。

show crypto isakmp sacommand中的MM_WAIT_MSG_6消息指示预共享密钥不匹配，如下例所示：

```
<#root>

ASA#

show crypto isakmp sa


Active SA: 1
Rekey SA: 0 (A tunnel reports 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1         IKE Peer: 10.7.13.20
            Type : L2L                                Role : initiator
```

```
            Rekey : no                                  State :
MM_WAIT_MSG_6
```

为了解决此问题，请在两台设备中重新输入预共享密钥；预共享密钥必须是唯一且匹配的。有关详细信息，请参阅“重新输入或恢复预共享密钥”。

## 删除并重新应用加密映射

当清除安全关联且这无法解决IPsec VPN问题时，请删除并重新应用相关加密映射，以解决包括间断性丢弃VPN隧道和一些VPN站点无法启动在内的各种问题。

警告：如果从接口删除加密映射，则itdefinitelydown与该加密映射关联的所有IPSec隧道。请谨慎地执行这些步骤，并在继续之前考虑组织的更改控制策略。

在Cisco IOS®中，使用以下命令删除和替换加密映射：

首先从接口中删除加密映射。请使用crypto mapcommand的no形式。

```
<#root>
router(config-if)#
no crypto map mymap
```

继续使用thenoform删除整个加密映射。

```
<#root>
router(config)#
no crypto map mymap 10
```

替换对等体 10.0.0.1 的接口 Ethernet0/0 上的加密映射。以下示例显示所需的最低加密映射配置：

```
<#root>
router(config)#
crypto map mymap 10 ipsec-isakmp
router(config-crypto-map)#
match address 101
router(config-crypto-map)#
set transform-set mySET
router(config-crypto-map)#
```

```
set peer 10.0.0.1
router(config-crypto-map)#
exit
router(config)#
interface ethernet0/0
router(config-if)#
crypto map mymap
```

使用以下命令在ASA上删除和替换加密映射：

首先从接口中删除加密映射。请使用crypto mapcommand的no形式。

```
<#root>
securityappliance(config)#
no crypto map mymap interface outside
```

继续使用thenoform删除其他加密映射命令。

```
<#root>
securityappliance(config)#
no crypto map mymap 10 match
   address 101
securityappliance(config)#
no crypto map mymap set
   transform-set mySET
securityappliance(config)#
no crypto map mymap set
   peer 10.0.0.1
```

替换对等体 10.0.0.1 的加密映射。以下示例显示所需的最低加密映射配置：

```
<#root>
securityappliance(config)#
crypto map mymap 10 ipsec-isakmp
securityappliance(config)#
crypto map mymap 10
```

```
   match address 101

securityappliance(config)#

crypto map mymap 10 set
   transform-set mySET

securityappliance(config)#

crypto map mymap 10 set
   peer 10.0.0.1

securityappliance(config)#

crypto map mymap interface outside
```

如果删除并且重新应用加密映射，并且如果前端的 IP 地址已经更改，这也会解决连接问题。

## 验证sysopt命令是否存在（仅限ASA）

命令sysopt connection permit-ipsecandsysopt connection permit-vpnallow来自IPsec隧道的数据包及其有效负载会绕过安全设备上的接口ACL。

如果未启用其中的一个命令，则安全设备上终止的 IPSec 隧道可能会失败。

在安全设备软件版本7.0及更低版本中，此情况的相关sysopt命令issysopt connection permit-ipsec。

在安全设备软件版本7.1(1)及更高版本中，此情况的相关sysopt命令issysopt connection permit-vpn。

在6.x中，默认情况下禁用此功能。使用/ASA 7.0(1)及更高版本时，默认情况下启用此功能。使用以下show命令可确定设备上是否启用了relevantsysoptcommand：

Cisco ASA

<#root>

```
securityappliance#

show running-config all sysopt

no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret

sysopt connection permit-vpn


!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

使用以下命令可为您的设备启用correctsysoptcommand：

Cisco ASA

```
<#root>

securityappliance(config)#

sysopt connection permit-vpn
```

如果不想使用thesysopt connectioncommand，请明确允许所需的相关流量从源到目标。

例如，在外部ACL中，从远程设备的远程到本地LAN，以及从远程设备的外部接口的“UDP端口500”到本地设备的外部接口。

## 验证 ISAKMP 身份

如果IPsec VPN隧道在IKE协商中发生故障，则故障可能是因为其对等体无法识别其对等体的身份。

当两个对等体使用 IKE 建立 IPSec 安全关联时，每个对等体会将其 ISAKMP 身份发送到远程对等体。

对等体发送的是其 IP 地址还是主机名，取决于每个对等体自身设置的 ISAKMP 身份。

默认情况下，防火墙单元的ISAKMP身份设置为IP地址。

通常，请以相同的方式设置安全设备及其对等体的身份，以避免 IKE 协商失败。

要对发送至对等体的阶段2 ID进行设置，请在全局配置模式下使用theisakmp identitycommand。

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication typ
```

或者

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection typ
```

或者

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (defaul
```

使用ASA配置迁移工具将配置从转移到ASA后，VPN隧道无法启动；日志中会显示以下消息：

**[IKEv1]：Group = x.x.x.x，IP = x.x.x.x，发现陈旧的PeerTblEntry，正在删除！**

**[IKEv1]：组= x.x.x.x，IP = x.x.x.x，从相关器表中删除对等项失败，不匹配！**

**[IKEv1]：组= x.x.x.x，IP = x.x.x.x，构造_ipsec_delete()：无SPI以标识第2阶段SA！**

**[IKEv1]：组= x.x.x.x，IP = x.x.x.x，从相关器表中删除对等项失败，不匹配！**

## 验证空闲/会话是否超时

如果空闲超时设置为 30 分钟（默认值），则意味着如果超过 30 分钟没有流量通过隧道，则将丢弃该隧道。

VPN Client将在30分钟后断开连接，而不管空闲超时参数如何，并且将出现**PEER_DELETE-IKE_DELETE_UNSPECIFIED**错误。

配置timeoutandsession timeoutasnonein使隧道变为alwaysup，并且让隧道即使在使用第三方设备时也不会被丢弃。

ASA

在组策略配置模式下或用户名配置模式下输入vpn-idle-timeoutcommand，以配置用户超时时长：

**<#root>**

```
hostname(config)#

group-policy DfltGrpPolicy attributes

hostname(config-group-policy)#

vpn-idle-timeout none
```

在组策略配置模式或用户名配置模式下使用vpn-session-timeoutcommand配置VPN连接的最长时间：

**<#root>**

```
hostname(config)#

group-policy DfltGrpPolicy attributes

hostname(config-group-policy)#
```

**vpn-session-timeout none**

当配置了tunnel-allconfigured时，不需要配置configureidle-timeouts，因为即使您配置VPN-idle timeout，它也不起作用，因为所有流量都通过隧道（因为配置了tunnel-all）。

因此，相关流量（甚至PC生成的流量）是相关流量，不会让空闲超时生效。

Cisco IOS®路由器

在全局配置模式下或加密映射配置模式下，使用crypto ipsec security-association idle-timecommand以配置IPsec SA空闲计时器。

默认情况下，IPsec SA 空闲计时器处于禁用状态。

<#root>

**crypto ipsec security-association idle-time**

*seconds*

时间以秒为单位计算，空闲计时器允许非活动对等体维持SA。seconds 参数的有效值范围是 60 到 86400。

## 验证 ACL 是否正确且是否绑定到加密映射

典型的 IPSec VPN 配置中会使用两个访问列表。一个访问列表用于免除从 NAT 进程发送至 VPN 隧道的流量。

另一个访问列表定义要加密的流量；这包括LAN到LAN设置中的加密ACL或远程访问配置中的分割隧道ACL。

当这些ACL配置错误或丢失时，流量可能只通过VPN隧道单向流动，也可能根本不在隧道中发送。

确保在全局配置模式下使用crypto map match address命令将加密ACL与加密映射绑定。

请确保已配置了完成 IPSec VPN 配置所需的所有访问列表，且这些访问列表定义了正确的流量。

此列表包含在您怀疑 ACL 是导致 IPSec VPN 出现问题的原因时要检查的简单项目。

请确保 NAT 免除和加密 ACL 指定了正确的流量。

如果有多个 VPN 隧道和多个加密 ACL，请确保这些 ACL 不会重叠。

请确保您的设备已配置为使用 NAT 免除 ACL。在路由器上，这意味着您使用theroute-mapcommand。

在ASA上，这意味着您使用thenat (0)命令。LAN 到 LAN 配置和远程访问配置都需要使用 NAT 免除 ACL。

此处，Cisco IOS®路由器配置为免除来自NAT在192.168.100.0 /24和192.168.200.0 /24或192.168.1.0 /24之间发送的流量。发送至其他任何位置的流量受 NAT 过载影响：

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

NAT 免除 ACL 仅适用于 IP 地址或 IP 网络（如上述示例 (access-list noNAT)），并且必须与加密映射 ACL 相同。

NAT免除ACL不适用于端口号（例如，23、25...）。

在VOIP环境中，网络之间的语音呼叫通过VPN进行通信，如果NAT 0 ACL配置不正确，则语音呼叫不起作用。

在排除故障之前，建议检查VPN连接状态，因为问题可能是由于NAT免除ACL的配置错误。

如果 NAT 免除 (nat 0) ACL 中存在配置错误，则会收到如下所示的错误消息。

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

不正确示例：

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
```

**eq 25**

如果NAT免除(nat 0)不起作用，请尝试将其删除并发出NAT 0命令以使其正常工作。

请确保您的 ACL 不是落后的，并且类型正确。

必须从配置 ACL 的设备的角度编写 LAN 到 LAN 配置的加密 ACL 和 NAT 免除 ACL。

这意味着ACL必须能到达其他ACL。在以下示例中，在192.168.100.0 /24和192.168.200.0 /24之间

建立了LAN到LAN隧道。

路由器 A 加密 ACL

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
```

路由器 B 加密 ACL

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

尽管此处未说明，但此概念同样适用于ASA安全设备。

在ASA中，远程访问配置的分割隧道ACL必须成为允许流量流入VPN Client需要访问网络的标准访问列表。

Cisco IOS®路由器可以对分割隧道使用扩展ACL。在扩展访问列表中，在分割隧道ACL中的源位置使用“any”相当于禁用分割隧道。

在拆分隧道的扩展ACL中仅使用源网络。

正确示例：

<#root>

**access-list 140 permit ip**

**10.1.0.0 0.0.255.255**

**10.18.0.0 0.0.255.255**

不正确示例：

<#root>

access-list 140 permit ip

**any**

10.18.0.0 0.0.255.255

Cisco IOS®

<#root>

```
router(config)#

access-list 10 permit ip 192.168.100.0

router(config)#

crypto isakmp client configuration group MYGROUP

router(config-isakmp-group)#

acl 10
```

Cisco ASA

<#root>

```
securityappliance(config)#

access-list 10 standard
   permit 192.168.100.0 255.255.255.0

securityappliance(config)#

group-policy MYPOLICY internal

securityappliance(config)#

group-policy MYPOLICY attributes

securityappliance(config-group-policy)#

split-tunnel-policy
   tunnelspecified

securityappliance(config-group-policy)#

split-tunnel-network-list
   value 10
```

站点到站点 VPN 隧道的 ASA 版本 8.3 中的 NAT 免除配置：

必须使用版本8.3的两个ASA在HOASA和BOASA之间建立站点到站点VPN。HOASA 上的 NAT 免除配置如下所示：

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

## 验证 ISAKMP 策略

如果 IPSec 隧道未启动，请检查 ISAKMP 策略是否与远程对等体匹配。此 ISAKMP 策略适用于站点到站点 (L2L) 和远程访问 IPSec VPN。

如果Cisco VPN Client或站点到站点VPN无法与远程端设备建立隧道，请检查两个对等体是否包含相同的加密、散列、身份验证和Diffie-Hellman参数值。

验证远程对等体策略何时指定了生存时间小于或等于发起方发送的策略中的生存时间。

如果生存时间不相同，则安全设备会使用较短的生存时间。如果不存在可接受的匹配，则 ISAKMP 将拒绝协商，并且无法建立 SA。

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

以下是详细日志消息：

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

此消息通常由于ISAKMP策略不匹配或遗漏的NAT 0语句而出现。

此外，系统还会显示以下消息：

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

此消息表明第1阶段完成后第2阶段消息位于队列中。此错误消息是由以下原因之一导致的：

- 任何对等体上的阶段不匹配
- ACL阻止对等体完成第1阶段

此消息通常紧跟**theRemoving peer from peer table failed，no match！**错误消息。

如果 Cisco VPN Client 无法连接前端设备，则问题可能是 ISAKMP 策略不匹配。前端设备必须与 Cisco VPN客户端的其中一个IKE建议匹配。

对于ASA上使用的ISAKMP策略和IPsec转换集，思科VPN客户端无法使用带有DES和SHA组合的策

略。

如果您使用 DES，则需要使用 MD5 散列算法，也可以使用其他组合，如 3DES 和 SHA 以及 3DES 和 MD5。

## 验证路由是否正确

请确保您的加密设备（例如路由器和ASA安全设备）具有正确的路由信息，以便通过VPN隧道发送流量。

如果网关设备后有其他路由器，请确保这些路由器知道如何到达隧道以及另一端有哪些网络。

VPN 部署中的路由的一个关键组件是反向路由注入 (RRI)。

RRI 会在 VPN 网关的路由表中放置远程网络或 VPN Client 的动态条目。

这些路由对安装路由的设备以及网络中的其他设备非常有用，这是因为 RRI 安装的路由可以通过路由协议（如 EIGRP 或 OSPF）进行再分配。

在 LAN 到 LAN 配置中，每个端点包含的路由所指向的网络应对流量进行加密，这一点非常重要。

在以下示例中，路由器 A 必须包含通过 10.89.129.2 连接到路由器 B 之后的网络的路由。路由器 B 必须包含连接到 192.168.100.0 /24 的类似路由：

确保每个路由器知道相应路由的第一种方法是为每个目标网络配置静态路由。例如，路由器 A 可以配置如下路由语句：

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

如果路由器A已替换为ASA，则配置可能如下所示：

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

如果每个端点之后存在大量网络，则静态路由的配置将变得难以维护。

建议您依照所述使用反向路由注入。RRI 会将加密 ACL 中列出的所有远程网络的路由放置在路由表中。

例如，路由器 A 的加密 ACL 和加密映射看起来与以下内容相似：

<#root>

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
```

**reverse-route**

```
 set transform-set mySET
 match address 110
```

如果路由器A被ah ASA取代，则配置可能如下所示：

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
```

**crypto map mymap 10 set reverse-route**

在远程访问配置中，路由更改并非始终必要。

然而，如果在 VPN 网关路由器或安全设备之后存在其他路由器，这些路由器需要以某种方式识别出 VPN Client 的路径。

在以下示例中，假设VPN Client在连接时的给定地址在10.0.0.0 /24范围内。

如果网关和其他路由器之间当前没有使用任何路由协议，则路由器（如路由器 2）上可以使用静态路由：

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

如果网关和其他路由器之间正在使用某种路由协议（EIGRP 或 OSPF），则建议依照所述使用反向路由注入。

RRI 会自动将 VPN Client 的路由添加到网关的路由表中。然后，这些路由可以分发到网络中的其他路由器。

Cisco IOS®路由器：

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

**reverse-route**

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Cisco ASA安全设备：

<#root>

```
crypto dynamic-map dynMAP 10 set transform-set mySET
```

**crypto dynamic-map dynMAP 10 set reverse-route**

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

如果为 VPN Client 分配的 IP 地址池与前端设备的内部网络重叠，则会发生路由问题。有关详细信息，请参阅专用网络重叠部分。

## 验证转换集是否正确

确保两个端点上的转换集所要使用的 IPsec 加密和散列算法是相同的。

有关详细信息，请参阅Cisco安全设备配置指南的Command参考。

对于ASA上使用的ISAKMP策略和IPsec转换集，思科VPN客户端无法使用带有DES和SHA组合的策略。

如果您使用 DES，则需要使用 MD5 散列算法，也可以使用其他组合，如 3DES 和 SHA 以及 3DES 和 MD5。

## 验证加密映射序列号和名称以及在 IPsec 隧道启动/结束时加密映射是否应用到正确的接口

如果在同一加密映射中配置了静态和动态对等体，则加密映射条目的顺序非常重要。

动态加密映射entrymust的序列号必须高于其他所有静态加密映射条目。

如果静态条目的编号高于动态条目，则与这些对等体的连接会失败，并会发生如下所示的调试。

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

安全设备中的每个接口仅允许一个动态加密映射。

以下是一个正确编号的加密映射示例，其中包含一个静态条目和一个动态条目。请注意，动态条目具有最高的序列号，并且已留下空间以便添加其他静态条目：

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
```

**crypto map mymap 60000 ipsec-isakmp dynamic ciscothe**

加密映射名称区分大小写。

当动态加密人序列不正确导致对等体命中错误的加密映射时，也会出现此错误消息。

这也是定义相关流量的加密访问列表不匹配导致的：**%ASA-3-713042： IKE Initiator unable to find policy：**

在要在同一接口中终止多个VPN隧道的场景中，创建具有相同名称（每个接口仅允许一个加密映射）但序列号不同的加密映射。

这一点适用于路由器和ASA。

同样，有关L2L和远程访问VPN方案的加密映射配置的详细信息，请参阅ASA：向现有L2L VPN添加新隧道或远程访问-Cisco。

## 验证对等体 IP 地址是否正确

创建和管理IPsec的连接特定记录的数据库。

对于ASA安全设备LAN到LAN (L2L) IPsec VPN配置，请在tunnel-group <name> type ipsec-

l2lcommand中指定隧道组的<name>作为远程对等体IP地址（远程隧道端）。

对等体IP地址必须与intunnel group name和Crypto map set addresscommands匹配。

使用 ASDM 配置 VPN 时，将使用正确的对等体 IP 地址自动生成隧道组名称。

如果未正确配置对等体IP地址，则日志中会包含以下消息，可以通过正确配置对等体IP地址来解决该问题。

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

当在ASA加密配置中未正确配置对等体IP地址时，ASA无法建立VPN隧道，且仅会在MM_WAIT_MSG4阶段挂起。

为了解决此问题，请更正配置中的对等体 IP 地址。

以下是当VPN隧道在MM_WAIT_MSG4状态挂起时，show crypto isakmp sacommand的输出。

<#root>

```
hostname#
```

**show crypto isakmp sa**

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG4
```

## 验证隧道组和组名称

```
%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

当由于组策略中指定的允许隧道与隧道组配置中的允许隧道不同而丢弃隧道时，会显示此消息。

<#root>

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

**Both lines read:**

```
  vpn-tunnel-protocol ipsec l2tp-ipsec
```

针对“默认组中现有的协议策略”启用“默认组中的 IPSec”策略。

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

## 禁用 L2L 对等体的 XAUTH

如果LAN到LAN隧道和远程访问VPN隧道配置在同一个加密映射中，则系统会对LAN到LAN对等体提示XAUTH信息，且LAN到LAN隧道出现故障，在show crypto isakmp sacommand的输出中显示“CONF_XAUTH”。

以下是 SA 输出的示例：

**<#root>**

```
Router#
```

**show crypto isakmp sa**

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

此问题仅适用于Cisco IOS®而ASA不会受到此问题的影响，因为它使用隧道组。

请在输入isakmp密钥时使用theno-xauthkeyword，以便设备不提示对等体提供XAUTH信息（用户名和口令）。

此关键字会禁用静态 IPSec 对等体的 XAUTH。在同一个加密映射中配置了 L2L 和 RA VPN 的设备上输入与以下类似的命令：

**<#root>**

```
router(config)#
```

**crypto isakmp key cisco123 address**
**   172.22.1.164 no-xauth**

在ASA充当Easy VPN Server的场景中，Easy VPN客户端由于Xauth问题而无法连接到头端。

在ASA中禁用用户身份验证以解决此问题，如下所示：

```
<#root>
ASA(config)#
tunnel-group example-group type ipsec-ra
ASA(config)#
tunnel-group example-group ipsec-attributes
ASA(config-tunnel-ipsec)#
isakmp ikev1-user-authentication none
```

请参阅本文档的Miscellaneoussection，以了解有关isakmp ikev1-user-authenticationcommand的详细信息。

## VPN 池耗尽

当分配给 VPN 池的 IP 地址范围不足时，可通过两种方法扩大 IP 地址的供给：

1. 取消现有范围，然后定义新范围。例如：

```
<#root>
CiscoASA(config)#
no ip local pool testvpnpool 10.76.41.1-10.76.41.254
CiscoASA(config)#
ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

2. 当不连续子网添加到 VPN 池时，您可以定义两个独立的 VPN 池，然后按照“隧道组属性”下的顺序进行指定。例如：

```
<#root>
CiscoASA(config)#
ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
CiscoASA(config)#
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
```

```
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

您指定池所遵循的顺序非常重要，因为 ASA 按照池在此命令中的出现顺序从这些池中分配地址。

在组政策地址池命令中的地址池设置始终会覆盖隧道组地址池命令中的本地池设置。

### VPN Client 流量的延迟问题

当VPN连接出现延迟问题时，请验证以下条件以解决此问题：

1. 验证数据包的 MSS 是否可以进一步减小。
2. 如果使用的是IPsec/tcp而不是IPsec/udp，则请配置represerve-vpn-flow。
3. 重新载入 Cisco ASA。

## VPN客户端无法与ASA连接

### 问题

当 X-authX 与 RADIUS 服务器一起使用时，Cisco VPN Client 无法进行身份验证。

### 解决方案

问题可能是 xauth 超时。增加 AAA 服务器的超时值以解决此问题。

例如：

```
<#root>
Hostname(config)#
aaa-server test protocol radius

hostname(config-aaa-server-group)#
aaa-server test host 10.2.3.4

hostname(config-aaa-server-host)#
timeout 10
```

### 问题

当 X-authX 与 RADIUS 服务器一起使用时，Cisco VPN Client 无法进行身份验证。

### 解决方案

首先，请确保身份验证正常工作。要缩小问题的范围，请先验证 ASA 本地数据库的身份验证。

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

如果正常工作，则问题与Radius服务器配置有关。

验证 Radius 服务器与 ASA 的连接。如果 ping 正常工作，未出任何问题，则请检查 ASA 的 Radius 相关配置和 Radius 服务器上的数据库配置。

您可使用debug radiuscommand对Radius相关问题进行故障排除。有关sampledebug radiusoutput，请参阅此示例输出。

在ASA上使用debugcommand之前，请参阅以下文档：警告消息。

## VPN Client 在第一次尝试时经常丢弃连接或出现以下错误：“Security VPN Connection terminated by peer.Reason 433.”或“Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)”

### 问题

Cisco VPN客户端用户在尝试连接头端VPN设备时收到此错误。

VPN客户端在第一次尝试时经常丢弃连接

安全VPN连接由对等项终止。Reason 433.

安全VPN连接被对等项原因433终止：（对等项未指定原因）

已尝试分配网络或广播IP地址，正在从池中删除(x.x.x.x)

### 解决方案 1

问题可能是通过ASA、Radius服务器、DHCP服务器或通过充当DHCP服务器的Radius服务器分配IP池。

请使用debug 加密命令，以验证网络掩码和IP地址是否正确。同时，请确认 IP 池不包括网络地址和广播地址。

Radius 服务器必须可以将正确的 IP 地址分配到客户端。

### 解决方案 2

如果扩展身份验证失败，也会发生此问题。您必须检查 AAA 服务器以对此错误进行故障排除。

检查服务器和客户端上的服务器身份验证密码。重新加载AAA服务器可以解决此问题。

### 解决方案 3

此问题的另一种解决方法是禁用威胁检测功能。

当不同不完整安全关联(SA)多次重新传输时，启用威胁检测功能的ASA会认为发生了扫描攻击，并且VPN端口被标记为主要威胁。

尝试禁用威胁检测功能，因为此功能会对 ASA 的处理造成大量开销。使用以下命令禁用威胁检测：

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

这可当作一种解决方法，用于验证是否解决实际问题。

确保在Cisco ASA上禁用威胁检测实际上会破坏几项安全功能，例如减少扫描尝试、无效SPI的DoS、应用检查失败的数据包以及未完成会话。

### 解决方案 4

未正确配置转换集时，也会出现此问题。正确配置转换集可解决问题。

## 远程访问和 EZVPN 用户连接到 VPN，但是无法访问外部资源

### 问题

远程访问用户连接到 VPN 后，将无法连接到 Internet。

远程访问用户无法访问位于同一个设备上其他 VPN 之后的资源。

远程访问用户仅可访问本地网络。

### 解决方案

尝试以下解决方案，以便解决此问题：

- 无法访问 DMZ 中的服务器
- VPN Client 无法解析 DNS
- 分割隧道 — 无法访问 Internet 或排除的网络
- 本地 LAN 访问
- 专用网络重叠

无法访问 DMZ 中的服务器

一旦VPN客户端与VPN前端设备(ASA/Cisco IOS®路由器)建立了IPsec隧道，VPN客户端用户就可以访问内部网络(10.10.10.0/24)资源，但他们无法访问DMZ网络(10.1.1.0/24)。

图解

检查分割隧道，在前端设备中添加 NO NAT 配置，以访问 DMZ 网络中的资源。

示例：

ASA 配置：

此配置显示如何配置 DMZ 网络的 NAT 免除，以便让 VPN 用户可访问 DMZ 网络：

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

在添加对应 NAT 配置的新条目之后，请清除 Nat 转换。

```
Clear xlate
Clear local
```

验证：

如果已建立隧道，请转到Cisco VPN客户端并选择Status > Route Details，以检查是否已显示DMZ和内部网络的安全路由。

有关将新VPN隧道或远程访问VPN添加到已经存在的L2L VPN配置所需的步骤，请参阅ASA：向现有L2L VPN添加新隧道或远程访问VPN - Cisco。

请参阅ASA：在ASA上允许VPN客户端分割隧道的配置示例，以获取有关如何允许VPN客户端在通过隧道连接到Cisco 5500系列自适应安全设备(ASA)时访问互联网的分步说明。

## VPN Client 无法解析 DNS

建立隧道后，如果VPN客户端无法解析DNS，问题可能是头端设备(ASA)中的DNS服务器配置。

此外，请检查 VPN Client 和 DNS 服务器之间的连接。DNS服务器配置必须在组策略下配置，并在隧道组常规属性中的组策略下应用；例如：

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !--- a


group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com


!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.


tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

VPN Client 无法根据名称连接内部服务器

VPN Client 无法根据名称对远程端或前端内部网络的主机或服务器执行 ping 操作。您需要启用 ASA 上的 split-dns 配置以解决此问题。

## 分割隧道 — 无法访问 Internet 或排除的网络

拆分隧道允许远程访问IPsec客户端有条件地以加密形式将数据包通过IPsec隧道定向或以明文形式定向到网络接口（解密），然后将其路由到最终目标。

默认情况下，分割隧道处于禁用状态，这会显示istunnelalltraffic。

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

仅Cisco VPN Client支持excludespecified选项，EZVPN Client不支持。

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

有关分割隧道的详细配置示例，请参阅以下文档：

- ASA：在ASA上允许VPN Client使用分割隧道的配置示例
- 路由器允许 VPN Client 使用分割隧道连接 IPsec 和 Internet 的配置示例

### 发夹溶液

对于进入某接口然后又从同一接口路由出去的 VPN 流量，此功能非常有用。

例如，在集中星型VPN网络中，安全设备是中心，远程VPN网络是分支，分支到分支通信流量必须进入安全设备，然后再次流出到其他分支。

请使用same-security-trafficconfiguration，以允许从同一接口进入和退出。

<#root>

securityappliance(config)#

**same-security-traffic permit intra-interface**

### 本地 LAN 访问

远程访问用户连接到 VPN 并且仅能连接到本地网络。

有关详细配置示例，请参阅ASA：允许VPN Client的本地LAN访问。

### 专用网络重叠

问题

如果无法在建立隧道之后访问内部网络，请检查分配给 VPN Client 的 IP 地址是否与前端设备之后的内部网络重叠。

解决方案

验证要为VPN客户端、前端设备的内部网络和VPN客户端内部网络分配的池中的IP地址位于不同的网络中。

您可以分配具有不同子网的同一个主网络，但是有时会发生路由问题。

有关进一步示例，请参阅无法访问DMZ中的服务器部分的DiagramandExampleof。

## 无法连接超过三个 VPN Client 用户

### 问题

只有三个VPN客户端可以连接到ASA/；第四个客户端的连接失败。失败时，将显示以下错误消息：

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

## 解决方案

在大多数情况下，此问题与组策略中的同时登录设置以及最大会话限制相关。

尝试以下解决方案，以便解决此问题：

- 配置同时登录数
- 使用CLI配置ASA
- 配置配置

## 配置同时登录数

如果选中了ASDM中的Inheritcheck框，则系统仅允许默认的用户同时登录数。同时登录的默认值为三(3)。

要解决此问题，请增加同时登录数的值。

1. 启动ASDM，然后导航到Configuration > VPN > Group Policy。
2. 选择适当的组，然后点击“编辑”按钮。
3. 进入Generaltab后，撤消Connection Settings下Simultaneous Logins的Inheritcheck框。在字段中选择相应的值。

   此字段的最小值为零(0)，这将禁用登录并阻止用户访问。

   当您从另一台PC使用同一用户帐户登录时，当前会话（从使用同一用户帐户的另一台PC建立的连接）将终止，并且新会话将建立。

这是默认行为，且不受 VPN 同时登录数影响。

## 使用CLI配置ASA

完成以下步骤以配置所需的同时登录数。在本例中，选择二十(20)作为期望值。

```
<#root>
```

```
ciscoasa(config)#
group-policy Bryan attributes
ciscoasa(config-group-policy)#
vpn-simultaneous-logins 20
```

要了解有关此命令的详细信息，请参阅Cisco安全设备命令参考。

在全局配置模式下使用vpn-sessiondb max-session-limitcommand，将VPN会话数限制为小于安全设备允许的值。

使用此命令的输出以删除会话限制。重新使用命令，以覆盖当前设置。

```
vpn-sessiondb max-session-limit {session-limit}
```

本示例显示如何将 VPN 最大会话限制数设置为 450：

```
<#root>
hostname#
vpn-sessiondb max-session-limit 450
```

## 配置

错误消息

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

解决方案

完成以下步骤，以便配置所需的同时登录数。针对此 SA，您也可以尝试将 Simultaneous Logins 设置为 5：

依次选择Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneous Logins，然后将登录数更改为5。

# 建立隧道后无法启动会话或应用程序并且传输缓慢

## 问题

建立 IPSec 隧道后，应用程序或会话不能在隧道中启动。

## 解决方案

使用ping命令，以检查网络或查看是否可从您的网络访问应用程序服务器。

对于通过路由器或/ASA设备的临时数据包，尤其是设置了SYN位的TCP数据段，其最大数据段大小(MSS)可能会出现问题。

## Cisco IOS®路由器-更改路由器的外部接口（隧道终端接口）中的MSS值

运行以下命令，以更改路由器的外部接口（隧道末端接口）中的 MSS 值：

```
<#root>

Router>

enable

Router#

configure terminal

Router(config)#

interface ethernet0/1


Router(config-if)#ip tcp adjust-mss 1300

Router(config-if)#

end
```

以下消息显示了 TCP MSS 的调试输出：

```
<#root>

Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

MMS 按照配置在路由器上调整到 1300。

有关详细信息，请参阅ASA和Cisco IOS®：VPN分段。

### ASA -请参阅/ASA文档

由于产生 MTU 大小错误消息和 MSS 问题，因此无法正确访问 Internet 或者通过隧道的传输缓慢。

为了解决此问题，请参阅以下文档：

- ASA和Cisco IOS®：VPN分段

## 无法从ASA启动VPN隧道

### 问题

您无法从ASA接口启动VPN隧道，并且建立隧道后，远程终端/VPN客户端无法ping通VPN隧道上ASA的内部接口。

例如，pn客户端无法通过VPN隧道启动到ASA内部接口的SSH或HTTP连接。

### 解决方案

除非在全局配置模式下配置management-accesscommand，否则无法从隧道的另一端对的内部接口执行ping操作。

```
<#root>

ASA-02(config)#

management-access inside


ASA-02(config)#

show management-access

management-access inside
```

此命令还有助于通过VPN隧道向ASA内部接口发起SSH初始化或http连接。

此信息也适用于 DMZ 接口。例如，如果您想要对/ASA的DMZ接口执行ping操作或想要从DMZ接口启动隧道，则需要使用management-access DMZ命令。

```
<#root>

ASA-02(config)#

management-access DMZ
```

如果VPN客户端无法连接，请确保ESP和UDP端口已打开。

但是，如果这些端口未打开，请尝试通过在VPN客户端连接条目下选择此端口来连接TCP 10000。

右键单击modify > transport选项卡> IPsec over TCP。

# 无法通过 VPN 隧道传递流量

## 问题

您无法通过 VPN 隧道传递流量。

## 解决方案

当ESP数据包被阻止时，也会发生此问题。要解决此问题，请重新配置VPN隧道。

当数据未加密，但仅通过VPN隧道解密时，可能会发生此问题，如以下输出所示：

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y


 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0
```

要解决此问题，请检查以下条件：

1. 如果加密访问列表与远程站点匹配，且 NAT 0 访问列表正确。
2. 如果路由正确且流量到达通过内部的外接口。示例输出显示解密完成，但是未发生加密。
3. 如果已在ASA上配置sopt permit connection-vpn命令。如果未配置，请配置此命令，因为它允许ASA将加密/VPN流量从接口ACL检查中排除。

# 为同一加密映射上的VPN隧道配置备用对等体

### 问题

您可能想要为单个 VPN 隧道使用多个备用对等体。

### 解决方案

配置多个对等体相当于提供回退列表。对于每个隧道，安全设备会尝试与列表中的第一个对等体协商。

如果该对等体不响应，则安全设备会按照顺序与列表中的下一个对等体协商，直到对等体做出响应或在列表中不再有对等体。

ASA已将加密映射配置为主要对等体。辅助对等体可添加在主对等体之后。

此示例配置将主对等体显示为 X.X.X.X，备用对等体为 Y.Y.Y.Y：

<#root>

ASA(config)#

**crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y**

## 禁用/重新启动 VPN 隧道

### 问题

为了暂时禁用 VPN 隧道并重新启动服务，请完成此部分所述的程序。

### 解决方案

在全局配置模式下使用crypto map interface命令可删除之前在接口上定义的加密映射集。

使用此命令的enoform，从接口中删除加密映射集。

<#root>

hostname(config)#

**no crypto map**

*map-name*

**interface**

*interface-name*

此命令可删除任何活动安全设备接口的加密映射集，并且使 IPsec VPN 隧道在该接口上保持不活动

状态。

要重新启动接口上的 IPsec 隧道，在该接口可提供 IPsec 服务之前，您必须将加密映射集分配到接口。

<#root>

hostname(config)#

**crypto map**

*map-name*

**interface**

*interface-name*

# 一些隧道未加密

## 问题

当 VPN 网关上配置了大量隧道时，一些隧道不传递流量。ASA 不会收到那些隧道的加密数据包。

## 解决方案

由于 ASA 未能通过隧道传递加密数据包，因此出现此问题。在 ASP 表中创建了重复的加密规则。

# 错误：- %ASA-5-713904：组= DefaultRAGroup，IP = x.x.x.x，...不支持的事务模式v2版本。隧道已终止。

## 问题

显示**%ASA-5-713904： Group = DefaultRAGroup， IP = 192.0.2.0，...不支持的事**务模式**v2 version.Tunnel terminatedererror**消息。

## 解决方案

显示Transaction Mode v2错误消息的原因是ASA仅支持IKE模式配置V6而不支持旧版V2模式。

请使用 IKE 模式配置 V6 版本来解决此错误。

# 错误：- %ASA-6-722036： Group client-group User xxxx IP x.x.x.x正在传输大数据包1220（阈值1206）

## 问题

ASA的日志中显示**%ASA-6-722036： Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206)**错误消息。

此日志意味着什么？如何解决该问题？

### 解决方案

此日志消息说明已向客户端发送了一个大型数据包。数据包的源不能识别客户端的 MTU。

这也可能是由于对不可压缩的数据进行了压缩所致。解决方法是使用svc compression nonecommand关闭SVC压缩，即可解决问题。

## 当在 VPN 隧道一端启用 QoS 时出现错误消息

### 问题

如果在VPN隧道一端启用QoS，则会收到以下错误消息：

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

### 解决方案

当隧道的一端执行QoS时，通常会导致此消息。当检测到数据包顺序混乱时，会发生这种情况。

您可以禁用 QoS 以停止此错误，但是只要流量可以通过隧道就可以忽略此错误。

## 警告：加密映射条目不完整

### 问题

当您运行crypto map mymap 20 ipsec-isakmpcommand时，您会收到以下错误：

**警告：加密映射**条目不完整

例如：

```
<#root>

ciscoasa(config)#

crypto map mymap 20 ipsec-isakmp

WARNING: crypto map entry incomplete
```

## 解决方案

在定义新的加密映射时，这是通常的警报；提醒必须在配置参数(如访问列表（匹配地址）、转换集和对等体地址)后才能起作用。

此外，如果配置中未显示您键入的用于定义加密映射的第一行代码，这也属于正常现象。

# 错误：- %ASA-4-400024： IDS：2151大ICMP数据包从到外部接口

## 问题

无法通过 vpn 隧道传递大型 ping 数据包。当我们尝试传递大型ping数据包时，会收到错误**%ASA-4-400024： IDS：2151 Large ICMP packet from to on interface outside**。

## 解决方案

禁用签名2150和2151以解决此问题。禁用签名后，ping操作将正常工作。

请使用以下命令禁用签名：

ASA(config)# ip audit signature 2151 disable

ASA(config)# ip audit signature 2150 disable

# 错误：- %ASA-4-402119： IPSEC：从remote_IP （用户名）到local_IP收到的协议数据包（SPI=spi，序列号= seq_num）反重播检查失败。

## 问题

我在 ASA 的日志消息中收到了以下错误：

错误：- %|**ASA-4-402119： IPSEC：从remote_IP (username)到local_IP收到的**协议数据包（**SPI=spi，序列**号=**seq_num）反重播**检查失败。

## 解决方案

要解决此错误，请使用crypto ipsec security-association replay window-sizecommand来改变窗口大小。

<#root>

hostname(config)#

**crypto ipsec security-association replay window-size 1024**

Cisco 建议您使用 1024 完整窗口大小以消除任何防重播问题。

# 错误消息- %ASA-4-407001：拒绝本地主机接口名称：内部地址流量，超过许可证数量限制

## 问题

少数主机无法连接到互联网，且此错误消息显示在系统日志中：

错误消息- %**ASA-4-407001：拒**绝本地主机接口名称：内部地址流量，超过许可证数量限制

## 解决方案

当用户数量超过所用许可证的用户限制时会收到此错误消息。可通过将许可证升级到更多用户来解决此错误。

根据需要，用户许可证可以包括 50、100 或无限用户数。

# 错误消息 - %VPN_HW-4-PACKET_ERROR:

## 问题

Error Message - %VPN_HW-4-PACKET_ERROR：错误消息表明路由器收到的具有HMAC的ESP数据包不匹配。此错误可能由以下问题引起：

- 有缺陷的 VPN H/W 模块
- 损坏的 ESP 数据包

## 解决方案

为了解决此错误消息：

- 除非出现流量中断，否则请忽略该错误消息。
- 如果出现流量中断，请替换模块。

# 错误消息：Command rejected： delete crypto connection between VLAN XXXX and XXXX， first。

## 问题

当您尝试在交换机的中继端口上添加允许的VLAN时会出现此错误消息：Command rejected： delete crypto connection between VLAN XXXX and VLAN XXXX， first.。

无法修改 WAN 边缘中继以允许附加 VLAN。也就是说，您无法在IPSEC VPN SPAtrunk中添加 VLAN。

此命令被拒绝，因为它会导致加密连接的接口VLAN属于允许的VLAN列表，从而构成潜在的 IPSec安全漏洞。

请注意，此行为适用于所有中继端口。

### 解决方案

不应该使用`no switchport trunk allowed vlan (vlanlist)`命令，请使用`switchport trunk allowed vlan` nonecommand或“`switchport trunk allowed vlan remove (vlanlist)`”命令。

## 错误消息- % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE：丢弃的数据包-会话x.x.x：27331到x.x.x.x：23的窗口缩放选项无效[Initiator(flag 0，factor 0) Responder (flag 1， factor 2)]

### 问题

当您尝试从 VPN 隧道远端的设备远程登录时，或者当您尝试从路由器本身远程登录时，会出现此错误：

错误消息- % **FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE：**丢弃的数据包-会话**x.x.x：27331到x.x.x.x：23的窗口**缩放选项无效[**Initiator(flag 0，factor 0) Responder (flag 1， factor 2)]**

### 解决方案

根据需要，用户许可证可以包括 50、100 或无限用户数。添加了窗口缩放功能，以便快速传输长距离网络(LFN)上的数据。

这些典型连接具有非常高的带宽，同时具有高延迟。

卫星连接网络是 LFN 的一个示例，因为卫星链路始终具有高传播延迟，但通常具有高带宽。

要启用窗口缩放功能以支持LFN，TCP窗口大小必须大于65,535。如果将TCP窗口大小增加到65,535以上，可以解决此错误消息。

## %ASA-5-305013：为转发和反向匹配的非对称NAT规则。请更新此问题流程

### 问题

VPN 隧道启动后，会显示以下错误消息：

**%ASA-5-**

**305013：**为转发和反向匹配的非对称**NAT**规则。请更新此问题流程

## 解决方案

为了解决此问题（当接口与使用NAT的主机不在同一接口上时），请使用映射地址（而不是实际地址）连接到主机。

此外，如果应用嵌入IP地址，请启用theinspectcommand。

# %ASA-5-713068：已收到非例行通知消息： notify_type

## 问题

如果 VPN 隧道未能启动，会显示以下错误消息：

**%ASA-5-713068：已收到非例行通知消息： notify_type**

## 解决方案

由于错误配置（即，当对等体上的策略或 ACL 未配置为相同时）而导致出现此消息。

策略和 ACL 匹配后，隧道会启动，不出现任何问题。

# %ASA-5-720012： (VPN-Secondary)无法更新备用设备上的IPSec故障转移运行时数据（或） %ASA-6-720012： (VPN-unit)无法更新备用设备上的IPsec故障转移运行时数据

## 问题

当您尝试升级思科自适应安全设备 (ASA) 时，会显示以下错误消息之一：

**%ASA-5-720012： (VPN-Secondary)无法更新**备用设备上的**IPSec故障**转移运行时数据。

**%ASA-6-720012： (VPN-unit)无法更新**备用设备上的**IPsec故障**转移运行时数据。

## 解决方案

这些错误消息是告知性错误。这些消息不影响 ASA 或 VPN 的功能。

当VPN故障切换子系统无法更新与IPsec相关的运行时数据时，这些消息会出现，因为备用设备上的相关IPsec隧道已被删除。

为了解决这些问题，请在活动单元上发出wr standbycommand。

# 错误：- %ASA-3-713063：没有为目标0.0.0.0配置IKE对等体地址

### 问题

显示**%ASA-3-713063： IKE Peer address not configured for destination 0.0.0.0**错误消息，并且隧道未能启动。

### 解决方案

当未为 L2L 隧道配置 IKE 对等地址时，会显示此消息。

如果更改加密映射的序列号，然后删除并重新应用加密映射，则可以解决此错误。

## 错误： %ASA-3-752006：隧道管理器无法调度KEY_ACQUIRE消息。

### 问题

%ASA-3-752006：隧道管理器无法调度KEY_ACQUIRE消息。Cisco ASA上可能记录了加密映射或隧道组配置错误。”错误消息。

### 解决方案

此错误消息由于加密映射或隧道组的错误配置而造成。确保两者均正确配置。有关此错误消息的详细信息，请参阅错误752006。

以下是一些纠正措施：

- 删除加密 ACL（例如，关联到动态映射）。
- 删除未使用的 IKEv2 相关配置（如有）。
- 验证加密 ACL 是否正确匹配。
- 删除重复的访问列表条目（如有）。

## 错误： %ASA-4-402116： IPSEC：从XX.XX.XX.XX (用户= XX.XX.XX.XX)到YY.YY.YY.YY收到了ESP数据包(SPI= 0x99554D4E，序列号= 0x9E)

在 LAN 到 LAN VPN 隧道设置中，在 ASA 的一端会收到以下错误消息：

解封的内部数据包与SA中协商的策略不匹配。

数据包将其目的地址指定为10.32.77.67，其源地址指定为10.105.30.1，其协议指定为icmp。

SA将其本地代理指定为10.32.77.67/255.255.255.255/ip/0，将其remote_proxy指定为10.105.42.192/255.255.255.224/ip/0。

### 解决方案

您需要验证在 VPN 隧道的两端定义的相关流量访问列表。两者必须匹配为精确的镜像。

## 由于错误 0xffffffff 而未能启动 64 位 VA 安装程序以启用虚拟适配器

### 问题

当AnyConnect连接失败时，会收到`Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0` xffffffflog消息。

### 解决方案

要解决此问题，请执行以下步骤：

1. 转至System > Internet Communication Management > Internet Communication 设置，确保 Turn Off Automatic Root Certificates 更新已禁用。
2. 如果已禁用，则请禁用已分配到受影响机器的GPO的整个管理模板，然后再次测试。

有关详细信息，请参阅Turn off Automatic Root Certificates更新。

## 在 Windows 7 中 Cisco VPN Client 无法与数据卡一起使用

### 问题

在 Windows 7 中 Cisco VPN Client 无法与数据卡一起使用。

### 解决方案

安装在 Windows 7 上的 Cisco VPN Client 无法与 3G 连接一起使用，因为在 Windows 7 中安装的 Cisco VPN Client 上不支持数据卡。

## 警报：“VPN功能可能根本无法工作”

### 问题

在尝试在ASA的外部接口上启用isakmp期间，会收到此警报消息：

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

此时，通过 ssh 访问 ASA。HTTPS 停止，且其他 SSL 客户端也受影响。

### 解决方案

此问题归结于不同模块（例如，记录器和加密）的内存要求不同。

确保您未执行logging queue 0命令。它使队列大小设置为8192，并且内存分配增加。

在ASA5505和ASA5510等平台中，这种内存分配往往会导致其他模块内存不足。

## IPSec 填充错误

### 问题

会收到以下错误消息：

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

### 解决方案

出现此问题的原因是IPSec VPN不使用哈希算法进行协商。数据包散列可确保ESP信道的完整性检查。

因此，在没有哈希的情况下，Cisco ASA会接受格式错误的数据包，而未检测到该数据包，并尝试解密这些数据包。

但是，由于这些数据包的格式不正确，ASA会在数据包解密过程中发现缺陷。这样会导致出现填充错误消息。

建议在 VPN 的转换集中包括散列算法并确保尽量减少对等体之间链路的畸形数据包。

## VPN 隧道在每 18 个小时之后断开

### 问题

即使生存时间设置为 24 小时，VPN 隧道也会在每 18 个小时之后断开。

### 解决方案

生存期是SA可用于密钥更新的最大时间。您在配置中输入作为生存时间的值不同于 SA 的密钥更新时间。

因此，必须在当前 SA 到期之前协商一个新的 SA（或在 IPsec 情况下为 SA 对）。

密钥更新时间必须始终短于生存时间，以便在第一次密钥更新尝试失败的情况下允许多次尝试。

RFC 未指定如何计算密钥更新时间。这留给实施者自行裁量。

因此，时间因平台而异。有些实施可使用随机因子来计算密钥更新计时器。

例如，如果ASA启动隧道，则通常在64800秒= 86400的75%时重新生成密钥。

如果路由器启动，则 ASA 可等待更长时间，以便为对等体留出更多时间来启动密钥更新。

因此，正常来说，VPN 会话会每 18 个小时断开以使用另一个密钥进行 VPN 协商。这样做时不得导致任何 VPN 丢弃或问题。

# LAN 到 LAN 隧道重新协商之后无法维持通信流量

## 问题

LAN 到 LAN 隧道重新协商之后无法维持通信流量。

## 解决方案

ASA会监控通过它的每个连接，并根据应用检查功能在其状态表中维护一个条目。

通过 VPN 的加密流量细节以安全关联 (SA) 数据库的形式进行维护。对于 LAN 到 LAN VPN 连接，它维护两种不同的通信流量。

一个是 VPN 网关之间的加密流量。另一个是 VPN 网关背后的网络资源和另一端后面的终端用户之间的通信流量。

当 VPN 终止时，删除此特殊 SA 的流量详细信息。

但是，此 TCP 连接的 ASA 维护的状态表条目由于无活动而变得过时，进而妨碍下载。

这意味着，当用户应用终止时，ASA仍会保留该特定流的TCP连接。

但是，在TCP空闲计时器过期后，TCP连接会丢失，并最终超时。

通过引入称为持续IPSec隧道流量的功能，可解决此问题。

Cisco ASA 集成了一条新命令 sysopt connection preserve-vpn-flows，以便在 VPN 隧道重新协商时保留状态表信息。

默认情况下禁用该命令。为此，当L2L VPN从中断中恢复并重新建立隧道时，Cisco ASA会维护TCP状态表信息。

# 错误消息指示已达到加密功能的带宽

## 问题

2900 系列路由器上会收到以下错误消息：

错误： **Mar 20 10:51:29：%CERM-4-TX_BW_LIMIT：**对于带有**securityk9**技术包许可证的加密功能，已达到最大**Tx**带宽限制85000 **Kbps**。

## 解决方案

这是已知问题，它是由于美国政府签发严格的指南而导致。

因此，securityk9许可证仅允许速率最高为90Mbps的负载加密，并且限制到设备的加密隧道/TLS会话的数量。

有关加密导出限制的详细信息，请参阅思科ISR G2 SEC和HSEC许可。

如果是思科设备，它派生出小于 85Mbps 的单向流量进出 ISR G2 路由器，双向总计为 170 Mbps。

此要求适用于思科 1900、2900 和 3900 ISR G2 平台。此命令有助于查看以下限制：

<#root>

Router#

**show platform cerm-information**

```
Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                    Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)       85000                  85000
 Rx Bandwidth(in kbps)       85000                  85000
 Number of tunnels             225                    225
 Number of TLS sessions       1000                   1000
---Output truncated----
```

要避免此问题，请购买HSECK9许可证。“hseck9”功能许可证提供增强的负载加密功能，增加 VPN 隧道计数和安全语音会话。

有关Cisco ISR路由器许可证的详细信息，请参阅软件激活。

# 问题：即使入站解密流量起作用，IPsec隧道的出站加密流量也会失败。

## 解决方案

在多次密钥更新但未清除触发条件之后，会在 IPsec 连接上发现到此问题。

如果检查show asp dropcommand的输出并验证发出的每个出站数据包的到期VPN情景计数器是否

增大，即可确定是否存在此问题。

# 其他

## AG_INIT_EXCH 消息显示在“show crypto isakmp sa”和“debug”命令输出中

如果未启动隧道，**AG_INIT**_EXCHmessage将显示在show crypto isakmp sacommand和indexbugoutput的输出中。

原因可能是isakmp策略不匹配，或者端口udp 500在途中被阻塞。

## 出现调试消息“Received an IPC message during invalid state”

此消息是告知性消息，与 VPN 隧道的断开没有任何关系。

# 相关信息

- ASA和Cisco IOS® : VPN分段
- Cisco ASA 5500 系列安全设备
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。