排除常见的 L2L 和远程访问 IPsec VPN 问题

目录

简介

背景信息

先决条件

IPsec VPN 配置不起作用

VPN客户端无法与ASA连接

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)”

远程访问和 EZVPN 用户连接到 VPN，但是无法访问外部资源

无法访问 DMZ 中的服务器

无法连接m=超过三个VPN客户端用户

建立隧道后无法启动会话或应用程序并且传输缓慢

无法从ASA启动VPN隧道

无法通过 VPN 隧道传递流量

在同一加密映射上为VPN隧道配置备份对等体

禁用/重新启动 VPN 隧道

一些隧道未加密

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

错误：-%ASA-6-722036：Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)

在VPN隧道的一端启用QoS时的错误消息

警告：加密映射条目不完整

错误：-%ASA-4-400024：IDS：来自外部接口的2151大型ICMP数据包

错误：-%ASA-4-402119：IPSEC:从Remote_IP（用户名）到Local_IP收到一个失败的反重播检查协议数据包（SPI=spi，序列号= seq_num）

错误消息 - %ASA-4-407001：拒绝本地主机interface_name:inside_address的流量，超出许可证数量限制

错误消息 - %VPN_HW-4-PACKET_ERROR:

错误消息：Command rejected:首先删除VLAN XXXX和XXXX之间的加密连接

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

%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

%ASA-5-713068：Received non-routine Notify message:notify_type

%ASA-5-720012:（VPN辅助）无法更新备用设备（或）%ASA-6-720012上的IPSec故障转移运行时数据：（VPN单元）无法更新备用单元上的IPsec故障转移运行时数据

错误：-%ASA-3-713063：IKE Peer address not configured for destination 0.0.0.0

Error:%ASA-3-752006:隧道管理器无法分派KEY_ACQUIRE消息

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

由于错误0xffffffff，无法启动64位VA安装程序以启用虚拟适配器

Cisco VPN客户端不能与Windows 7上的数据卡配合使用
预警:“VPN functionality may not work at all”
IPSec 填充错误
VPN隧道每18小时断开一次
重新协商LAN到LAN隧道后，流量不会得到维护
错误消息指示已达到加密功能的带宽
问题：IPsec隧道中的出站加密流量失败，即使入站解密流量正常工作
其他
相关信息

简介

本文档介绍最常见的IPsec VPN问题解决方案。

背景信息

本文档中介绍的解决方案直接来自思科技术支持团队已解决的服务请求。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需要尝试的常见步骤的摘要。

本文档中的配置示例用于路由器和安全设备，几乎所有概念都适用于VPN 3000。有关用于排除Cisco IOS®软件上的IPsec问题的常见debug命令的说明，请参阅IP安全故障排除 — 了解和使用debug命令。

注意：SA不会通过IPsec VPN隧道传递组播流量。

警告：本文档中提供的许多解决方案可能会导致设备上的所有 IPSec VPN 连接暂时断开。建议谨慎实施这些解决方案，并遵循您的变更控制策略。

先决条件

要求

思科建议了解以下思科设备上的IPsec VPN配置：

- 思科IOS®路由器
- Cisco PIX 5500 系列安全设备

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科IOS®
- Cisco PIX 5500 系列安全设备

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，但可以用作检查表，在您进行深度补救之前进行验证。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
- 检验ACL是否正确以及是否绑定到加密映射
- 验证 ISAKMP 策略
- 检验路由是否正确
- 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：出于空间方面的考虑，这些部分中的某些命令会向下移动到第二行。

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NAT-T未启用，VPN客户端用户通常看起来可以正常连接到ASA，但是他们无法访问安全设备背后的内部网络。如果NAT/PAT设备中的NAT-T未启用，则在ASA中可能会收到protocol 50 src inside:10.0.1.26 dst outside:10.9.694的常规转换创建失败(failed for protocol 50 src inside:10.0.1.26 dst outside:10.9.694)错误消息。

如果不能从同一IP地址同时完成登录，则安全VPN连接由客户端在本地终止。Reason 412:远程对等体不再响应错误消息。在头端VPN设备中启用NAT-T可解决此错误。



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。

下一个命令在思科安全设备上启用NAT-T。以下示例中的 20 是 keepalive 时间（默认值）。

ASA

<#root>

```
securityappliance(config)#

crypto isakmp nat-traversal 20
```

必须修改客户端，此操作才能正常工作。在Cisco VPN Client中，导航到Connection Entries，然后单击Modify。这将打开一个新窗口，您必须选择Transporttab。在此选项卡下，点击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来允许用于NAT-T、UDP 500和ESP端口的UDP 4500非常重要，因为ASA充当NAT设备。有关ASA中ACL配置的详细信息，请参阅使用NAT配置通过防火墙的IPsec隧道。

正确测试连接

VPN连接是从加密终端后面的设备测试的。许多用户都通过从加密端点运行ping命令来测试VPN连

接。虽然ping命令通常适用于此目的，但从正确的接口发出ping命令非常重要。如果ping的来源不正确，则当VPN连接正常工作时，它可能显示VPN连接失败。下面是一个示例：

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
```

在本例中，apinging必须源自任一路由器后面的网络内部。加密ACL仅配置为加密具有这些源地址的流量。源自任一路由器的外部接口的呼叫不加密。在特权EXEC模式下使用ping命令的扩展选项从路由器的内部接口发出ping:

<#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。用于测试连通性的ping命令也可以从带有insidekeyword的内部接口发出：

<#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ping命令来定位安全设备的内部接口。如果必须使用ping命令将内部接口作为目标，则必须在该接口上启用management-access，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1阶段也不起作用。在ASA上，如果连接失败，则SA输出类似于以下示例，指示可能存在不正确的加密对等体配置或ISAKMP建议配置不正确：

<#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，表示相关状态交换在主模式(MM)中失败。在第1阶段启用时加密SA输出；如以下示例：

<#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

如果没有表示IPsec VPN隧道按预期运行，则可能未启用ISAKMP。确保已在设备上启用ISAKMP。使用以下命令之一启用ISAKMP:

思科IOS®

<#root>

```
router(config)#

crypto isakmp enable
```

Cisco ASA(用您所需的接口替换外部):

<#root>

```
securityappliance(config)#

crypto isakmp enable outside
```

当您在外部接口上启用ISAKMP时，也会收到此错误：

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

在接口上启用ISAKMP之前，错误原因可能与ASA后面的客户端接收PAT到UDP端口500有关。删除PAT转换(clear xlate)后，即可启用ISAKMP。检验UDP 500和4500端口号是否保留用于与对等体协商ISAKMP连接。当接口上未启用ISAKMP时，VPN客户端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
```

要解决此错误，请在VPN网关的加密接口上启用ISAKMP。

启用/禁用 PFS

在IPsec协商中，完全向前保密(PFS)可确保每个新加密密钥与任何以前密钥无关。启用或禁用两个隧道对等体上的PFS;否则，在ASA/Cisco IOS®路由器中未建立LAN到LAN(L2L)IPsec隧道。完全转发保密(PFS)是Cisco专有技术，在第三方设备上不受支持。

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运行带有enable关键字的pfscommand。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，请运行此命令的no形式。一个组策略可以从另一个组策略继承 PFS 的值。运行此命令的no形式可防止值传输。

<#root>

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

no pfs
```

Cisco IOS®路由器

- 要指定在为加密映射条目请求新的安全关联时IPsec必须请求PFS，请在加密映射配置模式下运行set pfscommand。
- 要指定IPsec在收到新安全关联的请求时必须使用PFS，请在加密映射配置模式下运行set pfscommand。
- 要指定IPsec不得请求PFS，请运行此命令的no形式。默认情况下，如果未使用此命令指定组，并将group1用作默认值，则不会请求PFS。

```
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
```

清除旧安全关联或当前安全关联（隧道）

如果Cisco IOS®®路由器中出现此错误消息，则SA已过期或已清除。远程隧道终端设备不知道它使用过期的SA发送数据包（不是SA建立数据包）。 建立新的SA后，通信将恢复，因此通过隧道发起流量以创建新的SA并重新建立隧道。

<#root>

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

如果清除ISAKMP（第1阶段）和IPsec（第2阶段）安全关联(SA)，这通常是解决IPsec VPN问题的最佳解决方案。如果清除SA，则无需深入故障排除即可解决各种错误消息和行为。虽然此技术可在任何情况下轻松使用，但建议您在更改或添加当前IPsec VPN配置后首先清除SA。此外，虽然可以仅清除特定安全关联，但当您在设备上全局清除SA时，您会受益。清除安全关联后，可能需要通过隧道发送流量以重新建立它们。



警告：如果未指定要清除的安全关联，此处列出的命令会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
    1. Cisco Cisco IOS®

        <#root>

        ```
        router#
        show crypto isakmp sa
        router#
        show crypto ipsec sa
        ```

        ---

    2. Cisco ASA安全设备

        <#root>

        ```
        securityappliance#
        show crypto isakmp sa
        securityappliance#
        show crypto ipsec sa
        ```

2. 清除安全关联，因为可以按粗体显示的形式输入每个命令，也可以使用显示的选项输入。

A. 思科IOS®

1. ISAKMP（阶段 I）

<#root>

```
router#

clear crypto isakmp

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

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>
```

---

2. Cisco ASA安全设备

1. ISAKMP（阶段 I）

<#root>

```
securityappliance#

clear crypto isakmp sa
```

---

2. 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

如果用户经常通过L2L隧道断开连接，则此问题可能在ISAKMP SA中配置生命期。如果在ISAKMP生存期内出现任何差异，您可以收到%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（在/ASA中）。默认值为 86,400 秒（24 小时）。一般来说，较短的生命周期可提供更安全的ISAKMP协商（在某个点上），但是，随着生命周期缩短，安全设备可以更快地设置未来的IPsec SA。

当来自两个对等体的两个策略包含相同的加密、哈希、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期小于或等于比较的策略中的生存期时，将进行匹配。如果生存期不同，则使用较短的生存期（来自远程对等体的策略），并且找不到可接受的匹配项，IKE将拒绝协商，并且IKE SA未建立。

- 指定SA生存期：此示例将生存时间设置为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.

要解决此错误，请将thelifetimevalue设置为零(0)。 要将IKE安全关联的生存期设置为无穷大，VPN必须始终连接且不终止：

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

您还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，有助于防止偶发LAN到LAN或远程访问VPN中断。这包括VPN客户端、隧道以及在一段时间不活动后丢弃的隧道。此功能允许隧道终端监控远程对等体的持续存在并向该对等体报告其自身的存在状态。如果对等体没有响应，则端点会删除连接。要使ISAKMP keepalive正常工作，两个VPN终端都必须支持它们。

通过运行以下命令在Cisco IOS®中配置ISAKMP keepalive:

<#root>

```
router(config)#

crypto isakmp keepalive 15
```

运行以下命令以在ASA安全设备上配置ISAKMP keepalive:

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，必须禁用此功能才能解决问题。例如，如果VPN客户端位于阻止DPD数据包的防火墙后面。使用Cisco ASA时，对于名为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

1. 在遇到问题的客户端PC上，导航到%System Root% > Program Files > Cisco Systems >

VPN Client > Profiles以禁用IKE keepalive，并在适用情况下编辑连接的PCF文件。
2. 将ForceKeepAlives=0（默认值）更改为ForceKeepAlives=1。Keepalive是思科专有的，不受第三方设备支持。

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，可以归咎于简单的排版错误。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。确保已在每个VPN终端上正确输入任何预共享密钥。

在远程访问VPN中，检查有效的组名称和在CiscoVPN客户端中输入的预共享密钥。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，则可能会遇到此错误。

```
 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，则可以关闭一个或所有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。

运行以下命令，删除并重新输入对等体10.0.0.1或grouppngroupin 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
```

运行以下命令以删除并重新输入对等设备10.0.0.1的pre-shared-keysecretkeyfor /ASA安全设备:

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

VPN隧道的启动断开连接。出现此问题的原因是在第I阶段协商期间预共享密钥不匹配。show crypto isakmp命令中的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
```

要解决此问题，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

当清除安全关联并且无法解决IPsec VPN问题时，请删除并重新应用相关加密映射以解决各种问题，包括VPN隧道间歇性中断和某些VPN站点故障。



警告：如果从接口删除加密映射，则会删除与该加密映射关联的任何IPsec隧道。请谨慎继续，请参阅这些步骤，并在继续之前考虑组织的更改控制策略。

运行以下命令以删除和替换Cisco IOS®中的加密映射：

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

```
<#root>

router(config-if)#

no crypto map mymap
```

继续运行enoform以删除整个加密映射：

```
<#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。此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
```

运行这些命令以删除和替换ASA上的加密映射。首先从接口中删除加密映射。运行crypto mapcommand的no形式：

<#root>

```
securityappliance(config)#

no crypto map mymap interface outside
```

继续运行enoform以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。此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
```

如果删除并重新应用加密映射，这还可以解决头端IP地址已更改时的连接问题。

验证Sysopt命令是否存在（仅限ASA）

命令sysopt connection permit-ipsecandsysopt connection permit-vpnallow packets from an IPsec

tunnel and its payload to bypass interface ACLs on the security appliance。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，适用于此情况的相关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，适用于此情况的相关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。运行以下show命令以确定您的设备上是否启用了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)
```

运行以下命令以启用正确的设备系统命令：

Cisco ASA:

<#root>

```
securityappliance(config)#

sysopt connection permit-vpn
```

如果不希望运行sysopt connectioncommand，请明确允许从源到目标的所需流量。例如，在外部ACL中，从远程设备的远程到本地LAN，以及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

IPsec VPN中的IKE协商失败通常是由于对等体无法识别其伙伴的标识而导致的，这是此方法。当两个对等体使用IKE建立IPsec安全关联时，每个对等体将其ISAKMP标识发送到远程对等体。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，防火墙设备的ISAKMP身份设置为IP地址。

作为一般规则，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。要设置要发送到对等体的第2阶段ID，请在全局配置模式下运行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
```

如果VPN隧道在使用ASA配置迁移工具从ASA转移配置后无法启动；日志中出现以下消息：

[IKEv1]:Group = x.x.x.x, IP = x.x.x.x, Stale PeerTblEntry found, removing!

[IKEv1]:Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!

[IKEv1]:Group = x.x.x.x, IP = x.x.x.x, construct_ipsec_delete():No SPI to identify Phase 2 SA!

[IKEv1]:Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!

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），如果没有流量通过，则在30分钟后丢弃隧道。无论空闲超时参数如何，VPN客户端都会在30分钟后断开连接，并收到PEER_DELETE-IKE_DELETE_UNSPECIFIED错误。

将timeoutandsession timeoutasnone配置为使隧道alwaysup，这样，即使使用第三方设备，隧道也不会被丢弃。

ASA

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

<#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为VPN连接配置最大时间：

<#root>

```
hostname(config)#
```

group-policy DfltGrpPolicy attributes

hostname(config-group-policy)#

vpn-session-timeout none

配置了tunnel-all后，不需要配置reidle-timeoute，因为即使配置了VPN-idle timeout，它也不会在所有流量通过隧道时运行（因为已配置了tunnel-all）。

因此，流量（甚至PC生成的流量）不允许出现空闲超时。

Cisco IOS®路由器

在全局配置模式或加密映射配置模式下运行crypto ipsec security-association idle-timecommand以配置IPsec SA空闲计时器。默认情况下，禁用IPsec SA空闲计时器：

<#root>

crypto ipsec security-association idle-time

seconds

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

检验ACL是否正确以及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。另一个访问列表用于定义要加密的流量；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配置不正确或丢失时，流量会沿一个方向流经VPN隧道，或者根本不会通过隧道发送。

确保在全局配置模式下运行crypto map match address命令，将加密ACL与加密映射绑定。检查是否已配置所有访问列表以完成IPsec VPN配置，并且这些访问列表定义了正确的流量。此列表包含当您怀疑ACL是IPsec VPN问题的原因时要验证的项目。

确认NAT免除并加密ACL指定正确的流量。如果您有多个VPN隧道和多个加密ACL，请确保这些ACL不会重叠。另请检验您的设备是否已配置为使用NAT免除ACL。在路由器上，这意味着您正在运行theroute-mapcommand。在ASA上，您正在运行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。

在下一个示例中，Cisco IOS®路由器配置为免除从NAT发送192.168.100.0 /24和192.168.200.0 /24或192.168.1.0 /24之间的流量。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仅对IP地址或IP网络起作用，例如上述示例(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等）。 在VOIP环境中，网络之间的语音呼叫是通过VPN进行通信的，如果没有正确配置NAT 0 ACL，则语音呼叫不会运行。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配置错误造成的。

如果NAT免除(nat 0)ACL配置错误，您可能会收到如图所示的错误消息。

```
%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)无法正常工作，请尝试将其删除并运行NAT 0命令。确保您的ACL不是倒退的，并且它们是正确的类型。LAN对LAN配置的加密和NAT免除ACL必须从配置ACL的设备的角度编写。因此，ACL必须到达其他ACL。在本示例中，在192.168.100.0 /24和192.168.200.0 /24之间设置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
```

虽然未说明，但同样的概念适用于ASA安全设备。在ASA中，远程访问配置的分割隧道ACL必须作为允许流量进入VPN客户端需要访问的网络的访问列表。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，在拆分隧道ACL的源位置使用“any”与禁用拆分隧道类似。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
```

思科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隧道未启用，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客户端或站点到站点VPN无法与远程终端设备建立隧道，请检查两个对等项是否包含相同的加密、哈希、身份验证和Diffie-Hellman参数值。验证远程对等项策略指定的生存期是否小于或等于发起方发送的策略中的生存期。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的示例：

```
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ISAKMP策略不匹配或遗漏的NAT 0语句引起。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.
```

此消息表示第1阶段完成后，第2阶段消息在队列中。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

此消息通常在**Removing peer from peer table failed，no match！**错误消息后出现。如果Cisco VPN客户端无法连接头端设备，则问题可能是ISAKMP策略不匹配。头端设备必须与Cisco VPN客户端的一个IKE建议匹配。对于ASA上使用的ISAKMP策略和IPsec转换集，思科VPN客户端不能使用包含DES和SHA组合的策略。如果使用DES，则必须将MD5用于哈希算法，或者可以使用其他组合，例如3DES与SHA以及3DES与MD5。

检验路由是否正确

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。如果网关设备后面存在其他路由器，请验证这些路由器可以到达隧道，以及另一端存在哪些网络。VPN部署中路由的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。这些路由对安装它们的设备非常有用，对网络中的其他设备也很有用，因为RRI安装的路由可以通过EIGRP或OSPF等路由协议重分发。

在LAN到LAN配置中，每个终端都必须有通往网络的路由，它们必须在该路由中加密流量。在本例中，路由器A必须具有通过10.89.129.2到路由器B后面的网络的路由。路由器B必须具有通向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的网络配置静态路由。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
```

如果每个端点后面存在大量网络，则静态路由的配置将变得难以维护。相反，建议您使用反向路由注入。RRI为加密ACL中列出的所有远程网络放置路由表路由。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ASA替换，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。但是，如果VPN网关路由器或安全设备后面存在其他路由器，则这些路由器必须学习到VPN客户端的路径。在本示例中，假设VPN客户端在连接时的地址范围为10.0.0.0 /24。

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客户端分配的IP地址池与头端设备的内部网络重叠，则会发生路由问题。有关详细信息，请参阅重叠专用网络部分。

验证转换集是否正确

确保两端转换集使用的IPsec加密和哈希算法相同。有关详细信息，请参阅Cisco安全设备配置指南的命令参考。对于ASA上使用的ISAKMP策略和IPsec转换集，思科VPN客户端不能使用包含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、名称和加密映射是否应用到IPsec隧道开始/结束位置的正确接口

如果在同一加密映射上配置了静态和动态对等体，则加密映射条目的顺序至关重要。动态加密映射条目的序列号必须高于所有其他静态加密映射条目。如果静态条目的编号高于动态条目的编号，则与这些对等体的连接会失败，调试结果如图所示：

```
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只允许有一个动态加密映射。下面是一个正确编号的加密映射的示例，其中包含一个静态条目和一个动态条目。动态条目具有最高的序列号，并且预留空间以添加其他静态条目：

<#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。当动态加密映射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。这也由定义流量的加密访问列表不匹配导致：%ASA-3-713042:IKE Initiator unable to find policy:

如果多个VPN隧道在同一接口中终止，请创建具有相同名称（每个接口只允许一个加密映射），但序列号不同的加密映射。对于路由器和ASA，情况也是如此。请参阅ASA:向现有L2L VPN添加新隧道或远程访问 — Cisco有关L2L和远程访问VPN方案的加密映射配置的详细信息。

验证对等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中将隧道组的<name>指定为远程对等IP地址（远程隧道端）。对等体IP地址必须匹配隧道组名称和加密映射set 地址。当您使用ASDM配置VPN时，它会使用正确的对等IP地址自动生成隧道组名称。如果对等IP地址配置不正确，日志可能会包含此消息，这可以通过正确配置对等IP地址来解决：

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

当对等体IP地址在ASA加密配置上配置不正确时，ASA无法建立VPN隧道并仅在MM_WAIT_MSG4阶段中挂起。要解决此问题，请更正配置中的对等IP地址。以下是VPN隧道在MM_WAIT_MSG4状态下挂起时show crypto isakmp命令的输出：

<#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不同于隧道组配置中的允许隧道而丢弃隧道时，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
```

在默认组策略中启用IPSec到默认组策略中的现有协议。

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

禁用 L2L 对等体的 XAUTH

如果在同一加密映射上配置了LAN到LAN隧道和远程访问VPN隧道，则系统会提示LAN到LAN对等体提供XAUTH信息，并且LAN到LAN隧道在show crypto isakmp saccommand的输出中出现CONF_XAUTH失败。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®，其中ASA由于使用隧道组而不受此问题的影响。输入ISAKMP密钥时

运行o-xauthkeyword，因此设备不会提示对等设备提供XAUTH信息（用户名和密码）。 此关键字会禁用静态 IPSec 对等体的 XAUTH。在同一加密映射上配置了L2L和RA VPN的设备上运行与此类似的命令：

<#root>

```
router(config)#

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

在ASA充当Easy VPN服务器的场景中，Easy VPN客户端由于Xauth问题无法连接到头端。在ASA中禁用用户身份验证以解决问题：

<#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
```

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

VPN池已耗尽

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. 删除现有范围并定义新范围：

<#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. 当不连续子网必须添加到VPN池时，您可以定义两个单独的VPN池，然后在“tunnel-group attributes”下指定它们。 以下是一个示例：

```
<#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
```

指定池的顺序非常重要，因为ASA按照池在此命令中的显示顺序从这些池分配地址。group policy address pools命令中的地址池设置始终覆盖tunnel-group address-pool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IPsec/tcp而不是IPsec/udp，则配置represerve-vpn-flow。
3. 重新载入 Cisco ASA。

VPN客户端无法与ASA连接

问题

当Xauth与Radius服务器一起使用时，Cisco VPN客户端无法进行身份验证。

解决方案

有时，扩展验证超时，您可以增加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

最初，请确保身份验证正常运行。要缩小问题范围，首先在ASA上使用本地数据库验证身份验证。

```
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执行时没有任何问题，则检查ASA上与Radius相关的配置以及Radius服务器上的数据库配置。您可以运行debug radius命令来排除与radius相关的问题。有关sampledebug radiusoutput的信息，请参阅此示例输出。在ASA上使用debugcommand之前，请参阅此文档警告消息。

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客户端用户在尝试与头端VPN设备连接时收到此错误。

- VPN客户端在第一次尝试时经常断开连接。
- 安全VPN连接由对等项原因433终止。
- 安全VPN连接由对等项原因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

此问题可能涉及通过ASA、Radius服务器、DHCP服务器或通过充当DHCP服务器的Radius服务器分配的IP池。运行debug cryptocommand以验证网络掩码和IP地址是否正确。此外，请确认地址池不包含网络地址和广播地址。Radius服务器必须为客户端分配正确的IP地址。

解决方案 2

扩展身份验证失败也会导致此问题。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。当存在针对不同且不完整的安全关联(SA)的多个重新传输时，启用了威胁检测功能的ASA认为发生了扫描攻击，并且VPN端口被标记为主要威胁。禁用威胁检测功能，因为这会导致ASA处理出现开销问题。运行以下命令以禁用威胁检测：

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

这可以作为一种解决方法，以验证这是否解决了问题。确保您在Cisco ASA上禁用威胁检测，因为这会影响多个安全功能，例如减少扫描尝试、使用无效SPI的DoS、应用检测失败的数据包和不完整会话。

解决方案 4

当转换集配置不正确并且转换集的正确配置可解决此问题时，也会发生此问题。

远程访问和 EZVPN 用户连接到 VPN，但是无法访问外部资源

问题

- 一旦连接到VPN，远程访问用户就没有Internet连接。
- 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

尝试以下解决方案来解决问题：

- 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

但是，一旦建立了VPN客户端，即与VPN前端设备(ASA/Cisco IOS®路由器)的IPsec隧道，VPN客户端用户可以访问INSIDE网络(10.10.10.0/24)资源。它们无法访问DMZ网络(10.1.1.0/24)。

图解

验证分割隧道，不会将NAT配置添加到头端设备以访问DMZ网络中的资源。

ASA 配置

此配置显示如何为DMZ网络配置NAT免除，以使VPN用户能够访问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
```

为NAT配置添加新条目后，清除NAT转换。

```
Clear xlate
Clear local
```

验证

如果隧道已建立，请转到Cisco VPN客户端，然后选择Status > Route以验证DMZ和INSIDE网络的安全路由。

请参阅ASA:向现有L2L VPN添加新隧道或远程访问 — Cisco，了解将新VPN隧道或远程访问VPN添加到已存在的L2L VPN配置所需的步骤。您还可以参阅ASA:在ASA上允许VPN客户端分割隧道配置示例，了解有关如何允许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，则问题可能与头端设备(ASA)中的DNS服务器配置有关。 检查VPN客户端和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：

<#root>

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

```
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客户端无法按名称连接到内部服务器

VPN客户端无法按名称对远程或头端内部网络的主机或服务器执行ping操作。您必须在ASA上启用拆分DNS配置才能解决此问题。

分割隧道 — 无法访问 Internet 或排除的网络

分割隧道允许远程访问IPsec客户端有条件地以加密形式通过IPsec隧道将数据包定向到网络接口，或以明文解密形式将其路由到最终目的地。

默认情况下，分割隧道处于禁用状态，您可以看到它运行commandtunnelalltraffic。

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

只有思科VPN客户端（而不是EZVPN客户端）支持选项excludespecified。

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

有关拆分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

发夹解决方案

此功能对于进入接口但随后从同一接口路由出去的VPN流量非常有用。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。分支到分支的通信流量必须进入安全设备，然后再次传出到另一个分支。运行same-security-trafficconfiguration以允许流量进入和退出同一接口：

<#root>

```
securityappliance(config)#
```

same-security-traffic permit intra-interface

本地 LAN 访问

远程访问用户连接到VPN，并且只能连接到本地网络。有关更详细的配置示例，请参阅ASA:允许 VPN Client 的本地 LAN 访问。

专用网络重叠

问题

如果在建立隧道后无法访问内部网络，请检查分配给与前端设备后的内部网络重叠的VPN客户端的IP地址。

解决方案

验证分配给VPN客户端、前端设备的内部网络和VPN客户端内部网络的池中的IP地址是否位于不同的网络中。您可以为同一个主网络分配不同的子网，但有时会出现路由问题。有关更多示例，请参阅无法访问DMZ中的服务器部分的DiagramandExampleof。

无法连接m=超过三个VPN客户端用户

问题

只有三个VPN客户端可以连接到ASA/且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和最大会话限制有关。尝试以下解决方案来解决问题：

- 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ASDM中的Inheritcheckbox，则仅允许用户默认同时登录数。同时登录的默认值为3。要解决此问题，请增加同时登录的值。

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，撤消连接设置下Simultaneous Logins的Inheritcheck框。在字段中选择相应的值。

此字段的最小值为0，表示禁用登录并阻止用户访问。当您使用来自不同PC的相同用户帐户登录时，当前会话（从使用相同用户帐户的另一台PC建立的连接）将终止，并且新会话将建立。这是默认行为，与VPN同时登录无关。

使用CLI配置ASA

完成以下步骤以配置所需数量的同时登录。在本示例中，选择20作为所需值：

```
<#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，请参阅思科安全设备命令参考。在全局配置模式下运行vpn-sessiondb max-session-limitcommand，将VPN会话数限制为低于安全设备允许的值。运行此命令的覆盖以删除会话限制，然后再次运行该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

完成以下步骤以配置所需数量的同时登录。您也可以将此SA的同步登录设置为5。选择 Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneous Logins，并将登录次数更改为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

运行ping命令以检查网络或查找是否可从网络访问应用服务器。对于流经路由器或/ASA设备的临时数据包，尤其是设置了SYN位的TCP数据段，这可能是最大数据段大小(MSS)的问题。

Cisco IOS®路由器 — 更改路由器外部接口（隧道终端接口）中的MSS值

运行以下命令更改路由器外部接口（隧道终端接口）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)]
```

路由器上的MSS已按配置调整为1300。有关详细信息，请参阅ASA和Cisco IOS®:VPN 分段。

ASA — 请参阅/ASA文档

无法正确访问Internet或通过隧道传输缓慢，因为它会出现MTU大小错误消息和MSS问题。请参阅本文档以解决此问题：

- ASA和Cisco IOS®:VPN 分段

无法从ASA启动VPN隧道

问题

您不能从ASA接口并在建立隧道后启动VPN隧道。远程终端/VPN客户端无法ping通VPN隧道上ASA的内部接口。例如，VPN客户端无法通过VPN隧道启动到接口内部ASA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
```

此命令还帮助通过VPN隧道为ASA的内部接口建立ssh启动或http连接。此信息对于DMZ接口也同样适用。例如，如果您想对/ASA的DMZ接口执行ping操作，或者想从DMZ接口启动隧道，则需要运行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VPN客户端连接条目下选择此端口在TCP 10000上进行连接。右键单击Modify > Transport Tab > IPsec over TCP。

无法通过 VPN 隧道传递流量

问题

您不能通过VPN隧道传输流量。

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，也可能发生这种情况，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，并且NAT 0访问列表正确。

2. 如果路由正确且流量到达接口外部（该接口在内部通过），则输出示例显示解密已完成，但不发生加密。
3. 如果在ASA上配置了sopt permit connection-vpn命令。如果未配置，请配置此命令，因为它将加密的/VPN流量从接口ACL检查中免除到ASA。

在同一加密映射上为VPN隧道配置备份对等体

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。可以在主要对等体之后添加辅助对等体。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

要暂时禁用VPN隧道并重新启动服务，请完成本节中介绍的过程。

解决方案

在全局配置模式下运行crypto map接口命令，以删除之前定义的接口加密映射集。运行此命令的enoform以从接口删除加密映射集。

<#root>

hostname(config)#

no crypto map

map-name

interface

interface-name

此命令删除任何活动安全设备接口的加密映射集，并将IPsec VPN隧道更改为接口中的非活动状态。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：Group = 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版本。Tunnel terminatedererror**消息出现。

解决方案

“Transaction Mode v2”错误消息的原因是ASA仅支持IKE模式配置v6，而不支持旧的v2模式版本。使用IKE模式配置v6解决此错误。

错误：-%ASA-6-722036：Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)

问题

%ASA-6-722036:**Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206)** 错误消息显示在 **ASA** 的日志中。此日志意味着什么？如何解决该问题？

解决方案

此日志消息表明已向客户端发送了一个大型数据包。数据包的源不知道客户端的MTU。这可能是由于压缩了不可压缩的数据。您可以使用svc compression none命令关闭SVC压缩，这样可以解决此问题。

在VPN隧道的一端启用QoS时的错误消息

问题

如果在VPN隧道的一端启用了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

此消息通常在隧道的一端执行QoS时产生。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以阻止此过程，但是，只要流量可以穿过隧道，就可以忽略此过程。

警告：加密映射条目不完整

问题

运行crypto map mymap 20 ipsec-isakmpcommand时，可能会收到以下错误：**WARNING: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，这是正常警报；提醒：访问列表（匹配地址）、转换集和对等地址等参数必须配置后才能正常运行。查看键入的第一行以定义加密映射也是标准做法，它不会显示在配置中

。

错误：-%ASA-4-400024：IDS：来自外部接口的2151大型ICMP数据包

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会正常工作。运行以下命令以禁用签名：

- 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收到一个失败的反重播检查协议数据包（SPI=spi，序列号= seq_num）

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（用户名）到local_IP收到了一个未能通过反重播检查的协议数据包（SPI=spi，序列号= seq_num）**。

解决方案

要解决此错误，请运行crypto ipsec security-association replay window-size命令来改变窗口大小。

<#root>

hostname(config)#

crypto ipsec security-association replay window-size 1024

Cisco建议您使用完整的1024窗口大小来消除任何反重播问题。

错误消息 - %ASA-4-407001：拒绝本地主机interface_name:inside_address的流量，超出许可证数量限制

问题

很少有主机无法连接到Internet;系统日志中显示以下错误消息：错误消息 - %ASA-4-407001：拒绝本地主机接口名称：inside_address的流量，已超过许可证数量限制

解决方案

当用户数超过使用的许可证的用户限制时，会收到此错误消息。通过将许可证升级到包括更多用户数即可解决此错误。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

错误消息 — %VPN_HW-4-PACKET_ERROR：错误消息指示路由器收到的具有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

要解决此错误消息，请执行以下操作：

- 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:首先删除VLAN XXXX和XXXX之间的加密连接

问题

当您尝试将允许的 VLAN 添加到交换机上的中继端口时，会显示以下错误消息：Command rejected:首先删除VLAN XXXX和VLAN XXXX之间的加密连接。不能修改WAN边缘中继以允许其他VLAN。如果在IPSEC VPN SPAtrunk中无法添加VLAN。此命令被拒绝，因为它会导致属于允许VLAN列表的加密连接接口VLAN，从而可能导致IPSec安全漏洞。



注意：此行为适用于所有中继端口。

解决方案

不使用no switchport trunk allowed vlan(vlanlist)命令，请运行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.x:27331到x.x.x.x:23的无效窗口缩放选项[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.x:27331到x.x.x.x:23 pediaK的窗口缩放选项无效[Initiator(flag 0,factor 0)Responder(flag 1, factor2)]

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，以便在长距离网络(LFN)上快速传输数据。 这些通常是高带宽和高延迟的连接。具有卫星连接的网络就是LFN的一个例子，因为卫星链路通常具有高带宽的传播延迟。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窗口大小增加到大于65,535，则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:异步NAT规则匹配转发和反向。请更新此问题流程。

解决方案

要解决此问题，当与使用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inspectcommand。

%ASA-5-713068：Received non-routine Notify message: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：Received non-routine Notify message:notify_type

---

解决方案

此消息是由于配置错误（当对等体上的策略或ACL配置不同时）而出现的。一旦策略和ACL匹配，隧道将立即启动，没有任何问题。

%ASA-5-720012:（VPN辅助）无法更新备用设备（或）%ASA-6-720012上的IPSec故障转移运行时数据：（VPN单元）无法更新备用单元上的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辅助）无法更新备用设备上的IPSec故障转移运行时数据。**
- **%ASA-6-720012:（VPN单元）无法更新备用单元上的IPsec故障转移运行时数据。**

解决方案

这些错误消息是信息性错误，不会影响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，它们会出现，因为相关IPsec隧道已在备用设备上删除。要解决这些问题，请在主用设备上运行wr standbycommand。

错误：-%ASA-3-713063：IKE Peer address not configured for destination 0.0.0.0

问题

%ASA-3-713063:IKE Peer address not configured for destination 0.0.0.0错误消息出现，并且隧道无法显示。

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。

Error:%ASA-3-752006:隧道管理器无法分派KEY_ACQUIRE消息

问题

“%ASA-3-752006:Tunnel Manager failed to dispatch a KEY_ACQUIRE message.加密映射或隧道组可能配置错误。错误消息记录到 Cisco ASA。

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。确保两者都配置正确。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：

- 删除与动态映射关联的加密ACL。
- 删除未使用的 IKEv2 相关配置（如有）。
- 验证加密ACL是否正确匹配。
- 删除任何重复的访问列表条目。

Error:%ASA-4-402116:IPSEC:从XX.XX.XX.XX(user= XX.XX.XX.XX)到YY.YY.YY.YY收到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。

数据包将目的地址指定为10.32.77.67，将源地址指定为10.105.30.1，将协议指定为icmp。

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

解决方案

您必须验证VPN隧道两端定义的唯一流量访问列表。两者必须完全匹配为镜像映像。

由于错误0xffffffff，无法启动64位VA安装程序以启用虚拟适配器

问题

由于AnyConnect连接失败时收到错误消息0xffffff，无法启动64位VA安装程序以启用虚拟适配器。

解决方案

完成以下步骤以解决此问题：

1. 转至System > Internet Communication Management > Internet Communication设置，并确保Turn Off Automatic Root Certificates已禁用。
2. 如果禁用它，则禁用分配给受影响计算机的GPO的整个管理模板部分，然后重新测试。有关详细信息，请参阅关闭自动根证书更新。

Cisco VPN客户端不能与Windows 7上的数据卡配合使用

问题

Cisco VPN客户端不能与Windows 7上的数据卡配合使用。

解决方案

Windows 7上安装的Cisco VPN客户端无法与3G连接配合使用，因为Windows 7计算机上安装的

VPN客户端不支持数据卡。

预警:“VPN functionality may not work at all”

问题

在尝试在ASA的外部接口上启用ISAKMP期间，会收到以下警报消息：

```
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.
```

通过SSH和HTTPS对ASA的访问已停止，其他SSL客户端也会受到影响。

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。确保没有logging queue 0命令。这会导致队列大小设置为8192且内存分配增加。在ASA5505和ASA5510等平台中，这种内存分配往往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

发生此问题的原因是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，如果没有哈希值，Cisco ASA不会检测到格式错误的数据包，它会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的转换集中加入散列算法，并确保对等体之间的链路具有最小的数据包畸变。

VPN隧道每18小时断开一次

问题

VPN隧道每18小时断开一次，即使生命周期设置为24小时也如此。

解决方案

生存期是可用于密钥更新的SA的最长时间。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。在当前的SA到期之前，必须协商新的SA（对于IPsec来说是SA对）。重新生成密钥的时间必须小于生存期，以便在第一次重新生成密钥尝试失败时允许多次尝试。

RFC未指定如何计算密钥更新时间。这由您自行决定，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，则正常情况下它将在64800秒= 86400的75%重新生成密钥。如果路由器启动，则ASA可以等待更长时间为对等体提供更多时间以启动重新生成密钥。因此，VPN会话每18小时断开一次，以使用另一个密钥进行VPN协商是正常的。

重新协商LAN到LAN隧道后，流量不会得到维护

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根据应用检查功能监控每个经过的连接并在其状态表中维护条目。通过VPN的加密流量详细信息以安全关联(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，在用户应用终止时，ASA仍保留该特定流的TCP连接。在TCP空闲计时器到期后，TCP连接会成为杂散连接，并最终超时。通过引入名为持久IPSec隧道流的功能，已解决了此问题。新命令sysopt connection preserve-vpn-flows已集成到Cisco ASA中，以在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：

Error: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8500 Kbps的传输带宽限制。

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。根据securityk9许可证，它仅允许速率接近90 Mbps的负载加密，并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Cisco ISR G2 SEC和HSEC许可。

对于Cisco设备，其双向总流量为170 Mbps，即传入或传出ISR G2路由器的单向流量小于85 Mbps。此要求适用于Cisco 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----
```

为避免此问题，请购买HSECK9许可证。“hseck9”特性许可证提供增强的负载加密功能，增加了VPN隧道计数和安全语音会话。有关Cisco ISR路由器许可的详细信息，请参阅软件激活。

问题：IPsec隧道中的出站加密流量失败，即使入站解密流量正常工作

解决方案

在IPsec连接上多次重新生成密钥后已发现此问题，但触发条件尚不清楚。如果检查show asp dropcommand的输出并验证发送的每个出站数据包的Expired VPN上下文计数器是否增加，则可以确定存在此问题。

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，则show crypto isakmp命令的输出和debugoutput中将显示AG_INIT_EXCH消息。原因可能与ISAKMP策略不匹配或udp端口500被阻止有关。

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）。