# 最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案

## 目录


简介
先决条件
要求
使用的组件
规则
IPSec VPN配置不工作
问题
解决方案
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 PIX/ASA）
验证 ISAKMP 身份
验证空闲/会话是否超时
验证ACL是对加密映射的正确和已绑定的
验证 ISAKMP 策略
验证路由是否正确
验证转换集正确
验证加密映射序号，并且名称并且那加密映射在IPSec隧道开始/末端的正确的接口应用
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缓冲获得用尽
与延迟的问题VPN客户端流量的
VPN Client 无法与 ASA/PIX 连接
问题
解决方案
问题
解决方案

VPN客户端常见丢包连接在第一次尝试或“安全VPN连接由对等体终止。原因433."或“安全VPN连接由对等体433:(Reason终止没指定的对等体原因)”
问题
解决方案 1
解决方案 2
解决方案 3
解决方案 4
远程访问和 EZVPN 用户连接到 VPN，但是无法访问外部资源
问题
解决方案
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
发夹
本地 LAN 访问
专用网络重叠
无法连接超过三个 VPN Client 用户
问题
解决方案
配置同时登录数
使用 CLI 配置 ASA/PIX
配置集中器
建立隧道后无法启动会话或应用程序并且传输缓慢
问题
解决方案
Cisco IOS 路由器 — 更改路由器的外部接口（隧道末端接口）中的 MSS 值
PIX/ASA 7.X — 参阅 PIX/ASA 文档
无法从 ASA/PIX 启动 VPN 隧道
问题
解决方案
无法通过在VPN通道间的流量
问题
解决方案
配置VPN的备份对等请建立隧道在同样加密映射
问题
解决方案
禁用/重新启动VPN通道
问题
解决方案
没加密的一些通道
问题
解决方案
Error: - %ASA-5-713904 ：Group = DefaultRAGroup, IP = x.x.x.x, Client is using an unsupported Transaction Mode v2 version.Tunnel terminated.
问题

解决方案
Error: - %ASA-6-722036 ：Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)
问题
解决方案
Error:The authentication-server-group none command has been deprecated
问题
解决方案
当在 VPN 隧道一端启用 QoS 时出现错误消息
问题
解决方案
警告：crypto map entry will be incomplete
问题
解决方案
Error: - %ASA-4-400024 ：IDS:2151 Large ICMP packet from to on interface outside
问题
解决方案
Error: - %PIX|ASA-4-402119 ：IPSEC ：Received a protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.
问题
解决方案
错误消息 - %PIX|ASA-4-407001:Deny traffic for local-host interface_name: inside_address，超过的编号许可证限制
问题
解决方案
错误消息- %VPN_HW-4-PACKET_ERROR ：
问题
解决方案
错误消息：Command rejected:VLAN和之间的删除crypto连接，首先。
问题
解决方案
错误消息- % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE ：丢弃数据包-会话的x.x.x.x:27331无效窗口缩放选项x.x.x.x:23的[发起者(标志0,factor 0)响应方(标志1，要素2)]
问题
解决方案
%ASA-5-305013 ：为转发和反向匹配的不对称NAT规则。请更新此问题流
问题
解决方案
%PIX|ASA-5-713068 ：已接收非惯例通知消息：notify_type
问题
解决方案
%ASA-5-720012 ：(VPN第二)失败更新在备用装置(或) %ASA-6-720012的IPSec故障切换运行时数据：(VPN单元)失败更新在备用装置的IPsec故障切换运行时数据
问题
解决方案
Error: - %ASA-3-713063 ：为目的地没配置的IKE对等地址0.0.0.0

问题
解决方案
Error:%ASA-3-752006 ：通道管理器失败调度KEY_ACQUIRE消息。
问题
解决方案
Error:%ASA-4-402116 ：IPSEC ：接收一ESP数据包(SPI= 0x99554D4E，顺序number= 0x9E)从XX.XX.XX.XX (user= XX.XX.XX.XX)对YY.YY.YY.YY
解决方案
失败启动64位VA安装程序启用虚拟适配器由于错误0xffffffff
问题
解决方案
错误5 ：主机名不为此连接项存在。无法建立VPN联系。
问题
解决方案
Cisco VPN Client不与数据卡一起使用在Windows 7
问题
解决方案
警告消息："VPN功能可能不操作"
问题
解决方案
填充错误的IPSec
问题
解决方案
在远程站点电话的断线延迟时间
问题
解决方案
VPN通道在每18个小时之后断开
问题
解决方案
在对LAN通道的LAN重新协商后，通信流没有维护
问题
解决方案
错误消息阐明，带宽为crypto功能到达了
问题
解决方案
问题：在IPSec隧道的出站加密流量可能发生故障，即使入站解密流量工作。
解决方案
其他
AG_INIT_EXCH 消息显示在"show crypto isakmp sa"和"debug"命令输出中
出现调试消息"Received an IPC message during invalid state"
相关信息

# 简介

本文档包含 IPSec VPN 问题的最常见解决方案。这些解决方案直接来自 Cisco 技术支持已解决的

服务请求。其中许多解决方案可以在对 IPSec VPN 连接进行深入故障排除之前实施。结果，在您开始排除故障连接和呼叫思科技术支持前，本文提供普通的步骤清单尝试。

如果需要站点到站点VPN和远程访问VPN的配置示例文档，参考*远程访问VPN*、*Site to Site VPN (L2L)与PIX*， *Site to Site VPN (L2L)与IOS*和*Site to Site VPN (L2L)与*配置示例和TechNotes的*VPN3000*部分。

**注意：** 即使在本文的配置示例发挥作用在路由器和安全工具的，接近所有这些概念也是可适用的对VPN 3000集中器。

**注意：** 提供使用排除故障在Cisco IOS软件和PIX的IPsec问题普通的调试指令的说明的参考的IP安全故障排除-了解和使用debug命令。

**注意：** ASA/PIX不会通过在IPSec VPN通道的组播数据流。

**注意：** 您可以使用命令查找工具（仅限注册用户）查找本文档中使用的任何命令。

**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。建议根据更改控制策略略小心实施这些解决方案。

# 先决条件

## 要求

思科建议您有IPSec VPN配置知识在这些Cisco设备的：

- Cisco PIX 500 系列安全设备
- Cisco PIX 5500 系列安全设备
- Cisco IOS路由器
- Cisco VPN 3000 系列集中器（*可选*）

## 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 PIX 500 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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# IPSec VPN配置不工作

## 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。虽然这些解决方案未以任何特定顺序列出，但在您进行深入故障排除以及致电 TAC 之前，可以将它们用作验证或尝试的项目清单。所有这些解决方案都直接来自 TAC 服务请求，并且已解决众多的用户问题。

- 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 PIX/ASA）
- 验证 ISAKMP 身份
- 验证空闲/会话是否超时
- 验证ACL正确并且是已绑定的对加密映射
- 验证 ISAKMP 策略
- 验证路由是否正确
- 验证转换集正确
- 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缓冲获得用尽
- 与延迟的问题VPN客户端流量的

**注意：** 以下部分中的一些命令由于空间限制而分成两行。

## 启用 NAT 穿透（RA VPN 问题 1）

通过 NAT 穿透 (NAT-T)，VPN 流量可以通过 NAT 或 PAT 设备，例如 Linksys SOHO 路由器。如果未启用 NAT-T，通常 VPN Client 用户似乎可以连接到 PIX 或 ASA 而不会出现问题，但是他们无法访问安全设备之后的内部网络。

如果您未在 NAT/PAT 设备中启用 NAT-T，则会在 PIX/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. `Reason 412:The remote peer is no longer responding`错误消息。在前端 VPN 设备中启用 NAT-T，以解决此错误。

**注意：** 使用 Cisco IOS 软件版本 12.2(13)T 及更高版本时，默认情况下 Cisco IOS 中已启用 NAT-

T。

以下是用于在 Cisco 安全设备上启用 NAT-T 的命令。以下示例中的 20 是 keepalive 时间（默认值）。

**PIX/ASA 7.1 及更低版本**

```
pix(config)#isakmp nat-traversal 20
```

**PIX/ASA 7.2(1) 及更高版本**

```
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，选择 **Connection Entries** 并单击 Modify。此时将打开一个新窗口，您必须在其中选择 **Transport** 选项卡。在该选项卡下，选中 **Enable Transparent Tunneling** 和 IPSec over UDP（NAT/PAT）单选按钮。然后，单击 **Save** 并测试连接。

**注意：** 此命令同样适用于 PIX 6.x 和 PIX/ASA 7.x。

**注意：** 由于 PIX/ASA 充当 NAT 设备，因此通过 ACL 配置允许 UDP 4500（用于 NAT-T）、UDP 500 和 ESP 端口非常重要。要了解有关 PIX/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。

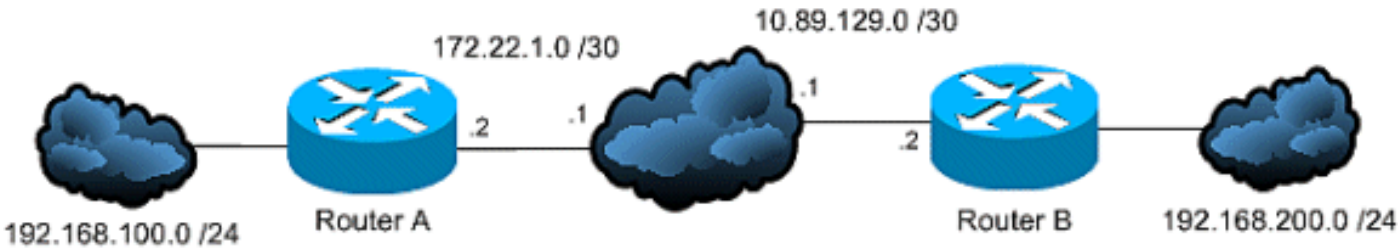
VPN 集中器

选择 **Configuration > Tunneling and Security >IPSEC >NAT Transparency > Enable:** ***在NAT-T的IPsec***为了启用在VPN集中器的NAT-T。

**注意：** NAT-T也让广泛VPN客户端通过PAT设备同时连接到所有头端它是否是PIX、路由器或者集中器。

## 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。以下述方案为例：




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
```

在此情况下，**ping** 必须来源于任一个路由器之后的“内部”网络。这是因为加密 ACL 仅配置为加密具

有那些源地址的流量。源自任一路由器的面向 Internet 接口的 ping 不会进行加密。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：

```
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
```

假设该图中的路由器已替换为 PIX 或 ASA 安全设备。用于测试连接的 ping 也可以源自具有 inside 关键字的内部接口：

```
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
```

**注意：** 建议不要使用 ping 来定位安全设备的内部接口。如果必须使用 ping 来定位内部接口，则必须在该接口上启用 management-access，否则设备不会应答。

```
securityappliance(config)#management-access inside
```

**注意：** 当问题存在与连接时，均等相位1 VPN不出来。在ASA，如果连接发生故障， SA输出类似于此示例，可能指示一不正确加密对等体配置和不正确ISAKMP提示配置：

```
Router#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no State : MM_WAIT_MSG2
```

**注意：** 状态可能是从MM_WAIT_MSG2到MM_WAIT_MSG5，表示担心的状态交换失败在主模式(MM)的。

**注意：** 当相位1是UP类似于此示例时， crypto SA输出了：

```
Router#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no State : MM_ACTIVE
```

## 启用 ISAKMP

如果根本没有任何迹象表明 IPSec VPN 隧道已启动，则可能是由于尚未启用 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`router(config)#crypto isakmp enable`
- Cisco PIX 7.1 及更低版本（使用所需接口替换 outside）`pix(config)#isakmp enable outside`
- Cisco PIX/ASA 7.2(1) 及更高版本（使用所需接口替换 outside）`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
```

该错误的原因可能是，可以在该接口上启用 isakmp 之前，ASA/PIS 之后的客户端通过 PAT 转换到 udp 端口 500。删除 PAT 转换 (clear xlate) 之后，就可以启用 isakmp。

**注意：** 请始终确保保留 UDP 500 和 4500 端口号，以用于与对等体进行 ISAKMP 连接协商。

**注意：** 当ISAKMP在接口时没有启用， VPN客户端表示错误消息类似于此消息：

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

**注意：** 为了解决此错误，请启用在VPN网关的crypto接口的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。在两个隧道对等体上启用或禁用 PFS；否则，在 PIX/ASA/IOS 路由器中不会建立 LAN 到 LAN (L2L) IPSec 隧道。

### PIX/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 **pfs** 命令并指定 enable 关键字。要禁用 PFS，请输入 **disable** 关键字。

```
hostname(config-group-policy)#pfs {enable | disable}
```

要从正在运行的配置中删除 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，以防止继承值。

```
hostname(config-group-policy)#no pfs
```

### 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，或者 IPsec 在接收新安全关联的请求时需要 PFS，请在加密映射配置模式下使用 **set pfs** 命令。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 — 指定当执行新的 Diffie-Hellman 交换时，IPsec 必须使用 768 位 Diffie-Hellman 主要模数组。
- group2 — 指定当执行新的 Diffie-Hellman 交换时，IPsec 必须使用 1024 位 Diffie-Hellman 主要模数组。

**示例：**

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

**注意：** 完全转发保密 (PFS) 是 Cisco 专有技术，在第三方设备上不支持。

## 清除旧的或现有的安全关联（隧道）

如果 IOS 路由器中出现以下错误消息，则导致该问题的原因是 SA 已过期或已被清除。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。

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

如果清除ISAKMP (相位I)和IPsec (相位II)安全关联(SA)，最简单和佳解决方案经常解决IPSec VPN问题。

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。

**注意：** 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：** 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**Cisco IOS**`router#show crypto isakmp sa` `router#show crypto ipsec sa` **Cisco PIX/ASA 安全设备**`securityappliance#show crypto isakmp sa` `securityappliance#show crypto ipsec sa` **注意：** 这些命令同样适用于 Cisco PIX 6.x 和 PIX/ASA 7.x
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。**Cisco IOSISAKMP（阶段 I）** `router#clear crypto isakmp ? <0 - 32766> connection id of SA <cr>`**IPsec（阶段 II）** `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>`**Cisco PIX/ASA 安全设备ISAKMP（阶段 I）** `securityappliance#clear crypto isakmp sa` **IPsec（阶段 II）** `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。如果任何差异在ISAKMP一生发生，您能接收**%PIX|ASA-5-713092** ：Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision 错误消息。对于 FWSM，您会收到 %FWSM-5-713092: `Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision` 在两个对等体中配置相同的值，以解决该错误。

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）。

PIX/ASA

`hostname(config)#isakmp policy 2 lifetime 14400`
IOS 路由器

`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 **lifetime** 值设置为 *0*，以将 IKE 安全关联的生存时间设置为无限。VPN 将始终处于连接状态并且不会终止。

hostname(config)#isakmp policy 2 lifetime 0
您能也**禁用在组政策的再Xauth**为了解决问题。

## 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。

- 使用以下命令在 Cisco IOS 中配置 ISAKMP keepalive：`router(config)#crypto isakmp keepalive 15`
- 使用以下命令，以在 PIX/ASA 安全设备上配置 ISAKMP keepalive：Cisco PIX 6.x`pix(config)#isakmp keepalive 15` Cisco PIX/ASA 7.x 及更高版本（针对名为 **10.165.205.222** 的隧道组）`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 PIX/ASA 7.x 及更高版本（针对名为 **10.165.205.222** 的隧道组）禁用 IKE keepalive 处理（默认情况下处于启用状态）。`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，选择 **%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 **ForceKeepAlives=0**（默认值）更改为 ForceKeepAlives=1。

**注意：** 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，IPSec VPN 隧道不能启动的原因可能只是一个简单的输入错误。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。**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；这是可以帮助避免深入排除故障的简单解决方案。

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 Client 和前端设备之间的组名称/预共享密钥不匹配，可能就会出现以下错误。

```
 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... may 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)
您也可以恢复预共享密钥，而无需在 PIX/ASA 安全设备上进行任何配置更改。请参阅 PIX/ASA 7.x：预共享密钥恢复。

**警告：** 如果删除加密相关命令，则可能会关闭一个或所有 VPN 隧道。请小心使用以下命令，在按照这些步骤操作之前，请参阅您组织的更改控制策略。

- 使用以下命令，以删除和重新输入 IOS 中对等体 10.0.0.1 或 vpngroup 组的预共享密钥 **secretkey**：Cisco LAN 到 LAN VPN`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`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 PIX/ASA 安全设备中对等体 10.0.0.1 的预共享密钥 **secretkey**：Cisco PIX 6.x`pix(config)#no isakmp key secretkey address 10.0.0.1 pix(config)#isakmp key secretkey address 10.0.0.1` Cisco PIX/ASA 7.x 及更高版本 `securityappliance(config)#tunnel-group 10.0.0.1 ipsec-attributes securityappliance(config-tunnel-ipsec)#no pre-shared-key securityappliance(config-tunnel-ipsec)#pre-shared-key secretkey`

## 预共享密钥不匹配

启动 VPN 隧道操作的连接断开。发生此问题的原因可能是阶段 I 协商期间预共享密钥不匹配。

如此示例所显示，在**show crypto isakmp sa**命令的**MM_WAIT_MSG_6**消息指示一不匹配的预共享密钥：

```
ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 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，请在两个设备上重新输入预共享密钥；预共享密钥必须唯一并且相匹配。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

当您清除安全关联和时它不解决IPSec VPN问题，删除并且重新应用包括断断续续丢弃VPN一些VPN站点通道和疏忽出现的相关加密映射为了解决多样化的问题。

**警告：** 如果从接口删除加密映射，这**一定**会关闭与该加密映射关联的所有 IPSec 隧道。请小心按照以下步骤操作，在继续之前，请考虑您组织的更改控制策略。

- 使用以下命令，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。请使用 **crypto map** 命令的 no 形式。`router(config-if)#no crypto map mymap` 继续使用 **no 形式**，以删除整个加密映射。`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：`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，以删除和替换 PIX 或 ASA 上的加密映射：首先从接口中删除加密映射。请使用 **crypto map** 命令的 no 形式。`securityappliance(config)#no crypto map mymap interface outside` 继续使用 **no 形式**，以删除其他加密映射命令。`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

```
：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
```

**注意：** 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 PIX/ASA）

**sysopt connection permit-ipsec** 和 sysopt connection permit-vpn 命令允许来自 IPsec 隧道的数据包及其有效负载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 命令为 **sysopt 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 命令为 **sysopt connection permit-vpn**。

在 PIX 6.x 中，默认情况下此功能处于**禁用**状态。使用 PIX/ASA 7.0(1) 及更高版本时，默认情况下此功能处于**启用**状态。使用以下 show 命令可确定您的设备上是否已启用相关 **sysopt** 命令：

- Cisco PIX 6.x
```
pix# show 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 no sysopt uauth allow-http-cache no sysopt
connection permit-ipsec !--- sysopt connection permit-ipsec is disabled no sysopt connection
permit-pptp no sysopt connection permit-l2tp no sysopt ipsec pl-compatible
```
- Cisco PIX/ASA 7.x
```
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)
```

使用以下命令可针对您的设备启用正确的 **sysopt** 命令：

- Cisco PIX 6.x 和 PIX/ASA 7.0
```
pix(config)#sysopt connection permit-ipsec
```
- Cisco PIX/ASA 7.1(1) 及更高版本
```
securityappliance(config)#sysopt connection permit-vpn
```

**注意：** 如果不希望使用**connection命令的sysopt**，则您必须明确地允许需要的流量，是关注数据流从来源到目的地，例如，从远程设备LAN到LAN本地设备和“UDP端口500"远程设备外部接口的对本地设备外部接口的，在外部ACL。

## 验证 ISAKMP 身份

如果IPSec VPN通道在IKE协商内失败，失败可以归结于PIX或认可其对等体标识的其对等体的无法。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，PIX 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 **isakmp identity** 命令

```
crypto isakmp identity address
```

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

或者

```
crypto isakmp identity auto
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by
connection type; IP address for !--- preshared key or cert DN for certificate authentication.
```

或者

```
crypto isakmp identity hostname
!--- Uses the fully-qualified domain name of !--- the host exchanging ISAKMP identity
information (default). !--- This name comprises the hostname and the domain name.
```

VPN通道不能在移动配置以后出来从PIX到ASA使用PIX/ASA配置迁移工具;这些消息在日志出现：

```
[IKEv1] Group= x.x.x.x IP = x.x.x.xPeerTblEntry![IKEv1] Group= x.x.x.x IP = x.x.x.x![IKEv1]
Group= x.x.x.x IP = x.x.x.x construct_ipsec_delete() SA2SPI![IKEv1] Group= x.x.x.x IP = x.x.x.x!
```

此问题发生默认情况下，因为PIX设置识别连接作为ASA识别作为**IP的主机名**。为了解决此问题，请使用**crypto isakmp identity命令**在全局配置模式如下所示：

```
crypto isakmp identity hostname !--- Use the fully-qualified domain name of !--- the host
exchanging ISAKMP identity information (default). !--- This name comprises the hostname and the
domain name.
```

当您接收INVALID_COOKIE错误消息时的，请发出**address命令crypto isakmp的标识**为了解决问题。

**注意：** 自软件版本 7.2(1) 开始，**isakmp identity** 命令已作废。有关详细信息，请参阅 Cisco 安全设备命令参考 7.2 版。

## 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，而不管空闲超时的设置如何，并且将出现 PEER_DELETE-IKE_DELETE_UNSPECIFIED 错误。

配置**空闲超时**和**会话超时，**因为**无**为了组成通道总是，并且，以便通道从未丢弃，既使当使用第三方设备。

### PIX/ASA 7.x 及更高版本

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

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-idle-
timeout none
```

请在组策略配置模式下或用户名配置模式下，使用 vpn-session-timeout 命令为 VPN 连接配置最大时长。

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-
session-timeout none
```

**注意：** 当您有通道**所有**已配置的时，您不需要配置**idle-timeout，**因为，即使您配置VPN IDLE超时，不会工作，因为所有流量通过通道(因为通道所有配置)。所以，关注数据流(甚至PC生成的流量)将是触发的并且没让的Idle-timeout进入操作。

### 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-time** 命令以配置 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。

**crypto ipsec security-association idle-time** *seconds*
时间单位为 *seconds*，即空闲计时器允许非活动对等体维持 SA 的时间。seconds 参数的有效值范围是 60 到 86400。

## 验证ACL是对加密映射的正确和已绑定的

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；其中包括 LAN 到 LAN 设置中的加密 ACL 或远程访问配置中的分割隧道 ACL。如果这些 ACL 未配置或配置不正确，则流量在 VPN 隧道中可能只会向一个方向流动，或者根本不通过该隧道发送。

**注意：** 确保绑定与加密映射的加密ACL通过使用**加密映射匹配address命令**在全局配置模式。

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。**注意：** 在VPN集中器上，您也许发现象这样的一本日志：`IKEL2L`为了避免此消息和为了带动通道，请确保加密ACL不交迭，并且其他已配置的VPN通道没有使用同样关注数据流。
- 请勿重复使用 ACL。即使 NAT 免除 ACL 和加密 ACL 指定的是相同流量，也请使用两个不同的访问列表。
- 对于远程访问配置，请勿对具有动态加密映射的相关流量使用访问列表。这会导致 VPN Client 无法连接到前端设备。如果为远程访问 VPN 配置的加密 ACL 不正确，将会收到 %ASA-3-713042: `IKE Initiator unable to find policy`:Intf 2 错误消息。**注意：** 如果这是VPN站点到站点通道，请确保匹配与对等体的访问列表。他们必须按顺序在对等体的反向顺序。有关说明如何在 Cisco VPN Client 和 PIX/ASA 之间设置远程访问 VPN 连接的示例配置，请参阅 PIX/ASA 7.x 和 Cisco VPN Client 4.x 通过 Windows 2003 IAS RADIUS（针对 Active Directory）进行的身份验证配置示例。
- 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 **route-map** 命令。在 PIX 或 ASA 上，这意味着您使用 **nat (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，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
```

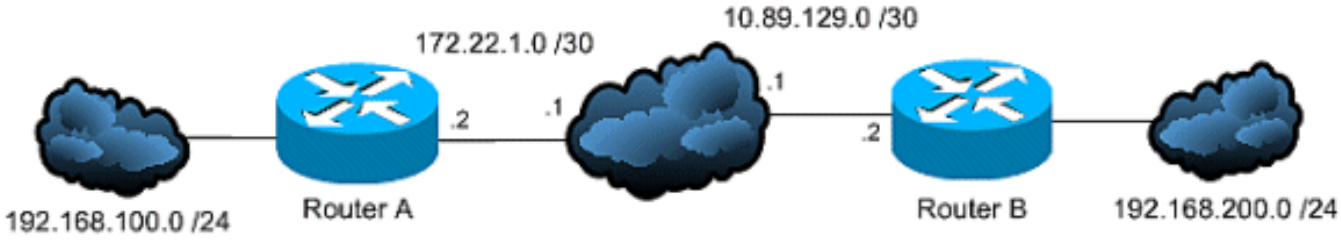
此处，PIX 配置为免除来自 NAT 在 **192.168.100.0 /24** 和 192.168.200.0 /24 或 192.168.1.0 /24 之间发送的流量。例如，所有其他流量都受 NAT 过载影响：

```
access-list noNAT extended permit ip 192.168.100.0 255.255.255.0 192.168.200.0 255.255.255.0 access-list noNAT extended permit ip 192.168.100.0 255.255.255.0 192.168.1.0 255.255.255.0 nat (inside) 0 access-list noNAT nat (inside) 1 0.0.0.0 0.0.0.0 global (outside) 1 interface
```

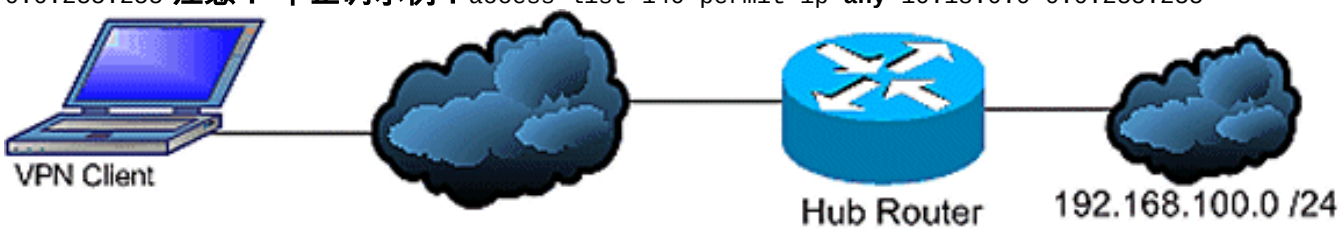
**注意：** NAT 免除 ACL 仅适用于 IP 地址或 IP 网

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 等等）。**注意：** 在VOIP环境，在网络之间的语音呼叫通过VPN被传达，语音呼叫不工作，如果NAT 0 ACL没有适当地配置。在通过深深VOIP排除故障前，被建议检查VPN连接状态，因为问题可能是NAT豁免ACL的误配置。**注意：** 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。`%PIX-3-305005: No translation group found for icmp src outside:192.168.100.41 dst inside:192.168.200.253 (type 8, code 0) %ASA-3-305005: No translation group found for udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p`**注意： 不正确示例：**`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 必须彼此**镜像**。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`**注意：** 虽然此处没有明示，但是此概念同样适用于 PIX 和 ASA 安全设备。在PIX/ASA，远程访问配置的独立的隧道ACL必须是允许流量对网络VPN客户端需要访问的**标准访问**列表。IOS路由器能使用扩展ACL独立的隧道。**注意：** 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。请在分割隧道的扩展 ACL 中仅使用源网络。**注意： 正确示例：**`access-list 140 permit ip 10.1.0.0 0.0.255.255 10.18.0.0 0.0.255.255` **注意： 不正确示例：**`access-list 140 permit ip any 10.18.0.0 0.0.255.255`



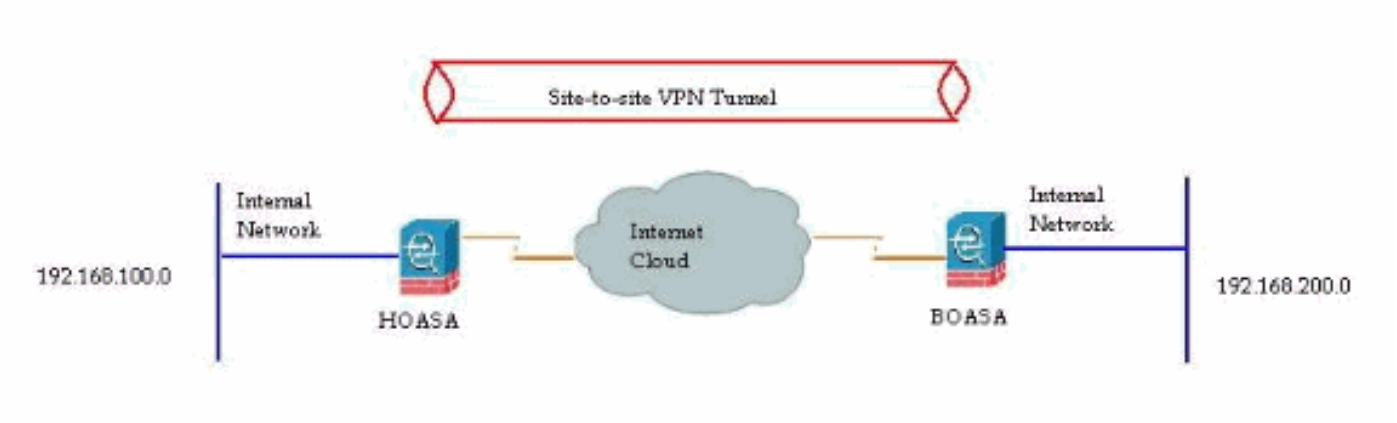

Cisco IOS`router(config)#access-list 10 permit ip 192.168.100.0 router(config)#crypto isakmp client configuration group MYGROUP router(config-isakmp-group)#acl 10` Cisco PIX 6.x`pix(config)#access-list 10 permit 192.168.100.0 255.255.255.0 pix(config)#vpngroup MYGROUP split-tunnel 10` Cisco PIX/ASA 7.x`securityappliance(config)#access-list 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`

如果NAT ACL不是不正确的配置的也没有配置在ASA，此错误在ASA 8.3出现：

```
%ASA-5-305013 NAT;udp srcx.x.x.x/xxxxx dstx.x.x.x/xxNAT
```

如果设置不正确，为了解决此问题，请验证配置正确或重新配置。

**NAT在ASA版本8.3的免税配置站点到站点VPN通道的：**




使用版本8.3，站点到站点VPN必须设立在HOASA和BOASA之间与两ASA。在HOASA的NAT免税配置看似类似于此：

```
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**，并检查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!"
```

这是详细日志消息：

```
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, dropping
```

通常，由于 ISAKMP 策略不匹配或缺少 NAT 0 语句就会出现此消息。

另外，此消息出现：

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

此消息表明第2阶段消息排队，在阶段1完成后。此错误消息可能是由以下原因之一造成的：

- 在相位的不匹配在任何对等体
- ACL阻塞从完成相位1的对等体

此消息通常来，在!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 Client 的其中一个 IKE 建议匹配。

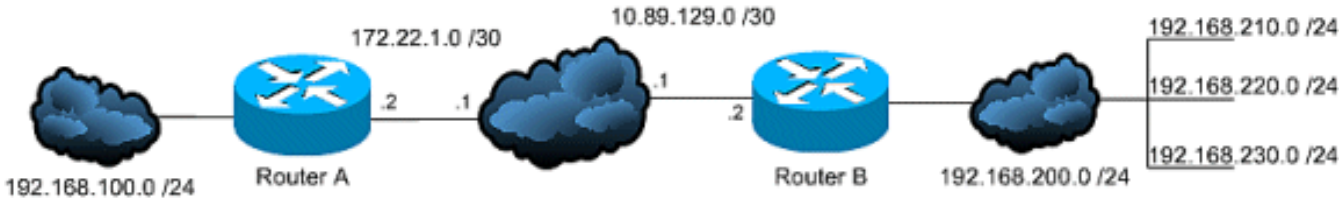
**注意：** 对于在 PIX/ASA 上使用的 ISAKMP 策略和 Ipsec 转换集，Cisco VPN Client 不能使用具有 DES 和 SHA 组合的策略。如果您使用 DES，则需要使用 MD5 散列算法，也可以使用其他组合，如 3DES 和 SHA 以及 3DES 和 MD5。

## 验证路由是否正确

路由几乎是每个 IPSec VPN 部署的关键部分。请确保您的加密设备（如路由器和 PIX 或 ASA 安全设备）具有正确的路由信息，以便通过您的 VPN 隧道发送流量。而且，如果您的网关设备之后存在其他路由器，请确保这些路由器了解如何到达隧道，并且了解另一端所使用的网络类型。

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 PIX 或 ASA，则配置看起来与以下内容相似：`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：`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
```

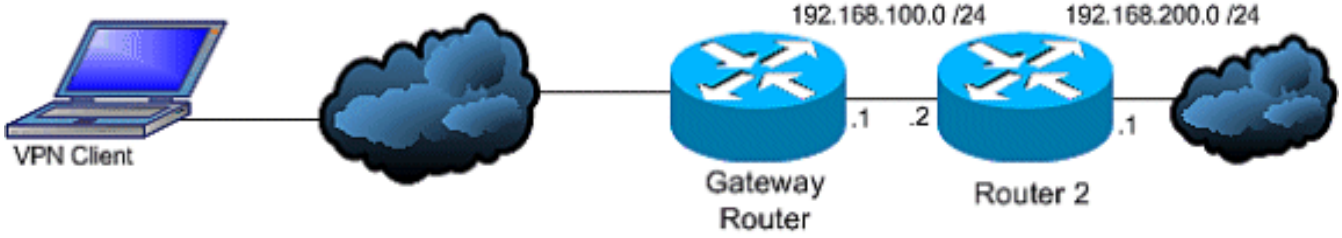
**`reverse-route`** `set transform-set mySET match address 110` 如果路由器 A 已替换为 PIX 或 ASA，则配置看起来与以下内容相似：`access-list cryptoACL extended permit ip 192.168.100.0`

```
   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：`crypto dynamic-map dynMAP 10 set transform-set mySET` **`reverse-route`** `crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP`Cisco PIX 或 ASA 安全设备：`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`

**注意：** 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命令参考部分。

**注意：** 对于在 PIX/ASA 上使用的 ISAKMP 策略和 Ipsec 转换集，Cisco VPN Client 不能使用具有 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。

## 验证加密映射序号，并且名称并且那加密映射在IPSec隧道开始/末端的正确的接口应用

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。动态加密映射条目的序列号**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!
```

**注意：** 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：

```
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 cisco
```

**注意：** 加密映射名称区分大小写。

**注意：** 此错误消息能也被看到，当造成对等体点击错误的加密映射时的动态crypto人顺序由定义了关注数据流的一不匹配的crypto访问列表不是正确，并且：`%ASA-3-713042 IKE Initiator unable to find policy:`

对于要在同一个接口中终止多个 VPN 隧道的方案，我们需要创建名称相同但序列号不同的加密映射（每个接口仅允许一个加密映射）。这也同样适用于路由器、PIX 和 ASA。

要了解有关在同一个接口中具有不同序列号的相同加密映射的集线器 PIX 配置的详细信息，请参阅为集线器和远程 PIX 之间的 IPsec 配置 VPN Client 和扩展身份验证。同样，要了解有关针对 L2L 和远程访问 VPN 方案的加密映射配置的详细信息，请参阅 PIX/ASA 7.X：将新隧道或远程访问添加到现有的 L2L VPN。

## 验证对等体 IP 地址是否正确

对于 PIX/ASA 安全设备 7.x LAN 到 LAN (L2L) IPsec VPN 配置，您必须在 tunnel-group <name> type ipsec-l2l 命令中将隧道组的 **<name>** 指定为远程对等体 IP 地址（远程隧道端），以创建和管理 IPsec 的连接特定记录的数据库。在 **tunnel group name** 和 Crypto map set address 命令中对等体 IP 地址必须匹配。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
```

在 PIX 6.x LAN 到 LAN (L2L) IPSec VPN 配置中，对等体 IP 地址（远程隧道端）必须与加密映射中的 **isakmp key address** 和 set peer 命令匹配，以便成功创建 IPSec VPN 连接。

当对端IP地址在ASA加密配置时未适当地配置， ASA不能设立VPN通道并且暂停在仅*MM_WAIT_MSG4*阶段。为了解决此问题，请更正对端IP地址在配置里。

这是输出**show crypto isakmp sa命令，**当VPN通道在MM_WAIT_MSG4状态时暂停。

```
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

```
%PIX|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。

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

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

**Both lines should 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-to-LAN隧道和远程访问VPN通道在同一个加密映射配置，提示LAN对LAN对等体输入Xauth信息，并且LAN-to-LAN隧道失效与“*CONF_XAUTH*”在输出**show crypto isakmp sa命令中**。

这是输出的SA的示例：

```
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
```

**注意：** 此问题只影响 Cisco IOS 和 PIX 6.x，因为 PIX/ASA 7.x 使用隧道组，所以不会受此问题影响。

请在输入 isakmp 密钥时使用 **no-xauth** 关键字，以使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：

```
router(config)#crypto isakmp key cisco123 address 172.22.1.164 no-xauth
```

在PIX/ASA 7.x作为Easy VPN Server的方案中， Easy VPN客户机无法连接到头端由于Xauth问题。禁用 PIX/ASA 中的用户身份验证，以便解决该问题（如下所示）：

```
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
```

请参阅本文档的其他部分，以了解有关 **isakmp ikev1-user-authentication** 命令的详细信息。

## VPN缓冲获得用尽

当IP地址范围分配到VPN池不是满足的时，您能扩大IP地址的可用性用两种方式：

1. 取消现有范围，并且定义新的范围。示例如下：`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. 当间断子网将被添加到VPN池时，您能定义两个独立的VPN池按顺序然后指定他们在“组属性下”。示例如下：`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`

您指定池的命令是非常重要，因为ASA从这些池分配地址按池在此命令出现的顺序。

**注意：** 在组政策地址池always命令的地址池设置改写在隧道群地址池命令的本地池设置。

## 与延迟的问题VPN客户端流量的

当有在VPN连接时的延迟问题，请验证以下为了解决此：

1. 如果可以进一步，减少数据包的MSS请验证。

2. 如果IPsec/tcp使用而不是IPsec/udp，则请配置保留VPN流。
3. 重新载入思科ASA。

# VPN Client 无法与 ASA/PIX 连接

## 问题

当X验证与RADIUS服务器一起使用时， Cisco VPN Client无法验证。

## 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：

```
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验证与RADIUS服务器一起使用时， Cisco VPN Client无法验证。

## 解决方案

最初，请确保验证适当地运作。要缩小问题，首先请验证与本地数据库的验证在ASA。

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

如果这良好工作，则应该与RADIUS服务器配置涉及问题。

验证RADIUS服务器的连接从ASA的。如果ping运作不出任何问题，则请检查在ASA的RADIUS相关在RADIUS服务器的配置和数据库配置。

您可能使用**debug radius命令**排除故障radius相关问题。对于示例**debug radius**输出，参考此**输出示例:**。

**注意：** 在您使用**debug命令**在ASA前，参考此文档：**警告消息**。

# VPN客户端常见丢包连接在第一次尝试或“安全VPN连接由对等体终止。原因433."或“安全VPN连接由对等体433:(Reason终止没指定的对等体原因)”

## 问题

当他们尝试连接用头端VPN设备时， Cisco VPN Client用户也许收到此错误。

“*VPN客户端丢包连接在第一次尝试*”或“*常见安全VPN连接由对等体终止。原因433."*或“*安全VPN连*

*接由对等体433:(Reason终止没指定的对等体原因)"或"尝试了分配网络或广播IP地址，删除(x.x.x.x)从池"*

## 解决方案 1

问题也许是IP池分配通过ASA/PIX， RADIUS服务器， DHCP服务器或通过作为DHCP服务器的RADIUS服务器。请使用 **debug crypto** 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

此问题也发生由于扩展认证的失败。您必须检查AAA服务器排除故障此错误。检查在服务器和客户端的服务器验证密码和重新加载AAA服务器也许解决此问题。

## 解决方案 3

此问题的另一应急方案是禁用威胁检测功能。通常，当有不同的不完整安全关联(SA)的时多重发，与启用的威胁检测功能的ASA认为扫描攻击发生，并且VPN端口被标记作为主要违者。设法禁用威胁检测功能，这能导致在处理的很多开销ASA。请使用这些命令为了禁用威胁检测：

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

关于此功能的更多信息，参考威胁检测。

**注意：** 如果这解决实际问题，这可以用于作为应急方案验证。确保禁用在思科ASA的威胁检测实际上减弱几个安全功能例如缓和扫描尝试，与无效的SPI的DoS，发生故障应用检查和不完整塞申斯的数据包。

## 解决方案 4

当转换集没有适当地配置时，此问题也出现。转换set resolve的正确的配置问题。

# 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。

远程访问用户能访问仅本地网络。

## 解决方案

设法这些解决方案为了解决此问题：

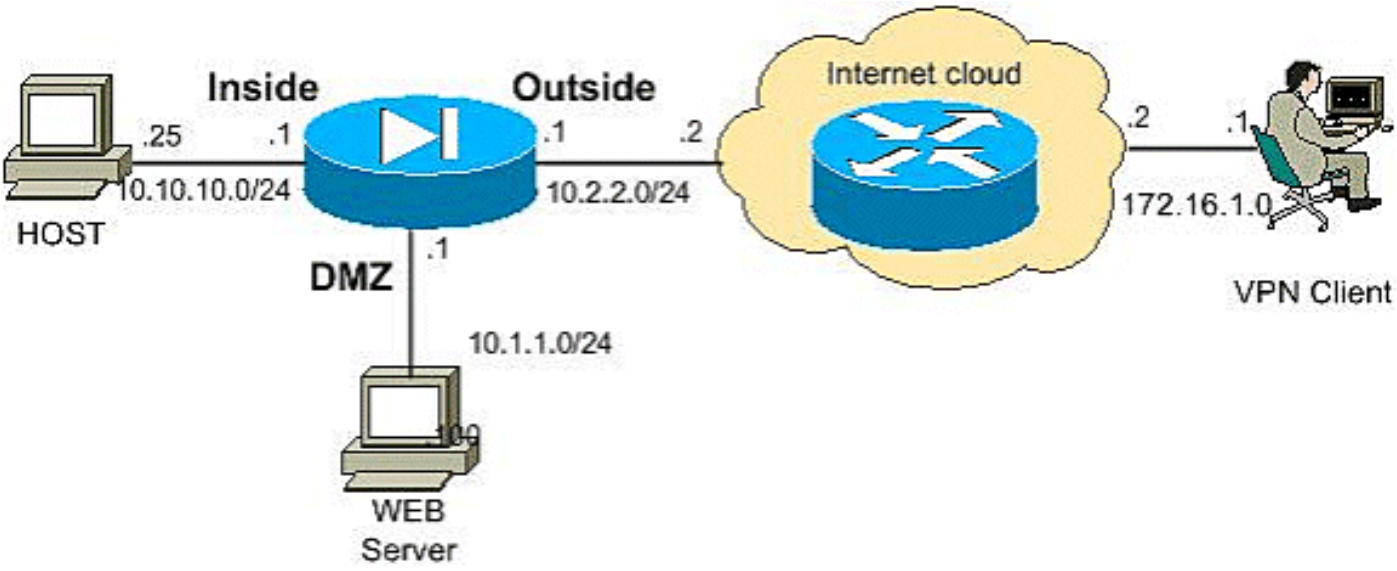
- 无法访问 DMZ 中的服务器

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

## 无法访问 DMZ 中的服务器

一旦VPN客户端设立IPSec隧道用VPN数据转发设备(PIX/ASA/IOS路由器)， VPN客户端用户能访问网络内部(10.10.10.0/24)资源，但是他们无法访问DMZ网络(10.1.1.0/24)。

**图表**




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/PIX |
| --- |
| ciscoasa#**show running-config** *!--- Split tunnel for the **inside network** access* access-list vpnusers_spitTunnelAcl permit ip 10.10.10.0 255.255.0.0 any *!--- Split tunnel for the **DMZ network** access* access-list vpnusers_spitTunnelAcl permit ip 10.1.1.0 255.255.0.0 any *!--- Create a pool of addresses from which IP addresses are assigned !--- dynamically to the remote VPN Clients.* ip local pool vpnclient 192.168.1.1-192.168.1.5 *!--- This access list is used for a nat zero command that prevents !--- traffic which matches the access list from undergoing NAT. !--- No Nat for the **DMZ network.*** access-list nonat-dmz permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 *!--- No Nat for the **Inside network.*** access-list nonat-in permit ip 10.10.10.0 255.255.255.0 192.168.1.0 255.255.255.0 *!--- NAT 0 prevents NAT for networks specified in the **ACL nonat*** . nat (DMZ) 0 access-list nonat-dmz nat (inside) 0 access-list nonat-in |

**ASA版本8.3配置：**

此配置显示如何配置DMZ网络的NAT免税为了使VPN用户访问DMZ网络：

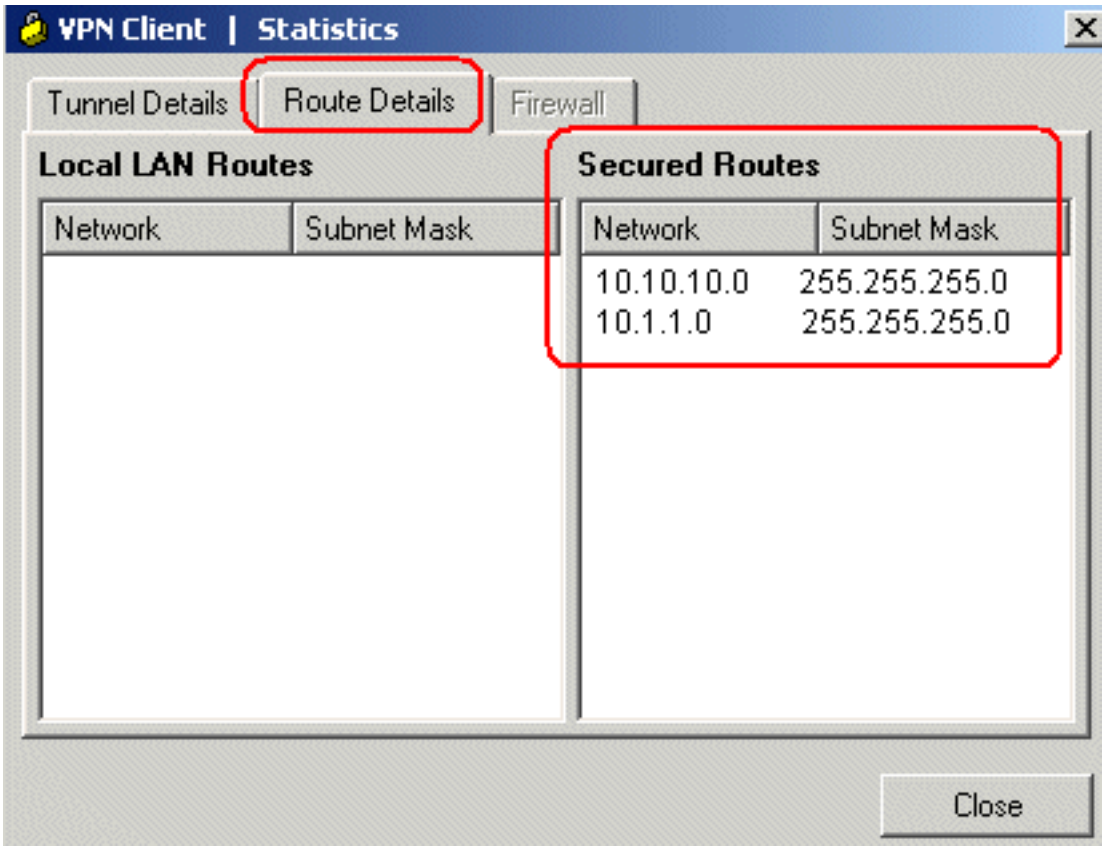
```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

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 Client** 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。




请参阅 PIX/ASA 7.x：DMZ 中的邮件服务器访问配置示例，以了解有关如何设置 PIX 防火墙以便访问位于隔离区 (DMZ) 网络中的邮件服务器的详细信息。

请参阅 PIX/ASA 7.x：将新隧道或远程访问添加到现有的 L2L VPN，以了解将新 VPN 隧道或远程访问 VPN 添加到已经存在的 L2L VPN 配置的必需步骤。

请参阅 PIX/ASA 7.x：在 ASA 上允许 VPN Client 使用分割隧道的配置示例，以了解有关如何允许 VPN Client 在通过隧道进入 Cisco 自适应安全设备 (ASA) 5500 系列安全设备时访问 Internet 的分步说明。

请参阅 PIX/ASA 7.x 和 Cisco VPN Client 4.x 通过 Windows 2003 IAS RADIUS（针对 Active Directory）进行的身份验证配置示例，以了解有关如何在 Cisco VPN Client（适用于 Windows 的 4.x 版本）和 PIX 500 系列安全设备 7.x 之间设置远程访问 VPN 连接的详细信息。

## VPN Client 无法解析 DNS

在建立隧道之后，如果 VPN Client 无法解析 DNS，则可能是前端设备 (ASA/PIX) 中的 DNS 服务器配置存在问题。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：

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP
address(172.16.1.1) !--- and the domain name(cisco.com) in the group policy. 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 !--- using 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

分割隧道使远程访问 IPSec 客户端可以有条件地以加密形式通过 IPsec 隧道定向数据包，或者以明文形式将数据包定向到网络接口，并解密，然后在网络中将数据包路由到最终目标。默认情况下，分割隧道处于禁用状态，这是指 tunnelall 流量。

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

**注意：** 仅 Cisco VPN Client 支持 ***excludespecified*** 选项，EZVPN Client 不支持该选项。

```
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：

- PIX/ASA 7.x：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
- VPN 3000 集中器上针对 VPN Client 使用分割隧道的配置示例

## 发夹

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，如果您建立了集中星型 VPN 网络，其中安全设备是中央，而远程 VPN 网络是分支，为使分支之间彼此通信，流量必须进入安全设备，然后再流向其他分支。

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

```
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 PIX/ASA 7.x：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

请始终确保池中要分配给 VPN Client、前端设备的内部网络和 VPN Client 内部网络的 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。

关于进一步示例，请参见*图表*和*示例*无法访问在DMZ部分的服务器。

## 无法连接超过三个 VPN Client 用户

### 问题

只有三个 VPN Client 可以连接到 ASA/PIX；连接第四个客户端时将失败。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。

设法这些解决方案为了解决此问题：

- 配置同时登录数
- 使用 CLI 配置 ASA/PIX
- 配置集中器配置集中器

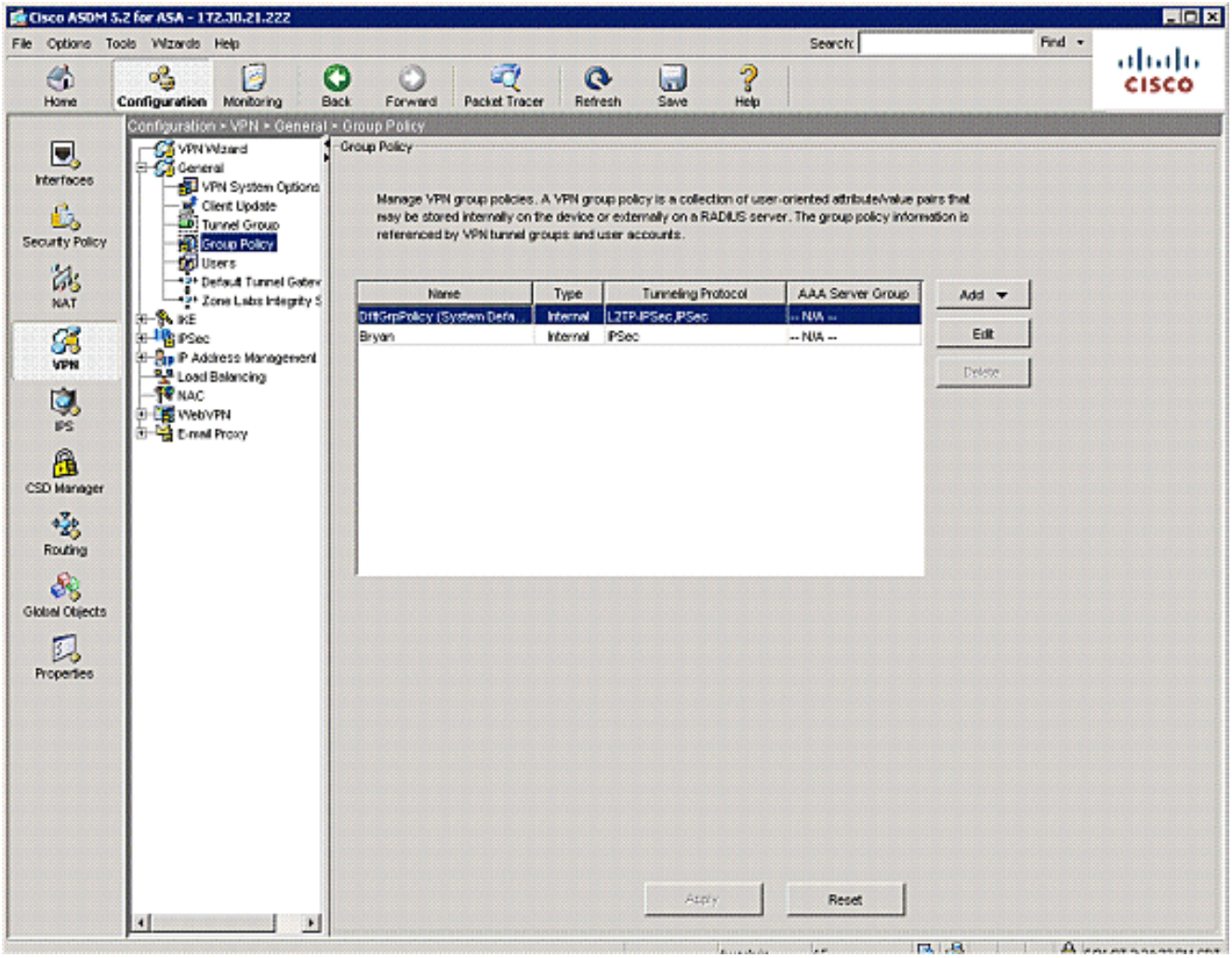
有关详细信息，请参阅 Cisco ASA 5500 系列版本 5.2 的所选 ASDM VPN 配置过程中的配置组策略部分。

### 配置同时登录数

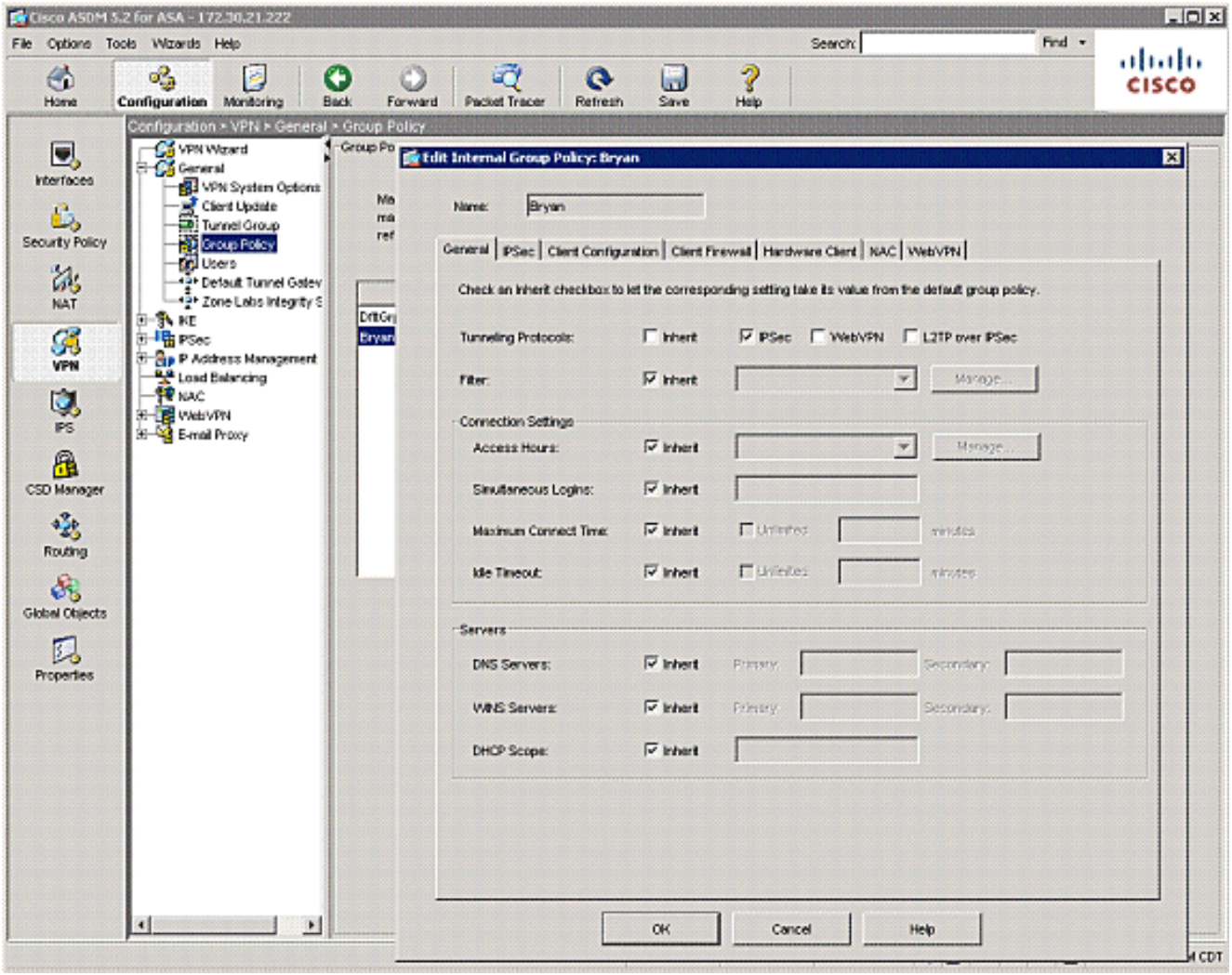
如果在ASDM的**继承**复选框被检查，只有同时登录默认号码为用户允许。同时登录数的默认值是3。

要解决此问题，请增加同时登录数的值。

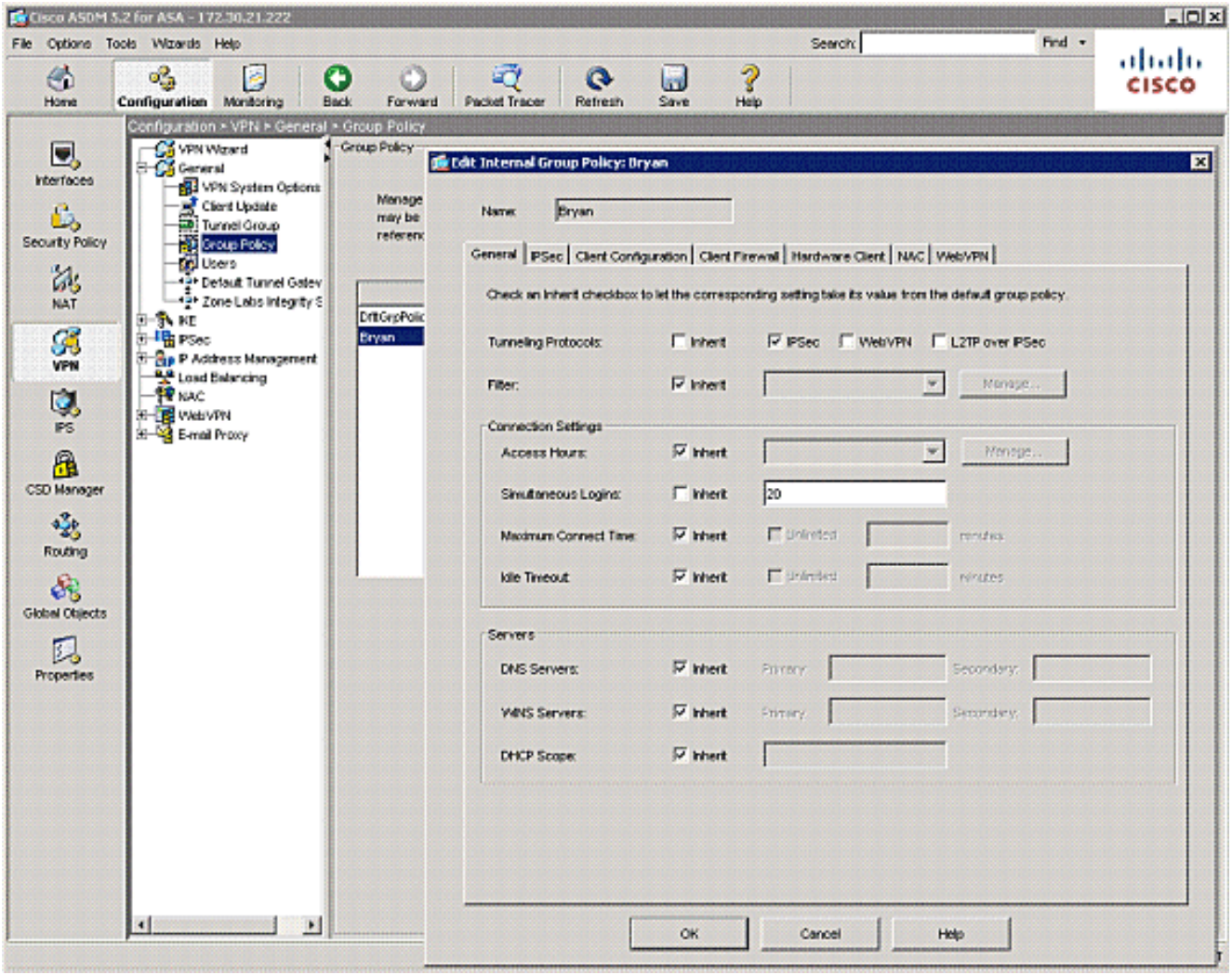
1. 启动 ASDM，然后导航到 **Configuration> VPN > Group Policy**。




2. 选择相应的 **Group** 并单击 Edit 按钮。




3. 在 **General** 选项卡中，取消选中 Connection Settings 下与 Simultaneous Logins 相对应的 Inherit 复选框。在字段中选择相应的值。




**注意：** 此字段的最小值是 0，表示禁用登录并且阻止用户访问。**注意：** 使用从不同的PC时的同一个用户帐户当您登陆，当前会话(从另一个PC的已建立连接使用同一个用户帐户)终止和个新会话设立。这是默认行为并且是独立对VPN同时登录。

## 使用 CLI 配置 ASA/PIX

完成以下步骤，以便配置所需的同时登录数。在本示例中，选择 20 作为所需的值。

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

要了解有关该命令的详细信息，请参阅 Cisco 安全设备命令参考 7.2 版。

在全局配置模式下使用 **vpn-sessiondb max-session-limit** 命令，将 VPN 会话数限制为小于安全设备允许的值。使用该命令的 no 形式，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：

```
hostname#vpn-sessiondb max-session-limit 450
```

## 配置集中器

### 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：

选择**Configuration > User Management > Groups > Modify 10.19.187.229 >General >同时登录**，并且更改登录数量到**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。可能是从路由器或 PIX/ASA 设备通过的临时数据包的最大数据段大小 (MSS) 有问题（特别是已设置 SYN 位的 TCP 数据段）。

### Cisco IOS 路由器 — 更改路由器的外部接口（隧道末端接口）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：

```
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：

```
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 PIX/ASA 7.x 和 IOS：VPN 分段。

### PIX/ASA 7.X — 参阅 PIX/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。请参阅以下文档，以解决该问题：

- PIX/ASA 7.x 和 IOS：VPN 分段
- PIX/ASA 7.0 问题：超出 MSS - HTTP 客户端无法浏览某些网站

## 无法从 ASA/PIX 启动 VPN 隧道

## 问题

您无法从 ASA/PIX 接口启动 VPN 隧道，并且建立隧道后，远程端点/VPN Client 无法对 VPN 隧道上 ASA/PIX 的内部接口执行 ping 操作。例如，VPN Client 可能无法通过 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-access** 命令，否则无法从隧道的另一端对 PIX 的内部接口执行 ping 操作。

```
PIX-02(config)#management-access inside PIX-02(config)#show management-access management-access
inside
```

**注意：** 此命令也可帮助通过 VPN 隧道启动到 ASA 内部接口的 ssh 或 http 连接。

**注意：** 此信息为DMZ接口适用。例如，如果您想要对 PIX/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。

```
PIX-02(config)#management-access DMZ
```

**注意：** 如果无法连接 VPN Client，请确保 ESP 和 UDP 端口已打开，但如果这些端口未打开，请在 VPN Client 连接条目下选择 TCP 10000 端口，然后尝试在该端口上进行连接。右键单击 **modify > transport 选项卡 > IPsec over TCP**。参考PIX/ASA 7.x支持在所有端口配置示例的IPSec over TCP关于IPSec over TCP的更多信息。

# 无法通过在VPN通道间的流量

## 问题

您无法通过在VPN通道间的流量。

## 解决方案

此问题发生由于在Cisco Bug ID描述的问题CSCtb53186 (仅限注册用户)。为了解决此问题，请重新加载ASA。参考bug欲知更多信息。

当ESP数据包阻塞时，此问题也许也出现。为了解决此问题，重新配置VPN通道。

此问题也许出现，当数据没有加密时，但是只解密在VPN通道如此输出所显示：

```
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
```

为了解决此问题，请检查以下：

1. 如果与远程站点的crypto访问列表匹配和那NAT 0访问列表正确。
2. 如果路由正确，并且流量点击通过通过的外部接口里面。输出示例:显示解密完成，但是加密不发生。
3. 如果sysopt permit连接VPN命令在ASA配置。如果没配置，请配置此命令，因为允许ASA豁免从接口ACL检查的encrypted/VPN流量。

# 配置VPN的备份对等请建立隧道在同样加密映射

## 问题

您要使用广泛备份对等单个VPN通道。

## 解决方案

配置多个对等项与提供fallback列表是等同的。每个通道，安全工具尝试协商与列表的第一对等体。

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应该有作为主对等体已经配置的加密映射。附属对等体可能在主要的一个以后被添加。

此配置示例显示主对等体作为X.X.X.X和备份对等作为Y.Y.Y.Y ：

```
ASA(config)#crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y
```

欲知更多信息，*参考在Cisco安全设备命令参考的*加密映射集对等体部分，*版本8.0*。

# 禁用/重新启动VPN通道

## 问题

为了临时地禁用VPN请建立隧道并且重新启动服务，完成在此部分描述的步骤。

## 解决方案

请使用**interface命令的加密映射**在全局配置模式删除一以前定义加密映射集对接口。请使用此命令**no表示**为了从接口删除加密映射集。

```
hostname(config)#no crypto map map-name interface interface-name
```

此命令删除加密映射集对所有即时安全审核设备接口并且使IPSec VPN通道不激活在该接口。

要重新启动在接口的IPSec隧道，您必须以前分配加密映射集到接口接口能提供IPSec服务。

```
hostname(config)#crypto map map-name interface interface-name
```

# 没加密的一些通道

## 问题

当通道大量在VPN网关时配置，一些通道不通过流量。ASA不收到那些通道的加密的信息包。

### 解决方案

因为ASA不能传递加密的信息包到通道，此问题出现。重复的加密规则在ASP表里创建。这是已知问题，并且归档Bug ID CSCtb53186 (仅限注册用户)涉及此问题。为了解决此问题，请重新加载ASA或升级软件对此bug修复的版本。

## Error: - %ASA-5-713904 ：Group = DefaultRAGroup, IP = x.x.x.x, Client is using an unsupported Transaction Mode v2 version.Tunnel terminated.

### 问题

显示 %ASA-5-713904: `Group = DefaultRAGroup, IP = 99.246.144.186, Client is using an unsupported Transaction Mode v2 version.`Tunnel terminated 错误消息。

### 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版本为了解决此错误。

## Error: - %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。应急方案是关闭SVC压缩与svc压缩none命令，解决问题。

## Error:The authentication-server-group none command has been deprecated

### 问题

如果将 VPN 配置从运行 7.0.x 版本的 PIX/ASA 传输到运行 7.2.x 的其他安全设备上，您会收到以下错误消息：

```
ERROR: The authentication-server-group none command has been deprecated.
The "isakmp ikev1-user-authentication none" command in the ipsec-attributes should be used
```

instead.

### 解决方案

7.2(1) 及更高版本中不再支持 **authentication-server-group** 命令。此命令已作废，并已转移到 tunnel-group general-attributes 配置模式。

有关此命令的详细信息，请参阅命令参考中的 isakmp ikev1-user-authentication 部分。

## 当在 VPN 隧道一端启用 QoS 时出现错误消息

### 问题

如果在 VPN 隧道的一端启用 QoS，您可能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 checking
```

### 解决方案

当隧道的一端执行 QoS 时，通常会产生此消息。当检测到数据包顺序不正确时，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：crypto map entry will be incomplete

### 问题

当您运行**加密映射mymap 20 ipsec-isakmp**命令时，您也许收到此错误：

```
crypto map entry will be incomplete
```

例如：

```
ciscoasa(config)#crypto map mymap 20 ipsec-isakmp WARNING: crypto map entry will be incomplete
```

### 解决方案

这是在您定义新加密映射时的正常警告，提醒您在其生效之前必须配置参数，例如 access-list（匹配地址）、转换集以及对等体地址。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。

## Error: - %ASA-4-400024 ：IDS:2151 Large ICMP packet from to on interface outside

### 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为了解决此问题。一旦签名禁用ping良好工作。

请使用这些命令为了禁用签名：

ASA(config)#ip**审计签名2151禁用**

ASA(config)#ip**审计签名2150禁用**

## Error: - %PIX|ASA-4-402119 ：IPSEC ：Received a protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.

### 问题

我在 ASA 的日志消息中收到了以下错误：

```
Error: - %PIX|ASA-4-402119 IPSEC Received a protocol packet (SPI=spi, sequence number= seq_num)
from remote_IP (username) to local_IP that failed anti-replay checking.
```

### 解决方案

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

```
hostname(config)#crypto ipsec security-association replay window-size 1024
```

**注意：** 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 - %PIX|ASA-4-407001:Deny traffic for local-host interface_name:inside_address，超过的编号许可证限制

### 问题

少量主机无法连接到互联网，并且此错误消息在Syslog出现：

```
 - %PIX|ASA-4-407001:Deny traffic for local-host interface_name:inside_address
```

### 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。此错误可以通过升级对用户较高的值的许可证解决。用户许可证能包括50， 100或者无限的用户如所需求。

## 错误消息- %VPN_HW-4-PACKET_ERROR ：

### 问题

- %VPN_HW-4-PACKET_ERROR 错误消息表明有路由器接收的HMAC的ESP数据包不匹配。此错误也许由这些问题造成：

- 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：

- 除非有数据流中断，请忽略错误消息。
- 如果有数据流中断，请替换模块。

# 错误消息：Command rejected:VLAN和之间的删除crypto连接，首先。

## 问题

当您尝试添加在中继端口的允许VLAN交换机的，此错误消息出现：`Command rejected:VLANVLANcrypto`。

不可能修改WAN边缘中继允许其他VLAN。即您是在**IPSEC VPN SPA**中继的无法添加VLAN。

此命令拒绝，因为允许它将导致属于接口的允许的VLAN列表，摆在一个潜在的IPSec安全突破口的一个crypto连接的接口VLAN。注意此行为适用于所有中继端口。

## 解决方案

而不是`Trunk VLAN (vlanlist)`命令，请使用`noneTrunkVLAN`或`"TrunkVLAN(vlanlist)"`命令。

# 错误消息- % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE ：丢弃数据包-会话的x.x.x.x:27331无效窗口缩放选项x.x.x.x:23的[发起者(标志0,factor 0)响应方(标志1，要素2)]

## 问题

此错误出现，当您设法从在VPN通道的远端的一个设备远程登录或，当您设法从路由器时远程登录：

```
- % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE -x.x.x.x:27331x.x.x.x:23[(0,factor 0)(12)]
```

## 解决方案

用户许可证能包括50， 100或者无限的用户如所需求。窗口比例缩放被添加允许数据迅速发射在长fat网络(LFN)的。这些典型地是与非常高带宽的连接，而且高延迟。因为卫星链路总是有高传播延迟，但是典型地有高带宽，与卫星连接的网络是LFN的一示例。对支持LFNs的Enable窗口比例缩放，TCP窗口尺寸必须是超过65,535。此错误消息可以通过增加TCP窗口尺寸是解决超过65,535。

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

## 问题

一旦VPN通道出来，此错误消息出现：

```
%ASA-5-305013 NAT
```

## 解决方案

为了解决此问题，当不在接口和使用NAT的主机一样，请使用被映射的地址而不是实际地址连接到主机。另外，请启用**inspect命令**应用程序是否嵌入IP地址。

# %PIX|ASA-5-713068 ：已接收非惯例通知消息：notify_type

## 问题

如果VPN通道不能出来，此错误消息出现：

```
%PIX|ASA-5-713068 notify_type
```

## 解决方案

此消息发生由于误配置(即，当策略或ACL没有配置是相同的在对等体)时。一旦策略和ACL匹配通道出来不出任何问题。

# %ASA-5-720012 ：(VPN第二)失败更新在备用装置(或) %ASA-6-720012的IPSec故障切换运行时数据：(VPN单元)失败更新在备用装置的IPsec故障切换运行时数据

## 问题

这些错误消息之一出现，当您设法升级思科可适应安全工具(ASA) ：

```
%ASA-5-720012 (VPN)IPSec
```

```
%ASA-6-720012 (VPN)IPsec
```

## 解决方案

这些错误消息是情报错误。消息不影响ASA或VPN的功能。

这些消息出现，当VPN故障切换子系统不能更新IPSec相关的运行时数据时，因为对应的IPSec隧道在备用装置删除。为了解决这些，请发出**wr standby命令**在活动装置。

归档两个Bug对这些Bug修复ASA的软件版本寻址此行为和升级。参考Cisco Bug ID CSCtj58420

(仅限注册用户)和CSCtn56517 (仅限注册用户)欲知更多信息。

## Error: - %ASA-3-713063 ：为目的地没配置的IKE对等地址0.0.0.0

### 问题

%ASA-3-713063 0.0.0.0错误消息没IKE出现，并且通道不能出来。

### 解决方案

当IKE对等地址没有为L2L通道时，配置此消息出现。此错误可以通过更改加密映射序号解决，然后删除和重新应用加密映射。

## Error:%ASA-3-752006 ：通道管理器失败调度KEY_ACQUIRE消息。

### 问题

%ASA-3-752006 KEY_ACQUIRE"错误消息被注册思科ASA。

### 解决方案

此错误消息可以由加密映射或隧道组的误配置造成。保证两个适当地配置。关于此错误消息的更多信息，参考错误752006。

这是某些纠正措施：

- 删除加密ACL (例如，关联对动态映射)。
- 删除未使用IKEv2相关的配置，如果其中任一个。
- 验证加密ACL适当地匹配。
- 删除重复的访问列表条目，如果其中任一个。

## Error:%ASA-4-402116 ：IPSEC ：接收一ESP数据包(SPI= 0x99554D4E，顺序number= 0x9E)从XX.XX.XX.XX (user= XX.XX.XX.XX)对YY.YY.YY.YY

在LAN到LAN VPN隧道设置，此错误在一端ASA接收：

SA

10.32.77.6710.105.30.1icmp

SA10.32.77.67/255.255.255.255/ip/0remote_proxy10.105.42.192/255.255.255.224/ip/0

### 解决方案

您需要验证在VPN通道的两端定义的关注数据流访问列表。两个应该配比作为确切的镜像。

## 失败启动64位VA安装程序启用虚拟适配器由于错误0xffffffff

### 问题

当AnyConnect不能连接时，`64VA0xffffffff`日志消息接收。

### 解决方案

要解决此问题，请执行以下步骤：

1. 去**系统>互联网通信Management>互联网通信设置**并且确保请**关闭更新**禁用的**自动根证明**。
2. 如果它禁用，则请禁用GPO的整个**管理模板**零件分配到受影响的计算机并且再测试。

参考请关闭自动根证明更新 欲知更多信息。

## 错误5 ：主机名不为此连接项存在。无法建立VPN联系。

### 问题

`5 VPN`错误消息在新的PC安装时接收。

### 解决方案

此问题归结于Cisco Bug ID CSCso94244 (仅限注册用户)。有关详细信息，请参阅此 Bug。

## Cisco VPN Client不与数据卡一起使用在Windows 7

### 问题

Cisco VPN Client不与数据卡一起使用在Windows 7。

### 解决方案

因为在Windows 7计算机，安装的VPN客户端不支持数据卡在Windows安装的Cisco VPN Client 7不与3G连接一起使用。

## 警告消息："VPN功能可能不操作"

### 问题

当尝试启用在ASA时外部接口的isakmp，此警告消息接收：

```
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.
```

这时，对ASA的访问通过SSH。HTTPS被终止，并且其他SSL客户端也受影响。

### 解决方案

此问题归结于内存要求由不同的模块例如记录器和crypto。确保您没有**logging queue 0**命令。它做队列大小设置为8192和存储器分配射击。

在平台中例如ASA5505和ASA5510，此存储器分配倾向于内存使其他模块挨饿(IKE和等)。Cisco Bug ID CSCtb58989 (仅限注册用户)被记录寻址一相似的行为。为了解决此，请配置logging queue对一点值，例如512。

## 填充错误的IPSec

### 问题

会收到以下错误消息：

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

### 解决方案

因为IPSec VPN协商，不用哈希算法，问题出现。数据包散列保证ESP信道的完整性检查。所以，没有切细，畸形的数据包由思科ASA接受未被发现，并且尝试解码这些数据包。然而，因为这些数据包是畸形的， ASA查找缺点，当解密数据包时。这导致被看到的填充符错误消息。

建议是包括散列算法在VPN的转换集和保证对等体之间的链路有最低的数据包畸形。

## 在远程站点电话的断线延迟时间

### 问题

断线延迟时间在远程站点电话体验。如何解决这一问题？

### 解决方案

skinny的禁用和sip检查为了解决此问题：

```
asa(config)# no inspect sip asa(config)# no inspect skinny
```

## VPN通道在每18个小时之后断开

### 问题

VPN通道在每18个小时之后断开，即使寿命设置24个小时。

### 解决方案

寿命是SA可以用于重新生成密钥的最大时间。您在配置里输入的值，因为寿命是与SA不同的重新生成密钥时期。所以，是必要的协商一旦IPsec的一个新的SA (或SA对)，在当前一个超时前。重新生成密钥时间小于寿命为了允许多尝试，万一第一重新生成密钥尝试一定总是发生故障。RFC不指定如何计算重新生成密钥时间。这被留下对实施的谨慎。所以，时间根据使用的平台将变化，软件版本等等。

一些实施能使用一个随机的要素计算重新生成密钥计时器。例如，如果ASA发起通道，然后是正常它将重新生成密钥在64800秒= 75% 86400。如果路由器启动，则ASA能等待更加长提供对等体更多时刻启动重新生成密钥。因此，是正常VPN会话断开每18个小时使用另一密钥VPN协商。这不能引起任何VPN丢弃或问题。

# 在对LAN通道的LAN重新协商后，通信流没有维护

## 问题

在对LAN通道的LAN重新协商后，通信流没有维护。

## 解决方案

ASA监控在其状态表里穿过它并且根据应用检查功能维护一个条目的每连接。穿过VPN以安全关联(SA)数据库的形式的加密流量详细信息维护。对于对LAN VPN连接的LAN，它维护两不同的通信流。一个是VPN网关之间的加密流量。其他是在网络资源在VPN网关背后和最终用户之间的通信流在另一端后。当VPN终止时，此特定的SA流详细信息删除。然而，此TCP连接的ASA维护的状态条目变得过时由于没有活动，阻碍下载。这意味着ASA将保留该特定的流量的TCP连接，当用户应用终止时。然而，在TCP空闲计时器超时后， TCP连接将变为迷路者和最终超时。

介绍呼叫Persistent IPSec被建立隧道的流的功能解决了此问题。new命令， sysopt连接保留VPN流，集成到Cisco ASA为了保留状态表信息在VPN通道的重新协商。默认情况下禁用该命令。通过启用此，思科ASA将维护TCP状态表信息，当L2L VPN从中断恢复并且重新建立通道。

# 错误消息阐明，带宽为crypto功能到达了

## 问题

此错误消息在2900系列路由器接收：

```
Error:Mar 20 10:51:29 %CERM-4-TX_BW_LIMIT 85000 KbpsTxsecurityk9crypto
```

## 解决方案

这是发生由于美国政府发出的严格指南的已知问题。根据此， securityk9许可证能只允许有效载荷加密至接近90Mbps的速率和对设备限制已加密tunnels/TLS会话数量。关于crypto出口限制的更多信息，参考的Cisco ISR G2 SEC和HSEC许可授权。

在Cisco设备的情况下，它比85Mbps单向数据流派生是较少在或在ISR G2路由器外面，有一个双向总计的170 Mbps。此需求申请思科1900， 2900和3900 ISR G2平台。此命令帮助您视线内这些限制：

```
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----
```

有被归档的bug寻址此行为。参考Cisco Bug ID CSCtu24534 (仅限注册用户)欲知更多信息。

为了避免此问题，您需要采购HSECK9许可证。"hseck9"功能许可证提供提高了与增加的VPN隧道计数和安全语音会话的有效载荷加密功能。关于许可授权的Cisco ISR路由器的更多信息，参考软件激活。

# 问题：在IPSec隧道的出站加密流量可能发生故障，即使入站解密流量工作。

## 解决方案

此问题在IPSec连接被观察了，在多个重新生成密钥后，但是触发情况不是清楚的。此问题出现可以通过检查**drop命令显示的asp的**输出和验证设立已到期VPN上下文计数器增加因为发送的每个出局信息包。参考Cisco Bug ID CSCtd36473 (仅限注册用户)欲知更多信息。

# 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_EXCH 消息会出现在 **show crypto isakmp sa** 命令的输出以及调试输出中。原因可能是由于 isakmp 策略不匹配，或者路径上的端口 udp 500 遭阻塞。

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

此消息是供参考消息并且与VPN通道的断开无关。

# 相关信息

- PIX/ASA 7.0 问题：超出 MSS - HTTP 客户端无法浏览某些网站
- PIX/ASA 7.x 和 IOS：VPN 分段
- Cisco ASA 5500 系列安全设备
- Cisco PIX 500 系列安全设备
- IPsec 协商/IKE 协议
- Cisco VPN 3000 系列集中器
- 技术支持和文档 - Cisco Systems