

# AnyConnect VPN 客户端故障排除指南 - 常见问题

## 目录

---

### [简介](#)

### [先决条件](#)

[要求](#)

[使用的组件](#)

### [故障排除过程](#)

[安装和虚拟适配器问题](#)

[连接断开或无法建立初始连接](#)

[关于通过流量的问题](#)

[AnyConnect 崩溃问题](#)

[分段/通过流量问题](#)

[自动卸载](#)

[有关填充集群 FQDN 的问题](#)

[备份服务器列表配置](#)

### [AnyConnect : 驱动程序数据库损坏问题](#)

[修复](#)

[修复失败](#)

[分析数据库](#)

### [错误消息](#)

[错误：无法更新会话管理数据库](#)

[解决方案 1](#)

[解决方案 2](#)

[错误：“Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register”](#)

[解决方案](#)

[错误：“收到来自安全网关的响应VPN协商请求的错误。Please contact your network administrator”](#)

[解决方案](#)

[错误：无法建立会话。session limit of 2 reached 警告消息。](#)

[解决方案 1](#)

[解决方案 2](#)

[错误：尝试将anyconnect连接到ASA时，VPN服务器上未启用Anyconnect](#)

[解决方案](#)

[错误：-%ASA-6-722036：组客户端组用户xxxx IP x.x.x.x传输大型数据包1220 \( 阈值1206 \)](#)

[解决方案](#)

[错误：安全网关已拒绝代理的vpn连接或重新连接请求。](#)

[解决方案](#)

[错误：“无法更新会话管理数据库”](#)

[解决方案](#)

---

[错误：“VPN客户端驱动程序遇到错误”](#)

[解决方案](#)

[错误：“无法处理来自xxx.xxx.xxx.xxx的响应”](#)

[解决方案](#)

[错误：“Login Denied, unauthorized connection mechanism, contact your administrator”（登录被拒绝，未授权连接机制，请与管理员联系）](#)

[解决方案](#)

[错误：“Anyconnect软件包不可用或已损坏。请与系统管理员联系”](#)

[解决方案](#)

[错误：“无法找到安全网关上的AnyConnect软件包”](#)

[解决方案](#)

[错误：“不支持通过远程桌面建立安全VPN”](#)

[解决方案](#)

[错误：“收到的服务器证书或其链不符合FIPS。无法建立 VPN 连接”](#)

[解决方案](#)

[错误：“证书验证失败”](#)

[解决方案](#)

[错误：“VPN代理服务遇到问题，需要关闭。很抱歉给您带来不便”](#)

[解决方案](#)

[错误：“无法打开此安装软件包。请验证软件包是否存在”](#)

[解决方案](#)

[错误：“应用转换时出错。请验证指定的转换路径是否有效。”](#)

[解决方案](#)

[错误：“VPN客户端驱动程序遇到错误”](#)

[解决方案](#)

[错误：“VPN重新连接导致不同的配置设置。正在重新初始化 VPN 网络设置。可能需要恢复使用专用网络的应用。”](#)

[解决方案](#)

[登录过程中出现 AnyConnect 错误](#)

[解决方案](#)

[AnyConnect 在 Windows 7 上断开连接后，IE 代理设置未恢复](#)

[解决方案](#)

[错误：在所有这些会话关闭之前，无法启用AnyConnect基础版。](#)

[解决方案](#)

[错误：连接到AnyConnect客户端后，Internet Explorer的Internet选项上的“连接”选项卡会隐藏。](#)

[解决方案](#)

[错误：当其他用户能够通过AnyConnect VPN成功连接时，少数用户收到“登录失败”错误消息](#)

[解决方案](#)

[错误：您正在查看的证书与您正在尝试查看的站点的名称不匹配。](#)

[解决方案](#)

[无法在 Windows 7 计算机上从 CSD Vault 启动 AnyConnect](#)

[解决方案](#)

[故障切换后 AnyConnect 配置文件未复制到备用设备](#)

[解决方案](#)

[如果 Internet Explorer 变为离线状态，AnyConnect 客户端会崩溃](#)

#### [解决方案](#)

[错误消息：TLS\\_PROTOCOL\\_ERROR\\_INSUFFICIENT\\_BUFFER](#)

#### [解决方案](#)

[错误消息：“由于主机条目无效，连接尝试失败”](#)

#### [解决方案](#)

[错误：“如果配置永远在线VPN，请确保您的服务器证书可以通过严格模式”](#)

#### [解决方案](#)

[错误：“An internal error occurred in the Microsoft Windows HTTP Services” \( Microsoft Windows HTTP服务中出现内部错误 \)](#)

#### [解决方案](#)

[错误：“SSL传输收到了安全通道故障。可能是安全网关上的加密配置不受支持的结果。”](#)

#### [解决方案](#)

### [相关信息](#)

---

## 简介

本文档介绍了一个故障排除场景，适用于无法通过 Cisco AnyConnect VPN 客户端运行的应用。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于运行 8.x 版本的思科自适应安全设备 (ASA)。

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。

## 故障排除过程

此典型的故障排除情况适用于通过基于 Microsoft Windows 的计算机的最终用户的 Cisco AnyConnect VPN 客户端不工作的应用程序。这些部分提出以下问题并提供这些问题的解决方案：

- [安装和虚拟适配器问题](#)
- [连接断开或无法建立初始连接](#)
- [关于通过流量的问题](#)
- [AnyConnect 崩溃问题](#)
- [分段/通过流量问题](#)

### 安装和虚拟适配器问题

请完成以下步骤：


## 1. 获取设备日志文件：

- Windows XP/Windows 2000：

```
<#root>  
  
\Windows\setupapi.log
```

- Windows Vista：

---

 注意：必须使隐藏文件夹可见，才能查看这些文件。

---

```
<#root>  
  
\Windows\Inf\setupapi.app.log  
  
  \Windows\Inf\setupapi.dev.log
```

如果您在 setupapi 日志文件中看到错误，可以将信息详细程度设置提高为“0x2000FFFF”。

## 2. 获取 MSI 安装程序日志文件：

如果这是初始 Web 部署安装，则此日志位于每位用户的临时目录中。

- Windows XP/Windows 2000：

```
<#root>  
  
\Documents and Settings\  
  
  \Local Settings\Temp\  
  
  \Temp\
```




```
<#root>
winmsd /nfo c:\msinfo.nfo
```

- Windows Vista :

```
<#root>
msinfo32 /nfo c:\msinfo.nfo
```

---

 注意：键入此提示后，请等待。可能需要二到五分钟完成文件。

---

- b. 通过命令提示符获取 systeminfo 文件转储：

Windows XP 和 Windows Vista：

```
<#root>
systeminfo c:\sysinfo.txt
```

要调试驱动程序问题，请参阅[AnyConnect：损坏的驱动程序数据库问题](#)。

## 连接断开或无法建立初始连接

如果遇到 AnyConnect 客户端连接问题，例如连接断开或无法建立初始连接，请获取这些文件：

- 从 ASA 中获取配置文件，以确定配置中是否存在导致连接失败的问题：

从 ASA 控制台键入 `write net x.x.x.x:ASA-Config.txt`，其中 `x.x.x.x` 是 TFTP 服务器在网络中的 IP 地址。

或者

从 ASA 的控制台，键入 `show running-config`。让屏幕上的配置完成，然后剪切并粘贴到文本编辑器并保存。

- ASA 事件日志：

1. 为了在 ASA 上为授权、WebVPN、安全套接字层 (SSL) 和 SSL VPN 客户端 (SVC) 事件启用日志记录，请发出以下 CLI 命令：

```
<#root>  
  
config terminal  
logging enable  
logging timestamp  
logging class auth console debugging  
logging class webvpn console debugging  
logging class ssl console debugging  
logging class svc console debugging
```

2. 发起 AnyConnect 会话，并确保可以重现故障。将控制台的日志输出捕获到文本编辑器并保存。
3. 要禁用记录，请发出 `no logging enable`。


- 来自客户端 PC 的 Windows 事件查看器的 Cisco AnyConnect VPN 客户端日志：

1. 选择 Start > Run。
2. 输入：

```
eventvwr.msc /s
```

3. 右键单击 Cisco AnyConnect VPN 客户端日志，并选择将日志文件保存为 AnyConnect.evt。

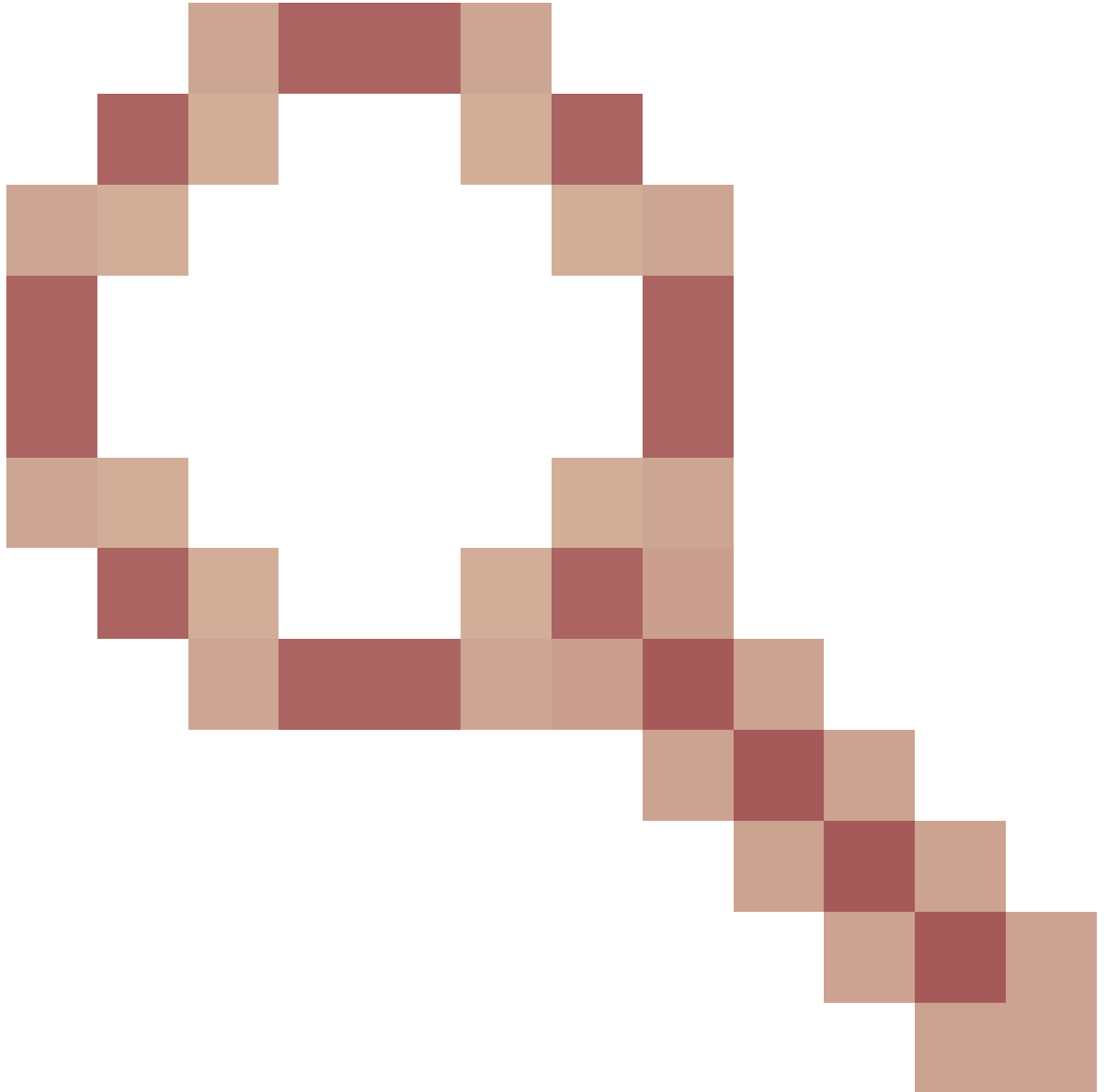
---

 注：请始终将其保存为 .evt 文件格式。

---

如果用户无法与 AnyConnect VPN 客户端连接，则问题可能与已建立的远程桌面协议 (RDP) 会话或客户端 PC 上启用的快速用户切换有关。用户可以看到 `AnyConnect profile settings mandate a single local user, but multiple local users are currently logged into your computer.A VPN connection will not be established` 错误消息出现在客户端 PC 上。要解决此问题，请断开所有已建立的

RDP 会话并禁用快速用户切换。此行为由客户端配置文件中的 [Windows 登录实施](#) 属性控制，但当前没有相关设置实际允许用户在多个用户同时登录同一台计算机时建立 VPN 连接。增强请求



### [CSCsx15061](#)

无法处理此功能。



注：确保端口443未被阻止，以便AnyConnect客户端可以连接到ASA。

当用户不能将 AnyConnect VPN 客户端连接到 ASA 时，问题也许由 AnyConnect 客户端版本与 ASA 软件镜像版本不兼容导致。在这种情况下，用户收到以下错误消息：`The installer was not able to start the Cisco VPN client, clientless access is not available.`

要解决此问题，请升级 AnyConnect 客户端版本，以与 ASA 软件镜像兼容。

当用户首次登录 AnyConnect 时，登录脚本不会运行。如果断开连接并再次登录，登录脚本将正常运行。这是预料之中的行为。

将AnyConnect VPN客户端连接到ASA时，您可能会收到以下错误：`User not authorized for AnyConnect Client access, contact your administrator.`



当 ASA 中缺少 AnyConnect 镜像时，将会看到此错误。一旦将镜像加载到 ASA，AnyConnect 就可以正常连接到 ASA。

此错误可以通过禁用数据报传输层安全 (DTLS) 来解决。转到配置 > 远程接入 VPN > 网络 (客户端) 接入 > AnyConnect 连接配置文件并取消选中启用 DTLS 复选框。这将禁用 DTLS。

当用户断开连接时，dartbundle文件会显示以下错误消息

: TUNNELPROTOCOLDPDMGR\_ERROR\_NO\_DPD\_RESPONSE : 安全网关无法响应失效对等体检测数据包。此错误意味着 DTLS 信道由于失效对等体检测 (DPD) 故障而中断。如果您调整 DPD 保持连接并发出以下命令，则会解决此错误：

```
<#root>
```

```
webvpn
  svc keepalive 30
  svc dpd-interval client 80
  svc dpd-interval gateway 80
```

在 ASA 版本 8.4 (1) 及更高版本中，svc keepalive 和 svc dpd-interval 命令分别应替换为 anyconnect keepalive 和 anyconnect dpd-interval 命令，如下所示：

```
<#root>
```

```
webvpn
anyconnect ssl keepalive 15
anyconnect dpd-interval client 5
anyconnect dpd-interval gateway 5
```

## 关于通过流量的问题

如果在 ASA 上通过 AnyConnect 会话将流量传递到专用网络时检测到问题，请完成以下数据收集步骤：

1. 从控制台获取 show vpn-sessiondb detail svc filter name <username> ASA 命令的输出。如果输出显示 Filter Name: XXXXX，则收集 show access-list XXXXX 的输出。验证访问列表 XXXXX 不会阻塞预计的通信流。
2. 从 AnyConnect VPN Client > Statistics > Details > Export 导出 AnyConnect 统计信息 (AnyConnect-ExportedStats.txt)。
3. 检查 nat 语句的 ASA 配置文件。如果启用了网络地址转换 (NAT)，则必须排除豁免由于 NAT 而返回到客户端的数据。例如，要对 NAT 排除 (nat 0) 来自 AnyConnect 池的 IP 地址，请在 CLI 上使用：

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. 确定是否需要针对设置启用隧道化默认网关。传统默认网关是非解密流量的最后选用网关。

示例：

```
<#root>

!--- Route outside 0 0 is an incorrect statement.

route outside 0 0 10.145.50.1
route inside 0 0 10.0.4.2

tunneled
```

例如，如果 VPN 客户端需要访问不在 VPN 网关的路由表里的资源，则数据包通过标准的默认网关路由。VPN 网关不需要完成内部路由表来解决此问题。可以在此实例中使用 tunneled 关键字。

5. 验证 ASA 的检查策略是否丢弃了 AnyConnect 流量。如果您实施思科 ASA 的模块化策略框架，则可以排除豁免 AnyConnct 客户端使用的特定应用。例如，您可以使用以下命令豁免瘦客户端协议。

```
<#root>

ASA(config)#
policy-map global_policy

ASA(config-pmap)#
class inspection_default

ASA(config-pmap-c)#
no inspect skinny
```

## AnyConnect 崩溃问题

完成以下数据收集步骤：

1. 确保 Microsoft 实用程序 Dr Watson 已启用。为此，请选择“开始”>“运行”，然后运行 Drwtsn32.exe。对此进行配置并单击 OK：

```
Number of Instructions      : 25
Number of Errors To Save   : 25
Crash Dump Type            : Mini
Dump Symbol Table          : Checked
Dump All Thread Contexts   : Checked
Append To Existing Log File : Checked
Visual Notification        : Checked
Create Crash Dump File     : Checked
```

当发生崩溃时，请从 C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson 收集 .log 和 .dmp 文件。如果显示这些文件正在使用中，则请使用 ntbackup.exe。

2. 获取来自客户端 PC 的 Windows 事件查看器的 Cisco AnyConnect VPN 客户端日志：

- a. 选择 Start > Run。


- b. 输入：

```
<#root>
```

```
eventvwr.msc /s
```

- c. 右键单击 Cisco AnyConnect VPN 客户端日志，并选择将日志文件保存为 AnyConnect.evt。

---

 注：请始终将其保存为 .evt 文件格式。

---

## 分段/通过流量问题

一些应用程序（例如 Microsoft Outlook）不工作。但是，隧道能通过其他流量，例如小 ping。

这可为网络中的分段问题提供线索。消费路由器尤其不擅长数据包分段和重组。

尝试一组 ping 操作，逐步扩大范围，以确定它是否会在达到特定大小时操作失败。例如，ping -l 500、ping -l 1000、ping -l 1500、ping -l 2000。

建议为遇到分段的用户配置特殊组，并将该组的 SVC 最大传输单元 (MTU) 设置为 1200。这允许您修正遇到此问题的用户，而不影响更多的用户群。

## 问题

一旦与 AnyConnect 连接，TCP 连接就暂停。

## 解决方案

要验证您的用户是否有分段问题，请调整 ASA 上 AnyConnect 客户端的 mtu。

```
ASA(config)#group-policy <name> attributes
                webvpn
                    svc mtu 1200
```

## 自动卸载

### 问题

一旦连接终止，AnyConnect VPN 客户端就自行卸载。客户端日志显示“保持已安装”设置为已禁用。

### 解决方案

尽管在自适应安全设备管理器 (ASDM) 上选择了保持已安装选项，AnyConnect 仍自行卸载。要解决此问题，请根据组策略配置 `svc keep-installer installed` 命令。

## 有关填充集群 FQDN 的问题

问题：AnyConnect 客户端已预填充主机名，而不是集群完全限定域名 (FQDN)。

如果您为 SSL VPN 设置了负载均衡集群并且客户端尝试连接集群，该请求将被重定向到 ASA 节点并且客户端成功登录。一段时间后，当客户端再次尝试连接集群时，连接到条目中不显示集群 FQDN，而是显示客户端已重定向到的 ASA 节点条目。

### 解决方案

发生这种情况的原因是 AnyConnect 客户端会保留最后一次连接的主机名。系统我们已观察到此行为，并报告了漏洞。有关该漏洞的完整详细信息，请参阅思科漏洞 ID [CSCsz39019](#)。建议的解决方法是将思科 AnyConnect 升级到版本 2.5。

## 备份服务器列表配置

配置备份服务器列表的目的是为了防止用户选择的主服务器无法访问。请在 AnyConnect 配置文件的备份服务器窗格中定义此配置。请完成以下步骤：

1. 下载 [AnyConnect 配置文件编辑器 \(仅限注册用户\)](#)。该文件名为

AnyConnectProfileEditor2\_4\_1.jar。

2. 使用 AnyConnect 配置文件编辑器创建 XML 文件。

- a. 转到服务器列表选项卡。
- b. 单击 Add。
- c. 在主机名字段中输入主服务器。
- d. 在主机地址字段的备份服务器列表下添加备份服务器。然后点击添加。

3. 有了 XML 文件后，需要将其分配给在 ASA 上使用的连接。

- a. 在 ASDM 中，依次选择配置 > 远程接入 VPN > 网络 ( 客户端 ) 接入 > AnyConnect 连接配置文件。
- b. 选择配置文件并点击编辑。
- c. 在“默认组策略”部分中点击管理。
- d. 选择组策略并点击编辑。
- e. 选择高级，然后点击 SSL VPN 客户端。
- f. 单击 New。然后，您需要为配置文件键入名称并分配 XML 文件。

4. 将客户端连接到会话，以便下载 XML 文件。

## AnyConnect：驱动程序数据库损坏问题

SetupAPI.log 文件中的此条目表示目录系统损坏：

W239 驱动程序签名类别列表“C:\WINDOWS\INF\certclas.inf”缺失或无效。错误0xfffffde5：未知错误。假设所有设备类都受驱动程序签名策略约束。

您还可以收到此错误消息：Error(3/17)：无法启动VA、设置共享队列或VA放弃共享队列。

您可以在客户端上收到此日志：“VPN客户端驱动程序遇到错误”。

### 修复

此问题是由于思科漏洞 ID [CSCsm54689](#) 引起的。要解决此问题，请确保在您启动 AnyConnect 前已禁用路由和远程访问服务。如果这不能解决问题，请完成这些步骤：

1. 以 PC 管理员身份打开命令提示符 ( 在 Vista 上为提升的命令提示符 ) 。
2. 运行 `net stop CryptSvc`。
3. 运行 :

```
esentutl /p%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

4. 出现提示时，选择确定以尝试修复。
5. 退出命令提示符。
6. 重新启动。

## 修复失败

如果修复失败，请完成这些步骤：

1. 以 PC 管理员身份打开命令提示符 ( 在 Vista 上为提升的命令提示符 ) 。
2. 运行 `net stop CryptSvc`。
3. 重命名 `%WINDIR%\system32\catroot2` to `catroot2_old` 目录。
4. 退出命令提示符。
5. 重新启动。

## 分析数据库

您可以随时分析数据库以确定它是否有效。

1. 以 PC 管理员身份打开命令提示符。
2. 运行 :

```
esentutl /g%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

有关详细信息，请参阅[系统目录数据库完整性](#)。

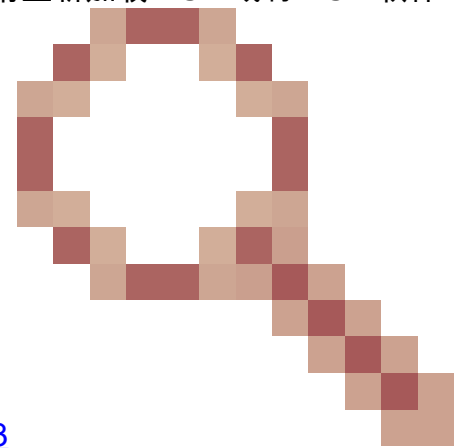
## 错误消息

### 错误：无法更新会话管理数据库

当SSL VPN通过Web浏览器连接时，会出现Unable to Update the Session Management Database.错误消息，并且ASA日志显示%ASA-3-211001: Memory allocation Error。自适应安全设备无法分配RAM 系统内存。

### 解决方案 1

此问题是由于思科漏洞 ID [CSCsm51093](#) 引起的。要解决此问题，请重新加载 ASA 或将 ASA 软件



升级到 Bug 中提及的临时版本。请参阅Cisco Bug ID [CSCsm51093](#)

。

### 解决方案 2

如果使用了威胁检测，则禁用 ASA 上的威胁检测也可以解决此问题。

错误：“Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register”

如果在笔记本电脑或 PC 上使用 AnyConnect 客户端，安装过程中会出现错误：

```
"Module C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register..."
```

遇到此错误时，安装程序无法继续，将删除客户端。

### 解决方案

这些是可能解决此错误的应急方案：

- 最新的 AnyConnect 客户端不再受 Microsoft Windows 2000 的正式支持。这是 2000 计算机

的注册问题。

- 删除 vmware 应用程序。一旦安装了 AnyConnect , vmware 应用程序即可添加回 PC。
- 将 ASA 添加到其受信任的站点。
- 将这些文件从 \ProgramFiles\Cisco\CiscoAnyconnect 文件夹复制到新文件夹 , 并运行 regsvr32 vpnapi.dll 命令提示符 :
  - vpnapi.dll
  - vpncommon.dll
  - vpncommoncrypt.dll
- 重新映像笔记本电脑/PC 上的操作系统。

AnyConnect 客户端上与此错误相关的日志消息与此类似 :

```
DEBUG: Error 2911: Could not remove the folderC:\Program Files\Cisco\Cisco AnyConnect VPN Client\.  
The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 2911. The arguments are:  
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,  
DEBUG: Error 2911: Could not remove the folder C:\Program Files\Cisco\Cisco AnyConnect VPN Client\.  
The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 2911. The arguments are:  
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,  
Info 1721. There is a problem with this Windows Installer package. A program required for this install to complete could not be run. Contact your support personnel or package vendor. Action: InstallHelper.exe, location: C:\Program Files\Cisco\Cisco AnyConnect VPN Client\InstallHelper.exe, command: -acl "C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\\" -r
```

错误：“收到来自安全网关的响应VPN协商请求的错误。Please contact your network administrator”

当客户端尝试使用思科 AnyConnect VPN 客户端连接 VPN 时，将收到此错误。

从安全网关收到此消息：

“Illegal address class”或“Host or network is 0”或“Other error”

## 解决方案

造成此问题的原因是 ASA 本地 IP 池耗尽。由于 VPN 池资源耗尽，必须扩大 IP 池范围。

针对此问题报告的思科漏洞 ID 是 [CSCsl82188](#)。如果用于分配的本地地址池资源耗尽，或者将 32



位子网掩码用于地址池，通常会出现此错误。解决方法是扩展地址池，并为池使用 24 位子网掩码。


错误：无法建立会话。session limit of 2 reached 警告消息。

当您尝试通过 AnyConnect VPN 客户端连接两个以上的客户端时，客户端上会收到登录失败错误消息，并且 ASA 日志中会出现无法建立会话警告消息。session limit of 2 reached 警告消息。我有 ASA 的 AnyConnect essential 许可证，ASA 运行版本 8.0.4。

## 解决方案 1

出现此错误的原因是 ASA 版本 8.0.4 不支持 AnyConnect essential 许可证。您需要将 ASA 升级到版本 8.2.2。这将解决该错误。

---

 注意：无论使用何种许可证，如果达到会话限制，用户都将收到login failed错误消息。

---

## 解决方案 2

如果使用 vpn-sessiondb max-anyconnect-premium-or-essentials-limit session-limit 命令设置允许建立的 VPN 会话数量限制，也会出现此错误。如果会话限制设置为两个，则即使安装的许可证支持更多会话，用户也无法建立两个以上的会话。请将会话限制设置为所需的 VPN 会话数，以避免出现此错误消息。

错误：尝试将anyconnect连接到ASA时，VPN服务器上未启用Anyconnect

尝试将 Anyconnect 连接到 ASA 时，会收到 VPN 服务器上未启用 Anyconnect 错误消息。

## 解决方案

如果通过 ASDM 在 ASA 的外部接口上启用 AnyConnect，则可以解决此错误。有关如何在外部接口上启用 AnyConnect 的详细信息，请参阅[在 ASA 上配置无客户端 SSL VPN \(WebVPN\)](#)。

错误：- %ASA-6-722036：组客户端组用户xxxx IP x.x.x.x传输大型数据包1220 ( 阈值1206 )

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

## 解决方案

此日志消息说明已向客户端发送了一个大型数据包。数据包的源不能识别客户端的 MTU。这也可能是由于对不可压缩的数据进行了压缩所致。解决方法是使用 svc compression none 命令关闭 SVC 压缩。这将解决该问题。

错误：安全网关已拒绝代理的vpn连接或重新连接请求。

当您连接到AnyConnect客户端时，会收到以下错误：“安全网关已拒绝代理的vpn连接或重新连接请求。”(The secure gateway has rejected the agent's vpn connect or reconnect request.)新连接需要重新进行身份验证，并且必须手动启动。如果此问题仍然存在，请与网络管理员联系。从安全网关收到了以下消息：no assigned address”。

当您连接到AnyConnect客户端时，也会收到此错误：“安全网关已拒绝连接尝试。需要尝试与同一安全网关或其他安全网关建立新连接，必须重新进行身份验证。从安全网关收到了以下消息：主机或网络为0”。

当您连接到AnyConnect客户端时，也会收到此错误：“安全网关已拒绝代理的vpn连接或重新连接请求。”(The secure gateway has rejected the agent's vpn connect or reconnect request.)新连接需要重新进行身份验证，并且必须手动启动。如果问题仍然存在，请与网络管理员联系。从安全网关收到以下消息：No License”。

## 解决方案

重新加载后，路由器缺少池配置。您需要将相关配置重新添加到路由器中。

```
<#root>
```

```
Router#
```

```
show run | in pool
```

```
ip local pool SSLPOOL 192.168.30.2 192.168.30.254  
  svc address-pool SSLPOO
```

“安全网关拒绝了代理的 VPN 连接或重新连接请求。新连接需要重新进行身份验证，并且必须手动启动。如果问题仍然存在，请与网络管理员联系。从安全网关收到以下消息：AnyConnect移动许可证缺失时，出现No License（无许可证）错误。安装许可证后，便可解决问题。

## 错误：“无法更新会话管理数据库”

当您尝试在WebPortal中进行身份验证时，会收到以下错误消息：“无法更新会话管理数据库”。

## 解决方案

此问题与 ASA 上的内存分配有关。如果 ASA 版本为 8.2.1，通常会遇到此问题。最初，需要使用 512MB RAM 才能实现完整功能。

要永久解决此问题，请将内存升级到 512MB。

作为临时解决方法，请尝试通过以下步骤释放内存：

1. 禁用威胁检测。
2. 禁用 SVC 压缩。
3. 重新加载 ASA。

## 错误：“VPN客户端驱动程序遇到错误”

尝试连接 AnyConnect 时，客户端计算机上会收到此错误消息。

### 解决方案

为了解决此错误，请完成以下步骤，手动将 AnyConnect VPN 代理设置为交互式：

1. 右键单击我的电脑 > 管理 > 服务和应用 > 服务 > 并选择思科 AnyConnect VPN 代理。
2. 右键单击属性，然后登录并选择允许服务与桌面交互。

这会将 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\vpnagent 的注册表类型值 DWORD 设置为 110 ( 默认值为 010 )。



**注意：**如果要使用此项，则首选在此实例中使用.MST转换。这是因为如果您使用这些方法手动设置此选项，则每次安装/升级流程后都需要设置此选项。因此，您需要确定导致此问题的应用。

在Windows PC上启用路由和远程访问服务(RRAS)时，AnyConnect失败，并且VPN客户端驱动程序遇到错误。错误消息。为了解决此问题，请确保在启动 AnyConnect 之前禁用路由和 RRAS。有关详细信息，请参阅思科漏洞 ID [CSCsm54689](#)。

## 错误：“无法处理来自xxx.xxx.xxx.xxx的响应”

AnyConnect 客户端无法连接到思科 ASA。AnyConnect 窗口中显示的错误是“无法处理来自 xxx.xxx.xxx.xxx 的响应”。

### 解决方案

要解决此错误，请尝试以下解决方法：

- 从 ASA 中移除 WebVPN，然后重新启用。<
- 将端口号从现在的 443 更改为 444，然后在 443 上重新启用 WebVPN。

有关如何启用 WebVPN 和更改 WebVPN 端口的详细信息，请参阅此[解决方案](#)。

错误：“Login Denied， unauthorized connection mechanism， contact your administrator” ( 登录被拒绝， 未授权连接机制， 请与管理员联系 )

AnyConnect 客户端无法连接到思科 ASA。AnyConnect 窗口中的错误是“登录被拒绝·未授权的连接机制

· 请与管理员联系”。

## 解决方案

此错误消息主要是由于配置不正确或配置不完整导致的。请检查配置，确保按要求配置，以解决此问题。

<

错误：“Anyconnect软件包不可用或已损坏。请与系统管理员联系”

尝试从 Macintosh 客户端启动 AnyConnect 软件以连接到 ASA 时，会发生此错误。

## 解决方案

为了解决这一问题，请完成以下步骤：

1. 将 Macintosh AnyConnect 软件包上传到 ASA 的闪存中。
2. 修改 WebVPN 配置以指定所使用的 AnyConnect 软件包。

```
webvpn
  svc image disk0:/anyconnect-macosx-i386-2.3.2016-k9.pkg 2
  svc image disk0:/anyconnect-macosx-powerpc-2.3.2016-k9.pkg 3
```

在 ASA 版本 8.4(1) 及更高版本中，svc image 命令应替换为 anyconnect image 命令，如下所示：

```
<#root>
hostname(config)#
webvpn

hostname(config-webvpn)#
anyconnect image disk0:/

anyconnect-win-3.0.0527-k9.pkg 1

hostname(config-webvpn)#
anyconnect image disk0:/

anyconnect-macosx-i386-3.0.0414-k9.pkg 2
```

## 错误：“无法找到安全网关上的AnyConnect软件包”

如果用户的 Linux 计算机试图通过启动 AnyConnect 连接到 ASA，会导致此错误。以下是完整错误消息：

```
<#root>
```

```
"The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again."
```

## 解决方案

为了解决此错误消息，请验证客户端计算机上使用的操作系统 (OS) 是否受 AnyConnect 客户端支持。

如果操作系统受支持，则验证是否在 WebVPN 配置中指定了 AnyConnect 软件包。有关详细信息，请参阅本文档的 [Anyconnect 软件包不可用或已损坏部分](#)。

## 错误：“不支持通过远程桌面建立安全VPN”

用户无法执行远程桌面访问。系统显示不支持通过远程桌面连接 Secure VPN 错误消息。

## 解决方案

此问题是由以下Cisco Bug ID导致的：[CSCsu2208](#)和[CSCso42825](#)。如果升级 AnyConnect VPN 客户端，可以解决此问题。有关详细信息，请参阅以下漏洞。

## 错误：“收到的服务器证书或其链不符合FIPS。无法建立 VPN 连接”

尝试将 VPN 连接到 ASA 5505 时，系统显示收到的服务器证书或证书链不符合 FIPS。无法建立 VPN 连接错误消息。

## 解决方案

为了解决此错误，必须在 AnyConnect 本地策略文件中禁用联邦信息处理标准 (FIPS)。通常可以在 `C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\AnyConnectLocalPolicy.xml` 路径下找到该文件。如果在此路径下找不到该文件，则在其他目录的路径（例如 `C:\Documents and Settings\AllUsers\Application Data\Cisco AnyConnectVPNClient\AnyConnectLocalPolicy.xml`）下查找该文件。找到该 xml 文件后，对文件进行如下更改：

将口令短语：

```
<FipsMode>true</FipsMode>
```

更改为：

```
<FipsMode>>false</FipsMode>
```

然后，重启计算机。用户必须具有管理权限才能修改该文件。

错误：“证书验证失败”

用户无法启动 AnyConnect，并且收到证书验证失败错误。

## 解决方案

AnyConnect 的证书身份验证方式与 IPsec 客户端不同。为了使证书身份验证正常运行，必须将客户端证书导入到浏览器中并更改连接配置文件，才能使用证书身份验证。还需要在 ASA 上启用以下命令，以便允许在外部接口上使用 SSL 客户端证书：

```
ssl certificate-authentication interface outside port 443
```

错误：“VPN代理服务遇到问题，需要关闭。很抱歉给您带来不便”

如果 Windows XP PC 上安装了 AnyConnect 版本 2.4.0202，它会在更新本地化文件时停止并显示 vpnagent.exe 失败错误消息。

## 解决方案

思科漏洞 ID [CSCsq49102](#) 中记录了此行为。建议的解决方法是禁用 Citrix 客户端。

错误：“无法打开此安装软件包。请验证软件包是否存在”

下载 AnyConnect 时，会收到此错误消息：

“请与系统管理员联系。安装程序失败，出现以下错误：无法打开此安装包。请验证软件包是否存在以及您是否具有访问权限，或者与应用供应商联系，验证此 Windows 安装程序包是否有效。”

## 解决方案

要解决此问题，请完成以下步骤：

1. 删除所有防病毒软件。
2. 禁用 Windows 防火墙。
3. 如果第 1 步或第 2 步都无法解决问题，请将计算机格式化，然后进行安装。
4. 如果问题仍然存在，请创建 [TAC 支持请求](#)。

错误：“应用转换时出错。请验证指定的转换路径是否有效。”

从 ASA 自动下载 AnyConnect 时会收到此错误消息：

```
<#root>
```

```
"Contact your system administrator. The installer failed with the following error:  
Error applying transforms. Verify that the specified transform paths are valid."
```

运行 MacOS 的情况下连接适用于 MacOS 的 AnyConnect 时，会收到此错误消息：

```
<#root>
```

```
"The AnyConnect package on the secure gateway could not be located. You may be  
experiencing network connectivity issues. Please try connecting again."
```

## 解决方案

为了解决此问题，请使用以下解决方法之一：

1. 此错误的根本原因可能是由于MST 转换文件损坏（例如，导入的文件）。请执行以下步骤来解决此问题：
  - a. 删除 MST 转换表。
  - b. 在 ASA 中为 MacOS 配置 AnyConnect 映像。
2. 在 ASDM 中，转到网络（客户端）接入 > AnyConnect 自定义 > 安装路径并删除 AnyConnect 软件包文件。确保软件包保留在网络（客户端）接入 > 高级 > SSL VPN > 客户端设置中。

如果这些解决方法都无法解决问题，请与[思科技术支持](#)部门联系。

错误：“VPN客户端驱动程序遇到错误”

收到此错误：

```
<#root>
```

```
The VPN client driver has encountered an error when connecting through Cisco  
AnyConnect Client.
```

## 解决方案

可以通过以下方法解决此问题：在卸载 AnyConnect 客户端时，删除防病毒软件，然后重新安装 AnyConnect 客户端。如果此解决方案不起作用，则重新格式化 PC 以解决此问题。

错误：“VPN重新连接导致不同的配置设置。正在重新初始化 VPN 网络设置。可能需要恢复使用专用网络的应用。”

尝试启动 AnyConnect 时，收到此错误：

```
<#root>
```

```
"A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restarted."
```

## 解决方案

要解决此错误，请使用以下解决方法：

```
group-policy <Name> attributes
    webvpn
        svc mtu 1200
```

在 ASA 版本 8.4(1) 及更高版本中，svc mtu 命令应替换为 anyconnect mtu 命令，如下所示：

```
<#root>
```

```
hostname(config)#
```

```
group-policy
```

```
    attributes
```



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

```
webvpn
```

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

```
anyconnect mtu 500
```

## 登录过程中出现 AnyConnect 错误

### 问题

AnyConnect 在连接到客户端时收到此错误：

```
The VPN connection is not allowed via a local proxy. This can be changed through AnyConnect profile settings.
```

### 解决方案

如果对 AnyConnect 配置文件进行如下更改，则可以解决此问题：

将此行添加到 AnyConnect 配置文件中：

```
<ProxySettings>IgnoreProxy</ProxySettings><
AllowLocalProxyConnections>
false</AllowLocalProxyConnections>
```

## AnyConnect 在 Windows 7 上断开连接后，IE 代理设置未恢复

### 问题

在 Windows 7 中，如果将 IE 代理设置配置为自动检测设置，并且 AnyConnect 向下推送新的代理设置，则在用户结束 AnyConnect 会话后，IE 代理设置不会恢复为自动检测设置。如果用户需要将代理设置配置为自动检测设置，则在这种情况下会遇到局域网问题。

### 解决方案

思科漏洞 ID [CSCtj51376](#) 中记录了此行为。建议的解决方法是升级到 [AnyConnect 3.0](#)。

错误：在所有这些会话关闭之前，无法启用 AnyConnect 基础版。

尝试启用 AnyConnect 基础版许可证时，会在思科 ASDM 上收到此错误消息：

<#root>

There are currently 2 clientless SSL VPN sessions in progress. AnyConnect Essentials can not be enabled until all these sessions are closed.

## 解决方案

这是 ASA 的正常行为。AnyConnect 基础版是拥有单独许可的 SSL VPN 客户端。它全部在 ASA 上配置，并提供完整的 AnyConnect 功能，以下情况下例外：

- 未安装思科 Secure Desktop (CSD) ( 包括 HostScan/存储库/缓存清理器 )
- 未安装无客户端 SSL VPN
- 可选的 Windows 移动支持

此许可证不能与共享 SSL VPN 高级许可证同时使用。当您需要使用其中一个许可证时，需要禁用其他许可。

错误：连接到AnyConnect客户端后，Internet Explorer的Internet选项上的“连接”选项卡会隐藏。

连接到 AnyConnect 客户端后，Internet Explorer 的 Internet 选项中的连接选项卡会隐藏起来。

## 解决方案

这是由于 msie-proxy lockdown 功能导致的。启用此功能，将会在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的“连接”选项卡。如果禁用此功能，则不会更改“连接”选项卡的显示会保持不变。

错误：当其他用户能够通过AnyConnect VPN成功连接时，少数用户收到“登录失败”错误消息

很多用户能够通过 AnyConnect VPN 成功连接，有少数用户则会收到“登录失败”错误消息。

## 解决方案

确保为用户选中了不要求预先身份验证复选框，则可以解决此问题。

错误：您正在查看的证书与您正在尝试查看的站点的名称不匹配。

在 AnyConnect 配置文件更新过程中，系统显示一个错误，指出证书无效。此问题仅在 Windows 上更新配置文件的过程中出现。该错误消息显示如下：

<#root>

The certificate you are viewing does not match with the name of the site you are trying to view.


## 解决方案

如果修改 AnyConnect 配置文件的服务器列表以使用证书的 FQDN，则可以解决此问题。

以下是 XML 配置文件的示例：

```
<ServerList>
  <HostEntry>
    <HostName>vpn1.ccsd.net</HostName>
  </HostEntry>
</ServerList>
```

---

 注：如果服务器的公有IP地址存在条目，如<HostAddress>，则将其删除并仅保留服务器的 FQDN(例如，<HostName>，但不保留<Host Address>)。

---

## 无法在 Windows 7 计算机上从 CSD Vault 启动 AnyConnect

从 CSD Vault 启动 AnyConnect 时，AnyConnect 不运行。该操作是在 Windows 7 计算机上尝试执行的。

## 解决方案

目前无法执行该操作，因为不受支持。

## 故障切换后 AnyConnect 配置文件未复制到备用设备

AnyConnect 3.0 VPN 客户端可以与 ASA 版本 8.4.1 软件配合使用。但是，在故障切换之后，没有与 AnyConnect 配置文件相关的配置复制。

## 解决方案

此问题已被发现并记录在思科漏洞 ID [CSCtn71662](#) 下。临时解决方法是手动将文件复制到备用单元设备。

## 如果 Internet Explorer 变为离线状态，AnyConnect 客户端会崩溃

发生这种情况时，AnyConnect 事件日志包含与以下内容类似的条目：

Description : Function:  
CAdapterNetworkStateIfc::SetConnectedStateToConnected  
File: .\AdapterNetworkStateIfc.cpp  
Line: 147  
Invoked Function: InternetSetOption  
Return Code: 12010 (0x00002EEA)  
Description: The length is incorrect for the option type

Description : Function: CTransportWinHttp::InitTransport  
File: .\CTransportWinHttp.cpp  
Line: 252  
Invoked Function: CConnectedStateIfc::SetConnectedStateToConnected  
Return Code: -25362420 (0xFE7D000C)  
Description: CADAPTERNETWORKSTATEIFC\_ERROR\_SET\_OPTION

## 解决方案

此行为已被发现并记录在思科漏洞 ID [CSCtx28970](#) 下。为了解决这个问题，请退出 AnyConnect 应用并重启。重启后，连接条目会重新显示。

## 错误消息：TLSPROTOCOL\_ERROR\_INSUFFICIENT\_BUFFER

AnyConnect 客户端无法连接，并且收到无法建立连接错误消息。在 AnyConnect 事件日志中，发现 TLSPROTOCOL\_ERROR\_INSUFFICIENT\_BUFFER 错误。

## 解决方案

如果头端的分离隧道配置了非常大的分离隧道列表（大约 180-200 个条目），并且在组策略（如 dns-server）中配置了一个或多个其他客户端属性，则会出现此错误。

要解决此问题，请完成以下步骤：

1. 减少分离隧道列表中的条目数。
2. 使用以下配置，禁用 DTLS：

```
group-policy groupName attributes
  webvpn
    svc dtls none
```

有关详细信息，请参阅思科漏洞 ID [CSCtc41770](#)。

## 错误消息：“由于主机条目无效，连接尝试失败”

使用证书对 AnyConnect 进行身份验证时，会收到由于主机条目无效，连接尝试失败错误消息。

## 解决方案

为了解决此问题，请尝试以下任一解决方案：

- 将 AnyConnect 升级到版本 3.0。
- 在计算机上禁用思科 Secure Desktop。

有关详细信息，请参阅思科漏洞 ID [CSCti73316](#)。

错误：“如果配置永远在线VPN，请确保您的服务器证书可以通过严格模式”

在 AnyConnect 上启用“永远在线”功能时，会收到如果您配置了永远在线 VPN，请确保您的服务器证书可以通过严格模式错误消息。

## 解决方案

此错误消息意味着，如果要使用“永远在线”功能，您需要在头端配置一个有效的服务器证书。如果没有有效的服务器证书，此功能将无法正常运行。“严格证书模式”是您在 AnyConnect 本地策略文件中设置的选项，目的是确保连接使用有效的证书。如果在策略文件中启用此选项并使用假证书进行连接，则连接将失败。

错误：“An internal error occurred in the Microsoft Windows HTTP Services” ( Microsoft Windows HTTP服务中出现内部错误 )

以下 AnyConnect 诊断报告工具 (DART) 显示一次失败的尝试：

<#root>

\*\*\*\*\*

Date : 03/25/2014  
Time : 09:52:21  
Type : Error  
Source : acvpnu

Description : Function: CTransportWinHttp::SendRequest  
File: .\CTransportWinHttp.cpp  
Line: 1170

Invoked Function: HttpSendRequest

Return Code: 12004 (0x00002EE4)  
Description:

An internal error occurred in the Microsoft  
Windows HTTP Services

\*\*\*\*\*

Date : 03/25/2014  
Time : 09:52:21  
Type : Error  
Source : acvpnu

Description : Function: ConnectIfc::connect  
File: .\ConnectIfc.cpp  
Line: 472

```
Invoked Function: ConnectIfc::sendRequest
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN
*****
Date       : 03/25/2014
Time       : 09:52:21
Type       : Error
Source     : acvpnui
```

```
Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 2999
Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN
```

Connection attempt failed. Please try again.

```
*****
```

另外，请参阅 Windows 计算机上的事件查看器日志。

## 解决方案

这可能是由于 Winsock 连接损坏造成的。请使用以下命令通过从命令提示符下使用以下命令重置连接，然后重启 Windows 计算机：

```
netsh winsock reset
```

有关详细信息，请参阅[如何在 Windows Server 2003、Windows XP 和 Windows Vista 中确定 Winsock2 损坏并恢复 Winsock2 知识库文章。](#)

错误：“SSL传输收到了安全通道故障。可能是安全网关上的加密配置不受支持的结果。”

以下 AnyConnect 诊断报告工具 (DART) 显示一次失败的尝试：

```
*****
```

```
Date       : 10/27/2014
Time       : 16:29:09
Type       : Error
Source     : acvpnui
```

```
Description : Function: CTransportWinHttp::handleRequestError
File: .\CTransportWinHttp.cpp
Line: 854
```

The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configuration

```
*****
```

```
Date       : 10/27/2014
Time       : 16:29:09
Type       : Error
```

Source : acvpnui

Description : Function: CTransportWinHttp::SendRequest  
File: .\CTransportWinHttp.cpp  
Line: 1199  
Invoked Function: CTransportWinHttp::handleRequestError  
Return Code: -30015418 (0xFE360046)  
Description: CTRANSPORT\_ERROR\_SECURE\_CHANNEL\_FAILURE

\*\*\*\*\*

Date : 10/27/2014  
Time : 16:29:09  
Type : Error  
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode  
File: .\ConnectIfc.cpp  
Line: 3026  
Invoked Function: ConnectIfc::TranslateStatusCode  
Return Code: -30015418 (0xFE360046)  
Description: CTRANSPORT\_ERROR\_SECURE\_CHANNEL\_FAILURE  
Connection attempt failed. Please try again.  
\*\*\*\*\*

## 解决方案

根据以下 KB 更新，Windows 8.1 不支持 RC4：

<http://support2.microsoft.com/kb/2868725>

使用命令“ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1”在 ASA 上为 SSL VPN 配置 DES / 3DES 密码，或者编辑客户端计算机上的 Windows 注册表文件，如下所述：

<https://technet.microsoft.com/en-us/library/dn303404.aspx>

## 相关信息

- [Cisco ASA 5500 系列自适应安全设备](#)
- [AnyConnect VPN 客户端常见问题](#)
- [Cisco Secure Desktop \(CSD\) 常见问题](#)
- [Cisco AnyConnect VPN 客户端](#)
- [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）。