AnyConnect 故障排除

收集用于故障排除的信息

查看统计详细信息

管理员或最终用户可查看当前 AnyConnect 会话的统计信息。

步骤 1 在 Windows 上，导航到**高级窗口** > **统计信息** > **VPN 文件夹**。在 Linux 上，单击用户 GUI 中的**详细信息 (Details)** 按钮。

步骤 2 根据客户端计算机上加载的软件包，从以下选项中进行选择。

- **Export Stats** - 将连接统计信息保存为一个文本文件，供以后分析和调试。
- **Reset** - 将连接信息重置为零。AnyConnect 将立即开始收集新数据。
- **Diagnostics** - 启动 AnyConnect 诊断和报告工具 (DART) 向导，该向导将捆绑指定日志文件和诊断信息，供客户端连接的分析和调试。

运行 DART 以收集用于故障排除的数据

DART 是 AnyConnect 诊断和报告工具，可用来收集数据以对 AnyConnect 安装和连接问题进行故障排除。DART 收集日志、状态和诊断信息，以供思科技术支持中心 (TAC) 分析。

DART 向导在运行 AnyConnect 的设备上运行。您可以从 AnyConnect 启动 DART 或不使用 AnyConnect 自行启动它。

注释 DART 需要 macOS、Ubuntu 18.04 和 Red Hat 7 的管理员权限才能收集日志。

此外，仅对于 ISE 终端安全评估，一旦发生 ISE 终端安全评估崩溃或终端变为不合规，您可以自动收集 DART（如果已配置）。要启用自动 DART，请将 DARTCount 设置为任意非零值。设置为 0 时，功能禁用。启用自动 DART 可防止因时间推移而导致数据丢失。在以下位置收集自动汇集的 DARTS：

- Windows — %LocalAppData%/Cisco/Cisco AnyConnect Secure Mobility Client
- macOS — ~/.cisco/iseposture/log

支持以下操作系统：

- Windows 的 ISE 安全评估代理
- macOS
- Linux

步骤 1 启动 DART：

- 对于 Windows 设备，请启动Cisco AnyConnect Secure Mobility Client。
- 对于 Linux 设备，请选择**应用程序 (Applications)** > **继承 (Internet)** > **思科 DART (Cisco DART)**

  或 /opt/cisco/anyconnect/dart/dartui。
- 对于 macOS 设备，请选择 **应用程序 (Applications)** > **思科 (Cisco)** > **思科 DART (Cisco DART)**。

步骤 2 单击**统计数据 (Statistics)** 选项卡，然后单击**诊断 (Diagnostics)**。

步骤 3 选择**默认 (Default)** 或**自定义 (Custom)** 捆绑创建。

- Default - 包括典型日志文件和诊断信息，例如 AnyConnect 日志文件、有关计算机的常规信息以及 DART 执行和不执行的功能的摘要。捆绑包的默认名称为 `DARTBundle.zip`，它会保存到本地桌面。
- Custom - 可指定要在捆绑中包含什么文件（或默认文件）和存储捆绑的位置。

  Linux 和 macOS 的成功路由和过滤更改不会记录在日志中，以便您可以更好地关注重要事件。否则，在系统日志事件速率限制下，重要事件可能减少和被忽视。此外，捕获过滤设置使您可以查看 macOS 的系统 pf 配置文件以及 AnyConnect 过滤配置文件。对于 Linux，即使对大多数这些配置的访问受限，iptables 和 ip6tables 输出也会显示在 DART 中，除非 DART 工具通过 sudo 运行。

注释　对于 macOS，只有**默认值 (Default)** 选项。您无法自定义捆绑包需要包括的文件。

注释　如果您选择**自定义 (Custom)**，则可以配置要在捆绑中包含哪些文件，并且为文件指定不同的存储位置。

步骤 4 如果DART似乎要花很长时间来收集默认文件列表，请单击**取消 (Cancel)**，重新运行DART，并选择**自定义 (Custom)**以选择较少的文件。

步骤 5 如果您选择**默认 (Default)**，DART 将开始创建捆绑包。如果您选择**自定义 (Custom)**，请继续按照向导提示指定日志、首选项文件、诊断信息和任何其他定制项。

在 DART 中显示 UDID

在 DART CLI 中，您可以显示客户端的唯一设备标识符 (UDID)。例如，对于 Windows，转到包含 dartcli.exe (C:\Program Files\Cisco\Cisco AnyConnect Secure Mobility Client) 的文件夹，然后输入 **dartcli.exe -u** 或 **dartclie.exe -udid**。

收集日志以收集关于安装或卸载问题的数据（适用于 Windows）

如果您遇到 AnyConnect 安装或卸载故障，需要收集日志，因为 DART 收集对此没有诊断能力。

在您解压 AnyConnect 文件的同一文件夹中运行 msiexec 命令：

- 对于安装故障，请输入

  ```
  C:/temp>msiexec /i anyconnect-win-version-pre-deploy-k9.msi /lvx c:/Temp/ac-install.log?
  ```

  其中 *c:/temp/ac-install.log?* 可以是您选择的文件名。

- 对于卸载故障，请输入

  ```
  c:/temp/msiexec /x anyconnect-win-version-pre-deploy-k9.msi /lvx c:/Temp/ac-install.log?
  ```

  其中 *c:/temp/ac-uninstall.log?* 可以是您选择的文件名。

注释　对于卸载故障，应该使用特定于当前已安装版本的 MSI。

您可以改变上述相同命令，以采集关于无法在 Windows 上正确安装或卸载的任何模块的信息。

获取计算机系统信息

对于 Windows，键入 **msinfo32 /nfo c:\msinfo.nfo**。

获取 Systeminfo 文件转储

对于 Windows，在 sysinfo 命令提示符中键入 **c:\sysinfo.txt**。

检查注册表文件

SetupAPI 日志文件中如下所示的条目表示找不到文件：

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

确保 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 注册表项存在。若没有此注册表项，将禁止所有 inf 安装包。

AnyConnect 日志文件的位置

日志保留在以下文件中：

- Windows- `\Windows\Inf\setupapi.app.log or \Windows\Inf\setupapi.dev.log`

  注释 在 Windows 中，您必须使隐藏的文件可见。

  如果是初次网络部署安装，则日志文件位于每位用户的临时目录下：

  `%TEMP%\anyconnect-win-4.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log`。

  如果升级来自于最佳网关推送，则日志文件位于以下位置：

  `%WINDIR%\TEMP\anyconnect-win-3.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log`。

  获取适用于您要安装的客户端版本的最新文件。*xxx* 因版本而异，*yyyyyyyyyyyyy* 指定安装的日期和时间。

- MacOS （10.12 及更高版本）- 日志记录数据库；使用控制台应用或 log 命令查询 VPN、DART 或 Umbrella 的日志
- MacOS （基于旧版文件的日志）- `/var/log/system.log`（用于所有其他模块）
- Linux Ubuntu-`/var/log/syslog`
- Linux Red Hat-`/var/log/messages`

运行 DART 以清除故障排除数据

在 Windows 中，您可以使用 DART 向导清除生成的日志。

步骤 1 使用管理员权限启动 DART。

步骤 2 单击**清除所有日志 (Clear All Logs)** 以开始清除日志。

AnyConnect 连接或断开连接问题

AnyConnect 无法建立初始连接或未断开连接

问题：AnyConnect 不会建立初始连接，或者当您单击“Cisco AnyConnect 安全移动客户端”(Cisco AnyConnect Secure Mobility Client) 窗口上的“断开连接”(Disconnect) 时出现意外结果。

解决方案：进行以下检查

- 如果使用 Citrix 高级网关客户端版本 2.2.1，请删除 Citrix 高级网关客户端，直到 Citrix 解决 CtxLsp.dll 问题。
- 如果您使用具有 AT&T Sierra 无线 875 网卡的 AT&T 通信管理器 6.2 版或 6.7 版，请执行以下步骤解决此问题：
  1. 禁用 Aircard 加速。
  2. 启动 **AT&T Communication Manager > 工具 (Tools) > 设置 (Settings) > 加速 (Acceleration) > 启动 (Startup)**。
  3. 键入 **manual**。
  4. 单击**停止 (Stop)**。
- 从 ASA 获取配置文件，查找连接失败的标志：
  - 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。
  - 从 ASA 的控制台，键入 **show running-config**。剪切并粘贴配置文件到文本编辑器并保存。
- 查看 ASA 事件日志：
  1. 在 ASA 控制台上，添加以下命令行以查看 ssl、webvpn、anyconnect 和 auth 事件：

     ```
     config terminal
     logging enable
     logging timestamp
     logging class auth console debugging
     logging class webvpn console debugging
     logging class ssl console debugging
     logging class anyconnect console debugging
     ```

  2. 尝试连接 AnyConnect 客户端，发生连接错误时，则将日志信息从控制台上剪切并粘贴至文本编辑器并保存。
  3. 键入 **`no logging enable`** 禁用日志记录。
- 使用 Windows 事件查看器从客户端计算机获取思科 AnyConnect VPN 客户端日志。
  1. 选择**开始 (Start) > 运行 (Run)** 并键入 **`eventvwr.msc /s`**。
  2. 在（Windows 7 的）应用和服务日志中找到`思科 AnyConnect VPN 客户端`，并选择**将日志文件另存为...**。。

3. 指定文件名，例如 `AnyConnectClientLog.evt`。您必须使用 `.evt` 文件格式。

- 修改 Windows 诊断调试实用程序。

1. 如 WinDbg 文档所示，附加 vpnagent.exe 进程。
2. 确定 IPv6/IPv4 IP 地址分配是否存在冲突。在事件日志中查找是否有已识别的冲突。
3. 如果发现冲突，则向要使用的客户端计算机注册表添加额外的路由调试。这些冲突在 AnyConnect 事件日志中可能会如下所示：

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

4. 通过添加特定的注册表项 (Windows) 或文件（Linux 和 macOS）为连接启用一次性的路由调试。

   - 在 32 位 Windows 中，DWORD 注册表值必须是 `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled`
   - 在 64 位 Windows 中，DWORD 注册表值必须是 `HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled`
   - 在 Linux 或 macOS 中，使用 sudo touch 命令在以下路径中创建文件：`/opt/cisco/anyconnect/debugroutes`

注释 密钥或文件将在启动隧道连接时删除。文件的密钥或内容的值不是重要的密钥时或文件足以启用调试。

启动 VPN 连接。找到此密钥或文件时，系统临时目录（在 Windows 中通常是 C:\Windows\Temp，在 macOS 或 Linux 中通常是 /opt/cisco/anyconnect）中将创建两个路由调试文本文件。如果已经存在这两个文件（debug_routechangesv4.txt4 和 debug_routechangesv6.txt），它们将会被覆盖。

AnyConnect 无法传输流量

问题：AnyConnect 客户端在连接后无法将数据发送到专用网络。

解决方案：进行以下检查

- 如果您使用具有 AT&T Sierra 无线 875 网卡的 AT&T 通信管理器 6.2 版或 6.7 版，请执行以下步骤解决此问题：
  1. 禁用 Aircard 加速。
  2. 启动 AT&T Communication Manager > 工具 (Tools) > 设置 (Settings) > 加速 (Acceleration) > 启动 (Startup)。
  3. 键入 **manual**。
  4. 单击**停止 (Stop)**。
- 获取 show vpn-sessiondb detail anyconnect filter name <username> 命令的输出。如果输出指定 Filter Name: XXXXX，则还要获取 show access-list XXXXX 命令的输出。验证 ACL 未阻止需要的流量。
- 从 AnyConnect VPN Client > Statistics > Details > Export 获取 DART 文件或输出 (AnyConnect-ExportedStats.txt)。观察统计、界面和路由表。
- 检查 ASA 配置文件中的 NAT 语句。如果已启用 NAT，则您必须排除从网络地址转换返回到客户端的数据。例如，要使 NAT 从 AnyConnect 池中排除 IP 地址，需要使用以下代码：

```
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
```

- 验证是否为设置启用了隧道化默认网关。传统默认网关是最不适合非解密流量的网关。

```
route outside 0.0.209.165.200.225
route inside 0 0 10.0.4.2 tunneled
```

  如果 VPN 客户端需要访问 VPN 网关路由表中未列出的资源，数据包将由标准默认网关传送。VPN 网关不需要完整的内部路由表。如果您使用隧道化关键字，则路由将处理来自 IPsec/SSL VPN 连接的解密流量。标准流量通常不会路由到 209.165.200.225，而来自 VPN 的流量将路由到 10.0.4.2 且已进行解密。
- 在使用 AnyConnect 建立隧道前后，收集 ipconfig /all 的文本转储和路由打印输出。
- 在客户端上执行网络数据包捕获，或在 ASA 上启用捕获。

注释 如果某些应用（例如 Microsoft Outlook）无法使用隧道，则在具有 ping 扩展集的网络中 ping 已知设备，可查看接受的大小（例如，ping -| 500，ping -| 1000，ping -| 1500，以及 ping -| 2000）。从 ping 结果中可对网络中的分段问题略知一二。然后，您可以为存在分段问题的用户配置一个特殊组，并将该组的 anyconnect mtu 设置为 1200。您也可从旧 IPsec 客户端复制 Set MTU.exe 实用程序，并强制将物理适配器 MTU 设置为 1300。重启后，查看是否有区别。

基于 VM 的子系统的连接问题

如果主机（Windows 10 或 macOS Big Sur）上的 AnyConnect VPN 处于活动状态，而适用于 Linux (WSL2) 或VMware Fusion VM 的 Windows 子系统遇到了连接问题，请按照以下步骤配置仅限于虚拟适配器的本地 LAN 拆分排除隧道子网。

步骤 1 在 ASDM 中，导航到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络[客户端]访问 (Network [Client] Access) > 高级 (Advanced) > AnyConnect 定制属性 (AnyConnect Custom Attributes)** 以配置新的自定义属性类型。

步骤 2 选择 **Add**（添加）并在“创建自定义属性”(Create Custom Attribute) 窗格中设置以下项：

a) 输入 **BypassVirtualSubnetsOnlyV4** (IPv4) 或 **BypassVirtualSubnetsOnlyV6** (IPv6) 作为新的类型。

b) 或者，输入说明。

c) 在 **AnyConnect 自定义属性名称 (AnyConnect Custom Attributes Names)** 中将名称和值设置为 *true*。

如果已在组策略中为特定 IP 协议配置了本地 LAN 通配符拆分排除，则客户端会将其限制为仅虚拟子网，但前提是同一 IP 协议启用了自定义属性。如果本地 LAN 通配符拆分排除未在组策略中配置，则由客户端为启用了自定义属性的IP协议添加，从而会导致相应地实施受限的本地LAN拆分排除。在未配置其他拆分-排除网络的情况下，所有物理适配器流量都将通过隧道传输，即类似于全隧道配置。

步骤 3 通过以下方式将先前创建的自定义属性类型和名称附加到组策略中：**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（[客户端）访问 Network [Client] Access > 组策略 (Group Policies) > 编辑 (Edit) > 高级 (Advanced) > AnyConnect 客户端 (AnyConnect Client) > 自定义属性 (Custom Attributes)**。

下一步做什么

要验证属性值是否设置正确，请检查 AnyConnect VPN 日志中是否存在以“已收到 VPN 会话配置”(Received VPN Session Configuration) 开头的消息。它应指明本地 LAN 通配符仅限于虚拟子网。

VPN 服务故障

VPN 服务连接失败

问题：您收到“Unable to Proceed, Cannot Connect to the VPN Service”消息。AnyConnect 的 VPN 服务未运行。

解决方案：确定是否有另一个应用与该服务冲突。请参阅确定服务的冲突项。

确定服务的冲突项

以下过程确定冲突是在启动时针对服务器的初始化还是针对其他运行的服务，例如，因为服务启动失败。

步骤 1 查看 Windows 管理工具下的服务，以确保思科 AnyConnect VPN 代理未运行。如果它正在运行并且仍然显示错误消息，则可能需要禁用甚至卸载工作站上的另一个 VPN 应用。在执行该操作后，重新启动，然后重复此步骤。

步骤 2 尝试启动思科 AnyConnect VPN 代理。

步骤 3 在事件查看器中检查 AnyConnect 日志以查找是否存在指出服务无法启动的消息。请注意步骤 2 的手动重新启动的时间戳以及工作站启动时的时间戳。

步骤 4 在事件查看器中检查系统和应用日志以查找任何冲突消息的相同通用时间戳。

步骤 5 如果日志指示启动服务失败，请查找在大致相同时间戳的其他信息性消息，这些消息指示以下情况之一：

- 文件缺失 - 从独立 MSI 安装重新安装 AnyConnect 客户端以排除缺失的文件。
- 另一相关服务中的延迟 - 禁止启动活动以缩短工作站的启动时间。
- 与另一应用或服务的冲突 - 确定是否另一项服务在侦听 vpnagent 使用的同一端口，或者是否某些 HIDS 软件阻止我们的软件侦听某个端口。

步骤 6 如果日志没有直接指向某个原因，请使用试错法来识别冲突。识别了最可能的候选项后，请从服务面板禁用这些服务（例如 VPN 产品、HIDS 软件、Spybot 清除程序、嗅探器、防病毒软件等）。

步骤 7 重新启动。如果 VPN 代理服务仍无法启动，请开始关闭操作系统的默认安装未安装的服务。

VPN 客户端驱动程序遇到错误（Microsoft Windows 更新后）

问题：如果您最近更新了 Microsoft certclass.inf 文件，在尝试建立 VPN 连接时会出现以下消息：

```
The VPN client driver has encountered an error.
```

如果检查 C:\WINDOWS\setupapi.log，会看到以下错误：

```
#W239 The driver signing class list “C:\WINDOWS\INF\certclass.inf” was missing or invalid.
 Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject to driver signing
 policy.
```

解决方案：在命令提示符下输入 **C:\>systeminfo** 或查看 C:\WINDOWS\WindowsUpdate.log，可查看最近安装了哪些更新。按照说明修复 VPN 驱动程序。

修复 VPN 客户端驱动程序错误

尽管执行的上述步骤可能表明目录未损坏，但密钥文件仍可能已被未签名的文件覆盖。如果此故障仍然存在，请通过向 Microsoft 提交案例来确定驱动程序签名数据库为什么损坏。

步骤 1 以管理员身份打开命令提示符。

步骤 2 输入 **net stop CryptSvc**。

步骤 3 分析数据库，通过输入 **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** 验证其有效性或将目录 %/WINDIR%\system32\catroot2 重命名为 catroot2_old。

步骤 4 出现提示时，选择**确定 (OK)** 尝试修复。退出命令提示符并重新启动。

驱动程序故障

修复 VPNVA.sys 中的驱动程序故障

问题：VPNVA.sys 驱动程序故障。

解决方案：找到被绑定到 Cisco AnyConnect 虚拟适配器的中间驱动程序，并取消选择它们。

修复 vpnagent.exe 中的驱动程序故障

步骤 1 创建名为 c:\vpnagent 的目录。

步骤 2 查看任务管理器中的“流程”(Process) 选项卡，确定 vpnagent.exe 中的进程 PID。

步骤 3 打开命令提示符并更改安装了调试工具的目录。默认情况下，Windows 的调试工具位于 `C:\Program Files\Debugging Tools`。

步骤 4 键入 **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst**，其中 *PID* 是 **vpnagent.exe** 的 PID。

步骤 5 使打开的窗口以最小化状态运行。监控时不可注销系统。

步骤 6 当发生故障时，将 c:\vpnagent 的内容压缩为 zip 文件。

步骤 7 使用 **!analyze -v** 进一步诊断 crashdmp 文件。

网络访问管理器的链路/驱动程序问题

如果网络访问管理器无法识别有线适配器，请尝试将网线拔出并重新插入。如果这无法解决问题，则链路可能有问题。网络访问管理器可能无法确定适配器的正确链路状态。请检查 NIC 驱动程序的连接属性。您可能在高级面板中看到“等待链路”(Wait for Link) 选项。设置为“开”(On) 时，有线 NIC 驱动程序初始化代码等待自动协商完成，再确定连接是否有效。

其他故障

AnyConnect 故障

问题：在系统重启后，您收到 the system has recovered from a serious error 消息。

解决方案：从 %temp% 目录（例如 C:\DOCUME~1\jsmith\LOCALS~1\Temp）中收集生成的 .log 和 .dmp 文件。复制文件或备份文件。请参阅如何备份 .log 或 .dmp 文件。

如何备份 .log 或 .dmp 文件

步骤 1 从“开始 > 运行”菜单运行名为 Dr. Watson (Drwtsn32.exe) 的 Microsoft 实用程序。

步骤 2 进行以下配置并单击**确定 (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
```

步骤 3 在客户端计算机上的“开始 > 运行”菜单中输入 **eventvwr.msc /s**，以从 Windows 事件查看器中获取思科 AnyConnect VPN 客户端日志。

步骤 4 在（Windows 7 的）应用和服务日志中找到**思科 AnyConnect VPN 客户端**，并选择**将日志文件另存为...**。。以 .evt 文件格式分配文件名，例如 AnyConnectClientLog.evt。

vpndownloader 中的 AnyConnect 故障（分层服务提供商 (LSP) 模块和 NOD32 AV）

问题：AnyConnect 在尝试建立连接时成功进行身份验证并建立了 SSL 会话，但随后在使用 LSP 或 NOD32 AV 时，AnyConnect 客户端在 vpndownloader 中发生故障。

解决方案：删除 2.7 版中的 Internet Monitor 组件，并升级到 ESET NOD32 AV 3.0 版。

蓝屏（AT&T 拨号器）

问题：如果您使用 AT&T 拨号器，则客户端操作系统有时会出现蓝屏，导致创建微型转储文件。

解决方案：升级到最新的 7.6.2 AT&T 全球网络客户端。

安全告警

Microsoft Internet Explorer 安全告警

问题：Microsoft Internet Explorer 中出现安全告警窗口，其中包含以下文字：

```
Information you exchange with this site cannot be viewed or changed by others. However,
there is a problem with the site's security certificate. The security certificate was issued
 by a company you have not chosen to trust. View the certificate to determine whether you
want to trust the certifying authority.
```

解决方案：连接到未识别为受信任网站的ASA时可能出现此告警。为防止出现此告警，请在客户端上安装一个受信任根证书。请参阅在客户端上安装受信任根证书。

“未知授权认证”(Certified by an Unknown Authority) 告警

问题：在浏览器中可能出现 Web Site Certified by an Unknown Authority 告警窗口。Security Alert 窗口的上半部分显示以下文本：

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

解决方案：在连接到不被识别为受信任站点的ASA时可能出现此安全告警。为防止出现此告警，请在客户端上安装一个受信任根证书。请参阅在客户端上安装受信任根证书。

在客户端上安装受信任根证书

开始之前

生成或获取将用作受信任根证书的证书。

注释 您可以通过将自签名证书安装为客户端上的受信任根证书，在短期内避免出现安全证书警告。但是我们不建议这样做，因为用户可能会无意中将浏览器配置为信任欺诈服务器上的证书，并且在连接到安全网关时可能不得不响应安全警告而给用户带来不便。

步骤 1 单击“安安全警报”(Security Alert) 窗口中的**查看证书 (View Certificate)**。

步骤 2 单击**安装证书 (Install Certificate)**。

步骤 3 单击**下一步 (Next)**。

步骤 4 选择**将所有证书放入下列存储 (Place all certificates in the following store)**。

步骤 5 单击**浏览 (Browse)**。

步骤 6 在下拉列表中，选择**受信任的根证书颁发机构 (Trusted Root Certification Authorities)**。

步骤 7 遵循证书导入向导提示继续操作。

掉线的连接

无线连接在引入有线连接时掉线（Juniper Odyssey 客户端）

问题：在 Odyssey 客户端上启用无线抑制后，如果引入有线连接，那么无线连接就会掉线。禁用无线抑制后，无线连接如预期的那样运行正常。

解决方案：配置 Odyssey 客户端。

配置 Odyssey 客户端

步骤 1 在 Network Connections 中，复制适配器的名称（与在其连接属性中显示的一样）。如果您编辑注册表，请先进行备份，然后再进行任何更改。一定要谨慎，因为如果修改错误，可能导致严重问题。

步骤 2 打开注册表并转到 HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual。

步骤 3 在 virtual 下创建新的字符串值。将适配器的名称从 Network 属性复制到注册表部分。额外的注册表设置一旦保存，就会在创建客户端 MSI 并下推到其他客户端时通过端口传递。

连接 ASA 失败 (Kaspersky AV Workstation 6.x)

问题：安装 Kaspersky 6.0.3 后（即使已禁用），到 ASA 的 AnyConnect 连接会在 CSTP state = CONNECTED 之后立即失败。系统会显示以下消息：

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway (proxy
 authentication, handshake, bad cert, etc.).
```

解决方案：卸载 Kaspersky 并访问其论坛获得其他更新。

没有 UDP DTLS 连接 (McAfee Firewall 5)

问题：使用 McAfee Firewall 5 时，UDP DTLS 连接无法建立。

解决方案：在 McAfee Firewall 中央控制台中，选择**高级任务 (Advanced Tasks)** > **高级选项和日志记录 (Advanced options and Logging)**，然后取消选中 McAfee Firewall 中的**自动阻止传入的片段 (Block incoming fragments automatically)** 复选框。

连接主机设备失败（Microsoft 路由和远程访问服务器）

问题：如果使用 RRAS，则当 AnyConnect 尝试建立到主机设备的连接时，事件日志中会记录以下终止错误：

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service “Routing and Remote Access” is incompatible with the Cisco AnyConnect
 VPN Client.
```

解决方案：禁用 RRAS 服务。

连接失败/缺少凭证（负载均衡器）

问题：由于缺少凭证而连接失败。

解决方案：第三方负载均衡器无法洞悉 ASA 设备上的负载。因为 ASA 中的负载均衡功能足够智能，能够在设备之间均衡地分配 VPN 负载，所以我们建议使用内部 ASA 负载均衡。

安装故障

若未找到根本原因，则不要编辑 Windows 注册表

如果您在安装、卸载或升级 AnyConnect 时收到故障消息，我们不建议直接修改 Windows 安装程序注册表项，否则可能会导致意外后果。确定正确的根本原因后，Microsoft 提供的工具可以对安装程序问题进行故障排除。

AnyConnect 无法下载 (Wave EMBASSY Trust Suite)

问题：AnyConnect 客户端无法下载，并出现以下错误消息：

```
“Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close.”
```

解决方案：将补丁更新上传到 1.2.1.38 版以解决所有 dll 问题。

不兼容问题

更新路由表失败（Bonjour 打印服务）

问题：如果您使用的是 Bonjour 打印服务，AnyConnect 事件日志会指出识别 IP 转发表失败。

解决方案：通过在命令提示符下键入 **net stop “bonjour service”** 禁用 BonJour 打印服务。Apple 公司已经推出了新版 mDNSResponder (1.0.5.11)。要解决此问题，请将新版 Bonjour 捆绑至 iTunes，且作为单独程序从 Apple 网站下载。

TUN 的版本不兼容（OpenVPN 客户端）

问题：错误表示此系统上已安装 TUN 版本，但该版本与 AnyConnect 客户端不兼容。

解决方案：卸载 Viscosity OpenVPN 客户端。

Winsock 目录冲突（LSP 症状 2 冲突）

问题：如果客户端上有 LSP 模块，可能会发生 Winsock 目录冲突。

解决方案：卸载 LSP 模块。

数据吞吐慢（LSP 症状 3 冲突）

问题：在 Windows 7 系统中使用 NOD32 Antivirus V4.0.468 x64 时可能出现数据吞吐慢。

解决方案：禁用 SSL 协议扫描。请参阅禁用 SSL 协议扫描。

禁用 SSL 协议扫描

步骤 1 转至“高级设置”(Advanced Setup) 中的 **协议过滤 (Protocol Filtering)** > **SSL** 并启用 SSL 协议扫描。

步骤 2 转到 **Web 访问保护 (Web access protection)** > **HTTP**、**HTTPS**，并选中 **不使用 HTTPS 协议检查 (Do not use HTTPS protocol checking)**。

步骤 3 返回到**协议过滤 (Protocol Filtering)** > **SSL** 并禁用 **SSL 协议扫描 (SSL protocol scanning)**。

DPD 失败（EVDO 无线网卡和 Venturi 驱动程序）

问题：如果客户端断开连接时您使用的是 EVDO 无线网卡和 Venturi 驱动程序，则事件日志会报告如下内容：

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
 DPD failure.
```

解决方案

- 检查应用、系统和 AnyConnect 事件日志中的相关断开连接事件，同时确定是否应用了 NIC 卡重置。
- 确保 Venturi 驱动程序为最新版本。在 6.7 版本的 AT&T 通信管理器中禁用 **Use Rules Engine**。

DTLS 流量失败（DSL 路由器）

问题：如果您与 DSL 路由器连接，则即使成功协商，DTLS 流量也可能会失败。

解决方案：连接到采用出厂设置的 Linksys 路由器。此设置支持稳定的 DTLS 会话且 ping 过程中无中断。添加规则以允许 DTLS 返回流量。

NETINTERFACE_ERROR（CheckPoint 和其他第三方软件，如 Kaspersky）

问题：尝试在用于建立 SSL 连接的计算机网络上检索操作系统信息时，AnyConnect 日志可能指示未能完全建立到安全网关的连接。

解决方案

- 如果是卸载完整性代理，然后安装 AnyConnect，请启用 TCP/IP。
- 确保如果在完整性代理安装上禁用 SmartDefense，则选中 TCP/IP。
- 如果在检索网络接口信息时第三方软件拦截或以其他方式阻止操作系统 API 调用，请检查是否有可疑的 AV、FW、AS 等。
- 确认设备管理器中只出现一个 AnyConnect 适配器实例。如果只有一个实例，则使用 AnyConnect 进行身份验证，并在 5 秒后手动从设备管理器启用适配器。
- 如果在 AnyConnect 适配器中启用了任何可疑的驱动程序，在“Cisco AnyConnect VPN 客户端连接”(Cisco AnyConnect VPN Client Connection) 窗口中取消选中它们予以禁用。

性能问题（虚拟机网络服务驱动程序）

问题：在某些虚拟机网络服务设备上使用 AnyConnect 时，会导致性能问题。

解决方案：取消选中 AnyConnect 虚拟适配器中所有即时消息设备的绑定。应用 dsagent.exe 驻留在 C:\Windows\System\dgagent 中。虽然其未出现在进程列表中，您可以用 TCPview (sysinternals) 打开套接字进行查看。当您终止此进程时，AnyConnect 将恢复正常运行。

已知的第三方应用冲突

我们已经知道，以下第三方应用获取Cisco AnyConnect Secure Mobility Client存在困难：

- Adobe 和苹果公司 - Bonjour 打印服务
  - Adobe Creative Suite 3
  - BonJour 打印服务
  - iTunes
- AT&T 通信管理器版本 6.2 和 6.7
  - AT&T Sierra 无线 875 卡
- AT&T 全球拨号器

- Citrix 高级网关客户端版本 2.2.1
- 防火墙冲突
  - 第三方防火墙可能会干扰 ASA 组策略中配置的防火墙功能。
- Juniper Odyssey 客户端
- Kaspersky AV 工作站 6.x
- McAfee 防火墙 5
- Microsoft Internet Explorer 8
- Microsoft 路由和远程接入服务器
- OpenVPN 客户端
- 负载均衡
- Wave EMBASSY Trust Suite
- 分层服务提供商 (LSP) 模块和 NOD32 AV
- EVDO 无线网卡和 Venturi 驱动程序
- DSL 路由器
- CheckPoint 和其他第三方软件（如卡巴斯基）
- 虚拟机网络服务驱动程序