排除Cisco安全客户端VPN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

收集故障排除信息

- 客户端 — 统计和DART
- 前端 — ASA
- 头端 — FTD
- 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

思科安全客户端：损坏的驱动程序数据库问题

- 修复
- 修复失败
- 分析数据库

错误消息

- Error:Unable to Update the Session Management Database
- 解决方案 1
- 解决方案 2
- Error:Cisco Secure Client安装期间的“Module failed to register”
- 解决方案
- Error:"An error was received from the secure gateway in response to the VPN negotiation request.Please contact your network administrator"
- 解决方案
- Error:Anyconnect not enabled on VPN server while trying to connect anyconnect to ASA
- 解决方案
- 错误：-%ASA-6-722036：Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)
- 解决方案
- Error:The secure gateway has rejected the agent's vpn connect or reconnect request.
- 解决方案
- Error:"The VPN client driver has encountered an error"
- 解决方案

Error:"Unable to process response from xxx.xxx.xxx.xxx"

解决方案

Error:"Login Denied , unauthorized connection mechanism , contact your administrator"

解决方案

Error:"Anyconnect package unavailable or corrupted.Contact your system administrator"

解决方案

Error:"The AnyConnect package on the secure gateway could not be located"

解决方案

Error:"Secure VPN via remote desktop is not supported"

解决方案

Error:"The server certificate received or its chain does not comply with FIPS.A VPN connection will not be established"

解决方案

Error:"Certificate Validation Failure"

解决方案

Error:"VPN Agent Service has encountered a problem and needs to close.We are sorry for the inconvenience"

解决方案

Error:"This installation package could not be opened.Verify that the package exists"

解决方案

Error:"Error applying transforms.Verify that the specified transform paths are valid."

解决方案

Error:"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 restored."

解决方案

登录时出现Cisco安全客户端错误

解决方案

Error:AnyConnect Essentials can not be enabled until all these sessions are closed.

解决方案

Error:Few users getting Login Failed Error message when others are able to connect successfully through AnyConnect VPN

解决方案

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

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

错误消息：TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

解决方案

错误消息："Connection attempt has failed due to invalid host entry"

解决方案

Error:"Ensure your server certificates can pass strict mode if you configure always-on VPN"

解决方案

Error:"An internal error occurred in the Microsoft Windows HTTP Services"

解决方案

Error:"The SSL transport received a Secure Channel Failure.May be a result of a unsupported crypto configuration on the Secure Gateway."

解决方案

相关信息

简介

本文档介绍Cisco Secure Client在Windows、macOS和Linux上的应用故障和断开问题。

先决条件

要求

在您使用此文档之前，请确保您拥有：

- 终端上的Cisco Secure Client 5.x（或头端支持的版本）。
- 能够收集DART捆绑包或客户端日志。
- 对VPN前端（ASA或FTD）的管理访问。

使用的组件

本文档中的信息基于：

- 客户端：思科安全客户端5.x（AnyConnect VPN模块）。
- 前端：带远程访问VPN的Cisco ASA 9.x或Cisco安全防火墙威胁防御(FTD)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

查看《产品管理员指南》中的Troubleshoot Cisco Secure Client。

故障排除过程

本文档详细介绍Cisco安全客户端VPN问题（包括AnyConnect），包括Windows、macOS、Linux和Cisco ASA/FTD头端配置上的应用故障、意外断开和常见错误。

- 不通过VPN隧道运行的应用。
- 客户端意外连接/断开连接。

- 客户端或头端上出现的常见错误消息。

这包括Windows、macOS和Linux上的VPN客户端，包括思科ASA和思科安全防火墙威胁防御(FTD)远程访问上的前端配置。 VPN.

提示：在故障排除之前，收集Cisco安全客户端DART捆绑包。您可以使用DART Analyzer BDB任务分析DART输出。

查看以下部分以解决常见问题和解决方案：

- 收集故障排除信息
- 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

收集故障排除信息

在更改配置之前收集客户端和头端数据。TAC通常请求DART捆绑包。

客户端 — 统计和DART

1. 导出连接统计信息
   - Windows 窗口版本:齿轮图标>高级窗口>统计信息> AnyConnect VPN >导出统计信息
   - macOS：“统计信息”图标>“导出统计信息”
   - Linux:客户端GUI的详细信息
2. 运行DART
   - Windows/Linux:齿轮图标>“高级窗口”>“诊断”
   - macOS：“应用程序”菜单>生成诊断报告

   将捆绑包附加到您的TAC案例，或使用Upload to TAC和SR编号和令牌。
3. 嵌入式浏览器问题：Advanced Window > General > Web Browser > Clear Data。

前端 — ASA

- show running-config
- show vpn-sessiondb detail anyconnect filter name <username>
- 调试示例：

```
configure 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
```

重现故障，捕获输出，然后启用no logging。

头端 — FTD

从FMC/CDO导出远程访问VPN策略和连接配置文件设置。收集故障窗口的FTD SSL VPN/连接日志。

安装和虚拟适配器问题

如果安装或虚拟适配器设置失败，请收集：

1. Windows安装日志：

```
%SystemRoot%\Inf\setupapi.dev.log
%SystemRoot%\Inf\setupapi.setup.log
```

2. MSI安装程序日志：%LOCALAPPDATA%\Temp\ 或%SystemRoot%\Temp\ — 文件名cisco-secure-client-win-*-install-*.log（最新版本为您的版本）。
3. 详细MSI（如果需要）：

```
msiexec /i cisco-secure-client-win-<version>-predeploy-k9.msi /lvx %TEMP%\ac-install.log
```

4. 系统信息:msinfo32 /nfo %TEMP%\msinfo.nfo和systeminfo > %TEMP%\sysinfo.txt

有关驱动程序数据库错误，请参阅Cisco安全客户端：驱动程序数据库问题损坏和管理员指南部分VPN客户端驱动程序遇到错误（在Microsoft Windows Update之后）。

连接断开或无法建立初始连接

如果您遇到Cisco Secure Client的连接问题，请在更改配置之前根据收集故障排除信息收集数据。

- 头端配置：show running-config或FTD的FMC/CDO导出策略。
- 客户端日志:收集DART捆绑包（请参阅收集信息）。 不要依赖旧版事件查看器.evt导出。
- ASA调试（如果需要）：在调试时启用logging class auth、webvpn、ssl和anyconnect;再现故障；捕获控制台输出；然后no logging enable。

如果用户无法连接，则问题可能与远程桌面协议(RDP)或快速用户交换有关。用户可看到：AnyConnect配置文件设置要求一个本地用户，但多个本地用户当前已登录到您的计算机。无法建立VPN连接。

断开RDP会话并禁用快速用户交换。在同一台计算机上不支持多个同时本地用户建立VPN。

注意：确保端口443（和UDP 443 for DTLS）未被阻止，以便客户端可以到达头端。

当用户无法连接时，问题可能是由于Cisco Secure Client版本和头端软件之间不兼容。用户可以接收：安装程序无法启动Cisco VPN客户端，无客户端访问不可用。请将该客户端升级到ASA或FTD远程访问VPN部署支持的版本。

首次登录Cisco Secure Client时，登录脚本可能会出现问题。如果断开连接并再次登录，登录脚本通常按预期运行。这可以是预期行为，具体取决于配置文件和脚本计时。

连接后，您会收到：User not authorized for AnyConnect Client access, contact your administrator。当头端缺少安全客户端映像时，通常会出现这种情况。上传正确的客户端映像，并在RA VPN/WebVPN配置中引用该映像。

当DTLS信道因失效对等体检测(DPD)故障而中断时，DART可以显示TUNNELPROTOCOLDPDMGR_ERROR_NO_DPD_RESPONSE。在ASA上调整keepalive:

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

仅将DTLS作为临时测试禁用(ASDM:Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Connection Profiles，取消选中Enable DTLS或FMC equivalent)。 首选修复DPD计时并允许UDP 443。

关于通过流量的问题

当检测到通过ASA通过Cisco安全客户端会话将流量传递到专用网络时出现问题时，请完成以下数据收集步骤：

1. 从ASA控制台获取show vpn-sessiondb detail anyconnect filter name <username>的输出。如果输出显示 Filter Name:XXXXX，收集show access-list XXXXX。检验访问列表是否未阻止预期流量。

2. 导出连接统计信息：Cisco Secure Client > Gear > Advanced Window > Statistics > AnyConnect VPN > Export Stats。

3. 检查ASA配置nat语句。如果启用了网络地址转换(NAT)，将返回客户端的流量排除在外。NAT免除AnyConnect池的示例：

```
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. 确定是否必须启用隧道默认网关。示例：

```
route outside 0 0 10.145.50.1
route inside 0 0 10.0.4.2 tunneled
```

如果客户端必须到达不在VPN网关路由表中的资源，则tunneled关键字会通过VPN隧道路由该流量。

5. 验证检查策略是否丢弃应用流量。您可以在模块化策略框架下免除协议。skinny示例：

```
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. 在崩溃后立即收集DART。
2. 注意vpnagent.exe / acvpnui.exe的Windows错误报告条目。

3. 客户端日志:%LOCALAPPDATA%\Cisco\Cisco Secure Client\Logs(验证您的版本的路径)。

分段/通过流量问题

当隧道传送较小的流量（如小量ping）时，某些应用程序（如Microsoft Outlook）无法工作。这可能表示路径上的分段。家用路由器通常不擅长分段和重组。

尝试一组扩展的ping:ping -l 500、ping -l 1000、ping -l 1500、ping -l 2000。

为受影响的用户配置专用组策略并设置较低的MTU:

```
group-policy <name> attributes
 webvpn
  anyconnect mtu 1200
```

自动卸载

问题

连接终止后，即使ASDM/FMC中显示keep installed处于选中状态，思科安全客户端也会自行卸载。

解决方案

```
group-policy <name> attributes
 webvpn
  anyconnect keep-installer installed
```

有关填充集群 FQDN 的问题

问题：AnyConnect 客户端预先填充了主机名，而不是集群完全限定域名 (FQDN)。

当您拥有用于SSL VPN的负载均衡集群且客户端连接时，请求可以重定向到集群节点并成功登录。在以后的连接尝试中，集群FQDN不会显示在Connect to中；可以改为显示最后一个节点的主机名。

解决方案

客户端缓存上次成功的主机名。清除缓存的条目或在配置文件服务器列表中设置集群FQDN。在Cisco Secure Client 5.x上验证。有关平台特定说明，请参阅Cisco Bug ID CSCsz39019。

备份服务器列表配置

当主服务器无法访问时，会配置备份服务器列表。在客户端配置文件的Backup Server窗格中定义它。完成这些步骤：

1. 根据头端安全客户端软件包或《安全客户端5.1配置文件配置指南》(Secure Client 5.1 Profile Configuration Guide)，使用配置文件编辑器编辑配置文件。在ASDM或FMC中分配配置文件。

2. 创建或编辑XML配置文件：
    1. 转到服务器列表选项卡。
    2. 单击 Add。
    3. 输入主服务器Hostname。
    4. 在备份服务器列表下添加备份服务器，然后单击Add。
3. 将配置文件分配给ASA上的连接：
    1. 在ASDM中：Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Connection Profiles。
    2. 选择配置文件并点击编辑。
    3. 在“默认组策略”部分中点击管理。
    4. 选择组策略并点击编辑。
    5. 选择Advanced，然后选择SSL VPN Client。
    6. 单击New，命名配置文件，然后分配XML文件。
4. 连接客户端以下载配置文件。

思科安全客户端：损坏的驱动程序数据库问题

SetupAPI.log文件中的此条目表明目录系统已损坏：

W239 驱动程序签名类别列表“C:\WINDOWS\INF\certclas.inf”缺失或无效。Error 0xffffffde5:未知错误。假设所有设备类都受驱动程序签名策略的约束。您还可接收：错误(3/17)：Unable to start VA, setup shared queue, or VA gave up shared queue。

您可以在客户端上接收此日志：“VPN 客户端驱动程序发生错误”。

修复

此问题与Cisco Bug ID CSCsm54689相关。请在启动Cisco Secure Client之前禁用路由和远程访问服务(RRAS)。如果问题仍然存在：

1. 在Windows上以Administrator身份打开命令提示符。
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 OK 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：

1. 在Windows上以Administrator身份打开命令提示符。
2. 运行 net stop CryptSvc。
3. 将%WINDIR%\system32\catroot2重命名为catroot2_old。
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其是否有效。

1. 在Windows上以Administrator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

Error:Unable to Update the Session Management Database

在基于浏览器的SSL VPN或Web门户身份验证期间可能出现此错误。客户端或门户显示无法更新会话管理数据库。ASA可以记录%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

与Cisco Bug ID CSCsm51093相关。根据Bug重新加载ASA或升级到固定版本。在FTD上，验证平台内存和RA VPN会话限制。

解决方案 2

可用头端内存：

1. 如果启用威胁检测，请禁用威胁检测。
2. 禁用AnyConnect压缩：anyconnect compression none在group-policy webvpn部分下。
3. 重新加载 ASA。
4. 在具有256 MB RAM的较旧ASA平台上，如果内存耗尽仍然存在，请升级到512 MB。

Error:Cisco Secure Client安装期间的“Module failed to register”

在Windows上安装期间，安装程序报告模块(例如vpnapi.dll)无法注册和回滚。

解决方案

- 暂时删除冲突的VMware虚拟网络适配器；重新安装安全客户端；重新添加VMware。
- 如果使用Web部署，请将前端FQDN添加到受信任站点。
- 从C:\Program Files\Cisco\Cisco Secure Client\，运行提升的：regsvr32 vpnapi.dll(和

vpncommon.dll,vpncommoncrypt.dll（如果存在）)。
- 如果安装仍然失败，请收集MSI详细日志（请参见安装部分）和DART。
- 作为最后手段，请修复Windows或从全新安全客户端卸载重新部署。

Error:"An error was received from the secure gateway in response to the VPN negotiation request.Please contact your network administrator"

当客户端与Cisco Secure Client连接时，网关会返回错误，例如“Illegal address class”、“Host or network is 0”或“Other error”。

解决方案

ASA或FTD本地IP池已耗尽或配置错误。展开VPN地址池并使用适当的掩码（例如/24而不是仅/32地址池）。 请参阅Cisco Bug ID CSCsl82188。

Error:Anyconnect not enabled on VPN server while trying to connect anyconnect to ASA

客户端报告AnyConnect/安全客户端未在VPN服务器上启用。

解决方案

启用远程访问VPN并在头端部署安全客户端映像。在ASA上：Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Connection Profiles。在FTD上：在FMC中配置RA VPN和客户端映像。使用远程访问VPN指南 — 非无客户端WebVPN专用配置。

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

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

解决方案

向客户端发送了一个大数据包（MTU或不可压缩的数据）。 禁用组策略的压缩：

```
group-policy <name> attributes
 webvpn
  anyconnect compression none
```

Error:The secure gateway has rejected the agent's vpn connect or reconnect request.

示例包括网关消息中的no assigned address、Host or network is 0或No License。

解决方案

在重新加载或故障切换后，验证头端是否具有已配置的IP本地池和组策略地址分配：

```
show running-config | include pool
ip local pool SSLPOOL 192.168.30.2 192.168.30.254
 anyconnect address-pool SSLPOOL
```

对于No License，请在头端安装或启用所需的安全客户端移动许可证。

Error:"The VPN client driver has encountered an error"

通常，虚拟适配器故障、RRAS冲突或Windows Update后驱动程序问题。

解决方案

1. 启动安全客户端之前禁用路由和远程访问服务(RRAS)。
2. 完成Cisco Secure Client:如果setupapi显示目录错误，则出现损坏的驱动程序数据库问题步骤。
3. 在Windows更新后，请使用安全客户端5.1管理员指南中的修复VPN客户端驱动程序错误。
4. 收集DART并在需要时联系TAC。请参阅Cisco Bug ID CSCsm54689。

Error:"Unable to process response from xxx.xxx.xxx.xxx"

Cisco安全客户端无法连接Unable to process response from <gateway>。

解决方案

- 在受影响的接口上禁用并重新启用远程访问VPN/WebVPN。
- 暂时将SSL VPN移至另一个端口（例如444），然后恢复443。

请参阅ASA上的SSL VPN客户端配置。如果错误仍然存在，请收集DART。

Error:"Login Denied , unauthorized connection mechanism , contact your administrator"

Cisco Secure Client显示Login Denied、unauthorized connection mechanism，请联系您的管理员。

解决方案

查看头端（ASA或FTD）上的连接配置文件和身份验证。 确保客户端身份验证方法（RADIUS、SAML、证书等）与配置文件匹配。验证组策略和隧道组分配。

Error:"Anyconnect package unavailable or corrupted.Contact your system administrator"

从Macintosh客户端启动Cisco Secure Client时可能出现此错误。

解决方案

1. 将macOS安全客户端软件包上传到头端闪存。
2. 在WebVPN配置中参考该指南：

```
webvpn
 anyconnect image disk0:/cisco-secure-client-macos-<version>-predeploy-k9.pkg 2
```

Error:"The AnyConnect package on the secure gateway could not be located"

在Linux（或其他平台）上，客户端无法从头端下载软件包。

<#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

验证客户端操作系统是否受支持以及头端上是否配置了正确的映像：

```
webvpn
 anyconnect image disk0:/cisco-secure-client-win-<version>-predeploy-k9.pkg 1
 anyconnect image disk0:/cisco-secure-client-macos-<version>-predeploy-k9.pkg 2
```

有关相关步骤，请参阅AnyConnect软件包不可用或已损坏。

Error:"Secure VPN via remote desktop is not supported"

用户看到通过远程桌面的Secure VPN不受支持。

解决方案

升级到受支持的Cisco Secure Client 5.x版本。请参阅Cisco Bug ID CSCsu2208和Cisco Bug ID CSCso42825。

Error:"The server certificate received or its chain does not comply with FIPS.A VPN connection will not be established"

客户端报告服务器证书或证书链不符合FIPS。

解决方案

如果终端上需要FIPS，请在前端使用符合FIPS的证书。如果不需要，请编辑C:\ProgramData\Cisco\Cisco Secure Client\AnyConnectLocalPolicy.xml并设置<FipsMode>false</FipsMode>，然后重新启动（需要管理员权限）。

Error:"Certificate Validation Failure"

用户无法启动Cisco Secure Client并接收证书验证失败。

解决方案

对于证书身份验证，导入客户端证书，配置证书身份验证配置文件，并在ASA上启用：

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

确保服务器证书与配置文件服务器列表中的FQDN匹配。

Error:"VPN Agent Service has encountered a problem and needs to close.We are sorry for the inconvenience"

安装、升级或连接期间，vpnagent.exe服务失败。

解决方案

1. 在Windows服务中重新启动Cisco Secure Client - AnyConnect VPN Agent。
2. 从头端Web部署进行修复或重新安装。
3. 如果服务重复失败，则收集DART。有关Citrix冲突，请参阅Cisco Bug ID CSCsq49102。

Error:"This installation package could not be opened.Verify that the package exists"

Web部署失败，出现Windows Installer错误，说明无法打开包。

解决方案

1. 验证是否已完全下载MSI;从头端门户重试。
2. 暂时禁用下载文件夹中的攻击性AV;收集详细的MSI日志。
3. 确保Windows Installer服务正在运行。
4. 如果问题仍然存在，请收集DART/MSI日志并打开TAC案例。

Error:"Error applying transforms.Verify that the specified transform paths are valid."

从头端自动下载失败，有时是因为MST转换损坏。

解决方案

1. 从头端AnyConnect自定义安装定义中删除自定义MST转换。
2. 在头端重新上传正确的安全客户端映像。
3. 在ASDM中：网络（客户端）访问(Network [Client] Access)> AnyConnect自定义(AnyConnect Custom)>安装(Installs) — 删除重复条目；将活动映像保留在“客户端设置”下。

Error:"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 restored."

当头端“推送”设置更改时，重新连接后可能会出现此消息。

解决方案

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

登录时出现Cisco安全客户端错误

问题：不允许通过本地代理进行VPN连接。可以通过AnyConnect配置文件设置进行更改。

解决方案

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

Error:AnyConnect Essentials can not be enabled until all these sessions are closed.

ASDM显示启用AnyConnect Essentials时正在进行的无客户端SSL VPN会话。

解决方案

AnyConnect基础版不能与高级共享SSL VPN许可证同时运行。在启用Essentials之前结束无客户端SSL VPN会话。Essentials不包括无客户端SSL VPN。

Error:Few users getting Login Failed Error message when others are able to connect successfully through AnyConnect VPN

有些用户收到Login Failed，而其他用户可以连接。

解决方案

确保没有为受影响的用户正确设置不需要预身份验证（或等效操作）。比较组策略和连接配置文件映射。

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

在Windows上更新配置文件期间，针对连接URL的证书验证失败。

解决方案

```
<ServerList>
 <HostEntry>
    <HostName>vpn1.example.com</HostName>
 </HostEntry>
</ServerList>
```



注意：如果证书是仅FQDN，则删除使用公共IP的<HostAddress>条目。

故障切换后 AnyConnect 配置文件未复制到备用设备

在ASA故障切换后，备用设备上缺少安全客户端配置文件相关的文件。

解决方案

请参阅Cisco Bug ID CSCtn71662。解决方法：手动将配置文件复制到备用设备。验证RA VPN配置

文件的状态故障切换配置同步。

错误消息：TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

Cisco安全客户端无法连接Unable to establish a connection。事件日志显示TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER。

解决方案

这种情况发生在非常大的拆分隧道列表（大约180-200个条目）以及其他组策略属性(例如，dns-server)的情况下。

1. 减少拆分隧道列表条目。
2. 暂时禁用DTLS:

```
group-policy groupName attributes
 webvpn
  anyconnect ssl dtls none
```

请参阅Cisco Bug ID CSCtc41770。

错误消息："Connection attempt has failed due to invalid host entry"

由于证书身份验证期间的主机条目无效，连接尝试失败。

解决方案

- 在配置文件服务器列表中使用有效的HostName(FQDN)。
- 使用支持的Cisco安全客户端5.x。
- 删除已弃用的Cisco Secure Desktop(CSD)策略（如果仍存在）。

请参阅Cisco Bug ID CSCti73316。

Error:"Ensure your server certificates can pass strict mode if you configure always-on VPN"

启用Always-On时，客户端可以报告服务器证书必须通过严格模式。

解决方案

Always-On需要与连接URL匹配的有效头端证书。如果证书不受信任或不匹配，则本地策略中的严格证书模式会导致失败。

请参阅Secure Client 5.1管理员指南中的由未知颁发机构认证。

Error:"An internal error occurred in the Microsoft Windows HTTP Services"

DART可以显示HttpSendRequest失败，并且Microsoft Windows HTTP Services中发生内部错误，出现CTransportWinHttp错误。

解决方案

这可能是由损坏的Winsock状态造成的。在提升的命令提示符下：netsh winsock reset

重新启动Windows并查看Microsoft有关重置Winsock的指南。

Error:"The SSL transport received a Secure Channel Failure.May be a result of a unsupported crypto configuration on the Secure Gateway."

当客户端和头端之间的TLS或密码协商失败时，Cisco安全客户端DART可以显示CTransportWinHttp错误和CTransPORT_ERROR_SECURE_CHANNEL_FAILURE。

解决方案

1. 在头端，仅使用TLS 1.2+ 和现代密码套件。不启用DES、3DES或RC4。
2. ASA示例：

```
ssl cipher tlsv1.2 custom "AES256-GCM-SHA384:AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-R
```

3. 检查服务器证书有效性和FQDN匹配。
4. 将客户端和头端升级到支持的版本。
5. 在Windows上，保持Schannel为TLS 1.2+;不要削弱过时头端的客户端加密。

相关信息

- Cisco Secure Client故障排除（管理员指南5.1）
- AnyConnect VPN客户端故障排除指南 — 外部常见问题
- Cisco安全客户端/AnyConnect常见问题

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）。