



AnyConnect VPN 客户端常见问题

问题

- 前言
 - 安装
 - 软件升级
 - 许可授权
 - 支持的设备
 - 支持的软件
 - 日志消息
 - 数据报传输层安全(DTL)
 - 支持的功能
 - 错误消息
 - 相关信息
-

前言

本文提供回答关于与Cisco AnyConnect VPN客户(常见问题)涉及的多数常见问题。

使用安全套接字层SSL协议和数据包TLS (DTL)协议， Cisco AnyConnect VPN客户提供远程用户对Cisco ASA 5500系列可适应安全工具的安全VPN连接。AnyConnect提供远程最终用户Cisco SSL VPN客户端的好处和不可用的技术支持应用和的功能给无客户端，基于浏览器的SSL VPN连接。

注意： 本文的目标受众是了解CLI命令和功能并且有与AnyConnect VPN客户端的配置的体验的网络管理员。

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

安装

Q. 什么级别权利为AnyConnect VPN客户端要求？

A. 对于第一次安装，您需要具备管理权限。但是，在随后的升级中无需任何管理级别的权限。

Q. 在AnyConnect安装或升级后，重新启动要求？

A. 不能。不同于IPSec VPN客户端，重新启动没有在AnyConnect安装或升级以后要求。

注意： 这应用对VPN仅模块。

软件升级

Q. 是否可以通过 ASA 关闭 AnyConnect 自动升级？

A. 是。请使用这些方法之一为了通过ASA关闭自动AnyConnect升级：

- 调节在ASA的配置文件禁用更新。

```
"<AutoUpdate UserControllable="false">>false</AutoUpdate>"
```

- 请使用一个本地策略禁用AnyConnect下载者。

```
BypassDownloader  
true
```

```
The client does not check for any dynamic content present on the ASA,  
including profile updates, translations, customization, optional  
modules, and core software updates.
```

<BypassDownloader>true</BypassDownloader>

参考AnyConnect本地策略文件参数和值欲知更多信息。

许可授权

Q. 如何才能为 ASA 获取 AnyConnect Mobile 许可证?

A. 移动许可证是一个已修复许可证在准许的安全套接字层SSL用户顶部现有的号码。它可以与 Premium SSL VPN 许可证或 AnyConnect Essentials 许可证配合使用。为有SSL许可证的一个现有单元要指令AnyConnect移动许可证，部件号是L-ASA-AC-M-55XX= (XX=05, 10, 20, 40, 50, 80根据型号)。也可以增加该 Mobile 许可证作为给新购买的设备准备的一种选择 (ASA-AC-M-55XX)。为一个现有单元要指令AnyConnect移动许可证，请联系您的思科分销商。对于有精华或高级版许可证的设备的评估许可证，参考AnyConnect的莫比尔(仅限注册用户)产品许可证注册。如果有在移动许可证需求的特定问题，请发送电子邮件对ac-mobile-license-request@cisco.com。

支持的设备

Q. Cisco VPN 3000 集中器是否支持 AnyConnect?

A. 不能。

Q. PIX安全工具支持AnyConnect VPN客户端?

A. 不PIX不支持AnyConnect VPN客户端。

Q. Cisco IOS® 设备是否支持 AnyConnect?

A. 是。

从 Cisco IOS 软件版本 12.4(15)T 起，仅按照版本 12.4T 新增安全功能注释所述在浏览器启动模式下提供支持。

从 Cisco IOS 软件版本 12.4(20)T 起，也支持独立模式。

有关详细信息，请参阅 SSL VPN 远程用户指南。

注意：

- DTL的支持从Cisco IOS版本15.1(2)T介绍。欲知更多信息，参考svc dtls发出命令。
- Cisco IOS设备不支持客户端Keepalive，直到12.4(20)T版本。
- 对于能导致断开连接的硬件加密更新问题，已经在用于 87x 平台的 12.4(T2) 中得到解决。
- 开始，在Cisco IOS前当前不支持登录。

Q. 苹果公司iPad或IP电话支持AnyConnect VPN客户端?

A. 是。Anyconnect VPN客户端支持从版本2.4的Apple iOS。目前，IP电话3G，IP电话3GS，IP电话4和iPod联系(第二代和以后)是支持的设备。iPad的支持预计是可用的用版本苹果公司iOS 4.2。欲知更多信息，参考版本注释思科苹果公司iOS的Anyconnect 2.4。配置相关信息，请参考用户指南思科苹果公司iOS的Anyconnect 2.4。

Q. 联络iPad、iPod或者IP电话AnyConnect VPN客户端到Cisco IOS路由器是否是可能的?

A. 不能。联络iPad、iPod或者IP电话AnyConnect VPN客户端到Cisco IOS路由器是不可能的。在运行版本8.0(3).1或以上的iPad/IP电话的AnyConnect能仅连接到ASA。Cisco IOS不由苹果公司iOS的AnyConnect VPN客户端支持。欲知更多信息，参考安全工具和版本注释的软件支持的部分Cisco AnyConnect安全移动客户端的2.4，苹果公司iOS 4.2和4.3。

Q. VPN会话故障切换(SSL)对双重网络服务提供商(ISP)是可能的，无需中断会话。例如，如果客户通过SSL VPN通信通过ISP1，并且，如果ISP1断开，这是否通过ISP2将接收连接没有丢失任何数据包(VPN会话)? 是否可以在Cisco 设备上做到这一点?

A. 如果指的是在前端上利用双重 ISP，则没有这样的可能。然而，如果是指类似于远程位置上的双重 ISP，SSL VPN 将可以恢复丢失的连接。如果连接中断，AnyConnect 将尝试重新连接。这是无法配置的，但可以自动执行。只要 ASA 上的会话仍然有效，且 AnyConnect 能够重新建立物理连接，会话就能够恢复。

支持的软件

Q. 什么是支持的MAC OS版本？

A. 从2.0的Cisco AnyConnect VPN客户版本到3.0支持Mac OS X版本10.4和以上。

Cisco AnyConnect VPN客户版本3.0支持Mac OS这些版本：

- Mac OS 10.5 (仅英特尔CPU)
- Mac OS 10.6.x (32位和64位)
- Mac OS X 10.7 (Lion)

其他AnyConnect客户端的支持信息，参考Cisco AnyConnect安全移动客户端的版本注释。

注意：在版本注释的Requirements部分，您能验证最低系统要求运行这些平台中的每一的AnyConnect客户端。

Q. AnyConnect是否需要Java和权限？

A. AnyConnect VPN客户端要求ActiveX或Java使用基于Web的连接/安装。对于ActiveX，用户需要需要权限安装到他们的Web浏览器(或它能事先装配)。如果不支持或未使用ActiveX，将尝试使用Java。其版本可以是1.4.x或1.5。Java实施是一种小程序，并且基于浏览器(无下载)。

在第一个连接，ActiveX/Java用于安装AnyConnect VPN客户端软件。此初始连接要求管理权限。后续的连接则无需管理权限(即使是客户端升级)。客户端有一个独立的安装程序，可在用户不具备管理权限时使用。

Q. 什么是支持的Windows OS版本？

A. 运行Microsoft Vista、Windows 7，Windows XP和Windows 2000的远程最终用户的AnyConnect客户端提供支持。

Cisco AnyConnect VPN客户版本3.0支持Windows操作系统的这些版本：

- Windows 7个x86 (32位)和x64 (64位)
- Windows比斯塔SP2 x86 (32位)和x64 (64位)
- Windows XP SP3 x86 (32位)

其他AnyConnect客户端的支持信息，参考Cisco AnyConnect安全移动客户端的版本注释。

注意：在版本注释的Requirements部分，您能验证最低系统要求运行这些平台中的每一的AnyConnect客户端。

Q. 什么是支持的Linux OS版本？

A. Cisco AnyConnect VPN客户支持多样化的Linux发布，例如Red帽子恩特普赖斯Linux、浅顶软呢帽核心、OpenSuse，Slackware和Ubuntu。

Cisco AnyConnect VPN客户版本3.0支持Linux操作系统的这些版本：

- Red帽子恩特普赖斯Linux 5桌面
- Red帽子恩特普赖斯Linux 6桌面
- Ubuntu 9.x和10.x

其他AnyConnect客户端的支持信息，参考Cisco AnyConnect安全移动客户端的版本注释。

Q. AnyConnect是否支持Windows莫比尔设备？什么是支持的版本？

A. AnyConnect是与Windows莫比尔5.0，6.0和6.1兼容。支持从版本2.3介绍至版本2.5。最新的AnyConnect客户端3.0不提供Windows莫比尔设备的支持。

由AnyConnect客户端版本2.5参考版本注释的Windows莫比尔部分Cisco AnyConnect安全移动客户端的，完整列表的版本2.5所有支持的Windows莫比尔设备。

关于在安装程序的完整详细信息，参考安装在Windows莫比尔设备的AnyConnect。

Q. AnyConnect是否支持新的Symbian软件？

A. 是。Symbian的一个分开的AnyConnect客户端启动与版本2.4.5。关于如何安装客户端的信息，参考Cisco AnyConnect安全移动客户端的Symbian用户指南，版本2.4.5。支持信息，参考Cisco AnyConnect安全移动客户端的2.4版本注释

Symbian的。

Q. 谷歌镀铬物浏览器支持AnyConnect VPN客户端？

A. 是。AnyConnect版本3.0支持它。关于完整详细信息支持的参考的AnyConnect 3.0计算机Oss。

Q. Anyconnect VPN客户端是否支持机器人操作系统？

A. 是。机器人的Cisco AnyConnect安全移动客户端2.4支持机器人设备。有关详细信息，请参阅以下文档：

- Cisco AnyConnect安全移动客户端的2.4版本注释机器人的
- Cisco AnyConnect安全移动客户端的用户指南，机器人的版本2.4

Q. 什么是AnyConnect和ASA不同的版本的兼容性详细信息？

A. 关于兼容性的信息，参考ASA、ASDM、Cisco Secure Desktop和AnyConnect兼容性。

Q. 有没有显示所有支持的AnyConnect功能关于不同的操作系统的兼容性矩阵？

A. 是。参考的AnyConnect安全移动性客户端特性、许可证和Oss，版本2.5欲知更多信息。本文关于不同的可用的许可证也描述功能支持。

Q. 安全套接字层SSL VPN (AnyConnect/无客户端)验证在Novell Linux桌面瘦客户端版本？

A. Cisco 尚未在这一版本的Linux上测试SSL VPN。最佳事例是确保您满足在版本注释定义的前提条件。假设您所提的问题是有关AnyConnect，那么接下来就可以尝试一下。这不会正式合格，但是，如果系统满足前提条件它也许良好工作。如果您所提的问题是有关无客户端SSL VPN，那么答案是应该可以有效运行，因为一般而言您只需要使用浏览器。

日志消息

Q. AnyConnect安装日志在哪里存储在Linux操作系统？

A. 在Linux操作系统上，这些日志在/opt/cisco/vpn存储。

Q. Windows AnyConnect安装日志在哪里存储在Windows操作系统？

A. 有安装的两个可能的位置注册Windows操作系统：

- 如果它是一个新安装，安装日志在用户的临时目录。为了找出此目录，请完成根据您的操作系统的这些步骤：
 - Windows XP和Windows 2000：去Start > Run，输入%temp%，并且点击OK键。
 - Windows Vista：进入在Search窗口的%temp%，并且按回车。
- 如果它是升级，安装日志在是典型地%SYSTEMDRIVE% \临时或\SystemRoot% \临时的系统的临时目录将查找；然而，日志也许在别处查找。

文件名使用一个规则类似于WinSetup-Release-2.0install-21333219012007.log。

数据报传输传送层安全(DTL)

Q. SSL隧道和DTLS隧道有何区别？这两种隧道中各自传输什么类型的数据流？

A. SSL隧道是首先创建到ASA中的TCP隧道。完全建立该隧道后，客户端会尝试协商UDP DTLS隧道。在DTLS隧道的建立过程中，数据可以通过SSL隧道进行传输。当DTLS隧道完全建立后，所有数据都会移动到DTLS隧道，SSL隧道则仅用于偶尔出现的控制信道数据流。如果UDP中有异常情况发生，则会切断DTLS隧道，所有数据将重新通过SSL隧道进行传输。

数据发送方式的决策非常具有动态性。在处理每个网络绑定数据包的同时，代码中有一个点，在这里将会决定是使用SSL连接还是DTLS连接。如果DTL连接是健康的在该瞬间，数据包通过DTL连接发送。否则就通过SSL连接发送。

首先会建立SSL连接，然后数据就会通过这一连接进行传输，与此同时，也会尝试建立DTLS连接。一旦DTLS连接建立起来，上文所述代码中的决策点就会立即开始通过DTLS连接（而不是SSL连接）来发送数据包。另一方面，控制数据包始终通过SSL连接进行传输。

关键点在于是否认为连接正常。如果DTL，一份不可靠协议，是在使用中的，并且DTL连接无论什么原因变坏了，客户端不认识此，直到对端死机检测(DPD)发生。因此，在这短短的一段时间内，通过 DTLS 连接传输的数据就会丢失，因为该连接仍被认为是正常的。一旦发生 DPD，数据会立即通过 SSL 连接发送，DTLS 会重新连接。

ASA 将通过上次接收数据的连接来发送数据。因此，如果客户端已确定 DTLS 连接不正常，并且开始通过 SSL 连接发送数据，ASA 就会通过 SSL 连接进行回复。通过 DTLS 连接来接收数据时，ASA 将恢复使用 DTLS 连接。

Q. 在什么平台上数据报传输支持传送层安全(DTL) ?

A. Windows 2000、Windows XP、Windows比斯塔、Mac OS和Linux操作系统支持DTL。

Q. DTLS 是否同时支持 32 位和 64 位平台?

A. 是。

Q. 两个通道是否(SSL和DTL)，会话的空闲超时能必须被断开?

A. 当 DTLS 隧道处于活动状态时，该隧道就是需要设置空闲超时的唯一隧道。因为只有少量的控制信道数据流通过 SSL 隧道，所以当 DTLS 隧道处于活动状态时，SSL 几乎始终处于空闲状态，因而无需设置空闲超时。如果 UDP 中有异常情况发生，然后切断了 DTLS 隧道，那么此时空闲超时就适用于 SSL 隧道。

不幸地用多数Windows计算机，他们从未“空闲”许多人真认为空闲超时不工作。关于为空闲超时设定“数据阈值”这一问题已经有过很多讨论，但即便如此，这也是一项棘手的任务。为了真做Windows计算机空闲，您必须从计算机的物理接口的网络设置取消微软网络和文件和打印共享。

Q. AnyConnect 通过代理服务器进行连接，但并没有使用 DTLS。为什么?

A. AnyConnect SSL VPN客户端在您的浏览器(仅Internet Explorer能使用一个已配置的代理服务器)。然而，当连接时，它不协商数据报传输传送层安全(DTL)用户数据报协议(UDP)通道。使用仅TLS TCP，当您连接这样时，因为代理服务器配置不是可配置到代理DTL使用的UDP数据包。

Q. 当我使用数据报传输传送层安全(DTL)时在AnyConnect VPN通道，我不能下载大文件和有连通性问题。如何能解决此问题?

A. 请确保未阻止 UDP 端口，因为 DTLS 要使用该端口。再检查 ISP 是否阻止或断开了 DTLS。在与 AnyConnect 进行连接的接口上启用 DTLS。关于启用DTL的更多信息，参考启用数据报传输传送层安全(DTL)与AnyConnect (SSL)连接。

支持的功能

Q. 是否可以在 AnyConnect 上保存口令凭证，这样就无需要求用户进行身份验证（口令存储功能）?

A. 不，保存在AnyConnect的密码凭证是不可能的。

Q. 启动拨号程序功能联机在AnyConnect VPN客户端?

A. 不拨号程序和第三方应用发射器不为在登录(SBL)前的AnyConnect开始支持。

Q. AnyConnect 和 SSL 版本各有什么要求?

A. AnyConnect 要求将 ASA 配置为接受 TLSv1 数据流，并针对 TLSV1.0 配置浏览器设置。

AnyConnect VPN客户端不能建立与这些ASA设置的连接SSL服务器版本的：

- SSL SERVER-VERSION SSLV3
- SSL SERVER-VERSION SSLV3-ONLY (CSCSH76698)

Q. 如果希望在用户通过 VPN 进行连接时自动映射网络驱动器，而一旦用户断开 VPN 则同时断开网络驱动器，有没有什么办法可以做到这一点?

A. 是。您必须写脚本为了达到此。参考文字欲知更多信息，并且部署写脚本。

Q. AnyConnect VPN客户端能否通过IPSec VPN客户端隧道工作？

A. 此功能尚未得到官方支持。这不工作的原因，当使用，当设计是，因为IPSec VPN客户端和AnyConnect VPN客户端尝试对路由流量到他们的虚拟适配器。IPSec VPN客户端拦截AnyConnect流量在瞬时消息传送(IM)层。

Q. AnyConnect (或无客户端SSL VPN)用户可以开始从AnyConnect VPN客户端的管理更改？

A. 不AnyConnect没有任何选项里面它触发或开始密码更改。

密码更改从首端只被触发，当要求作为与终止或轻量级目录访问协议(LDAP)密码到期的MSCHAPv2 RADIUS一部分。他们“登陆对网络”的客户能更改他们的激活目录(AD)密码使用同一Ctrl-Alt-Delete机制假设(在洛金前的开始)。

Q. AnyConnect 是否支持单个地址的池？如果希望ASA执行端口地址转换(PAT)，这样所有远程客户端出现在网络内部作为单个地址，区分由来源TCP端口号？

A. AnyConnect 要求每个客户端使用一个唯一的 IP 地址。因此，PAT 池在这种情况下不适用于 AnyConnect。一定，通过执行的设备PAT (例如主页)不是与AnyConnect的一个问题。

Q. 有没有方式允许用户选择验证证书？

A. 是。您必须设置<AutomaticCertSelection>元素到错误在客户端配置文件。

示例如下：

```
<AnyConnectProfile>
<ClientInitialization>
  <AutomaticCertSelection>false</AutomaticCertSelection>
</ClientInitialization>
</AnyConnectProfile>
```

欲知更多信息，参考自动证书选择。

Q. 在 SSL VPN 上是否可以实现此功能：用户可以同时创建两条隧道，接入网络之后，如果一条隧道出现故障，VPN 客户端可以自动将用户转到第二条隧道？

A. SSL VPN 无法同时使用多个隧道，也无法在一条隧道出现故障的情况下转到另一个隧道。

Q. DHCP服务器能否分配DNS和WINS服务器到AnyConnect VPN客户端？

A. DHCP 分配过程中只会将 IP 地址分配给客户端。DNS 和 WINS 等参数是通过组策略设置分配的，而不是通过 DHCP 确定的。

Q. 只有当我连接对公司网络时，我希望能处理登录脚本。能否运行登录脚本，在AnyConnect建立VPN连接后而不是在登录(SBL)前的良好的开端，必须是每次运行我启动计算机(我是否希望对VPN)？

A. AnyConnect在版本2.4和以上介绍OnConnect脚本功能。版本注释的参考的Scripting部分Cisco AnyConnect VPN客户的，版本2.4。关于执行脚本的全部信息，参考Cisco AnyConnect VPN客户管理员指南的Scripting部分，版本2.4。

Q. 在与全部磁盘加密软件的登录(SBL)功能前AnyConnect开始例如加密，任何地方PointSec和PGP？

A. 可以，AnyConnect 2.2 版支持这样做。

Q. 有没有什么方法可以支持 SOCKS 类型代理？

A. AnyConnect 不支持 SOCKS 类型代理。SOCKS 不是 HTTPS 代理，所以 Cisco 不支持 SOCKS 代理。

AnyConnect 将通过“HTTPS”(具体而言是 HTTPS 1.1)代理在 SSL 模式下工作。另外，还会使用通过“基本”或 NTLM 进行授权的身份验证代理。

您必须启用代理的使用https 1.1先进的Internet Explorer设置的。

Q. 如何提示远程用户下载客户端？

A. 您可以使用组策略 webvpn 或用户名 webvpn 配置模式中的 svc ask 命令，通过安全设备提示远程 SSL VPN 客户端用户下载客户端：

```
svc ask {none | enable [default {webvpn | svc} timeout value]}
```

svc ask enable 命令可以提示远程用户下载客户端或转到无客户端连接的门户页，并无限时地等待用户响应。

- svc ask enable default svc - 立即下载客户端。
- svc ask enable default webvpn - 立即转到门户页。
- svc ask enable default svc timeout value - 提示远程用户下载客户端或转到门户页，在按持续时间值进行等待后若无响应则执行默认操作，即下载客户端。
- svc ask enable default webvpn timeout value - 提示远程用户下载客户端或转到门户页，在按持续时间值进行等待后若无响应则执行默认操作，即显示门户页。

Q. AnyConnect是什么重新连接行为？

A. 如果连接中断，AnyConnect 将尝试重新连接。此行为自动和不可配置。只要ASA的会话有效，会话将恢复，如果AnyConnect能重建物理连接。

版本2.2包括允许AnyConnect重新连接，在PC睡眠后的漫游功能。客户端将持续不确定尝试，直到首端告诉它不能重新连接，并且客户端不会立即切断通道，当系统参加冬眠/待机。对于不希望使用此功能的客户，请将会话超时设置到一个较低的值，以防转入休眠或恢复重新连接。

Q. 当重新连接发生时， AnyConnect虚拟适配器 (VA)摆动或路由表更改？

A. 即使是低级别的重新连接也不会如此。这是仅发生在 SSL 或 DTLS 上的重新连接。这些尝试大约会持续 30 秒，然后就会放弃。如果 DTLS 失败，它只是断开而已。如果 SSL 失败，将会引发高级别的重新连接。高级别的重新连接将彻底重新执行路由。如果在重新连接分配的客户端地址 (或影响VA)的任何其他配置参数，没有更改，则VA没有禁用

Q. AnyConnect VPN客户端是否支持二要素验证？

A. AnyConnect VPN客户端从ASA版本8.2(x)开始支持二要素验证。版本不支持它在8.2.(x)之前。

Q. AnyConnect VPN客户端是否支持从在同样PC同时安装的其他供应商的其他VPN客户端？

A. AnyConnect 2.5安装能共存以其他VPN客户端，包括IPSec客户端，所有支持的终端的;然而，当其他VPN客户端运作时，思科不支持运行AnyConnect。

Q. AnyConnect是否支持互联网连接共享 (ICS) ？

A. 互联网连接共享 (ICS) 不是与AnyConnect兼容。您必须禁用适当的AnyConnect功能的ICS。

当您设法启动在ICS已经运行的PC时的AnyConnect， AnyConnect返回此错误消息：

VPN客户端代理程序无法创建进程间通信维修站。

为了解决此问题，请禁用ICS并且再启动AnyConnect。

Q. ASA是否支持CSD IOS设备的PRE洛金评估， 当连接对AnyConnect时？

A. 目前， ASA不支持它。参考的增强请求CSCtr63396 (仅限注册用户)欲了解更详细的信息。

Q. 如何检查AnyConnect是否连接或不从在Windows机器的DOS提示符？

A. 完成这些步骤：

1. 在Windows机器，请点击Start > Run，键入cmd，并且按回车为了打开命令提示符窗口。
2. 发出此on命令CLI：

```
C:\Program Files\Cisco\Cisco AnyConnect VPN Client> vpncli.exe state
```

```
Cisco AnyConnect VPN Client (version 2.5.0193) beta.
```

```
Copyright (c) 2004 - 2010 Cisco Systems, Inc. All Rights Reserved.
```

```
>> state: Connected  
>> state: Connected  
>> registered with local VPN subsystem.  
>> state: Connected  
>> state: Connected
```

Q. IP地址分配到AnyConnect客户端可以是相同的象客户端PC机的原始IP地址？

A. 不能。ASA（由设计）分配内部IP地址到所有用户。没有指定的IP地址，如果是对路由流量回到最终用户，ASA将需要是一切的默认网关在网络。这从网络设计方面不会是可实现的。

Q. AnyConnect是否是FIP投诉客户端？

A. 是。开始与AnyConnect版本2.4，它是FIP投诉客户端。它在ASA要求您采购FIP许可证为了去。许可证(每个ASA)提供您对必填信息的获取为了有AnyConnect FIP兼容版本。参考的FIP和附加安全性在新的AnyConnect本地策略欲了解更详细的信息。

Q. AnyConnect VPN客户端是否支持分割DNS功能？

A. 是。开始用版本3.0.4235，AnyConnect支持Windows和Mac机器的真的分割DNS功能。参考的分割DNS功能增强欲了解更详细的信息。

Q. 将打开在客户端的两个方式的什么端口为了AnyConnect能正常运行？

A. AnyConnect 3.0，这些端口将允许的：

```
TLS (SSL) - TCP 443  
SSL Redirection - TCP 80 (optional)  
DTLS - UDP 443 (optional but HIGHLY recommended)  
IPsec/IKEv2 - UDP 500, UDP 4500 (and the client services port used for SSL)  
Legacy IPsec IKEv1 - ESP mode - UDP 500, Protocol 50  
IPsec/NAT-T - UDP 500, UDP 4500  
IPsec/TCP - TCP XXX (admin definable)  
IPsec/UDP - UDP 500, UDP XXX (admin definable)
```

欲知更多信息，参考AnyConnect VPN客户端的端口信息。

Q. 什么属性由DAP报告，当AnyConnect客户端连接，不用CSD支持时，并且CSD在ASA启用？

A. 当CSD为AnyConnect平台时不是可用的，但是CSD在ASA启用，AnyConnect执行一条“CSD旁路”。当CSD旁路执行时，AnyConnect报告这些DAP属性：

```
endpoint.os.version = "MacOS" | "Palm WebOS" | "Linux" | "Pocket PC" |  
"Apple Plugin" | "Unknown"  
endpoint.feature = "failure"
```

“苹果公司插件”属性为iPad和IP电话报告。“掌上型计算机WebOS”为运行WebOS的设备报告，例如掌上型计算机Pre。“Linux”为Linux桌面和嵌入式Linux派生的客户端报告(例如用户网真客户端)。“掌上电脑”为Windows莫比尔设备报告。“MacOS”为Apple MAC设备报告。“未知”为所有其它设备报告。

例如，在IP电话客户端的DAP trace将显示此信息：

```
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]  
["clienttype"]="AnyConnect"  
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.feature="failure"  
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.os.version="Apple Plugin"
```

IOS设备的DAP属性在一些ASA版本可能被中断。结果，如果其不工作，请确保您不遇到在Cisco Bug ID CSCtj46900（仅限注册用户）的问题。

Q. 在苹果公司IOS设备存储本地的哪些四保护类(A类、B、C或者D)用于存储AnyConnect数据(例如用户凭证、VPN会话等等)？

A. IP电话的AnyConnect客户端不存储用户凭证。数字证书没有在Apple的cert存储存储并且通过苹果公司保护，没有思

科。

AnyConnect直接地存储非敏感-当前主题， URI处理程序设置和本地化数据的数据。AnyConnect不设置此数据的任何特殊加密属性。其他内容(配置文件，连接属性等等)是通过苹果公司VPN特定被处理的全部API。根据苹果公司，配置在.plist存储，不用任何已添加保护(即中集集团D)。

Q. 在机器人的AnyConnect是否支持VPN负载均衡功能?

A. 是。此功能从机器人版本的2.4 AnyConnect支持。欲了解更详细的信息，参考此表。

错误消息

Q. AnyConnect VPN客户端安装失效与此错误消息：错误1722。有一问题用此Windows安装程序包。如何能解决此问题?

A. AnyConnect 安装失败，并出现这一错误：

```
MSI (s) (D8:70) [14:59:10:750]: Product: Cisco AnyConnect VPN Client
-- Error 1722. There is a problem with this Windows Installer package

A program run as part of the setup did not finish as expected. Contact
your support personnel or package vendor. Action VACon_Install,
location: C:\Program Files\Cisco\Cisco AnyConnect VPN Client\VACon.exe, command:
-install "C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnva.inf" VPNVA
```

1722 错误是有关 MSI 操作失败的通用代码。在这种情况下，正如 MSI 日志中所显示的，虚拟适配器安装程序已经失败。因此，您需要检查是否存在此注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce。

另外，您能设法这些操作之一为了解决问题：

- 执行此命令为了执行AnyConnect的平静的安装：

```
msiexec /quiet /norestart /i anyconnect.msi
```

- 扫描您的AnyConnect的注册涉及假密钥并且删除他们。

Q. 当他们连接到VPN集中器通过SSL VPN客户端时，在Microsoft代理后的用户收到此错误：不支持代理服务器提供的身份验证协议都。如何能解决此问题?

A. 该错误消息通常意味着，代理服务器所配置使用的身份验证机制在 SSL VPN 客户端上不受支持。

AnyConnect 将通过 HTTPS (具体而言是 HTTPS 1.1) 代理在 SSL 模式下工作。另外，还会使用通过“基本”或 NT Lan Manager 进行授权的身份验证代理。当您使用代理服务器时，推荐使用 NTLM。

有AnyConnect VPN客户端的Internet Explorer代理

如果有Internet Explorer配置与代理，您必须通过设置的代理连接激活使用HTTP 1.1使用AnyConnect VPN客户端。如果此选项没有设置， AnyConnect VPN客户端连接不出来。

在 Internet Explorer 的“工具”菜单中选择“Internet 选项”。单击高级选项卡。，和在HTTP 1.1设置下，检查使用HTTP 1.1通过代理连接。

此Internet Explorer设置如何影响AnyConnect ?

AnyConnect，类似SVC，使用Windows互联网(WinINet)预隧道连接。这是一种用于执行初始身份验证和下载更新内容的连接。WinINet 是一种编程式接口，Internet Explorer 也会在后台加以利用。WinINet通过在Internet Explorer的选项菜单显示配置。该菜单中有一项是通过代理使用 http:1.1。

因此，当 VPNDownloader 连接到前端以执行验证时，它将通过 WinINet API 执行该操作。这就是所发生的隧道前操作的一部分。

数据实际通道在不用WinINet的单独的信道发生，并且它是只知道关于ProxyIP的此单独的信道：ProxyTCPPort。

简而言之，请认为AnyConnect GUI/VPNDownloader和浏览器启动作为Internet Explorer扩展为协商隧道连接。但是，所有的隧道数据都通过不使用 WinINet 的单独信道来传输。

Q. 当我尝试安装Windows机器的时AnyConnect VPN客户端，我收到此错误消息：管理员权限要求安装VPN客户端。

如何能解决此问题？

A. 设法这些应急方案之一为了解决此问题：

- 禁用客户端防火墙、所有防病毒软件和运行在客户端机器的任何第三方软件。
- 验证操作系统的兼容性在客户端机器的。参考Cisco AnyConnect安全移动客户端版本注释欲知更多信息。
- 请验证，如果语言自定义配置，如果是，禁用它。

请使用ASDM检查路径：Configuration>远程访问VPN >语言本地化>客户端MST语言转换。

- 保证RunOnce注册表项(HKEY_LOCAL_MACHINE \软件\ Microsoft \ Windows \ CurrentVersion \ RunOnce)存在如提供在Cisco Bug ID CSCsr54507 (仅限注册用户)上。
- 添加ASA的IP地址或名称到在Web浏览器的可信的站点列表。欲知更多信息，参考Cisco Bug ID CSCsu54601 (仅限注册用户)。

Q. 当同一个文件名的新配置文件上传对ASA闪存时， AnyConnect VPN客户端下载更旧的配置文件。如何能解决此问题？

A. 再次发出 `svc profile` 命令以重新加载缓存（首选）。或者您能手工复制从disk0的配置文件：复制到 `cache:/stc/profiles`。

或者，上传一个不同的文件名对于新配置文件(例如profile1.xml、profile2.xml等等)和映射此新建的文件名对组将更新与新配置文件信息的AnyConnect关于其导航。

Q. AnyConnect与此错误消息的VPN客户端软件崩溃：Cisco AnyConnect VPN客户下载者遇到了问题并且需要关闭。如何能解决此问题？

A. 出现此错误的原因在于 `biolsp.dll` 驱动程序。这是该驱动程序的一个已知问题。通过更新该驱动程序即可解决此错误。

Q. 当我尝试连接AnyConnect VPN客户端版本2.4时，我收到此错误消息：证书问题遇到了。VPN连接不会被建立。如何能解决此问题？

A. 此错误生成由于在Cisco Bug ID描述的问题CSCtb73337 (仅限注册用户)。AnyConnect客户端版本2.4不与Cisco IOS头端一起使用，当的证书没有委托或有在URL输入的主机名的不匹配对那对CN使用时(公用名称)或SAN (附属的替代方案名称)在Cisco IOS路由器证书。

AnyConnect 2.4不能连接Cisco IOS头端由于certificate verify失败错误。

此问题可以是解决的通过这些应急方案之一：

- 确保路由器证书委托(导入到证书存储里)然后匹配在证书的CN/SAN对那URL。如果没有DNS条目，则您能通过更新主机文件使用本地DNS条目主机名在证书。
- 对以前版本的降级AnyConnect : 2.3.

Q. 当我连接对与AnyConnect版本2.5的ASA在我的Linux计算机时，我收到此错误：在安全网关的AnyConnect包不能查找。如何能解决此问题？

A. 验证您在WebVPN配置里上传正确AnyConnect包(Linux)对ASA并且指定此镜像。请使用这些命令执行这些任务：

- 复制镜像文件：

```
hostname#copy tftp flash
```

- 指定镜像的优先级使用AnyConnect :

```
hostname(config-webvpn)#svc image anyconnect-linux-2.X.XXXX-k9.pkg 1
```

Q. 我无法使用 AnyConnect 进行连接，并收到这一错误：ANYConnect is not enabled on the VPN Server。如何能解决此问题？

A. ANYConnect在VPN服务器错误错误消息没有启用也许发生由于这些原因：

- 您未装载在ASA的包文件。
- 包文件的版本在ASA的是与在PC (AnyConnect VPN客户端)的使用的版本MSI不同。

例如，您也许有在ASA安装的AnyConnect VPN客户端版本2.1的包和有在PC安装的2.3 MSI。要避免此问题，应该在ASA 和 PC 上使用相同的版本。

Q. 当我尝试连接用Internet Explorer 7时的AnyConnect VPN客户端，我收到此错误消息：安全证书的撤销信息此站点的不是可用的。是否要继续？三次，在窗口去离开前，我点击Yes单选按钮。此错误为什么出现，并且如何解决？

A. 安全证书的撤销信息此站点的不是可用的错误消息通常归结于与您使用的证书的一问题，以及尝试连接的浏览器。这通常意味着，您在证书中配置了 http 或 ldap CRL 分发点，并且浏览器也已配置为对此进行检查，但却无法达到该分发点。

为了解决此问题，请验证服务器证书撤销选项的检查(查找在工具> Internet选项>Advanced选项卡下>请检查服务器证书撤销(要求重新启动浏览器))被不选定。如果选项被检查，请不选定选项，并且保存设置为了解决此问题。

Q. 在使用了后，我无法连接Windows比斯塔的AnyConnect VPN客户端睡眠和恢复功能。我收到在AnyConnect GUI的此错误消息：VPN客户端驱动程序遇到错误。此错误为什么出现，并且如何解决？

A. 此问题在Cisco Bug ID CSCsm60339 (仅限注册用户)描述。

为了解决此问题，请重新启动PC，并且设法重新连接通道。应急方案是应用在KB-952876描述的ICM Hotfixes 。

Q. 我接收此错误消息：接收的服务器证书或其一系列不遵照FIP。如何能解决此问题？

A. 在失败的尝试登陆期间对AnyConnect客户端，您也许收到错误消息。关于如何解决此问题的信息，参考的Anyconnect ‘服务器证书接收的或其一系列不遵照FIP’ 。

相关信息

- PIX/ASA安全工具FAQ
- Cisco Secure Desktop (CSD) 常见问题
- 问答

版权所有 ©1992-2014 思科系统

文件创建日期: 2013 年 8 月 5 日

http://www.cisco.com/cisco/web/support/CN/108/1081/1081893_anyconnect-faqs.html
