ASA 8.X：AnyConnect Start Before Logon 功能配置

目录

简介

使用*在登录*(SBL)前的*开始*启用，用户看到AnyConnect GUI登录对话，在Windows ®登录对话框出现前。此情况下将首先建立 VPN 连接。Start Before Logon 仅可用于 Windows 平台，管理员通过此功能可以控制登录脚本的使用、密码缓存以及网络驱动器到本地驱动器的映射等。您可使用 SBL 功能激活 VPN，使其作为登录序列的一部分。默认情况下 SBL 处于禁用状态。

关于配置AnyConnect VPN客户端功能的更多信息，参考配置AnyConnect客户端特性的部分。

注意： 在 AnyConnect 客户端中，您要为 SBL 执行的唯一一项配置便是启用该功能。网络管理员将根据自身所处情况的要求执行登录前的处理操作。登录脚本可分配给一个域或个人用户。通常，域管理员为 Active Directory 中的用户或组定义了批处理文件或类似文件。用户一旦登录，将立即执行登录脚本。

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以下软件和硬件版本：

- 运行软件版本 8.x 的 Cisco ASA 5500 系列自适应安全设备
- Cisco AnyConnect VPN 2.0 版

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。

背景信息

SBL 的作用是在登录 PC 之前先将远程计算机连接到公司的基础架构。例如，用户可能位于公司物理网络之外，无法访问公司资源，直到他或她的 PC 加入公司网络。SBL 处于启用状态时，在用户看到 Microsoft 登录窗口前，将首先连接 AnyConnect 客户端。当 Microsoft 登录窗口出现时，用户也必须照常登录 Windows。

以下是使用 SBL 的几个原因：

- 用户的 PC 加入了 Active Directory 基础架构。
- 用户无法在 PC 上拥有缓存凭证，即组策略禁止缓存凭证。
- 用户运行的登录脚本必须从网络资源执行或要求访问网络资源。
- 用户拥有的网络映射驱动器需要通过 Active Directory 基础架构进行身份验证。
- 网络组件（例如 MS NAP/CS NAC）可能需要连接到基础架构。

SBL 会创建一个网络，相当于加入本地公司 LAN。SBL 处于启用状态时，因为用户可访问本地基础架构，则通常针对办公室中的用户运行的登录脚本也可用于远程用户。

有关如何创建登录脚本的信息，请参阅此 Microsoft TechNet 文章 。

有关如何在 Windows XP 中使用本地登录脚本的信息，请参阅此 Microsoft 文章 。

另外，可以对系统进行配置，使其禁止用于 PC 登录的缓存凭证。在这种情况下，用户必须能够与公司网络中的域控制器进行通信，以使其凭证在访问 PC 前得以验证。SBL 要求在其调用时存在网络连接。在某些情况下无法实现这一点，因为无线连接可能要依靠用户凭证才能连接到无线基础架构。因为 SBL 模式先于登录过程的凭证阶段，因此在这种情况下不存在连接。在这种情况下，需要配置无线连接以在登录过程中缓存凭证，或者需要配置另外的无线身份验证以使 SBL 正常运行。

安装 Start Before Logon 组件（仅适用于 Windows）

必须在核心客户端已安装后才能安装 Start Before Logon 组件。另外，AnyConnect 2.2 Start Before Logon 组件要求安装核心 AnyConnect 客户端软件 2.2 版或更高版本。如果使用 MSI 文件预部署 AnyConnect 客户端和 Start Before Logon 组件（例如，您身在一个拥有自己的软件部署（Altiris、Active Directory 或 SMS）的大公司），则必须确保正确的安装顺序。如果通过 Web 部署和/或更新 AnyConnect，则当管理员加载 AnyConnect 时，系统将自动处理安装顺序。有关完整的安装信息，请参阅 Cisco AnyConnect VPN 客户端 2.2 版的发行版本注释。

在Windows比斯塔\ Windows 7和PRE Vista开始之间的区别在登录前

启用SBL的步骤在Windows比斯塔和Windows轻微有所不同7个系统。PRE Vista系统使用组分呼叫的虚拟专用网络图形识别和验证(VPNGINA)实现SBL。Vista和Windows 7个系统使用呼叫PLAP的一个组件实现SBL。

在AnyConnect客户端， Windows比斯塔开始，在登录功能叫作PRE洛金接入服务商(PLAP)前，是一个可连接的证件供应商。此功能使网络管理员可以在登录前执行特定任务，比如收集凭证或连接到网络资源。PLAP在登录前的提供开始在Windows比斯塔、Windows 7和Windows 2008服务器作用。PLAP 可分别通过 vpnplap.dll 和 vpnplap64.dll 支持 32 位和 64 位版本的操作系统。PLAP 功能支持 Windows Vista x86 和 Windows Vista x64 版本。

注意： 在此部分，在PRE Vista平台的登录功能和PLAP在Windows比斯塔和Windows的登录功能前是指开始7个系统前， VPNGINA是指开始。

在 Vista 之前的系统中，Start Before Logon 使用一种称为 VPN 图形识别和身份验证动态链接库 (vpngina.dll) 的组件提供 Start Before Logon 功能。作为 Windows Vista 一部分的 Windows PLAP 组件取代了 Windows GINA 组件。

用户按 Ctrl+Alt+Del 组合键可激活 GINA。而对于 PLAP，按 Ctrl+Alt+Del 组合键后将打开一个窗口，用户可从中选择登录到系统或通过该窗口右下角的 Network Connect 按钮激活任何网络连接（PLAP 组件）。

接下来的部分将介绍 VPNGINA 和 PLAP SBL 的设置及过程。有关在 Windows Vista 平台上启用和使用 SBL 功能 (PLAP) 的完整说明，请参阅在 Windows Vista 系统上配置 Start Before Logon (PLAP)。

用于启用 SBL 的 XML 设置

UseStartBeforeLogon 的元素值可用于打开 (true) 或关闭 (false) 此功能。如果在配置文件中将该值设为 **true**，则将发生额外的处理过程作为登录序列的一部分。有关其他详细信息，请参阅 Start Before Logon 说明。设置在CiscoAnyConnect.xml文件的<UseStartBefore Logon>值为trueto enable (event) SBL ：

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

若要禁用 SBL，请将该值设为 **false**。

若要启用 UserControllable 功能，请在启用 SBL 时使用此语句：

```
<UseStartBeforeLogon userControllable="false">true</UseStartBeforeLogon>
```

任何与此属性相关联的用户设置都存储在别处。

启用 SBL

为了尽量缩短下载时间，AnyConnect 客户端仅请求（从安全设备）下载其支持的每个功能所需的核心模块。若要启用新功能（例如 SBL），您必须在组策略 WebVPN 配置模式或用户名 WebVPN 配置模式下使用 **svc modules** 命令指定模块名称：

```
[no] svc modules {none | value string}
```
SBL 的字符串值是 **vpngina**。

在本示例中，网络管理员为组策略远程工作者进入组策略属性模式，而为组策略进入 WebVPN 配置模式，并指定字符串 VPNGINA 以启用 SBL：

```
hostname(config)# group-policy telecommuters attributes hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```
此外，管理员必须确保 AnyConnect <profile.xml> 文件（其中 <profile.xml> 是网络管理员指定给 XML 文件的名称）的 <UseStartBeforeLogon> 语句设为 **true**，例如：

```
UseStartBeforeLogon UserControllable="false">true
```
Start Before Logon 开始生效前，必须重新启动系统。您还必须在安全设备上指定允许使用 SBL 或其他任何用于实现额外功能的模块。有关详细信息，请参阅启用用于实现额外 AnyConnect 功能的模块，第 2-5 页 (ASDM) 部分或启用用于实现额外 AnyConnect 功能的模块，第 3-4 页 (CLI) 中的说明。

使用 CLI 配置 Start Before Logon

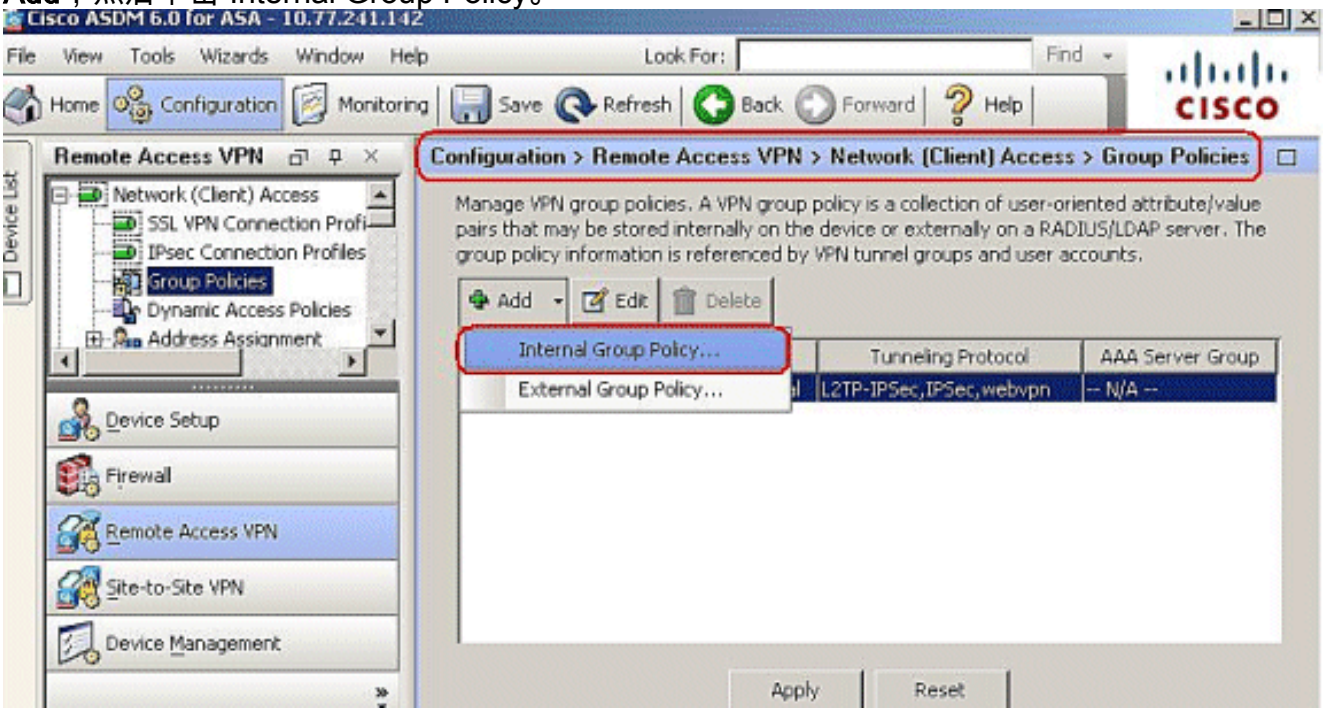
本方案将向您说明如何使用 CLI 设置 XML 文件：

1. 创建要推送到客户端 PC 的配置文件，如下所示：
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```
2. 将该文件复制到安全设备的闪存中：
```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```
3. 在安全设备上，在 AnyConnect 连接的其他相关设置都正确的情况下，将该配置文件作为可用配置文件添加到 WebVPN 全局部分：`hostname(config-group-policy)# webvpn hostame(config-group-webvpn)# svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml`
4. 编辑您使用的组策略，并添加 **svc modules** 和 svc profile 命令：`hostname(config)# group-policy GroupPolicy internal hostname(config)# group-policy GroupPolicy attributes hostname(config-group-policy)# webvpn hostame(config-group-webvpn)# svc modules value vpngina hostame(config-group-webvpn)# svc profiles value ReallyNewProfile`

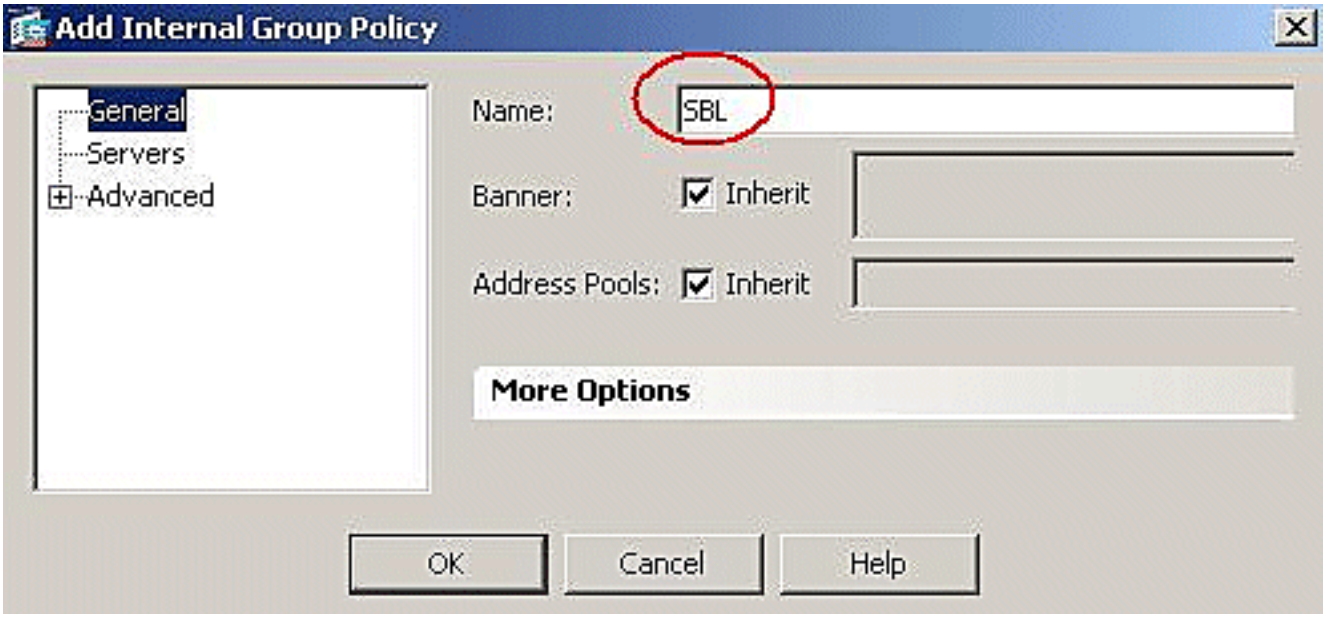
使用 ASDM 配置 Start Before Logon

请完成以下步骤，以使用 ASDM 配置 SBL：

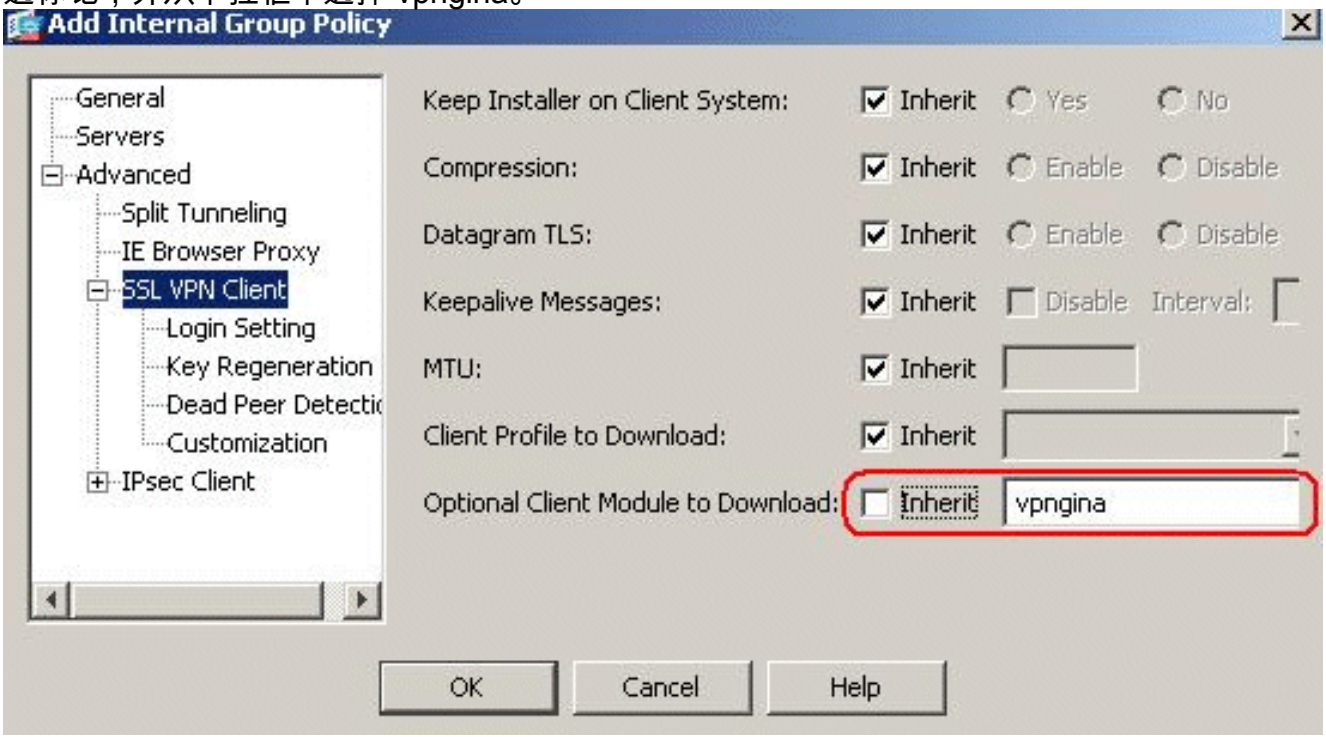
1. 创建要推送到客户端 PC 的配置文件，如下所示：
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```
2. 将该配置文件作为 **AnyConnectProfile.xml** 保存到本地计算机中。
3. 启动 ASDM，转至主页。
4. 转至 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add**，然后单击 Internal Group Policy。



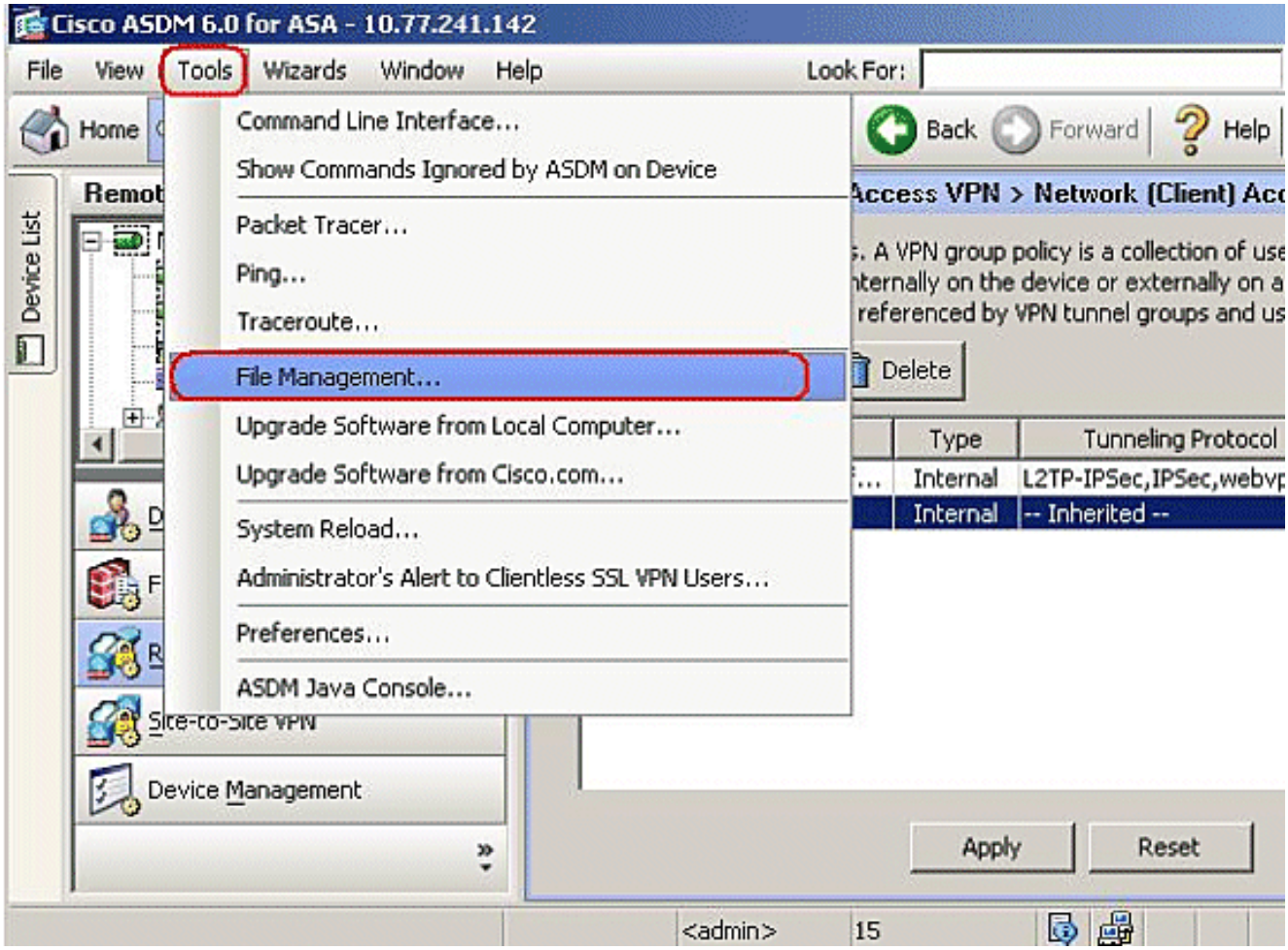
5. 输入组策略的名称，例如 **SBL**。



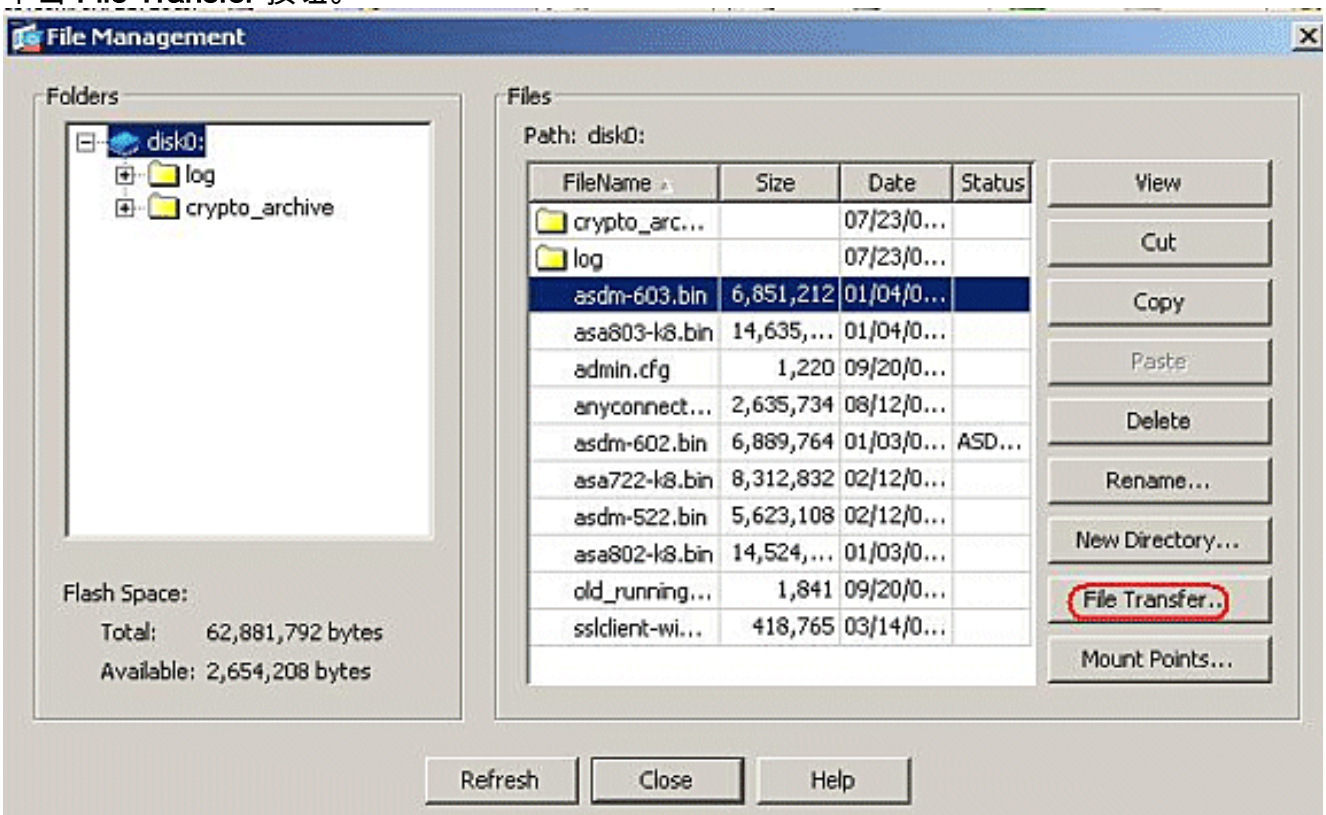
6. 转至 **Advanced > SSL VPN Client**。删除 **Optional Client Module to Download** 中的 Inherit 复选标记，并从下拉框中选择 vpngina。



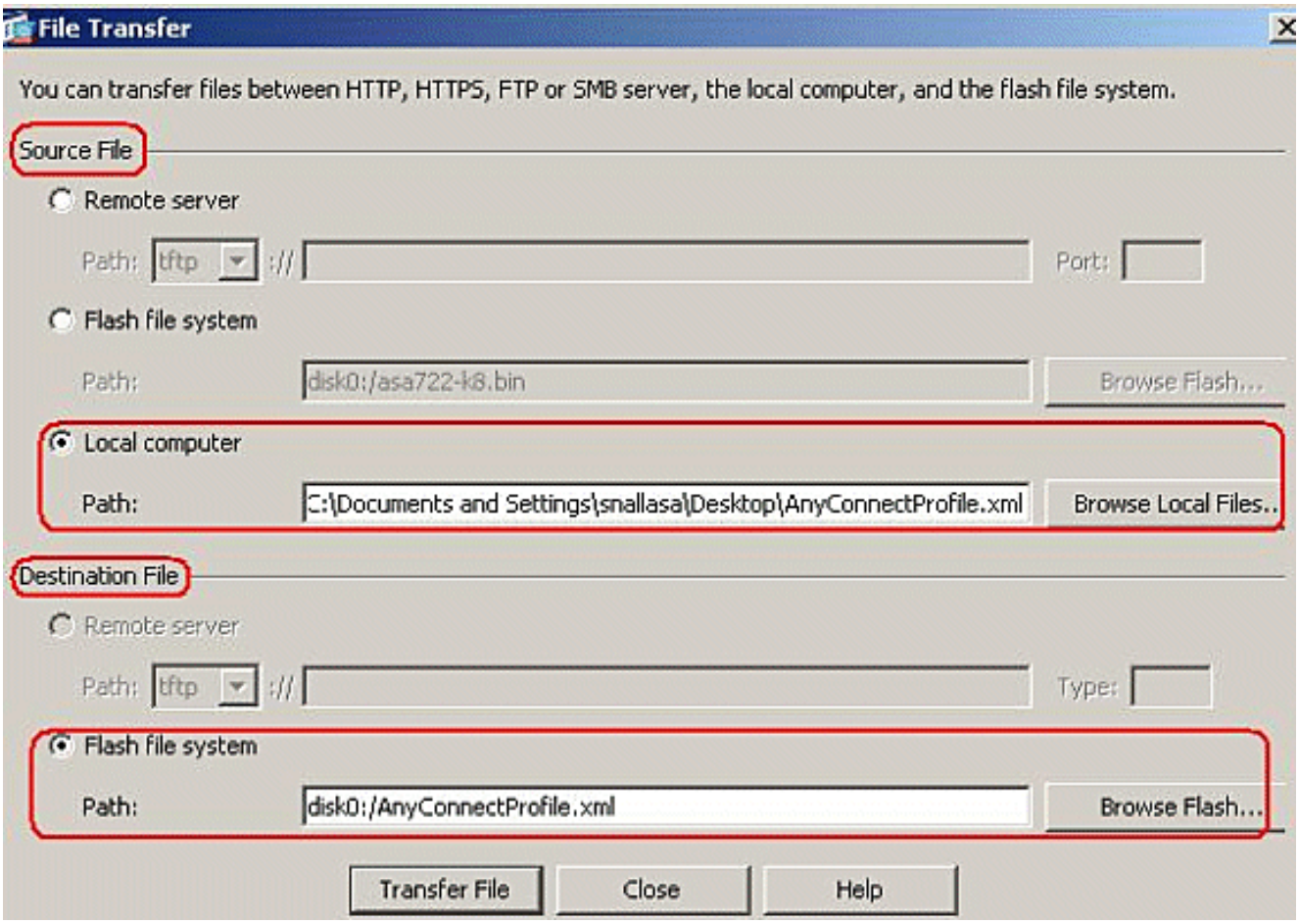
7. 为了转接配置文件**AnyConnectProfile.xml**从本地计算机闪烁，请去工具，**并且**点击 FileManagement。



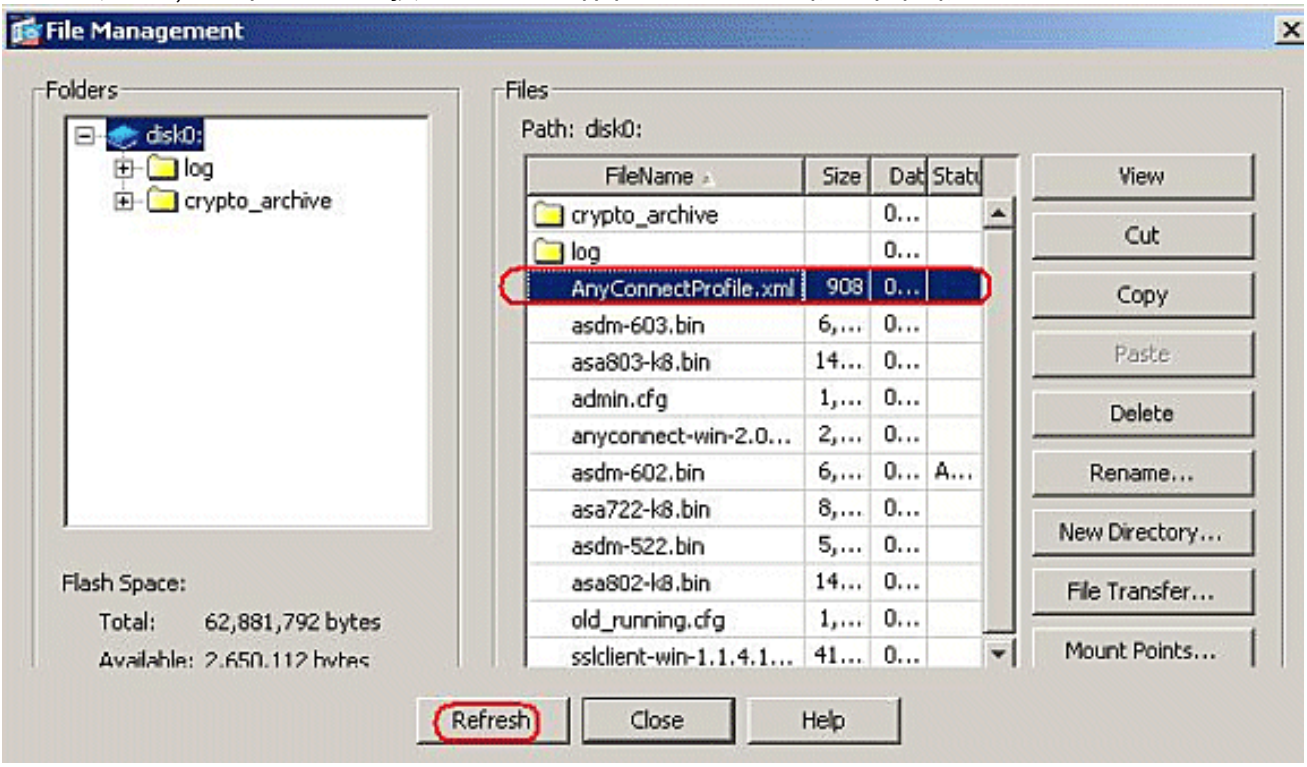
8. 单击 **File Transfer** 按钮。



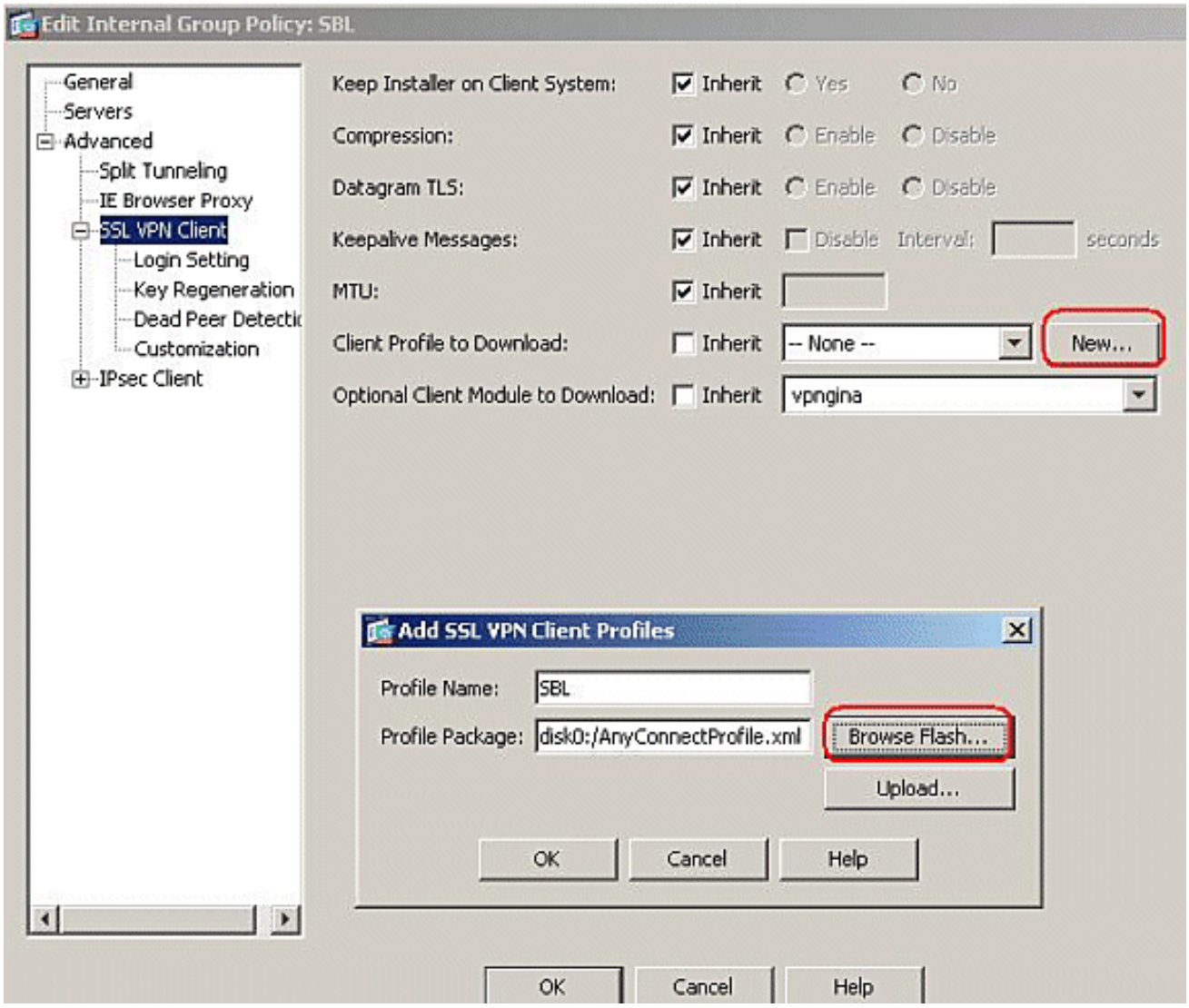
9. 要将配置文件从本地计算机传输到 ASA 闪存，请在 **Source File** 部分选择 XML 文件的路径 (local computer)，并根据要求选择 Destination File 路径。



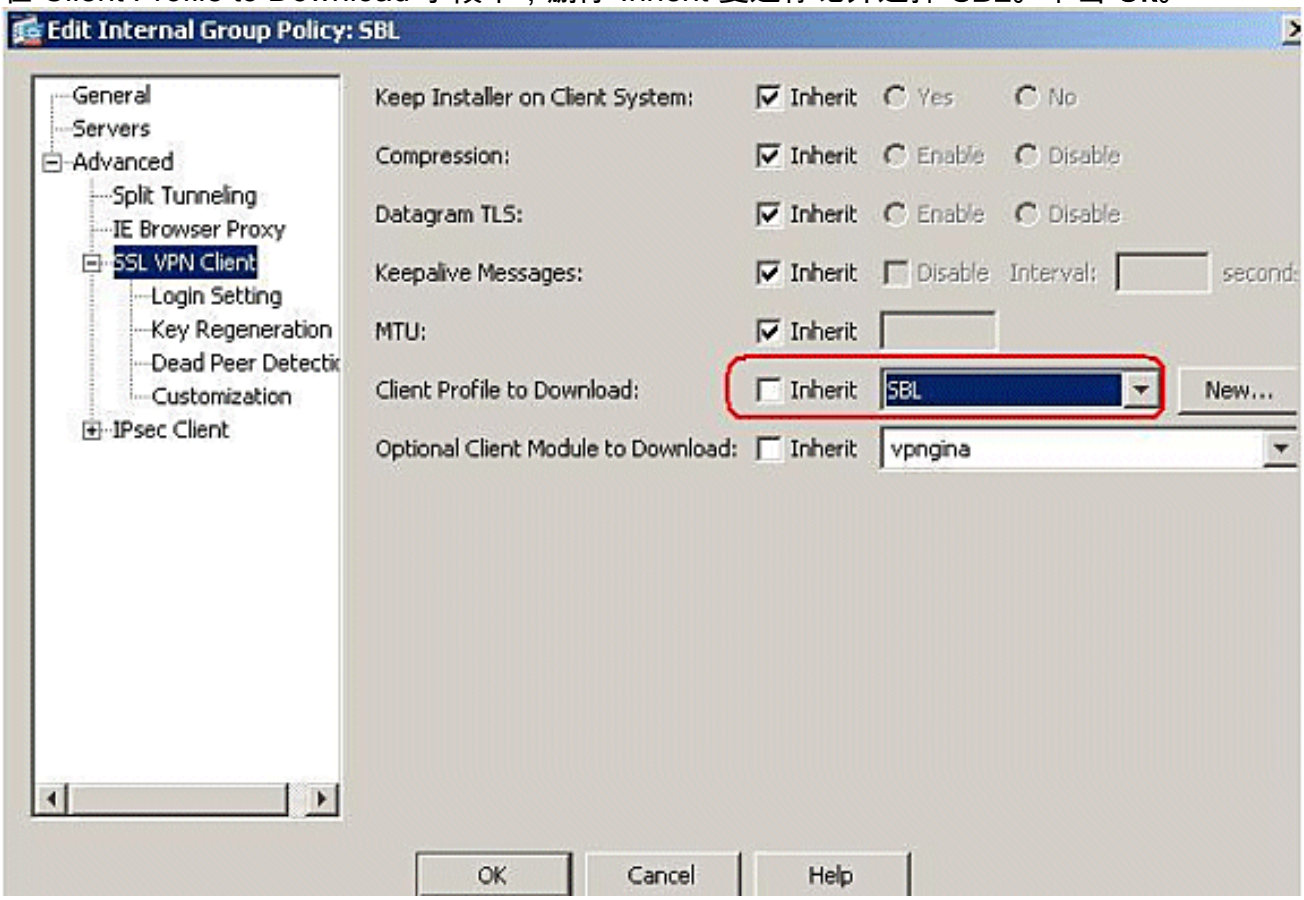
10. 传输完成后，单击 **Refresh** 按钮以验证该配置文件是否已存储在闪存中。



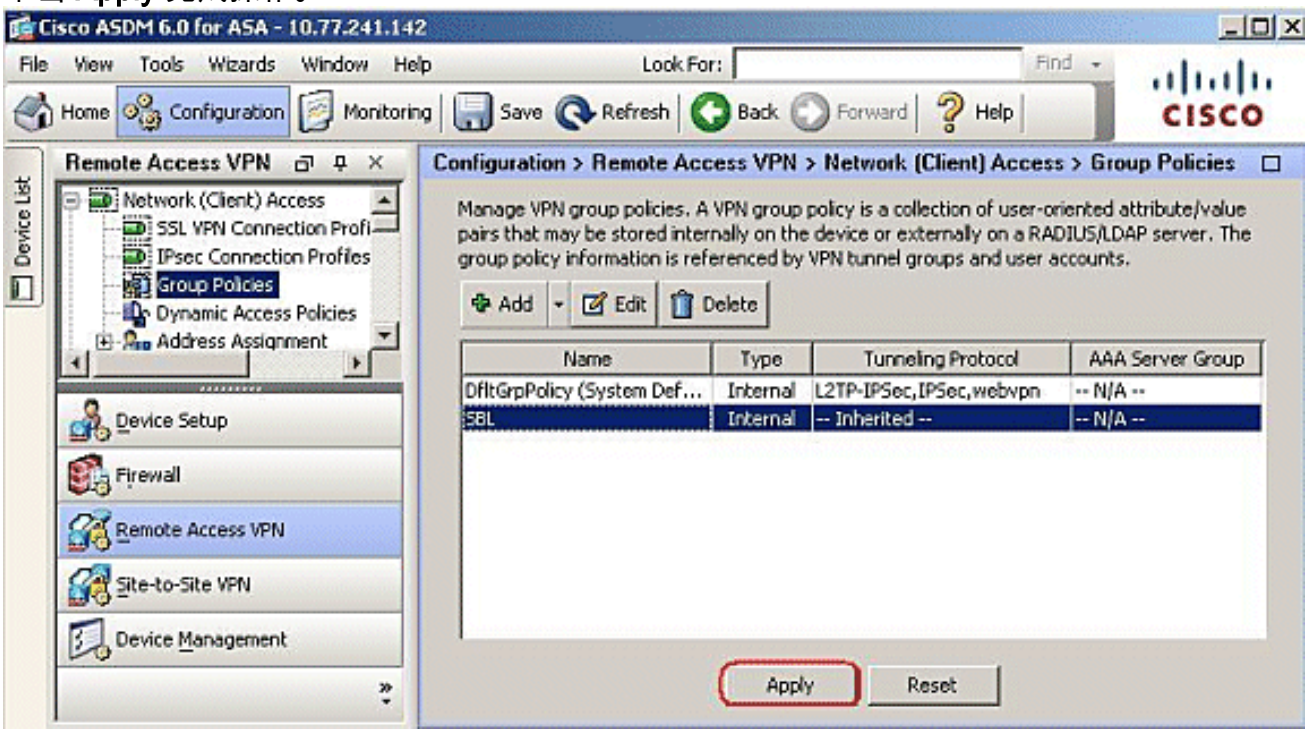
11. 将配置文件指定给内部组策略 (SBL)。按照以下路径操作：**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Edit SBL (Internal Group Policy) > Advanced > SSL VPN Client > Client Profile to Download**，然后单击 New 按钮。在 **Add SSL VPN Client Profiles** 中，单击 Browse 按钮以选择配置文件 (AnyConnectProfile.xml) 存储在 ASA 闪存中的位置。分配Namefor配置文件，例如， SBL。**点击**完整的OKTO。



12. 在 Client Profile to Download 字段中，删除 Inherit 复选标记并选择 **SBL**。单击 **Ok**。



13. 单击 **Apply** 完成操作。



使用清单文件

上载到安全设备的 AnyConnect 程序包中包含一个称为 VPNManifest.xml 的文件。以下示例显示了该文件的示例内容：

```
<?xml version="1.0" encoding="UTF-7"?> <vpn rev="1.0">
<file version="2.1.0150" id="VPNCore"
   is_core="yes" type="exe" action="install">
   <uri>binaries/anyconnect-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>
 <file version="2.1.0150" id="gina"
   is_core="yes" type="exe" action="install" module="vpngina">
   <uri>binaries/anyconnect-gina-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>
</vpn>
```

安全设备上存储了已配置的配置文件（如步骤 1 中的说明），并存储了一个或多个 AnyConnect 程序包，这些程序包包含 AnyConnect 客户端本身、下载程序实用程序、清单文件以及其他任何可选模块或支持文件。

当远程用户通过 WebLaunch 或当前独立客户端连接到安全设备后，将首先下载并运行下载程序。下载程序使用清单文件来确定远程用户的 PC 上是否有需要升级的当前客户端或确定是否需要执行新的安装。清单文件也包含有关是否必须下载和安装任何可选模块（此例中为 VPNGINA）的信息。也将从安全设备中推送客户端配置文件。可通过组策略 (webvpn) 命令模式下配置的 **svc modules value vpngina** 命令激活 VPNGINA 的安装，如步骤 4 中所述。安装 AnyConnect 客户端和 VPNGINA 后，用户将在下次重新启动时，在登录 Windows 域之前看到 AnyConnect 客户端。

用户连接时，将向用户 PC 传送客户端和配置文件；然后安装客户端和 VPNGINA；用户将在下次重新启动时，在登录之前看到 AnyConnect 客户端。

安装 AnyConnect 时，将在客户端 PC 上提供一个示例配置文件：**C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**。

SBL 故障排除

如果 SBL 出现问题，请采用以下过程：

1. 确保配置文件已推送。
2. 删除之前的配置文件；在硬盘上搜索这些配置文件，找到其所在位置：*.xml.
3. 转到“添加或删除程序”，确认 AnyConnect 和 AnyConnect VPNGINA 是否都已安装。
4. 卸载 AnyConnect 客户端。
5. 清除事件查看器中的用户 AnyConnect 日志，然后重新测试。
6. 通过 Web 浏览回到安全设备，以重新安装客户端。
7. 确保配置文件也同时出现。
8. 重新启动一次。下次重新启动时，您将看到 Start Before Logon 提示符。
9. 将 AnyConnect 事件日志以 .evt 格式发送给 Cisco。
10. 如果看到此错误，请删除用户配置文件并使用默认配置文件：`Description: Unable to parse the profile` **`C:\Documents and Settings\All Users\Application Data\Cisco \Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml.`** `Host data not available.`

问题 1

在尝试上载 AnyConnect 配置文件时出现此错误消息：Error in validating the XML file against the latest schema。如何解决此问题？

解决方案 1

此错误消息主要由 AnyConnect 配置文件中的语法或配置问题引发。要解决此问题，请确保配置的 AnyConnect 配置文件与 Cisco AnyConnect VPN 客户端管理员指南的示例 AnyConnect 配置文件和 XML 架构部分中所示的示例 AnyConnect 配置文件相似。

相关信息

- Cisco AnyConnect VPN Client 管理员指南，版本 2.0
- 创建登录脚本 - Windows TechNet
- 在 Windows Vista 系统上配置 Start Before Logon (PLAP)
- 通过 AnyConnect SSL VPN 客户端进行 ASA 8.x VPN 访问的配置示例
- Cisco AnyConnect VPN 客户端
- Cisco ASA 5500 系列自适应安全设备
- 技术支持和文档 - Cisco Systems