ASA ：使用ASDM的Smart Tunnel配置示例

目录

简介

智能隧道是基于TCP的应用与专用站点之间的连接，使用无客户端（基于浏览器）SSL VPN会话，安全设备作为路径，安全设备作为代理服务器。您可以确定要向其授予智能隧道访问权限的应用，并指定每个应用的本地路径。对于在Microsoft Windows上运行的应用，您还需要匹配校验和的SHA-1哈希值，作为授予智能隧道访问权限的条件。

*Lotus SameTime*和*Microsoft Outlook Express*是您可能希望授予智能隧道访问权限的应用程序示例。

根据应用是客户端还是启用Web的应用，智能隧道配置需要以下步骤之一：

- 创建客户端应用的一个或多个智能隧道列表，然后将列表分配给要为其提供智能隧道访问的组策略或本地用户策略。
- 创建一个或多个书签列表条目，指定符合智能隧道访问条件的启用Web的应用的URL，然后将列表分配给要为其提供智能隧道访问的DAP、组策略或本地用户策略。您还可以列出启用Web的应用，以便通过无客户端SSL VPN会话在智能隧道连接中自动提交登录凭证。

本文档假设Cisco AnyConnect SSL VPN客户端配置已进行且工作正常，以便可以在现有配置上配置智能隧道功能。有关如何配置Cisco AnyConnect SSL VPN客户端的详细信息，请参阅ASA 8.x:在 ASA 上允许 AnyConnect VPN 客户端使用分割隧道的配置示例）。

注意：确保在ASA 8.x的*ASDM 6.0(2)*部分中介绍的步骤4.b到4.l:*在ASA上不执行AnyConnect*

VPN客户端的允许分割隧道配置示例，以便配置智能隧道功能。

本文档介绍如何在Cisco ASA 5500系列自适应安全设备上配置智能隧道。

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8.0(2)的思科ASA 5500系列自适应安全设备
- 运行Microsoft Vista、Windows XP SP2或Windows 2000 Professional SP4（带Microsoft Installer 3.1版）的PC
- Cisco 自适应安全设备管理器 (ASDM) 版本 6.0(2)

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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

智能隧道访问配置

智能隧道表显示智能隧道列表，每个列表标识符合智能隧道访问资格的一个或多个应用及其关联的操作系统(OS)。 由于每个组策略或本地用户策略都支持一个智能隧道列表，因此必须将要支持的非基于浏览器的应用分组到智能隧道列表中。配置列表后，您可以将其分配给一个或多个组策略或本地用户策略。

通过智能隧道窗口(**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**)，您可以完成以下步骤：

- **添加智能隧道列表并将应用添加到列表**要添加智能隧道列表并将应用添加到列表，请完成以下步骤：单击 **Add**。系统将显示Add Smart Tunnel List对话框。输入列表名称，然后单击 **Add**。ASDM会打开Add Smart Tunnel Entry对话框，通过该对话框可以将智能隧道的属性分配给列表。为智能隧道分配所需属性后，单击**OK**。ASDM在列表中显示这些属性。根据需要重复这些步骤以完成列表，然后在Add Smart Tunnel List（添加智能隧道列表）对话框**中单**击OK（确定）。
- **更改智能隧道列表**要更改智能隧道列表，请完成以下步骤：双击列表或在表中选择列表，然后单击“**编辑”**。单击**Add**将新的智能隧道属性集插入列表或在列表中选择条目，然后单击Edit或**Delete**。
- **删除列表**要删除列表，请在表中选择该列表，然后单击“**删除”**。

- **添加书签**在配置和分配智能隧道列表后，您可以通过为服务添加书签并点击Add或Edit Bookmark对话框中的**Enable Smart Tunnel**选项，使智能隧道易于使用。

智能隧道访问允许基于客户端TCP的应用使用基于浏览器的VPN连接连接到服务。与插件和传统技术、端口转发相比，它为用户提供了以下优势：

- 智能隧道提供比插件更好的性能。
- 与端口转发不同，智能隧道无需将本地应用的用户连接到本地端口，从而简化了用户体验。
- 与端口转发不同，智能隧道不要求用户具有管理员权限。

智能隧道要求、限制和限制

一般要求和限制

智能隧道具有以下一般要求和限制：

- 发起智能隧道的远程主机必须运行32位版本的Microsoft Windows Vista、Windows XP或Windows 2000;或Mac OS 10.4或10.5。
- 智能隧道自动登录仅支持Windows上的Microsoft Internet Explorer。
- 浏览器必须启用Java、Microsoft ActiveX或两者。
- 智能隧道仅支持在运行Microsoft Windows的计算机和安全设备之间放置的代理。智能隧道使用Internet Explorer配置（即，用于Windows系统范围的配置）。 如果远程计算机需要代理服务器来访问安全设备，则连接终止端的URL必须位于从代理服务中排除的URL列表中。如果代理配置指定发往ASA的流量通过代理，则所有智能隧道流量都通过代理。在基于HTTP的远程访问场景中，有时子网不提供用户对VPN网关的访问。在这种情况下，ASA前面的代理用于在Web和最终用户位置之间路由流量，从而提供Web访问。但是，只有VPN用户可以配置放置在ASA前面的代理。这样做时，他们必须确保这些代理支持CONNECT方法。对于需要身份验证的代理，智能隧道仅支持基本摘要身份验证类型。
- 当智能隧道启动时，安全设备会从用户用于启动无客户端会话的浏览器进程中隧道传输所有流量。如果用户启动浏览器进程的另一个实例，则会将所有流量传递到隧道。如果浏览器进程相同，且安全设备不提供对给定URL的访问，则用户无法打开该URL。解决方法是，用户可以使用与用于建立无客户端会话的浏览器不同的浏览器。
- 状态故障切换不会保留智能隧道连接。用户必须在故障切换后重新连接。

Windows要求和限制

以下要求和限制仅适用于Windows:

- 只有Winsock 2（基于TCP的应用程序）才符合智能隧道访问的条件。
- 安全设备不支持Microsoft Outlook Exchange(MAPI)代理。端口转发和智能隧道都不支持MAPI。对于使用MAPI协议的Microsoft Outlook Exchange通信，远程用户必须使用AnyConnect。
- 使用智能隧道或端口转发的Microsoft Windows Vista用户必须将ASA的URL添加到受信任站点区域。要访问“受信任站点”区域，请启动Internet Explorer，然后选择“工具”>“Internet选**项”，然**后单击“安**全”**选项卡。Vista用户还可以禁用保护模式，以便于智能隧道访问；但是，思科建议不采用此方法，因为它增加了攻击的漏洞。

Mac OS要求和限制

这些要求和限制仅适用于Mac OS:

- Safari 3.1.1或更高版本或Firefox 3.0或更高版本
- Sun JRE 1.5或更高版本
- 只有从门户页面启动的应用才能建立智能隧道连接。此要求包括对Firefox的智能隧道支持。在首次使用智能隧道时使用Firefox启动另一个Firefox实例需要名为csco_st的用户配置文件。如果此用户配置文件不存在，会话会提示用户创建一个配置文件。
- 使用TCP且动态链接到SSL库的应用可以通过智能隧道工作。
- 智能隧道不支持Mac OS上的以下功能和应用：代理服务自动登录使用两级名称空格的应用基于控制台的应用，如Telnet、SSH和cURL使用dlopen或dlsym查找libsocket调用的应用程序静态链接的应用程序，用于查找libsocket调用

配置

本部分提供有关如何配置本文档所述功能的信息。

添加或编辑智能隧道列表

通过Add Smart Tunnel List对话框，可以向安全设备配置添加智能隧道条目列表。通过Edit Smart Tunnel List对话框，可以修改列表的内容。

字段

列表名称 — 输入应用程序或程序列表的唯一名称。名称中的字符数没有限制。请勿使用空格。配置智能隧道列表后，列表名称会显示在无客户端SSL VPN组策略和本地用户策略中的Smart Tunnel List属性旁。分配一个名称，以帮助您将其内容或用途与可能配置的其他列表区分开。

添加或编辑智能隧道条目

通过Add or Edit Smart Tunnel Entry对话框，可以在智能隧道列表中指定应用的属性。

- **应用ID** — 输入字符串以命名智能隧道列表中的条目。该字符串对于操作系统是唯一的。通常，它会命名要授予智能隧道访问权限的应用。为了支持选择为其指定不同路径或哈希值的应用程序的多个版本，您可以使用此属性区分条目，指定操作系统以及每个列表条目支持的应用程序的名称和版本。字符串最多可以包含 64 个字符。
- **进程名**称(Process Name) — 输入应用程序的文件名或路径。字符串最多可包含128个字符Windows要求将此值与远程主机上应用路径的右侧完全匹配，以便对应用进行智能隧道访问。如果仅指定Windows的文件名，则SSL VPN不会对远程主机实施位置限制以限定应用进行智能隧道访问。如果指定路径，并且用户将该应用程序安装在另一个位置，则该应用程序不符合条件。只要字符串的右侧与您输入的值匹配，应用程序就可以驻留在任何路径上。如果应用存在于远程主机上的多条路径之一上，则要授权应用进行智能隧道访问，请在此字段中仅指定应用的名称和扩展，或为每个路径创建唯一的智能隧道条目。对于Windows，如果要向从命令提示符启动的应用程序添加智能隧道访问，必须在智能隧道列表中一个条目的进程名称中指定"cmd.exe"，并在另一个条目中指定应用程序本身的路径，因为"cmd.exe"是该应用程序的父项。Mac OS需要该进程的完整路径，且区分大小写。为避免为每个用户名指定路径，请在部分路径（例如~/bin/vnc）前插入一个代号(~)。
- **OS** — 单击Windows或Mac以指定应用的主机OS。
- **哈希** -(*可选，仅适用于Windows*)要获取此值，请将可执行文件的校验和输入实用程序，该实用

程序使用SHA-1算法计算哈希。此类实用程序的一个示例是Microsoft文件校验和完整性验证器(FCIV)，该验证器可在“文件校验和完整性验证器”实用程序的“可用性”和“说明”中找到。安装FCIV后，将要散列化的应用程序的临时副本放在不包含空格的路径(例如c:/fciv.exe)上，然后在命令行(例如fciv.exe -sha1 c:\msimn.exe)输入fciv.exe -sha1应用程序以显示SHA-1散列。SHA-1哈希始终为40个十六进制字符。在授权应用进行智能隧道访问之前，无客户端SSL VPN会计算与应用ID匹配的应用的哈希值。如果结果与哈希值匹配，它将限定应用进行智能隧道访问。输入哈希值可以合理保证SSL VPN不会限定与您在应用ID中指定的字符串匹配的非法文件。由于校验和因应用程序的每个版本或补丁而异，因此您输入的哈希只能与远程主机上的一个版本或补丁匹配。要为一个应用的多个版本指定哈希，请为每个哈希值创建一个唯一的智能隧道条目。**注意：**如果您输入哈希值并且希望支持具有智能隧道访问权限的应用的未来版本或补丁，则必须在将来更新智能隧道列表。智能隧道访问突然出现问题可能表明包含哈希值的应用程序与应用程序升级不同步。不输入哈希值可以避免此问题。

- 配置智能隧道列表后，必须将其分配给组策略或本地用户策略，以便其变为活动状态，如下所示：要将列表分配到组策略，请选择**Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add or Edit > Portal**，然后从Smart Tunnel List属性旁边的下拉列表中选择智能隧道名称。要将列表分配给本地用户策略，请选择**Config > Remote Access VPN> AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN**，然后从Smart Tunnel List属性旁边的下拉列表中选择智能隧道名称。

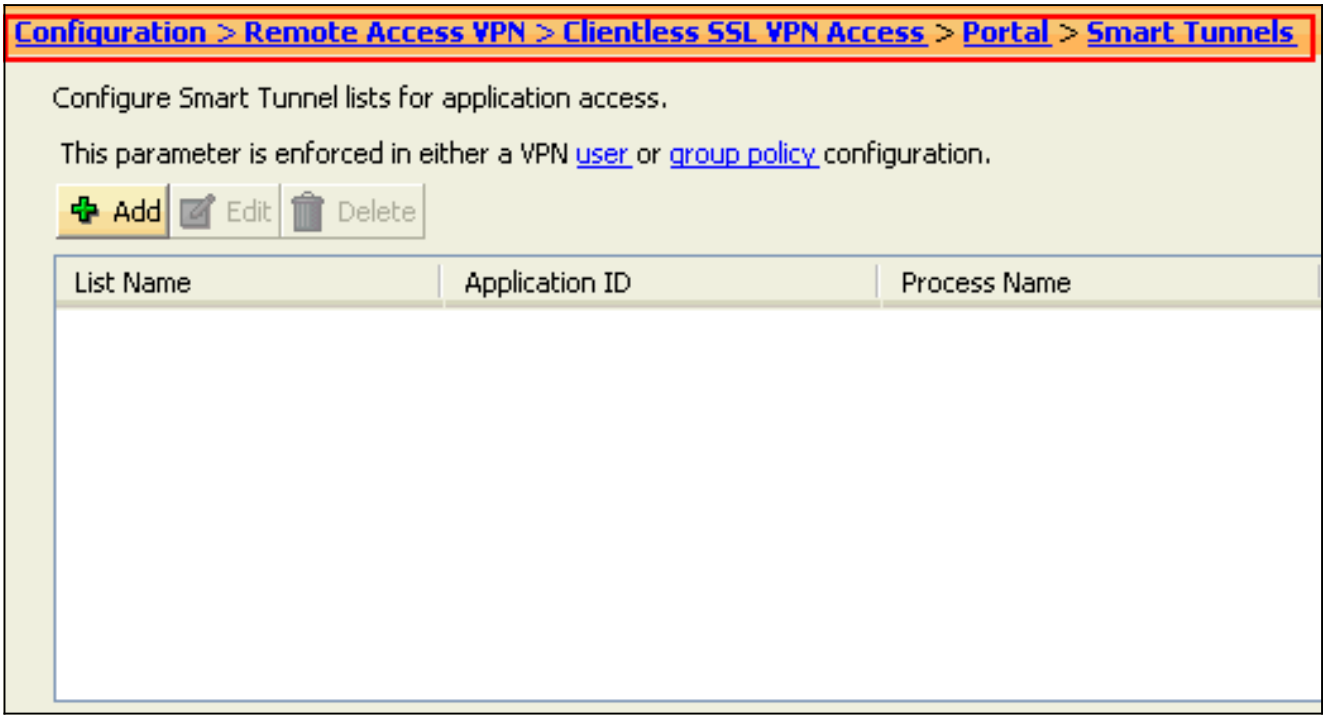
使用ASDM 6.0(2)的ASA智能隧道（Lotus示例）配置

本文档假设基本配置（如接口配置）已完成且工作正常。

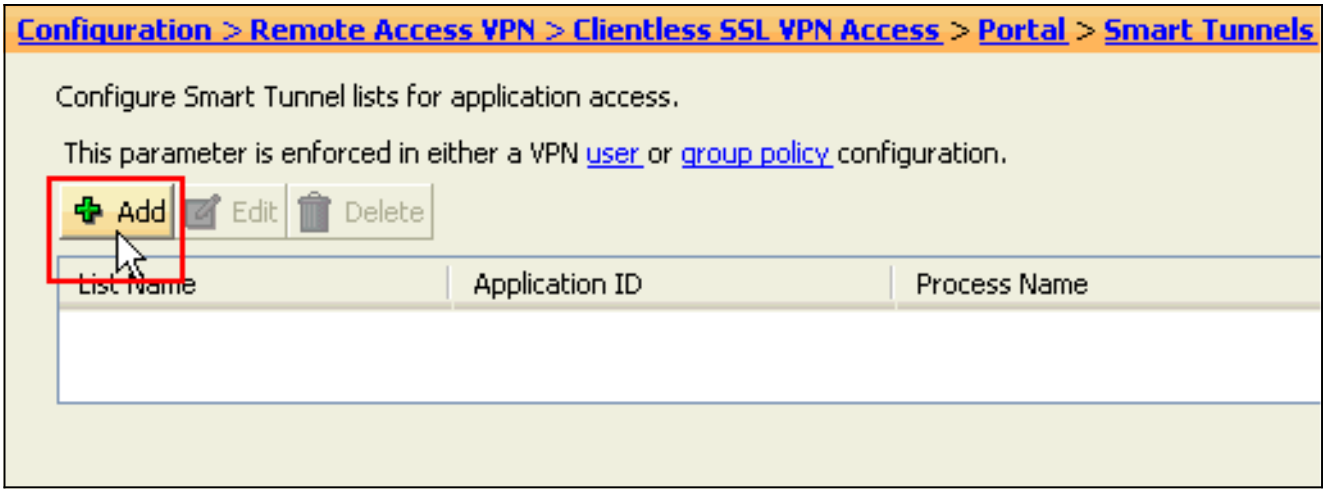
要配置智能隧道，请完成以下步骤：

注意：在此配置示例中，为Lotus应用配置了智能隧道。

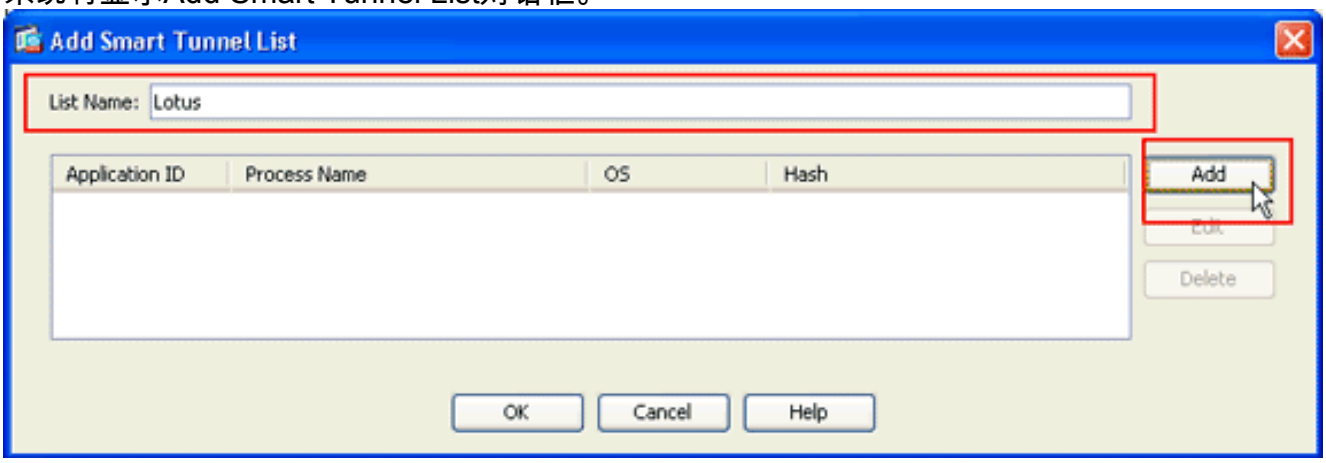
1. 选择**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**以启动智能隧道配置。



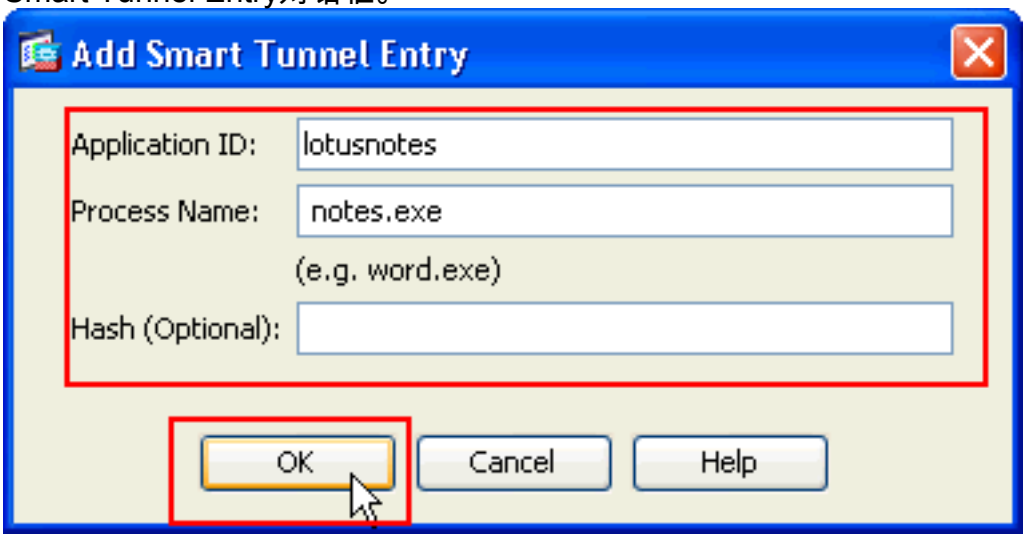
2. 单击 **Add**。



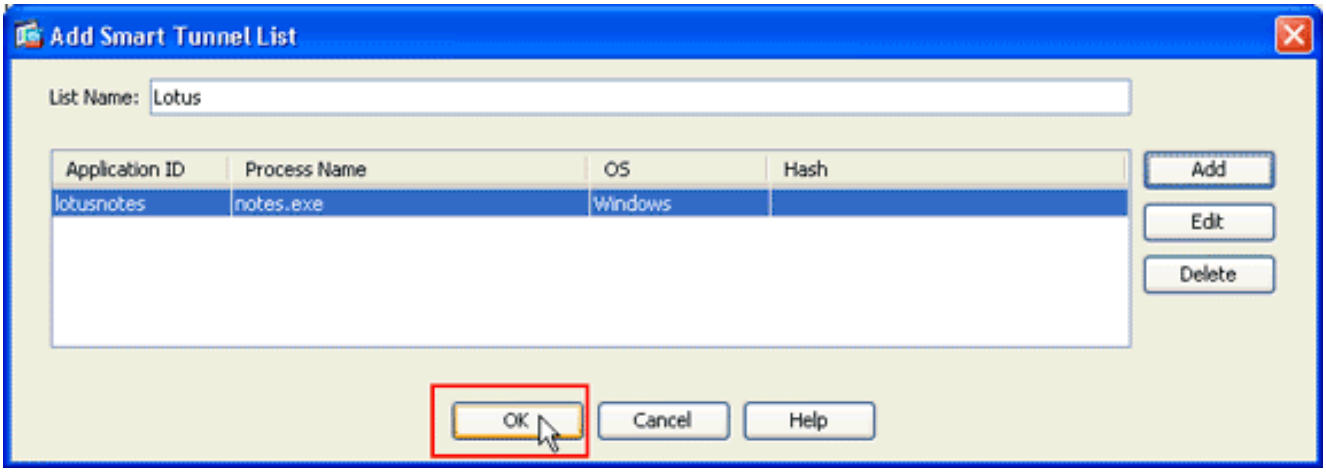
系统将显示Add Smart Tunnel List对话框。



3. 在Add Smart Tunnel List（添加智能隧道列表）对话框中，单击**Add(添加)**。系统将显示Add Smart Tunnel Entry对话框。

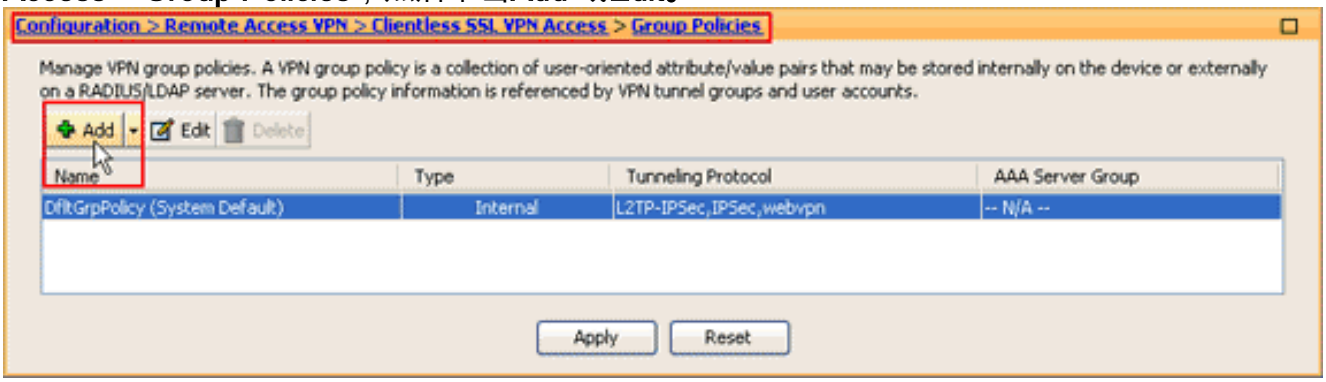


4. 在应用ID字段中，输入一个字符串以标识智能隧道列表中的条目。
5. 输入应用程序的文件名和扩展名，然后单击**确定**。
6. 在添加智能隧道列表对话框中，单击**确定**。

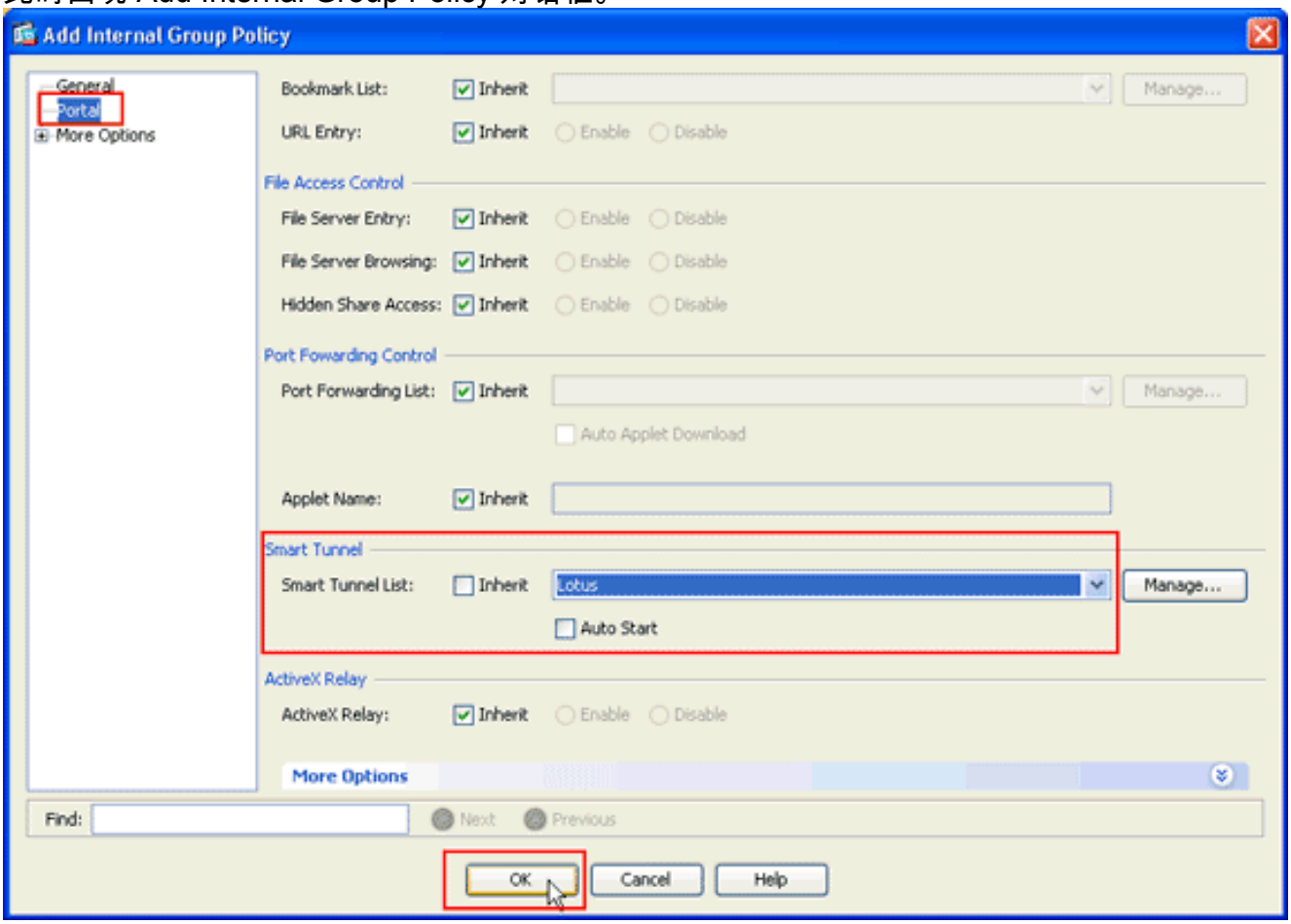


注意：以下是等效的CLI配置命令：

7. 将列表分配给要向其提供对关联应用的智能隧道访问的组策略和本地用户策略，如下所示：要将列表分配给组策略，请选择**Configuration > Remote Access VPN> Clientless SSL VPN Access > Group Policies**，然后单击**Add** 或**Edit**。



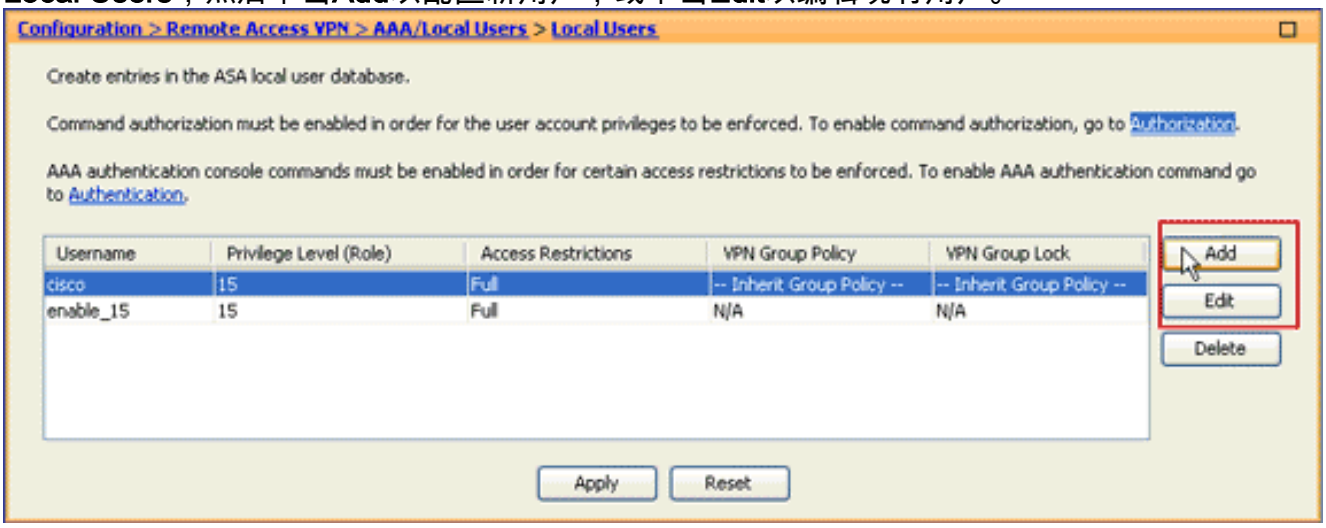
此时出现 Add Internal Group Policy 对话框。



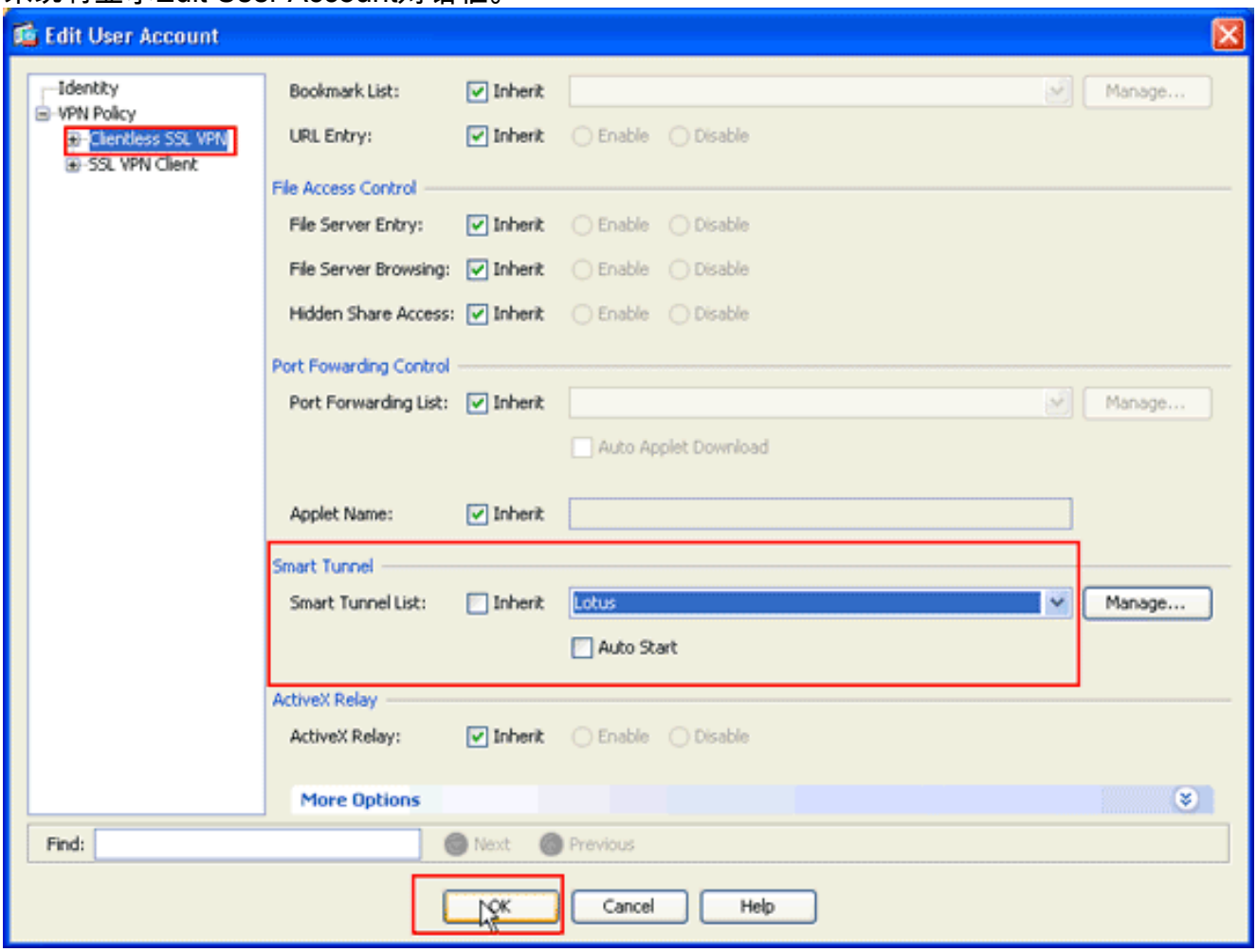
8. 在Add Internal Group Policy对话框中，单击**Portal**，从Smart Tunnel List下拉列表中选择智能

隧道名称，然后单击**OK**。**注意**：本示例使*用*Lotus作为智能隧道列表名称。

9. 要将列表分配给本地用户策略，请选择**Configuration > Remote Access VPN> AAA Setup > Local Users**，然后单击**Add**以配置新用户，或单击**Edit**以编辑现有用户。



系统将显示Edit User Account对话框。



10. 在Edit User Account（编辑用户帐户）对话框中，单击**Clientless SSL VPN**，从Smart Tunnel List（智能隧道列表）下拉列表中选择智能隧道名称，然后单击**OK（确定）**。**注意**：本示例使*用*Lotus作为智能隧道列表名称。

智能隧道配置已完成。

故障排除

我无法使用无客户端门户中带书签的智能隧道URL进行连接。为什么会发生此问题，我如何解决？

此问题是由于Cisco Bug ID CSCsx05766(仅限注册客户)中描述的问题。 要解决此问题，请将Java Runtime插件降级到较旧版本。

能否获取在WebVPN中配置的智能隧道链路的URL?

在ASA上使用智能隧道时，您无法获取URL或隐藏浏览器的地址栏。用户可以查看在使用智能隧道的WebVPN中配置的链路的URL。因此，他们可以更改端口并访问服务器以获得其他服务。

要解决此问题，请使用WebType ACL。有关详细信息，请参阅WebType访问控制列表。

相关信息

- Cisco ASA 5500 系列自适应安全设备
- 在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例
- 技术支持和文档 - Cisco Systems