ASA ：使用ASDM的Smart Tunnel配置示例

目录

简介

一个巧妙的通道是一基于TCP的应用程序和一个私有站点之间的一连接，使用一无客户端(基于浏览器的) SSL VPN会话用安全工具作为路和安全工具作为代理服务器。您能识别您要准许聪明的通道访问和指定本地路径对每应用程序的应用程序。对于在Microsoft Windows运行的应用程序，您能也需要校验和的SHA-1哈希的匹配，当授权的聪明的通道访问一个条件。

*Lotus SameTime*和*Microsoft Outlook Express*是您也许要准许聪明的通道访问应用程序的示例。

从属应用程序是否是客户端或是支持Web的应用程序，聪明的隧道配置要求这些步骤之一：

- 建立客户端应用的一个或更多聪明的通道列表，然后分配列表到您要提供聪明的通道访问的组策略或本地用户策略。
- 创建指定有资格的支持Web的应用程序URL聪明的通道访问的一个或更多书签列表项，然后分配列表到DAP，组策略，或者本地用户策略您要提供聪明的通道访问。您能也列出自动化登录凭证提交在聪明的隧道连接的在无客户端SSL VPN会话的支持Web的应用程序。

本文假设，思科AnyConnect SSL VPN客户端配置已经被做并且适当地运作，以便聪明的通道功能在现有配置可以配置。关于如何配置思科AnyConnect SSL VPN客户端的更多信息，参考ASA 8.x

：在 ASA 上允许 AnyConnect VPN 客户端使用分割隧道的配置示例）。

参考配置一项聪明的通道通道策略关于如何与巧妙的通道一起配置分割隧道的更多信息。

注意： 确保*对4.I的步骤4.b*在ASA配置里描述使用*ASA 8.x的*ASDM 6.0(2)部分*：允许分割隧道ASA配置示例的AnyConnect VPN客户端没有*执行为了配置聪明的通道功能。

本文描述如何配置在Cisco ASA 5500系列自适应安全设备的巧妙的通道。

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Cisco ASA 5500系列自适应安全设备
- 运行Microsoft Vista、Windows XP SP2或者Windows 2000 Professional SP4以Microsoft安装程序版本3.1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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

聪明的通道访问配置

聪明的通道表显示聪明的通道列表，其中每一识别合格一个或更多的申请对聪明的通道访问和其相关的操作系统(OS)。由于每项组策略或本地用户策略支持一聪明的通道列表，您必须分组基于nonbrowser的应用程序支持到一聪明的通道列表。在列表的配置后，您能分配它到一个或更多组修正或本地用户策略。

注意： 关于聪明的隧道配置的更多信息，参考配置聪明的通道访问。

聪明的通道窗口(**Configuration>远程访问VPN >无客户端SSL VPN访问>门户>巧妙的通道**)允许您完成这些步骤：

- **添加一聪明的通道列表并且添加应用程序到列表**完成这些步骤为了添加一聪明的通道列表和添加应用程序到列表：单击 **Add**。添加巧妙的通道列表对话框出现。输入列表名称，然后单击 **Add**。ASDM打开添加巧妙的通道条目对话框，给您分配一个巧妙的通道属性对列表。在您为巧妙的通道后分配希望的属性，请点击OK键。ASDM显示在列表的那些属性。如所需要重复这些

步骤为了完成列表，然后点击OK键在添加巧妙的通道列表对话框内。
- **更改一聪明的通道列表**完成这些步骤为了更改一聪明的通道列表：在表里双击列表或选择列表，并且单击**编辑**。单击**添加**插入新的一套聪明的隧道属性到列表或选择在列表的一个条目，并且单击**编辑**或**删除**。
- **删除列表**为了删除列表，选择列表在表里，和点击**删除**。
- **添加一张书签**在一聪明的通道列表的配置和分配之后，您能使一个巧妙的通道易用通过添加服务的一张书签和单击在添加的**Enable (event)聪明的通道**选项或编辑书签对话框。

聪明的通道访问给客户端基于TCP的应用程序使用一基于浏览器的VPN连接连接到服务。它提供以下优点给用户，与插件和传统技术比较，端口转发：

- 聪明的通道提供比插件改善性能。
- 不同于端口转发，巧妙的通道简化用户体验由不要求本地应用程序的用户连接对本地端口。
- 不同于端口转发，巧妙的通道不要求用户有管理员权限。

聪明的通道需求、限制和限制

一般要求和限制

巧妙的通道有以下一般要求和限制：

- 产生巧妙的通道的远程主机必须运行Microsoft Windows Vista、Windows XP或者Windows 2000 32位版本;或者Mac OS 10.4或10.5。
- 巧妙的通道自动登录支持Windows的只有微软Internet Explorer。
- 必须启用浏览器与Java， Microsoft ActiveX或者两个。
- 巧妙的通道支持仅代理被放置在运行Microsoft Windows和安全工具的计算机之间。巧妙的通道使用Internet Explorer配置(即供在Windows的全系统的使用使用打算的那个)。如果远程计算机要求代理服务器到达安全工具，连接的终止的末端的URL必须在从代理服务排除的URL列表。如果代理配置指定为ASA注定的流量通过代理，所有聪明的隧道流量通过代理。在一个基于http的远程访问方案中，子网有时不提供用户访问对于VPN网关。在这种情况下，在ASA前面被放置的代理对路由流量在Web和最终用户的位置提供Web访问之间。然而，只有VPN用户能配置在ASA前面被放置的代理。当执行如此时，他们必须确保这些代理支持连接方法。对于需要验证的代理，巧妙的通道支持仅基本文摘认证类型。
- 当聪明通道开始，安全工具以隧道传输从浏览器进程的所有流量用户过去常常启动无客户端会话。如果用户开始浏览器进程的另一个实例，通过所有流量到通道。如果浏览器进程是相同的，并且安全工具不提供存取对于给的URL，用户不能打开它。作为应急方案，用户能使用从用于的那个的一个不同的浏览器建立无客户端会话。
- 有状态故障切换不保留聪明的隧道连接。用户必须在故障切换以后重新连接。

Windows需求和限制

以下需求和限制只适用于Windows ：

- 仅Winsock 2，基于TCP的应用程序有资格聪明的通道访问。
- 安全工具不支持Microsoft Outlook Exchange (MAPI)代理。端口转发和巧妙的通道不支持MAPI。对于Microsoft Outlook Exchange通信使用MAPI协议，远程用户必须使用AnyConnect。
- 使用聪明的通道或端口转发Microsoft Windows Vista的用户必须添加ASA的URL到可信的站点

区域。为了访问可信的站点区域，请开始Internet Explorer，并且选择**工具> Internet选项**，并且点击**安全选项卡**。Vista用户能也禁用已保护模式为了实现聪明的通道访问;然而，因为增加漏洞攻击，思科推荐此方法。

Mac OS需求和限制

这些需求和限制只适用于Mac OS ：

- Safari 3.1.1或以上或者Firefox 3.0或以上
- Sun JRE 1.5或以上
- 从入口页面开始的仅应用程序能建立聪明的隧道连接。此需求包括Firefox的聪明的通道支持。使用Firefox开始Firefox另一个实例在一个巧妙的通道的第一次使用期间要求名为csco_st的用户配置文件。如果此用户配置文件不存在，会话提示用户创建一。
- 与SSL库动态地连接的应用程序使用TCP能在一个巧妙的通道工作。
- 巧妙的通道不支持这些功能和应用程序在Mac OS ：代理服务自动登录使用两层的名称空间的应用程序基于控制台的应用程序，例如Telnet、SSH和卷毛应用程序使用dlopen或dlsym找出libsocket呼叫静态连接的应用程序找出libsocket呼叫

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

添加或编辑聪明的通道列表

添加巧妙的通道列表对话框让您添加聪明的通道条目列表到安全工具配置。编辑巧妙的通道列表对话框让您修改列表的内容。

字段

列表名—输入一唯一的名称对于应用列表或程序。没有在字符数量的限制在名称的。请勿使用空间。在聪明的通道列表的配置后，列表名在无客户端SSL VPN组策略和本地用户策略的聪明的通道列表属性旁边出现。分配将帮助您与其他列表区分其内容或目的名称您可能配置。

添加或编辑聪明的通道条目

添加或编辑巧妙的通道条目对话框让您指定一应用程序的属性在一聪明的通道列表的。

- **申请ID** —输入字符串命名条目在聪明的通道列表。字符串为OS是唯一。一般，它命名应用程序授权聪明的通道访问。为了支持您选择指定不同的路径或Hash值应用程序的多个版本，您能使用此属性区分条目，指定OS和每列表项支持的应用程序的名称和版本。字符串可以是64个字符。
- **进程名**—输入文件名或路径对应用程序。字符串可以是128个字符Windows要求此值完全匹配对应用程序路径的右侧远程主机的合格对聪明的通道访问的申请。如果指定仅文件名对于Windows， SSL VPN不强制执行在远程主机的一位置限制合格对聪明的通道访问的申请。如果指定路径，并且用户在另一个位置安装应用程序，该应用程序不合格。应用程序在所有路径能驻留，只要字符串匹配的右侧您输入的值。为了授权对聪明的通道访问的申请，如果是存在远

程主机的几个路径之一，或者请在此字段指定应用程序的仅名称和分机或请创建每个路径的一个唯一聪明的通道条目。对于Windows，如果想要对从prompt命令开始的应用程序的添加聪明的通道访问，您必须指定“cmd.exe”在一个条目进程名在聪明的通道列表的和指定路径到在另一个条目的应用程序，因为“cmd.exe”是应用程序的parent。Mac OS要求完整路径对进程并且区分大小写。为了避免指定每个用户名的一个路径，请插入代字号(|)在部分路径前(例如，~/bin/vnc)。

- **OS** —点击Windows或Mac为了指定应用程序的主机OS。
- **哈希**— (*可选和仅可适用对于Windows*)为了得到此值，请输入可执行文件的校验和到使用SHA-1算法，计算哈希的工具。这样工具一示例是Microsoft文件校验和完整性检验器(FCIV)，是可用的在http://support.microsoft.com/kb/841290/ 。在安装FCIV以后，请放置应用程序的临时拷贝被切细在例如不包含空间的路径(c ：/fciv.exe)，然后输入fciv.exe -sha1应用程序在line命令(例如， fciv.exe -sha1 c:\msimn.exe)显示SHA-1哈希。SHA-1哈希总是40十六进制字符。在授权对聪明的通道访问的申请前，无客户端SSL VPN计算匹配申请ID的应用程序的哈希。如果结果匹配值哈希，它合格对聪明的通道访问的申请。输入哈希提供一个合理的保证SSL VPN不合格匹配字符串您在申请ID指定的一个非法文件。由于校验和变化与应用程序的每版本或补丁程序，您进入的哈希能只匹配一版本或补丁程序在远程主机。为了指定超过应用程序的一个版本的一哈希，请创建每个Hash值的一个唯一聪明的通道条目。**注意：** 您必须在将来更新聪明的通道列表，如果输入Hash值，并且要支持一应用程序的未来版本或补丁程序与聪明的通道访问的。与聪明的通道访问的一突然的问题也许是征兆包含Hash值的应用程序不是最新与应用升级。您能通过不输入哈希避免此问题。
- 一旦配置聪明的通道列表，您必须分配它到组策略或本地用户策略为了它能变为活动如下：为了分配列表到组策略，选择**设置>远程访问VPN>无客户端SSL VPN访问>组策略>Add或编辑>门户**和从下拉列表选择聪明的通道名称在聪明的通道列表属性旁边。为了分配列表到本地用户策略，选择**设置的设置>远程访问VPN> AAA >本地用户>Add或编辑> VPN策略>无客户端SSL VPN**和从下拉列表选择聪明的通道名称在聪明的通道列表属性旁边。

ASA聪明的通道(Lotus示例)配置使用ASDM 6.0(2)

本文假设，基本配置，例如接口配置，完成并且适当地运作。

注意： 要使 ASDM 可配置 ASA，请参阅允许 ASDM 进行 HTTPS 访问。

注意： 除非更换端口号，否则无法在同一 ASA 接口上启用 WebVPN 和 ASDM。有关详细信息，请参阅在相同 ASA 接口上同时启用 Webvpn 和 ASDM。

完成这些步骤为了配置一个巧妙的通道：

注意： 在本例中配置示例，巧妙的通道为Lotus应用程序配置。

1. 选择**Configuration>远程访问VPN >无客户端SSL VPN访问>门户>巧妙的通道**为了开始聪明的隧道配置。
2. 单击 **Add**。添加巧妙的通道列表对话框出现。
3. 在添加巧妙的通道列表对话框中，请单击**添加**。添加巧妙的通道条目对话框出现。
4. 在申请ID字段，请输入字符串识别在聪明的通道列表内的条目。
5. 输入文件名和扩展名应用程序的，并且点击OK键。
6. 在添加巧妙的通道列表对话框中，请点击OK键。**注意：** 以下是等效的 CLI 配置命令：
7. 分配列表到您要提供对相关的应用程序的聪明的通道访问的组策略和本地用户策略如下：为了分配列表到组策略，选择**Configuration>远程访问VPN>无客户端SSL VPN访问>组策略**，和单击**添加**或**编辑。**此时出现 Add Internal Group Policy 对话框。

8. 在添加内部组策略对话框中，请点击**门户**，从聪明的通道列表下拉列表选择聪明的通道名称，并且点击OK键。**注意：** 此示例使用*Lotus*作为聪明的通道列表名。
9. 为了分配列表到本地用户策略，选择**Configuration>远程访问VPN> AAA请设置>本地用户**，并且单击**添加**配置配置新用户或单击**编辑**编辑一个现有用户。编辑用户帐户对话框出现。
10. 在编辑用户帐户对话框中，请点击**无客户端SSL VPN**，从聪明的通道列表下拉列表选择聪明的通道名称，并且点击OK键。**注意：** 此示例使用*Lotus*作为聪明的通道列表名。

聪明的隧道配置完成。

故障排除

我无法连接使用按书签的聪明的通道URL在无客户端门户。此问题为什么出现，并且如何能解决它？

此问题发生由于在Cisco Bug ID描述的问题CSCsx05766 (仅限注册用户)。为了解决此问题，请降级Java运行时插件对早版本。

能否错误在WebVPN配置的聪明的通道链路的URL ？

当巧妙的通道在ASA时使用，您不能错误URL或隐藏浏览器的地址栏。用户能查看在WebVPN配置的链路URL该使用巧妙的通道。结果，他们能更换端口和访问某些其他服务的服务器。

为了解决此问题，请使用WebType ACL。参考创建WebType ACL欲知更多信息。

相关信息

- Cisco ASA 5500 系列自适应安全设备
- AnyConnect VPN客户端的版本注释，版本2.3
- 在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例
- 技术支持和文档 - Cisco Systems