PIX/ASA：IPsec VPN 客户端自动更新功能配置示例

目录

简介

本文档介绍如何在 Cisco ASA 5500 系列自适应安全设备和 Cisco PIX 500 系列安全设备上配置 Cisco VPN Client 自动更新功能。

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 7.x 及更高版本的 Cisco ASA 5500 系列自适应安全设备
- 运行版本 7.x 及更高版本的 Cisco PIX 500 系列安全设备
- Cisco Adaptive Security Device Manager (ASDM)版本5.x和以上
- Cisco VPN Client 4.x 及更高版本

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。

如何使用 CLI 配置 Windows 的客户端更新

客户端更新功能让位于中心位置的管理员可以自动通知 VPN 客户端用户存在 VPN 客户端软件和 VPN 3002 硬件客户端镜像的更新。

在隧道组 ipsec 属性配置模式中发出 **client-update** 命令以配置客户端更新。如果客户端运行的软件版本位于修订版号列表中，则不需要更新其软件。如果客户端运行的软件版本不在此列表中，则应进行更新。您可以指定最多四个客户端更新条目。

命令语法如下：

client-update type *type* {url *url-string*} {rev-nums *rev-nums*} no client-update *[type]*

- **rev-nums** rev-nums — 指定此客户端的软件或固件镜像。最多可输入四个（使用逗号分隔）。
- *type* — 指定要通知客户端更新的操作系统。操作系统列表包括以下条目：Microsoft Windows：所有基于 Windows 的平台Win9X：Windows 95、Windows 98 和 Windows ME 平台Winnt ：Windows NT 4.0、Windows 2000 和 Windows XP 平台vpn3002：VPN 3002 硬件客户端
- **url** url-string — 指定软件/固件镜像的 URL。此 URL 必须指向相应于客户端的文件。

以下示例配置一个名为 remotegrp 的远程访问隧道组的客户端更新参数。它指定了修订版号 4.6.1 以及用于检索更新的 URL，即 https://support/updates。

ASA
hostname(config)#**tunnel-group remotegrp type ipsec_ra** hostname(config)#**tunnel-group remotegrp ipsec-attributes** hostname(config-ipsec)#**client-update type windows url https://support/updates/rev-nums 4.6.1**

如何使用 ASDM 配置 Windows 的客户端更新

本文档假设基本配置（例如接口配置）已完成并且可以正常工作。

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

ASDM 包含两种客户端更新：一种通过隧道组支持 Windows 客户端和 VPN 3002 硬件客户端，另一种支持将 ASA 设备作为自动更新服务器。

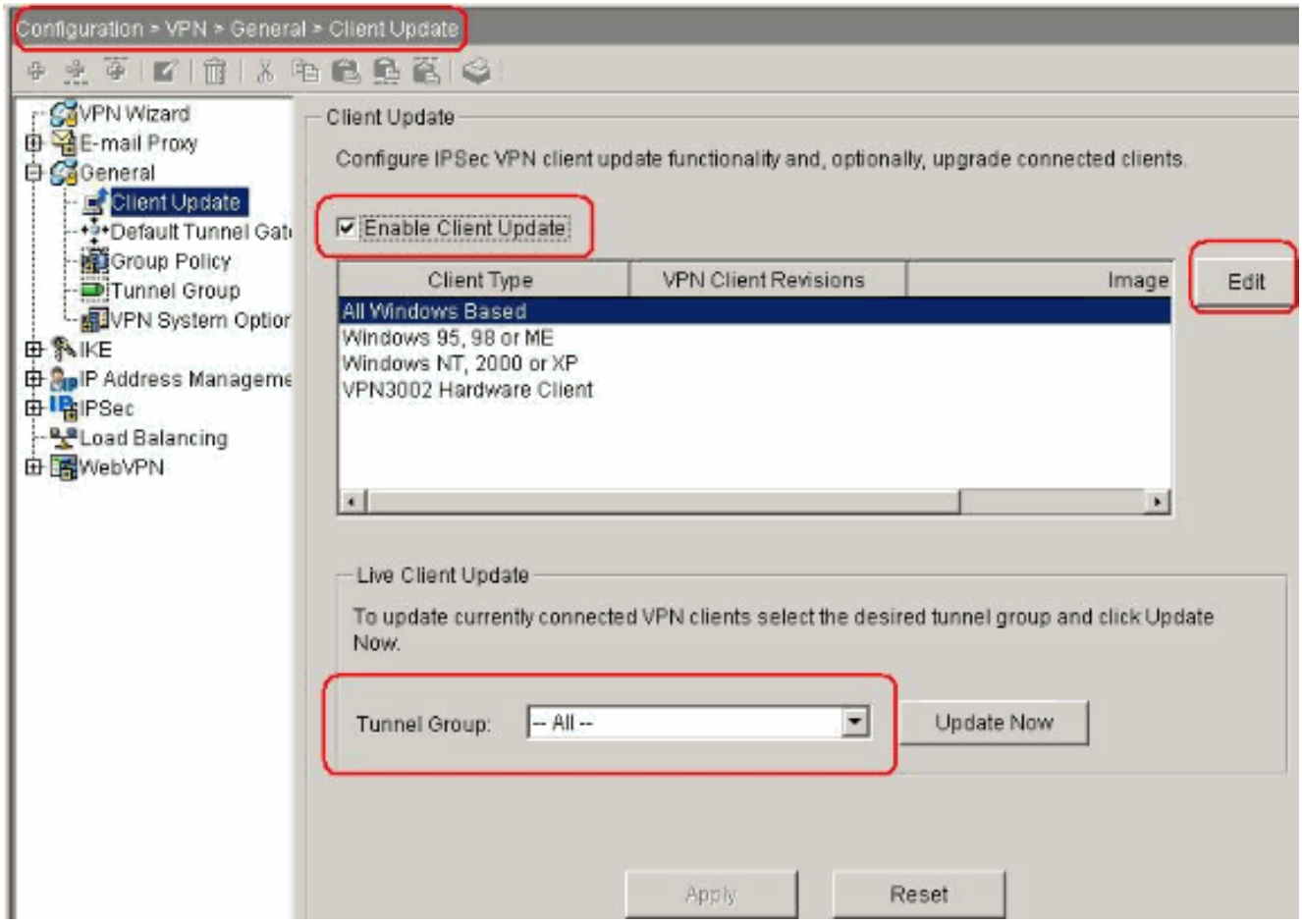
远程用户可以使用过期的 VPN 软件或硬件客户端版本。您可在任何时间执行客户端更新以实现下列功能：

- 启用更新客户端版本。
- 指定要应用更新的客户端类型和修订版号。
- 提供用于获取更新的 URL 或 IP 地址。
- 选择是否通知 Windows 客户端用户应更新其 VPN 客户端版本。
- 对于 Windows 客户端，您可以为用户提供一种完成更新的机制。
- 对于 VPN 3002 硬件客户端用户，将自动进行更新而不会通知。

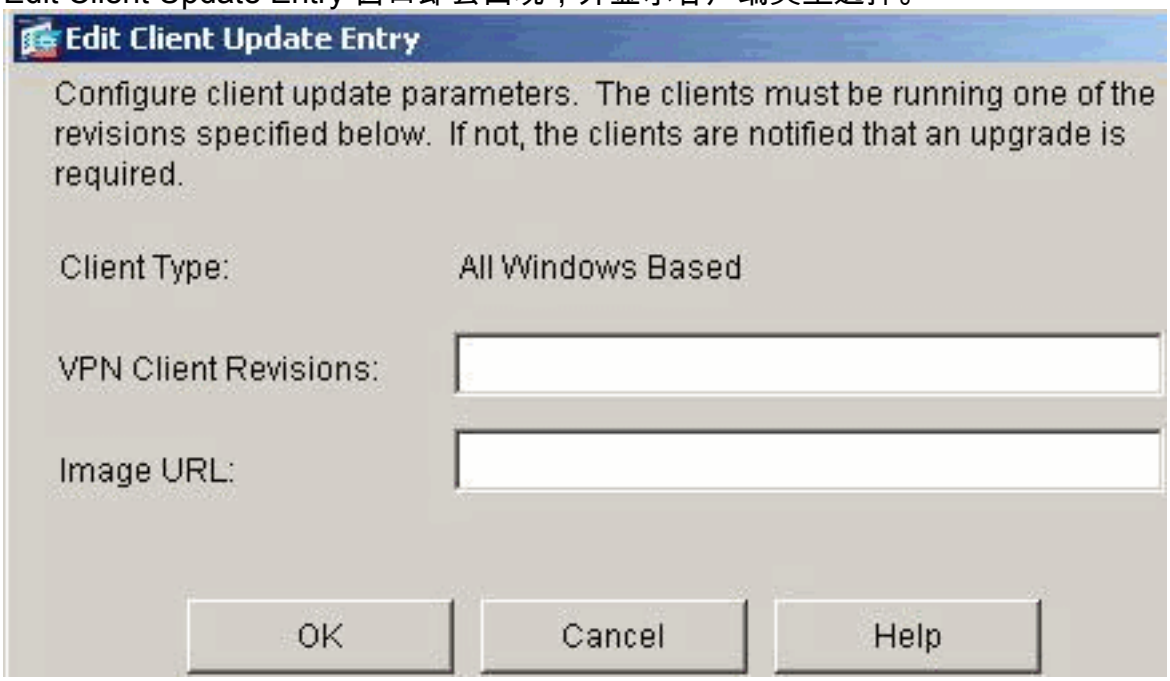
执行以下步骤以配置客户端更新：

1. 选择 **Configuration > VPN > General > Client Update** 以转至客户端更新窗口。客户端更新窗口即会打开。选中 **Enable Client Update** 复选框以启用客户端更新。选择要应用客户端更新的

客户端类型。可用的客户端类型有 **All Windows-Based、Windows 95, 98 or ME、Windows NT 4.0, 2000 or XP 以及 VPN 3002 Hardware Client**。如果客户端运行的软件版本位于修订版号列表中，则不需要更新其软件。如果客户端运行的软件版本不在此列表中，则应进行更新。您最多可以指定其中三种客户端更新条目。选择 All Windows Based 包括所有可用的 Windows 平台。如果选择此项，则不要指定其他 Windows 客户端类型。单击 **Edit** 以指定用于客户端更新的更新软件或固件镜像的可接受客户端版本和来源。

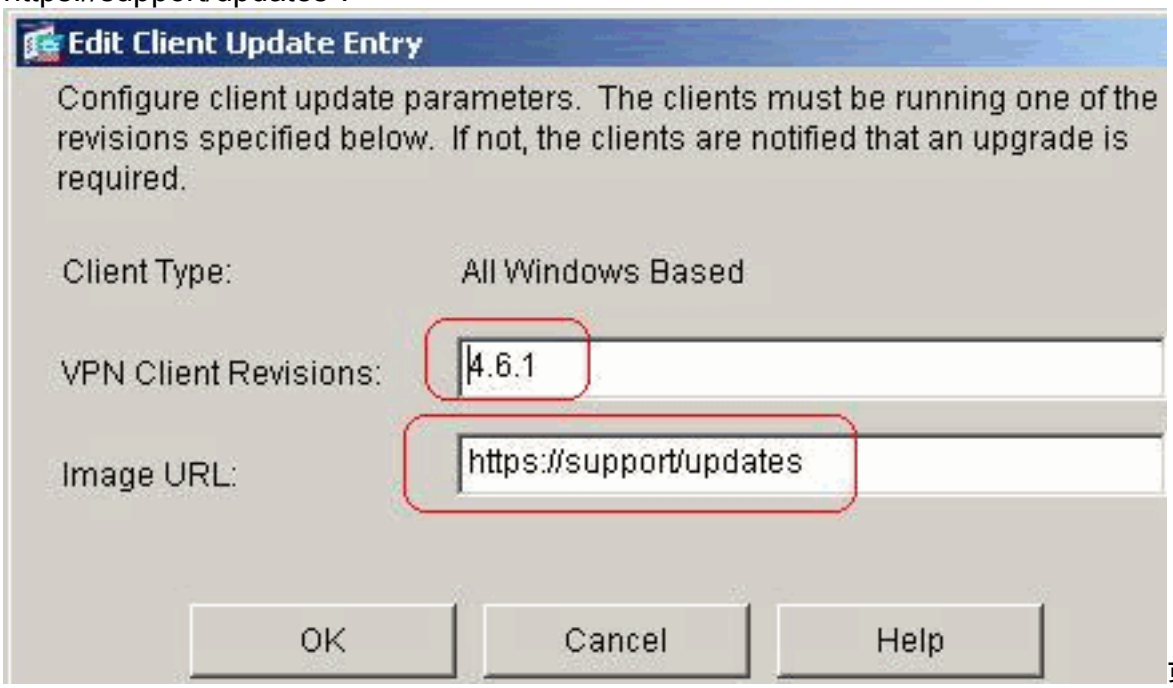


2. Edit Client Update Entry 窗口即会出现，并显示客户端类型选择。



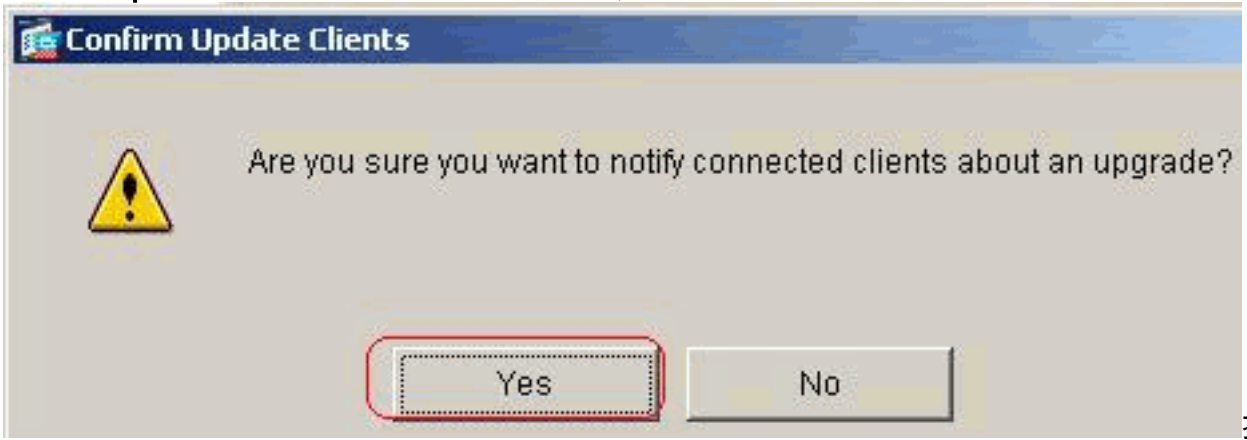
3. 指定要应用于整个安全设备中的选定类型的所有客户端的客户端更新。即指定客户端类型、更新镜像所在的 URL 或 IP 地址，以及该客户端可接受的修订版号或编号。您最多可以指定四个修订版号（使用逗号分隔）。单击 **OK** 后，您的条目将会出现在 Client Upgrade 窗口的相应表

列中。如果客户端修订版号匹配其中一个指定的修订版号，则不需要更新客户端。**注意：** 对于所有 Windows 客户端，您必须使用协议 http:// 或 https:// 作为 URL 前缀。对于VPN 3002硬件客户端，您必须指定协议tftp://。它将为远程访问隧道组中版本号早于 4.6.1 的所有 Windows 客户端启动客户端更新，并将用于检索更新的 URL 指定为 https://support/updates：



或者，您也可以为单独的客户端类型而非所有 Windows 客户端配置客户端更新，您可以在步骤 1-c 看到这些类型。VPN3002 客户端更新无需用户干预，用户不会收到任何通知消息。如果您在 URL 末尾包含应用程序名称，则可以让浏览器自动运行此应用程序；例如：**https://support/updates/vpnclient.exe。**

4. 或者，您可以选择向需要更新其客户端的具有过期 Windows 客户端的活动用户发送通知。请使用 Client Update 窗口的 Live Client Update 区域以发送此通知。选择隧道组（或 All），然后单击 **Update Now**。即会出现一个对话框，并要求您确认要通知已连接的客户端进行升级。



指定用户将会看到一个弹出窗口，在此窗口中可以启动浏览器并从 URL 指定的站点中下载更新软件。此消息中唯一可配置的部分是 URL。（请参阅步骤 1-b 或 1-c。）非活动用户将会在下次登录时收到通知消息。您可以将此通知发送给所有隧道组的所有活动客户端，或者将其发送给特定隧道组的客户端。如果客户端修订版号匹配其中一个指定的修订版号，则不需要更新客户端，并且不会向用户发送任何通知消息。VPN3002 客户端更新无需用户干预，用户不会收到任何通知消息。

验证

当前没有可用于此配置的验证过程。

相关信息

- 技术支持和文档 - Cisco Systems