RV016、RV042、RV042G和RV082 VPN路由器上的常规防火墙设置

目标

防火墙可保护内部网络免受外部网络（例如Internet）的攻击。防火墙对网络安全至关重要。根据您的安全需求，有多种不同的设置可以启用或禁用特定服务。

本文的目的是显示如何在RV016、RV042、RV042G和RV082 VPN路由器上启用或禁用常规防火墙设置。

适用设备

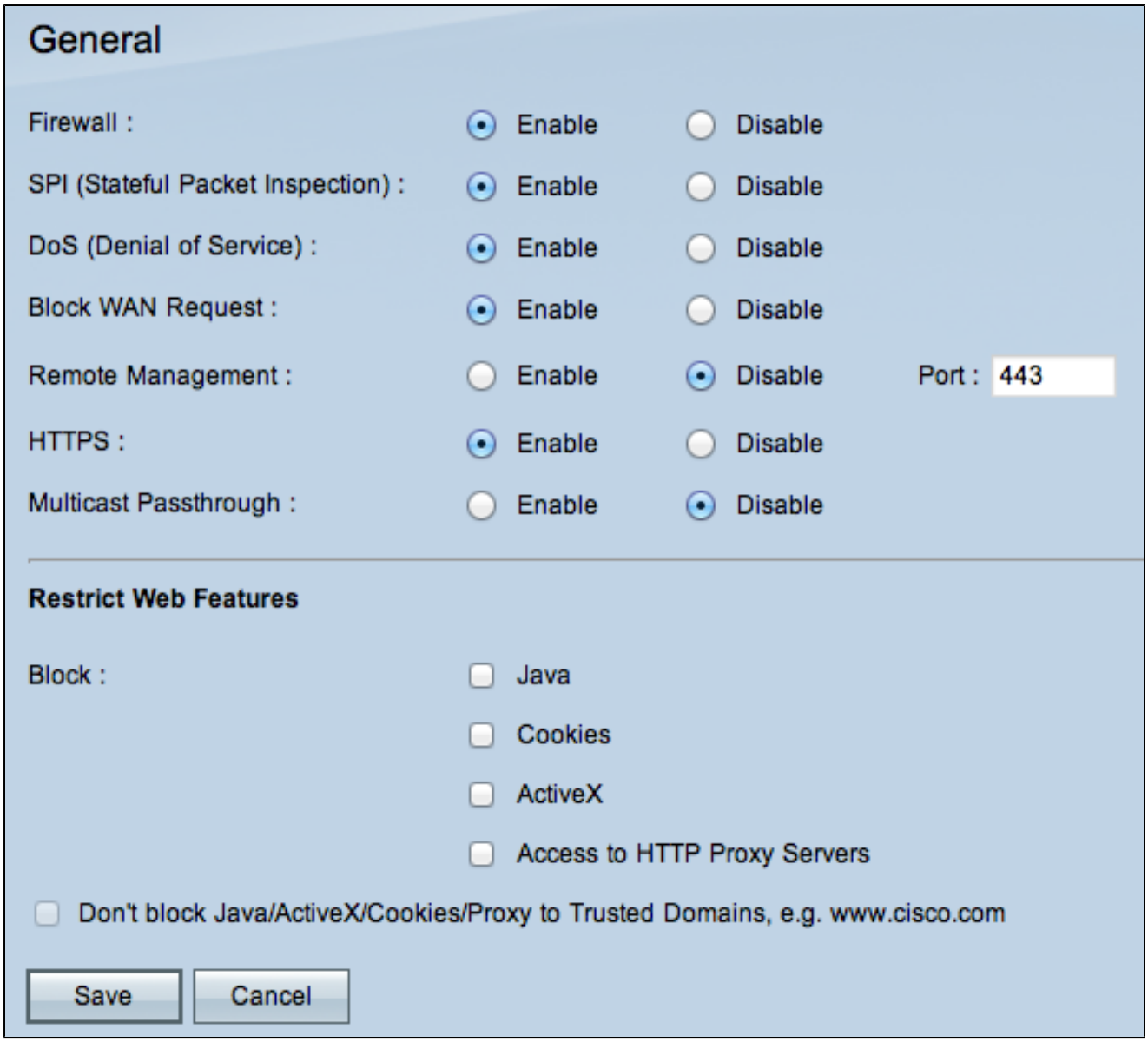
- RV016
- RV042
· RV042G
- RV082

软件版本

•v4.2.1.02

常规防火墙设置

步骤1:登录路由器配置实用程序并选择Firewall > General。将打开General页面：



第二步：单击Enable或Disable单选按钮，根据用户要求启用或禁用防火墙中的可用设置。

以下字段说明如下：

·防火墙 — 启用此功能后，路由器将对通过此路由器的所有流量执行深度数据包检测，并丢弃不符合预定义协议行为的数据包。

· SPI（状态数据包检测） — 路由器的防火墙使用状态数据包检测(SPI)来检查防火墙上的流量。它监控网络连接状态，例如TCP数据流和UDP通信。 防火墙会区分不同连接类型的合法数据包，并且防火墙仅允许与已知活动连接匹配的数据包，而拒绝所有其他数据包。

· Dos（拒绝服务） — 启用此功能后，路由器将阻止来自Internet的DOS（拒绝服务）攻击。DOS攻击会导致路由器的CPU繁忙，因此无法为常规流量提供服务。

·阻止WAN请求 — 启用此选项后，路由器将忽略来自Internet的PING请求，因此它看起来是隐藏的。这有助于通过隐藏网络端口提供安全性，从而使主动变更者无法轻松访问网络。

·远程管理 — 启用此功能后，路由器允许从Internet访问Web配置实用程序。输入将打开给WAN端主机的端口号。默认设置为443。用户建立远程连接时必须指定此端口。

· HTTPS — 启用时，可以从WAN端通过HTTPS会话而不是常规HTTP访问Web配置实用程序。这将使您的远程Web会话受SSL加密算法保护。如果禁用HTTPS功能，则用户无法通过使用QuickVPN进行连接。如果禁用，则使用安全性较低的HTTP连接。

·组播直通 — 如果路由器上当前运行的是IGMP代理，当启用组播直通时，路由器将允许IP组播流量从互联网进入。

注意：要禁用防火墙，必须将管理员密码从默认值更改为其他值。SPI（状态数据包检测）、DoS（拒绝服务）、Block WAN Request和Remote Management字段呈灰色显示。

第三步：在Restrict Web Features区域中，选中任意或所有复选框以限制相应功能。

· Java - Java是网站的编程语言。要阻止Java，请选中Java复选框。 如果拒绝Java，则可能无法访问用此编程语言编写的Internet站点，因此，如果连接到路由器的设备不需要访问使用Java创建的网站，则继续访问并阻止Java小程序是安全的。 另一方面，网络犯罪分子使用Java作为其攻击的一部分，即在访问受恶意软件感染的网站时确定操作系统并发起操作系统指定的攻击。例如，当您访问被黑客入侵的网站时，会触发一个JAR（Java存档）文件，要求您执行它的功能，但会秘密地用它来确定计算机的操作系统。

· Cookie - Cookie是存储在PC上、供Internet站点在用户与其进行交互时使用的数据。要阻止Cookie，请选中Cookie复选框。如果您希望阻止cookie，则网站在从设备访问时无法保存任何先前的访问信息。优点是不保存恶意cookie（第三方跟踪cookie），这会带来安全风险。

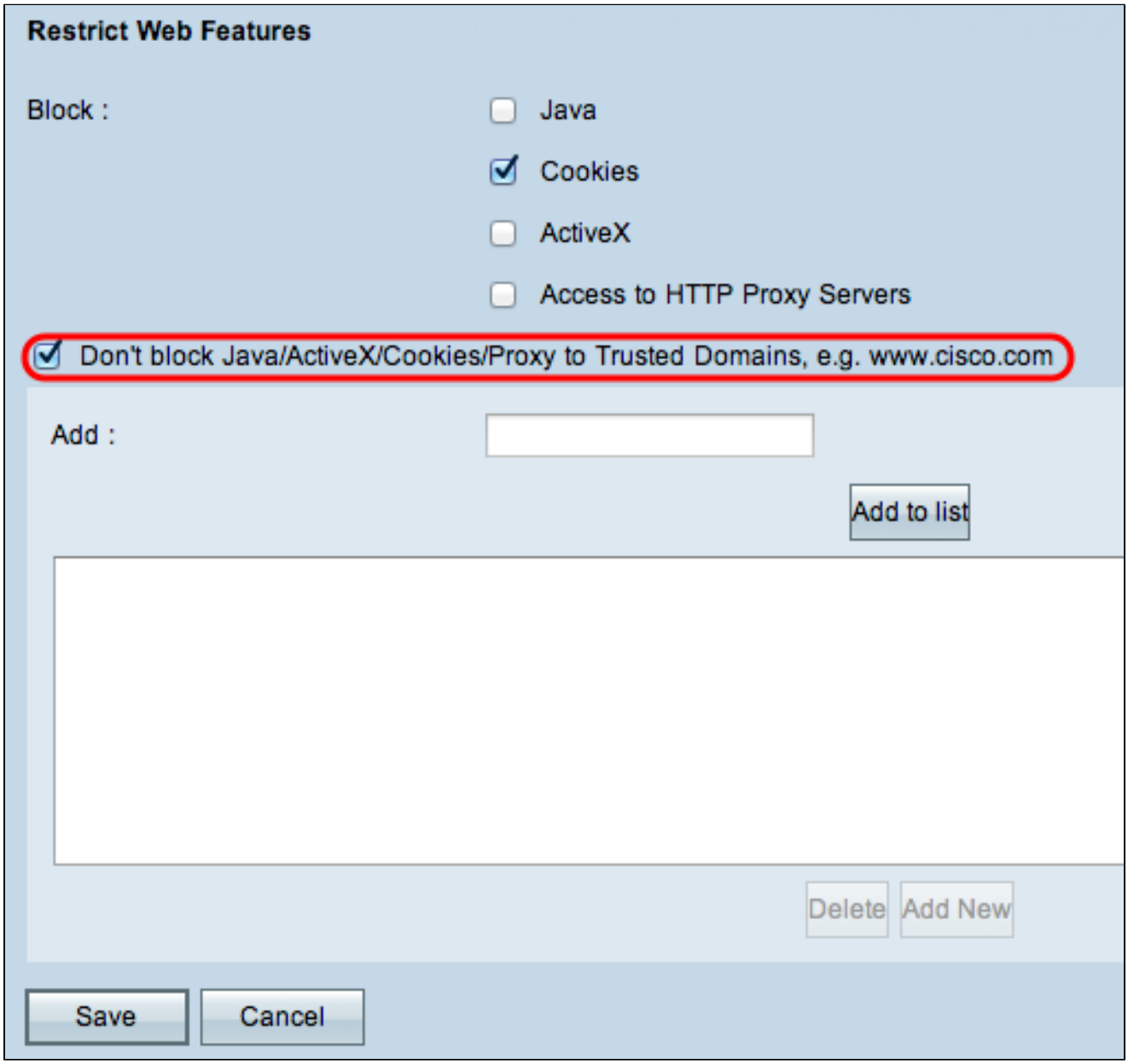
· ActiveX - ActiveX是Microsoft Windows的一个软件组件，可用于开发应用程序或控制小型程序，如在Internet站点上使用的加载项。如果允许ActiveX，它有助于改善浏览时的体验；它允许网站运行动画和其他类似程序。另一方面，如果访问包含网络犯罪分子开发的恶意ActiveX软件的网页，则可能会造成计算机损坏，因而存在潜在风险。要阻止ActiveX，请选中ActiveX复选框。如果阻止ActiveX，则当您希望访问某些使用ActiveX执行的Internet站点时，可能会出现问题。

·访问代理HTTP服务器 — 如果您希望匿名通过代理服务器进行冲浪并拒绝对代理服务器的访问，请选中访问代理HTTP服务器复选框。HTTP代理服务器对黑客隐藏最终用户的详细信息。他们充当中间人，因此您不能直接访问Internet。但是，如果本地用户能够访问WAN代理服务器，他们或许能够找到一种方法来绕过路由器上的内容过滤器，并访问路由器阻止的Internet站点。

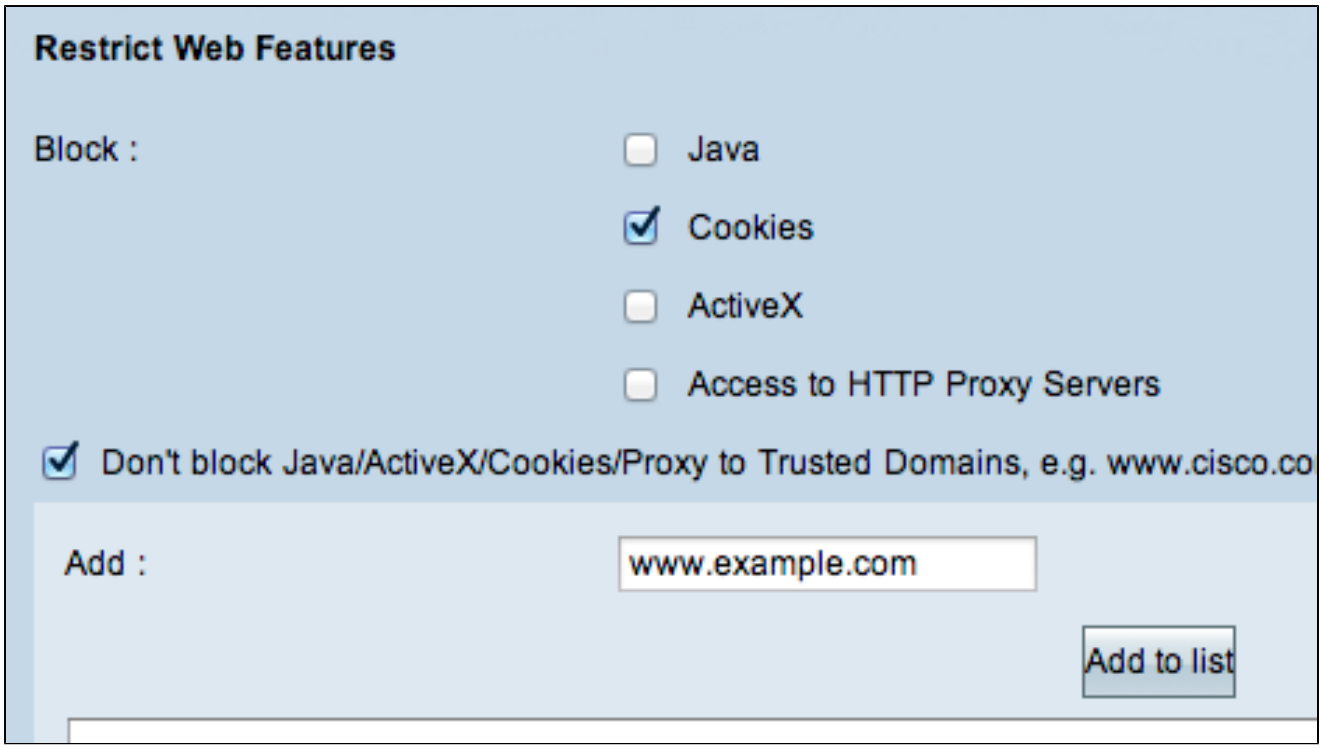
第四步：单击Save以保存设置。

添加受信任域

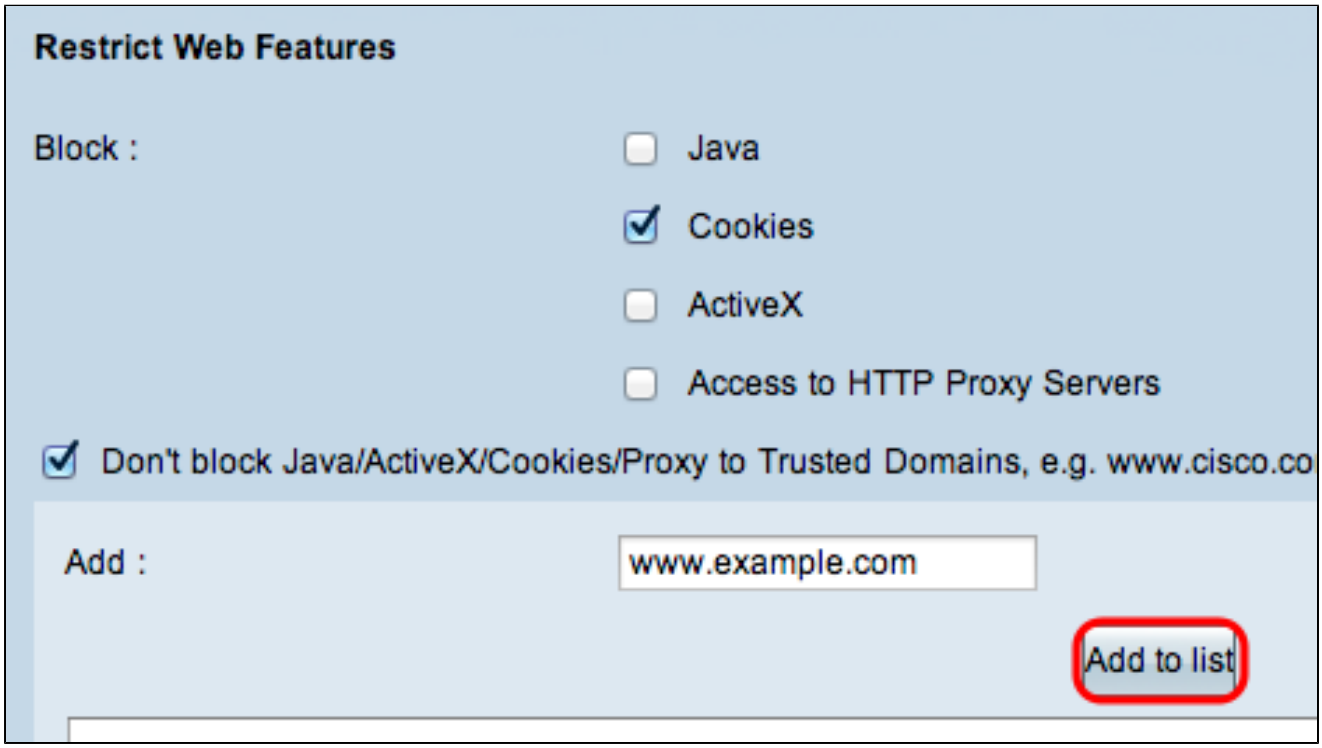
即使其中一个Web功能可能被阻止，用户也可以允许为指定的受信任域启用这些功能。



步骤1:选中Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains按钮。仅当用户在General Firewall Settings的第3步中选择阻止任何Web功能时，此选项才可用。



第二步：在添加字段中，输入要添加到受信任域列表的域。

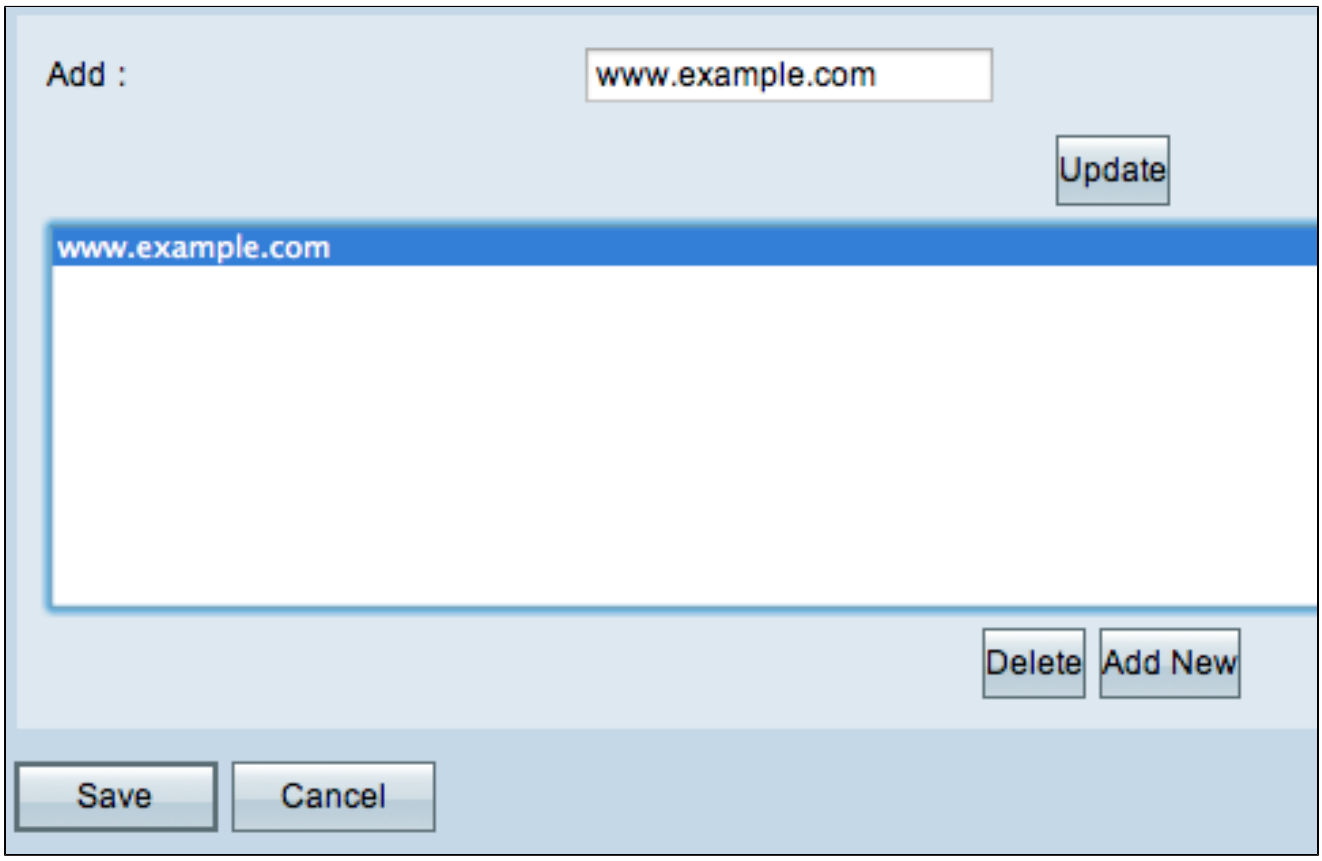


第三步：单击Add to list。域将添加到受信任列表。

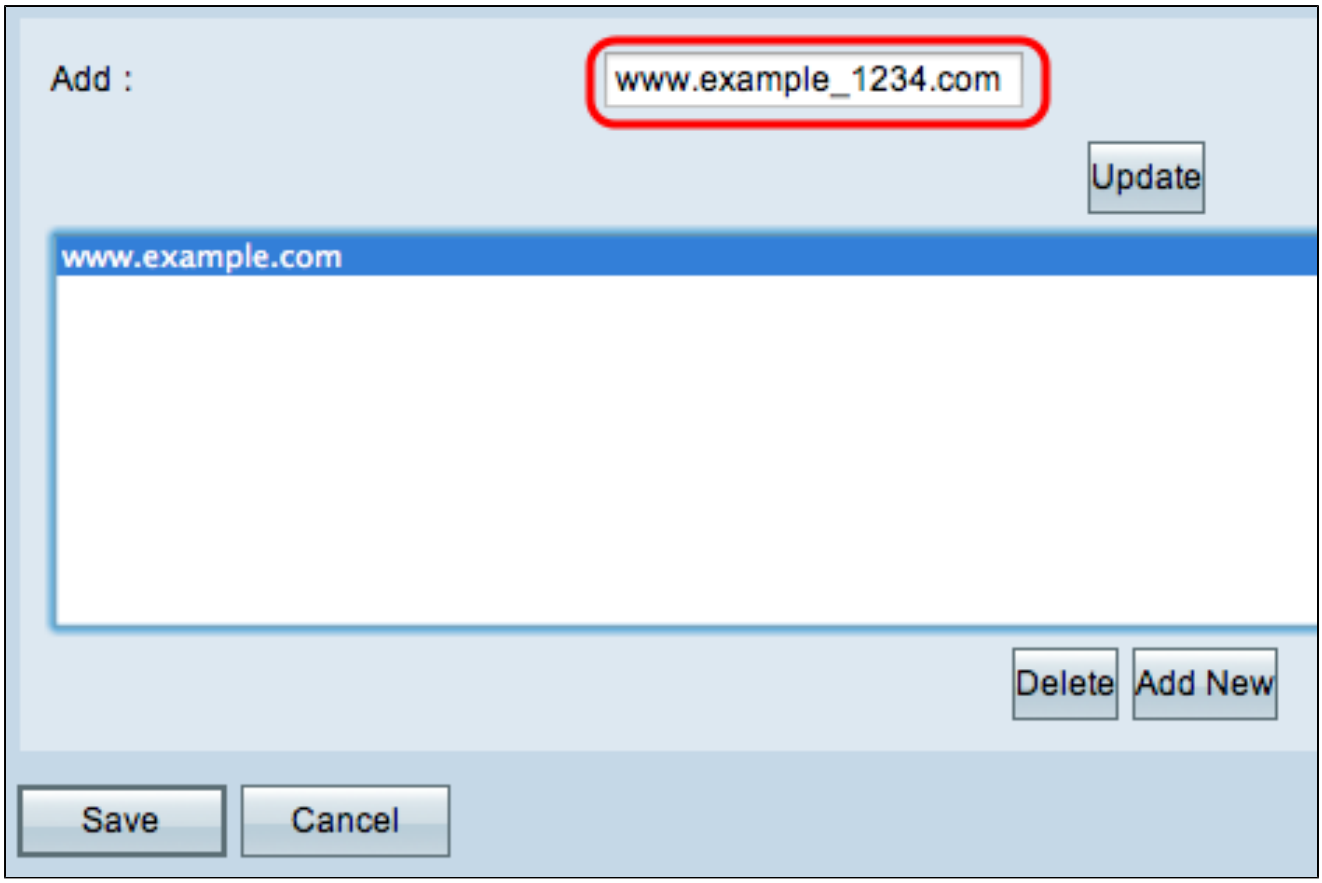
第四步：单击Save保存更改。

更新受信任域

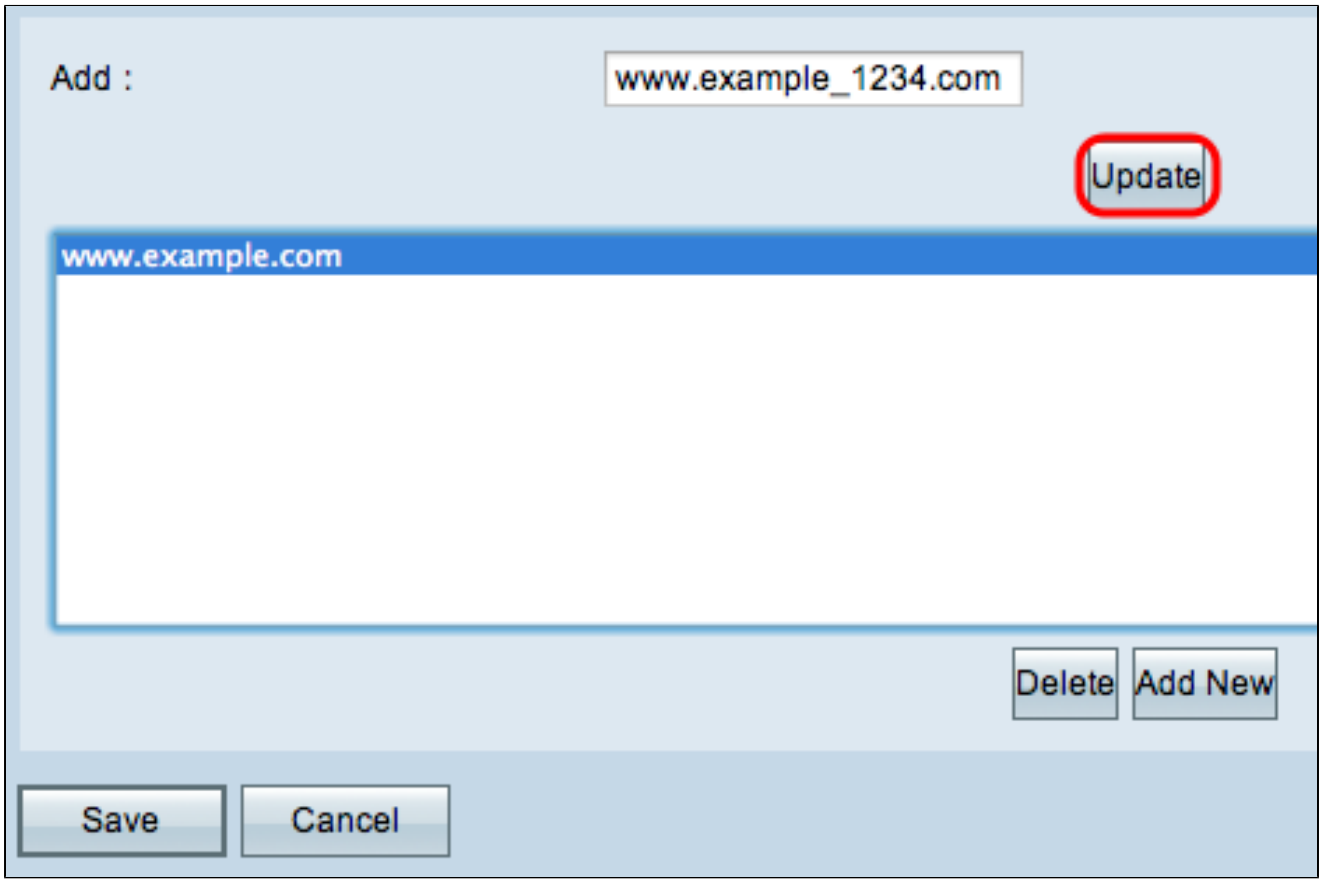
本节指导用户如何编辑受信任域。



步骤1:从受信任域列表中选择要编辑的域。



第二步：在添加字段中，输入所需域的更新域名。

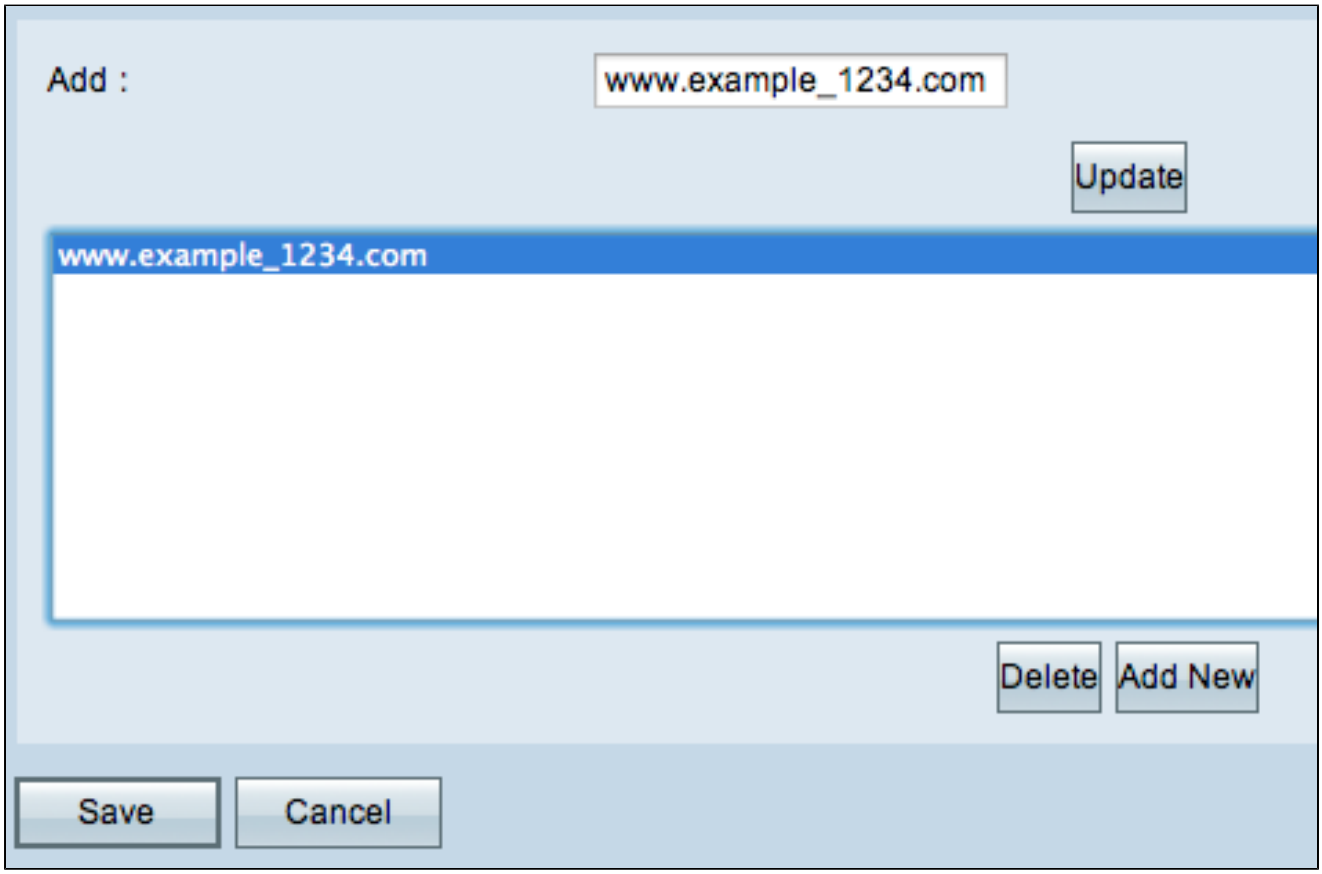


第三步：单击更新。

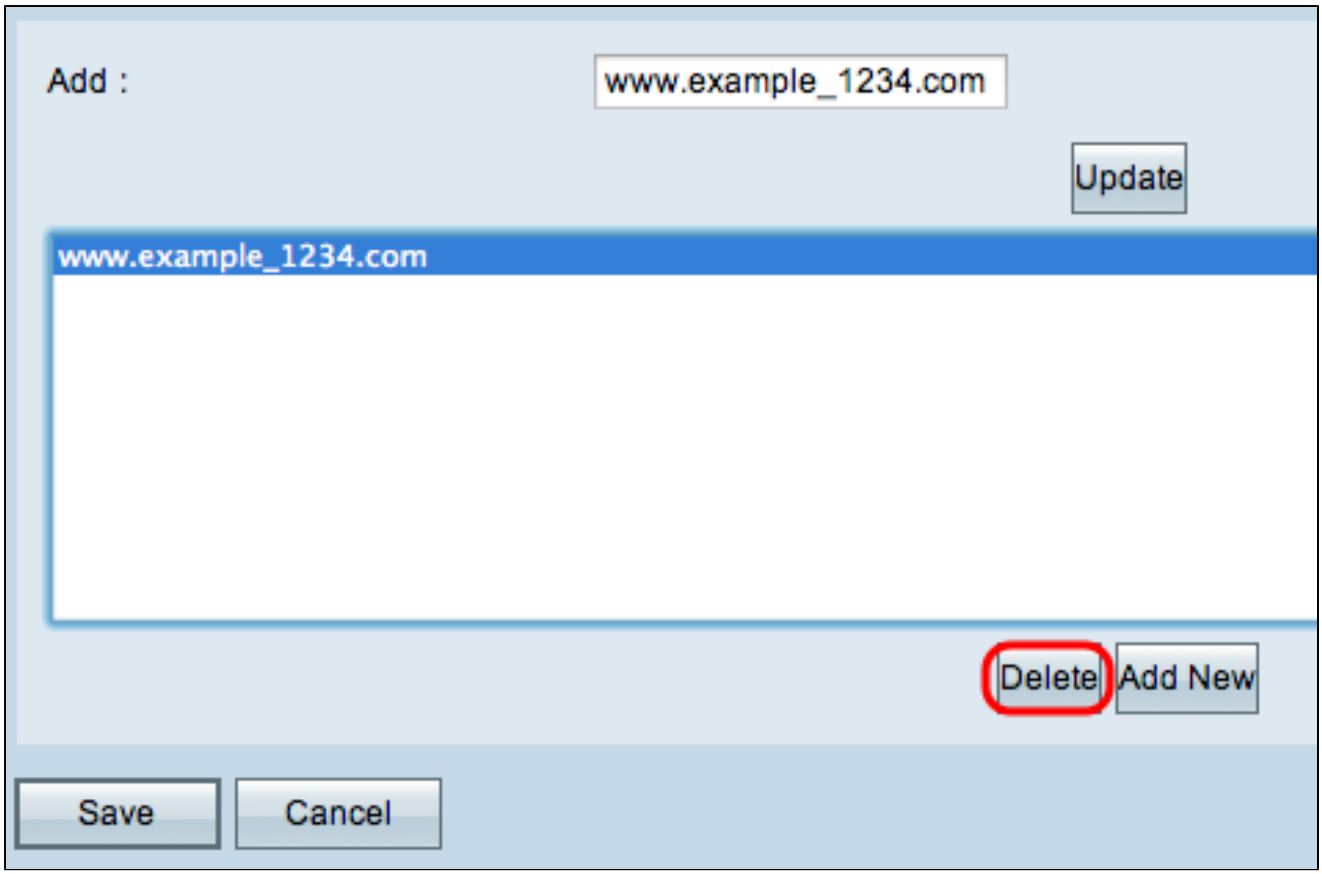
第四步：单击Save保存更改。

删除受信任域

本节指导用户如何删除受信任域。



步骤1:选择要删除的域。



第二步：单击删除。域删除成功。

第三步：单击Save保存更改。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。