Allgemeine Firewall-Einstellungen der VPN-Router RV016, RV042, RV042G und RV082

Ziel

Eine Firewall schützt ein internes Netzwerk vor einem externen Netzwerk wie dem Internet. Firewalls sind für die Netzwerksicherheit unverzichtbar. Es stehen verschiedene Einstellungen zur Verfügung, mit denen Sie bestimmte Dienste je nach Ihren Sicherheitsanforderungen aktivieren oder deaktivieren können.

In diesem Artikel wird erläutert, wie Sie allgemeine Firewall-Einstellungen auf RV016-, RV042-, RV042G- und RV082-VPN-Routern aktivieren oder deaktivieren.

Unterstützte Geräte

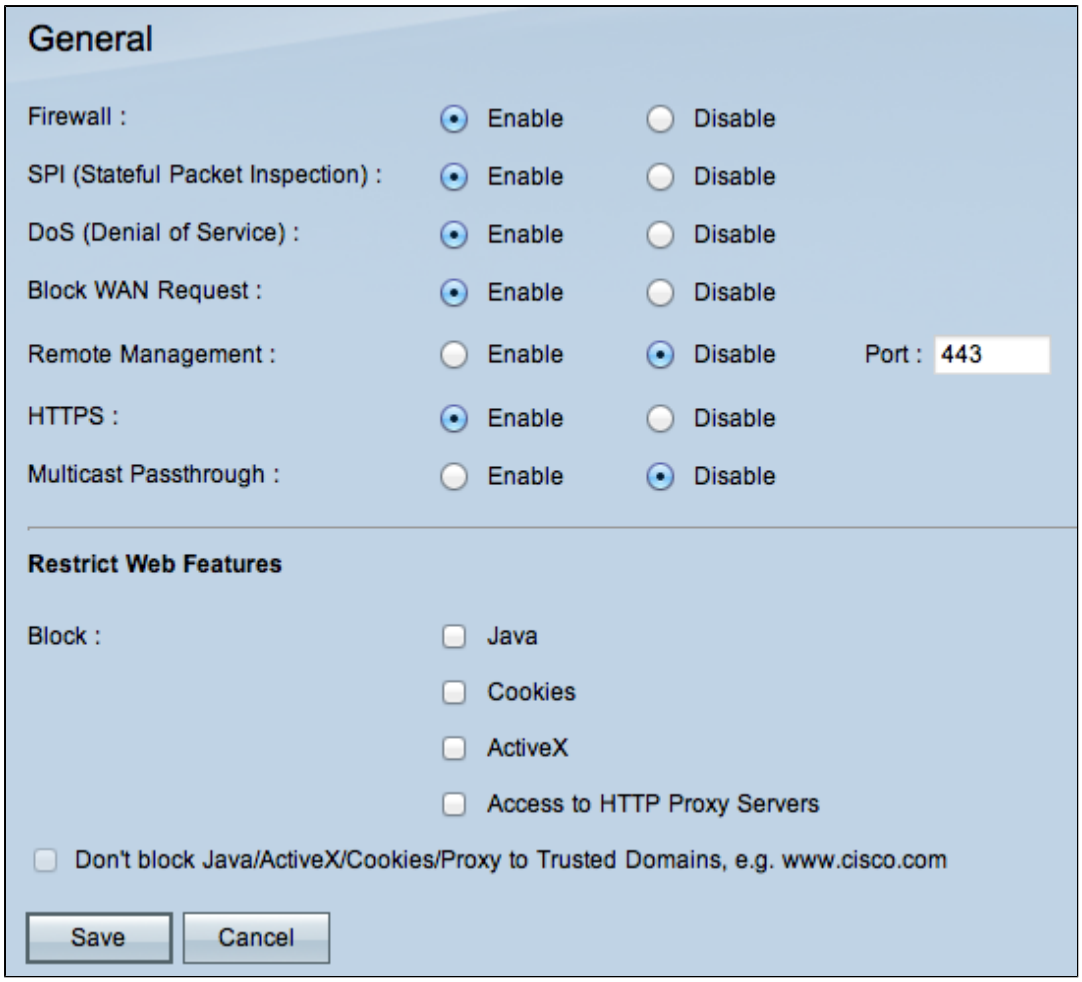
RV016
â€¢RV042
ãƒ» RV042G
RV082

Software-Version

ãƒ» v4.2.1.02

Allgemeine Firewall-Einstellungen

Schritt 1: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **Firewall > General (Firewall > Allgemein)**. Die Seite *Allgemein* wird geöffnet:



Schritt 2: Klicken Sie auf das Optionsfeld **Aktivieren** oder **Deaktivieren**, um die in der Firewall verfügbaren Einstellungen je nach Benutzeranforderungen zu aktivieren oder zu deaktivieren.

Die folgenden Felder werden wie folgt beschrieben:

ãƒ» Firewall - Wenn diese Funktion aktiviert ist, führt der Router Deep Packet Inspection für den gesamten Datenverkehr durch diesen Router durch und verwirft die Pakete, die nicht dem vordefinierten Protokollverhalten folgen.

ãƒ» SPI (Stateful Packet Inspection) - Die Firewall des Routers verwendet Stateful Packet Inspection (SPI), um den Datenverkehr an der Firewall zu überprüfen. Es überwacht den Status von Netzwerkverbindungen wie TCP-Streams und UDP-Kommunikation. Die Firewall unterscheidet legitime Pakete von verschiedenen Verbindungstypen, und nur Pakete, die mit einer bekannten aktiven Verbindung übereinstimmen, werden von der Firewall zugelassen, alle anderen werden abgelehnt.

ãƒ» DoS (Denial of Service) - Wenn diese Funktion aktiviert ist, verhindert der Router DOS-Angriffe (Denial of Service), die aus dem Internet stammen. DOS-Angriffe führen dazu, dass die CPU Ihres Routers ausgelastet ist, sodass dieser keine Dienste für den normalen Datenverkehr bereitstellen kann.

ãƒ» WAN-Anfrage blockieren: Wenn diese Option aktiviert ist, ignoriert der Router PING-Anfragen aus dem Internet, sodass sie ausgeblendet zu sein scheinen. Dies erhöht die Sicherheit, da die Netzwerk-Ports verborgen bleiben, sodass Eindringlinge nicht so einfach auf das Netzwerk zugreifen können.

ãƒ» Remote-Management - Wenn diese Funktion aktiviert ist, ermöglicht der Router den Zugriff auf

das Webkonfigurationsprogramm über das Internet. Geben Sie die Portnummer ein, die für Hosts auf der WAN-Seite geöffnet wird. Die Standardeinstellung ist 443. Dieser Port muss angegeben werden, wenn der Benutzer eine Remote-Verbindung herstellt.

ãƒ» HTTPS: Wenn diese Funktion aktiviert ist, kann der Zugriff auf das Webkonfigurationsprogramm über eine HTTPS-Sitzung von der WAN-Seite statt über normales HTTP erfolgen. Dadurch ist Ihre Remote-Websitzung durch SSL-Verschlüsselungsalgorithmen geschützt. Wenn die HTTPS-Funktion deaktiviert ist, können Benutzer keine Verbindung über QuickVPN herstellen. Wenn deaktiviert, wird eine weniger sichere HTTP-Verbindung verwendet.

ãƒ» Multicast-Passthrough: Wenn ein IGMP-Proxy derzeit auf dem Router ausgeführt wird und Multicast-Passthrough aktiviert ist, lässt der Router IP-Multicast-Datenverkehr aus dem Internet zu.

Hinweis: Um die Firewall zu deaktivieren, muss das Administratorkennwort vom Standard abweichen. Die Felder *SPI* (Stateful Packet Inspection), *DoS (*Denial of Service), *Block WAN Request* und *Remote Management* sind ausgegraut.

Schritt 3: Aktivieren Sie im Bereich Web-Features einschränken eines oder alle Kontrollkästchen, um das entsprechende Feature einzuschränken.

ãƒ» Java - Java ist eine Programmiersprache für Webseiten. Um Java zu blockieren, aktivieren Sie das Kontrollkästchen **Java**. Wenn Sie Java ablehnen, dann können Sie möglicherweise nicht auf Internet-Sites zugreifen, die in dieser Programmiersprache geschrieben sind, sodass es sicher ist, Java-Applets zu blockieren, wenn das mit dem Router verbundene Gerät nicht auf die mit Java erstellten Websites zugreifen muss. Cyber-Kriminelle hingegen nutzen Java als zentralen Bestandteil ihres Angriffs, d. h. sie ermitteln das Betriebssystem und starten einen betriebssystemspezifischen Angriff, wenn Sie Websites besuchen, die mit Malware infiziert sind. Wenn Sie beispielsweise eine gehackte Website besuchen, wird eine JAR-Datei (Java Archive) ausgelöst, die Sie auffordert, ihre Funktion auszuführen, die aber heimlich verwendet wird, um das Betriebssystem des Computers zu bestimmen.

ãƒ» Cookies - Ein Cookie ist eine auf dem PC gespeicherte und von Internetseiten verwendete Information, wenn Benutzer mit ihnen interagieren. Um Cookies zu blockieren, aktivieren Sie das Kontrollkästchen **Cookies**. Wenn Sie Cookies blockieren möchten, können die Websites keine vorherigen Besucherinformationen speichern, wenn sie vom Gerät aus aufgerufen werden. Der Vorteil besteht darin, dass schädliche Cookies (Tracking-Cookies von Drittanbietern) nicht gespeichert werden, was ein Sicherheitsrisiko darstellt.

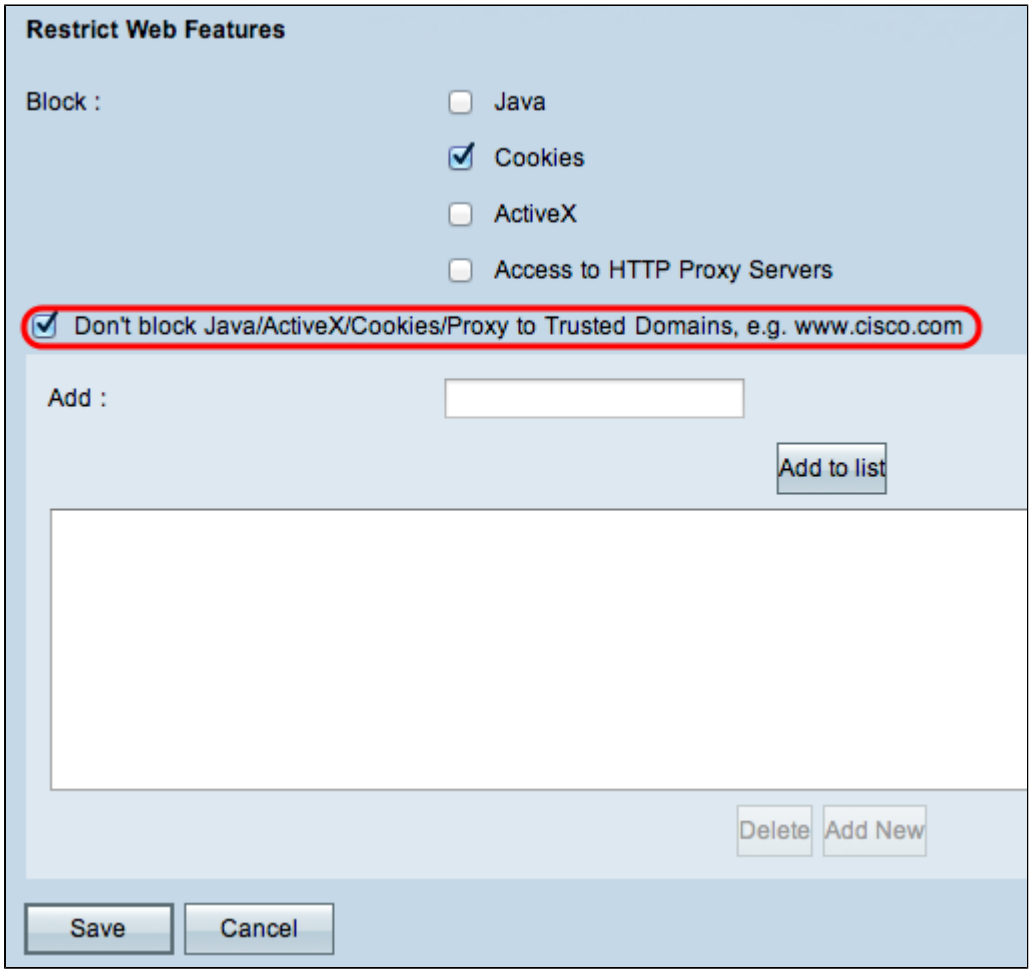
ãƒ» ActiveX - ActiveX ist eine Softwarekomponente von Microsoft Windows, die zur Entwicklung von Anwendungen oder zur Steuerung kleiner Programme wie Add-ons verwendet werden kann, die auf Websites im Internet verwendet werden. Wenn Sie ActiveX zulassen, kann es Ihnen beim Surfen helfen. Es ermöglicht Websites, Animationen und andere ähnliche Programme auszuführen. Andererseits besteht ein potenzielles Risiko, wenn Sie Webseiten besuchen, die schädliche ActiveX-Software enthalten, die von Cyber-Kriminellen entwickelt wurde und Schäden am Computer verursachen kann. Um ActiveX zu blockieren, aktivieren Sie das Kontrollkästchen **ActiveX**. Wenn Sie ActiveX blockieren, haben Sie möglicherweise Probleme, wenn Sie auf bestimmte Websites zugreifen möchten, die ActiveX zum Ausführen verwenden.

ãƒ» Zugriff auf Proxy-HTTP-Server - Wenn Sie anonym durch einen Proxy-Server surfen und den Zugriff auf den Proxy-Server verweigern möchten, aktivieren Sie das Kontrollkästchen **Zugriff auf Proxy-HTTP-Server**. HTTP-Proxy-Server verbergen Details von Endbenutzern vor Hackern. Sie arbeiten als Vermittler, sodass Sie nicht direkt auf das Internet zugreifen. Wenn lokale Benutzer jedoch Zugriff auf WAN-Proxy-Server haben, können sie möglicherweise die Inhaltsfilter auf dem Router umgehen und auf Websites im Internet zugreifen, die vom Router blockiert werden.

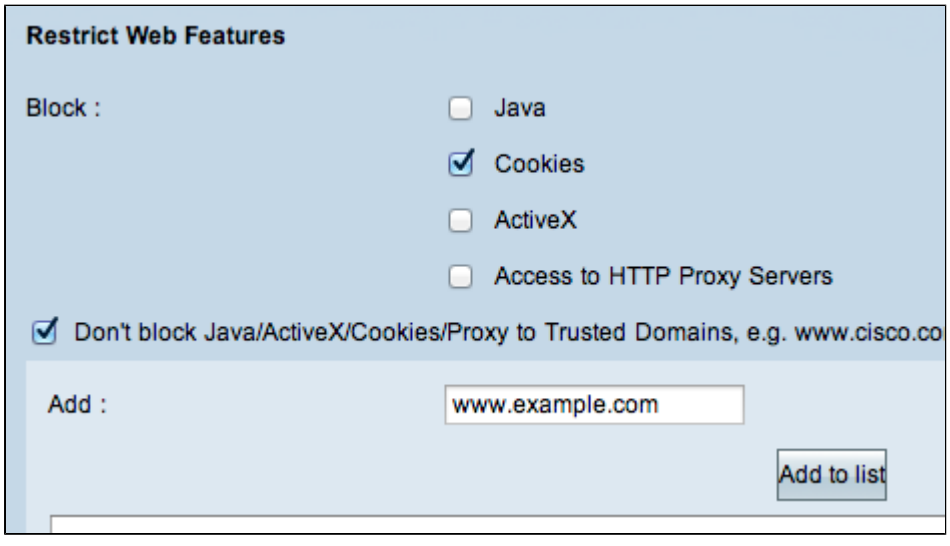
Schritt 4: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Vertrauenswürdige Domänen hinzufügen

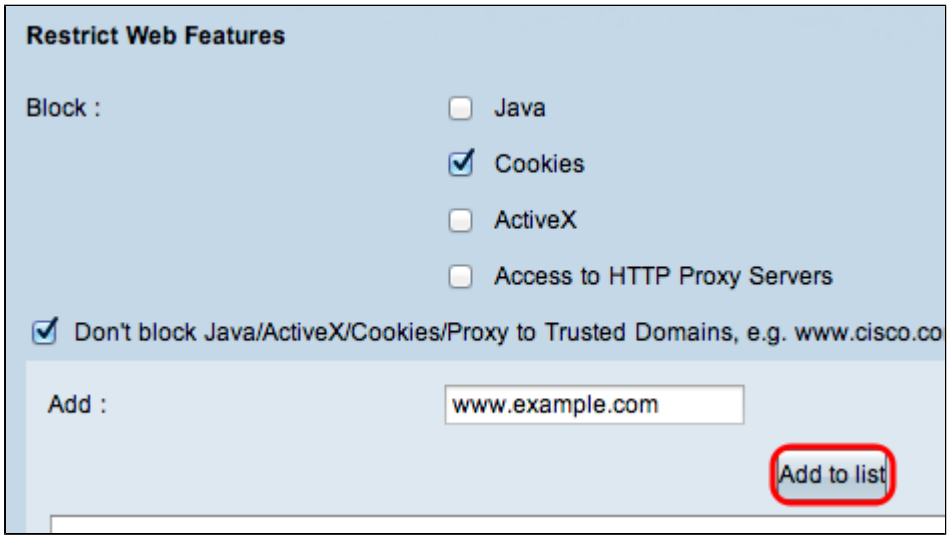
Obwohl eine der Webfunktionen blockiert werden kann, kann der Benutzer die Aktivierung dieser Funktionen für bestimmte vertrauenswürdige Domänen zulassen.



Schritt 1: Aktivieren Sie die Schaltfläche **Java/ActiveX/Cookies/Proxy nicht für vertrauenswürdige Domänen sperren**. Diese Option ist nur verfügbar, wenn der Benutzer eine der Webfunktionen in Schritt 3 der *allgemeinen Firewall-Einstellungen* blockiert.



Schritt 2: Geben Sie im Feld *Add (Hinzufügen*) die Domäne ein, die der Liste der vertrauenswürdigen Domänen hinzugefügt werden soll.

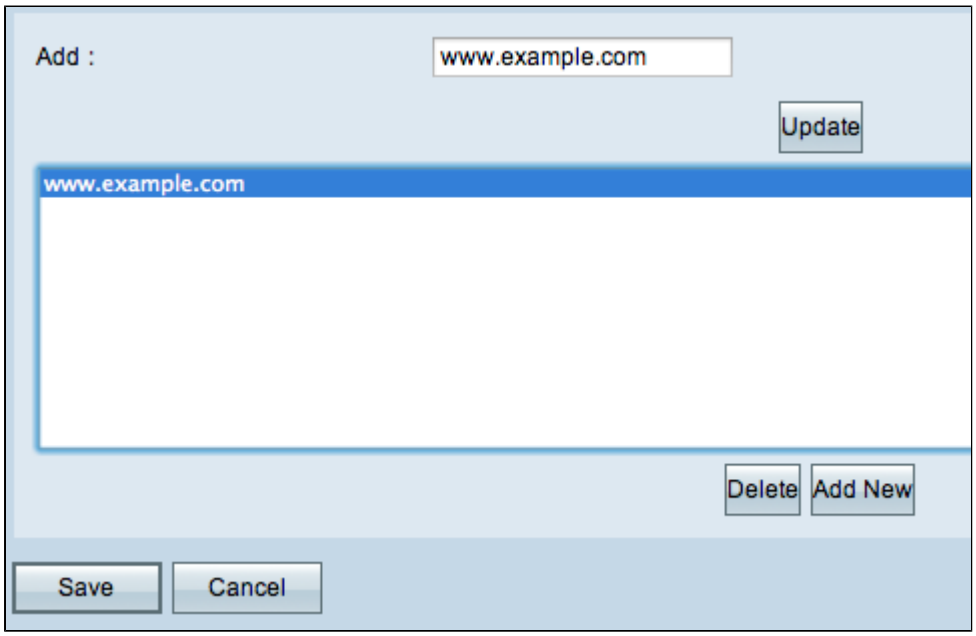


Schritt 3: Klicken Sie auf **Zur Liste hinzufügen.** Die Domäne wird der Liste der vertrauenswürdigen Domänen hinzugefügt.

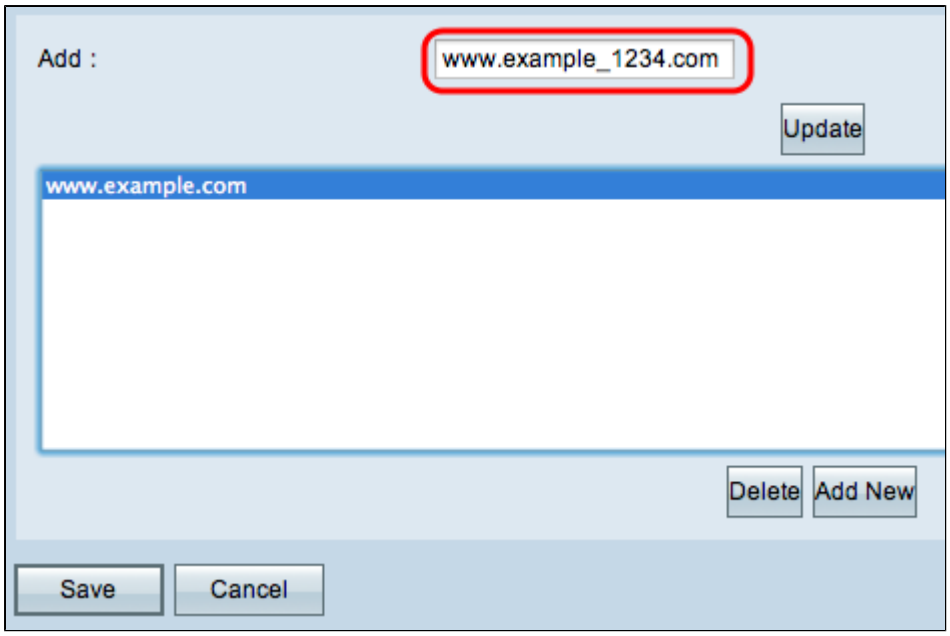
Schritt 4: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktualisieren einer vertrauenswürdigen Domäne

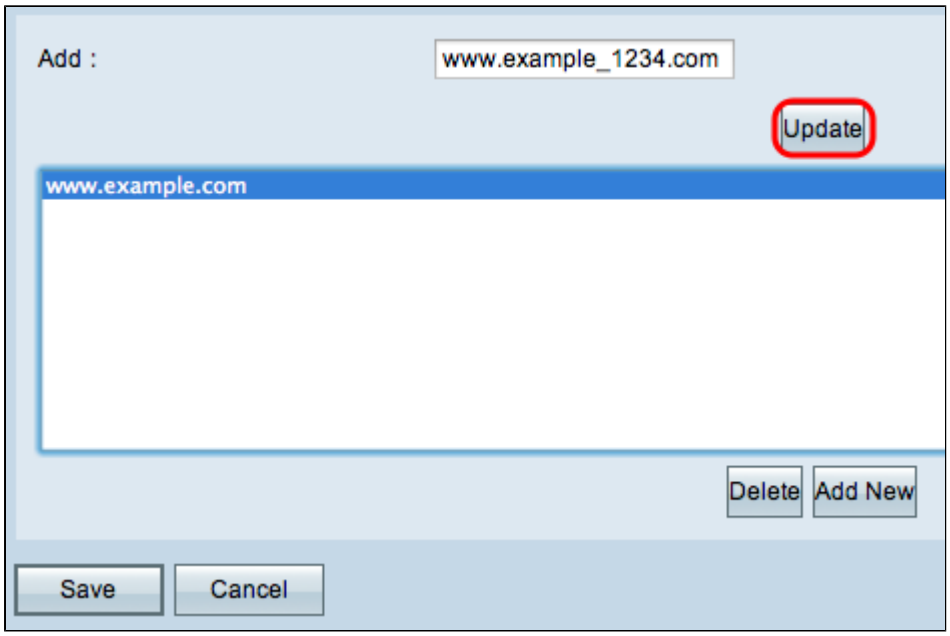
Dieser Abschnitt führt den Benutzer durch die Bearbeitung einer vertrauenswürdigen Domäne.



Schritt 1: Wählen Sie aus der Liste der vertrauenswürdigen Domänen die Domäne aus, die Sie bearbeiten möchten.



Schritt 2: Geben Sie im Feld *Add* (*Hinzufügen*) den aktualisierten Domänennamen für die erforderliche Domäne ein.

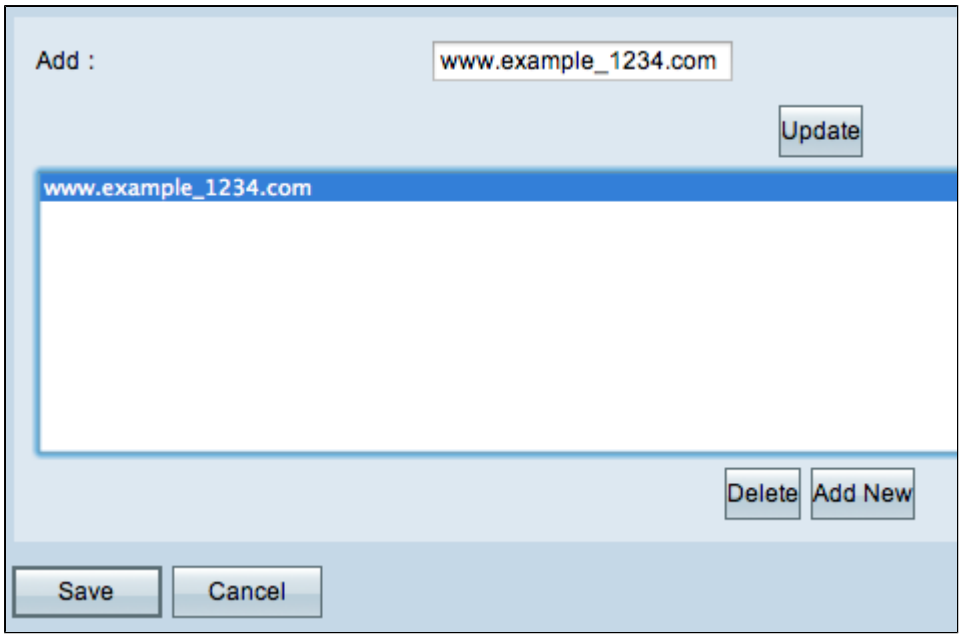


Schritt 3: Klicken Sie auf **Aktualisieren**.

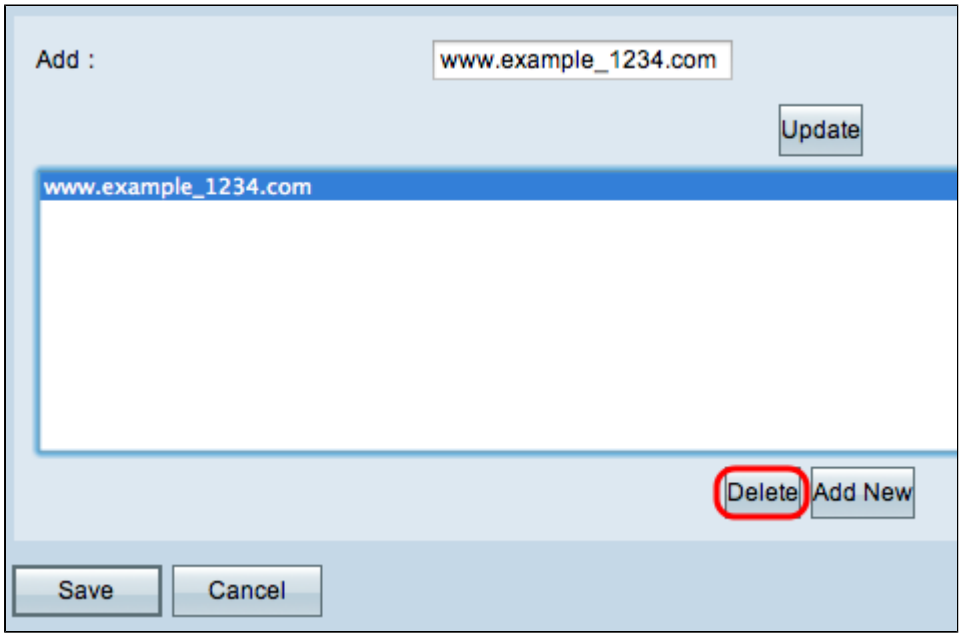
Schritt 4: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Löschen einer vertrauenswürdigen Domäne

Dieser Abschnitt führt den Benutzer durch die Schritte zum Löschen einer vertrauenswürdigen Domäne.



Schritt 1: Wählen Sie die Domäne aus, die Sie löschen möchten.



Schritt 2: Klicken Sie auf **Löschen**. Die Domäne wurde gelöscht.

Schritt 3: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.