Konfigurieren der allgemeinen Firewall-Einstellungen für den RV016, RV042, RV042G und RV082

Ziel

Die integrierte Firewall für den RV016, RV042, RV042G und RV082 blockiert standardmäßig bestimmte Arten von Datenverkehr. Die Art des blockierten Datenverkehrs, z. B. HTTPS-, TCP- und ICMP-Anforderungen sowie Remote-Management-Datenverkehr, kann angepasst werden. Die Firewall selbst kann ebenfalls aktiviert oder deaktiviert werden. Außerdem können bestimmte Aspekte von Websites blockiert werden, bei denen es sich um Sicherheitslücken handeln kann. Diese Website-Funktionen können, wenn sie entsperrt werden, potenziell schädliche Daten auf Ihrem Computer speichern.

In diesem Dokument wird erläutert, wie Sie die allgemeinen Firewall-Einstellungen für den RV016, RV042, RV042G und RV082 konfigurieren.

Unterstützte Geräte

RV016

â€¢RV042

ãƒ» RV042G

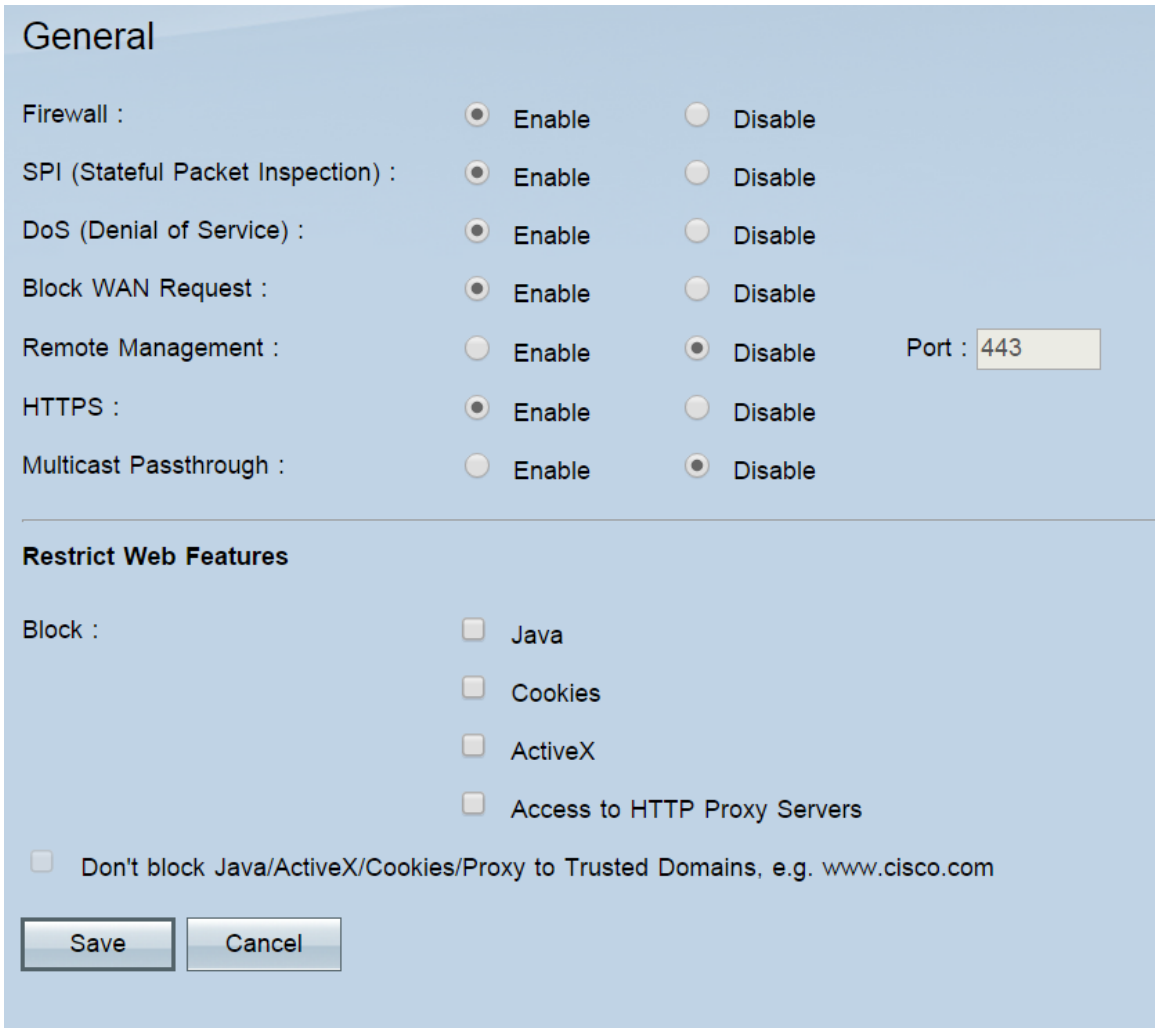
RV082

Software-Version

ãƒ» v4.2.3.06

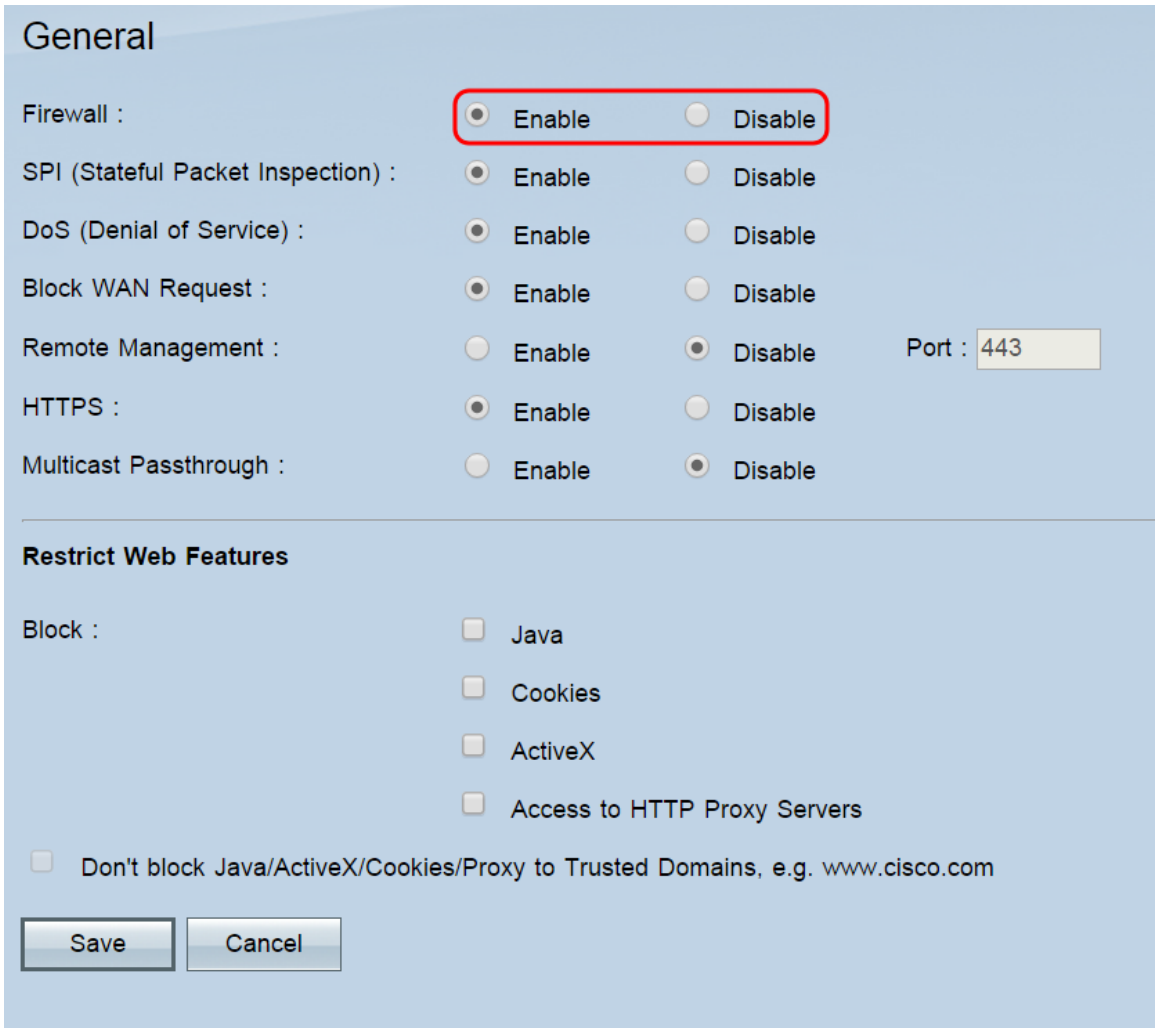
Konfigurieren der allgemeinen Firewall-Einstellungen

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



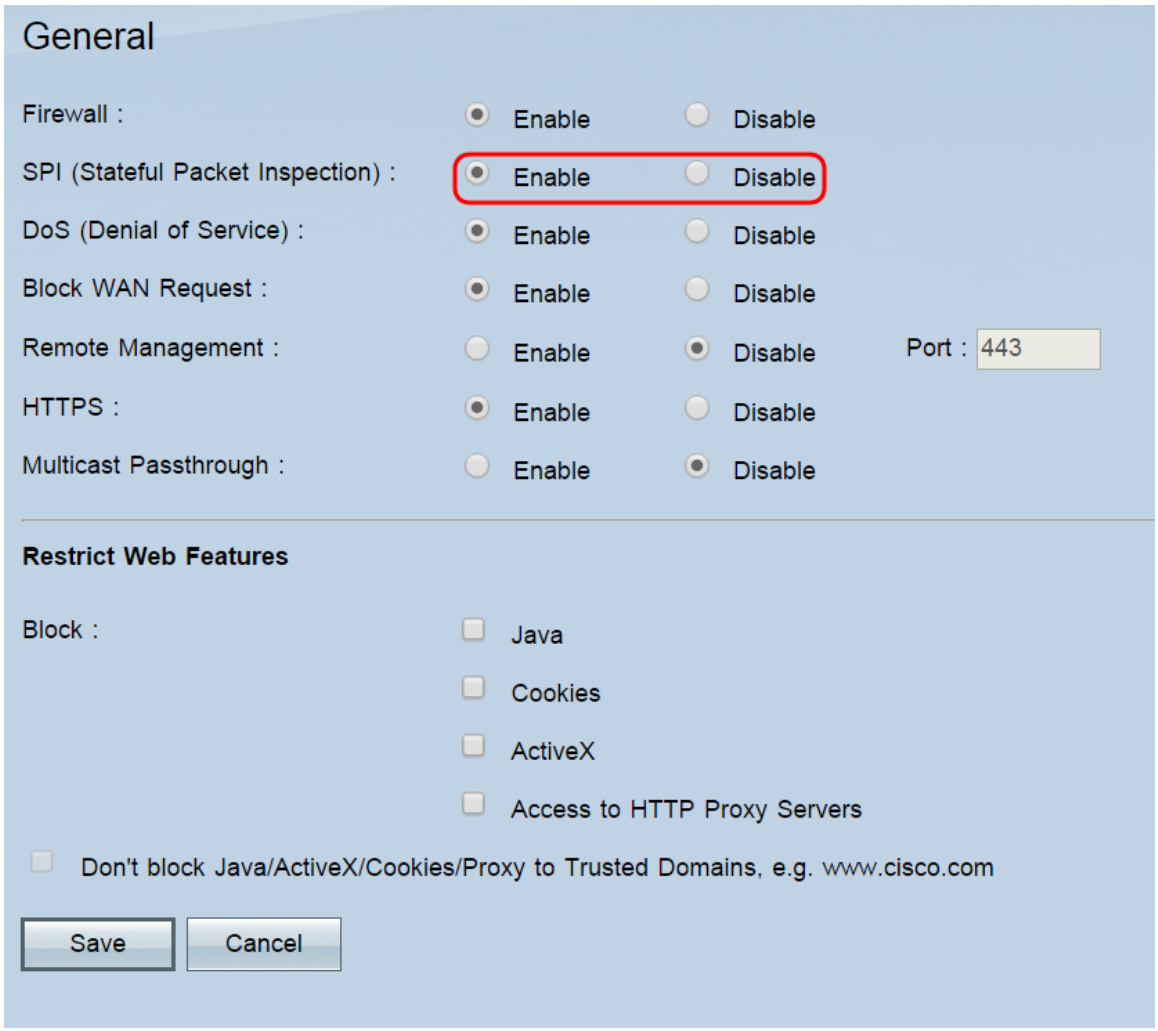
Allgemeine Funktionen

Schritt 1: Wählen Sie im Feld *Firewall* ein Optionsfeld aus, um die Firewall zu **aktivieren** oder zu **deaktivieren**. Die Firewall ist standardmäßig aktiviert. Eine Deaktivierung wird nicht empfohlen. Durch Deaktivieren der Firewall werden auch Zugriffsregeln und Content-Filter deaktiviert.

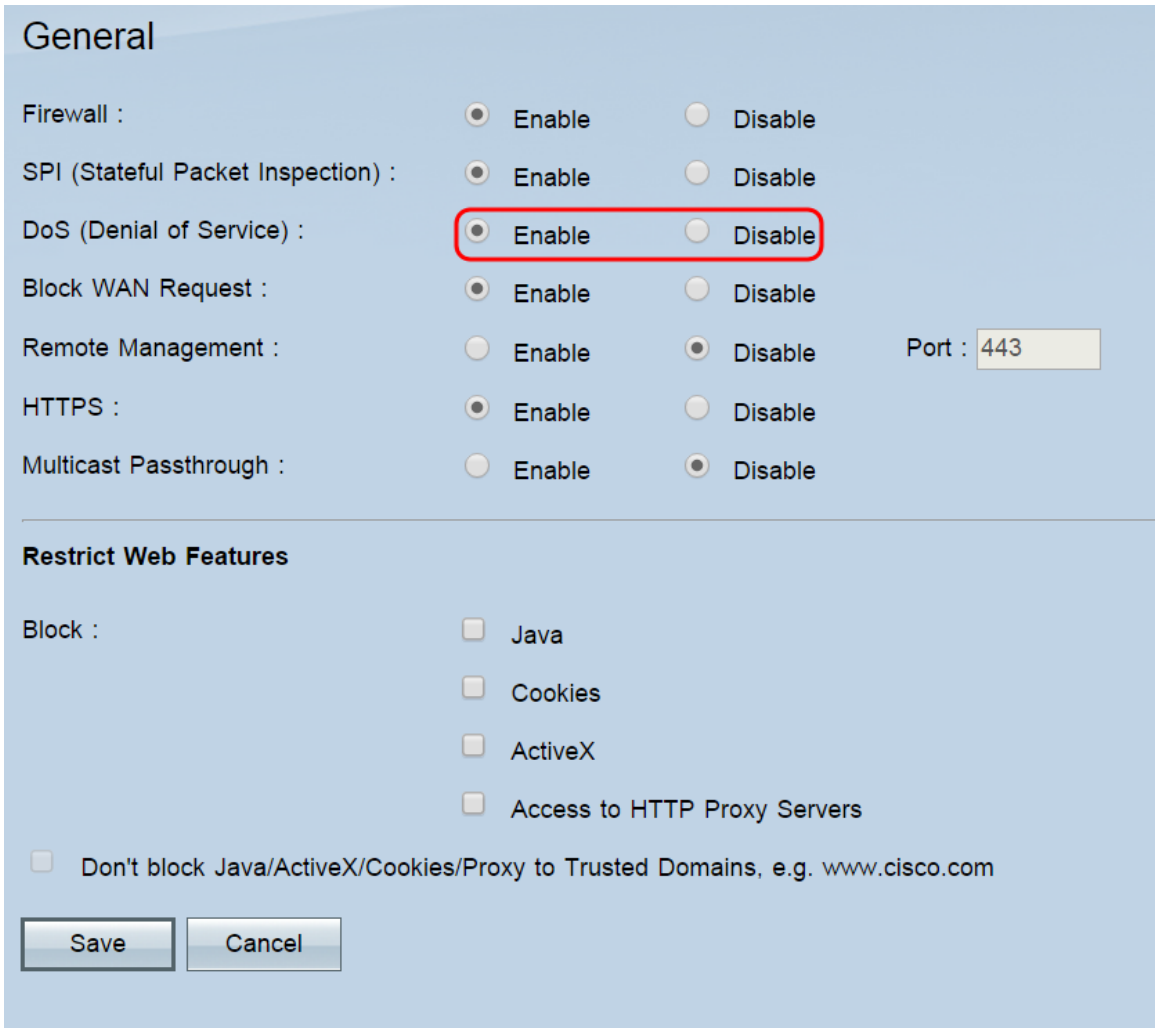


Hinweis: Wenn Sie die Firewall deaktivieren möchten und weiterhin das Standard-Administratorkennwort verwenden, wird eine Meldung angezeigt, in der Sie darauf hingewiesen werden, dass Sie das Kennwort ändern müssen. Sie können die Firewall erst deaktivieren, wenn Sie dies getan haben. Klicken Sie auf **OK**, um zur Kennwortseite zu wechseln, oder auf **Abbrechen**, um auf dieser Seite zu bleiben.

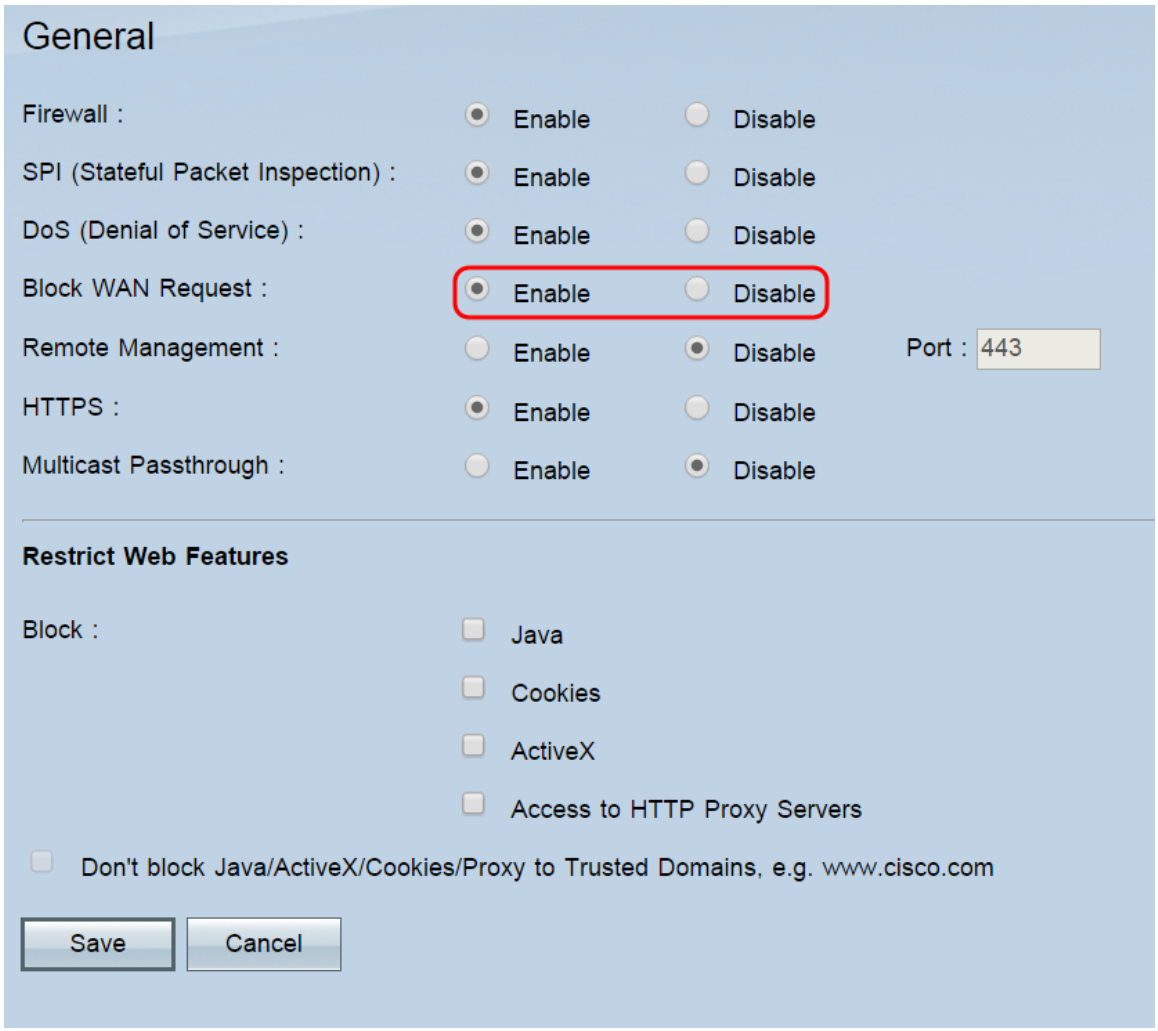
Schritt 2: Wählen Sie im SPI (Stateful Package Inspection) entweder das Optionsfeld **Aktivieren** oder **Deaktivieren aus**. SPI ist standardmäßig aktiviert. Mit dieser Funktion kann der Router alle Pakete überprüfen, bevor diese zur Verarbeitung gesendet werden. Diese Funktion kann nur aktiviert werden, wenn die Firewall aktiviert ist.



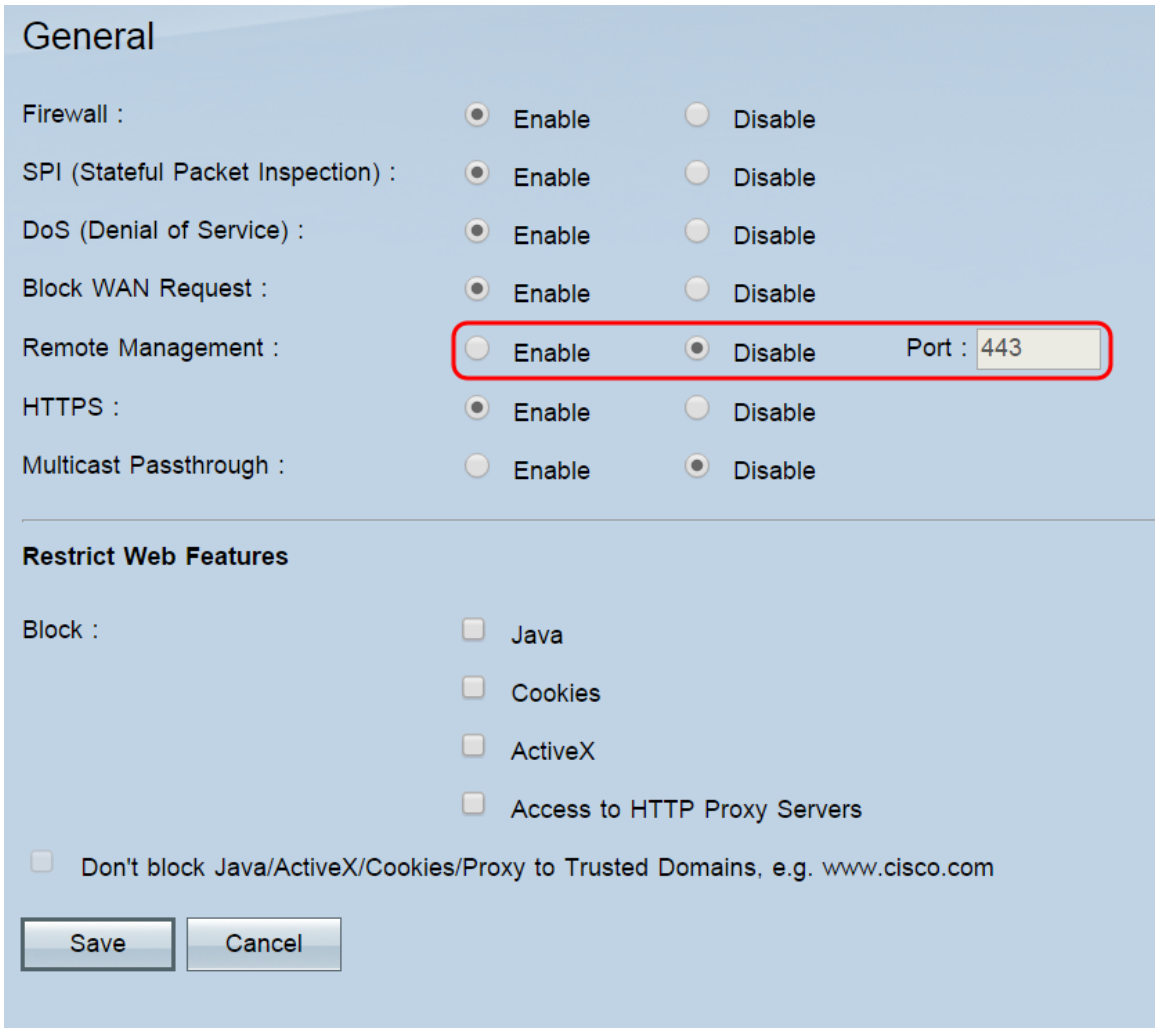
Schritt 3: Wählen Sie im Feld *DoS (Denial of Service*) entweder das Optionsfeld **Aktivieren** oder **Deaktivieren aus**. DoS ist standardmäßig aktiviert. Diese Funktion verhindert externe Angriffe auf das interne Netzwerk (z. B. SYN Flooding, Schlumpf, LAND, Ping of Death, IP-Spoofing und Reassembly-Angriffe). Diese Funktion kann nur aktiviert werden, wenn die Firewall aktiviert ist.



Schritt 4: Wählen Sie im Feld *WAN-Anforderung blockieren* entweder das Optionsfeld **Aktivieren** oder **Deaktivieren aus**. Die Blockierung von WAN-Anfragen ist standardmäßig aktiviert. Mit dieser Funktion kann der Router nicht akzeptierte TCP- und ICMP-Anforderungen aus dem WAN löschen. Hacker können so den Router nicht finden, indem sie einen Ping an die WAN-IP-Adresse senden. Diese Funktion kann nur aktiviert werden, wenn die Firewall aktiviert ist.



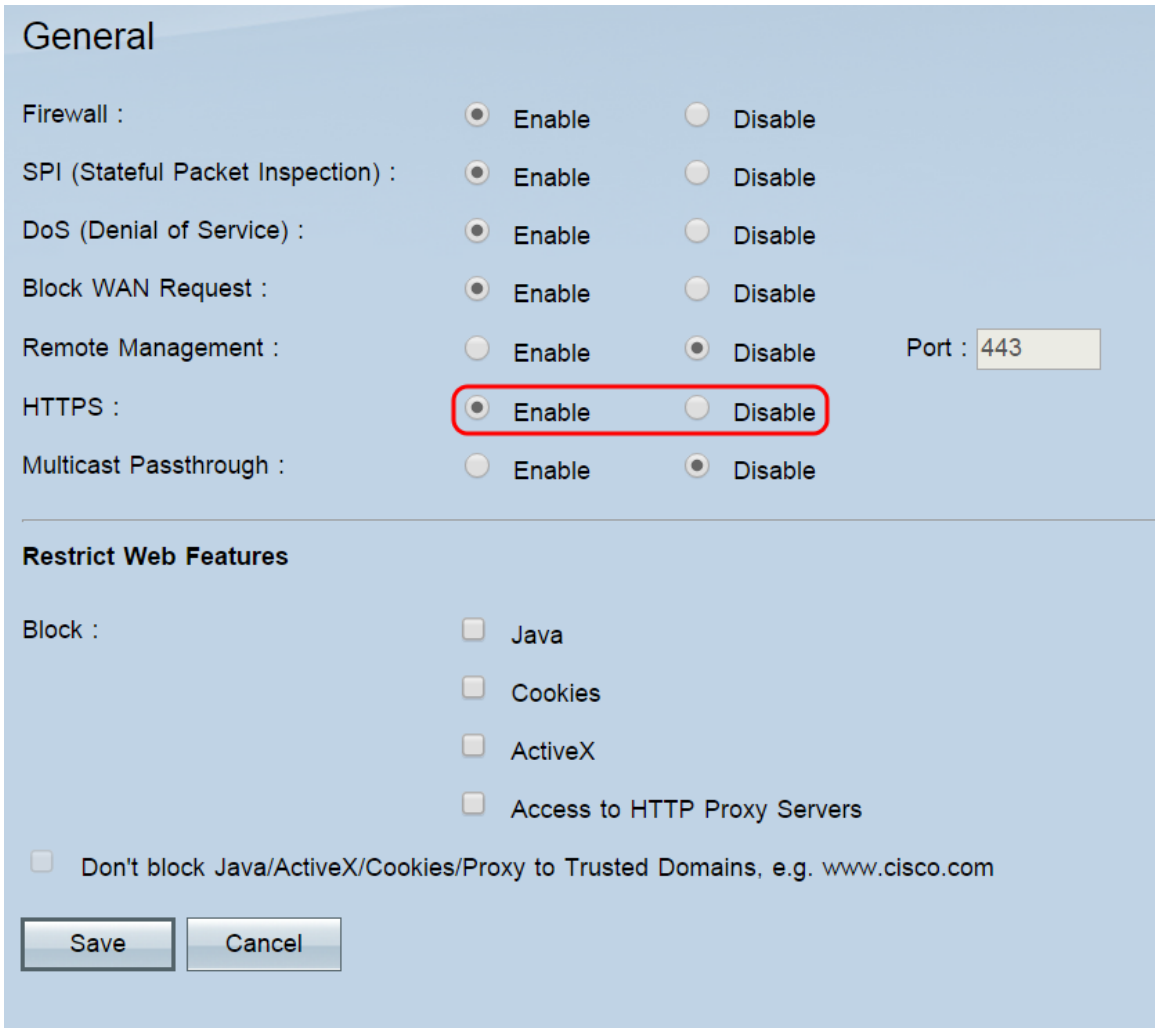
Schritt 5: Wählen Sie im Feld *Remote Management* entweder das Optionsfeld **Enable (Aktivieren)** oder **Disable (Deaktivieren)** aus. Die Remote-Verwaltung ist standardmäßig deaktiviert. Mit dieser Funktion können Sie von einem beliebigen Standort im Internet eine Verbindung zum Webkonfigurationsprogramm des Routers herstellen. Wenn Sie diese Funktion aktivieren, können Sie den für Remote-Verbindungen verwendeten Port im Feld Port festlegen. Der Standardwert ist 443.



Hinweis: Wenn Sie das Standard-Administratorkennwort verwenden, wird eine Meldung angezeigt, in der Sie darauf hingewiesen werden, dass Sie das Kennwort ändern müssen. Klicken Sie auf **OK,** um zur Kennwortseite zu gelangen, oder auf **Abbrechen,** um auf dieser Seite zu bleiben. Das Kennwort muss geändert werden, damit nicht autorisierte Benutzer nicht mit dem Standardkennwort auf den Router zugreifen können.

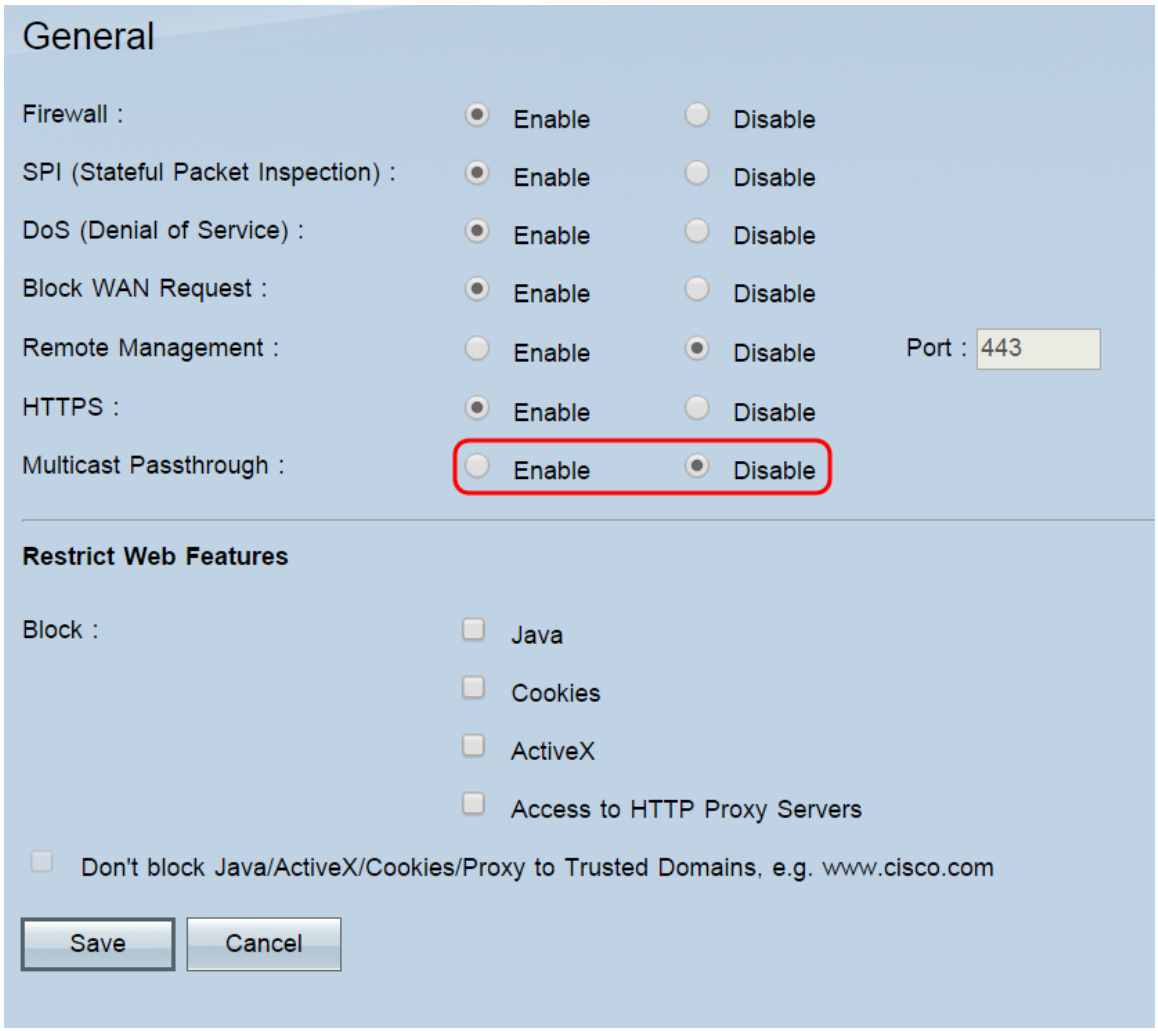
Hinweis: Wenn die Remoteverwaltung aktiviert ist, können Sie von einem beliebigen Browser aus auf das Webkonfigurationsprogramm zugreifen, indem Sie **http://<WAN-IP-Adresse des Routers>:<Port> eingeben**. Wenn HTTPS aktiviert ist, geben Sie stattdessen **https://<WAN-IP-Adresse des Routers>:<Port>** ein.

Schritt 6: Wählen Sie im Feld *HTTPS* entweder das Optionsfeld **Aktivieren** oder **Deaktivieren aus**. HTTPS ist standardmäßig aktiviert. Diese Funktion ermöglicht sichere HTTP-Sitzungen.



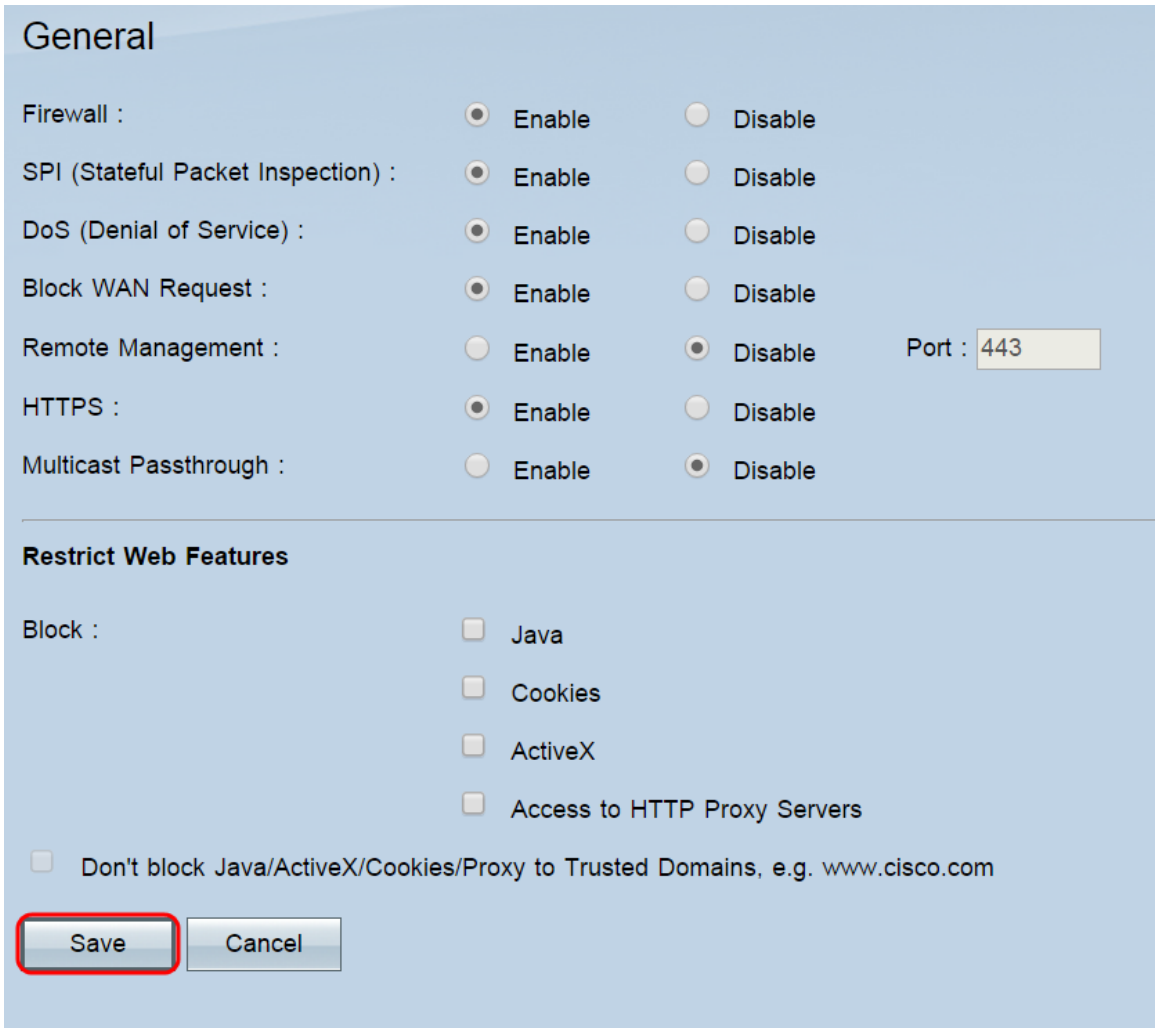
Hinweis: Wenn diese Funktion deaktiviert ist, können Benutzer keine Verbindung über QuickVPN herstellen.

Schritt 7. Wählen Sie im Feld *Multicast-Passthrough* entweder das Optionsfeld **Aktivieren** oder **Deaktivieren aus**. Multicast-Passthrough ist standardmäßig deaktiviert. Diese Funktion ermöglicht die Übertragung von IP-Multicast-Paketen an die entsprechenden LAN-Geräte und wird für Internetspiele, Videokonferenzen und Multimedia-Anwendungen verwendet.



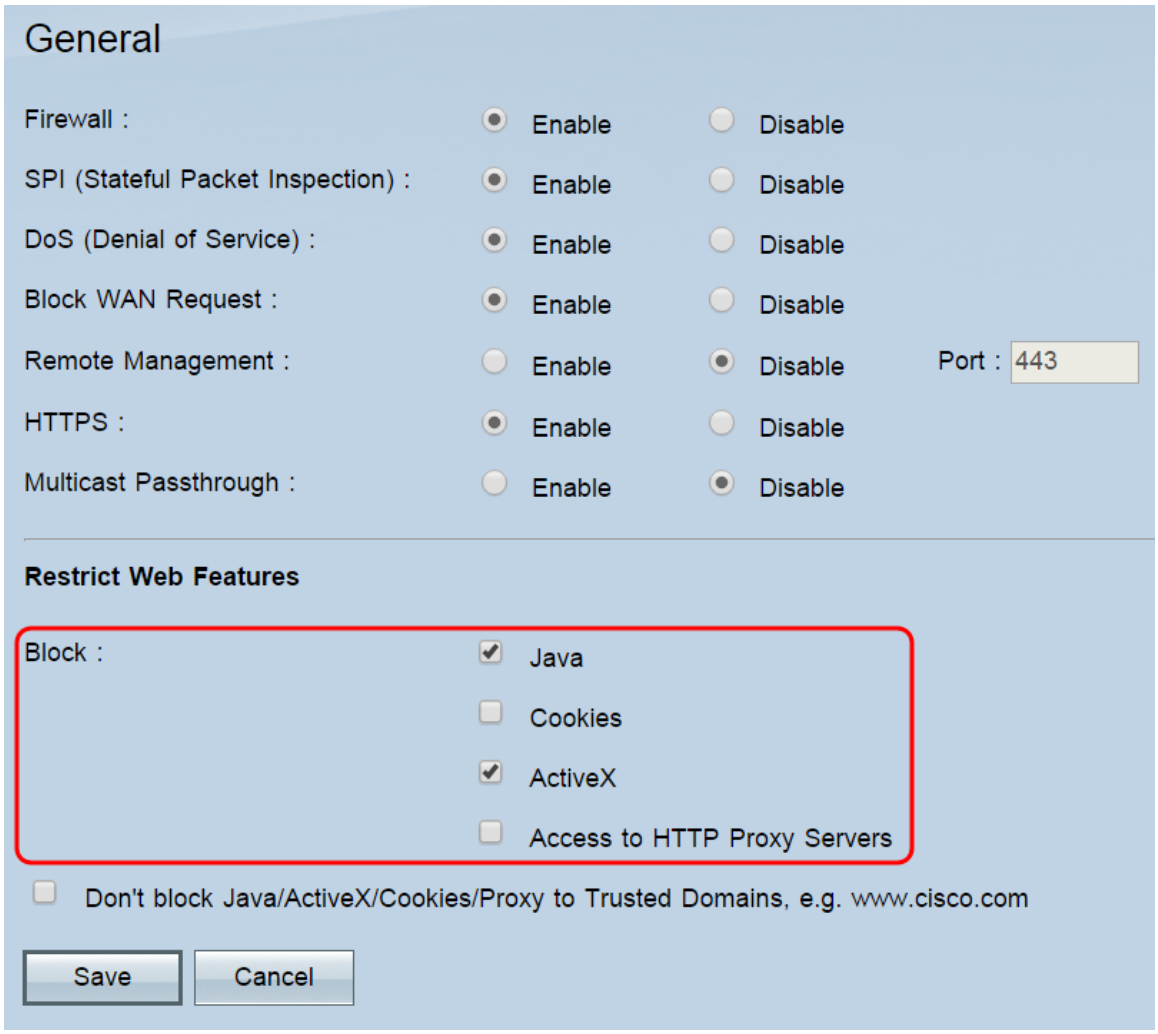
Hinweis: RV016, RV042, RV042G und RV082 unterstützen das Weiterleiten von Multicast-Datenverkehr über einen IPSec-Tunnel nicht.

Schritt 8: Klicken Sie auf **Speichern**.



Web-Funktionen

Schritt 1: Aktivieren Sie im Feld *Blockieren* die Kontrollkästchen der Webfunktionen, die Sie in der Firewall blockieren möchten. Wenn Sie für einige Domänen gesperrte Funktionen zulassen möchten, können diese Domänen in Schritt 2 einer Ausnahmeliste hinzugefügt werden. Keine der Funktionen ist standardmäßig blockiert.



Folgende Optionen sind verfügbar:

ãƒ» Java - Java ist eine Programmiersprache für Webseiten. Wenn Sie dieses Kontrollkästchen aktivieren, werden Java-Applets blockiert (kleine Programme, die in Webseiten eingebettet sind, aber außerhalb des Webbrowsers ausgeführt werden). Dies kann jedoch dazu führen, dass Websites, die diese Funktion verwenden, nicht ordnungsgemäß funktionieren.

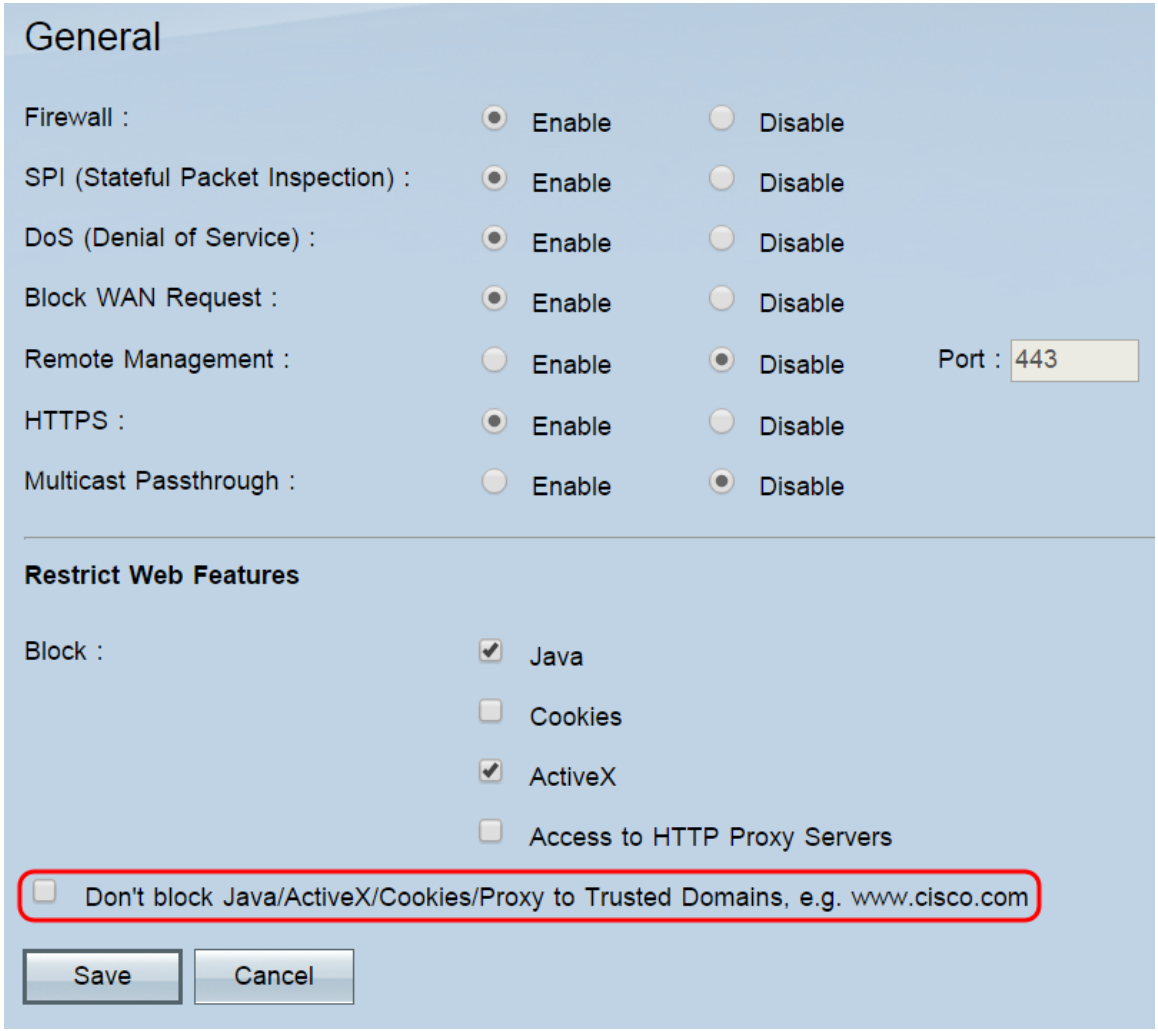
ãƒ» Cookies - Ein Cookie ist eine Datei, die von einer Website lokal auf dem PC eines Benutzers gespeichert wird. Das Blockieren von Cookies kann dazu führen, dass Websites, die sich darauf verlassen, sich falsch verhalten.

ãƒ» ActiveX - ActiveX ist ein von Microsoft entwickeltes Software-Framework. Dieses Framework kann zum Ausführen bestimmter Teile von Webseiten verwendet werden. Wenn Sie dieses Kontrollkästchen aktivieren, werden diese Komponenten blockiert. Dies kann jedoch dazu führen, dass Websites, die ActiveX verwenden, nicht ordnungsgemäß funktionieren.

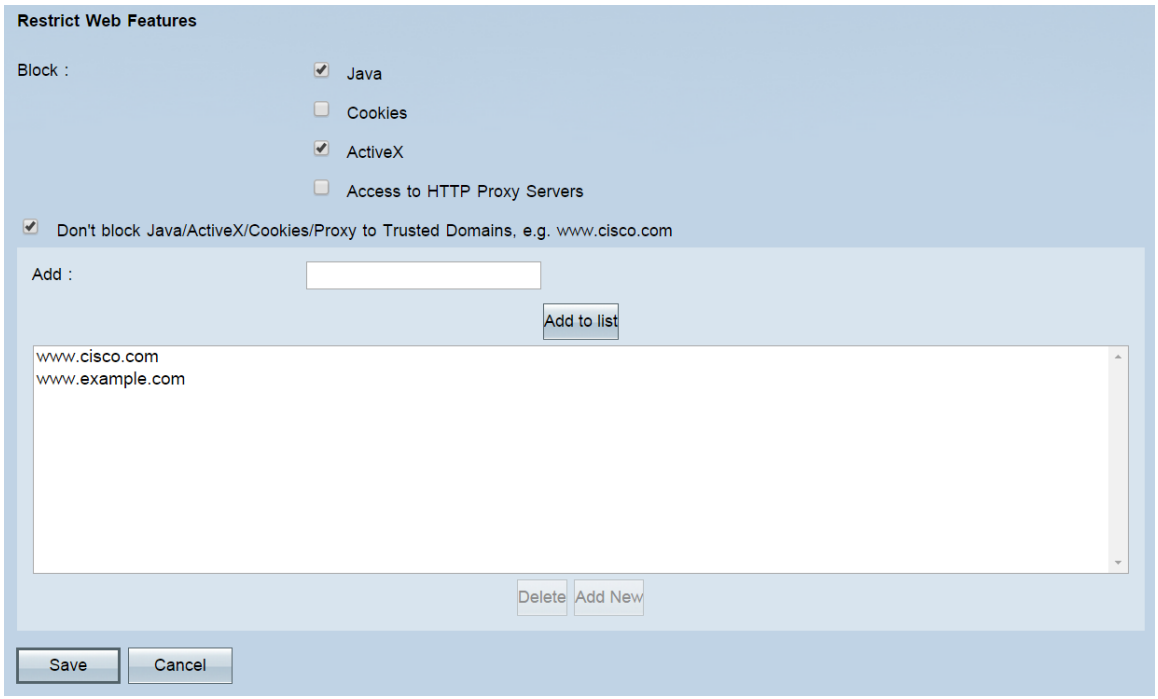
ãƒ» Zugriff auf HTTP-Proxy-Server â€" Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Zugriff auf HTTP-Proxy-Server blockieren möchten. Die Verwendung von WAN-Proxy-Servern kann die Sicherheit des Routers beeinträchtigen.

Schritt 2: Aktivieren Sie das Kontrollkästchen **Java/ActiveX/Cookies/Proxy nicht für vertrauenswürdige Domänen blockieren,** um die Liste der vertrauenswürdigen Domänen zu öffnen, in der Sie Domänen hinzufügen oder entfernen können, für die blockierte Webfunktionen zulässig sind. Dieses Feld ist standardmäßig deaktiviert und nur verfügbar, wenn Sie ein vorheriges Kontrollkästchen aktiviert haben, um eine Funktion zu blockieren. Ist das Kontrollkästchen

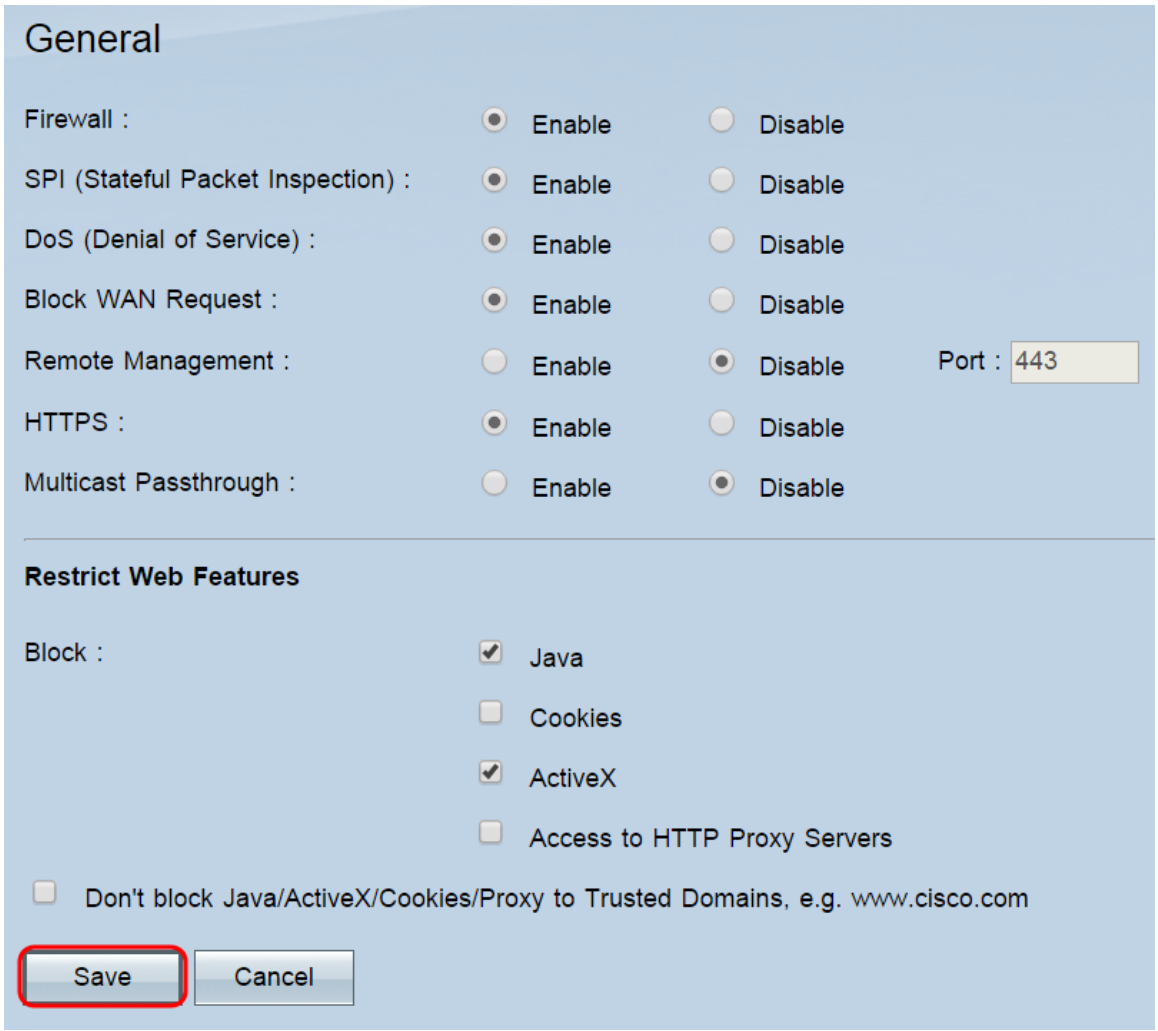
deaktiviert, werden die Funktionen für alle Websites gesperrt.



Schritt 3. (Optional) Wenn Sie das Kontrollkästchen **Java/ActiveX/Cookies/Proxy nicht für vertrauenswürdige Domänen blockieren** aktiviert haben, wird eine Liste der vertrauenswürdigen Domänen angezeigt. Um eine Domäne zur Liste hinzuzufügen, geben Sie sie in das Feld *Hinzufügen ein*, und klicken Sie auf **Zur Liste hinzufügen**. Wenn Sie eine vorhandene Domäne ändern möchten, klicken Sie in der Liste auf die Domäne, bearbeiten Sie sie im Feld *Hinzufügen*, und klicken Sie dann auf **Aktualisieren**. Um eine Domäne aus der Liste zu löschen, klicken Sie in der Liste auf die Domäne und anschließend auf **Löschen**.



Schritt 4: Klicken Sie auf **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.