Algemene firewallinstellingen op de RV016, RV042, RV042G en RV082 VPN-routers

Doel

Een firewall beschermt een intern netwerk tegen een extern netwerk zoals het internet. Firewalls zijn van vitaal belang voor de netwerkbeveiliging. Er zijn verschillende instellingen beschikbaar die specifieke services kunnen in- of uitschakelen op basis van uw beveiligingsbehoeften.

Het doel van dit artikel is te laten zien hoe u algemene firewallinstellingen kunt in- of uitschakelen op RV016, RV042, RV042G en RV082 VPN-routers.

Toepasselijke apparaten

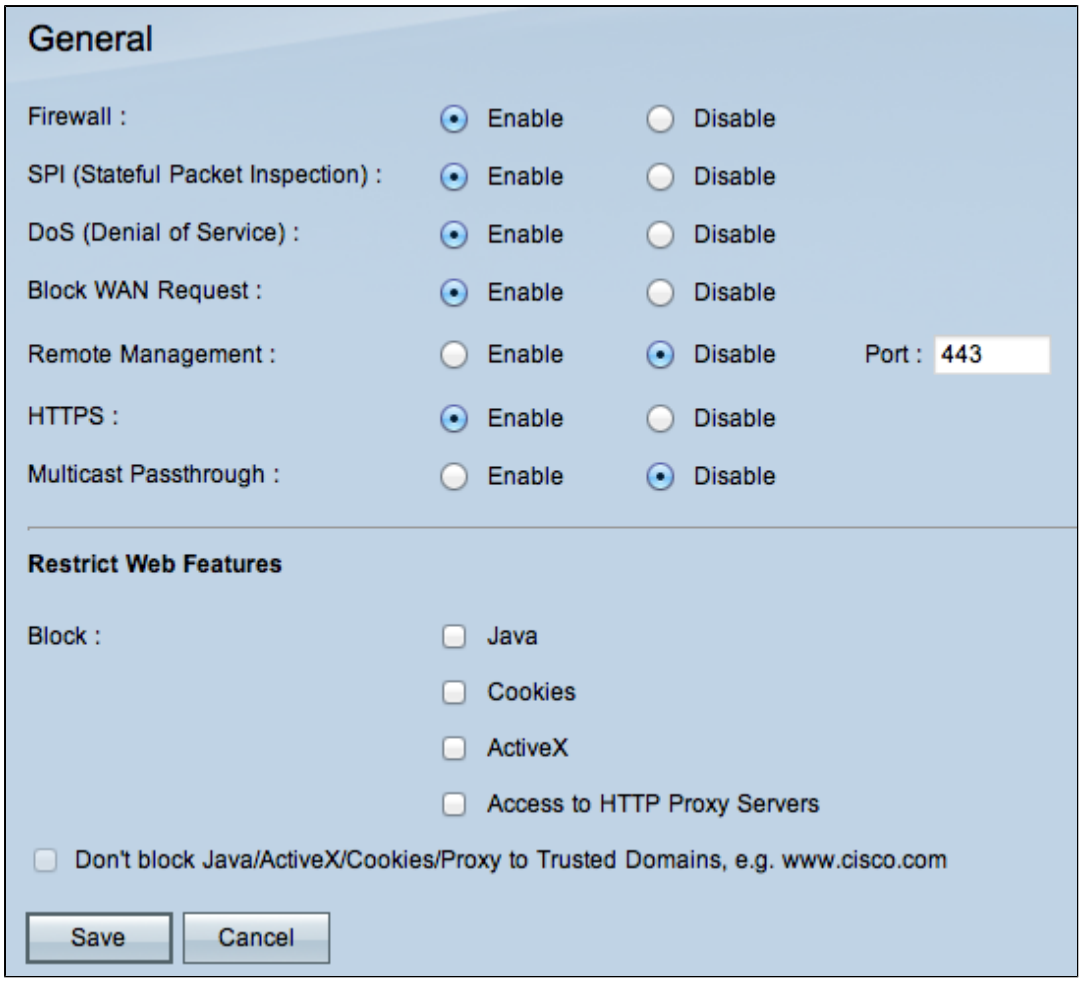
· RV016
â€¢RV042
· RV042G
· RV082

Softwareversie

· v4.2.1.02

Algemene firewallinstellingen

Stap 1. Log in het hulpprogramma Routerconfiguratie en kies **Firewall > Algemeen**. De *pagina Algemeen* wordt geopend:



Stap 2. Klik op de radioknop **Inschakelen** of **uitschakelen** om de beschikbare instellingen in de firewall in te schakelen of uit te schakelen volgens de gebruikerseisen.

De volgende velden worden als volgt beschreven:

· Firewall â€" Wanneer deze functie is ingeschakeld, zal de router een diepe pakketinspectie uitvoeren op al het verkeer dat door deze router gaat en de pakketten laten vallen die niet het vooraf gedefinieerde protocolgedrag volgen.

· SPI (Stateful Packet Inspection) â€" de firewall van de router gebruikt Stateful Packet Inspection (SPI) om het verkeer bij de firewall te bekijken. Het controleert de staat van netwerkverbindingen zoals TCP-stromen en UDP-communicatie. De firewall onderscheidt legitieme pakketten voor verschillende soorten verbindingen en alleen pakketten die overeenkomen met een bekende actieve verbinding worden toegestaan door de firewall, alle andere worden afgewezen.

· Dos (Denial of Service) â€" Wanneer deze functie is ingeschakeld, voorkomt de router DOS-aanvallen (Denial of Service) die van het internet komen. DOS-aanvallen zorgen ervoor dat de CPU van uw router bezet is, zodat er geen services kunnen worden geleverd aan regelmatig verkeer.

· Blokkeer WAN-verzoek â€" Wanneer dit is ingeschakeld, zal de router PINGverzoeken van het internet negeren, zodat het verborgen zal lijken. Dit helpt beveiliging te bieden door de netwerkpoorten te verbergen, zodat de overtreders niet gemakkelijk toegang hebben tot het netwerk.

· Beheer op afstand â€" Wanneer deze functie is ingeschakeld, geeft router toegang tot het hulpprogramma voor webconfiguratie via internet. Voer het poortnummer in dat voor hosts aan de WAN-kant wordt geopend. De standaardinstelling is 443. Deze poort moet worden opgegeven wanneer de gebruiker een externe verbinding tot stand brengt.

· HTTPS â€” Als dit is ingeschakeld, kan het hulpprogramma voor webconfiguratie worden benaderd via een HTTPS-sessie vanaf de WAN-kant in plaats van via gewone HTTP. Deze zal uw externe websessie beschermd door SSL-encryptie algoritmen. Als de functie HTTPS uitgeschakeld is, kunnen gebruikers geen verbinding maken met QuickVPN. Indien uitgeschakeld, maakt het gebruik van een minder beveiligde HTTP verbinding.

· Multicast Passthrough â€” Als een IGMP Proxy momenteel op de router wordt uitgevoerd, wanneer Multicast Passthrough is ingeschakeld, zal de router IP Multicast-verkeer van internet naar binnen laten komen.

Opmerking: om de firewall uit te schakelen, moet het beheerderswachtwoord in de standaardinstelling worden gewijzigd. De velden *SPI* (Stateful Packet Inspection), *DoS* (Denial of Service), *Block WAN request* en *Remote Management* zijn grijs.

Stap 3. In het gedeelte Web Properties beperken, schakelt u een of alle selectievakjes in om de corresponderende functie te beperken.

· Java â€” Java is een programmeertaal voor websites. Als u Java wilt blokkeren, schakelt u het selectievakje **Java in**. Als u Java weigert, dan kunt u niet in staat zijn om toegang te krijgen tot internetsites die in deze programmeertaal zijn geschreven, dus het is veilig om door te gaan en blokkeert Java applets als het apparaat dat is aangesloten op de router niet hoeft om toegang te hebben tot de websites die met Java zijn gemaakt. Aan de andere kant, Cyber-criminelen gebruiken Java als een integraal onderdeel van hun aanval, dat is om het OS te bepalen en een OS-gespecificeerde aanval te lanceren wanneer u websites bezoekt die zijn geïnfecteerd door malware. Bijvoorbeeld, wanneer u een gehackte website bezoekt, wordt een JAR (Java Archive) bestand geactiveerd dat u vraagt om zijn functie uit te voeren, maar heimelijk wordt het gebruikt om het OS van de computer te bepalen.

Cookies â€” Een cookie is gegevens die op de pc worden opgeslagen en door internetsites worden gebruikt wanneer gebruikers ermee communiceren. Om cookies te blokkeren, kruist u het selectievakje **Cookies aan**. Als u cookies wilt blokkeren, dan kunnen de websites geen eerdere bezoekinformatie opslaan wanneer ze via het apparaat worden benaderd. Het voordeel is dat kwaadaardige cookies (third party tracking cookies) niet worden opgeslagen, wat een veiligheidsrisico oplevert.

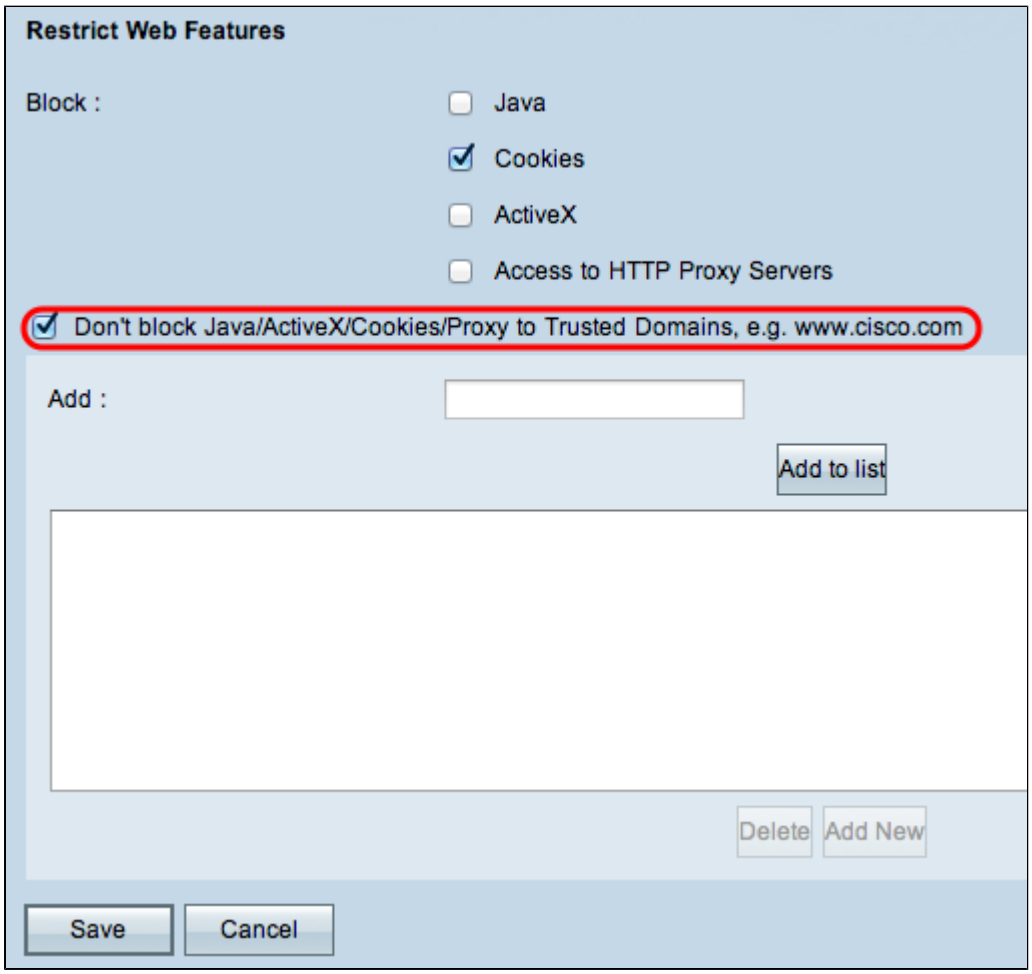
ActiveX â€” ActiveX is een softwarecomponent van Microsoft Windows die kan worden gebruikt om toepassingen te ontwikkelen of kleine programma's zoals add-ons te controleren die op internetsites worden gebruikt. Als u ActiveX toestaat, kan het helpen uw ervaring te verbeteren wanneer u bladert; het staat websites toe om animaties en andere gelijkaardige programma's in werking te stellen. Aan de andere kant is er een mogelijk risico als u webpagina's bezoekt die kwaadaardige ActiveX-software bevatten die is ontwikkeld door cybercriminelen en die schade aan de computer kan veroorzaken. Als u ActiveX wilt blokkeren, schakelt u het selectievakje **ActiveX in**. Als u ActiveX blokkeert, kunt u problemen hebben als u bepaalde internetsites wilt openen die ActiveX gebruiken om uit te voeren.

· Toegang tot Proxy HTTP Server â€” Als u anoniem wilt surfen via een proxyserver en toegang tot de proxyserver ontzeggen, controleer dan het aanvinkvakje **Access to Proxy HTTP Server**. HTTP Proxy Servers verbergen gegevens van eindgebruikers van hackers. Ze werken als tussenpersonen en u hebt dus geen rechtstreekse toegang tot het internet. Als lokale gebruikers echter toegang hebben tot WAN-proxyservers, kunnen ze mogelijk een weg vinden rond de inhoudsfilters op de router en toegang krijgen tot internetsites die door de router worden geblokkeerd.

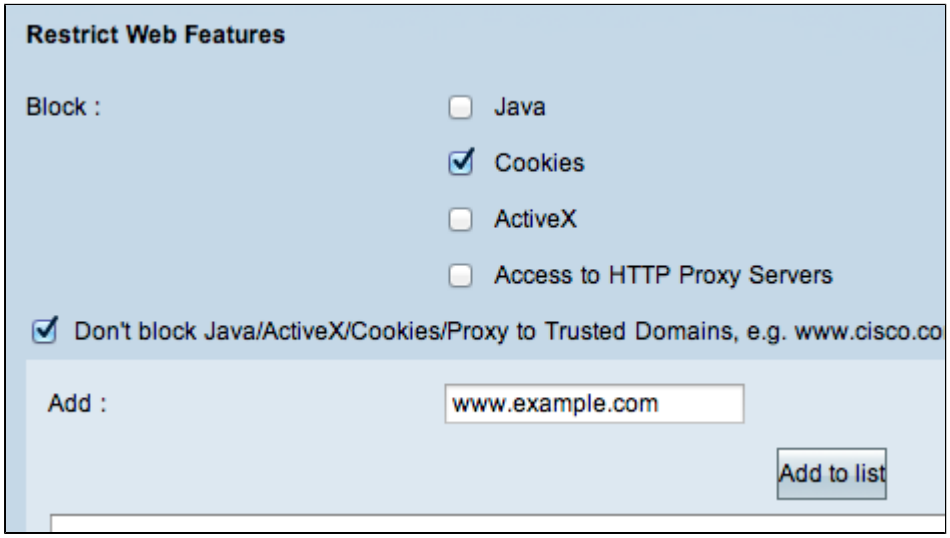
Stap 4. Klik op **Opslaan** om de instellingen op te slaan.

Vertrouwde domeinen toevoegen

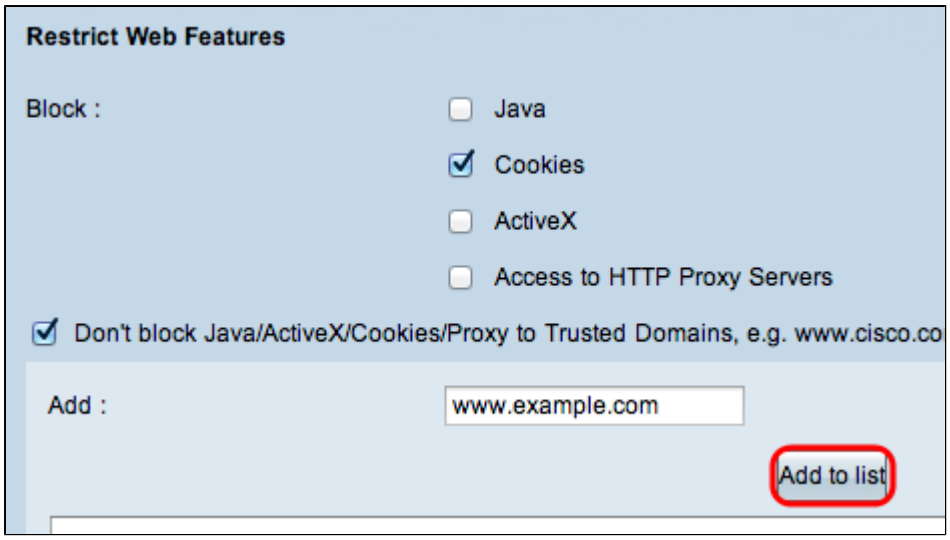
Hoewel een van de webfuncties kan worden geblokkeerd, kan de gebruiker deze functies toch inschakelen voor bepaalde vertrouwde domeinen.



Stap 1. Klik op de knop **Java/ActiveX/Cookies/Proxy to Trusted Domains niet blokkeren**. Deze optie is alleen beschikbaar indien de gebruiker heeft besloten een van de webfuncties in Stap 3 van de *Algemene Firewall-instellingen* te blokkeren.



Stap 2. Voer in het veld *Add* het domein in dat moet worden toegevoegd aan de lijst met vertrouwde domeinen.

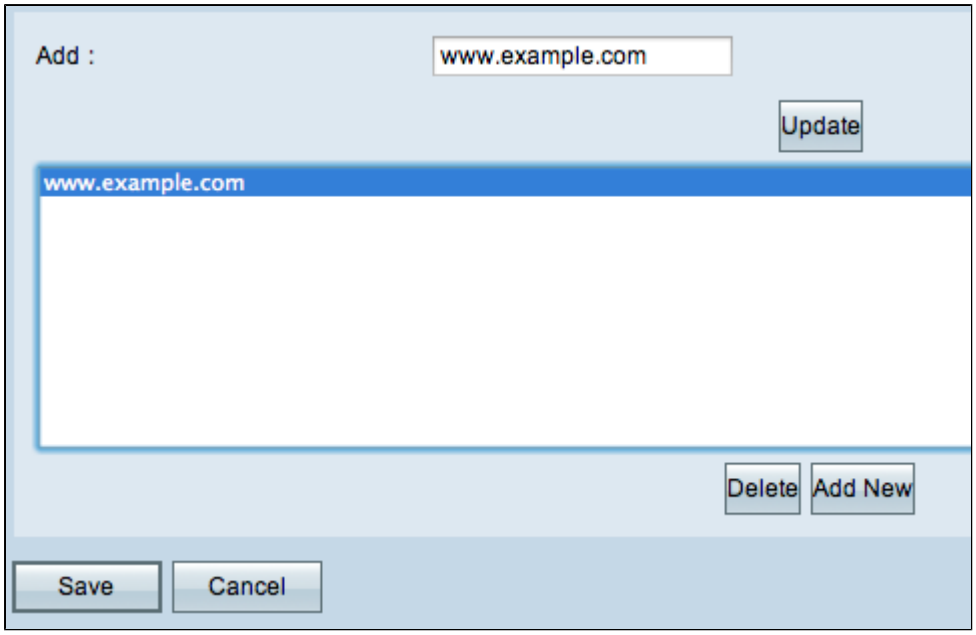


Stap 3. Klik op **Toevoegen aan lijst.** Het domein wordt toegevoegd aan de vertrouwde lijst.

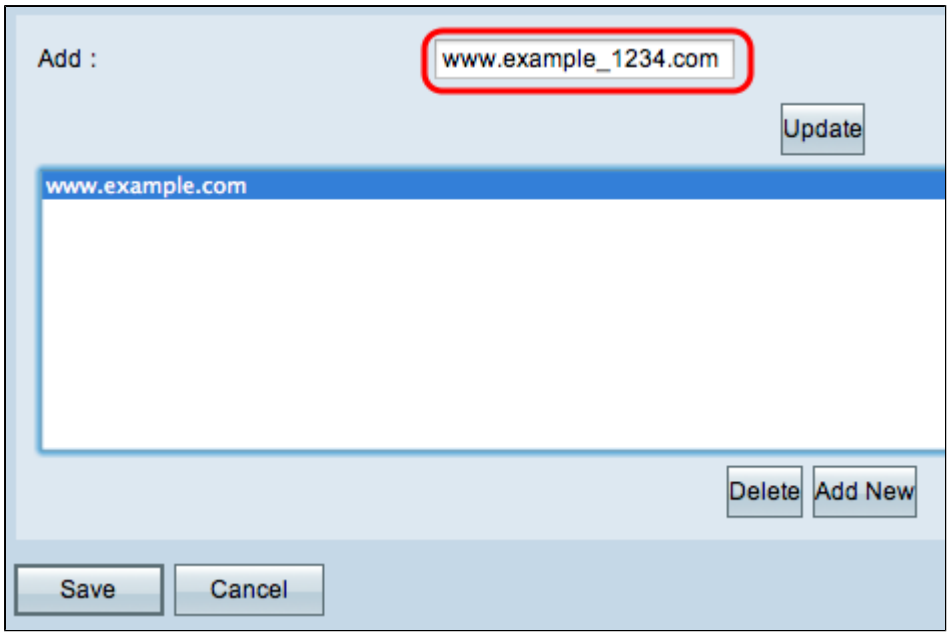
Stap 4. Klik op **Opslaan** om de wijzigingen op te slaan.

Een betrouwbaar domein bijwerken

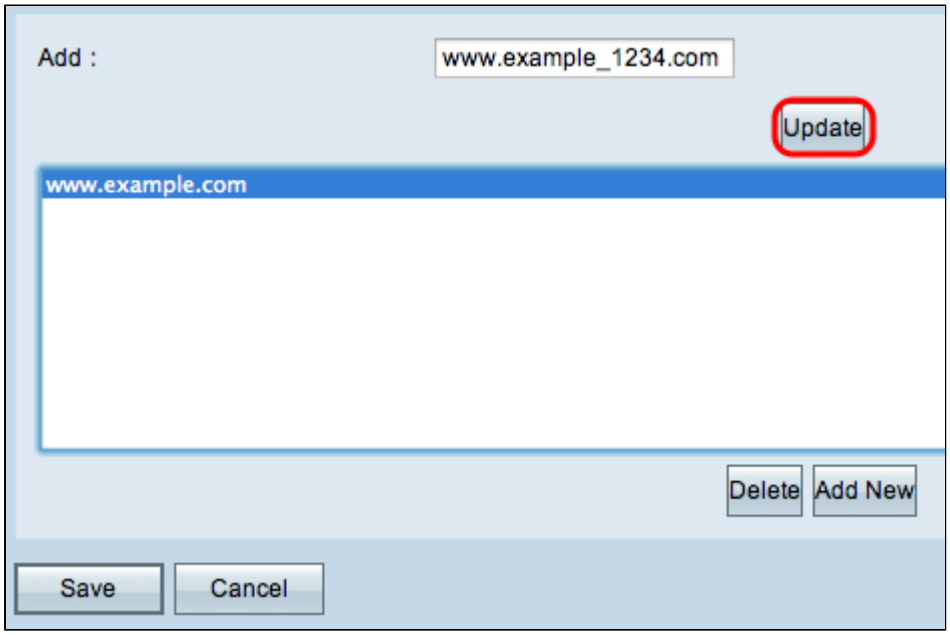
Deze sectie begeleidt de gebruiker hoe een vertrouwd domein te bewerken.



Stap 1. Kies het domein dat u wilt bewerken uit de lijst met vertrouwde domeinen.



Stap 2. Voer in het veld *Add* de bijgewerkte domeinnaam voor het vereiste domein in.

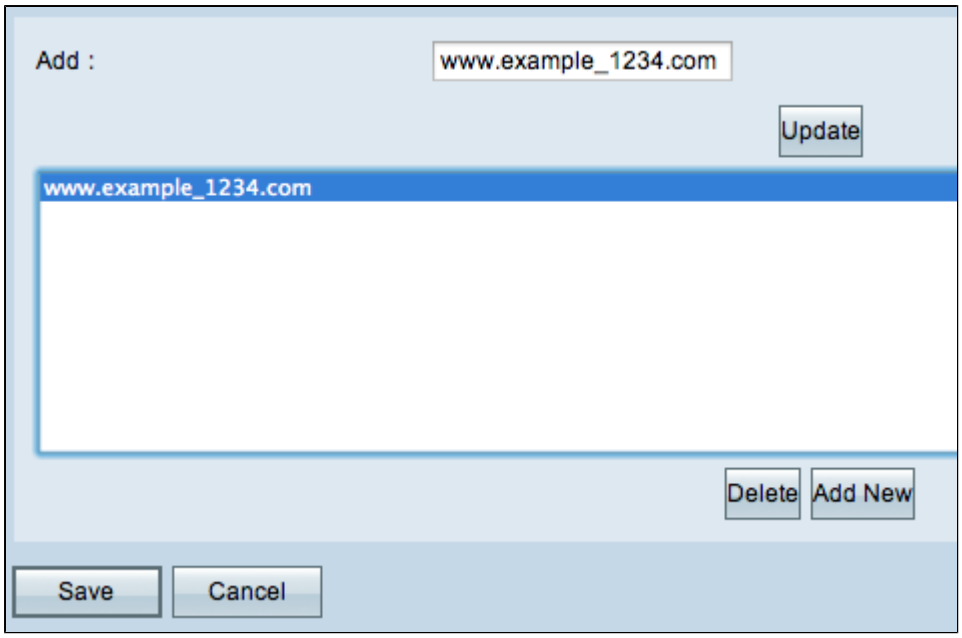


Stap 3. Klik op **Bijwerken**.

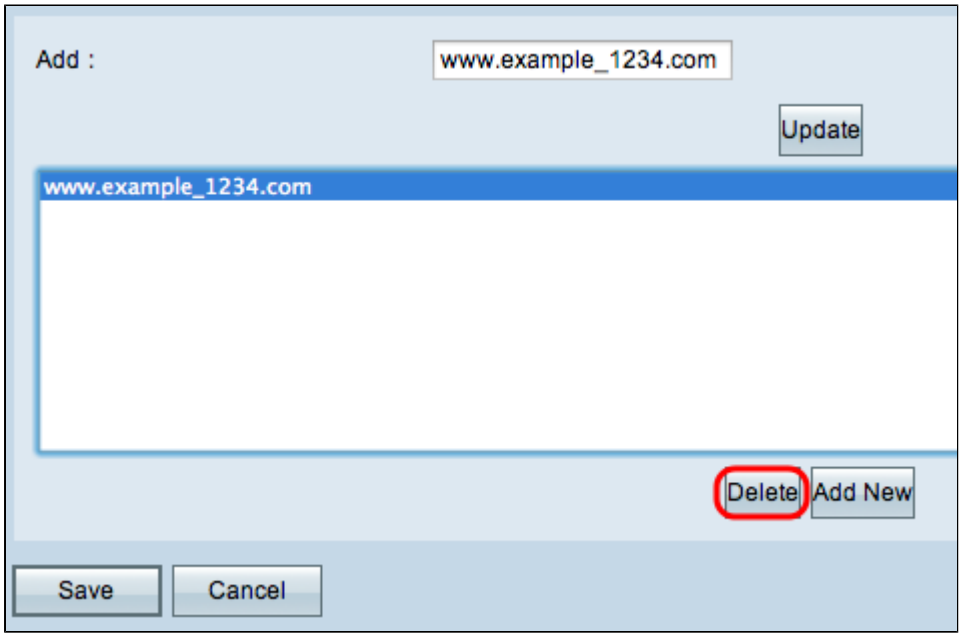
Stap 4. Klik op **Opslaan** om de wijzigingen op te slaan.

Een vertrouwd domein verwijderen

Deze sectie begeleidt de gebruiker hoe een vertrouwd domein te verwijderen.



Stap 1. Kies het domein dat u wilt verwijderen.



Stap 2. Klik op **Verwijderen**. Het domein is verwijderd.

Stap 3. Klik op **Opslaan** om de wijzigingen op te slaan.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.