Algemene firewallinstellingen configureren voor de RV016, RV042, RV042G en RV082

Doel

De ingebouwde firewall voor de RV016, RV042, RV042G en RV082 blokkeert standaard bepaalde soorten verkeer. De soorten verkeer die worden geblokkeerd, zoals HTTPS-, TCP- en ICMP-verzoeken en verkeer voor extern beheer, kunnen worden aangepast. De firewall zelf kan ook worden ingeschakeld of uitgeschakeld. Daarnaast kunnen bepaalde aspecten van websites die kwetsbaarheden op het gebied van beveiliging kunnen zijn, ook worden geblokkeerd. Wanneer deze websitefuncties worden vrijgegeven, kunnen mogelijk schadelijke gegevens op uw computer worden opgeslagen.

Het doel van dit document is om u te laten zien hoe u de algemene firewallinstellingen kunt configureren op de RV016, RV042, RV042G en RV082.

Toepasselijke apparaten

· RV016

â€¢RV042

· RV042G

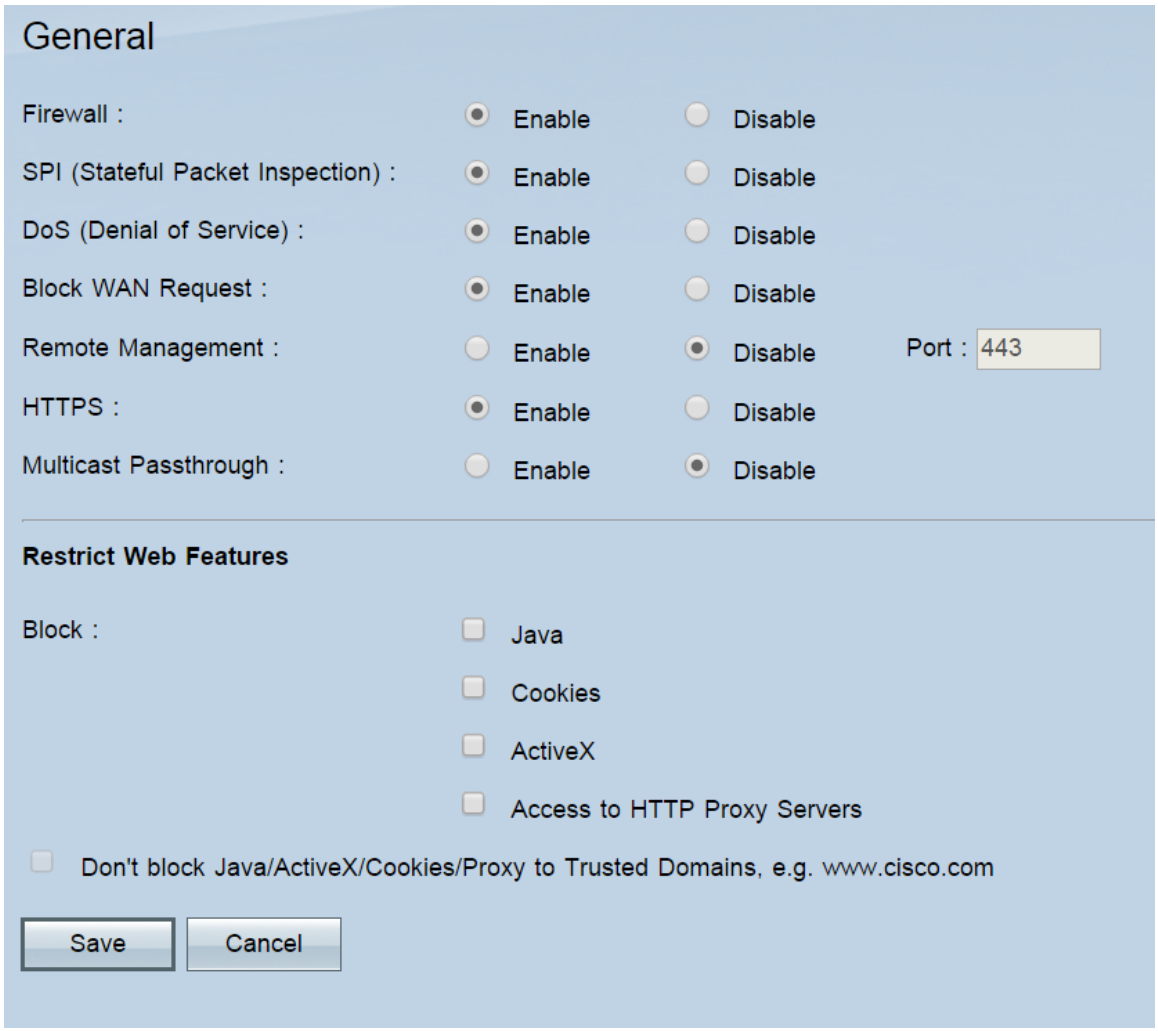
· RV082

Softwareversie

· v4.2.3.06

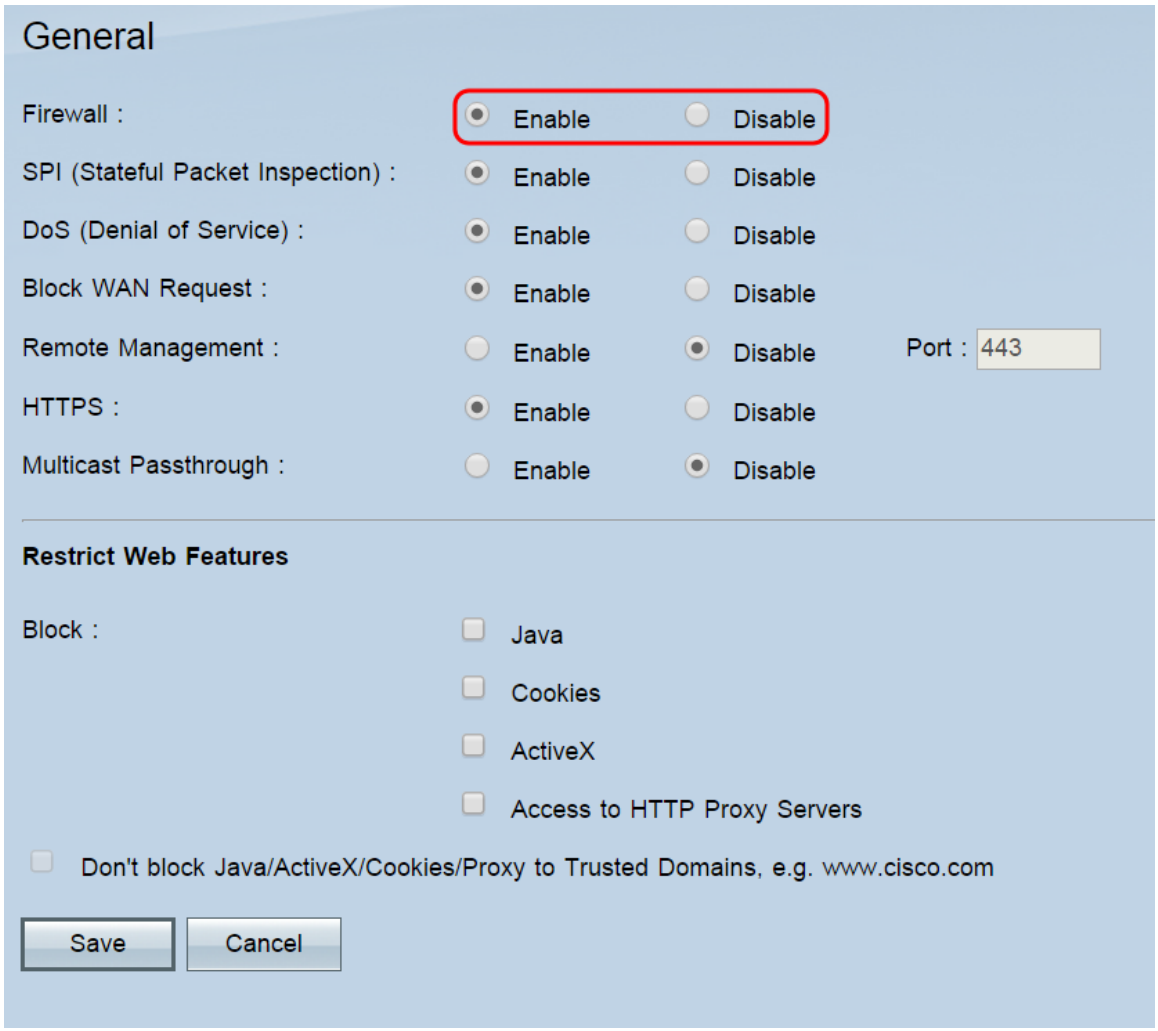
Algemene firewallinstellingen configureren

Stap 1. Log in bij het hulpprogramma voor webconfiguratie en kies **Firewall > Algemeen**. De *pagina Algemeen* wordt geopend.



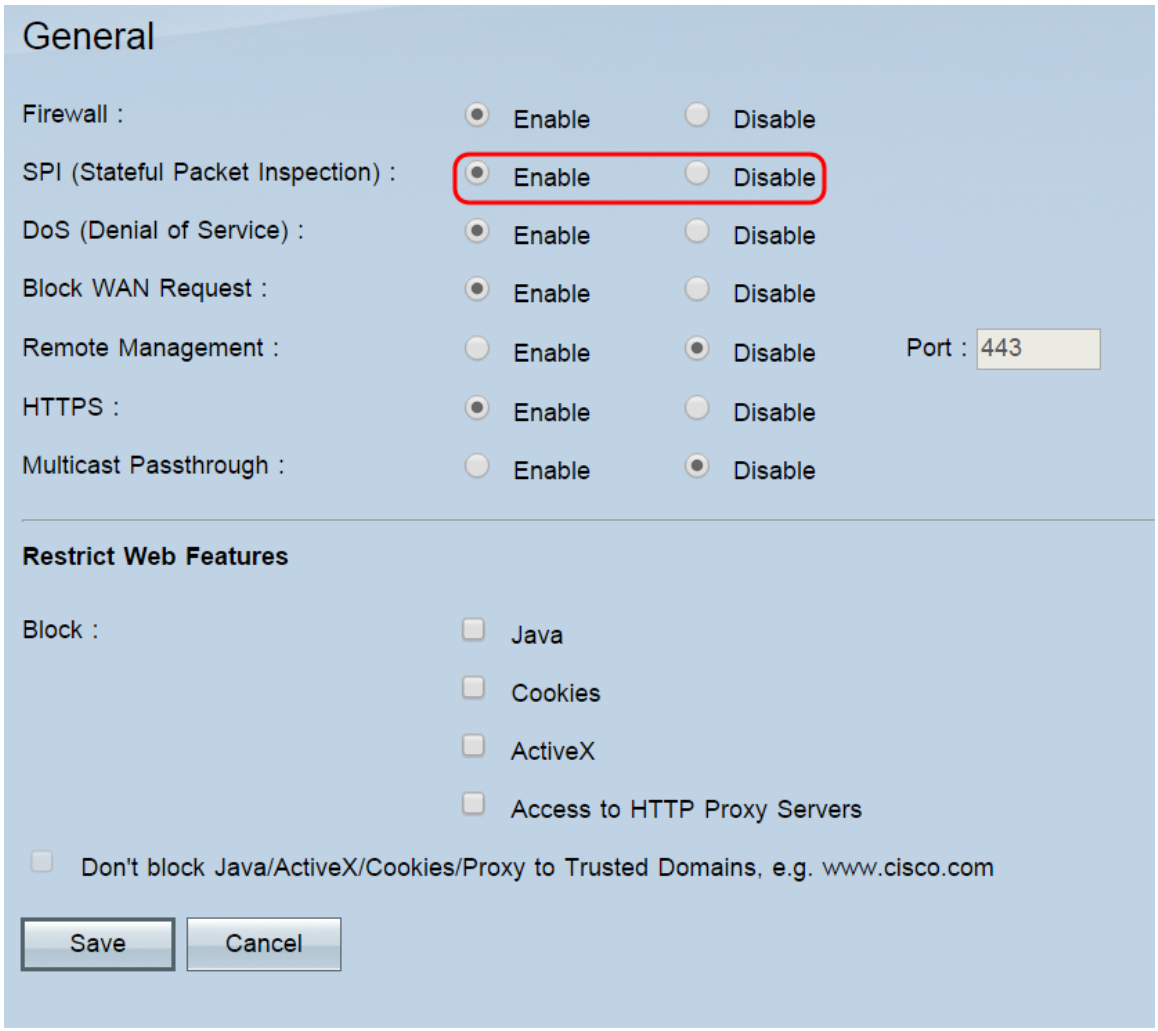
Algemene functies

Stap 1. Selecteer in het veld *Firewall* een keuzerondje om de firewall in te **schakelen** of **uit te schakelen**. De firewall is standaard ingeschakeld; het wordt niet aangeraden de firewall uit te schakelen. Als u de firewall uitschakelt, worden ook toegangsregels en contentfilters uitgeschakeld.

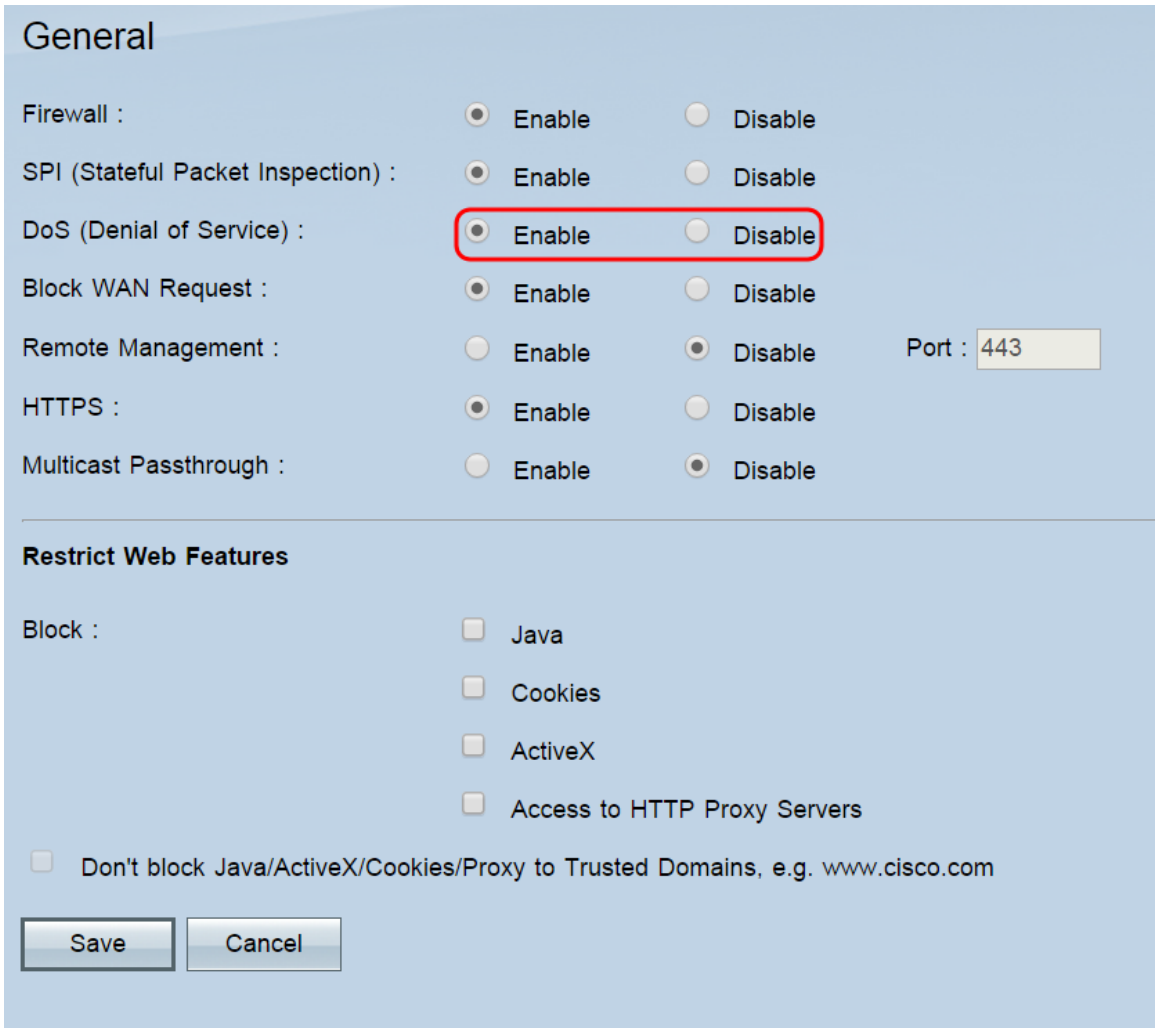


Opmerking: als u de firewall wilt uitschakelen en nog steeds het standaard beheerderswachtwoord gebruikt, verschijnt er een waarschuwing dat u het wachtwoord moet wijzigen; u kunt de firewall pas uitschakelen als u dit doet. Klik op **OK** om door te gaan naar de wachtwoordpagina of op **Annuleren** om op deze pagina te blijven.

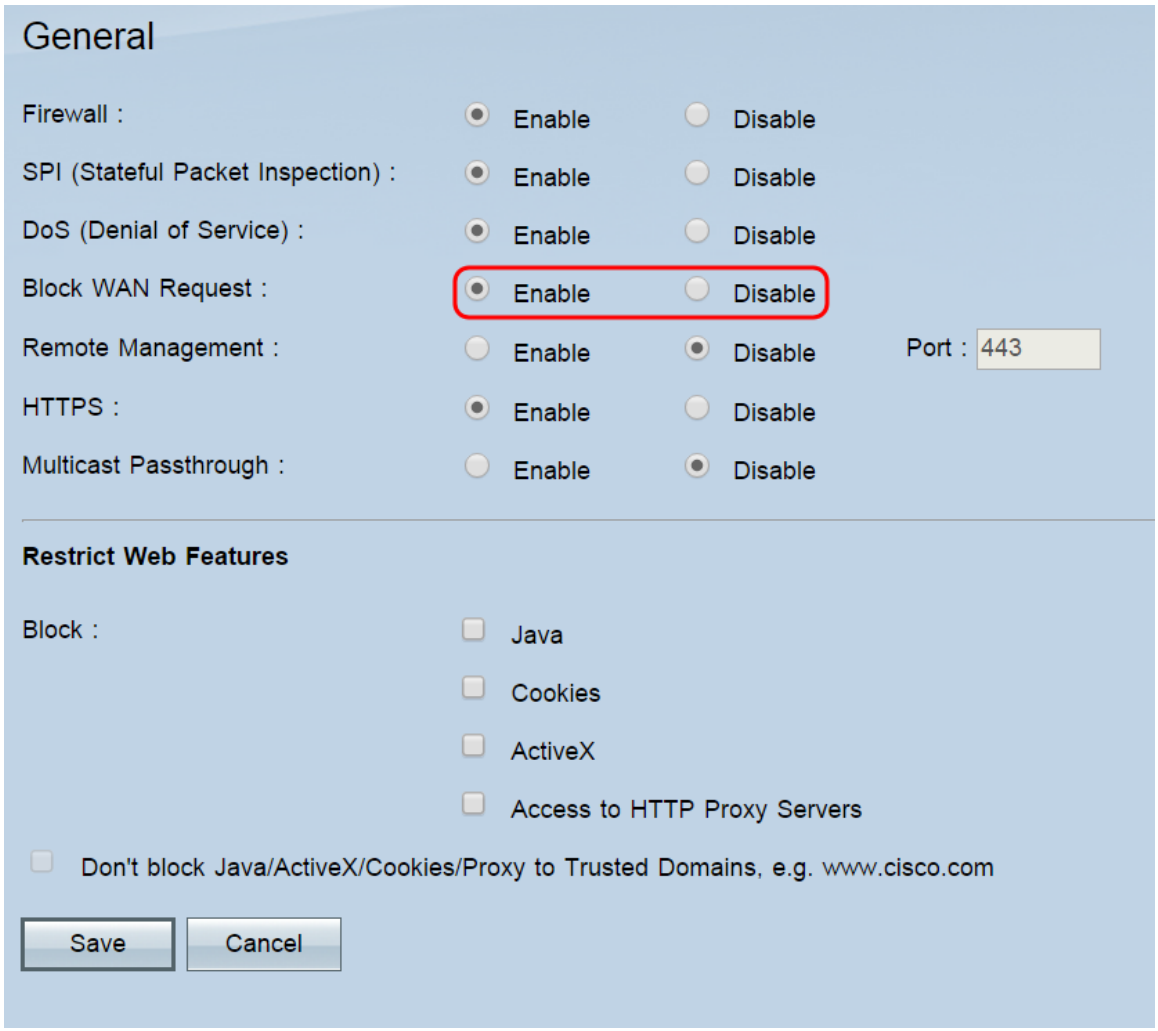
Stap 2. Selecteer in het veld SPI (Stateful Package Inspection) de radioknop **Enable** of **Disable**. SPI is standaard ingeschakeld. Deze eigenschap staat de router toe om alle pakketten te inspecteren alvorens hen te verzenden om worden verwerkt. Dit kan alleen worden ingeschakeld als de firewall is ingeschakeld.



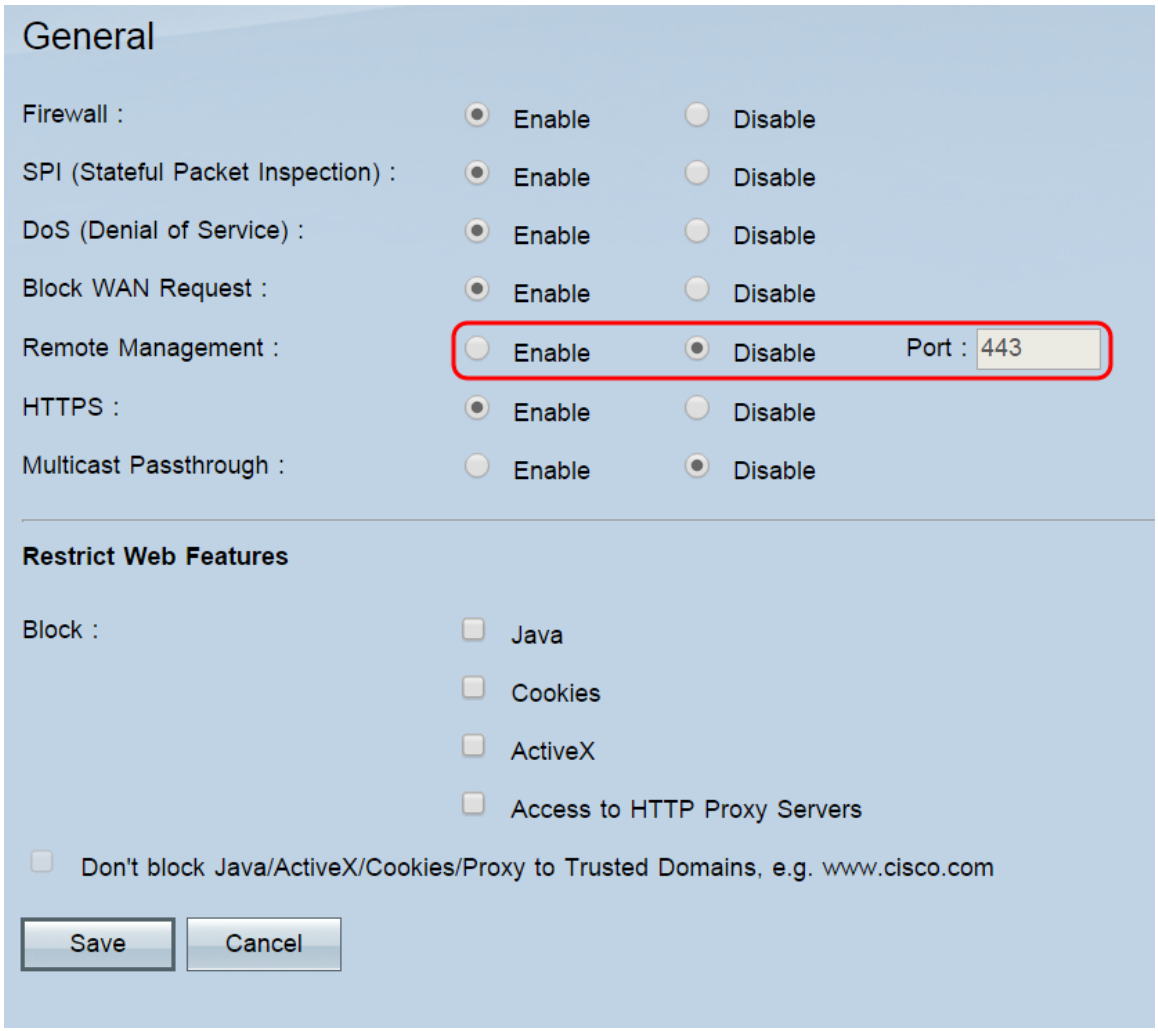
Stap 3. In het veld *DoS (Denial of Service)* selecteert u de keuzerondje **Enable** of **Disable**. DoS is standaard ingeschakeld. Deze functie voorkomt dat het interne netwerk externe aanvallen kan uitvoeren (zoals SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing en hermontage aanvallen). Dit kan alleen worden ingeschakeld als de firewall is ingeschakeld.



Stap 4. Selecteer in het veld *WAN-verzoek blokkeren* de radioknop **Inschakelen** of **Uitschakelen**. De aanvraag voor WAN-blokkering is standaard ingeschakeld. Deze eigenschap laat de router onaanvaarde TCP en ICMP verzoeken van WAN laten vallen, die hackers verhinderen de router te vinden door het IP van WAN adres te pingelen. Dit kan alleen worden ingeschakeld als de firewall is ingeschakeld.



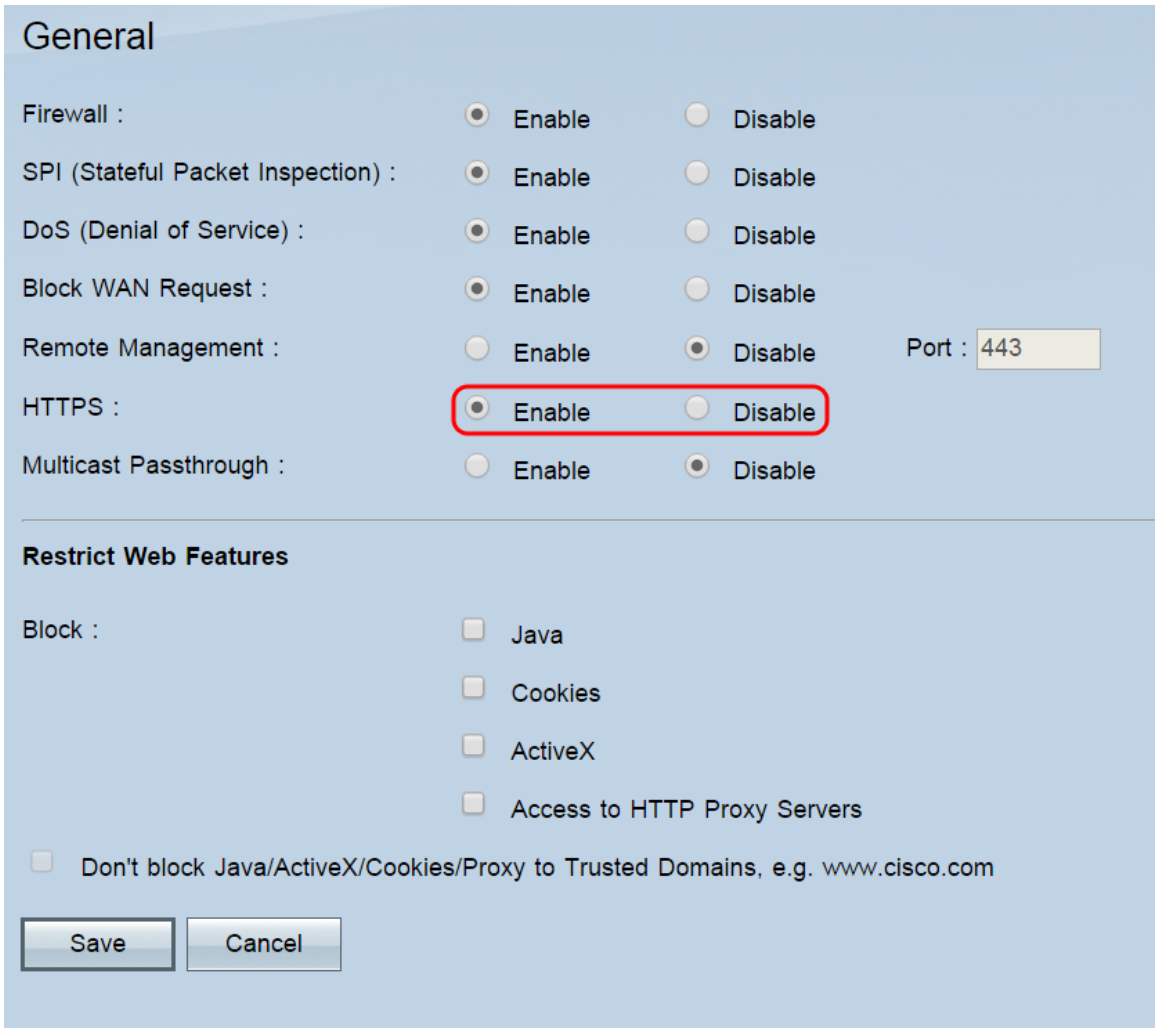
Stap 5. Selecteer in het veld *Beheer op afstand* de knop **Inschakelen** of **Uitschakelen**. Remote Management is standaard uitgeschakeld. Deze eigenschap staat u toe om met het nut van de het Webconfiguratie van de router van overal op Internet te verbinden. Als u deze functie inschakelt, kunt u de poort voor externe verbindingen instellen in het veld Port. De standaardwaarde is 443.



Opmerking: als u het standaardbeheerderswachtwoord gebruikt, verschijnt er een bericht met de waarschuwing dat u het wachtwoord moet wijzigen; klik op **OK** om door te gaan naar de wachtwoordpagina of **Annuleren** om op deze pagina te blijven. Verandering van het wachtwoord is noodzakelijk om onbevoegde gebruikers te verhinderen de router met het standaardwachtwoord toegang te hebben.

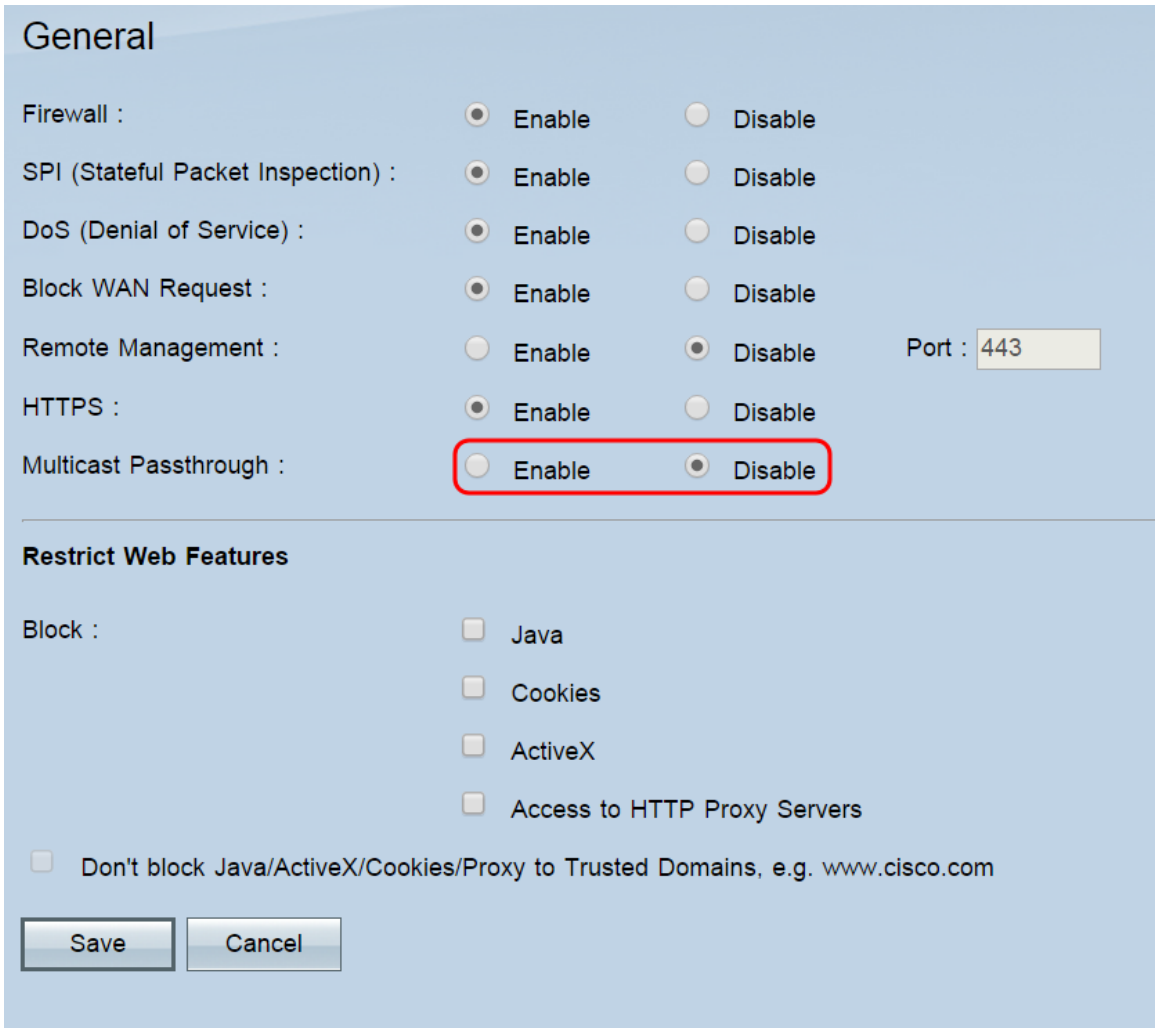
N.B.: Als extern beheer is ingeschakeld, kunt u het hulpprogramma voor webconfiguratie vanuit elke browser benaderen door **http://<WAN IP-adres van de router>:<poort>** in te voeren. Als HTTPS is ingeschakeld, voert u in plaats daarvan **https://<WAN IP-adres van de router><port>in**.

Stap 6. Selecteer in het veld *HTTPS* de keuzerondje **Inschakelen** of **Uitschakelen**. HTTPS is standaard ingeschakeld. Deze eigenschap staat veilige HTTP-sessies toe.



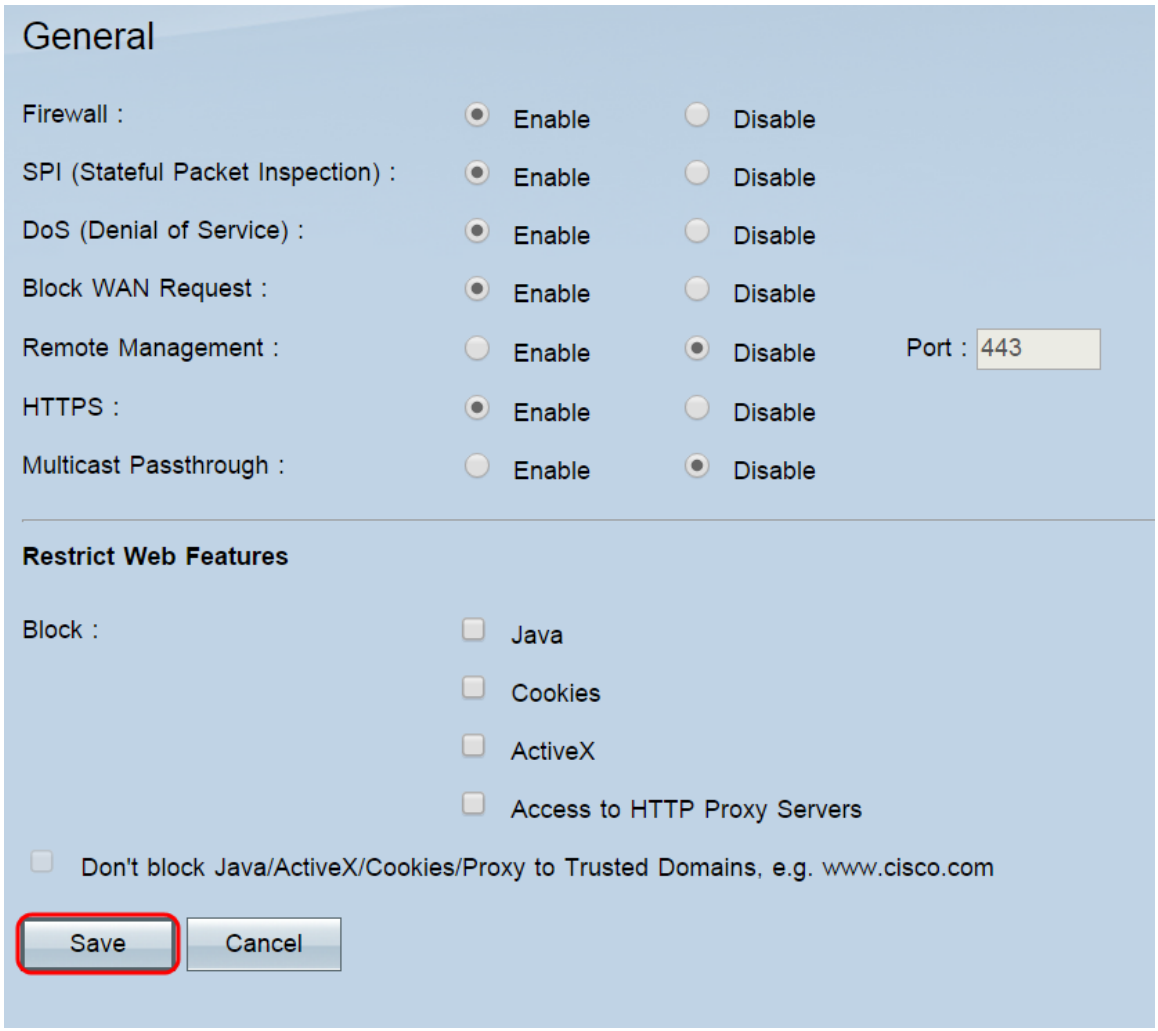
Opmerking: als deze functie is uitgeschakeld, kunnen gebruikers geen verbinding maken met QuickVPN.

Stap 7. Selecteer in het veld *Multicast-passthrough* de keuze **Inschakelen** of **Uitschakelen**. Multicast-passthrough is standaard uitgeschakeld. Deze eigenschap laat IP multicast pakketten toe om aan hun overeenkomstige LAN apparaten worden uitgezonden, en wordt gebruikt voor de spelen van Internet, videoconferencing, en toepassingen van verschillende media.



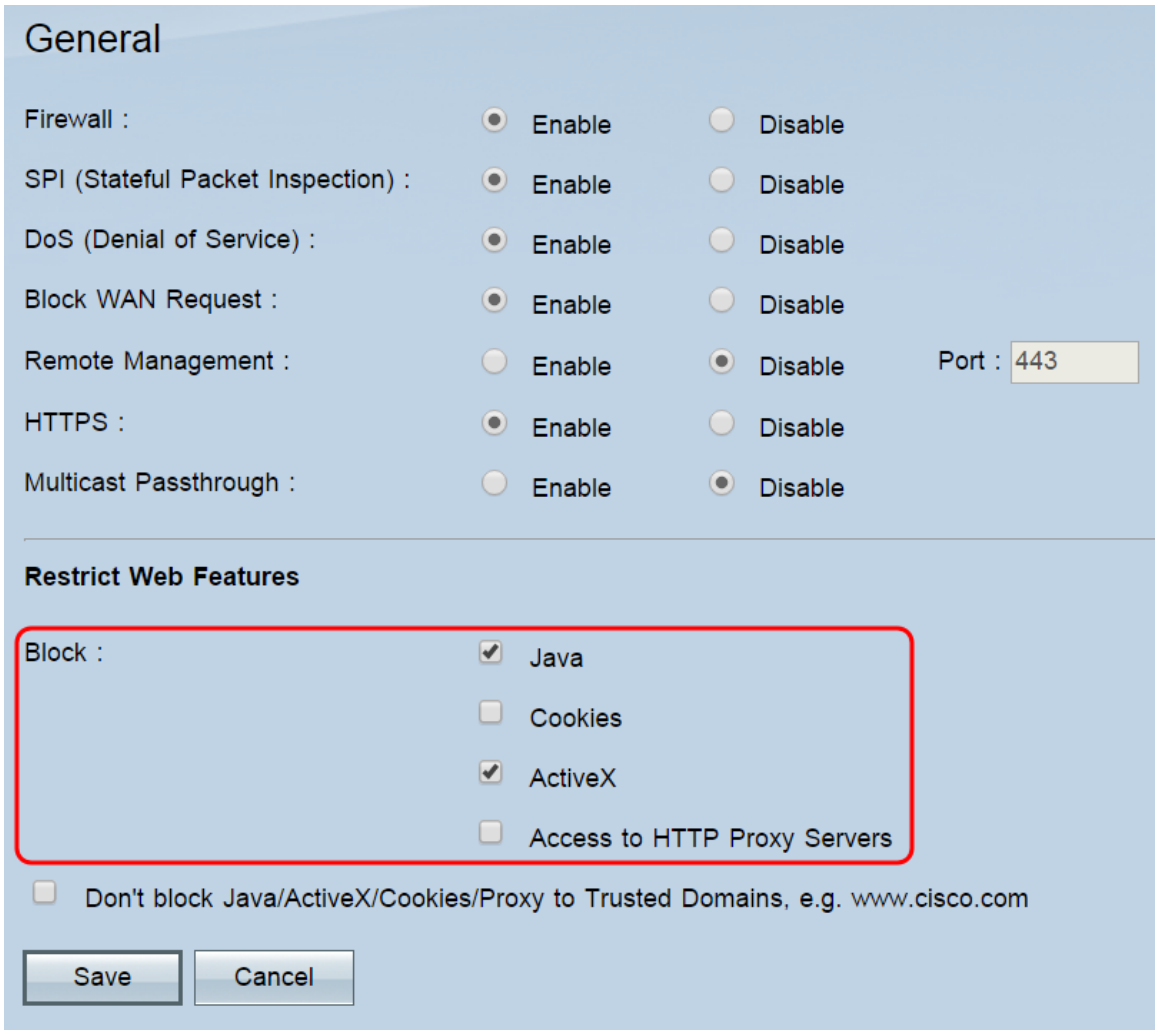
Opmerking: de RV016, RV042, RV042G en RV082 ondersteunen geen multicast-verkeer via een IPSec-tunnel.

Stap 8. Klik op **Save** (Opslaan).



Webfuncties

Stap 1. Selecteer in het veld *Blokkeren* de selectievakjes van de webfuncties die u wilt blokkeren bij de firewall. Als u geblokkeerde functies voor bepaalde domeinen wilt toestaan, kunnen die domeinen worden toegevoegd aan een uitzonderingslijst in Stap 2. Geen van de functies is standaard geblokkeerd.



De opties zijn:

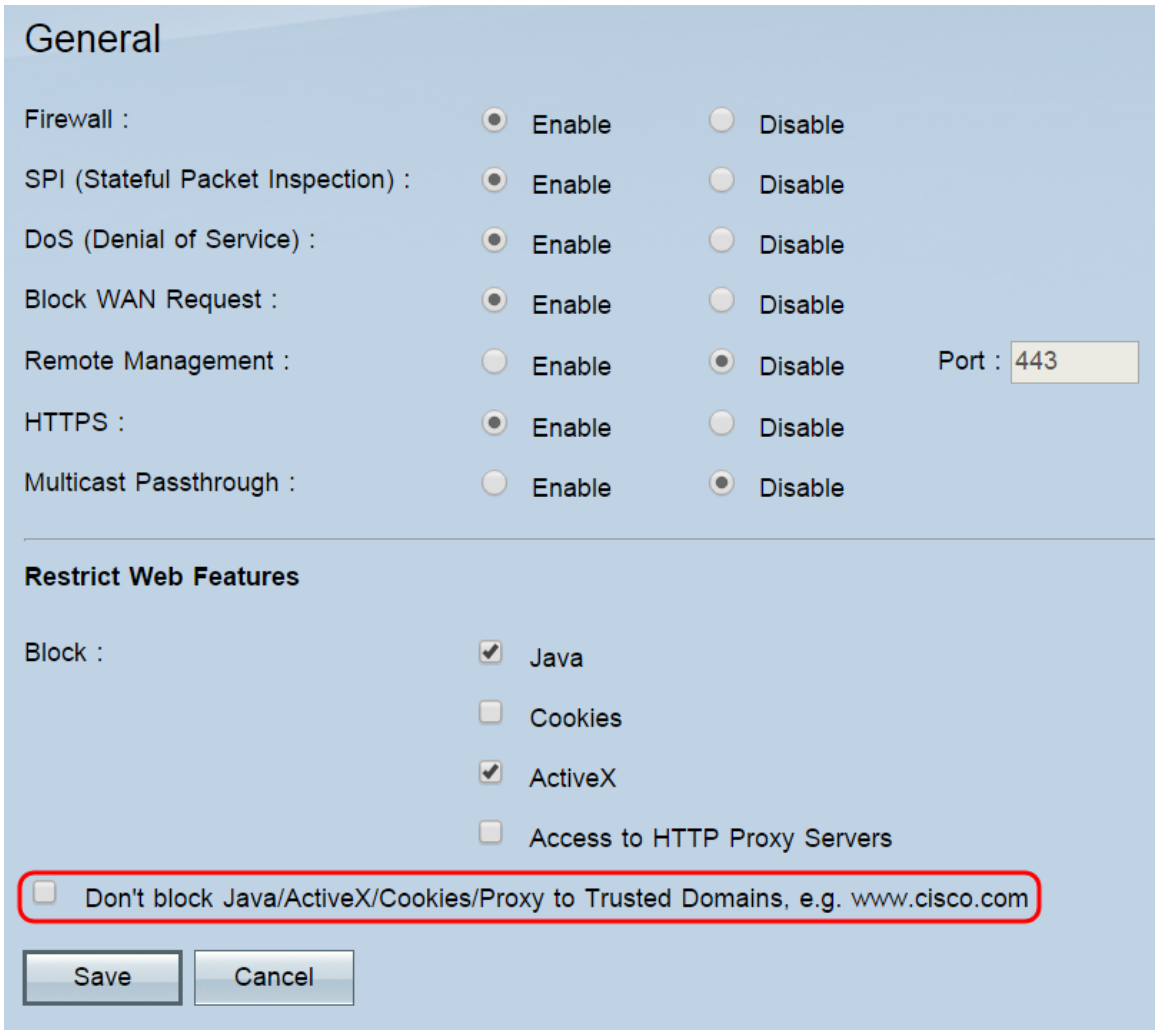
· Java â€" Java is een programmeertaal voor websites. Als u dit selectievakje inschakelt, worden Java-applets geblokkeerd (kleine programma's die in webpagina's zijn ingesloten maar buiten de webbrowser worden uitgevoerd), maar het kan ervoor zorgen dat websites die deze functie gebruiken, niet correct werken.

· Cookies â€" Een cookie is gegevens die een website lokaal op de pc van een gebruiker opslaat. Het blokkeren van cookies kan ertoe leiden dat websites die erop vertrouwen zich onjuist gedragen.

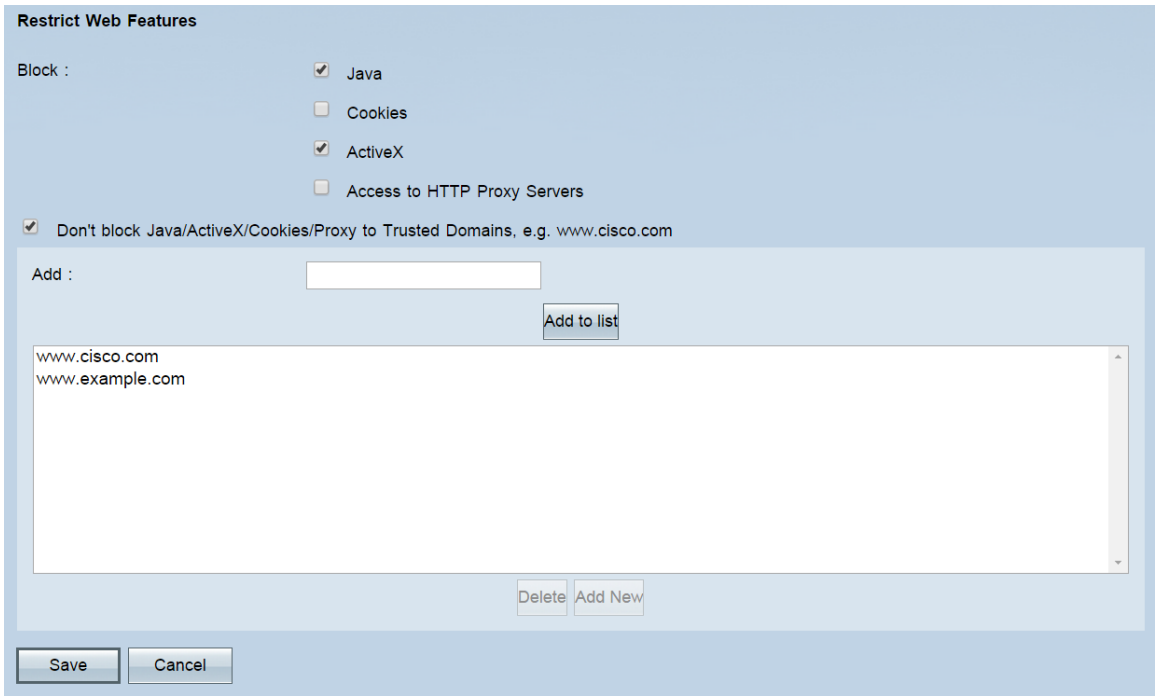
ActiveX â€" ActiveX is een softwareframework dat door Microsoft is ontwikkeld. Dit kader kan worden gebruikt om bepaalde delen van webpagina's uit te voeren. Als u dit selectievakje aanvinkt, worden deze componenten geblokkeerd, maar kunnen websites die ActiveX gebruiken, hierdoor onjuist functioneren.

· Toegang tot HTTP Proxy servers â€" Vink dit vakje aan als u toegang tot HTTP proxy servers wilt blokkeren. Het gebruik van WAN-proxyservers kan de beveiliging van de router in gevaar brengen.

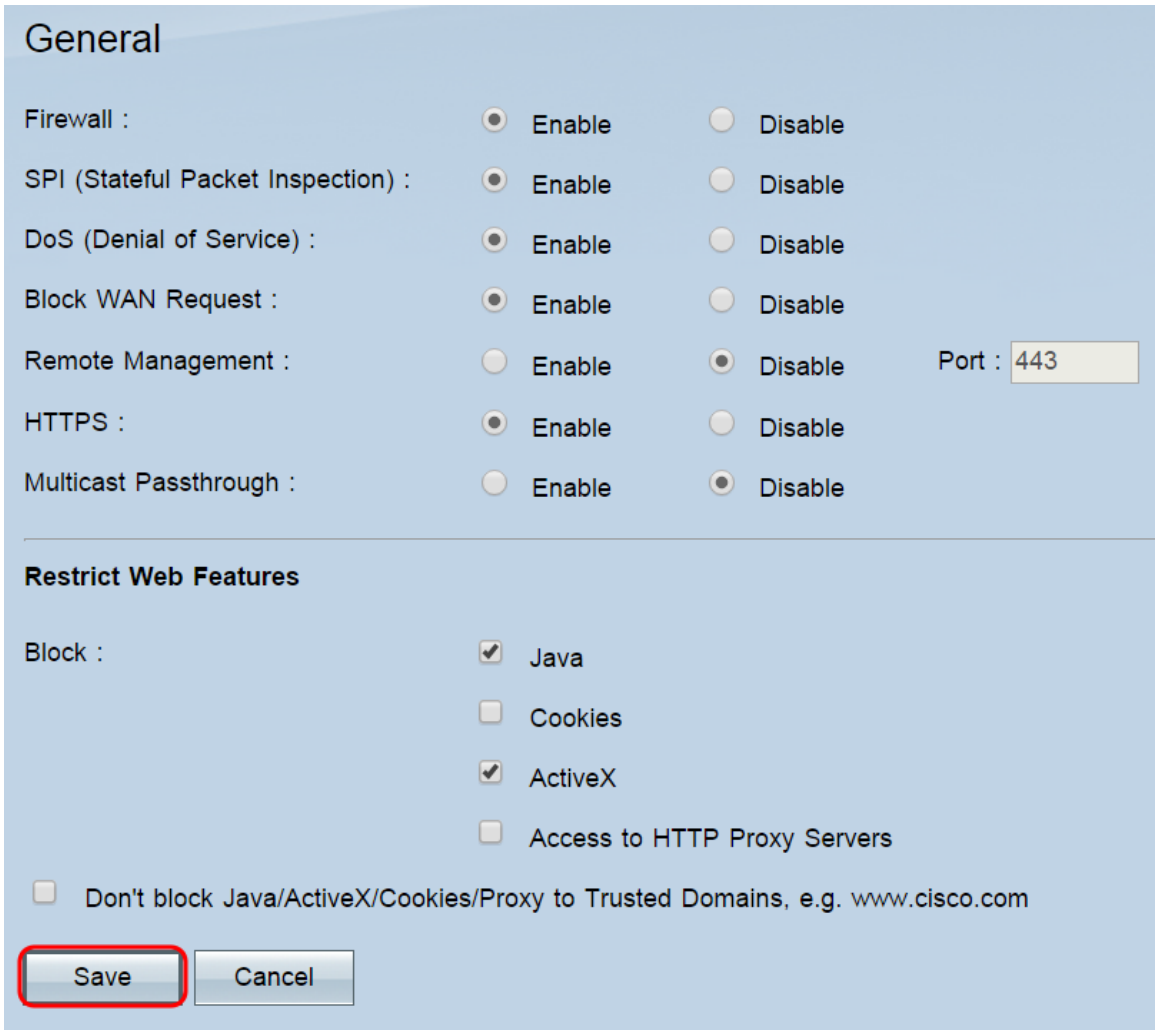
Stap 2. Schakel het selectievakje **Java/ActiveX/Cookies/Proxy niet blokkeren naar Trusted Domains in** om de lijst met vertrouwde domeinen te openen, waar u domeinen kunt toevoegen of verwijderen waar geblokkeerde webfuncties zijn toegestaan. Dit veld is standaard niet ingeschakeld en is alleen beschikbaar als u een vorig vakje hebt ingeschakeld om een functie te blokkeren. Indien niet ingeschakeld, worden de functies geblokkeerd voor alle websites.



Stap 3. (Optioneel) Als u het selectievakje **Java/ActiveX/Cookies/Proxy to Trusted Domains** hebt ingeschakeld, verschijnt er een lijst met vertrouwde domeinen. Als u een domein aan de lijst wilt toevoegen, voert u het in het veld *Toevoegen in* en klikt u op **Toevoegen aan lijst**. Als u een bestaand domein wilt wijzigen, klikt u op het domein in de lijst, vervolgens bewerkt u het in het veld *Toevoegen* en klikt u vervolgens op **Bijwerken**. Als u een domein uit de lijst wilt verwijderen, klikt u op het domein in de lijst en vervolgens klikt u op **Verwijderen**.



Stap 4. Klik op **Save** (Opslaan).



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.