Configurare le impostazioni generali del firewall su RV016, RV042, RV042G e RV082

Obiettivo

Per impostazione predefinita, il firewall incorporato per RV016, RV042, RV042G e RV082 blocca alcuni tipi di traffico. È possibile modificare i tipi di traffico bloccati, ad esempio le richieste HTTPS, TCP e ICMP, e il traffico di gestione remota. Il firewall stesso può essere attivato o disattivato. Inoltre, alcuni aspetti dei siti web che possono essere vulnerabilità della sicurezza possono anche essere bloccati. Queste funzionalità del sito Web, se sbloccate, possono memorizzare dati potenzialmente dannosi nel computer.

Lo scopo di questo documento è quello di mostrare come configurare le impostazioni generali del firewall su RV016, RV042, RV042G e RV082.

Dispositivi interessati

· RV016

RV042

RV042G

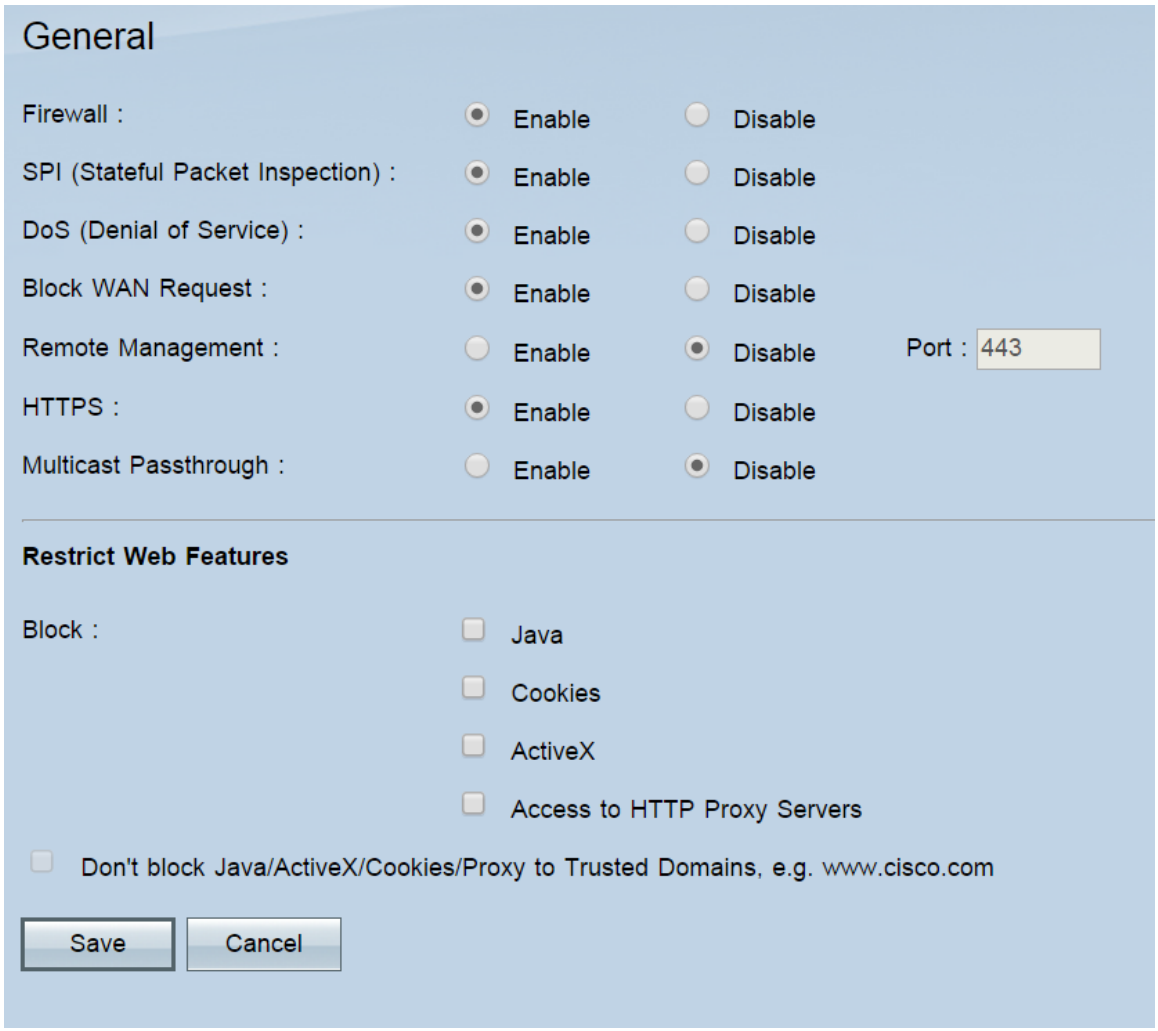
RV082

Versione del software

· v4.2.3.06

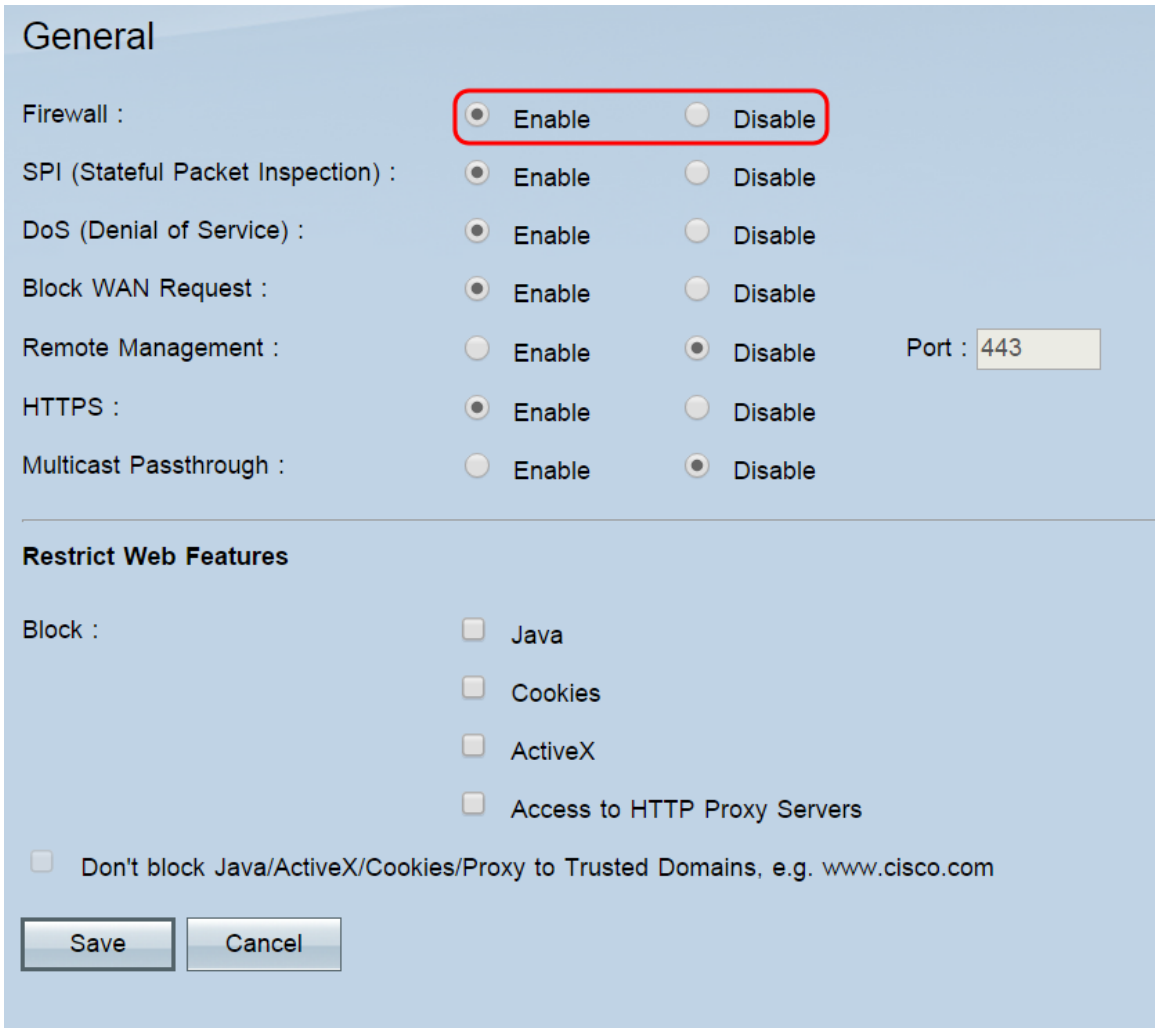
Configurazione delle impostazioni generali del firewall

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Firewall > Generale**. Viene visualizzata la pagina *Generale*.



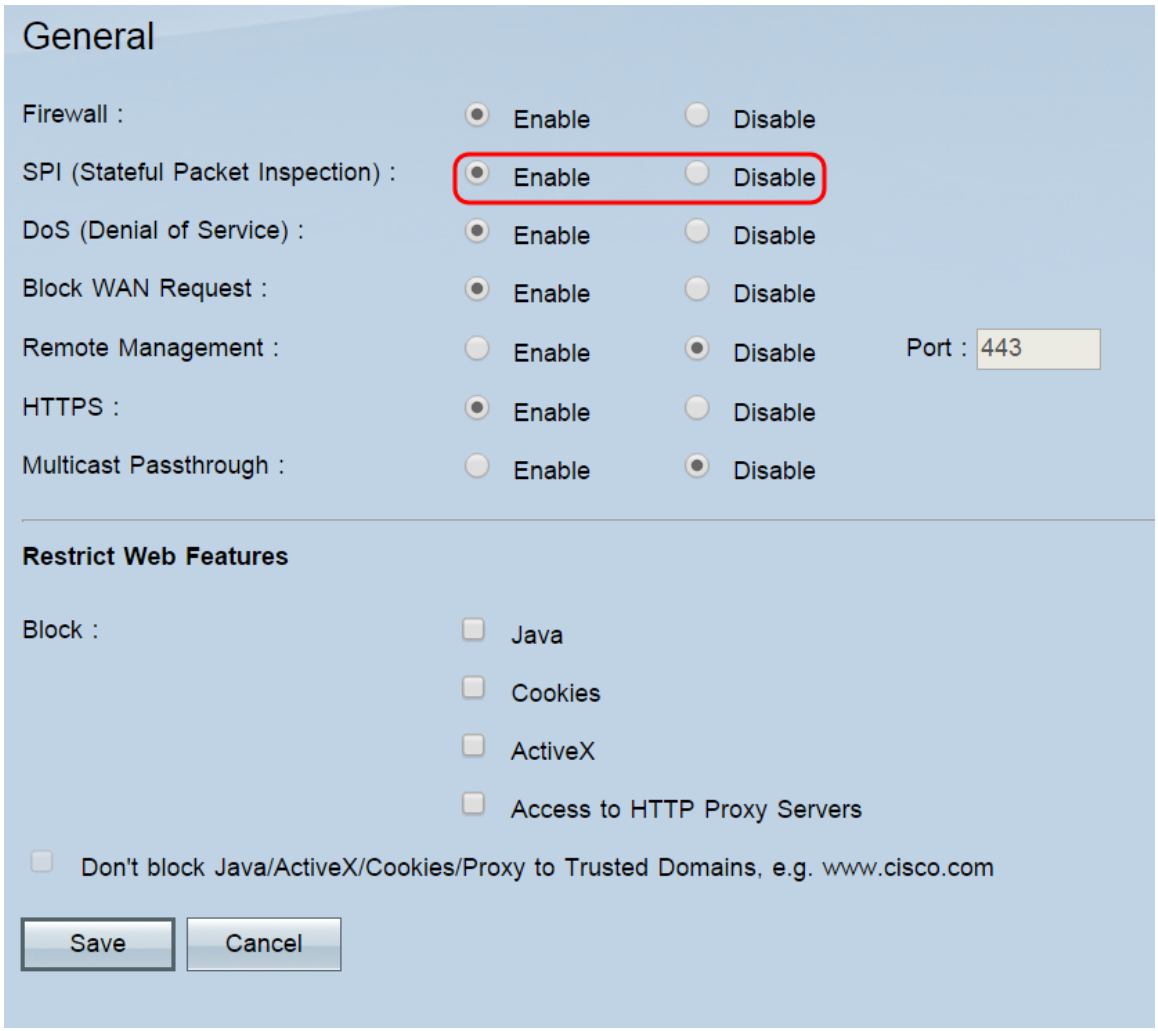
Caratteristiche generali

Passaggio 1. Nel campo *Firewall*, selezionare un pulsante di opzione per **abilitare** o **disabilitare** il firewall. Il firewall è attivato per impostazione predefinita; la disattivazione non è consigliata. La disattivazione del firewall disattiva anche le regole di accesso e i filtri contenuti.

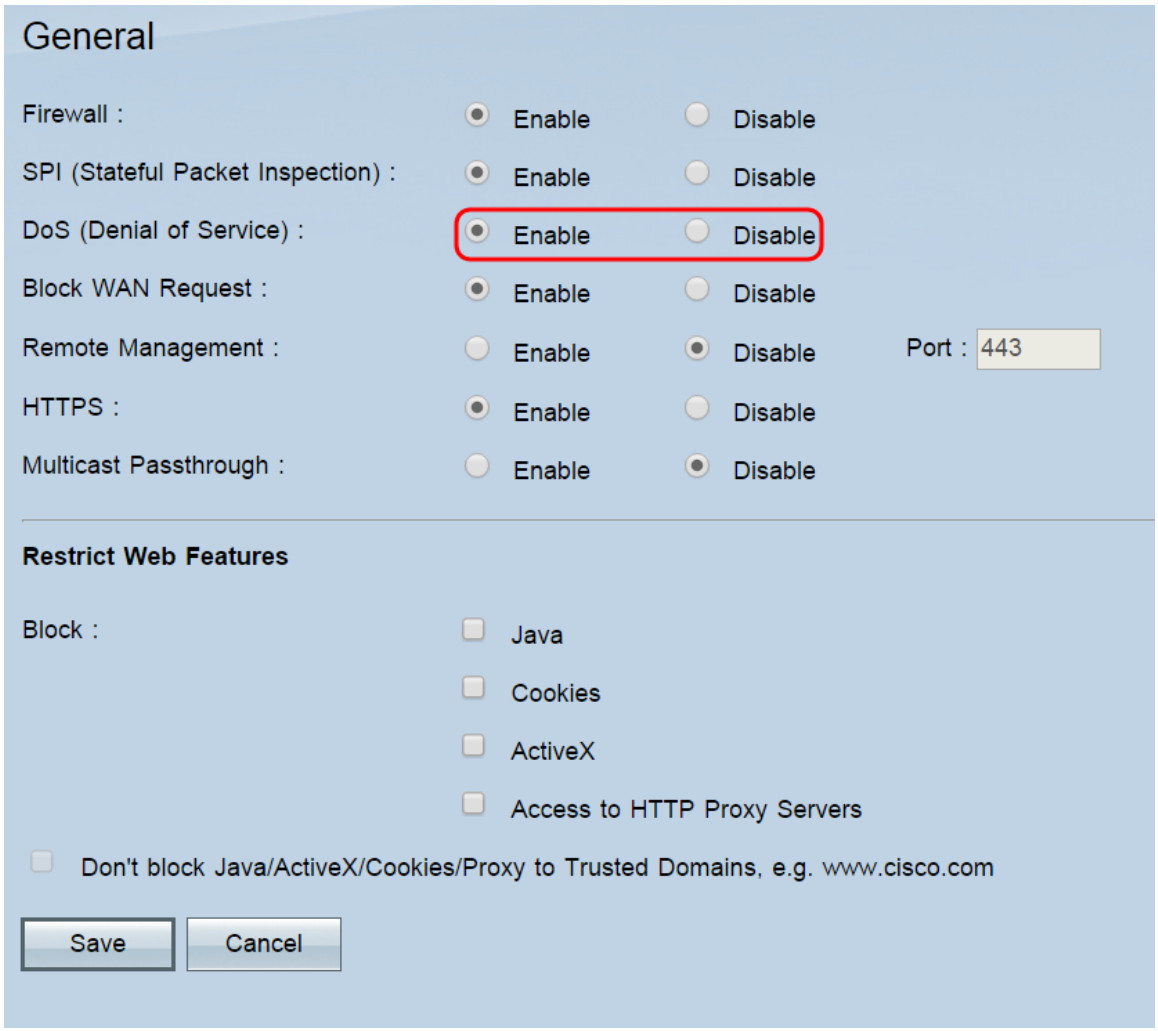


Nota: se si desidera disattivare il firewall e si utilizza ancora la password predefinita dell'amministratore, verrà visualizzato un messaggio che avverte della necessità di modificare la password. In questo caso, non sarà possibile disattivare il firewall. Fare clic su **OK** per passare alla pagina della password o su **Annulla** per rimanere in questa pagina.

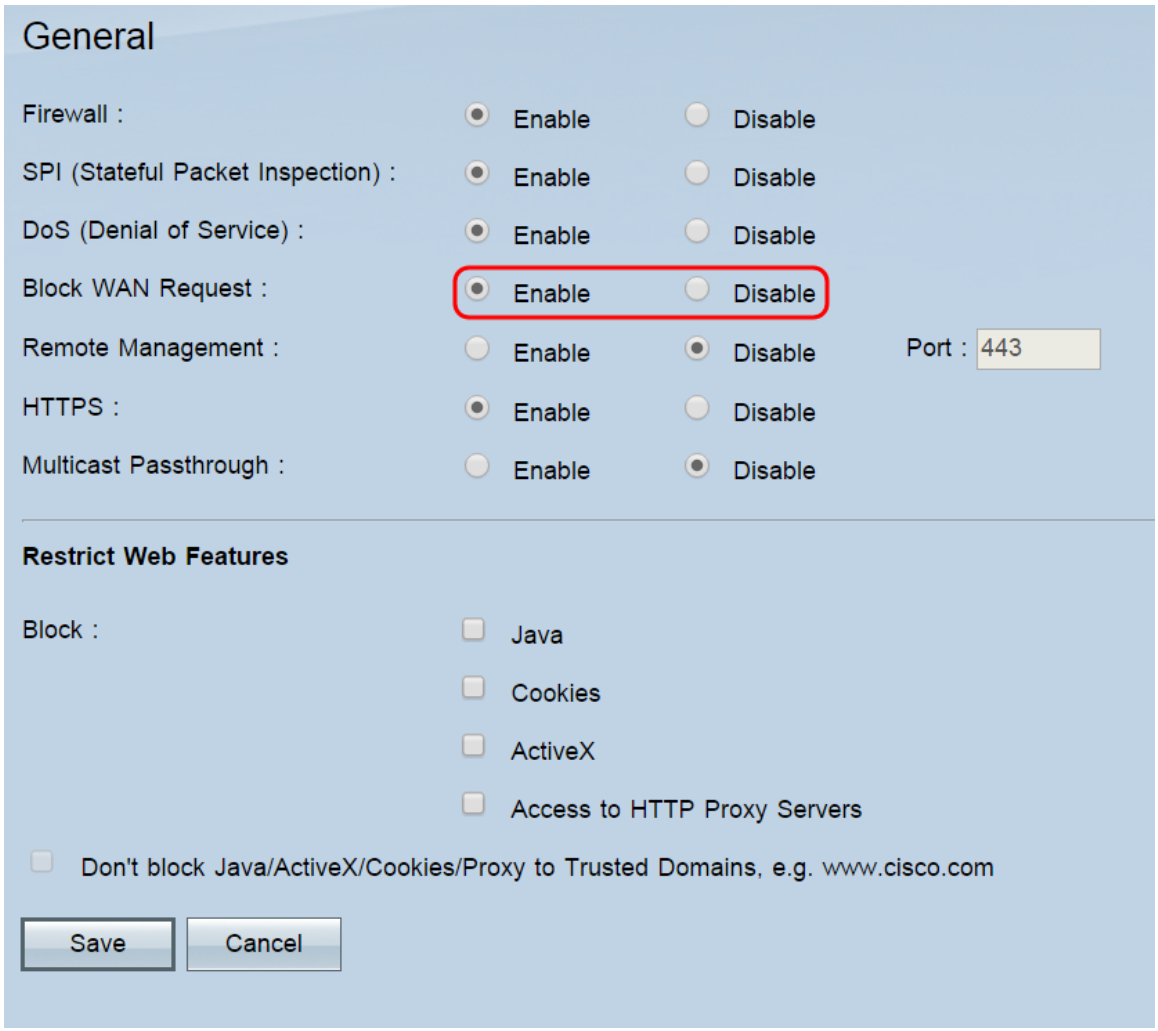
Passaggio 2. In SPI (Stateful Package Inspection), selezionare il pulsante di opzione **Enable** (Abilita) o **Disable** (Disabilita). L'interfaccia SPI è attivata per impostazione predefinita. Questa funzione consente al router di ispezionare tutti i pacchetti prima di inviarli per l'elaborazione. Questa opzione può essere attivata solo se il firewall è attivato.



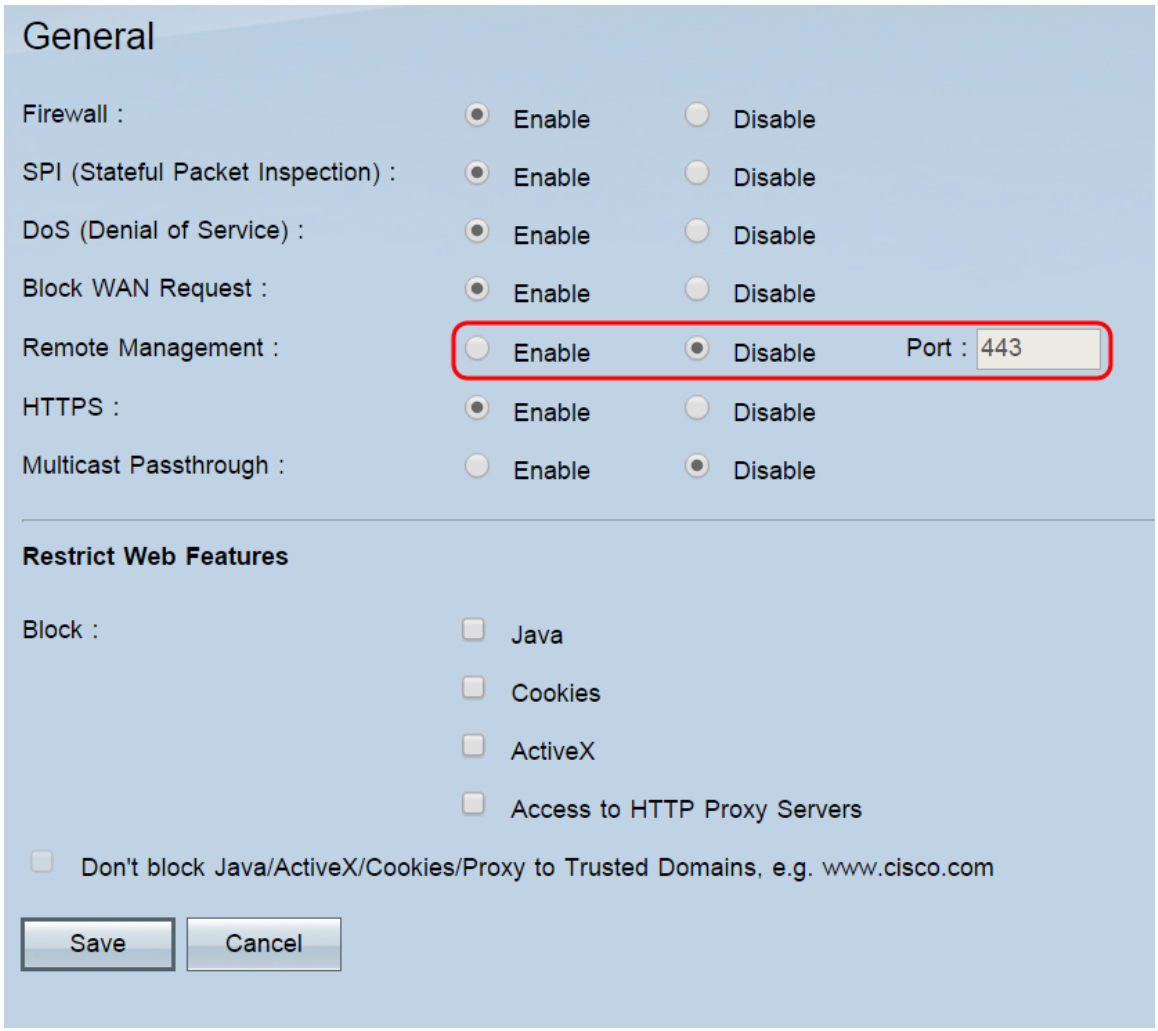
Passaggio 3. Nel campo *DoS (Denial of Service)*, selezionare il pulsante di scelta **Abilita** o **Disabilita**. DoS è attivato per impostazione predefinita. Questa funzione impedisce alla rete interna di attacchi esterni (come SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing e attacchi di riassemblaggio). Questa opzione può essere attivata solo se il firewall è attivato.



Passaggio 4. Nel campo *Blocca richiesta WAN*, selezionare il pulsante di scelta **Abilita** o **Disabilita**. La richiesta di blocco WAN è abilitata per impostazione predefinita. Questa funzione consente al router di eliminare le richieste TCP e ICMP non accettate dalla WAN, impedendo agli hacker di trovare il router eseguendo il ping dell'indirizzo IP della WAN. Questa opzione può essere attivata solo se il firewall è attivato.



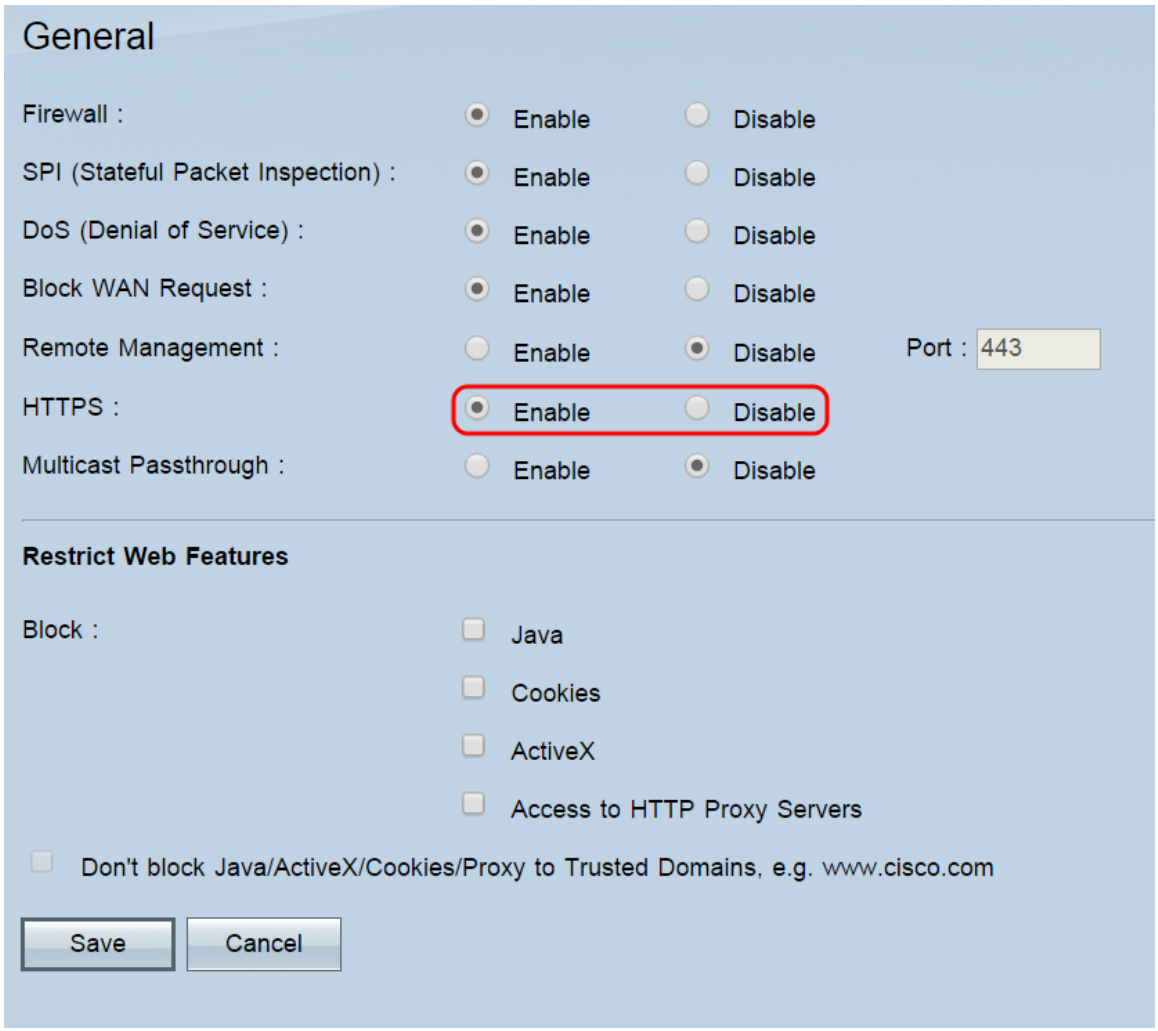
Passaggio 5. Nel campo *Gestione remota*, selezionare il pulsante di opzione **Abilita** o **Disabilita**. Gestione remota è disabilitata per impostazione predefinita. Questa funzione consente di connettersi all'utility di configurazione Web del router da qualsiasi posizione su Internet. Se si attiva questa funzione, è possibile impostare la porta utilizzata per le connessioni remote nel campo Porta. Il valore predefinito è 443.



Nota: se si utilizza la password predefinita dell'amministratore, verrà visualizzato un messaggio che avverte della necessità di modificare la password. Fare clic su **OK** per passare alla pagina della password oppure su **Annulla** per rimanere in questa pagina. La modifica della password è necessaria per impedire agli utenti non autorizzati di accedere al router con la password predefinita.

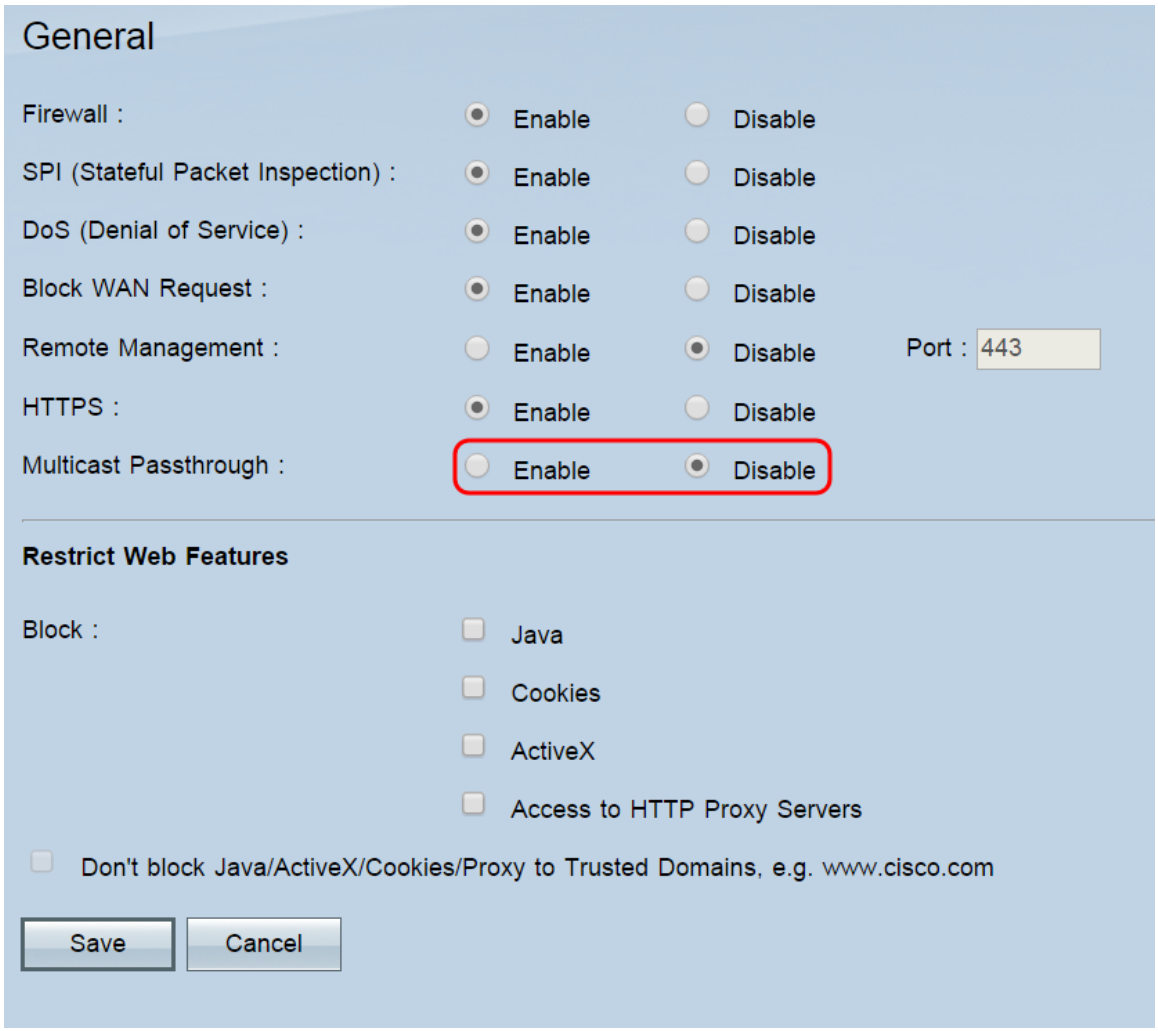
Nota: quando la gestione remota è abilitata, è possibile accedere all'utility di configurazione Web da qualsiasi browser immettendo **http://<indirizzo IP WAN del router>:<porta>**. Se HTTPS è abilitato, immettere **https://<indirizzo IP WAN del router>:<porta>**.

Passaggio 6. Nel campo *HTTPS*, selezionare il pulsante di scelta **Abilita** o **Disabilita**. HTTPS è abilitato per impostazione predefinita. Questa funzionalità consente sessioni HTTP protette.



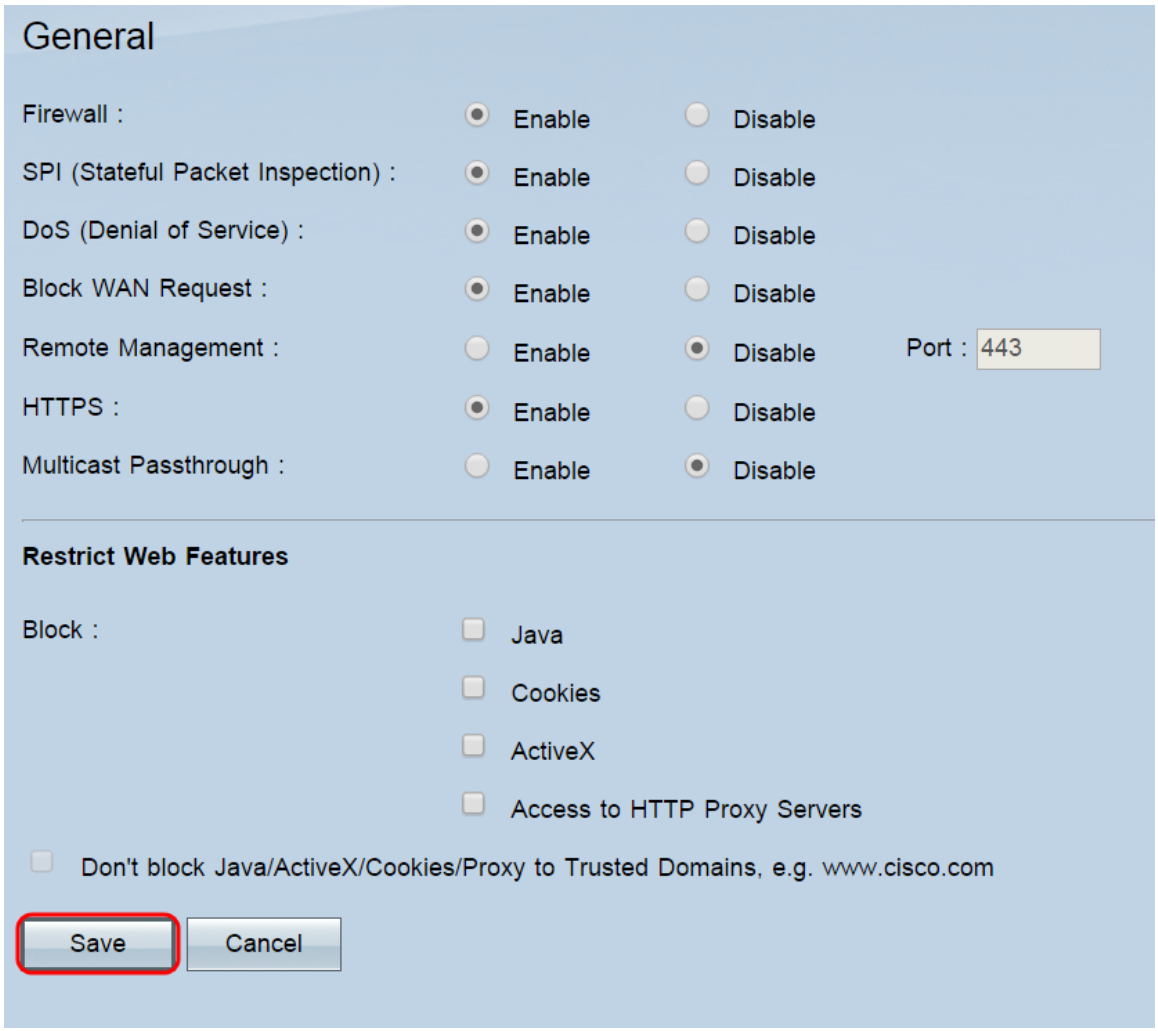
Nota: se questa funzione è disabilitata, gli utenti non possono connettersi utilizzando QuickVPN.

Passaggio 7. Nel campo *Multicast PassThrough*, selezionare il pulsante di opzione **Abilita** o **Disabilita**. Multicast PassThrough è disabilitato per impostazione predefinita. Questa funzione consente di trasmettere i pacchetti IP multicast ai dispositivi LAN corrispondenti e viene utilizzata per giochi Internet, videoconferenze e applicazioni multimediali.



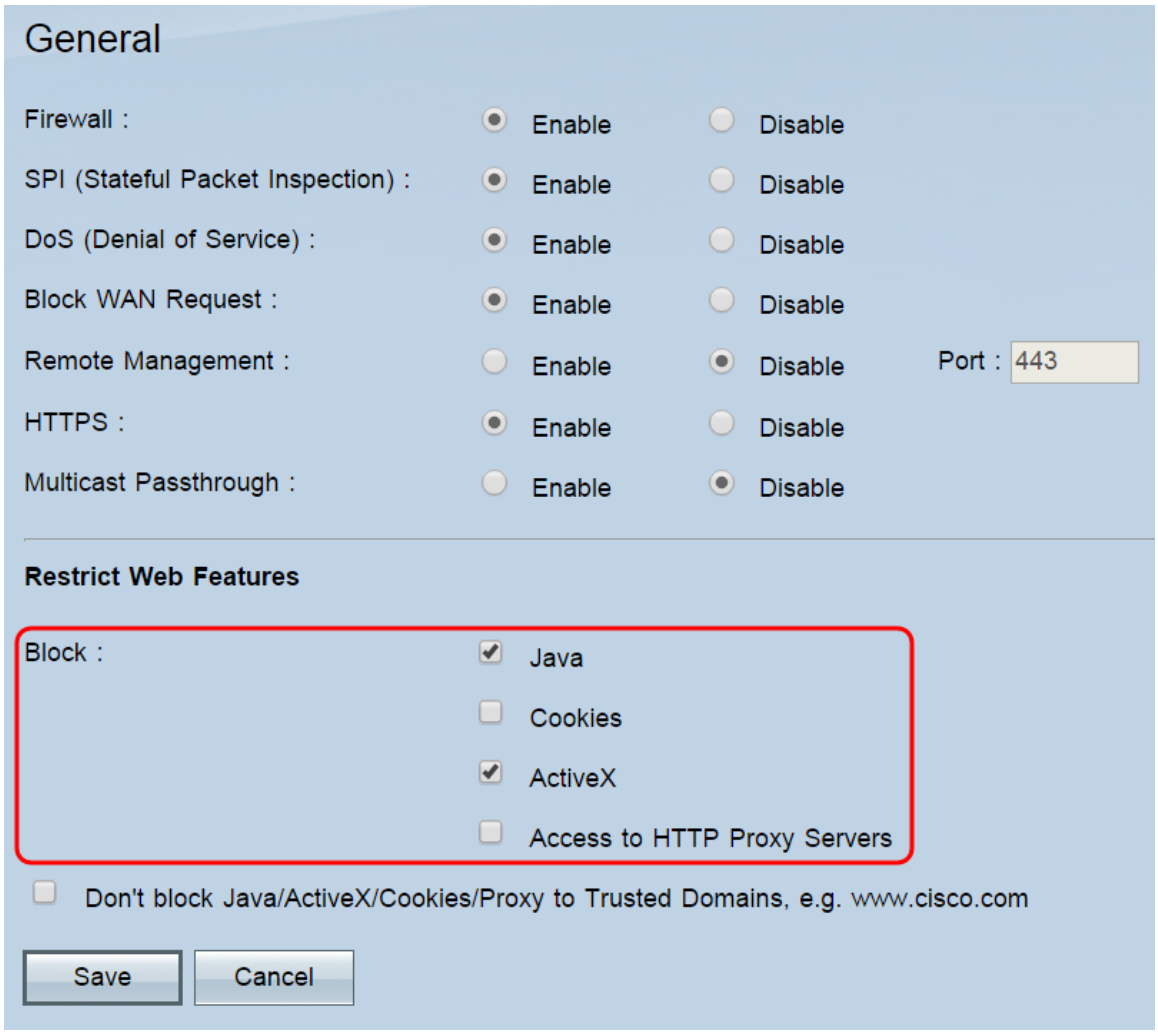
Nota: gli RV016, RV042, RV042G e RV082 non supportano il passaggio di traffico multicast su un tunnel IPSec.

Passaggio 8. Fare clic su **Salva**.



Funzionalità Web

Passaggio 1. Nel campo *Blocca*, selezionare le caselle di controllo delle funzionalità Web che si desidera bloccare nel firewall. Se si desidera consentire funzionalità bloccate per alcuni domini, è possibile aggiungere tali domini a un elenco di eccezioni nel passaggio 2. Nessuna delle feature è bloccata per default.



Le opzioni sono:

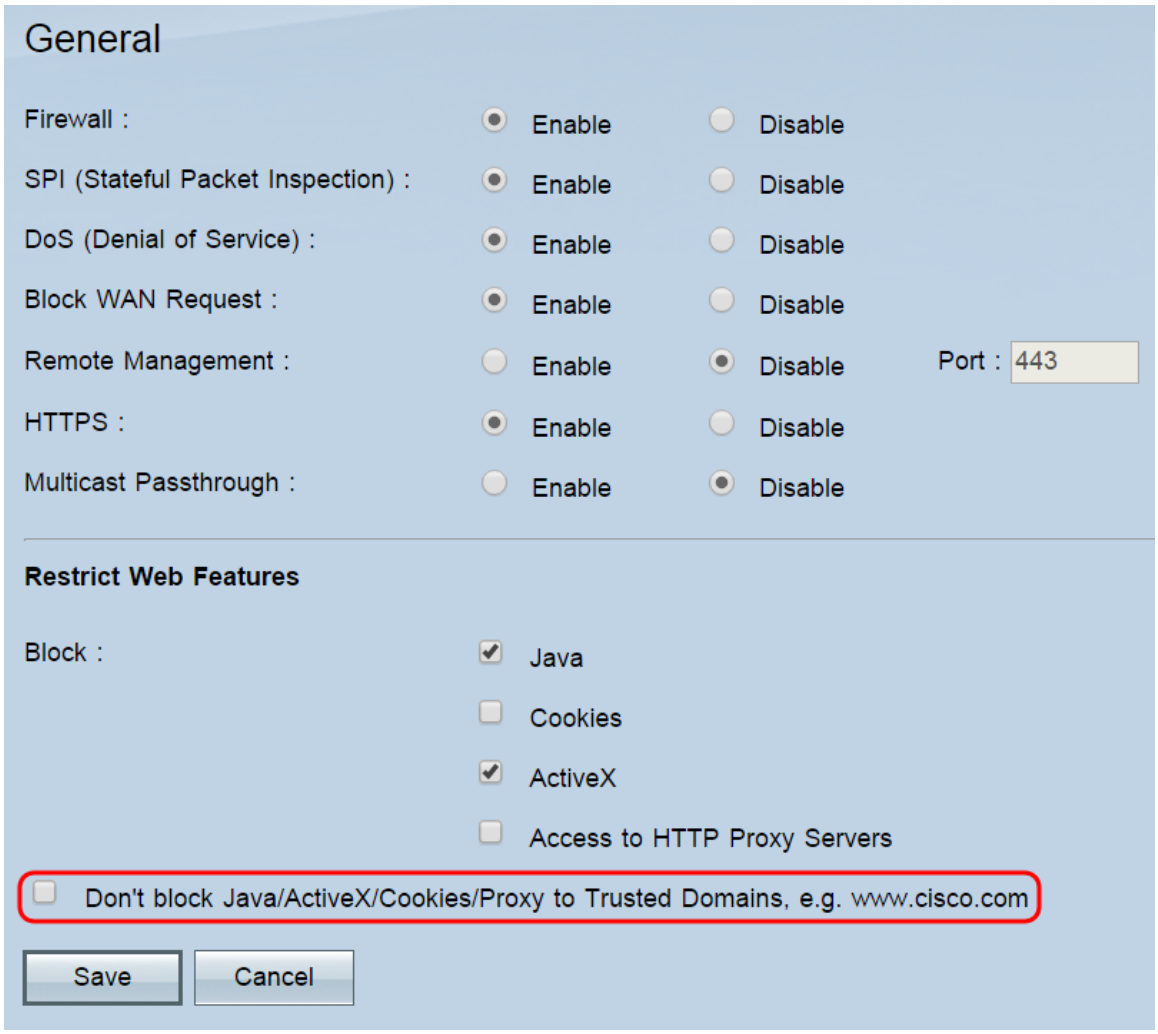
· Java: Java è un linguaggio di programmazione per i siti Web. Se si seleziona questa casella, le applet Java (piccoli programmi incorporati nelle pagine Web ma eseguiti all'esterno del browser Web) verranno bloccate, ma i siti Web che utilizzano questa funzionalità potrebbero non funzionare correttamente.

· Cookie: un cookie è costituito da dati che un sito Web memorizza localmente sul PC di un utente. Il blocco dei cookie può causare un comportamento non corretto dei siti Web che li utilizzano.

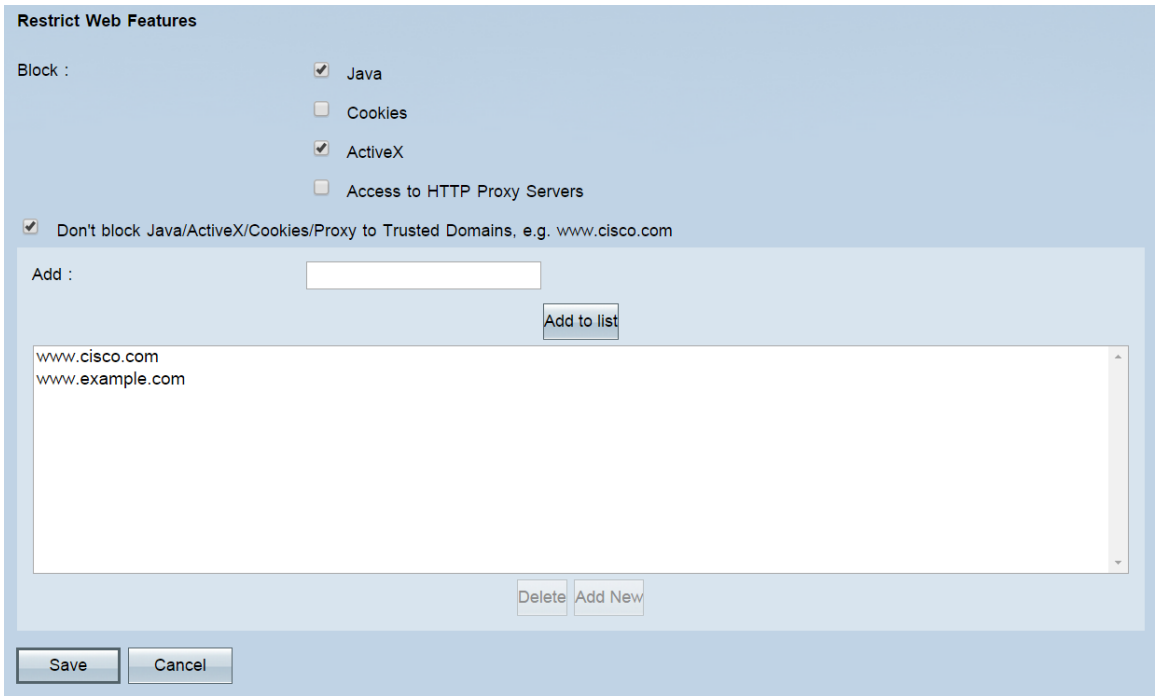
· ActiveX: ActiveX è un framework software sviluppato da Microsoft. Questo framework può essere utilizzato per eseguire alcune parti di pagine Web. La selezione di questa casella blocca questi componenti, ma potrebbe causare il funzionamento non corretto dei siti Web che utilizzano ActiveX.

· Accesso ai server proxy HTTP: selezionare questa casella se si desidera bloccare l'accesso ai server proxy HTTP. L'utilizzo di server proxy WAN può compromettere la sicurezza del router.

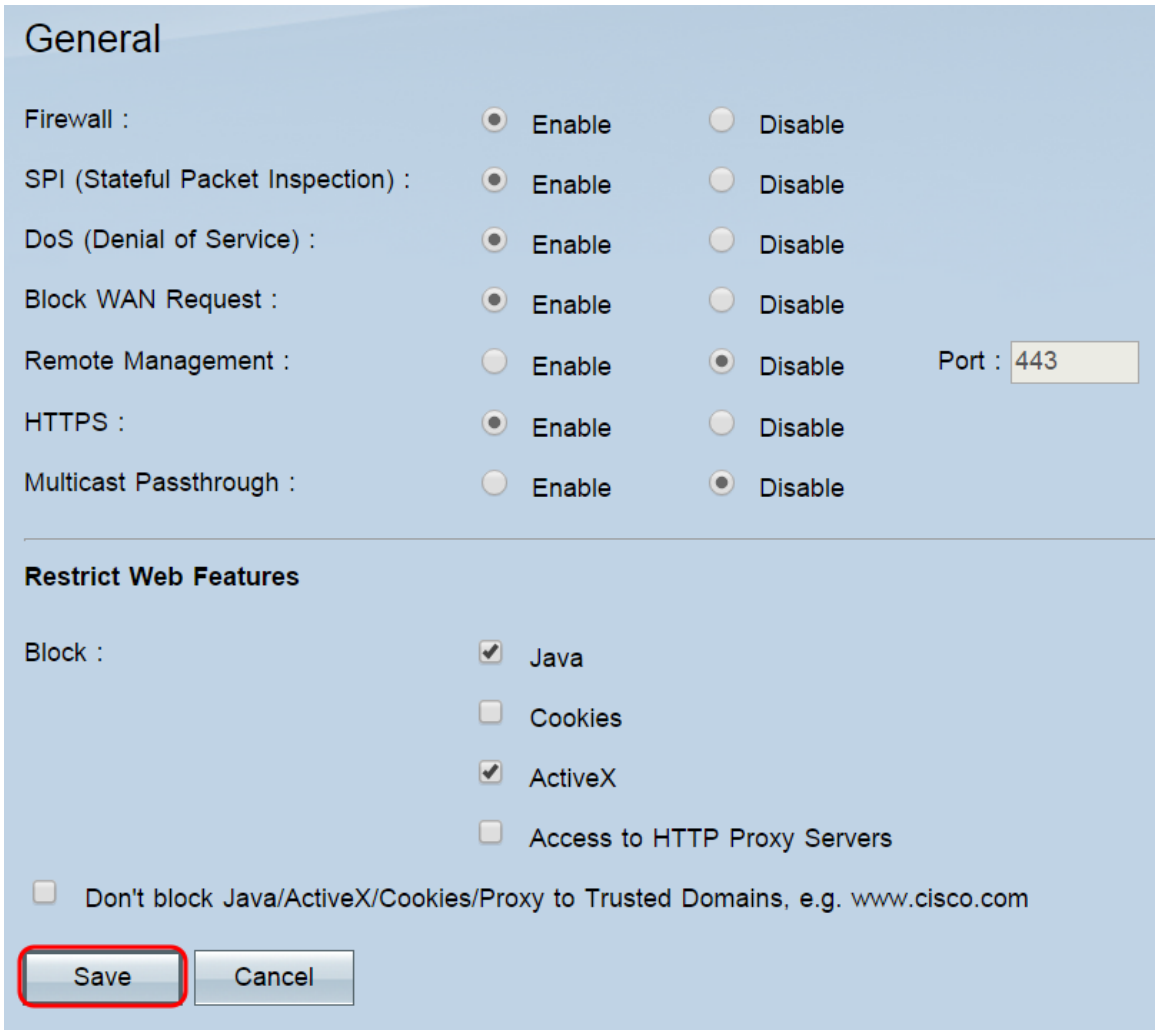
Passaggio 2. Selezionare la casella di controllo **Non bloccare Java/ActiveX/Cookie/Proxy in domini trusted** per aprire l'elenco dei domini trusted, in cui è possibile aggiungere o rimuovere domini in cui sono consentite funzionalità Web bloccate. Questo campo è deselezionato per impostazione predefinita ed è disponibile solo se è stata selezionata una casella precedente per bloccare una feature. Se deselezionata, le funzionalità verranno bloccate per tutti i siti Web.



Passaggio 3. (Facoltativo) Se è stata selezionata la casella di controllo **Non bloccare Java/ActiveX/Cookie/Proxy in domini trusted**, verrà visualizzato un elenco di domini trusted. Per aggiungere un dominio all'elenco, immetterlo nel campo *Aggiungi* e fare clic su **Aggiungi all'elenco**. Se si desidera modificare un dominio esistente, fare clic su di esso nell'elenco, quindi modificarlo nel campo *Aggiungi* e fare clic su **Aggiorna**. Per eliminare un dominio dall'elenco, fare clic su di esso nell'elenco, quindi fare clic su **Elimina**.



Passaggio 4. Fare clic su **Salva**.



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).