Impostazioni generali del firewall sui router VPN RV016, RV042, RV042G e RV082

Obiettivo

Un firewall protegge una rete interna da una rete esterna, ad esempio Internet. I firewall sono fondamentali per la sicurezza della rete. Sono disponibili diverse impostazioni che consentono di attivare o disattivare servizi specifici in base alle esigenze di protezione.

L'obiettivo di questo articolo è mostrare come abilitare o disabilitare le impostazioni generali del firewall sui router VPN RV016, RV042, RV042G e RV082.

Dispositivi interessati

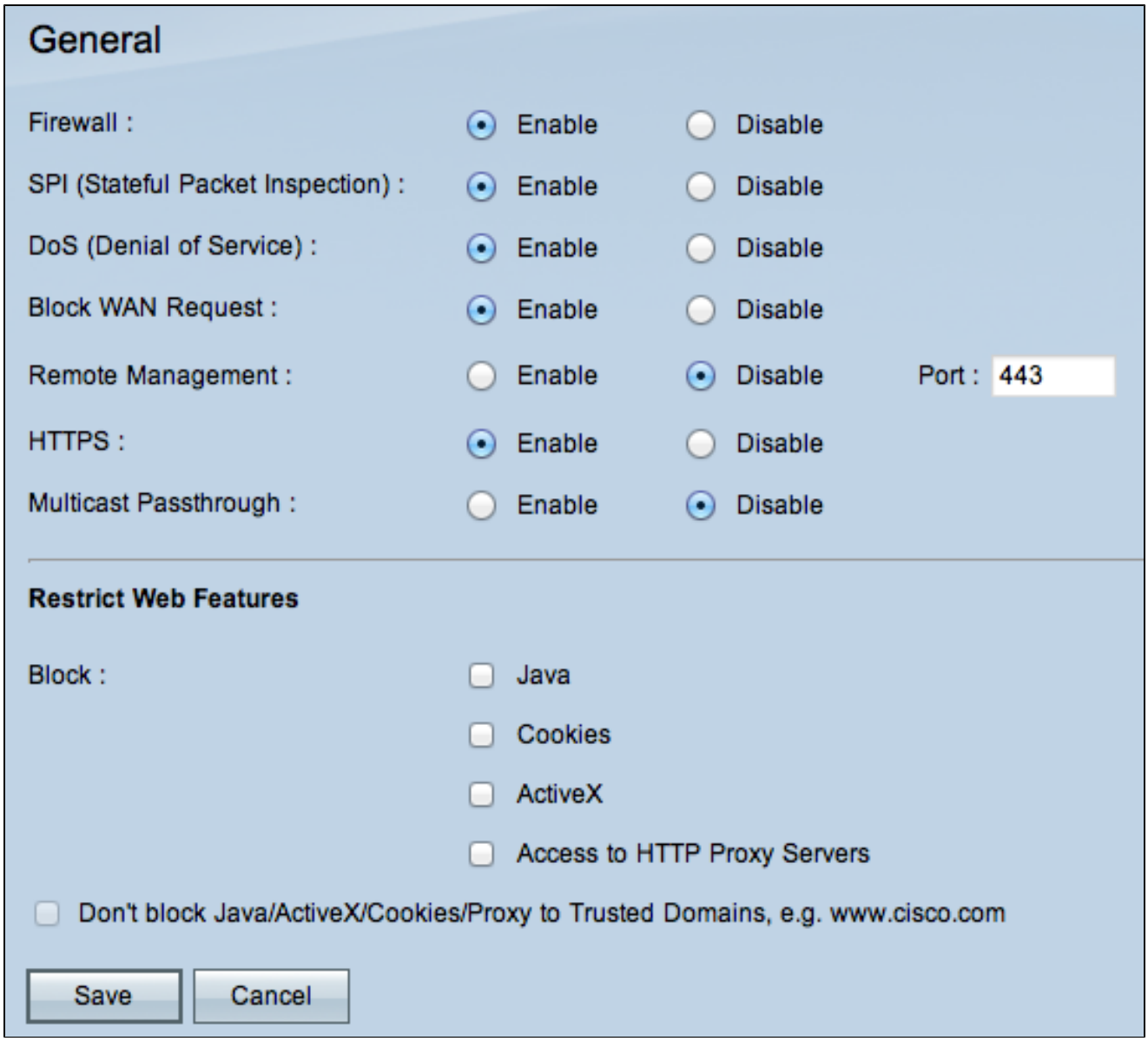
· RV016
RV042
RV042G
RV082

Versione del software

· v4.2.1.02

Impostazioni generali firewall

Passaggio 1. Accedere all'utilità di configurazione del router e scegliere Firewall > Generale. Viene visualizzata la pagina Generale.



Passaggio 2. Fare clic sul pulsante di opzione Abilita o Disabilita per abilitare o disabilitare le impostazioni disponibili nel firewall in base ai requisiti utente.

Di seguito sono descritti i campi che seguono.

· Firewall: quando questa funzione è abilitata, il router esegue l'ispezione approfondita dei pacchetti su tutto il traffico che attraversa il router e scarta i pacchetti che non seguono il comportamento predefinito del protocollo.

· SPI (Stateful Packet Inspection): il firewall del router utilizza Stateful Packet Inspection (SPI) per esaminare il traffico sul firewall. Controlla lo stato delle connessioni di rete, ad esempio i flussi TCP e le comunicazioni UDP. Il firewall distingue i pacchetti legittimi per i diversi tipi di connessione e solo i pacchetti che corrispondono a una connessione attiva nota sono consentiti dal firewall, tutti gli altri vengono rifiutati.

· Dos (Denial of Service): quando questa funzione è abilitata, il router impedisce gli attacchi DOS (Denial of Service) provenienti da Internet. Gli attacchi DOS provocano l'utilizzo della CPU del router, che non è in grado di fornire servizi per il traffico regolare.

· Blocca richiesta WAN: quando questa opzione è abilitata, il router ignora le richieste PING provenienti da Internet, in modo che appaiano nascoste. In questo modo è possibile garantire la sicurezza nascondendo le porte di rete in modo che i violatori non possano accedere facilmente alla rete.

· Gestione remota: quando questa funzione è abilitata, il router consente di accedere all'utility di configurazione Web da Internet. Immettere il numero di porta che verrà aperta agli host sul lato WAN. L'impostazione predefinita è 443. È necessario specificare questa porta quando l'utente stabilisce una connessione remota.

· HTTPS: se abilitata, è possibile accedere all'utility di configurazione Web tramite una sessione HTTPS dal lato WAN anziché tramite il normale protocollo HTTP. La sessione Web remota sarà protetta dagli algoritmi di crittografia SSL. Se la funzionalità HTTPS è disabilitata, gli utenti non possono connettersi tramite QuickVPN. Se è disattivata, la connessione HTTP utilizzata sarà meno sicura.

· Multicast Passthrough: se sul router è in esecuzione un proxy IGMP, quando il Multicast Passthrough è abilitato il router consentirà al traffico IP Multicast di accedere da Internet.

Nota: per disabilitare il firewall, è necessario modificare la password predefinita dell'amministratore. I campi SPI (Stateful Packet Inspection), DoS (Denial of Service), Block WAN Request e Remote Management sono disattivati.

Passaggio 3. Nell'area Limita funzionalità Web selezionare una o tutte le caselle di controllo per limitare la funzionalità corrispondente.

· Java: Java è un linguaggio di programmazione per i siti Web. Per bloccare Java, selezionare la casella di controllo Java. Se si nega Java, potrebbe non essere possibile accedere ai siti Internet scritti in questo linguaggio di programmazione, quindi è sicuro procedere e bloccare le applet Java se il dispositivo connesso al router non deve accedere ai siti Web creati con Java. D'altra parte, i cyber-criminali usano Java come parte integrante del loro attacco, che è quello di determinare il sistema operativo e lanciare un attacco specificato dal sistema operativo quando si visitano siti web che sono infettati dal malware. Ad esempio, quando si visita un sito Web piratato, viene attivato un file JAR (Java Archive) che chiede di eseguire la sua funzione ma segretamente viene utilizzato per determinare il sistema operativo del computer.

· Cookie: i cookie sono dati memorizzati sul PC e utilizzati dai siti Internet quando gli utenti

interagiscono con essi. Per bloccare i cookie, selezionare la casella di controllo Cookie. Se si desidera bloccare i cookie, i siti Web non possono salvare le informazioni sulle visite precedenti quando vi si accede dal dispositivo. Il vantaggio è che i cookie dannosi (cookie di rilevamento di terze parti) non vengono salvati, il che comporta un rischio per la sicurezza.

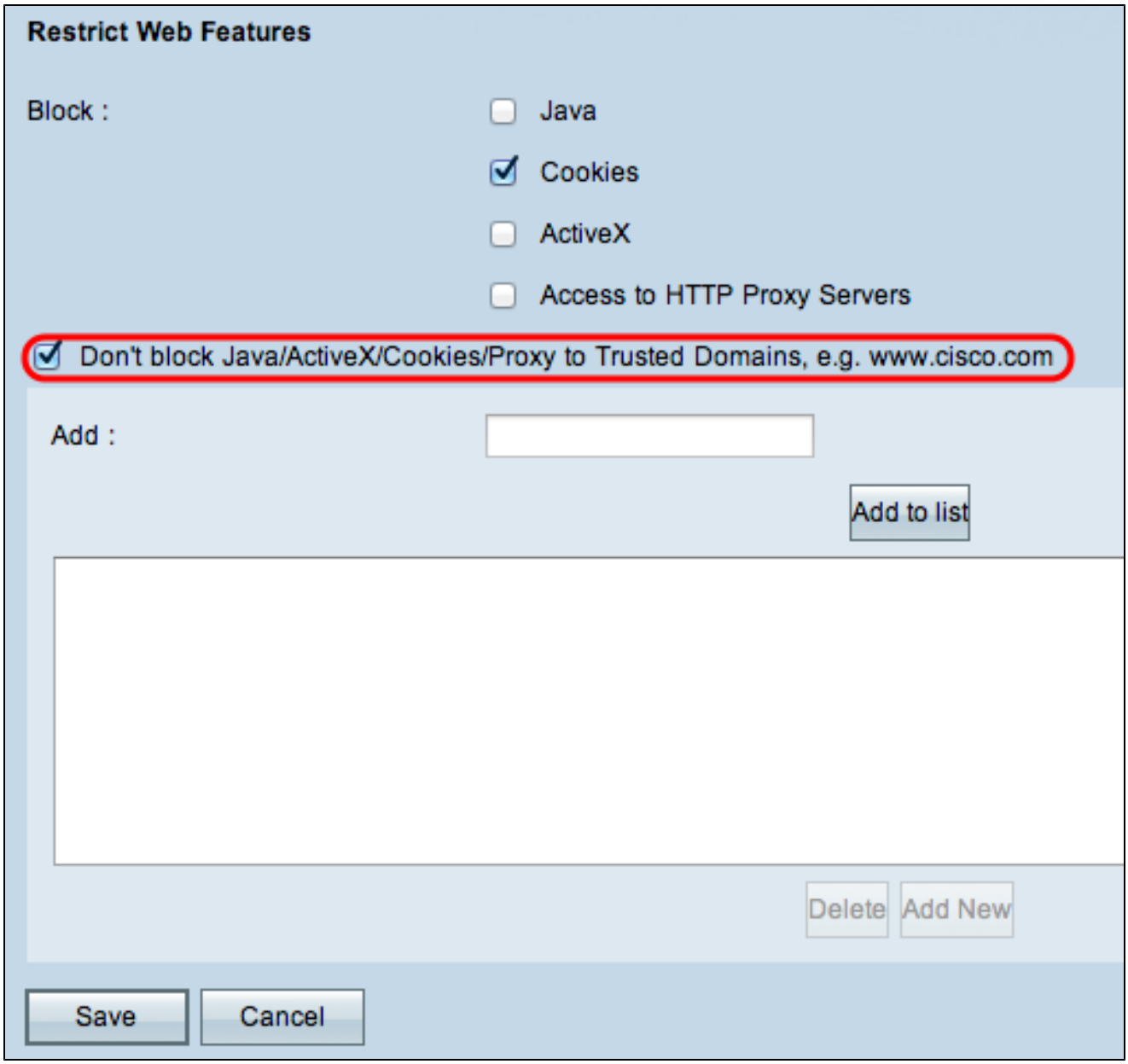
· ActiveX: ActiveX è un componente software di Microsoft Windows che può essere utilizzato per sviluppare applicazioni o controllare piccoli programmi, ad esempio componenti aggiuntivi utilizzati nei siti Internet. Se si consente ActiveX, è possibile migliorare l'esperienza di esplorazione, consentendo ai siti Web di eseguire animazioni e altri programmi simili. D'altra parte, esiste un rischio potenziale se si visitano pagine Web contenenti software ActiveX dannoso sviluppato da criminali informatici che possono causare danni al computer. Per bloccare ActiveX, selezionare la casella di controllo ActiveX. Se si blocca ActiveX, è possibile che si verifichino problemi se si desidera accedere a determinati siti Internet che utilizzano ActiveX per l'esecuzione.

· Accesso al server HTTP proxy: se si desidera navigare in modo anonimo attraverso un server proxy e negare l'accesso al server proxy, selezionare la casella di controllo Accesso al server HTTP proxy. I server proxy HTTP nascondono i dettagli degli utenti finali agli hacker. Lavorano come intermediari e quindi non si accede direttamente a Internet. Tuttavia, se gli utenti locali hanno accesso ai server proxy WAN, potrebbero essere in grado di aggirare i filtri dei contenuti sul router e accedere ai siti Internet bloccati dal router.

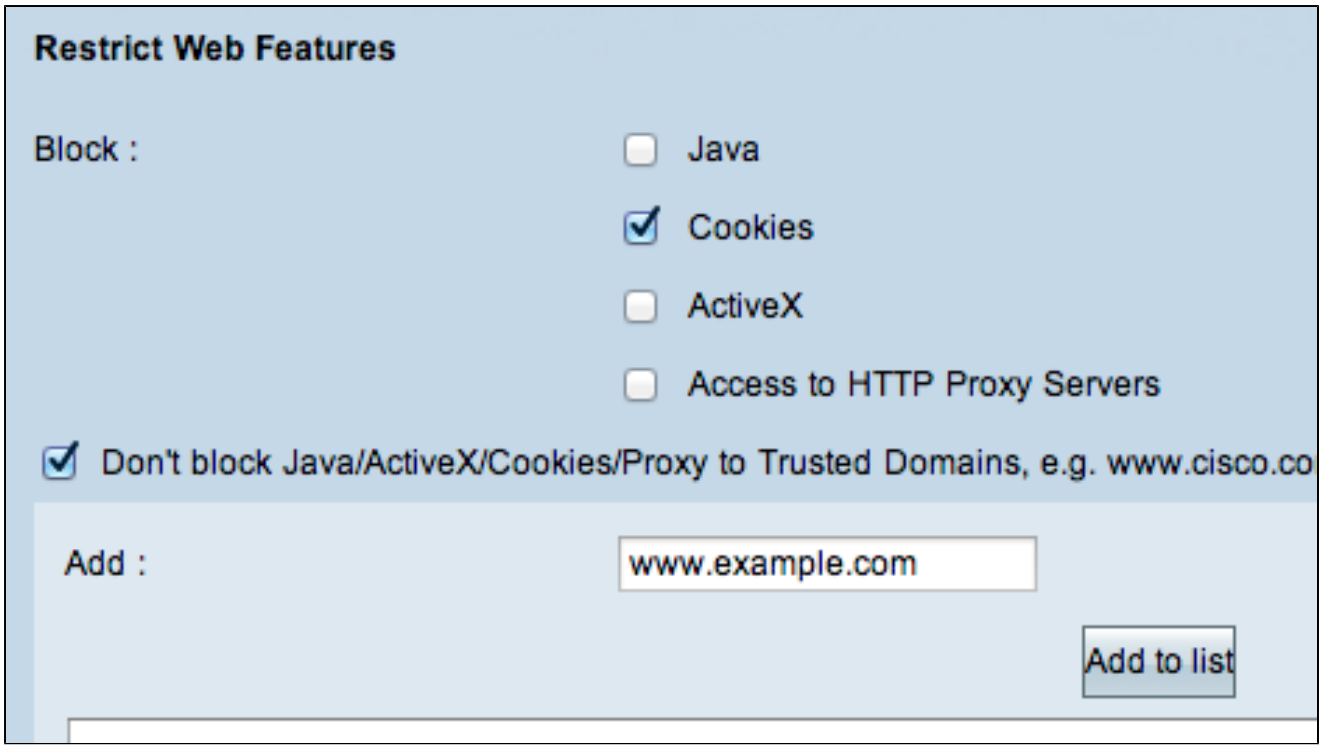
Passaggio 4. Per salvare le impostazioni, fare clic su Save (Salva).

Aggiungi domini trusted

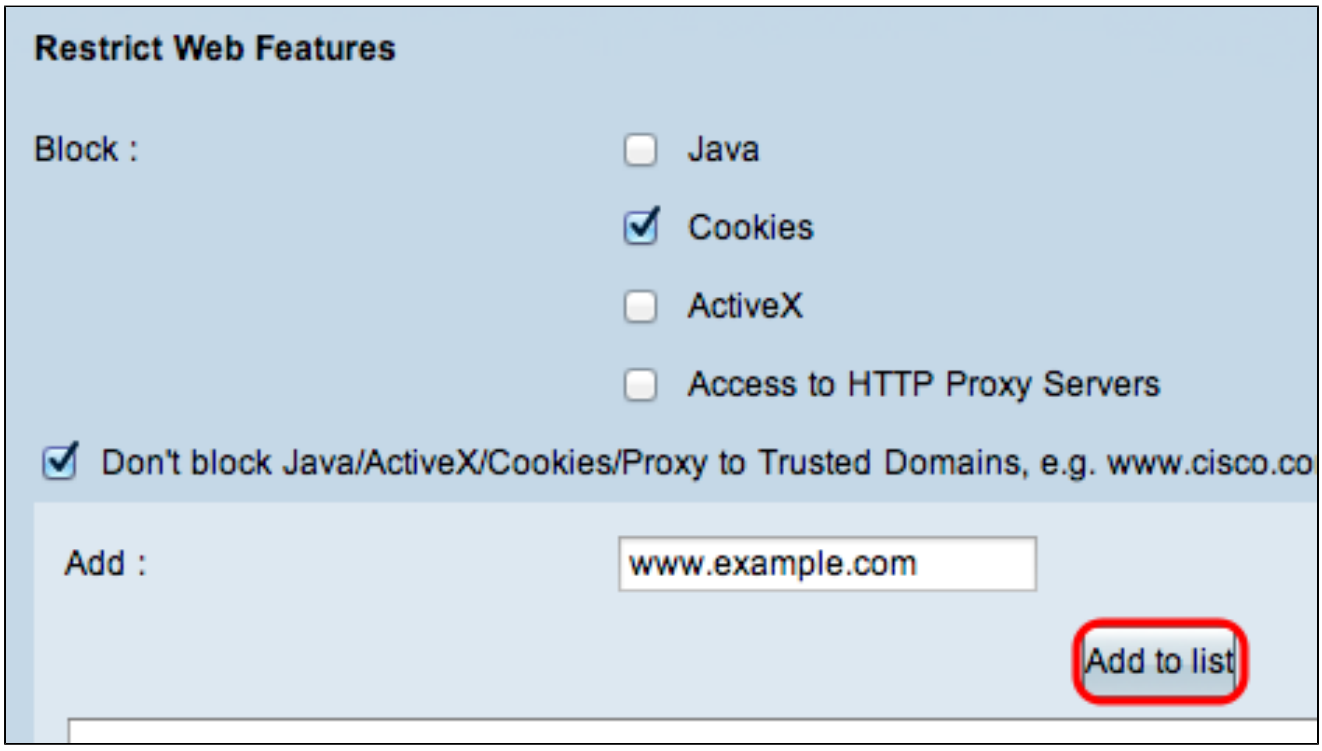
Anche se una delle funzionalità Web potrebbe essere bloccata, l'utente può consentire l'attivazione di tali funzionalità per i domini trusted specificati.



Passaggio 1. Selezionare il pulsante Non bloccare Java/ActiveX/Cookie/Proxy in domini trusted. Questa opzione è disponibile solo se l'utente ha scelto di bloccare le funzionalità Web nel passaggio 3 di Impostazioni generali firewall.



Passaggio 2. Nel campo Add (Aggiungi), immettere il dominio da aggiungere all'elenco dei domini trusted.

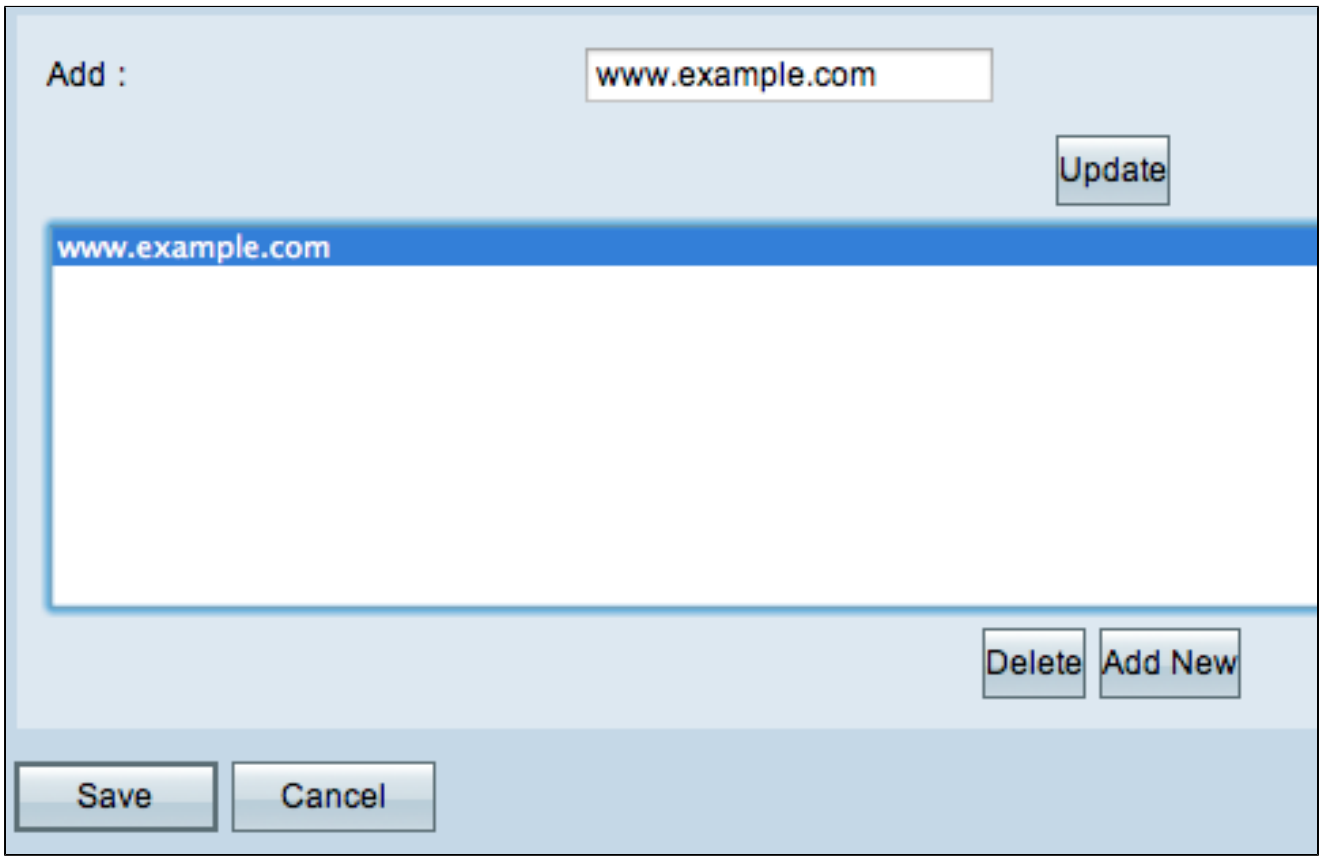


Passaggio 3. Fare clic su Aggiungi all'elenco. Il dominio viene aggiunto all'elenco dei domini trusted.

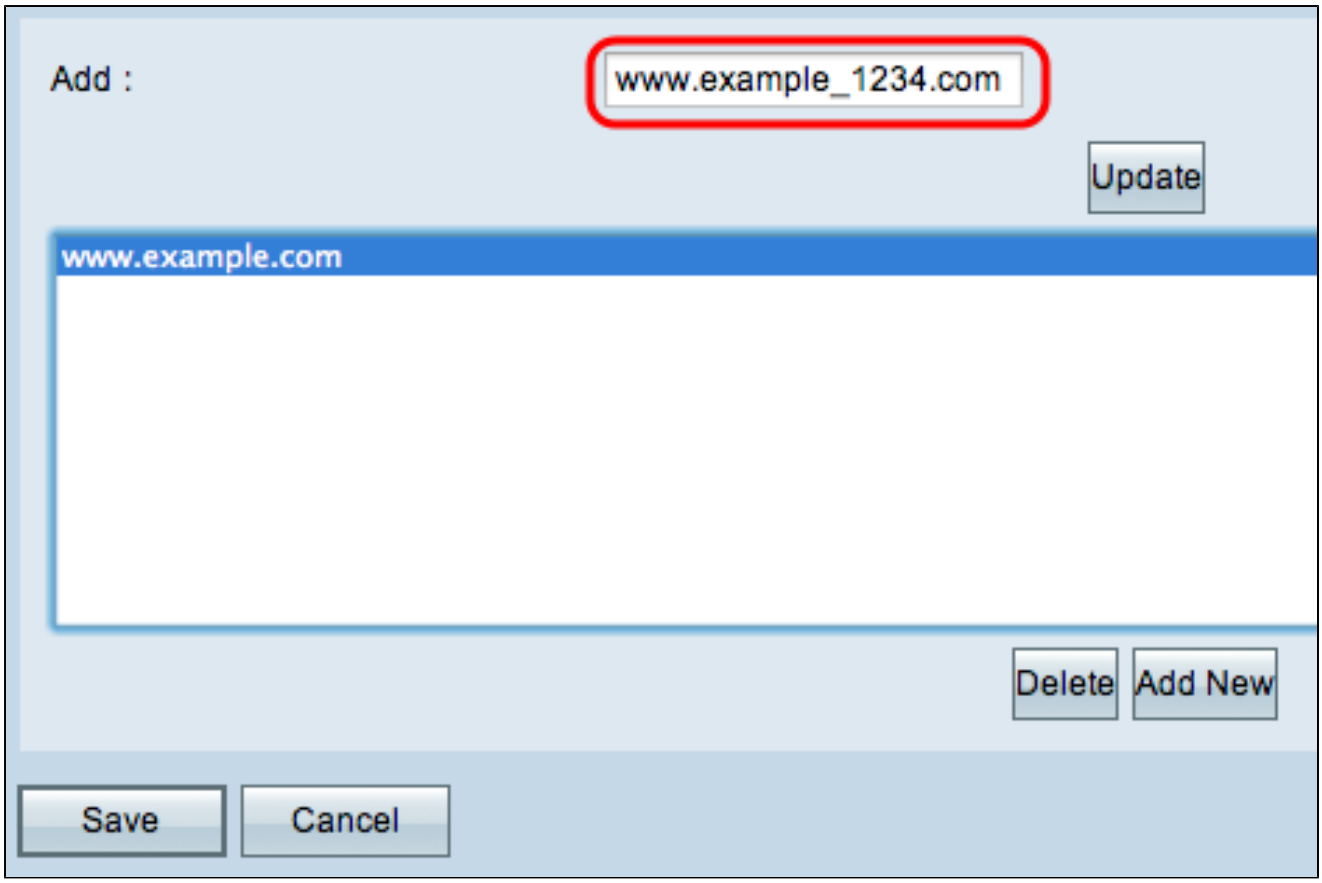
Passaggio 4. Fare clic su Salva per salvare le modifiche.

Aggiornare un dominio trusted

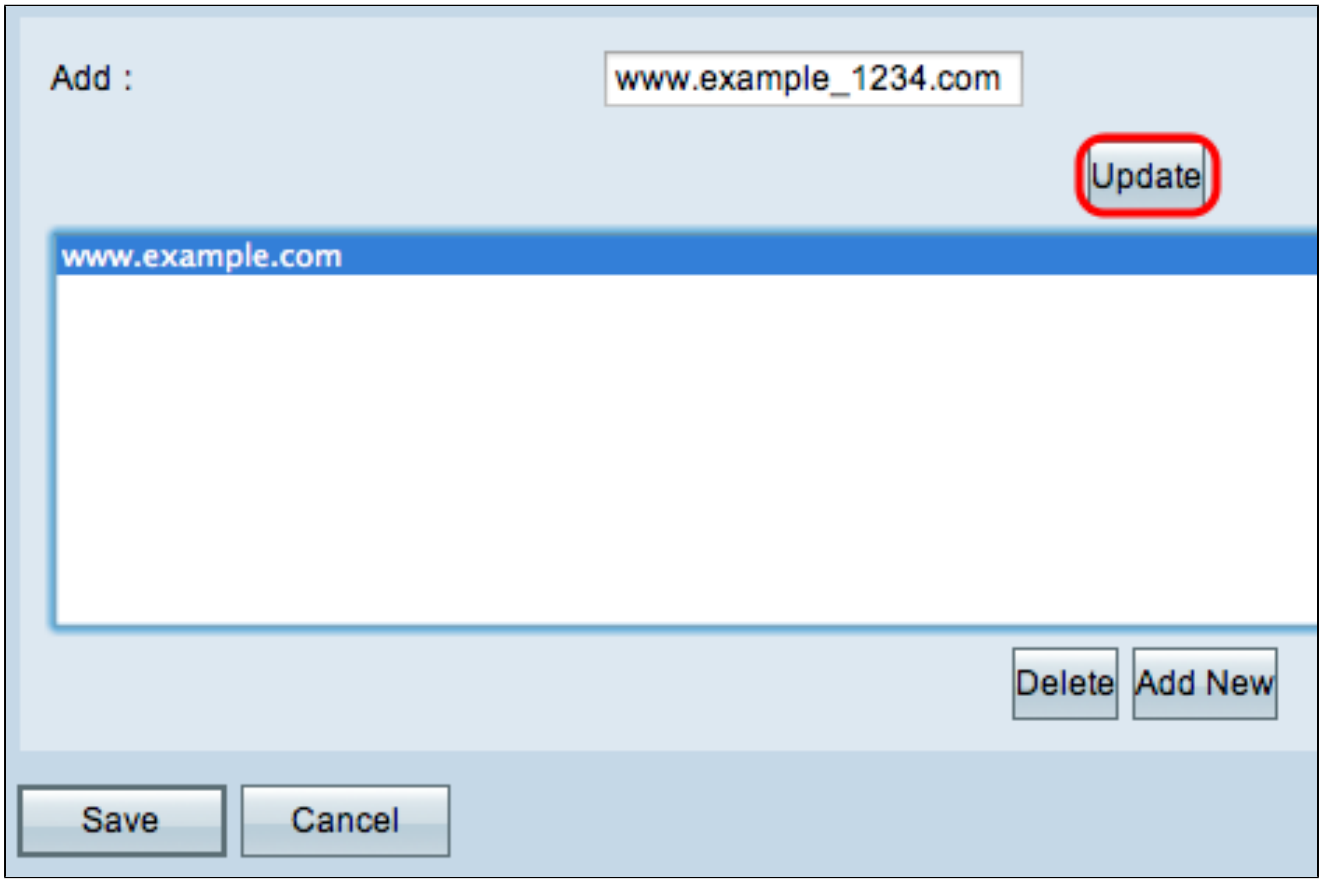
In questa sezione viene illustrato come modificare un dominio trusted.



Passaggio 1. Selezionare il dominio che si desidera modificare dall'elenco dei domini trusted.



Passaggio 2. Nel campo Add (Aggiungi), immettere il nome di dominio aggiornato per il dominio richiesto.

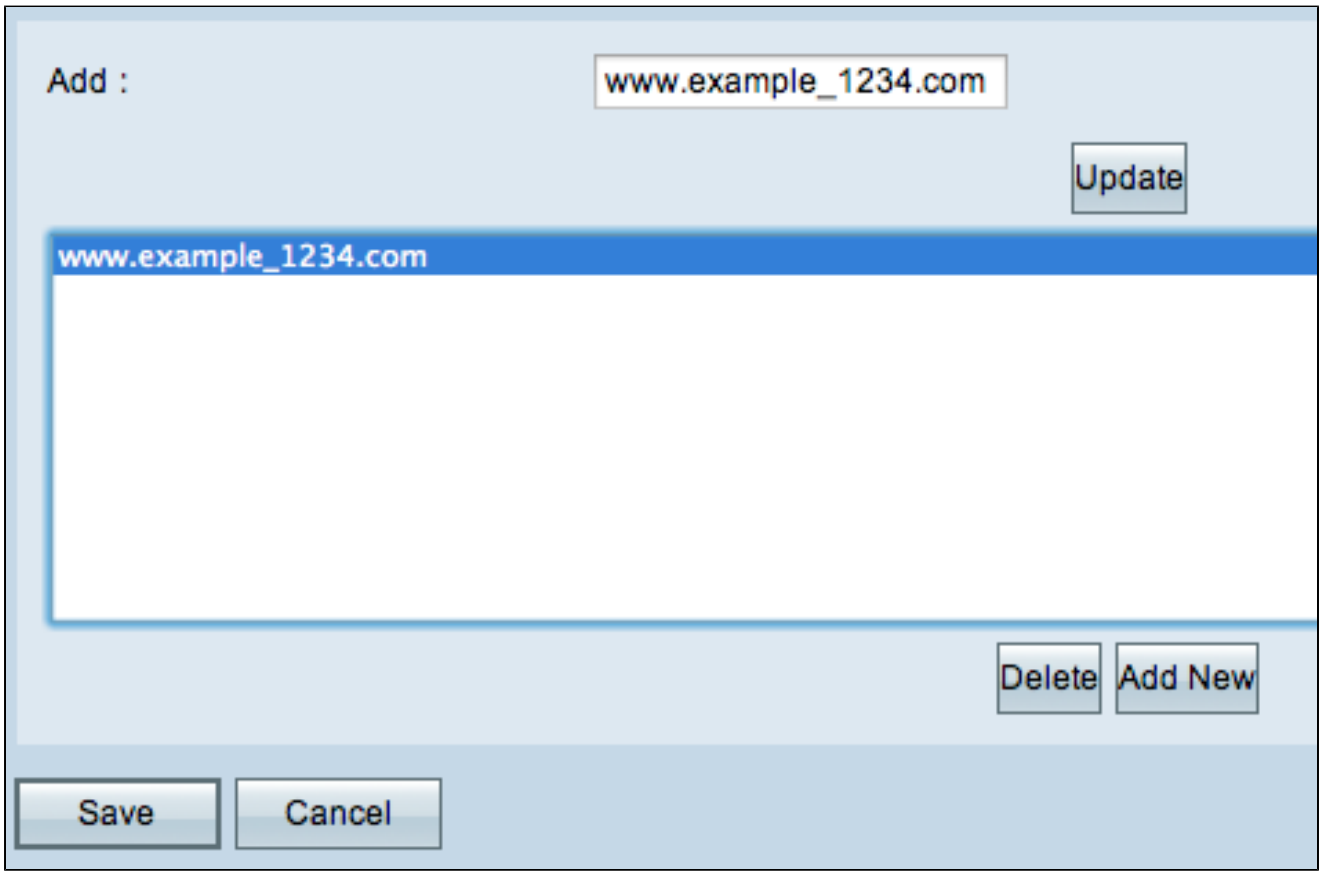


Passaggio 3. Fare clic su Aggiorna.

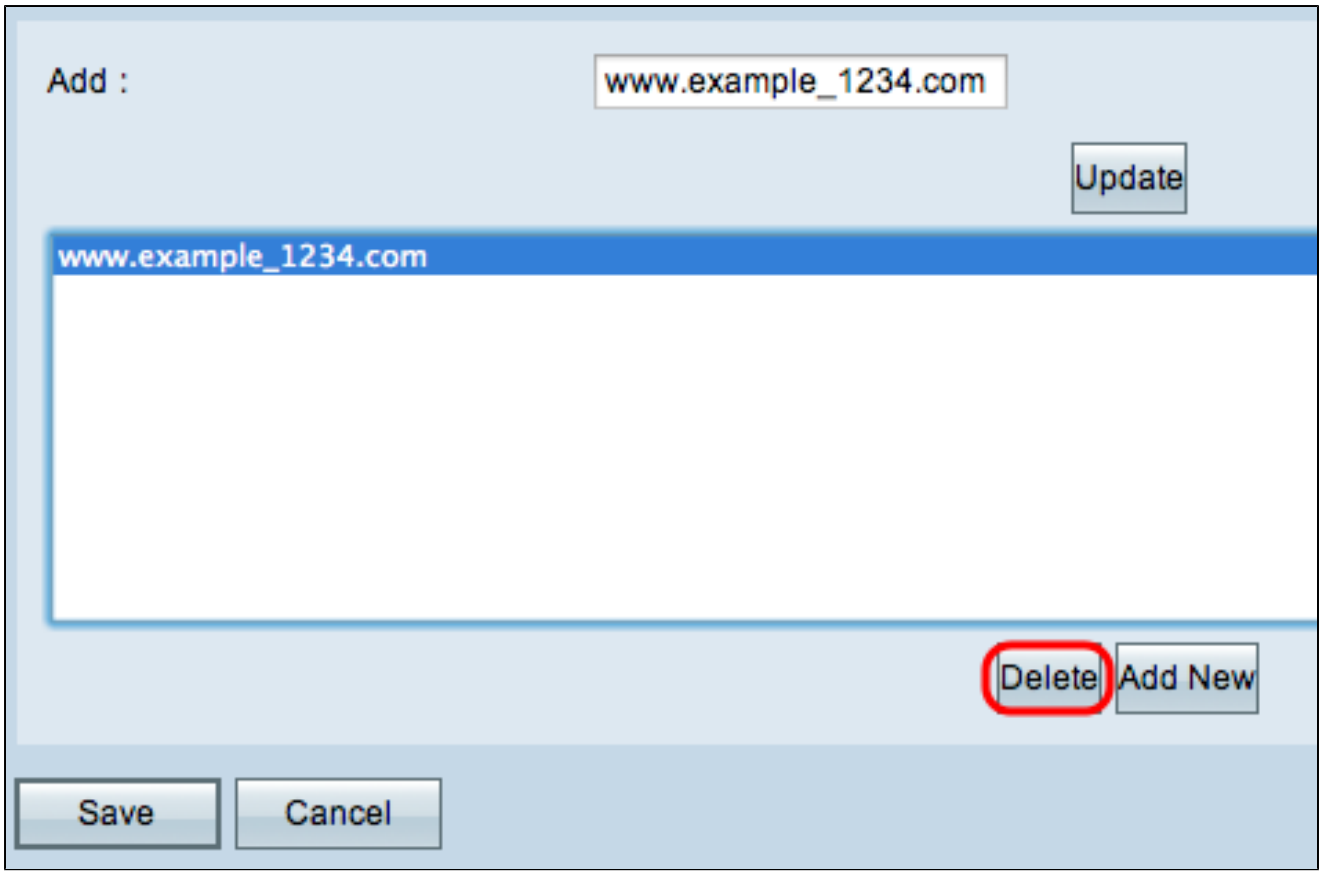
Passaggio 4. Fare clic su Salva per salvare le modifiche.

Eliminare un dominio trusted

In questa sezione viene illustrato come eliminare un dominio trusted.



Passaggio 1. Scegliere il dominio da eliminare.



Passaggio 2. Fare clic su Elimina. Il dominio viene eliminato.

Passaggio 3. Fare clic su Salva per salvare le modifiche.

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).