

RV016、RV042、RV042G和RV082 VPN路由器上的常規防火牆設定

目標

防火牆可保護內部網路免受外部網路（例如Internet）的影響。防火牆對網路安全至關重要。根據您的安全需求，可使用多種不同的設定來啟用或禁用特定服務。

本文的目的是顯示如何在RV016、RV042、RV042G和RV082 VPN路由器上啟用或禁用常規防火牆設定。

適用裝置

- RV016
- RV042
- RV042G
- RV082

軟體版本

- v4.2.1.02

常規防火牆設定

步驟 1. 登入路由器配置實用程式，然後選擇Firewall > General。General頁面隨即開啟：

General

Firewall :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
SPI (Stateful Packet Inspection) :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
DoS (Denial of Service) :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
Block WAN Request :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
Remote Management :	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Port : <input type="text" value="443"/>
HTTPS :	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
Multicast Passthrough :	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	

Restrict Web Features

Block :	<input type="checkbox"/> Java
	<input type="checkbox"/> Cookies
	<input type="checkbox"/> ActiveX
	<input type="checkbox"/> Access to HTTP Proxy Servers
	<input type="checkbox"/> Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.com

步驟 2. 按一下「Enable」或「Disable」單選按鈕，以根據使用者要求啟用或停用防火牆中的可用設定。

以下欄位說明如下：

· 防火牆 — 啟用此功能後，路由器將對通過此路由器的所有流量執行深度資料包檢測，並丟棄不符合預定義協定行為的資料包。

· SPI (狀態資料包檢測) — 路由器的防火牆使用狀態資料包檢測(SPI)來檢查防火牆上的流量。它監控網路連線狀態，例如TCP資料流和UDP通訊。 防火牆會針對不同型別的連線區分合法資料包，並且防火牆僅允許與已知活動連線匹配的資料包，而拒絕所有其他資料包。

· Dos (拒絕服務) — 啟用此功能後，路由器將阻止來自Internet的DOS (拒絕服務) 攻擊。DOS攻擊會導致路由器的CPU繁忙，從而無法向常規流量提供服務。

·阻止WAN請求 — 啟用此功能後，路由器將忽略來自Internet的PING請求，使其顯示為隱藏。這有助於通過隱藏網路埠提供安全性，從而使主動變更者無法輕鬆訪問網路。

·遠端管理 — 啟用此功能後，路由器允許從Internet訪問Web配置實用程式。輸入將開啟給WAN端主機的埠號。預設設定為443。使用者建立遠端連線時必須指定此埠。

·HTTPS — 啟用時，可通過WAN端的HTTPS會話（而不是常規HTTP）訪問Web配置實用程式。這將使您的遠端Web會話受SSL加密演算法保護。如果禁用HTTPS功能，則使用者無法使用QuickVPN進行連線。如果禁用，則使用安全性較低的HTTP連線。

·組播傳輸 — 如果路由器上當前運行的是IGMP代理，則當啟用組播傳輸時，路由器將允許IP組播流量從網際網路進入。

注意：要禁用防火牆，必須將管理員密碼從預設值更改為其他值。SPI（狀態封包檢查）、DoS（拒絕服務）、Block WAN Request和Remote Management欄位均呈灰色顯示。

步驟 3.在「限制Web功能」區域中，選中任意或所有覈取方塊以限制相應功能。

·Java - Java是網站程式語言。要阻止Java，請選中Java覈取方塊。如果拒絕Java，則可能無法訪問用此程式語言編寫的網際網路站點，因此，如果連線到路由器的裝置不需要訪問使用Java建立的網站，則繼續訪問並阻止Java小程序是安全的。另一方面，網路犯罪分子使用Java作為其攻擊的一個有機組成部分，即確定作業系統並在您訪問受惡意軟體感染的網站時發起由作業系統指定的攻擊。例如，當您訪問被駭客入侵的網站時，會觸發一個JAR(Java Archive)檔案，要求您執行它的功能，但會秘密地用它來確定電腦的作業系統。

·Cookie — 使用者與Internet站點互動時，Cookie儲存在PC上並由Internet站點使用的資料。要阻止Cookie，請選中Cookie覈取方塊。如果您希望阻止cookie，則從裝置訪問時，網站無法儲存任何以前的訪問資訊。其好處是不儲存惡意cookie（第三方跟蹤cookie），這會帶來安全風險。

·ActiveX — ActiveX是Microsoft Windows的一個軟體元件，可用於開發應用程式或控制小型程式，如在Internet站點上使用的載入項。如果允許ActiveX，它有助於改善瀏覽時的體驗；它允許網站運行動畫和其他類似程式。另一方面，如果訪問包含網路犯罪分子開發的惡意ActiveX軟體的網頁，則存在潛在風險，此類軟體可能會對電腦造成損壞。要阻止ActiveX，請選中ActiveX覈取方塊。如果阻止ActiveX，則如果要訪問某些使用ActiveX執行的Internet站點，可能會出現問題。

·對Proxy HTTP Server的訪問 — 如果您希望匿名通過Proxy伺服器進行衝浪並拒絕對Proxy伺服器的訪問，請選中Access to Proxy HTTP Server覈取方塊。HTTP Proxy伺服器會針對駭客隱藏終端使用者的詳細資訊。他們充當中間人，因此您不直接訪問Internet。但是，如果本地使用者能夠訪問WAN代理伺服器，他們也許能夠找到一種方法來避開路由器的內容過濾器，並訪問被路由器阻止的網際網路站點。

步驟 4.按一下「Save」以儲存設定。

新增受信任域

即使其中一個Web功能可能被阻止，使用者也可以允許為指定的受信任域啟用這些功能。

Restrict Web Features

Block :

- Java
- Cookies
- ActiveX
- Access to HTTP Proxy Servers

Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.com

Add :

Add to list

Delete Add New

Save Cancel

步驟 1.選中Don't block Java/ActiveX/Cookie/Proxy to Trusted Domains按鈕。僅當使用者在General Firewall Settings的步驟3中選擇了阻止任何Web功能時，此選項才可用。

Restrict Web Features

Block :

- Java
- Cookies
- ActiveX
- Access to HTTP Proxy Servers

Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.co

Add :

步驟 2. 在Add欄位中，輸入要新增到受信任域清單中的域。

Restrict Web Features

Block :

- Java
- Cookies
- ActiveX
- Access to HTTP Proxy Servers

Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains, e.g. www.cisco.co

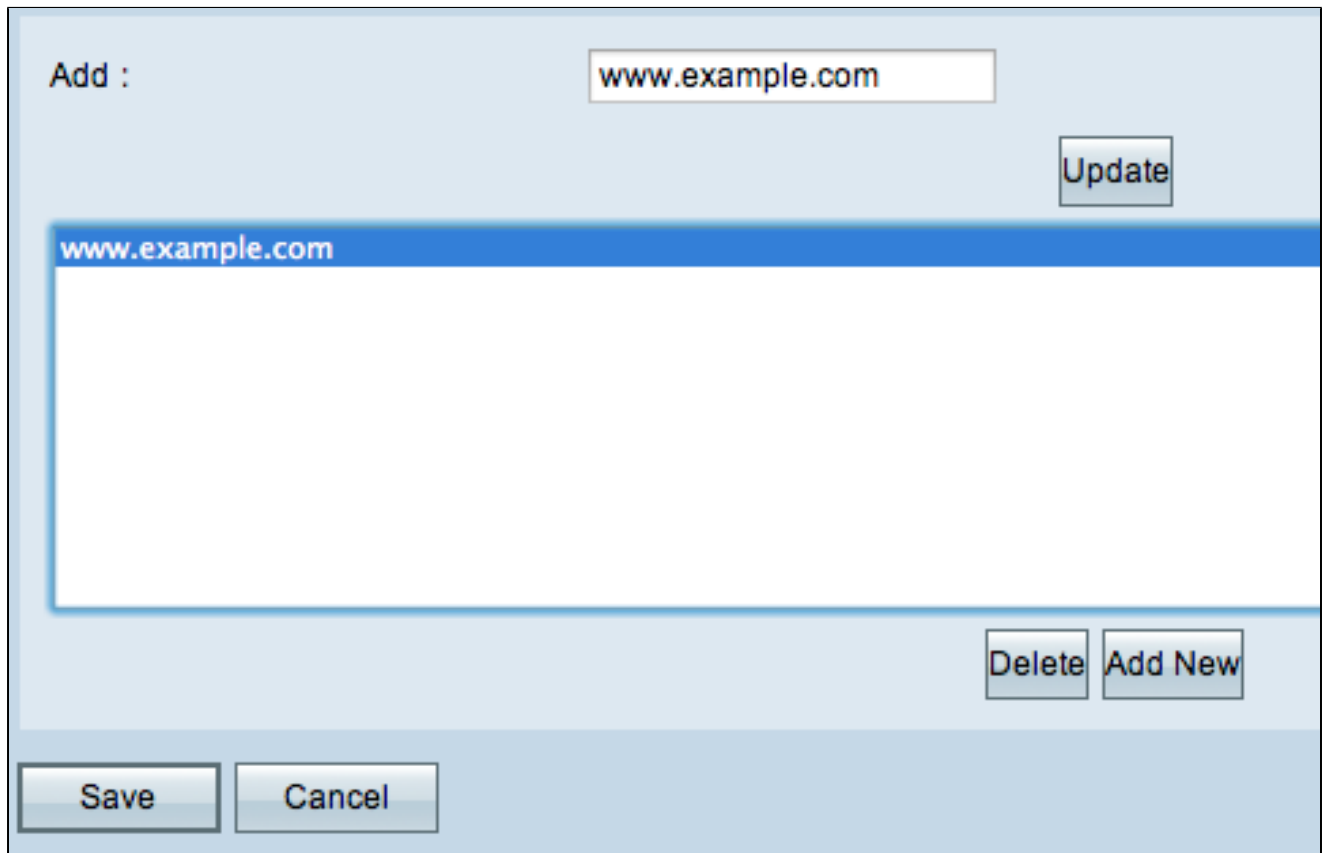
Add :

步驟 3. 按一下Add to list。域將新增到受信任清單中。

步驟 4. 按一下「Save」以儲存變更。

更新受信任的域

本節指導使用者如何編輯受信任的域。



The screenshot shows a user interface for managing trust domains. At the top left, there is a label "Add :" followed by a text input field containing "www.example.com". To the right of this input field is a button labeled "Update". Below the input field is a large, empty rectangular area with a blue border, which appears to be a list or table of trust domains. At the bottom right of this area are two buttons: "Delete" and "Add New". At the bottom of the entire interface are two buttons: "Save" and "Cancel".

步驟 1. 從受信任的域清單中選擇要編輯的域。

Add :

www.example.com

步驟 2. 在「Add」欄位中，輸入所需域的更新域名。

Add :

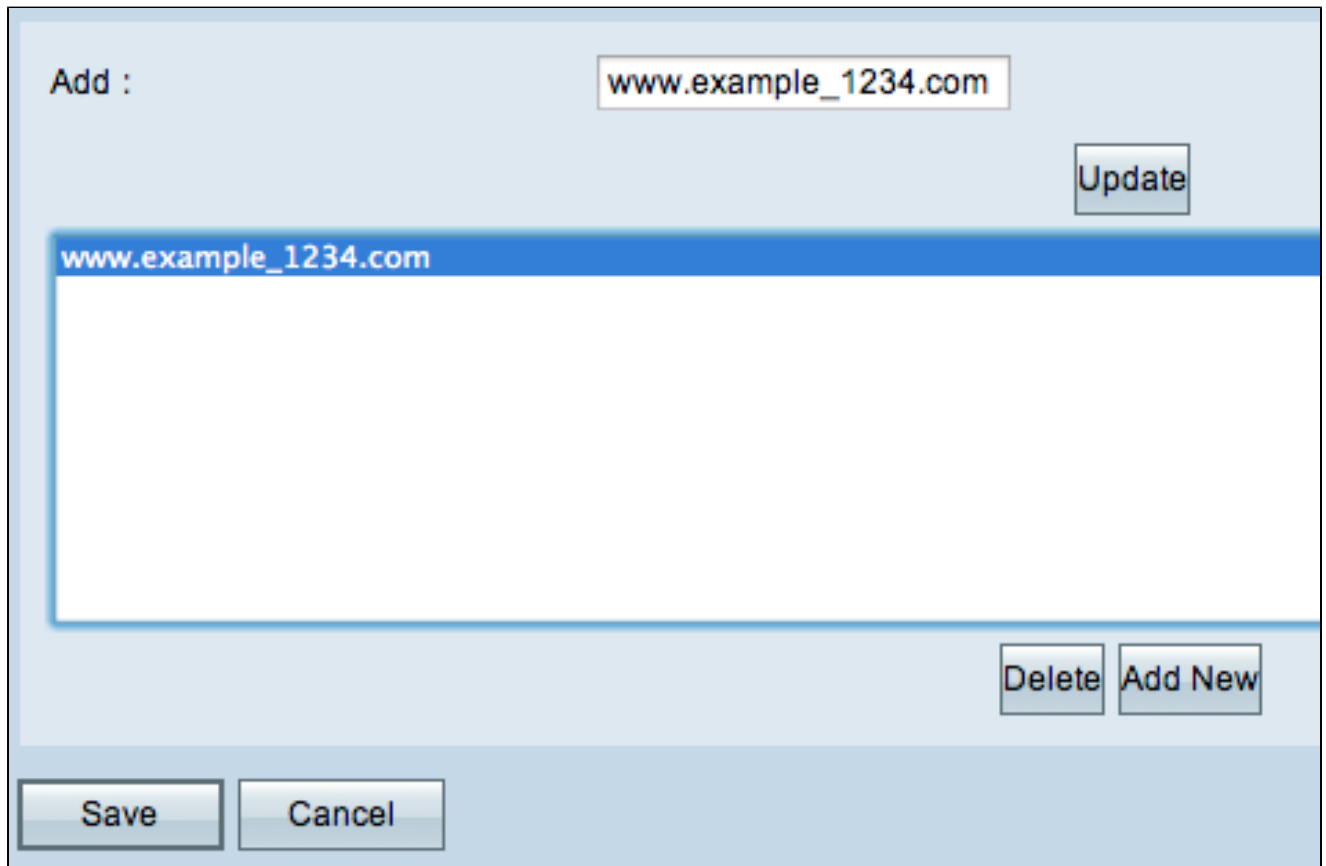
www.example.com

步驟 3.按一下「Update」。

步驟 4.按一下「Save」以儲存變更。

刪除受信任的域

本節指導使用者如何刪除受信任的域。



The screenshot shows a web management interface with a light blue background. At the top left, there is a label "Add :" followed by a text input field containing "www.example_1234.com". To the right of this field is a button labeled "Update". Below the input field is a large white area representing a list of domains. The first item in the list, "www.example_1234.com", is highlighted with a blue background. At the bottom right of the list area are two buttons: "Delete" and "Add New". At the very bottom of the interface are two buttons: "Save" and "Cancel".

步驟 1.選擇要刪除的域。

Add :

步驟 2. 按一下「Delete」。域即被刪除。

步驟 3. 按一下「Save」以儲存變更。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。