

CVR100W VPN路由器上的基本防火牆配置

目標

防火牆是一組旨在保護網路安全的功能。路由器被視為強大的硬體防火牆。這是因為路由器能夠檢查所有傳入流量並捨棄任何不需要的封包。本文說明如何在CVR100W VPN路由器上配置基本防火牆設定。

適用的裝置

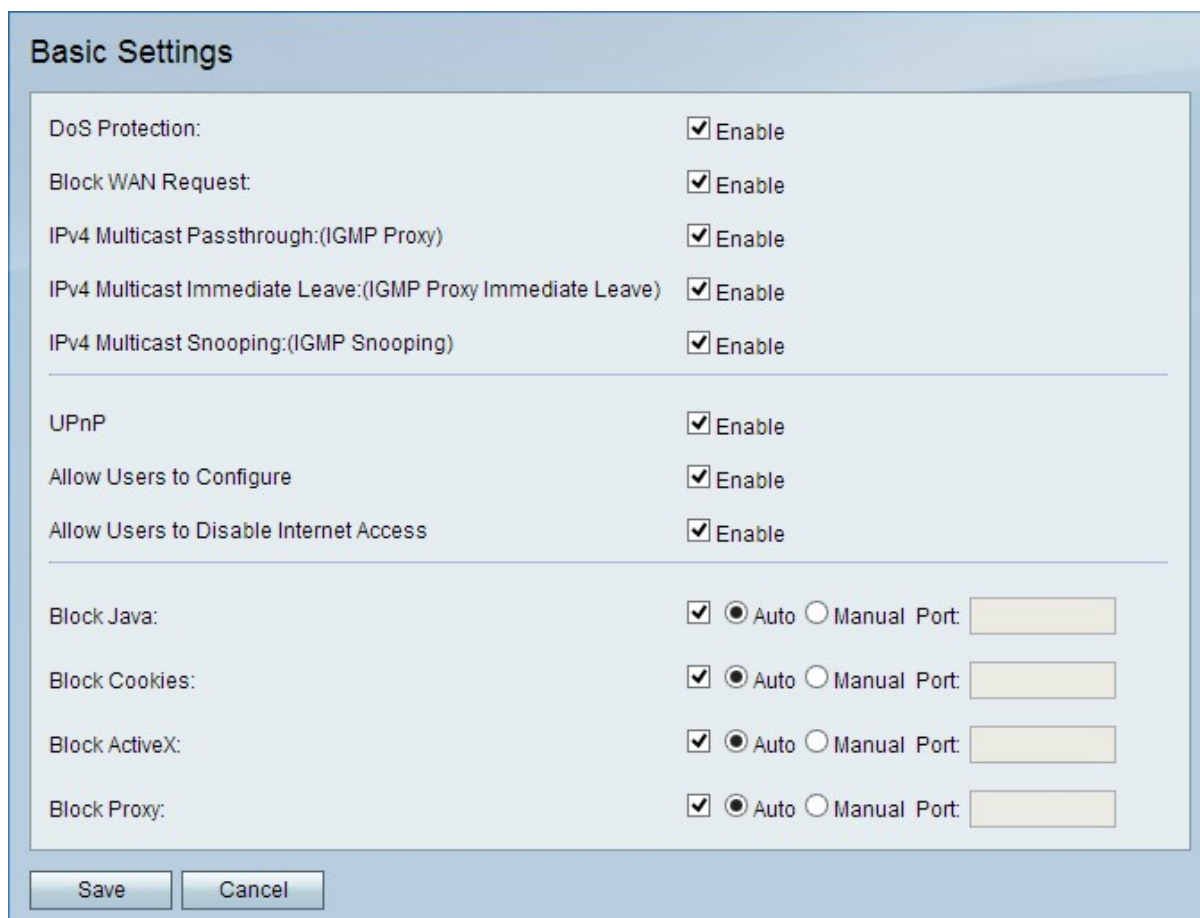
·CVR100W

軟體版本

•1.0.1.19

基本防火牆配置

步驟1.登入到Web配置實用程式並選擇Firewall > Basic Settings。將開啟Basic Settings頁面：



Basic Settings	
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Request:	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Snooping:(IGMP Snooping)	<input checked="" type="checkbox"/> Enable
<hr/>	
UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input checked="" type="checkbox"/> Enable
<hr/>	
Block Java:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
<hr/>	
<input type="button" value="Save"/>	<input type="button" value="Cancel"/>

附註：步驟2到13是可選的。您可以根據需要配置這些選項。

步驟2.要在CVR100W上啟用拒絕服務(DoS)保護，請在「DoS保護」欄位中選中**Enable**。DoS保護用於防止網路遭受分散式拒絕服務(DDoS)攻擊。DDoS攻擊旨在將網路泛洪到網路資

源不可用的程度。CVR100W使用DoS保護，通過限制和刪除不需要的資料包來保護網路。

步驟3.要阻止從WAN到CVR100W的所有ping請求，請選中Block WAN Request欄位中的**Enable**。

步驟4.若要允許IPv4多點傳送流量從網際網路通過CVR100W，請在IPv4 Multicast Passthrough欄位中勾選**Enable**。IP多點傳送是一種方法，用於在單次傳輸中將IP資料包傳送至指定的接收者群組。

步驟5. IGMP代理是路由器使用IGMP消息傳遞與其他裝置互動的一種方式。立即離開使CVR100W能夠以最佳速度離開組播組。要啟用IGMP代理立即離開，請在IPv4 Multicast Immediate Leave欄位中選中**Enable**。

步驟6.要啟用IGMP監聽（允許網路上的其他交換機監聽電腦和CVR100W之間來回傳送的消息），請在IPv4 Multicast Snooping欄位中選中**Enable**。

步驟7.若要啟用通用即插即用(UPnP)，請在UPnP欄位中勾選**Enable**。UPnP允許自動發現可與CVR100W通訊的裝置。

步驟8.為了允許具有支援UPnP裝置的使用者配置UPnP埠對映規則，請在Allow Users to Configure欄位中選中**Enable**。埠對映或埠轉發用於允許外部主機和專用LAN中提供的服務之間的通訊。

步驟9.為了允許使用者禁用對裝置的Internet訪問，請選中Allow Users to Disable Internet Access欄位中的**Enable**。

步驟10.要阻止下載Java小程式，請檢查「阻止Java」欄位中的**阻止Java**。出於惡意目的而建立的Java小程式可能對網路造成安全威脅。一旦下載，有敵意的java小程式就可以利用網路資源。點選與所需塊方法對應的單選按鈕。

- 自動 — 自動阻止java。
- 手動埠 — 輸入要在其中阻止java的特定埠。

步驟11.如果不希望網站建立Cookie，請選中Block Cookie欄位中的**Block Cookie**。Cookie由網站建立，用來儲存這些使用者的資訊。Cookie可以跟蹤使用者的網路歷史記錄，這可能導致隱私受到侵犯。點選與所需塊方法對應的單選按鈕。

- 自動 — 自動阻止cookie。
- 手動埠 — 輸入用於阻止cookie的特定埠。

步驟12.若要阻止下載ActiveX小程式，請檢查「阻止ActiveX」欄位中的**阻止ActiveX**。ActiveX是一種缺乏安全性的小程式。在電腦上安裝ActiveX小程式後，它可以執行使用者能夠執行的任何操作。它可能會在作業系統中插入有害代碼、瀏覽安全內部網、更改密碼，或者檢索並傳送文檔。點選與所需塊方法對應的單選按鈕。

- 自動 — 自動阻止ActiveX。
- 手動埠 — 輸入用於阻止ActiveX的特定埠。

步驟13.若要封鎖代理伺服器，請檢查Block Proxy欄位中的**Block Proxy**。代理伺服器是在兩個不同的網路之間提供鏈路的伺服器。惡意代理伺服器可以記錄傳送給它們的所有未加密資料，如登入名或密碼。點選與所需塊方法對應的單選按鈕。

- 自動 — 自動阻止代理伺服器。

·手動埠 — 輸入用於阻止代理伺服器的特定埠。

步驟14.按一下**Save**以儲存所做的任何更改。