

適用於RV160/RV260路由器的DMZ選項

目標

本文檔將介紹在RV160X/RV260X系列路由器上設定非軍事區 — DMZ主機和DMZ子網的兩個選項。

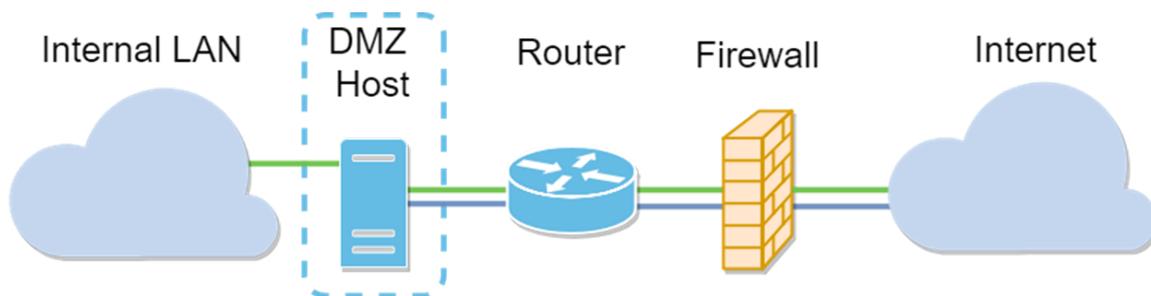
需求

- RV160X
- RV260X

簡介

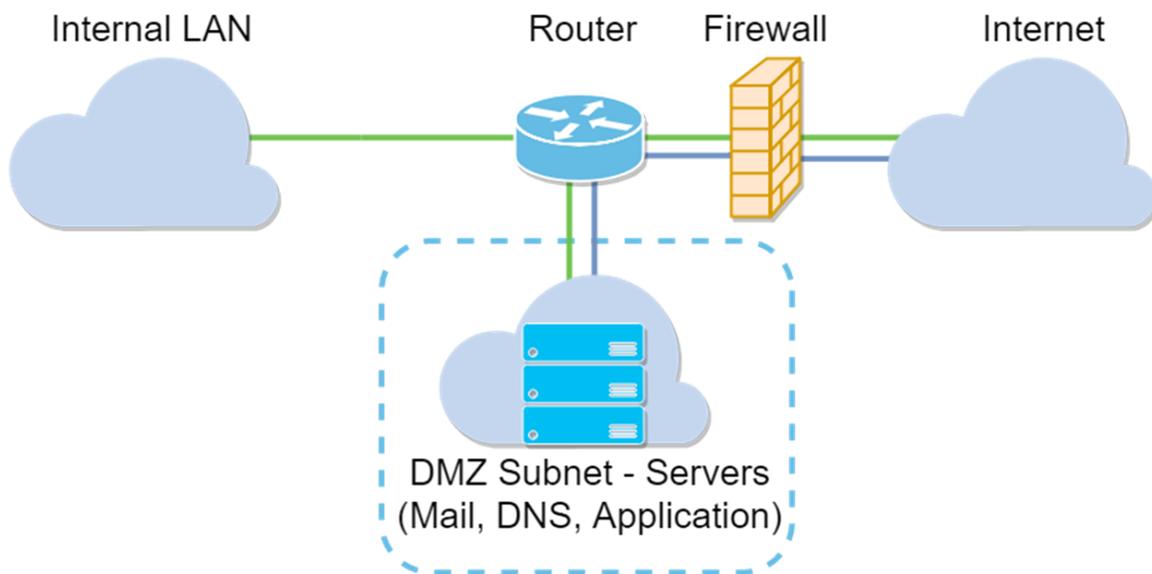
DMZ是網路中的一個位置，它對Internet開放，同時保護防火牆後的區域網(LAN)。將主網路與單個主機、整個子網或「子網」分隔開，可確保通過DMZ訪問您的網站伺服器的人無法訪問您的LAN。思科提供兩種在您的網路中使用DMZ的方法，這兩種方法在運行方式上都有重要區別。下面是視覺參考，突出顯示了兩種操作模式之間的差異。

主機DMZ拓撲



附註：使用主機DMZ時，如果主機被惡意攻擊者破壞，您的內部LAN可能會受到進一步的安全入侵。

子網DMZ拓撲



DMZ型別	比較	對比度
主機	隔離流量	單個主機，完全開啟網際網路
子網/範圍	隔離流量	多種裝置和型別，完全開啟網際網路。僅適用於RV260硬體。

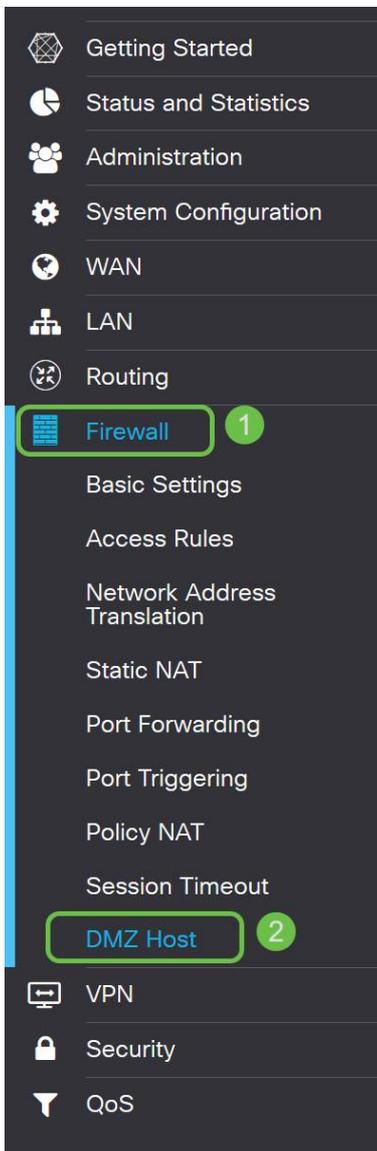
關於IP定址

本文使用IP編址方案，這些方案在使用上有一定的細微差別。在規劃DMZ時，可以考慮使用私有或公有IP地址。私有IP地址對您來說是唯一的，只在LAN上。公共IP地址對於您的組織來說是唯一的，並且由您的Internet服務提供商分配。要獲取公共IP地址，您需要聯絡您的(ISP)。

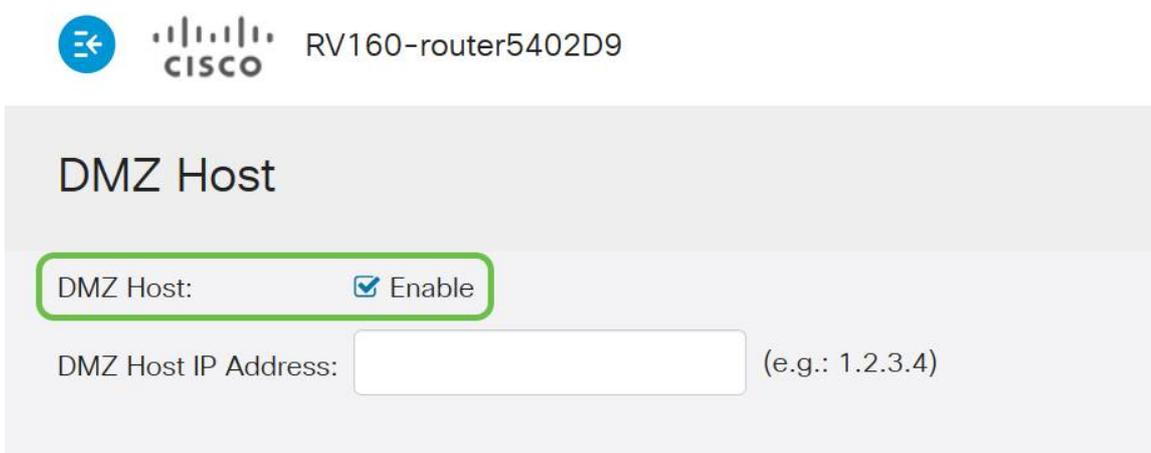
配置DMZ主機

此方法所需的資訊包括目標主機的IP地址。IP地址可以是公有地址也可以是私有地址，但公有IP地址應該與WAN IP地址處於不同的子網中。RV160X和RV260X上均提供DMZ Host選項。按照以下步驟配置DMZ主機。

步驟1。登入到路由裝置後，在左側選單欄中按一下**Firewall > DMZ Host**。



步驟2.按一下**Enable**覈取方塊。



步驟3.輸入您要開啟以訪問WAN的主機的指定IP地址。



RV160-router5402D9

DMZ Host

DMZ Host: Enable

DMZ Host IP Address: (e.g.: 1.2.3.4)

步驟4.對您的編址方案滿意時，按一下apply按鈕。

Apply

Cancel

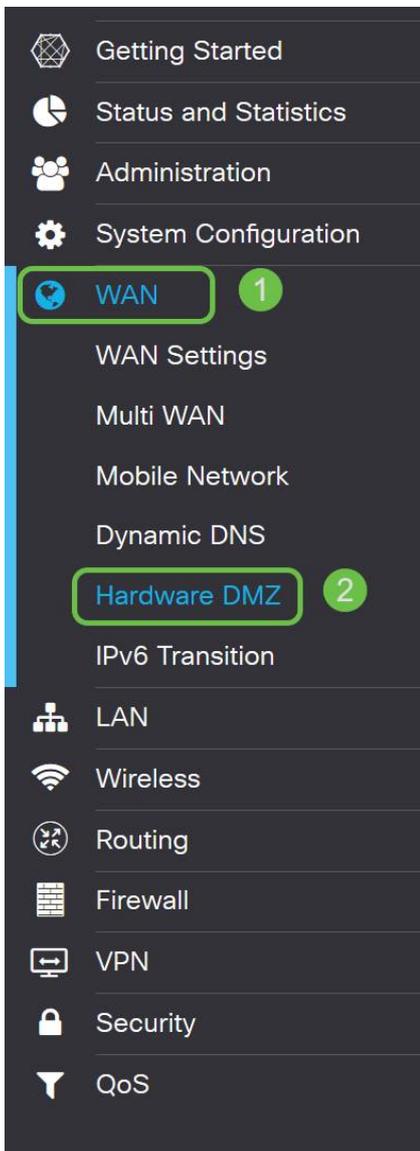
附註：如果您僅使用RV160X系列並且想要跳至驗證說明，請按一下此處[轉到本文檔的該部分](#)。

配置硬體DMZ

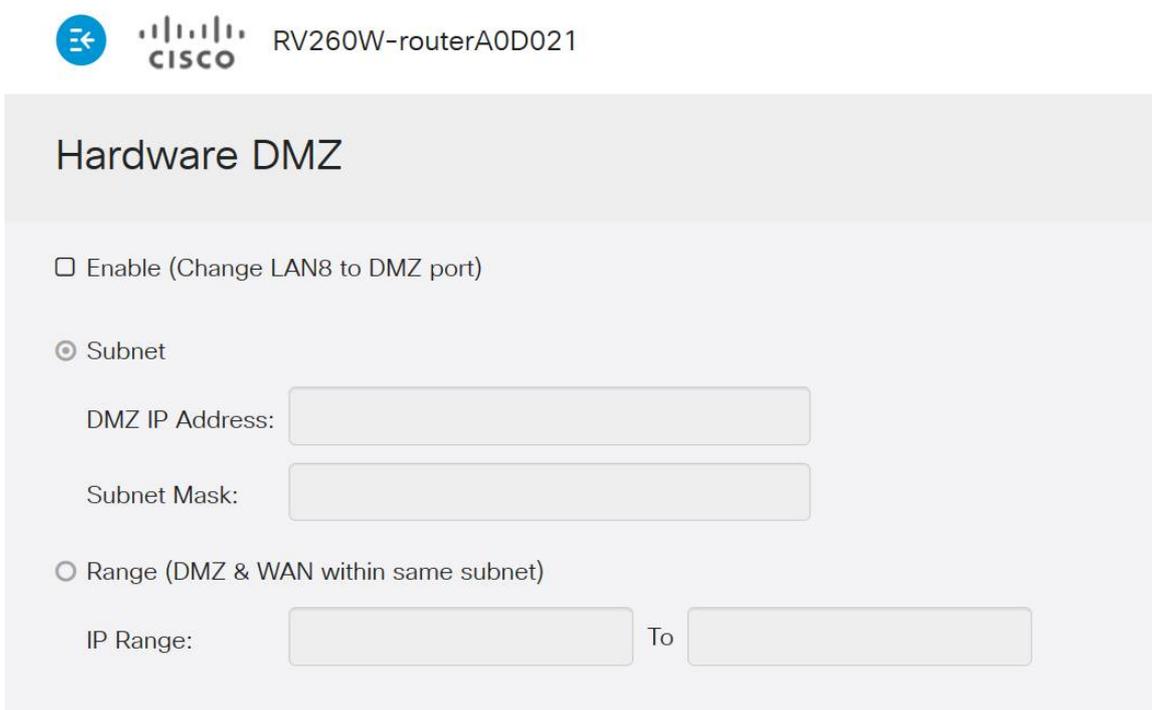
此方法僅適用於RV260X系列，需要根據您選擇的方法提供不同的IP編址資訊。這兩種方法實際上都使用子網來定義非軍事區，不同之處在於子網用於建立非軍事區的量。在本例中，選項為 — *all*或*部分*。子網(*all*)方法需要DMZ本身的IP地址以及子網掩碼。此方法佔用屬於該子網的所有IP地址。而Range(*some*)方法允許您定義要位於DMZ內的連續IP地址範圍。

附註：無論哪種情況，您都需要與您的ISP合作來定義子網的IP編址方案。

步驟1.登入到RV260X裝置後，按一下WAN > Hardware DMZ



附註：螢幕截圖取自RV260X使用者介面。下面是此頁面上顯示的硬體DMZ選項的螢幕截圖。



步驟2.按一下**Enable (將LAN8更改為DMZ埠)** 覈取方塊。這會將路由器上的第8個連線埠轉換為僅DMZ「視窗」，轉換為需要增強安全性的服務。

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

步驟3.按一下**Enable**後，資訊性消息顯示在可選選項的下方。檢視可能影響您網路的點的詳細資訊，然後按一下**OK, I agree with above**復選框。

 When hardware DMZ is enabled, the dedicated DMZ Port (LAN8) will be:

- * Disabled as Port Mirror function, if Port Mirror Destination is DMZ Port (LAN > Port Settings);
- * Removed from LAG Port (LAN > Port Settings);
- * Removed from Monitoring Port of Port Mirror (LAN > Port Settings);
- * Changed to "Force Authorized" in Administrative State (LAN > 802.1X Configuration);
- * Changed to "Excluded" in "Assign VLANs to ports" table (LAN > VLAN Settings).

OK, I agree with the above.

步驟4.下一步分為兩個可能的選項：子網和範圍。在下面的示例中，我們選擇了子網方法。

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address: 164.33.100.250

Subnet Mask: 255.255.255.248

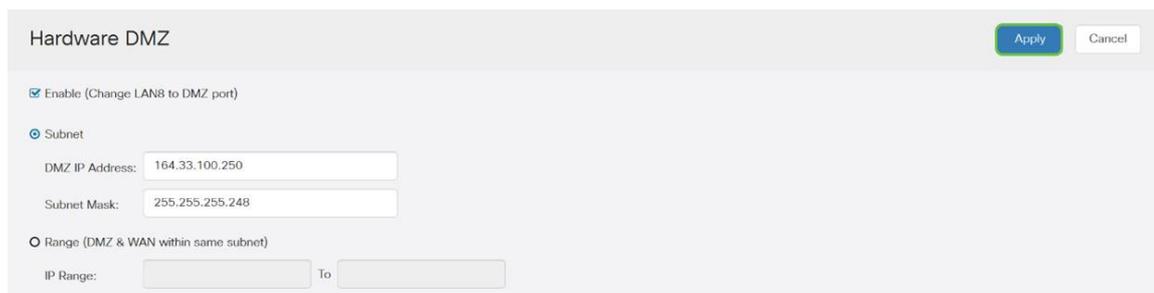
Range (DMZ & WAN within same subnet)

IP Range:

To

附註：如果您打算使用Range方法，則需要按一下**Range**單選按鈕，然後輸入ISP分配的IP地址範圍。

步驟6. 按一下**Apply** (在右上角) 接受DMZ設定。

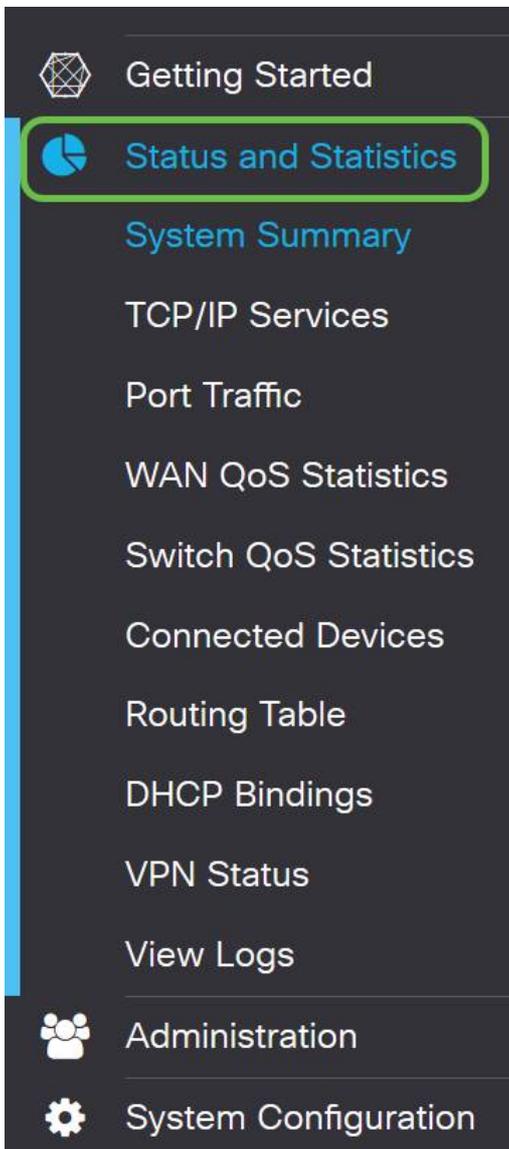


The screenshot shows the 'Hardware DMZ' configuration page. The 'Enable' checkbox is checked. The 'Subnet' radio button is selected. The 'DMZ IP Address' field contains '164.33.100.250' and the 'Subnet Mask' field contains '255.255.255.248'. The 'Range' radio button is unselected. The 'IP Range' and 'To' fields are empty. In the top right corner, the 'Apply' button is highlighted in green, and the 'Cancel' button is in grey.

確認DMZ設定正確

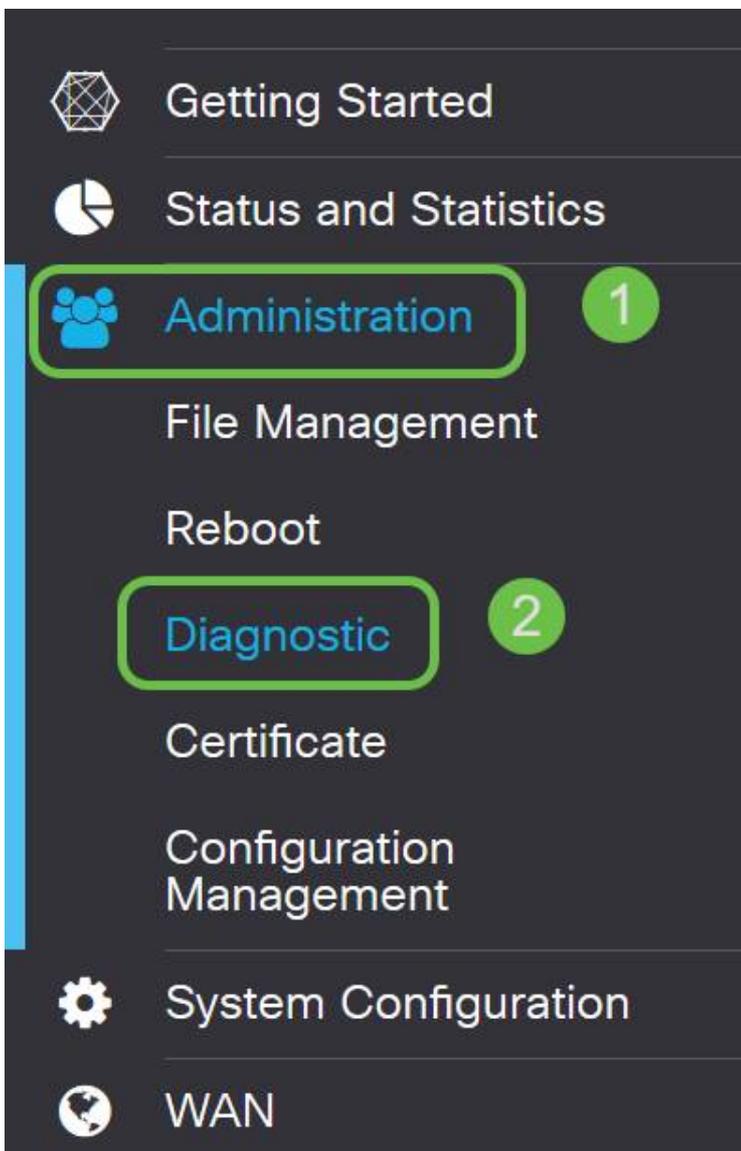
檢驗DMZ是否配置為可適當接受來自其區域外部的流量，ping測試就足夠了。首先，我們將通過管理介面檢查DMZ的狀態。

步驟1. 若要確認您的DMZ是否已設定，請導覽至**Status & Statistics**，頁面將會自動載入System Summary頁面。連線埠8或「Lan 8」會將DMZ的狀態列為「*Connected*」。



我們可以使用可信的ICMP ping功能測試DMZ是否按預期運行。ICMP訊息（或只是「ping」）會嘗試敲打DMZ的門。如果DMZ回應說「Hello」，ping操作完成。

步驟2.要將瀏覽器導航至ping功能，請按一下**Administration > Diagnostic**。



步驟3.輸入DMZ的IP地址，然後點選Ping按鈕。



如果ping成功，您會看到類似上述的消息。如果ping失敗，則表示無法訪問DMZ。檢查您的DMZ設定，確保它們配置正確。

結論

現在，您已經完成了DMZ的設定，應該能夠從LAN外部訪問服務。