

在RV042、RV042G和RV082 VPN路由器上非軍事區(DMZ)中配置多個公共IP

目標

隔離區(DMZ)是一個組織的內部網路，可供不受信任的網路使用。根據安全性，DMZ位於受信任和不受信任的網路之間。維護DMZ有助於提高組織內部網路的安全性。當訪問控制清單(ACL)繫結到介面時，其訪問控制元素(ACE)規則將應用於到達該介面的資料包。與「訪問控制清單」中的任何ACE都不匹配的資料包與預設規則相匹配，預設規則的操作是丟棄不匹配的資料包。

本文檔的目標是向您展示如何配置DMZ埠以允許多個公共IP地址，並為路由器裝置上的IP定義訪問控制清單(ACL)。

適用裝置

- RV042
- RV042G
- RV082

軟體版本

- v4.2.2.08

DMZ配置

步驟 1. 登入到Web Configuration Utility頁面並選擇Setup > Network。此時將打開Network頁：

Network

Host Name : (Required by some ISPs)

Domain Name : (Required by some ISPs)

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4

IPv6

LAN Setting

MAC Address : 50:57:A8:79:F3:7A

Device IP Address :

Subnet Mask :

Multiple Subnet : Enable

WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

DMZ Setting

Enable DMZ

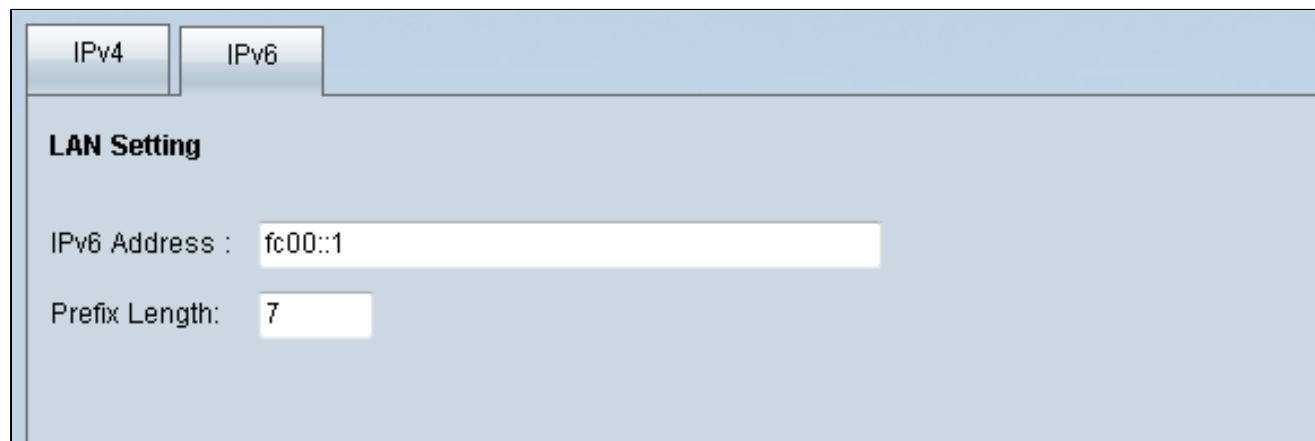
Interface	IP Address	Configuration
DMZ	0.0.0.0	

步驟 2.在IP Mode 欄位中，按一下Dual-Stack IP 單選按鈕以啟用IPv6地址配置。

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

步驟 3.按一下位於LAN Setting 欄位中的IPv6頁籤，以便能夠在IPv6地址上配置DMZ。



The screenshot shows the 'LAN Setting' configuration page with the 'IPv6' tab selected. The 'IPv6 Address' field is set to 'fc00::1' and the 'Prefix Length' field is set to '7'.

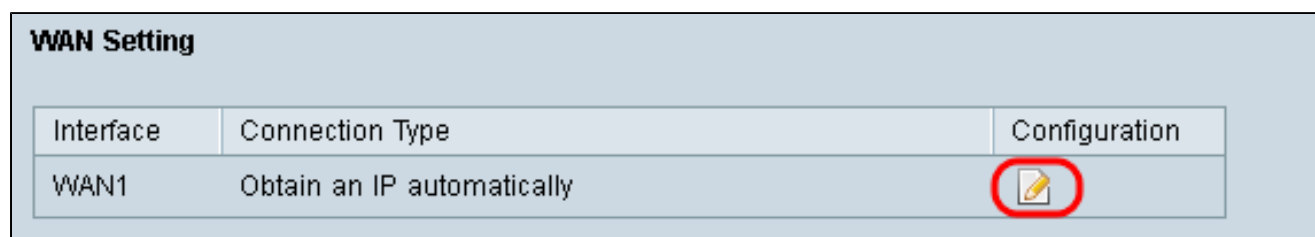
步驟4.向下滾動到DMZ Setting區域，然後按一下DMZ覈取方塊以啟用DMZ




The screenshot shows the 'DMZ Setting' section. The 'Enable DMZ' checkbox is checked and circled in red. Below it is a table with columns for Interface, IP Address, and Configuration.

Interface	IP Address	Configuration
DMZ	::64	

步驟 5.在WAN Setting 欄位中，按一下Edit按鈕以編輯WAN1設定的IP Static。



The screenshot shows the 'WAN Setting' section. A table lists WAN1 with the connection type 'Obtain an IP automatically'. The 'Configuration' column for WAN1 contains an edit icon circled in red.

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

此時將打開Network頁：

Network

Edit WAN Connection

Interface : WAN1

WAN Connection Type : Static IP

Specify WAN IP Address : 192.168.3.1

Subnet Mask : 255.255.255.0

Default Gateway Address : 192.168.3.2

DNS Server (Required) 1 : 0.0.0.0

2 : 0.0.0.0

MTU : Auto Manual 1500 bytes

Save Cancel

步驟 6.從WAN Connection Type下拉選單中選擇Static IP。

步驟 7.在指定WAN IP地址欄位中輸入顯示在System Summary頁上的WAN IP地址。

步驟 8.在Subnet Mask欄位中輸入子網掩碼地址。

步驟 9.在Default Gateway Address欄位中輸入預設網關地址。

步驟 10.在DNS Server (Required) 1欄位中輸入顯示在System Summary頁上的DNS伺服器地址。

注意：DNS伺服器地址2是可選的。

步驟 11.選擇自動或手動作為「最大傳輸單位(MTU)」。如果選擇手動，請輸入手動MTU的位元組數。

步驟 12. 按一下Save頁籤以儲存設定。

ACL定義

步驟 1. 登入到Web Configuration Utility頁並選擇Firewall > Access Rules。此時將打開Access Rules頁：



The screenshot shows the 'Access Rules' configuration page. At the top, there are tabs for 'IPv4' and 'IPv6'. Below the tabs, there is a summary bar indicating 'Item 1-3 of 3 Rows' and 'per page : 5'. The main content is a table with the following columns: Priority, Enable, Action, Service, Source Interface, Source, Destination, Time, Day, and Delete. The table contains three rows of rules:

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

At the bottom of the table, there are buttons for 'Add' and 'Restore to Default Rules'. On the right side, there are navigation arrows and a page indicator 'Page 1 of 1'.

附註：當您輸入「存取規則」頁面時，無法編輯預設的存取規則。

步驟 2. 按一下Add按鈕以增加新的訪問規則。



This screenshot is identical to the previous one, but the 'Add' button at the bottom left of the table is highlighted with a red circle.

現在，訪問規則頁將顯示服務和排程區域的選項。

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

步驟 3. 從Action下拉選單中選擇Allow以允許該服務。

步驟 4. 從Service下拉選單中選擇All Traffic [TCP&UDP/1-65535] 以啟用DMZ的所有服務。

步驟 5. 從Log下拉選單中選擇Log packets match this rule，以僅選擇與訪問規則匹配的日誌。

步驟 6. 從Source Interface下拉選單中選擇DMZ。這是存取規則的來源。

步驟 7. 從Source IP下拉選單中選擇Any。

步驟 8. 從Destination IP下拉選單中選擇Single。

步驟 9.在Destination IP欄位中輸入允許訪問規則的目標的IP地址。

步驟 10.在Scheduling區域中，從Time下拉選單中選擇Always，以使訪問規則始終處於活動狀態。

注意：如果從Time下拉選單中選擇Always，則訪問規則預設情況下將在Effective on欄位中設定為Everyday。

注意：您可以從時間下拉選單中選擇間隔來選擇特定的時間間隔(訪問規則對此有效)。然後，您可以從有效於覈取方塊中選擇希望訪問規則處於活動狀態的天。

步驟 11.按一下Save儲存設定。

注意：如果出現彈出窗口，請按「確定」增加其他訪問規則，或按「取消」返回「訪問規則」頁。

現在會顯示您在上一步中建立的存取規則

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	DMZ	Any	192.168.10.27 ~ 192.168.10.27	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	DMZ	Any	Any	Always		

步驟 12.按一下Edit圖示編輯已建立的訪問規則。

步驟 13.按一下刪除圖示以刪除建立的存取規則。

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）。