

在RV016、RV042、RV042G和RV082 VPN路由器上配置帶子網掩碼的非軍事化區域埠

目標

非軍事區(DMZ)是組織內部網路的一部分，它可用於不可信網路，例如Internet。DMZ有助於提高組織內部網路的安全性。不是所有內部資源都可以從Internet訪問，而是只有某些主機（如Web伺服器）可用。

當訪問控制清單(ACL)繫結到介面時，訪問控制元素(ACE)規則將應用於到達該介面的資料包。與ACL中的任何ACE都不匹配的資料包將匹配到預設規則，預設規則的操作是丟棄不匹配的資料包。本文介紹如何設定DMZ連線埠並允許流量從DMZ到達特定目的地IP位址。

適用裝置

- RV016
- RV042
- RV042G
- RV082

軟體版本

- v4.2.2.08

帶子網的DMZ配置

步驟 1. 登入到Router Configuration Utility頁面，然後選擇Setup > Network。Network 頁面隨即開啟：

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 : 64:9E:F3:88:C6:88

Device IP Address :

Subnet Mask :


Multiple Subnet : Enable

WAN Setting

Interface	Connection Type	Configuration
WAN1	Static IP	

DMZ Setting

Enable DMZ

Interface	IP Address	Configuration
DMZ	0.0.0.0	

步驟 2. 要在IPv4或IPv6地址上配置DMZ，請按一下LAN Setting (LAN設定) 欄位中的相應頁籤。

注意：如果要配置IPv6,必須啟用IP模式區域中的雙堆疊IP。

步驟 3. 向下滾動到DMZ Setting欄位，然後點選Enable DMZ單選按鈕以啟用DMZ。

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	
WAN2	Obtain an IP automatically	

Interface	IP Address	Configuration
DMZ	0.0.0.0	

步驟 4. 按一下DMZ配置圖示配置子網。IPv4和IPv6的[配置](#)可以以下方式完成：

IPv4組態

Network

Edit DMZ Connection

Interface : DMZ

Subnet Range (DMZ & WAN within same subnet)

Specify DMZ IP Address : 10.10.10.1

Subnet Mask : 255.255.255.0

Save Cancel

步驟 5. 按一下Subnet單選按鈕，將DMZ配置為與WAN不同的另一個子網。對於子網IP，應配置以下內容

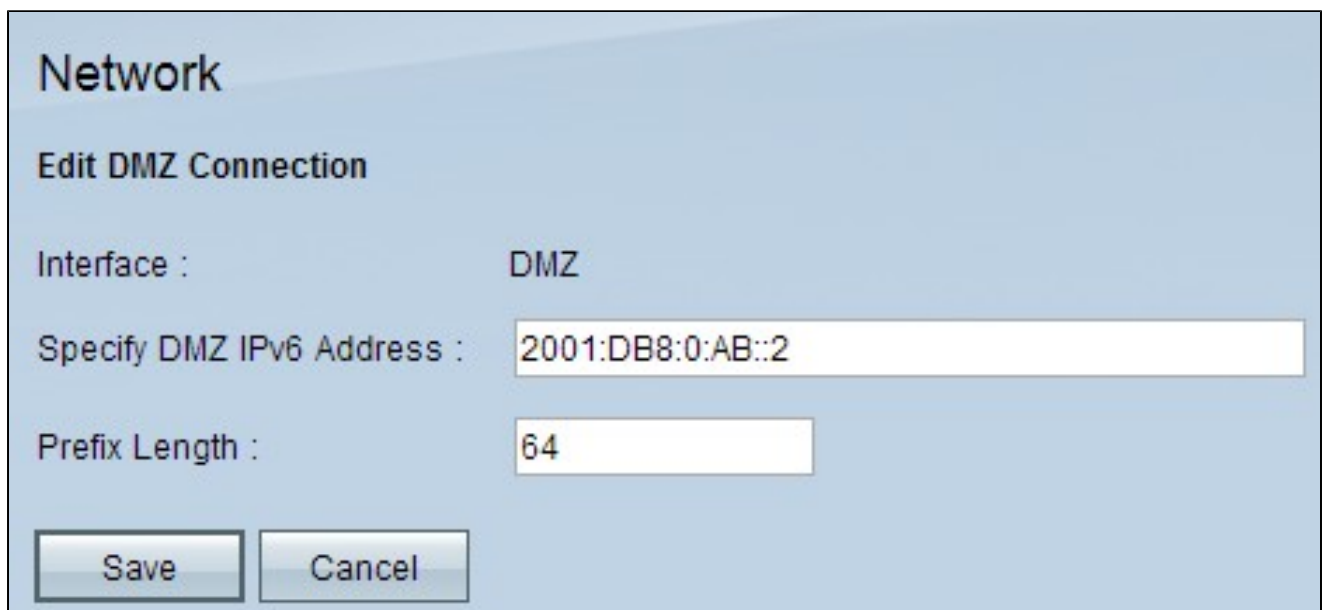
·指定DMZ IP地址 — 在指定DMZ IP地址欄位中輸入DMZ IP地址。

·子網掩碼 — 在子網掩碼欄位中輸入子網掩碼。

警告：DMZ中具有IP地址的主機不如內部LAN中的主機安全。

步驟 6.按一下Range將DMZ配置為與WAN位於同一子網中。在DMZ埠的IP範圍欄位中輸入IP地址範圍。

IPv6配置



The screenshot shows a 'Network' configuration window titled 'Edit DMZ Connection'. The 'Interface' is set to 'DMZ'. The 'Specify DMZ IPv6 Address' field contains the value '2001:DB8:0:AB::2'. The 'Prefix Length' field contains the value '64'. At the bottom of the window, there are two buttons: 'Save' and 'Cancel'.

注意：對於IPv6配置，可以使用以下選項：

步驟 7.指定DMZ IPv6地址 — 輸入IPv6地址。

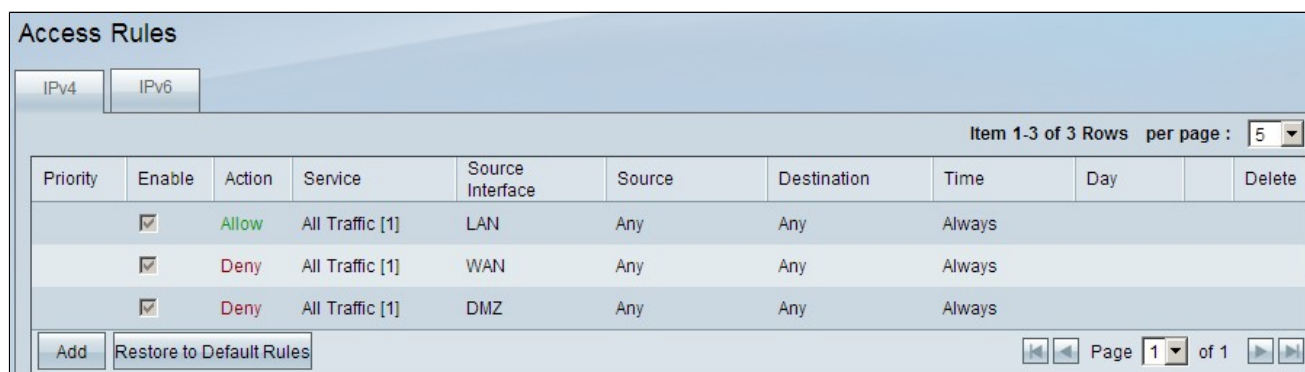
步驟 8.字首長度 — 要輸入上面提到的DMZ IP地址域的字首長度。

步驟 9.按一下「Save」以儲存組態。

訪問規則配置

完成此配置是為了定義在多個子網掩碼上配置的IP的訪問清單。

步驟 1. 登入到 Router Configuration Utility 頁面，然後選擇 Firewall > Access Rules。Access Rules 頁面隨即開啟：



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		

Item 1-3 of 3 Rows per page : 5

Add Restore to Default Rules Page 1 of 1

注意：無法編輯預設訪問規則。

步驟 2. 按一下 Add 按鈕新增新訪問規則。Access Rules 頁面將更改，以顯示「服務」和「排程」區域。

注意：通過選擇 Access Rules 頁面上的相應頁籤，可以對 IPv4 和 IPv6 執行此配置操作。以下步驟中提到 IPv4 和 IPv6 特定的配置步驟。

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 that match this rule，以僅選擇與訪問規則匹配的日誌。

步驟 6.從Source Interface下拉式清單中選擇DMZ，該清單是存取規則的來源。

步驟 7.從Source IP下拉選單中選擇Any。

步驟 8.從Destination IP下拉選單中選擇以下任何可用選項。

- Single — 選擇Single可將此規則應用於單個IP地址。
- 範圍 — 選擇範圍，將此規則應用於某個IP地址範圍。輸入範圍的第一個和最後一個IP地址。此選項僅在IPv4中可用。
- 子網 — 選擇子網以將此規則應用於子網。輸入IP地址和CIDR表示法編號，用於分配IP地址和路由子網的Internet協定資料包。此選項僅在IPv6中可用。
- Any — 選擇Any將規則應用於任何IP地址。

Timesaver：如果要配置IPv6訪問規則，請跳至步驟10。

步驟 9.從Time下拉選單中選擇要定義規則何時處於活動狀態的方法。它們是：

- 始終 — 如果從「時間」下拉選單中選擇「始終」，訪問規則將始終應用於流量。
- Interval — 如果從Time下拉選單中選擇Interval，則可以選擇訪問規則處於活動狀態的特定時間間隔。指定時間間隔後，從「生效時間」覈取方塊中選擇希望訪問規則處於活動狀態的天數。

步驟 10.按一下Save儲存設定。

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		

Item 1-4 of 4 Rows per page : 5

Add Restore to Default Rules Page 1 of 1

步驟 11.按一下Edit圖示編輯建立的訪問規則。

步驟 12.按一下Delete圖示可刪除建立的訪問規則。

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）。