

# 在RV042、RV042G和RV082 VPN路由器上的去军事化区域(DMZ)中配置多个公共IP

## 目标

隔离区(DMZ)是一个组织的内部网络，可用于不受信任网络。根据安全性，DMZ位于受信任和不受信任的网络之间。维护DMZ有助于提高组织内部网络的安全性。当访问控制列表(ACL)绑定到接口时，其访问控制元素(ACE)规则将应用于到达该接口的数据包。与访问控制列表中的任何ACE都不匹配的数据包与默认规则匹配，默认规则的操作是丢弃不匹配的数据包。

本文档的目的是向您展示如何配置DMZ端口以允许多个公有IP地址，并为路由器设备上的IP定义访问控制列表(ACL)。

## 适用设备

- RV042
- RV042G
- RV082

## 软件版本

- v4.2.2.08

## DMZ配置

步骤1:登录到Web配置实用程序页面，然后选择Setup > Network。网络页面打开：

## 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

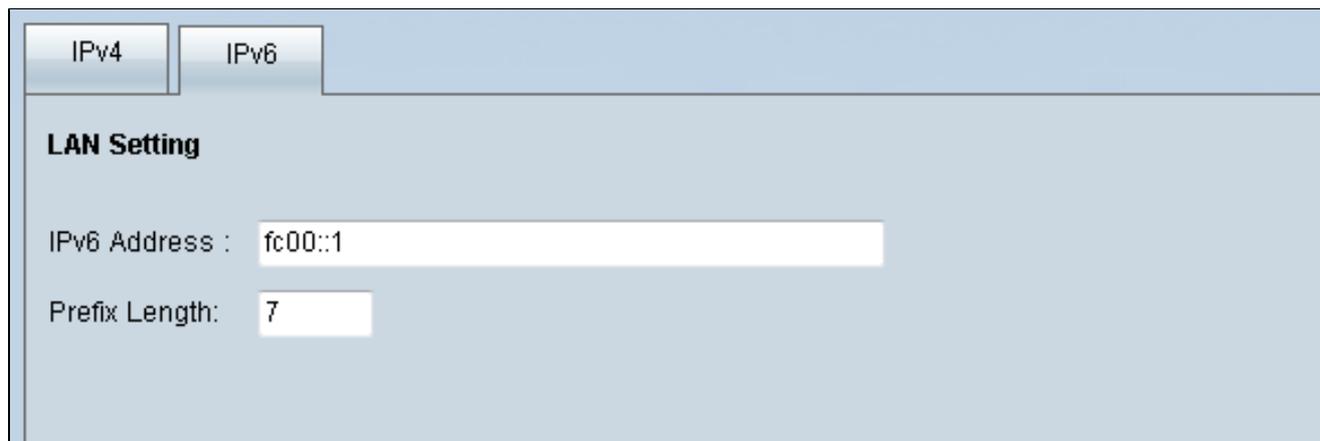
Interface	IP Address	Configuration
DMZ	0.0.0.0	

第二步：在IP Mode字段中，单击Dual-Stack IP单选按钮以启用IPv6地址的配置。

### IP Mode

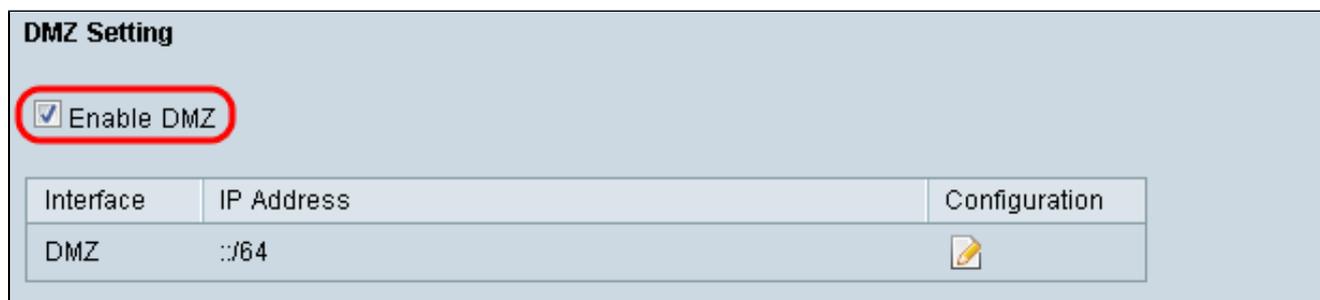
Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

第三步：单击LAN Setting字段中的IPv6选项卡，以便能够在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'.

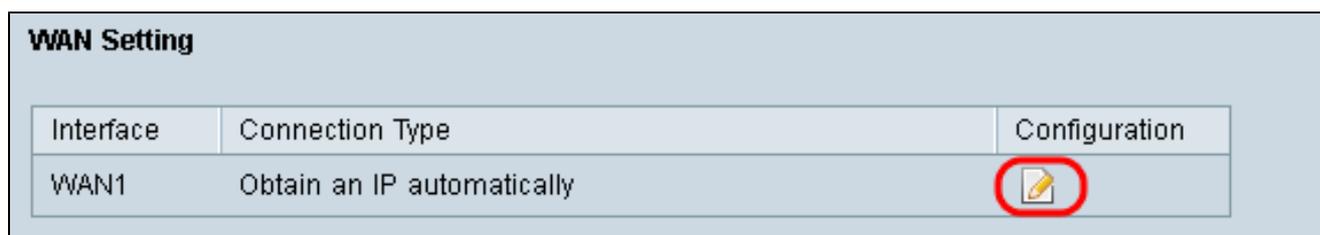
步骤4.向下滚动到DMZ设置区域，然后点击DMZ复选框以启用DMZ



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	

第五步：在WAN Setting字段中，单击Edit按钮以编辑WAN1设置的IP Static。



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

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

Network页面打开：

## 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

第六步：从WAN Connection Type下拉列表中选择Static IP。

步骤 7.在Specify WAN IP Address字段中输入显示在System Summary页上的WAN IP地址。

步骤 8在子网掩码字段中输入子网掩码地址。

步骤 9在默认网关地址字段中输入默认网关地址。

步骤 10在DNS Server(Required)1字段中输入显示在System Summary页面上的DNS Server地址。

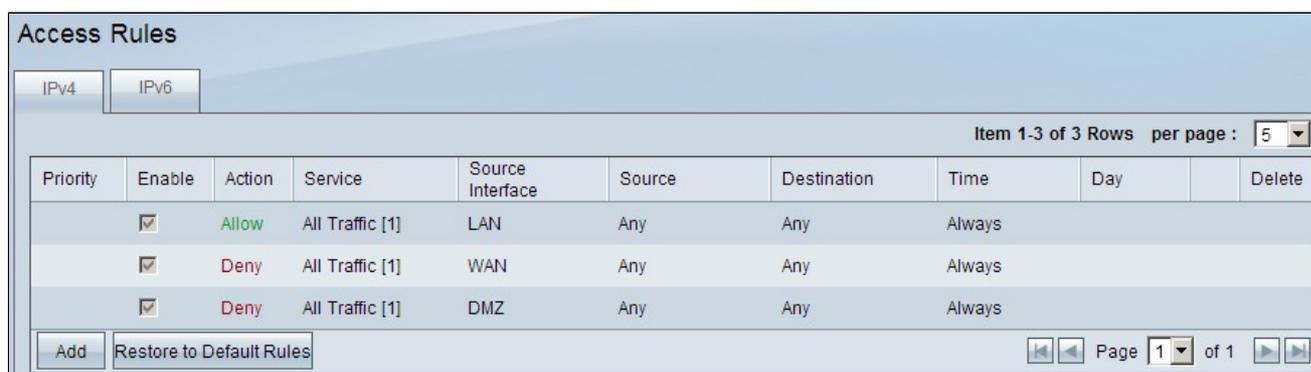
注意：DNS服务器地址2是可选的。

步骤 11选择最大传输单位(MTU)为自动或手动。如果选择手动，请输入手动MTU的字节。

步骤 12单击Save选项卡保存设置。

## ACL定义

步骤1:登录到Web Configuration Utility页面，然后选择Firewall > Access Rules。将打开访问规则页面：



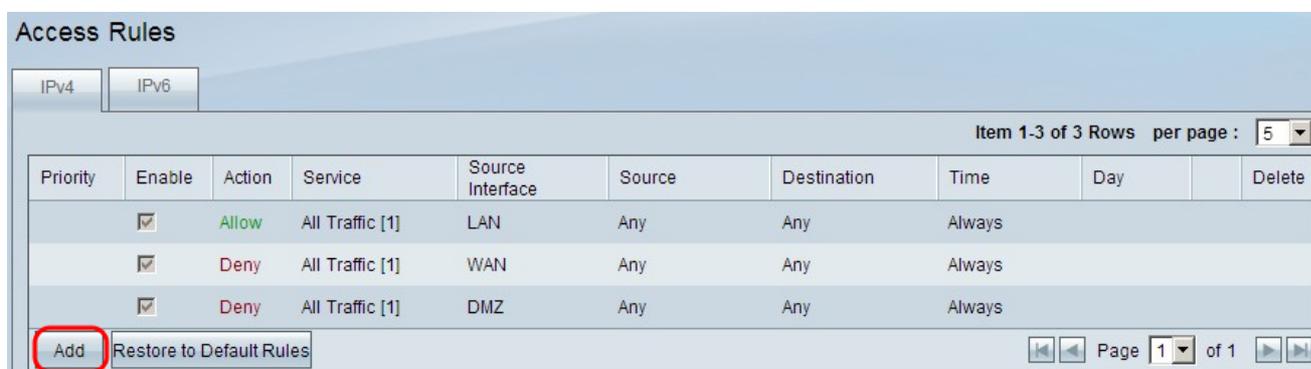
The screenshot shows the 'Access Rules' configuration page. At the top, there are tabs for 'IPv4' and 'IPv6'. Below the tabs, there is a summary bar indicating 'Item 1-3 of 3 Rows' and 'per page : 5'. The main part of the page is a table with the following columns: Priority, Enable, Action, Service, 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'.

注意：输入Access Rules页面时，无法编辑默认访问规则。

第二步：单击Add按钮以添加新的访问规则。



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

Access Rules页面现在将显示Service和Scheduling区域的选项。

## 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

第三步：从操作下拉列表中选择允许以允许该服务。

第四步：从Service下拉列表中选择All Traffic [TCP&UDP/1~65535] 以启用DMZ的所有服务。

第五步：从Log下拉列表中选择Log packets match this rule，以仅选择与访问规则匹配的日志。

第六步：从Source Interface下拉列表中选择DMZ。这是访问规则的来源。

步骤 7.从Source IP下拉列表中选择Any。

步骤 8从Destination IP下拉列表中选择Single。

步骤 9在Destination IP字段中输入允许访问规则的目标IP地址。

步骤 10在Scheduling区域中，从Time下拉列表中选择Always，以使访问规则始终处于活动状态。

注：如果从Time下拉列表中选择Always，则默认情况下，访问规则将在Effective on字段中设置为Everyday。

注意：您可以通过从Time下拉列表中选择Interval来选择特定时间间隔(访问规则对其处于活动状态)。然后，您可以从Effective on复选框中选择希望访问规则处于活动状态的天数。

步骤 11单击Save保存设置。

注意：如果出现弹出窗口，请按“确定”添加另一个访问规则，或者按“取消”返回到“访问规则”页面。

此时将显示您在上一步中创建的访问规则



The screenshot shows the 'Access Rules' configuration page. It has tabs for 'IPv4' and 'IPv6'. Below the tabs, it indicates 'Item 1-4 of 4 Rows' and 'per page : 5'. The table contains the following data:

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		

At the bottom, there are buttons for 'Add' and 'Restore to Default Rules', and a pagination control showing 'Page 1 of 1'.

步骤 12单击Edit图标编辑创建的访问规则。

步骤 13点击Delete图标以删除创建的访问规则。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。