

# 多个公共IP的配置在非敏感区域(DMZ) RV042、RV042G和RV082 VPN路由器的

## 客观

非敏感区域(DMZ)是组织的一个内部网络，安排可用一个不信任的网络。根据安全，DMZ下跌在委托的和不信任的网络之间。DMZ的维护帮助改进安全ofto组织的内部网络。当访问控制表(ACL)一定对接口时，其访问控制元素(ACE)规则被运用于到达该接口的信息包。不匹配其中任一在访问控制表的ACE的信息包被匹配对动作是丢弃不匹配信息包的默认规则。

本文目标将显示您如何配置DMZ端口允许多个公共IP地址和定义IP的访问控制表(ACL)在路由器设备。

## 可适用的设备

- RV042
- RV042G
- RV082

## 软件版本

- v4.2.2.08

## 非军事区配置

步骤1.日志到Web配置实用工具页里和选择**设置>网络**。网络页打开：

## 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	

**Step 2.**在Mode字段的IP中，请点击Dual-Stack IP单选按钮对enable (event) IPv6地址的配置。

**步骤3.**点击位于LAN的IPv6选项setting字段能配置在IPv6地址的DMZ。

IPv4 IPv6

**LAN Setting**

IPv6 Address : fc00::1

Prefix Length: 7

步骤下来4.Scroll对设置区域的DMZ和点击DMZ复选框对enable (event) DMZ

**DMZ Setting**

Enable DMZ

Interface	IP Address	Configuration
DMZ	::64	

第 5 步：在setting字段的广域网中请点击编辑按钮编辑WAN1设置的IP静态。

**WAN Setting**

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	

网页打开：

**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

步骤6.从WAN连接类型下拉列表选择静态IP。

步骤7.输入在*IP Address*字段的指定广域网的系统汇总页显示的广域网IP地址。

步骤8.输入子网掩码地址在子网掩码字段。

步骤9.输入默认网关地址在默认网关地址字段。

步骤10.输入在*DNS服务器*的系统汇总页显示的DNS服务器地址(需要) 1个字段。

**Note:** DNS服务器地址2是可选的。

步骤11.选择最大传输单元(MTU)是**自动或指南**。如果选择指南请输入手工的MTU的字节。

步骤12. 点击**Save**选项保存您的设置。

## ACL定义

步骤1.日志到Web配置实用工具页里和选择**防火墙>Access规则**。访问规则页打开：

**Note:**当您进入时访问规定默认访问规则不可能被编辑的页。

步骤2.点击**Add**按钮增加一个新的访问规则。

访问规则页当前将显示**服务和安排**地区的选项。

### 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

步骤3.选择从动作下拉列表允许允许服务。

步骤4.从服务下拉列表选择所有数据流[TCP&UDP/1~65535]到enable (event) DMZ的所有服务。

步骤5.选择日志信息包匹配从日志下拉列表的此规则选择匹配访问规则仅的日志。

步骤6.从源接口下拉列表选择DMZ。这是访问规则的来源。

步骤7.从来源IP下拉列表选择其中任一。

步骤8.从目的地IP下拉列表选择单个。

步骤9.输入将提供的目的地的IP地址在目的地IP字段的访问规则。

第10.步。在安排地区中从时间下拉列表总是请选择一直做访问规则激活。

**Note:**如果从时间下拉列表总是选择，默认情况下访问规则将设置对每天在有效在字段。

**Note:**您能通过选择间隔选择特定时间时间间隔(哪些访问规则是活跃的)从时间下拉列表。然后，您能选择您希望访问规则是活跃的从有效在复选框的日。

步骤11.点击“Save”保存您的设置。

**Note:**如果弹出窗口出现请按‘好’增加另一个访问规则或者按‘取消’返回到访问规则页。

您在上一步创建的访问规则当前显示

步骤12。点击**Edit**图标编辑被创建的访问规则。

第13步。点击**Delete**图标删除被创建的访问规则。