在RV016、RV042、RV042G和RV082 VPN路由器上配置带子网掩码的去军事化区域端口

目标

非军事区(DMZ)是组织的内部网络的一部分，可用于不受信任的网络，例如Internet。DMZ有助于提高组织内部网络的安全性。并非所有内部资源都可从Internet访问，而是只有某些主机（如Web服务器）可用。

当访问控制列表(ACL)绑定到接口时，访问控制元素(ACE)规则应用于到达该接口的数据包。与ACL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。本文介绍如何配置DMZ端口并允许流量从DMZ传输到特定目标IP地址。

适用设备

- RV016
- RV042
- RV042G
- RV082

软件版本

- v4.2.2.08

带子网的DMZ配置

步骤1:登录到Router Configuration Utility页面，然后选择Setup > Network。网络页面打开：

Network

Host Name : router88c688 (Required by some ISPs)

Domain Name : router88c688.com (Required by some ISPs)

IP Mode

Mode	WAN	LAN
IPv4 Only	IPv4	IPv4
Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4 | IPv6

LAN Setting

MAC Address : 64:9E:F3:88:C6:88

Device IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

Multiple Subnet : Enable Add/Edit

WAN Setting

Interface	Connection Type	Configuration
WAN1	Static IP	

DMZ Setting

Enable DMZ

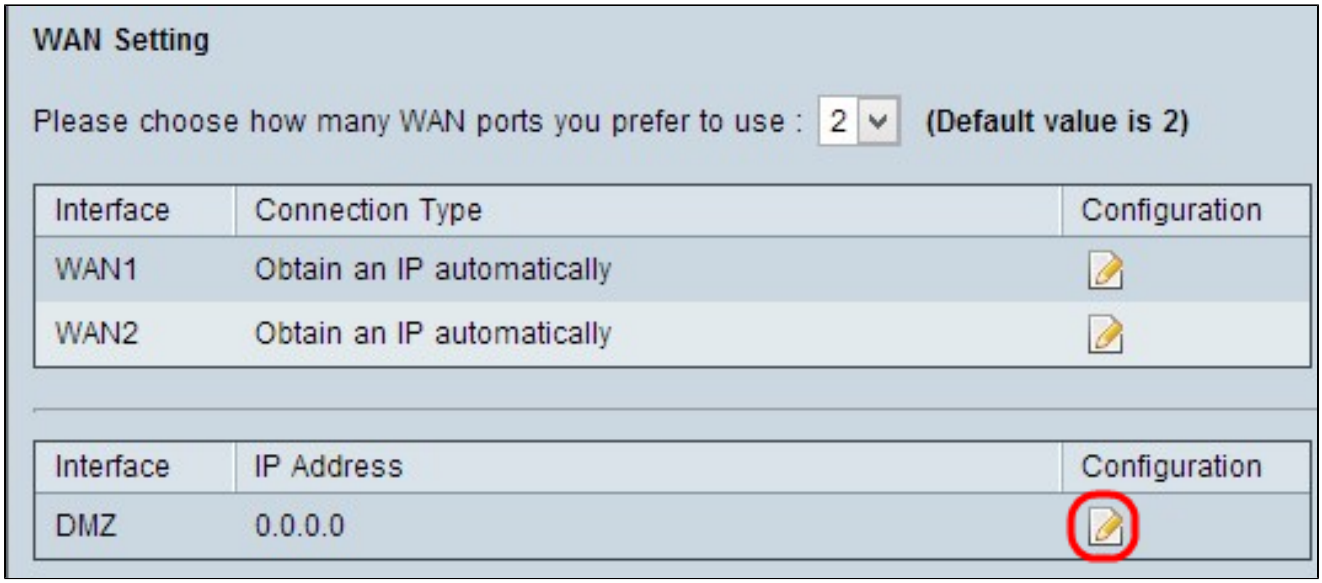
Interface	IP Address	Configuration
DMZ	0.0.0.0	

Save Cancel

第二步：要在IPv4或IPv6地址上配置DMZ，请点击LAN Setting（LAN设置）字段中的相应选项卡。

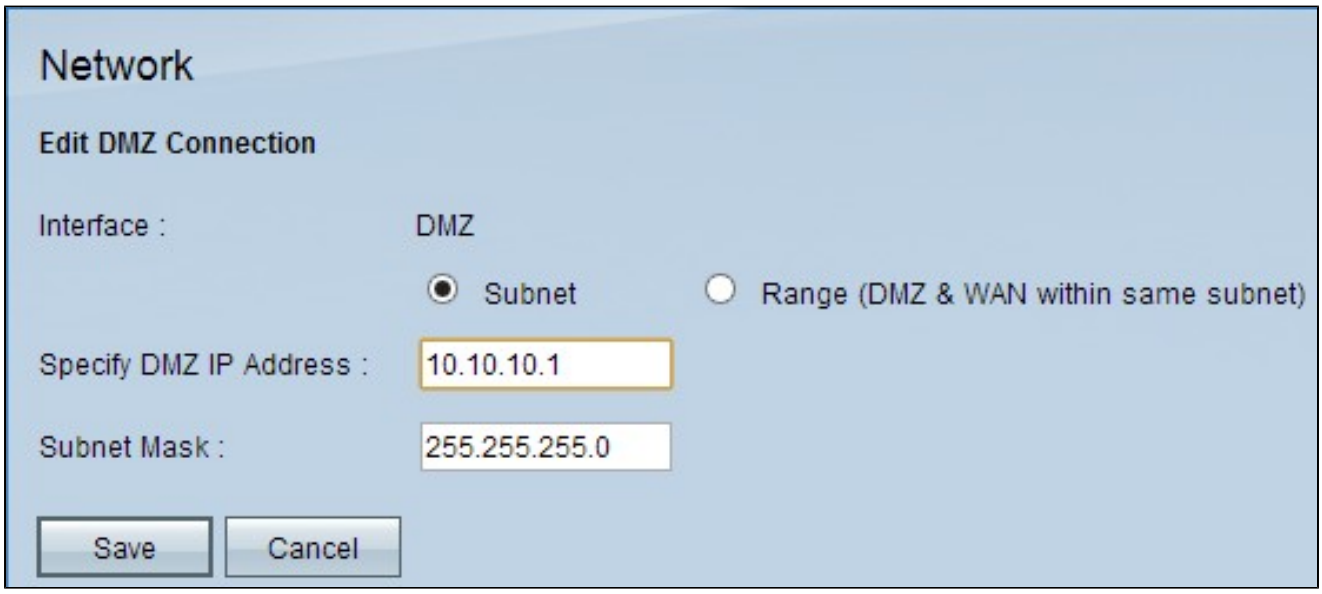
注意：如果要配置IPv6,必须启用IP模式区域中的双堆栈IP。

第三步：向下滚动到DMZ Setting字段，然后点击Enable DMZ单选按钮以启用DMZ。



第四步：单击DMZ配置图标配置子网。可以通过以下方式为IPv4和IPv6进行配置：

IPv4配置



第五步：单击Subnet单选按钮，将DMZ配置到除WAN子网之外的其他子网。对于子网IP，应配置以下内容

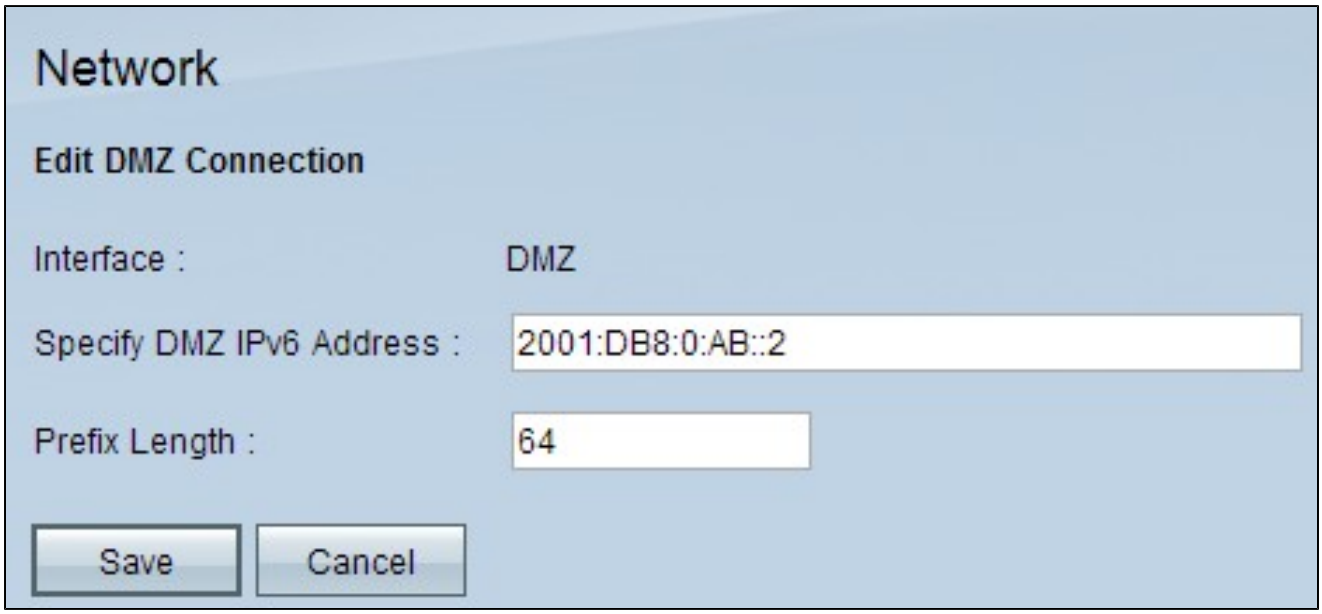
·指定DMZ IP地址(Specify DMZ IP Address) — 在指定DMZ IP地址字段中输入DMZ IP地址。

·子网掩码 — 在Subnet Mask（子网掩码）字段中输入子网掩码。

警告：DMZ中具有IP地址的主机不如内部LAN中的主机安全。

第六步：单击Range将DMZ配置为与WAN位于同一子网中。IP地址范围将在DMZ端口的IP范围字段中输入。

IPv6配置



注意：对于IPv6配置，以下选项可用：

步骤 7.指定DMZ IPv6地址(Specify DMZ IPv6 Address) — 输入IPv6地址。

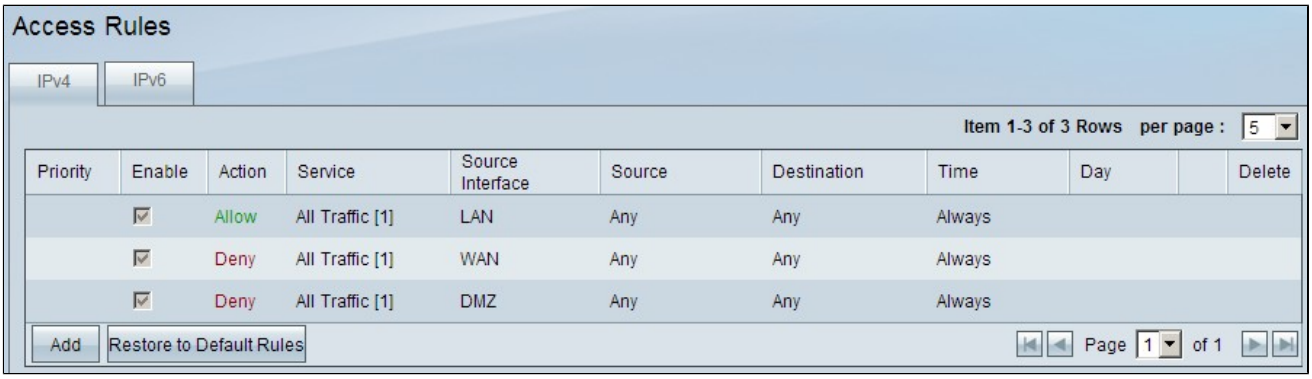
步骤 8Prefix Length — 输入上述DMZ IP地址域的前缀长度。

步骤 9单击Save保存配置。

访问规则配置

完成此配置是为了定义在多个子网掩码上配置的IP的访问列表。

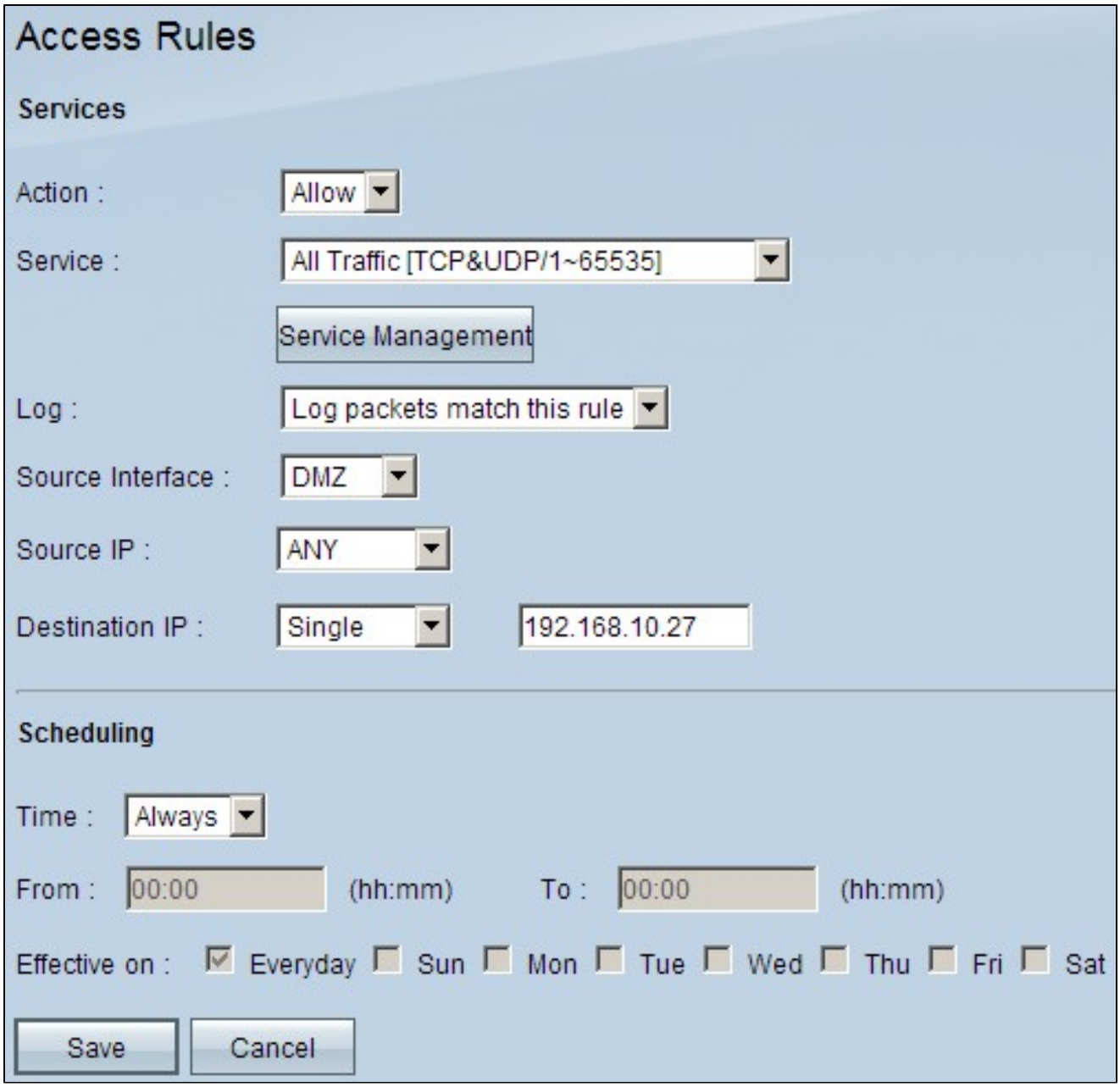
步骤1:登录到Router Configuration Utility页面，然后选择Firewall > Access Rules。将打开访问规则页面：



注意：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。Access Rules页面将更改，以显示“服务”和“调度”区域。

注意：通过选择Access Rules页面上的相应选项卡，可以对IPv4和IPv6执行此配置。以下步骤中介绍了特定于IPv4和IPv6的配置步骤。



第三步：从Action下拉列表中选择Allow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 that match this rule，以仅选择与访问规则匹配的日志。

第六步：从作为访问规则源的Source Interface下拉列表中选择DMZ。

步骤 7.从Source IP下拉列表中选择Any。

步骤 8从Destination IP下拉列表中选择以下任何可用选项。

· Single — 选择Single可将此规则应用于单个IP地址。

· Range — 选择范围，将此规则应用于某个IP地址范围。输入范围的第一个和最后一个IP地址。此选项仅在IPv4中可用。

·子网 — 选择子网以将此规则应用于子网。输入IP地址和CIDR表示编号，用于分配IP地址和路由子网的Internet协议数据包。此选项仅在IPv6中可用。

· Any — 选择Any将规则应用于任何IP地址。

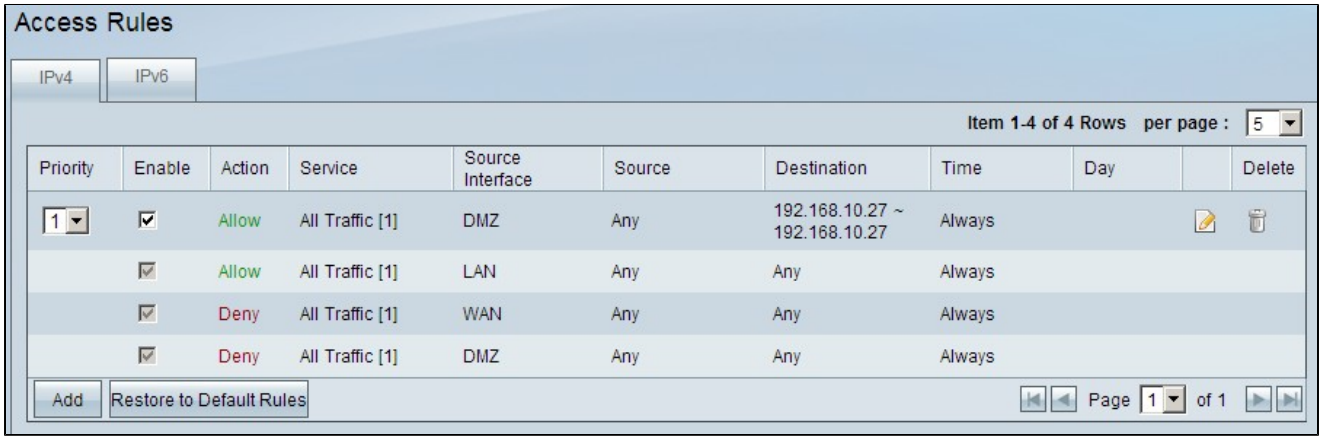
Timesaver：如果要配置IPv6访问规则，请跳至步骤10。

步骤 9从时间(Time)下拉列表中选择要定义规则何时处于活动状态的方法。它们是：

·始终 — 如果从“时间”下拉列表中选择“始终”，访问规则将始终应用于流量。

· Interval — 如果从Time下拉列表中选择Interval，则可以选择访问规则处于活动状态的特定时间间隔。指定时间间隔后，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 10单击Save保存设置。



步骤 11单击Edit图标编辑创建的访问规则。

步骤 12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）。

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）。