

RV160/RV260路由器的DMZ选项

目标

本文档将介绍在RV160X/RV260X系列路由器上设置隔离区 — DMZ主机和DMZ子网的两个选项。

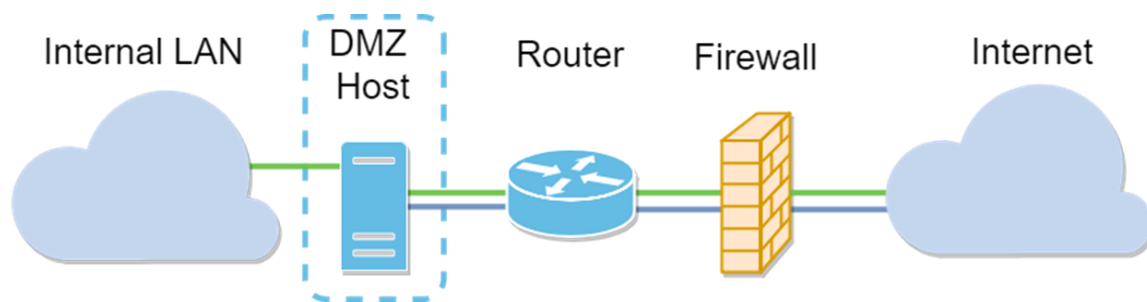
要求

- RV160X
- RV260X

简介

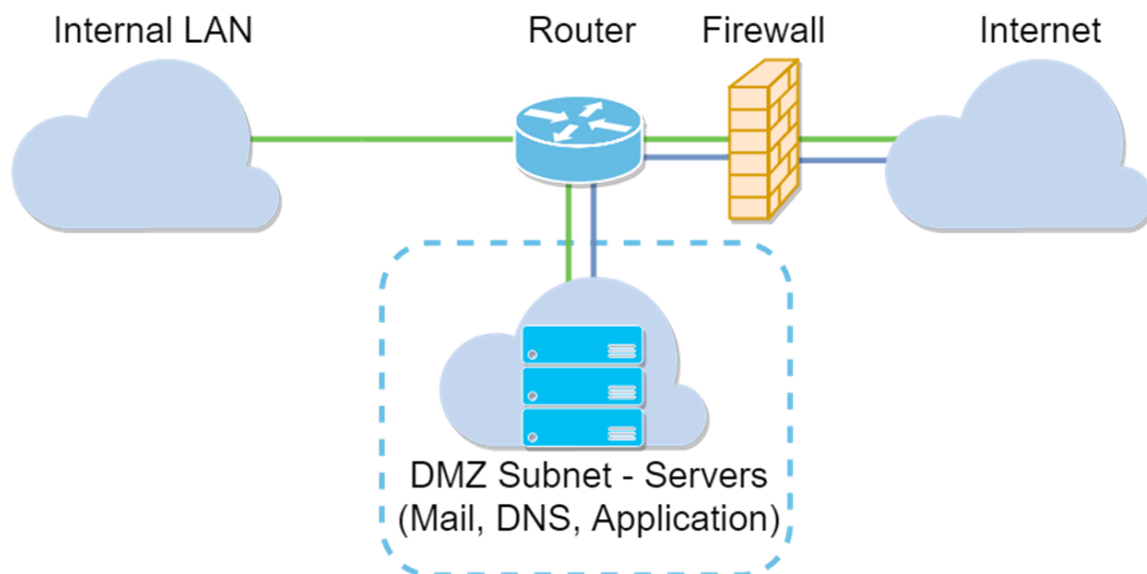
DMZ是网络上的一个位置，在防火墙后保护您的局域网(LAN)的同时，它对互联网开放。将主网络与单台主机或整个子网络或“子网”分离，可确保通过DMZ访问网站服务器的人员无法访问您的LAN。思科提供两种在网络中使用DMZ的方法，这两种方法在运行方式上都有重要区别。以下是视觉参考，突出显示了两种操作模式之间的区别。

主机DMZ拓扑



注意：当使用主机DMZ时，如果主机受到不良影响者的危害，您的内部LAN可能会受到进一步的安全入侵。

子网DMZ拓扑



DMZ类型	比较	对比度
主机	隔离流量	单台主机，完全开放互联网
子网/范围	隔离流量	多种设备和类型，完全开放到互联网。仅适用于RV260硬件。

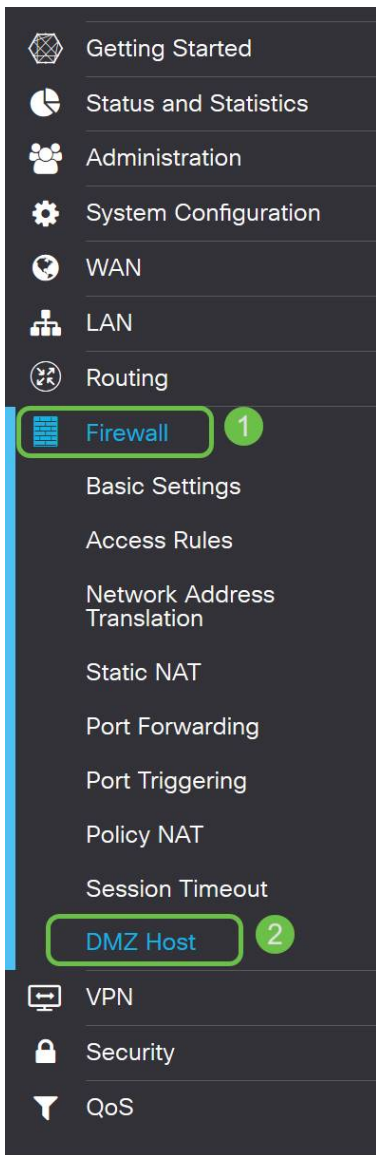
关于IP编址

本文利用IP编址方案，使其使用有些微妙。在规划DMZ时，您可以考虑使用私有或公有IP地址。私有IP地址对您来说是唯一的，只对您的LAN。公有IP地址对您的组织是唯一的，由您的互联网服务提供商分配。要获取公有IP地址，您需要联系您的(ISP)。

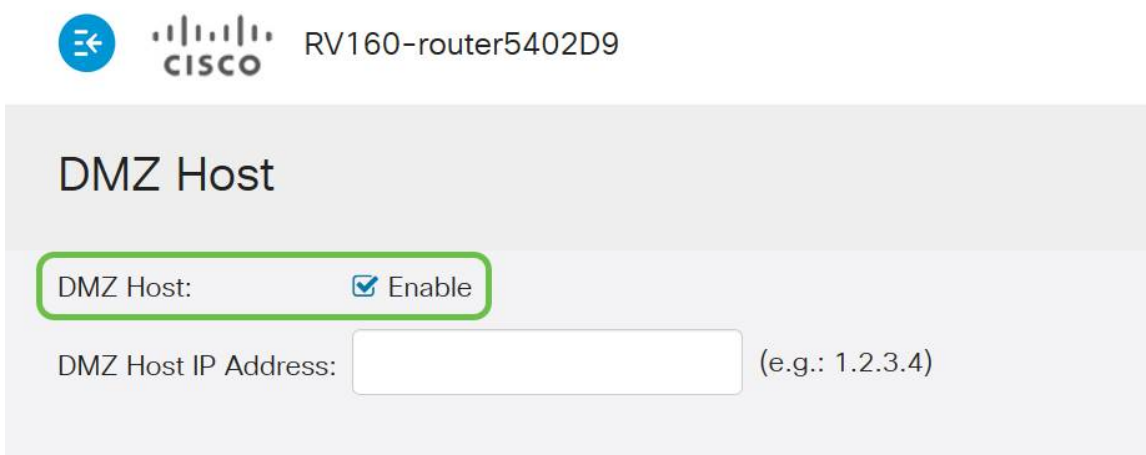
配置DMZ主机

此方法所需的信息包括目标主机的IP地址。IP地址可以是公有地址，也可以是私有地址，但公有IP地址应与WAN IP地址位于不同的子网中。RV160X和RV260X均提供DMZ主机选项。按照以下步骤配置DMZ主机。

步骤1.登录路由设备后，在左侧菜单栏中单击**Firewall > DMZ Host**。



步骤2.单击“启用”复选框。



步骤3.输入要打开以访问WAN的主机的指定IP地址。



DMZ Host

DMZ Host: EnableDMZ Host IP Address: (e.g.: 1.2.3.4)

步骤4.对您的地址感到满意后，点击应用按钮。

ApplyCancel

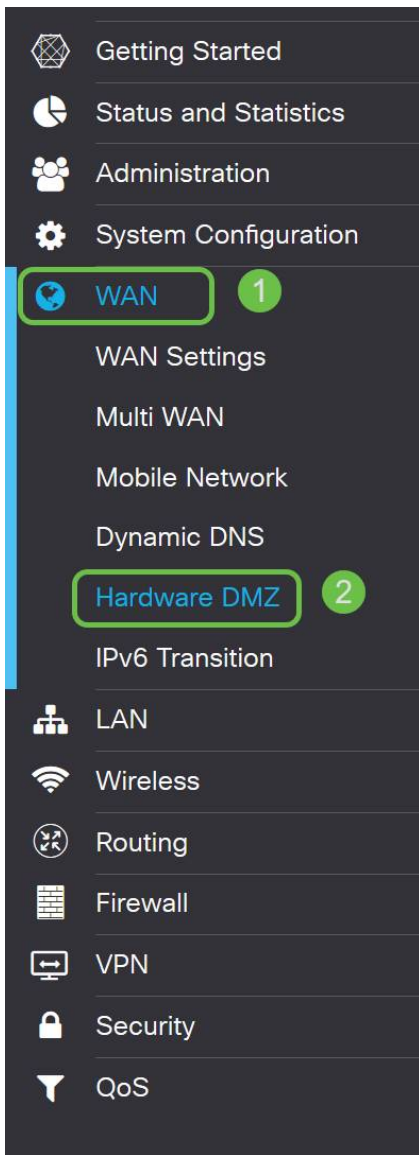
注意：如果您只使用RV160X系列，并且想跳至验证说明，请[单击此处转至本文档的该部分](#)。

配置硬件DMZ

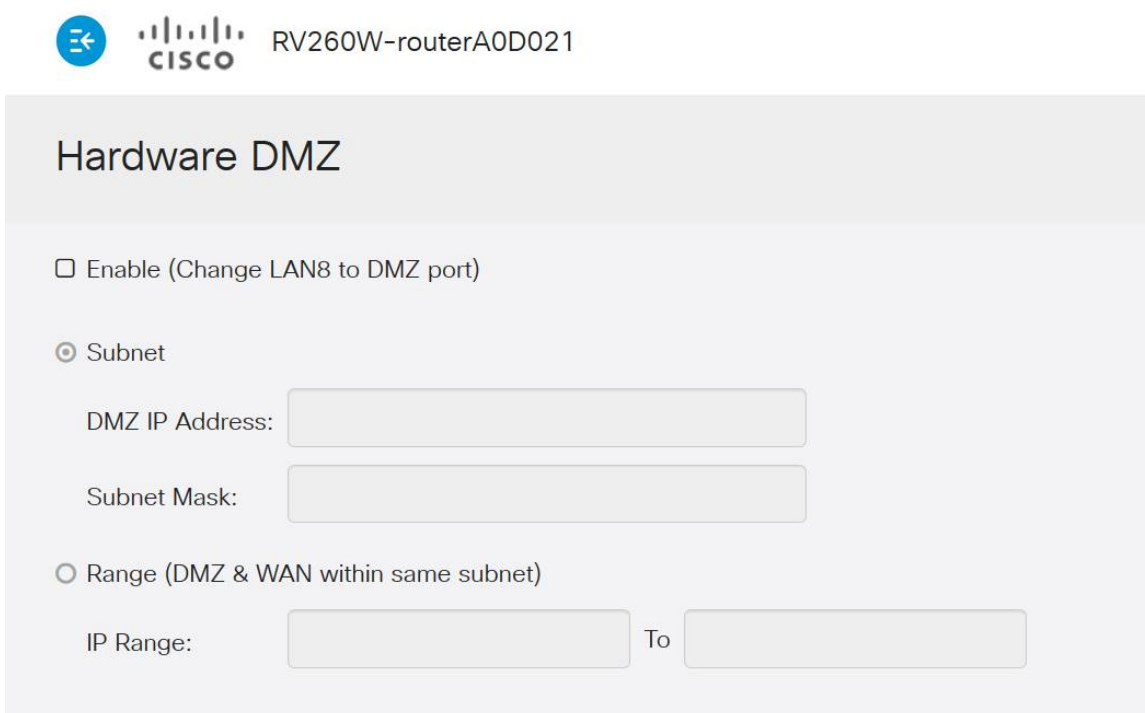
此方法仅适用于RV260X系列，根据您选择的方法，需要不同的IP编址信息。这两种方法都确实使用子网来定义区域，区别在于子网的多少用于创建隔离区。在这种情况下，选项是 — 全部或部分。子网(*all*)方法需要DMZ本身的IP地址以及子网掩码。此方法占用属于该子网的所有IP地址。而“范围”(某些)方法允许您定义要位于DMZ内的连续IP地址范围。

注意：无论哪种情况，您都需要与ISP合作来定义子网的IP编址方案。

步骤1.登录RV260X设备后，单击WAN > Hardware DMZ



注意： 屏幕截图从RV260X用户界面拍摄。下面是将显示在此页面上的硬件DMZ选项的屏幕截图。



步骤2.单击**Enable(Change LAN8 to DMZ port)**复选框。这会将路由器上的第8个端口转换为仅DMZ的“窗口”，转换为需要增强安全性的服务。

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet


DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

步骤3.单击“启用”后，可选选项下方会显示一条信息性消息。查看可能影响网络的点的详细信息，然后单击“确定，我同意以上”复选框。

 When hardware DMZ is enabled, the dedicated DMZ Port (LAN8) will be:

- * Disabled as Port Mirror function, if Port Mirror Destination is DMZ Port (LAN > Port Settings);
- * Removed from LAG Port (LAN > Port Settings);
- * Removed from Monitoring Port of Port Mirror (LAN > Port Settings);
- * Changed to "Force Authorized" in Administrative State (LAN > 802.1X Configuration);
- * Changed to "Excluded" in "Assign VLANs to ports" table (LAN > VLAN Settings).

OK, I agree with the above.

步骤4.下一步分为两个潜在选项：子网和范围。在下面的示例中，我们选择了子网方法。

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address: 164.33.100.250

Subnet Mask: 255.255.255.248

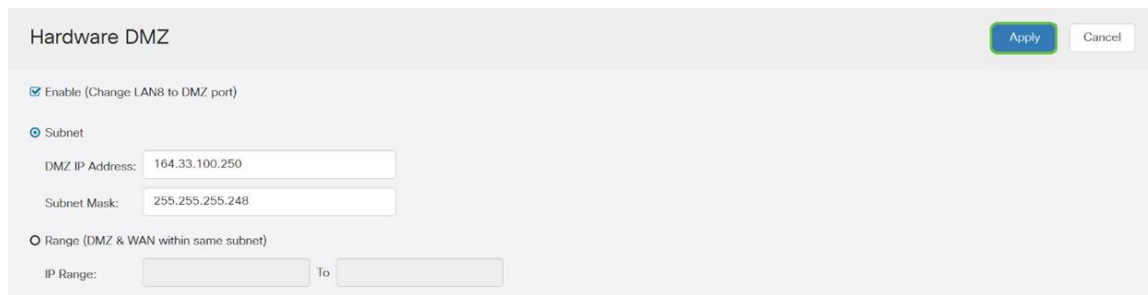
Range (DMZ & WAN within same subnet)

IP Range:

To

注意：如果要使用Range方法，则需要单击**Range**单选按钮，然后输入ISP分配的IP地址范围。

步骤6.单击**Apply**（在右上角）接受DMZ设置。

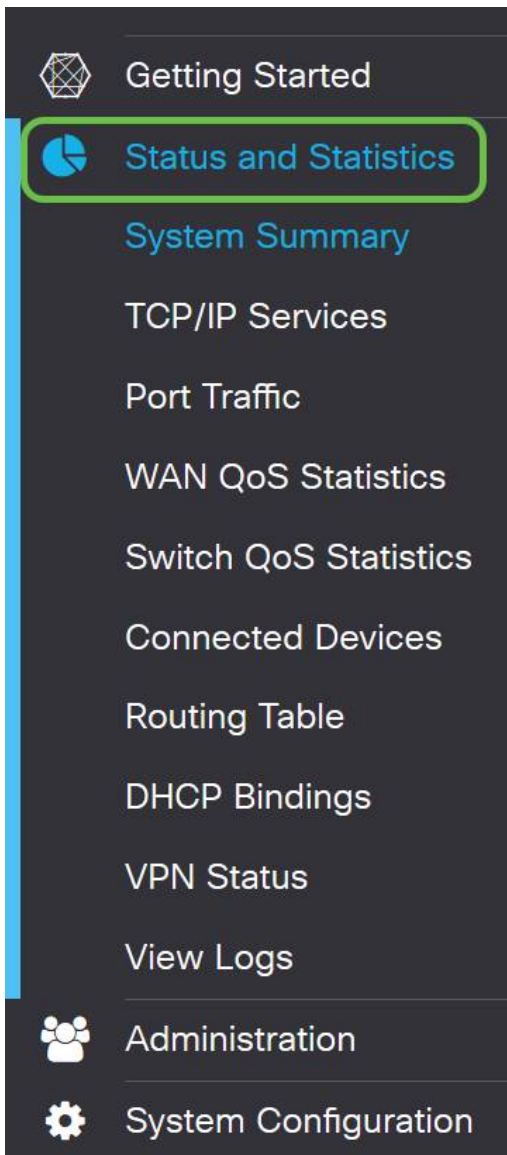


The screenshot shows the 'Hardware DMZ' configuration page. At the top right, there are two buttons: 'Apply' (highlighted in green) and 'Cancel'. Below the title, there is a checked checkbox for 'Enable (Change LAN8 to DMZ port)'. Underneath, the 'Subnet' radio button is selected. The 'DMZ IP Address' field contains '164.33.100.250' and the 'Subnet Mask' field contains '255.255.255.248'. The 'Range (DMZ & WAN within same subnet)' radio button is unselected. The 'IP Range' field is empty, followed by a 'To' label and another empty field.

确认DMZ设置正确

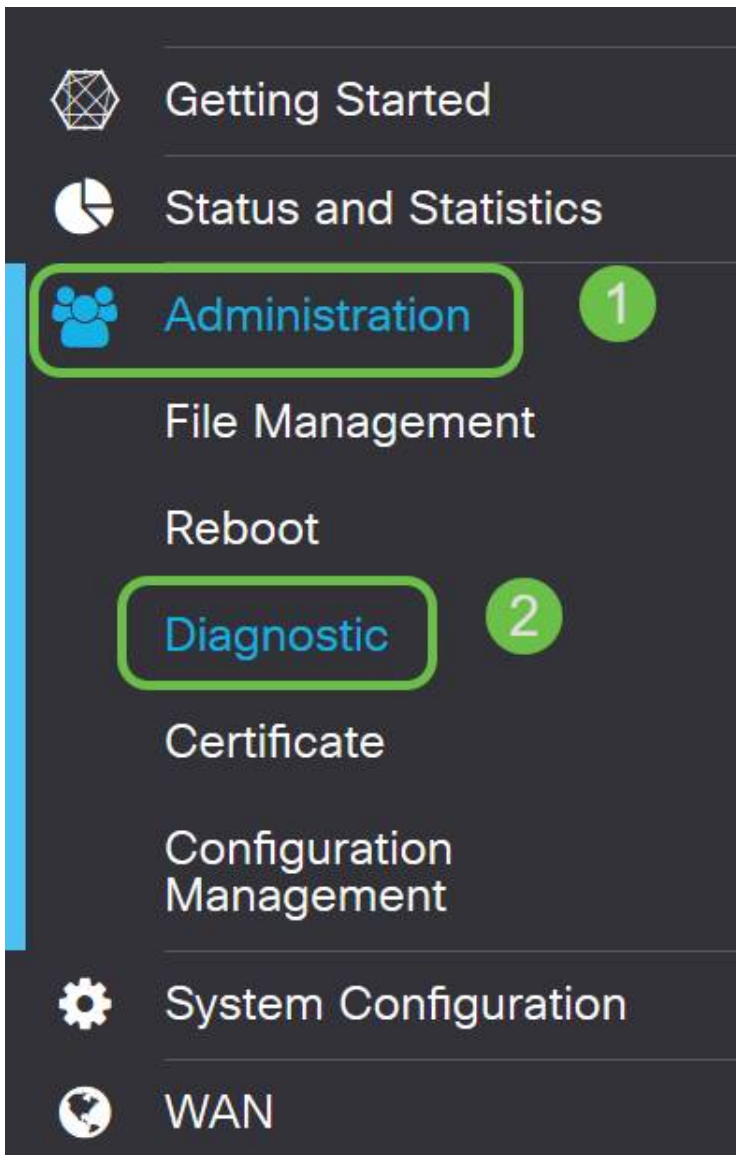
检验DMZ是否配置为适当接受来自其区域外源的流量，ping测试就足够了。首先，我们将通过管理界面来检查DMZ的状态。

步骤1.要验证DMZ是否已配置，请导航至“状态和统计”，该页将自动加载“系统摘要”页。端口8或“Lan 8”将DMZ的状态列为“*Connected*”。

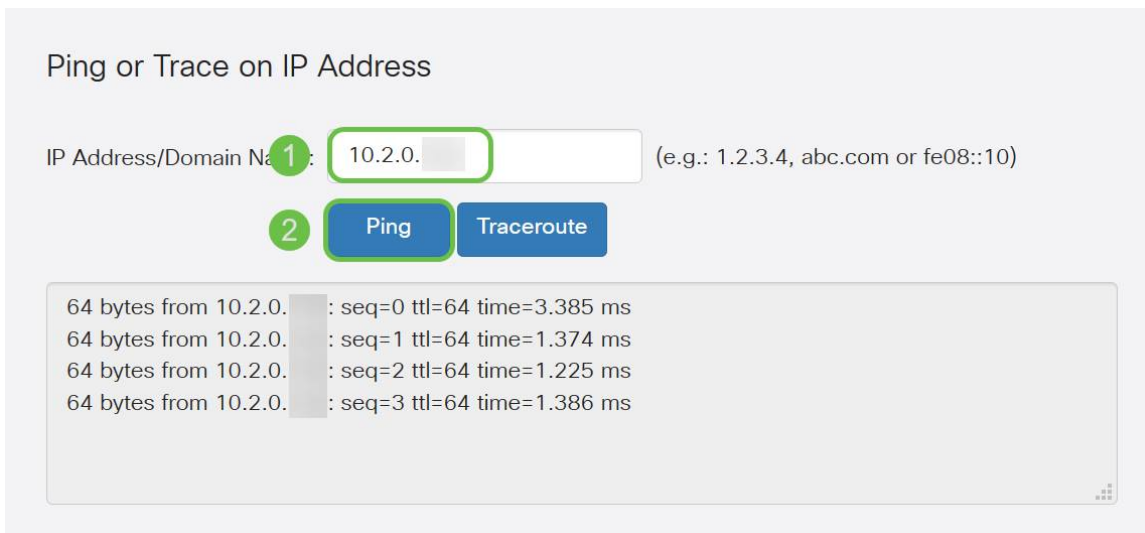


我们可以使用可信ICMP ping功能测试DMZ是否按预期运行。ICMP消息或仅“ping”尝试敲开DMZ的门。如果DMZ以“Hello”回复，则ping操作完成。

步骤2.要导航浏览器到ping功能，请单击“管理”>“诊断”。



步骤3.输入DMZ的IP地址，然后单击Ping按钮。



如果ping成功，您将看到类似上面的消息。如果ping失败，则表示无法访问DMZ。检查您的DMZ设置，确保它们已正确配置。

结论

既然您已完成DMZ的设置，您应该能够开始从LAN外部访问服务。