

RV160/RV260路由器的DMZ选项

客观

本文将包括在设置一个非敏感区域的两个选项- DMZ主机和DMZ子网在RV160X/RV260X系列路由器。

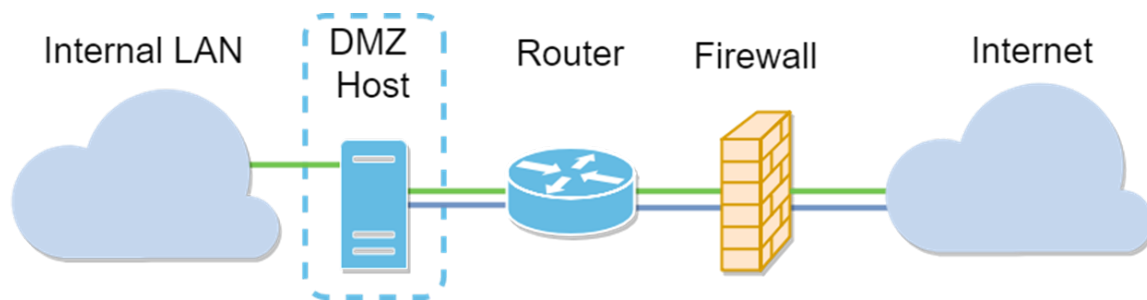
Requirements

- RV160X
- RV260X

Introduction

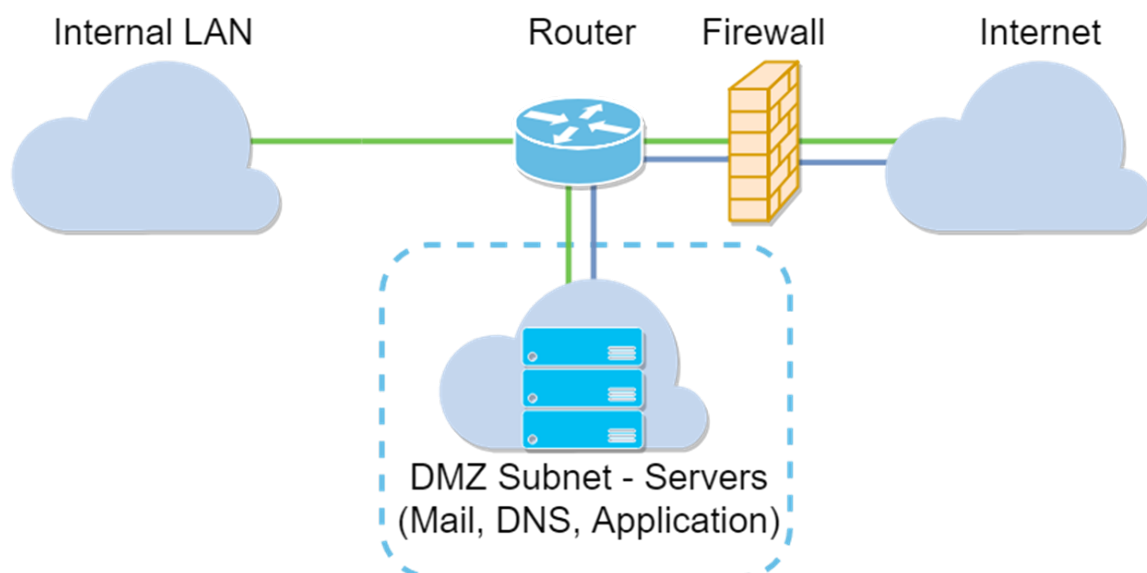
DMZ是开放的对互联网，当巩固您的区域网的网络的一个位置(LAN)时在防火墙后。分离主干网从单个主机或一个整个子网络或者“子网”保证访问您的网站服务器的人们通过DMZ，不会访问您的LAN。两个运载在Cisco提供使用DMZs两个方法在您的网络该他们如何的重要差异运行。下面是视觉参考高亮度显示两个操作模式之间的区别。

主机DMZ拓扑



Note:当使用主机DMZ，如果主机由BAD演员攻陷您的内部LAN时可能是受进一步安全入侵支配。

子网DMZ拓扑



DMZ类型	比较	对比
主机	分离数据流	单个主机，对互联网充分地打开
子网/范围	分离数据流	多个设备和类型，对互联网充分地打开。仅可用在RV260硬件。

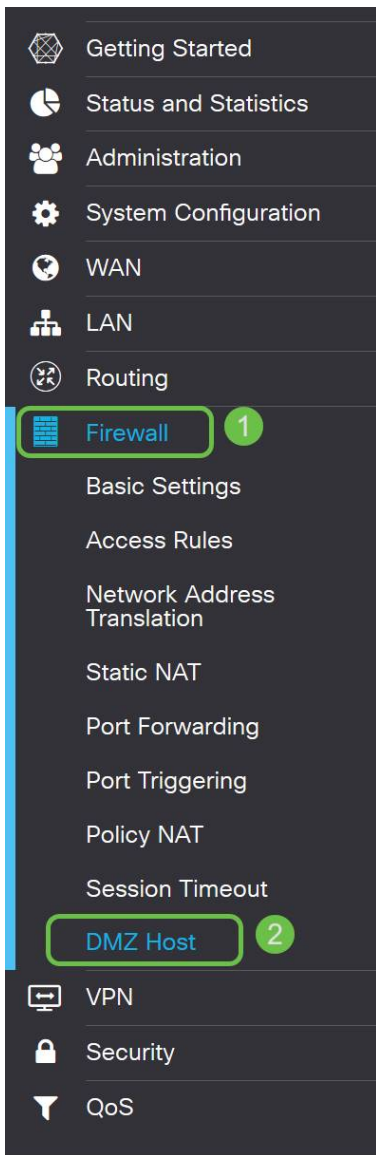
关于IP编址

此条款利用运载在他们的使用方法的某细微差异的IP编址方案。在计划您的DMZ您可以考虑使用一个公共或专用IP地址。一个专用IP地址对您将是仅唯一，在您的LAN。一个公共IP地址对您的组织将是唯一和由您的互联网服务提供商分配。获得您将需要与您联系的一个公共IP地址(ISP)。

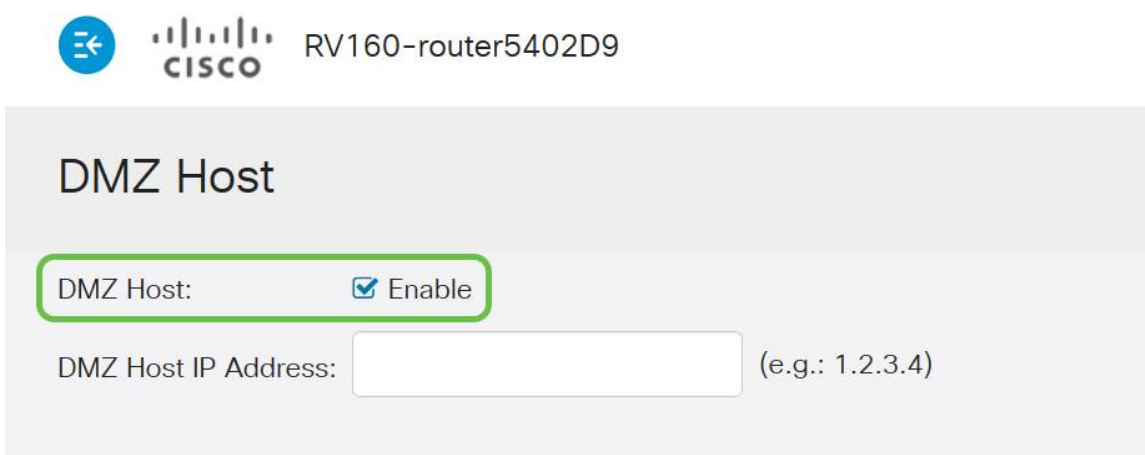
配置DMZ主机

此方法的需的信息包括目的主机的IP地址。IP地址可以是公共或专用的，但是公共IP地址比广域网IP地址应该在一个不同的子网。DMZ Host选项是可用的在RV160X和RV260X。配置DMZ主机在下面步骤后。

第 1 步：在登录到您的路由设备以后，在左边菜单栏请点击**防火墙 > DMZ主机**。



步骤2. 点击Enable复选框。



步骤3. 输入您希望对WAN接入打开主机的选定的IP地址。



DMZ Host

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

第 4 步：当对您的寻址满足，请点击应用按钮。

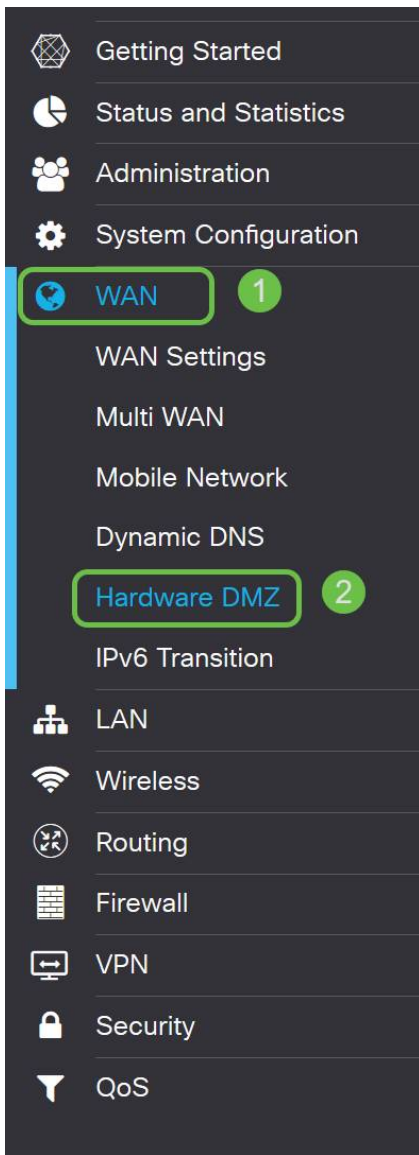
Note:如果与仅RV160X系列一起使用并且要跳过到验证指令，请[点击此处移动向本文的该部分](#)。

配置硬件DMZ

可用对仅RV260X系列，此方法要求根据您选择的方法的另外IP寻址信息。两个方法的确使用子网定义区域，是的区别多少子网络用于创建非敏感区域。在这种情况下，选项是-所有或一些。子网(全部)方法与子网掩码一起要求DMZ的IP地址。此方法占用属于该子网络的所有IP地址。而范围(一些)方法允许您定义在DMZ内将位于的IP地址的一个持续范围。

Note:无论如何您将需要与您的ISP一起使用定义子网络的IP编址方案。

第 1 步：在登录到您的RV260X设备以后，请点击广域网>硬件DMZ



Note: 屏幕画面从RV260X用户界面被采取。下面的硬件DMZ选项屏幕画面在此页将显示。

  RV260W-routerA0D021

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2. 点击**Enable (event) (对DMZ端口的更改LAN8)**复选框。这将转换在路由器的第8个端口成DMZ “仅窗口”成需要高级安全的服务。

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet


DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

第 3 步：在点击**Enable (event)**以后一个供参考消息在可选择的选项之下显示。查看可能影响您的网络并且点击**OK**的点的详细资料，**我同意上述复选框**。

 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.

第 4 步：下一步分裂成两个潜在的选项、子网和范围。在下面的示例中我们的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

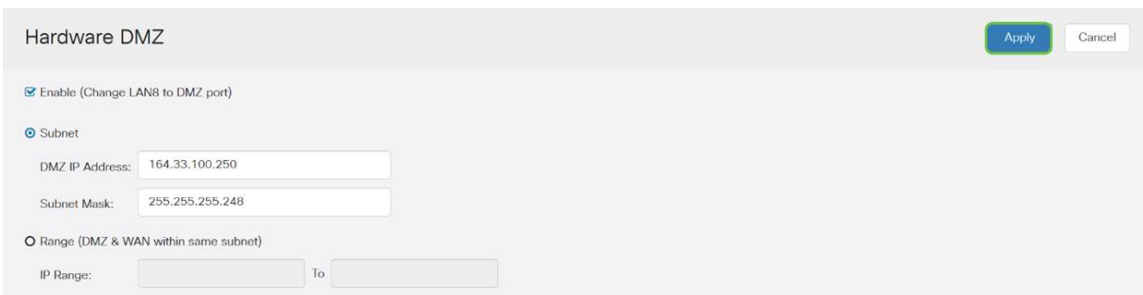
Range (DMZ & WAN within same subnet)

IP Range:

To

Note:如果打算使用范围方法，则您将需要点击**范围**圆形按钮，则输入您的ISP分配的IP地址的范围。

步骤6. 点击**适用**(在右上角)接受DMZ设置。

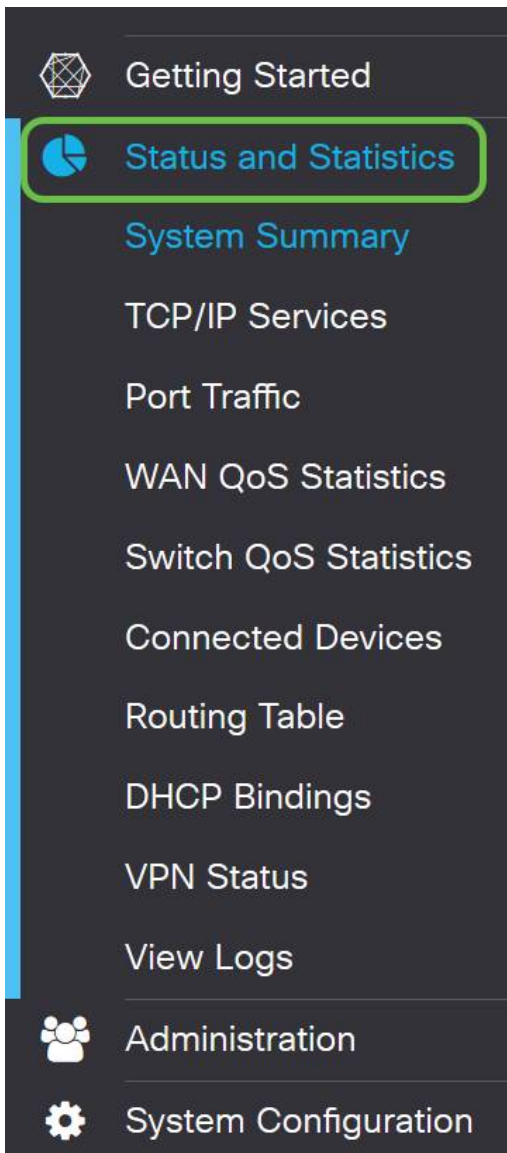


The screenshot shows the 'Hardware DMZ' configuration page. The 'Enable (Change LAN8 to DMZ port)' checkbox is checked. The 'Subnet' radio button is selected. The 'DMZ IP Address' field contains '164.33.100.250' and the 'Subnet Mask' field contains '255.255.255.248'. The 'Range (DMZ & WAN within same subnet)' radio button is unselected. The 'IP Range' and 'To' fields are empty. In the top right corner, the 'Apply' button is highlighted in green, and the 'Cancel' button is visible next to it.

确认DMZ适当地设置

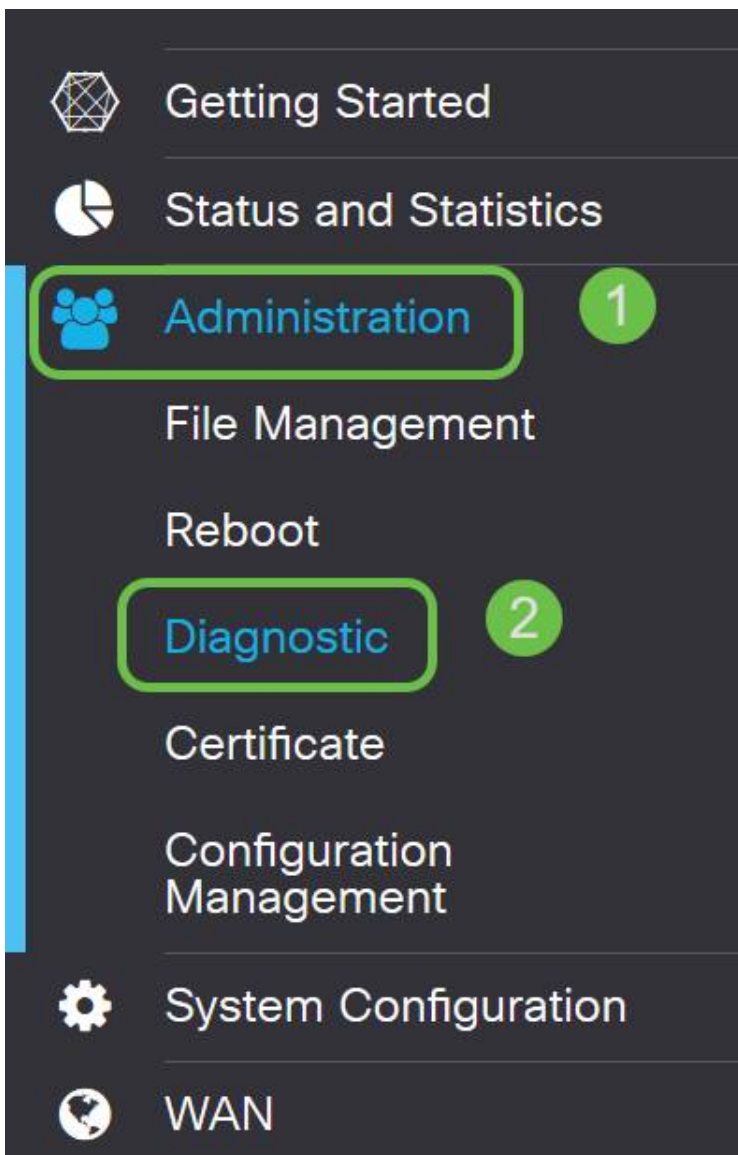
DMZ配置验证适当地接收从来源的数据流在其区域外面，ping测试将足够了。首先虽则，我们将路过管理界面检查DMZ的状态。

第 1 步：您的DMZ配置要验证，连接对**状态&统计数据**，页将自动地装载系统汇总页。端口8或“LAN 8”将列出DMZ的状态作为“连接”。



如果DMZ运行得正如所料，我们能使用可信任的ICMP Ping功能测试。ICMP信息或“连接”，尝试敲DMZ的门。如果DMZ通过说“Hello”回应ping完成。

Step 2.要连接您的浏览器到ping功能，请点击**Administration > 诊断**。



步骤3.输入DMZ的IP地址并且点击Ping按钮。



如果ping是成功的您将看到一个消息类似在上面。如果ping发生故障，意味着DMZ无法被到达。检查您的DMZ设置保证他们适当地被配置。

[结论](#)

即然您完成了DMZ的设置，您应该能开始访问服务从LAN外面。