

# DMZ Options for RV160/RV260 Routers

## Objective

This document will cover the two options in setting up a Demilitarized Zone -DMZ host and DMZ subnet on RV160X/RV260X series routers.

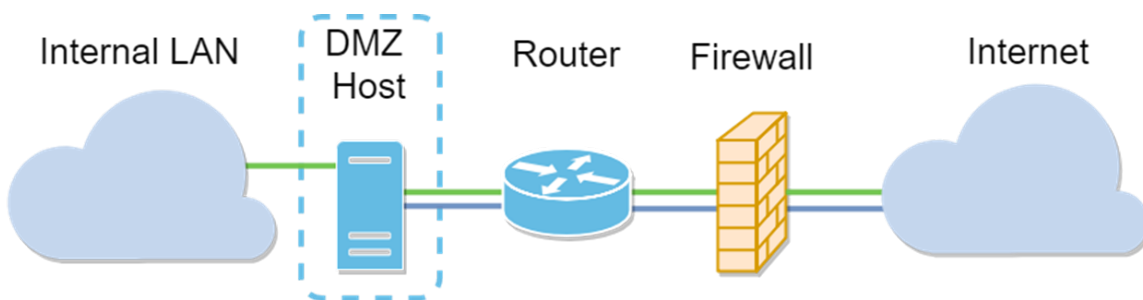
## Requirements

- RV160X
- RV260X

## Introduction

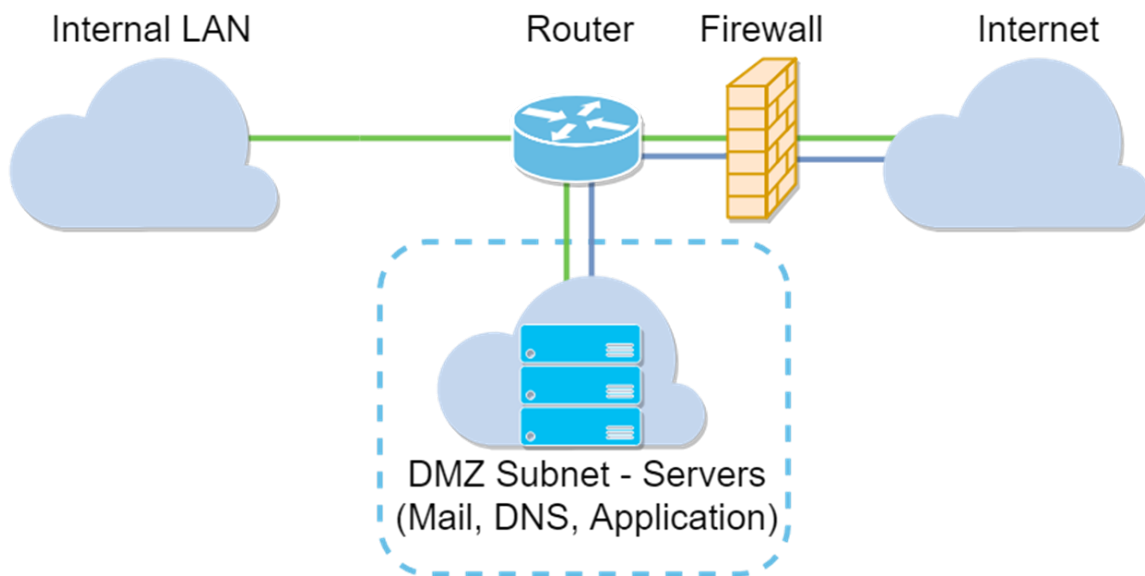
A DMZ is a location on a network that is open to the internet while securing your local area network (LAN) behind a firewall. Separating the main network from either a single host or an entire sub-network, or "subnet" ensures that people visiting your website server via the DMZ, won't have access to your LAN. Cisco offers two methods of using DMZs in your network that both carry important distinctions in how they operate. Below are visual references highlight the difference between the two operating modes.

## Host DMZ Topology



**Note:** When using a host DMZ, if the host is compromised by a bad-actor your internal LAN may be subject to further security intrusion.

## Subnet DMZ Topology



DMZ Type	Compare	Contrast
Host	Segregates traffic	Single host, fully open to the internet
Subnet / Range	Segregates traffic	Multiple devices and types, fully open to the internet. <b>Available only on RV260 hardware.</b>

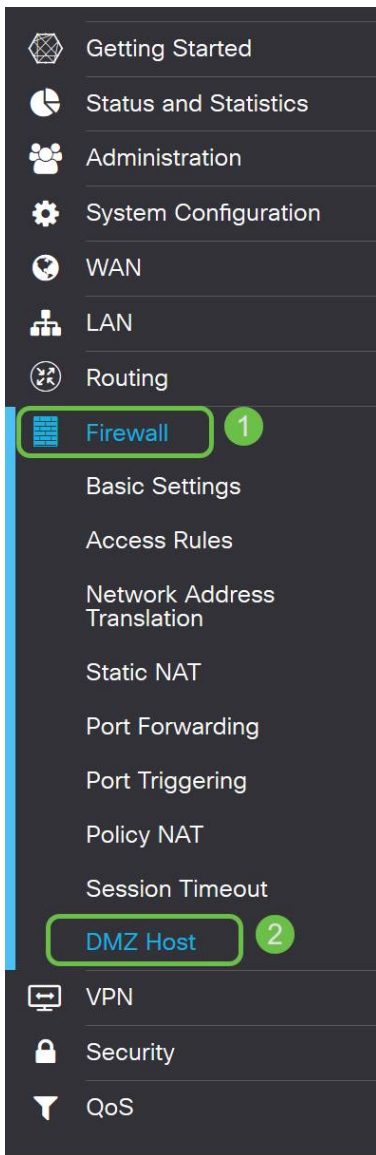
## Regarding IP Addressing

This article makes use of IP addressing schemes that carry some nuance in their usage. In planning your DMZ you may consider using either a private or public IP address. A private IP address will be unique to you, only on your LAN. A public IP address will be unique to your organization and is assigned by your Internet Service Provider. To procure a public IP address you will need to contact your (ISP).

## Configuring DMZ Host

The information required for this method includes the intended host's IP address. The IP address can be either public or private, but the public IP address should be in a different subnet than the WAN IP address. The DMZ Host option is available on both the RV160X and RV260X. Configure the DMZ Host following the steps below.

Step 1. After logging into your routing device, in the left-hand menu bar click **Firewall > DMZ Host**.



Step 2. Click the **Enable** checkbox.



## DMZ Host

DMZ Host:  Enable

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

Step 3. Enter the designated IP address of the host you wish to open up to WAN access.



## DMZ Host

DMZ Host:

Enable

DMZ Host IP Address:

10.2.

(e.g.: 1.2.3.4)

Step 4. When satisfied with your addressing, click the apply button.

Apply

Cancel

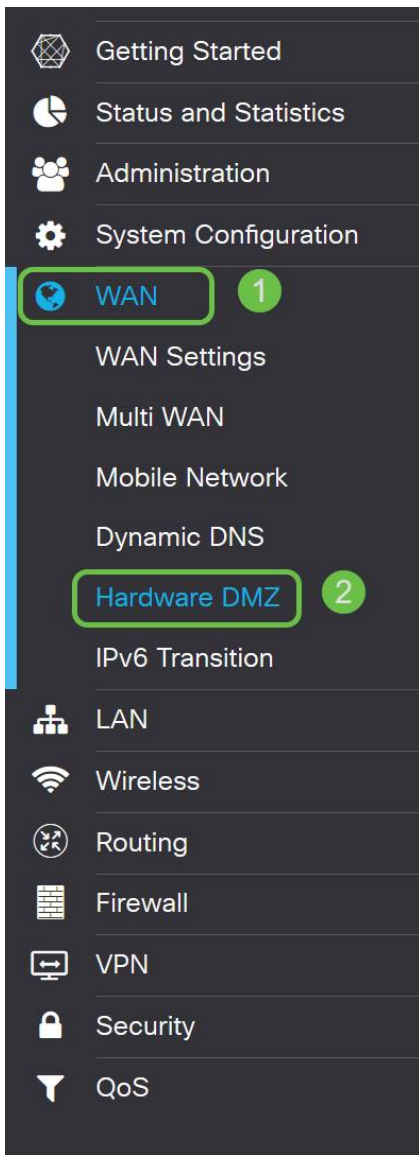
**Note:** If you're working with an RV160X series only and want to skip to the verification instructions, [click here to move to that section of this document](#).

## Configuring Hardware DMZ

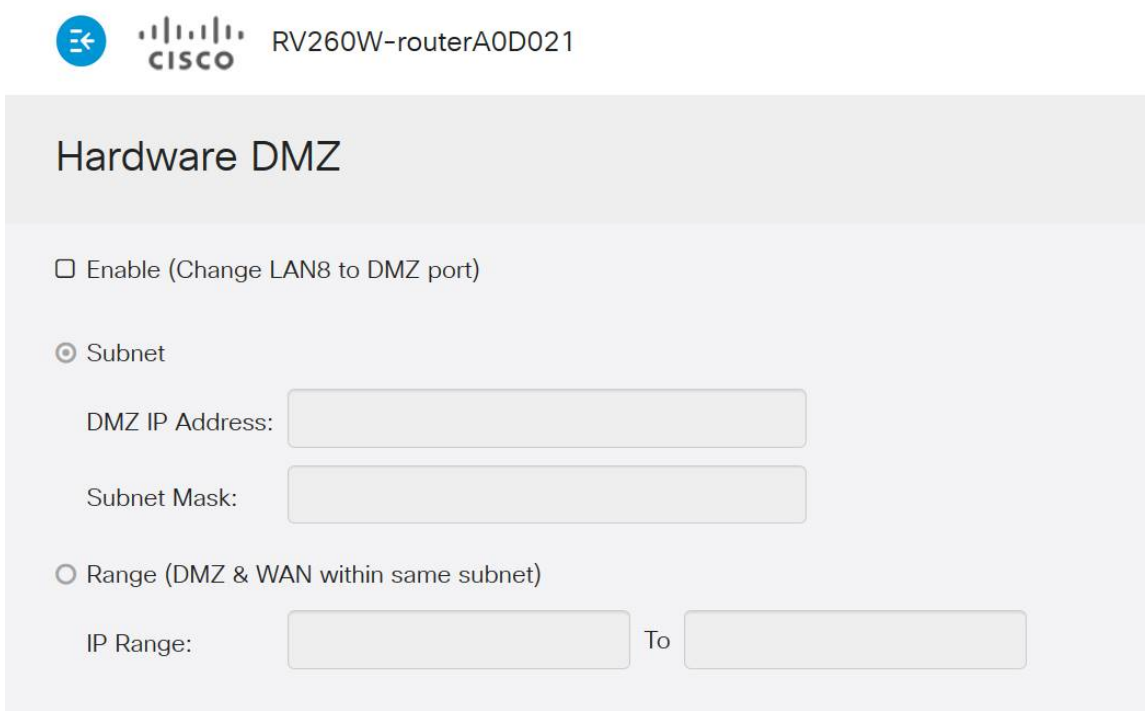
Available to the RV260X series only, this method requires different IP addressing information based on the method you choose. Both methods indeed use subnetworks to define the zone, the difference being how much of the subnetwork is used to create the demilitarized zone. In this case, the options are - *all* or *some*. The Subnet (*all*) method requires the IP address of the DMZ itself, along with the subnet mask. This method occupies all of the IP addresses belonging to that subnetwork. Whereas the Range (*some*) method allows you to define a continuous range of IP addresses to be located within the DMZ.

**Note:** In either case you will need to work with your ISP to define the subnetwork's IP addressing scheme.

Step 1. After logging into your RV260X device, click **WAN > Hardware DMZ**



**Note:** The screenshots are taken from the RV260X user interface. Below is the screenshot of Hardware DMZ options that will be displayed on this page.



Step 2. Click the **Enable (Change LAN8 to DMZ port)** checkbox. This will convert the 8<sup>th</sup> port on the router into a DMZ only "window" to services that require enhanced security.

### Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet


DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range:  To

Step 3. After clicking *Enable* an informational message displays below the selectable options. Review the details for points that may affect your network and click the **OK, I agree with the above** checkbox.

 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.

Step 4. The next step splits into two potential options, Subnet and Range. In our example below we've selected the **Subnet** method.

## Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

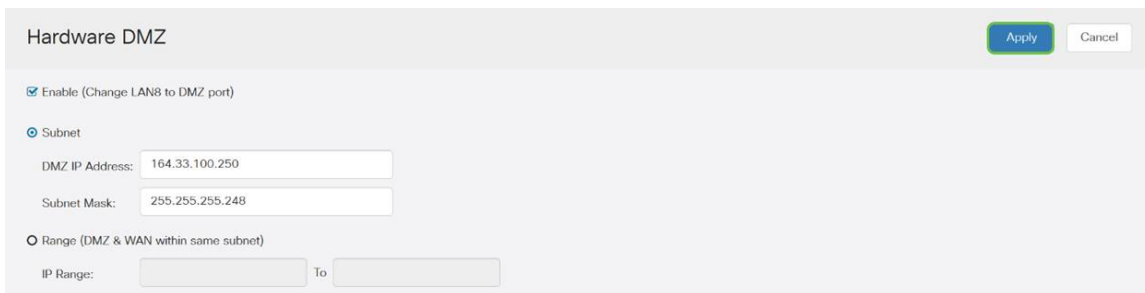
Range (DMZ & WAN within same subnet)

IP Range:

To

**Note:** If you intend to use the Range method, then you will need to click the **Range** radial button, then enter the range of IP addresses assigned by your ISP.

Step 6. Click **Apply** (in the upper right hand corner) to accept the DMZ settings.

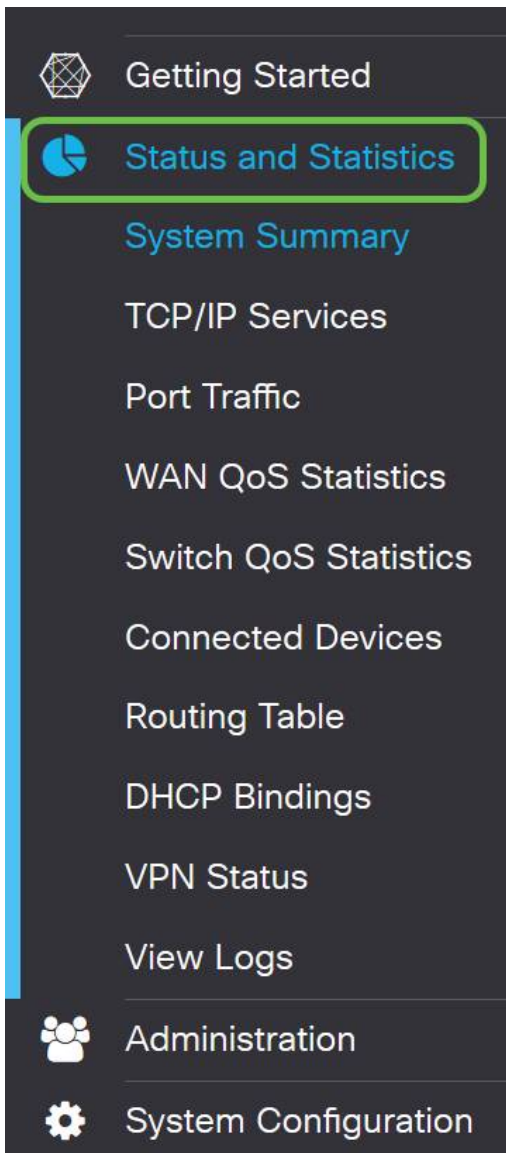


The screenshot shows the Hardware DMZ configuration page. At the top right, there are two buttons: "Apply" (highlighted in blue) and "Cancel". The configuration options are the same as in the previous image, with the "Subnet" radio button selected and the "Apply" button highlighted.

## Confirming the DMZ is setup properly

Verifying the DMZ is configured to appropriately accept traffic from sources outside of its zone, a ping test will suffice. First though, we'll stop by the administration interface to check the status of the DMZ.

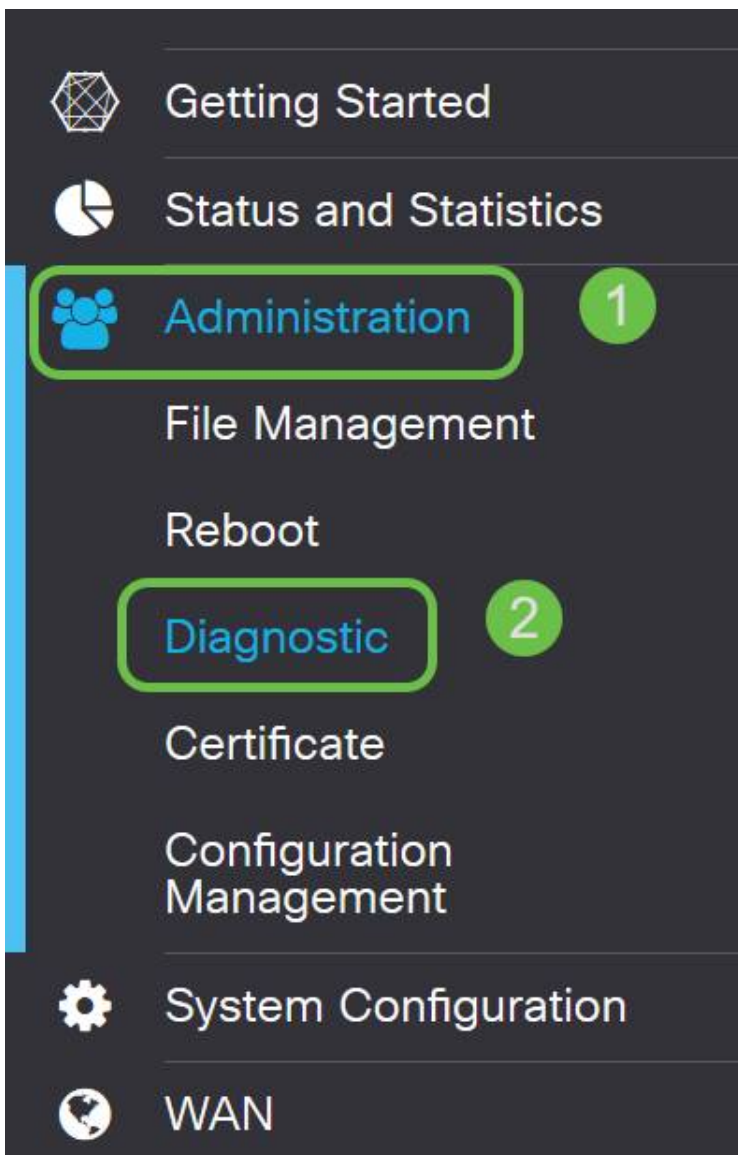
Step 1. To verify your DMZ is configured, navigate to **Status & Statistics**, the page will load the System Summary page automatically. Port 8 or "Lan 8" will list the status of the DMZ as "*Connected*".



We can use the trusty ICMP ping feature to test if the DMZ is operating as expected. The ICMP message or just "ping", attempts to knock on the door of the DMZ. If the DMZ responds by saying "Hello" the ping is completed.

Step 2. To navigate your browser to the ping feature, click **Administration > Diagnostic**.





Step 3. Enter the **IP address of the DMZ** and click the **Ping** button.



If the ping is successful you will see a message like the above. If the ping fails, it means the DMZ is unable to be reached. Check your DMZ settings to ensure they are configured appropriately.

## Conclusion

Now that you've completed the setup of the DMZ, you should be able to begin accessing the services from outside the LAN.