Opciones DMZ para routers RV160/RV260

Objetivo

Este documento tratará las dos opciones para configurar un host de zona desmilitarizada -DMZ y una subred DMZ en los routers serie RV160X/RV260X.

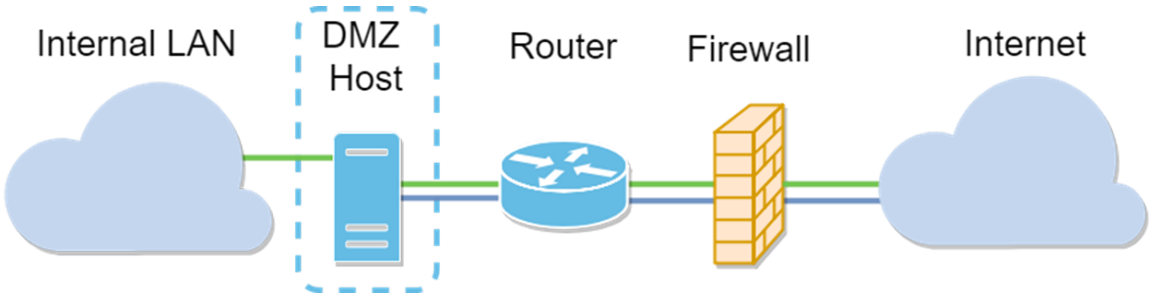
Requirements

- RV160X
- RV260X

Introducción

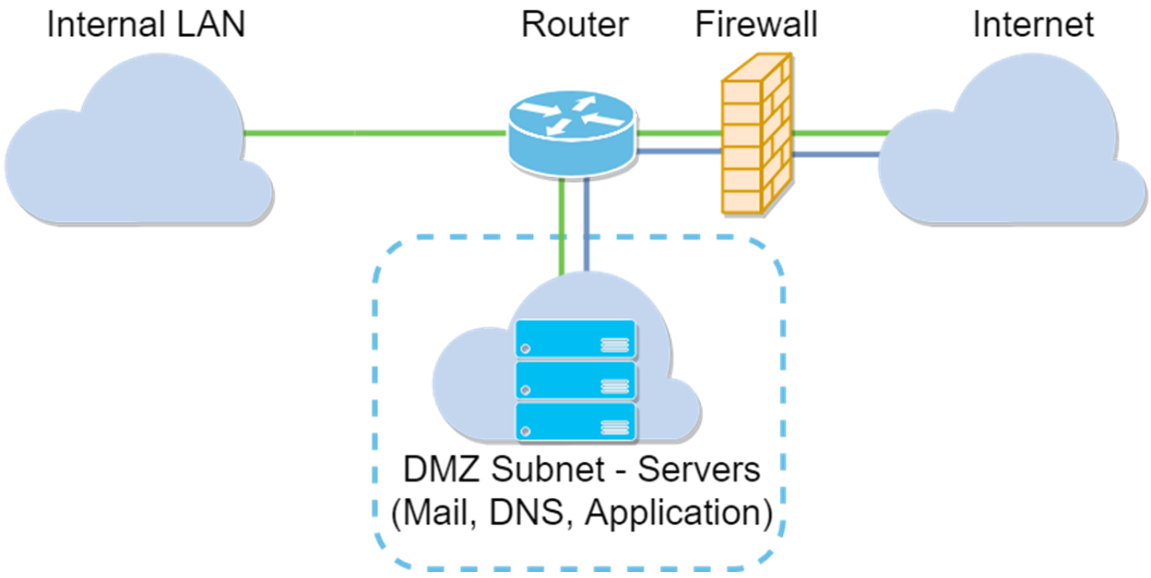
Una DMZ es una ubicación de una red abierta a Internet mientras protege la red de área local (LAN) detrás de un firewall. La separación de la red principal de un solo host o de toda una subred, o "subred", garantiza que las personas que visiten el servidor de su sitio web a través de la DMZ no tengan acceso a su LAN. Cisco ofrece dos métodos de uso de DMZ en su red que contienen importantes distinciones en su funcionamiento. A continuación se muestran las referencias visuales que resaltan la diferencia entre los dos modos operativos.

Topología DMZ del host



Nota: Al utilizar una DMZ de host, si el host se ve comprometido por un mal actor, su LAN interna puede estar sujeta a más intrusiones de seguridad.

Topología DMZ de subred



Tipo DMZ	Comparar	Contraste
Host	Segrega el tráfico	Host único, totalmente abierto a Internet
Subred/intervalo	Segrega el tráfico	Varios dispositivos y tipos, totalmente abiertos a Internet. **Disponible sólo en hardware RV260.**

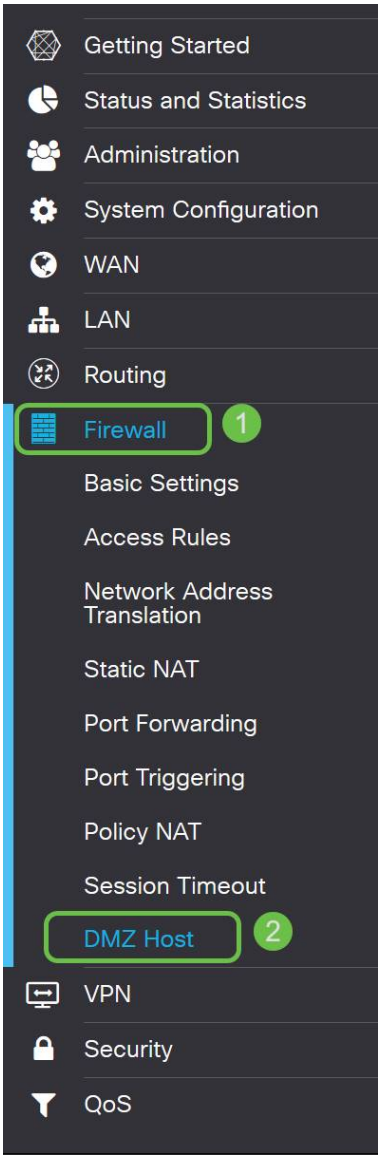
Acerca del direccionamiento IP

Este artículo hace uso de esquemas de direccionamiento IP que contienen algunos matices en su uso. Al planificar su DMZ, puede considerar el uso de una dirección IP privada o pública. Una dirección IP privada será exclusiva para usted, sólo en su LAN. Una dirección IP pública será exclusiva de su organización y su proveedor de servicios de Internet la asignará. Para obtener una dirección IP pública, deberá ponerse en contacto con el (ISP).

Configuración de DMZ Host

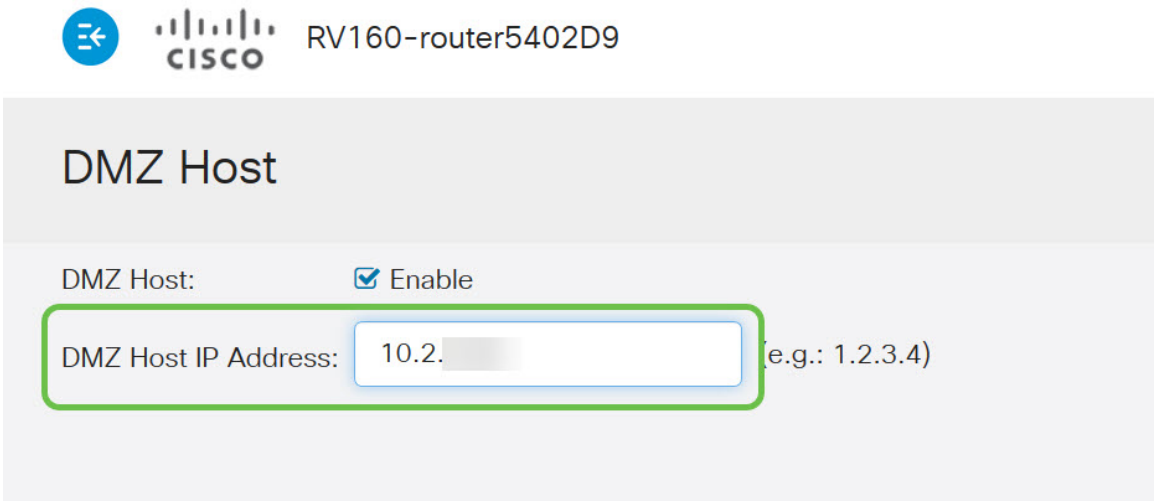
La información requerida para este método incluye la dirección IP del host deseado. La dirección IP puede ser pública o privada, pero la dirección IP pública debe estar en una subred diferente de la dirección IP de WAN. La opción DMZ Host está disponible tanto en el RV160X como en el RV260X. Configure el host DMZ siguiendo los pasos que se indican a continuación.

Paso 1. Después de iniciar sesión en el dispositivo de ruteo, en la barra de menú izquierda haga clic en **Firewall > DMZ Host.**



Paso 2. Haga clic en la casilla **Enable**.

Paso 3. Introduzca la dirección IP designada del host que desea abrir al acceso WAN.



Paso 4. Cuando esté satisfecho con el direccionamiento, haga clic en el botón Aplicar.

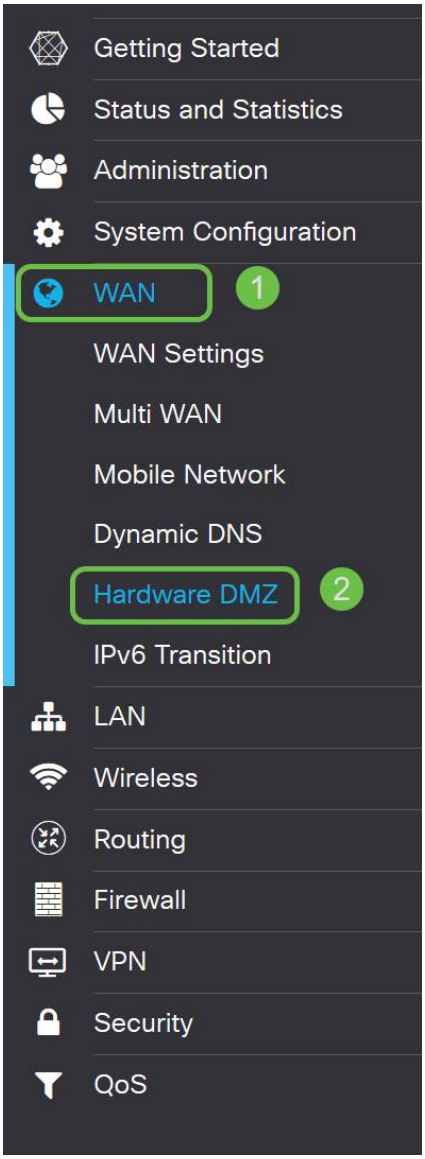
Nota: Si sólo trabaja con una serie RV160X y desea saltar a las instrucciones de verificación, haga clic aquí para ir a esa sección de este documento.

Configuración de DMZ de hardware

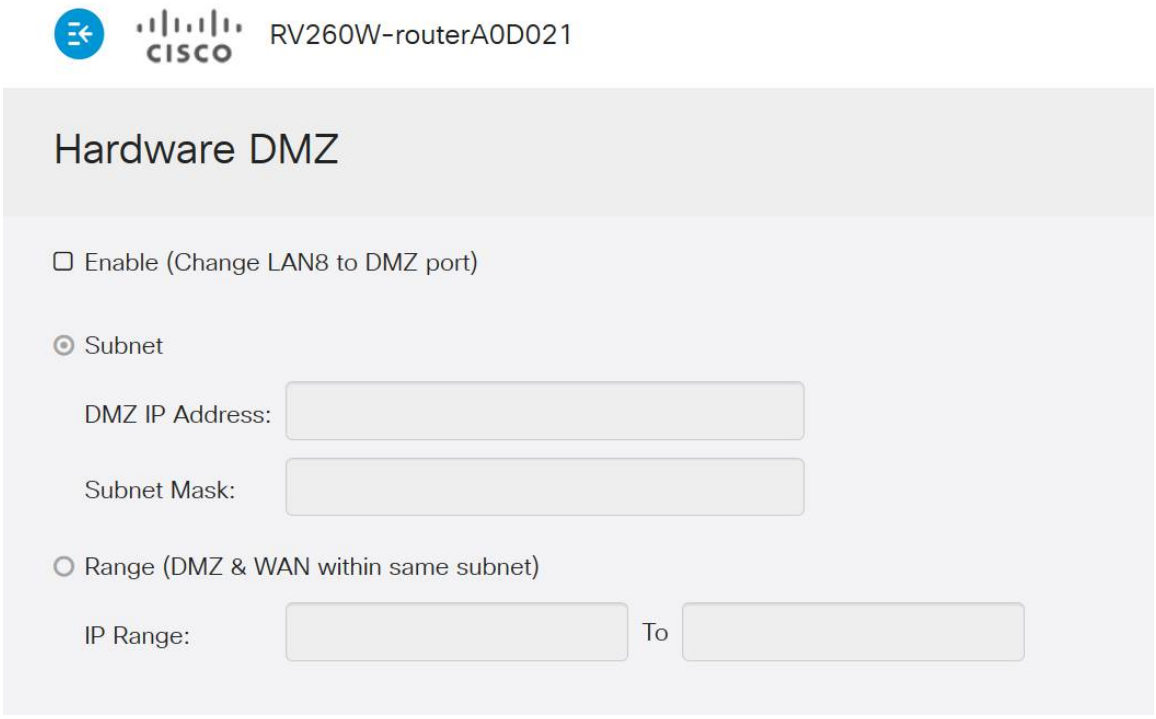
Disponible sólo para la serie RV260X, este método requiere información de direccionamiento IP diferente en función del método que elija. Ambos métodos utilizan subredes para definir la zona, la diferencia es cuánto de la subred se utiliza para crear la zona desmilitarizada. En este caso, las opciones son - *todas* o *algunas*. El método Subnet (*all*) requiere la dirección IP de la propia DMZ, junto con la máscara de subred. Este método ocupa todas las direcciones IP que pertenecen a esa subred. Mientras que el método Range (*algunos*) permite definir un rango continuo de direcciones IP que se ubicarán dentro de la DMZ.

Nota: En cualquier caso, deberá trabajar con el ISP para definir el esquema de direccionamiento IP de la subred.

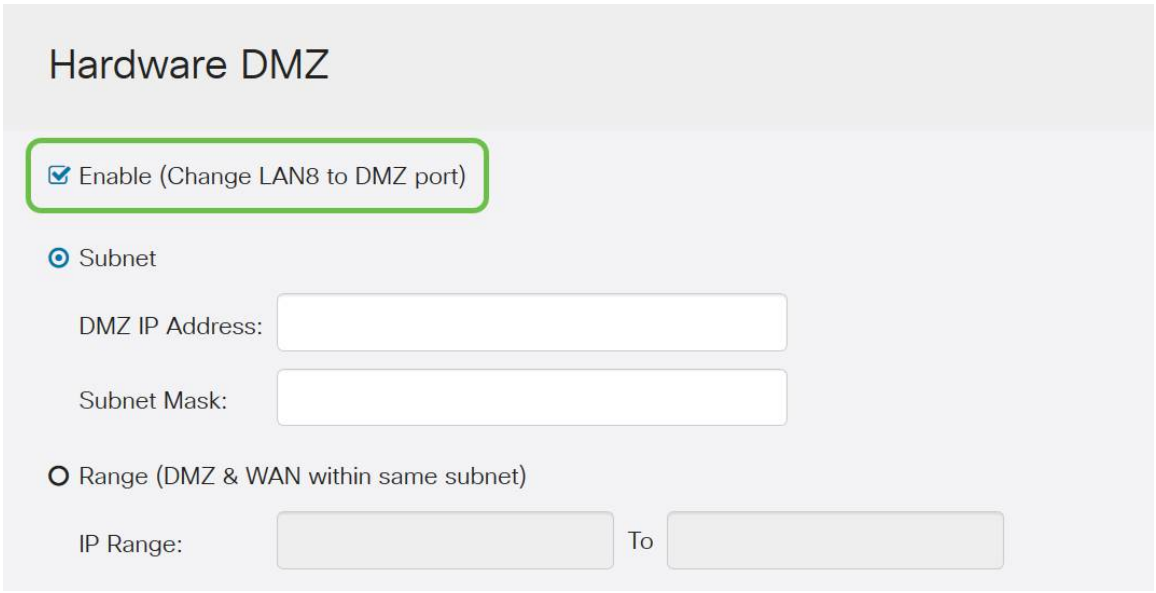
Paso 1. Después de iniciar sesión en el dispositivo RV260X, haga clic en **WAN > Hardware DMZ**



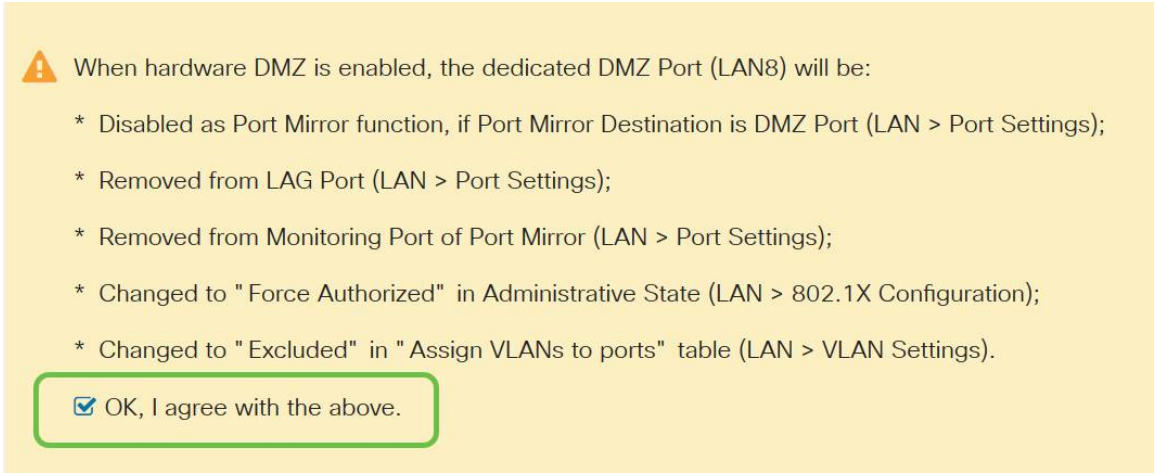
Nota: Las capturas de pantalla se toman de la interfaz de usuario de RV260X. A continuación se muestra la captura de pantalla de las opciones de DMZ de hardware que se mostrarán en esta página.



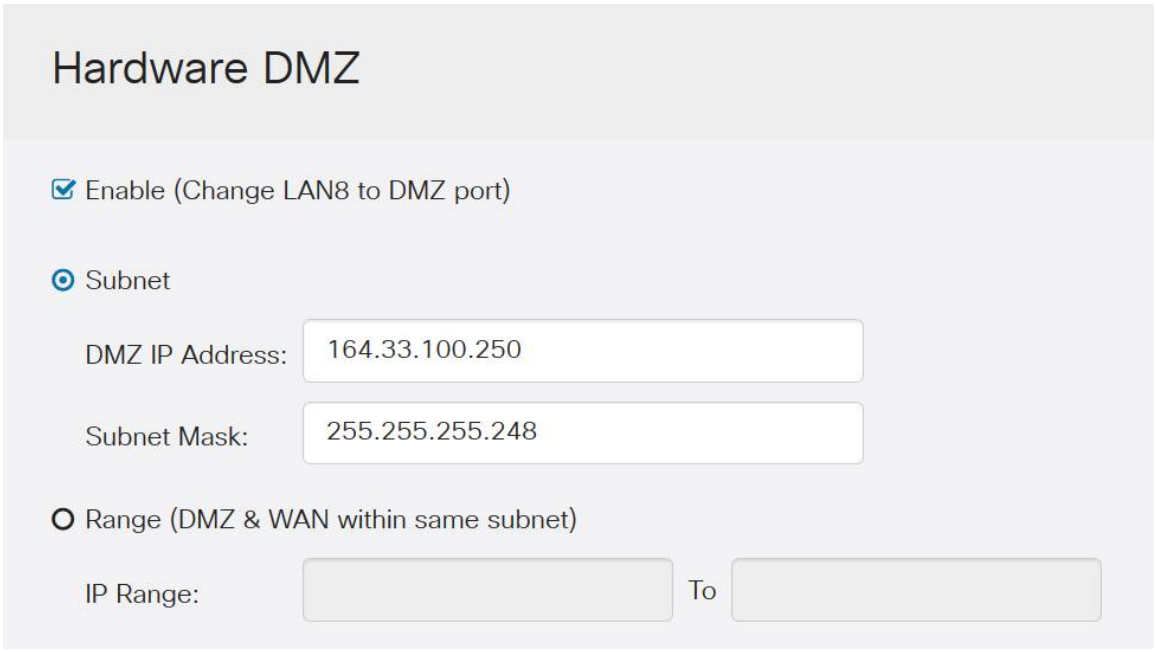
Paso 2. Haga clic en la casilla de verificación **Enable (Cambiar LAN8 a puerto DMZ)**. Esto convertirá el puerto 8° del router en una "ventana" solo de DMZ a servicios que requieren una seguridad mejorada.



Paso 3. Después de hacer clic en *Habilitar* se muestra un mensaje informativo debajo de las opciones seleccionables. Revise los detalles de los puntos que pueden afectar a su red y haga clic en la **casilla Aceptar, estoy de acuerdo con la** casilla **anterior.**

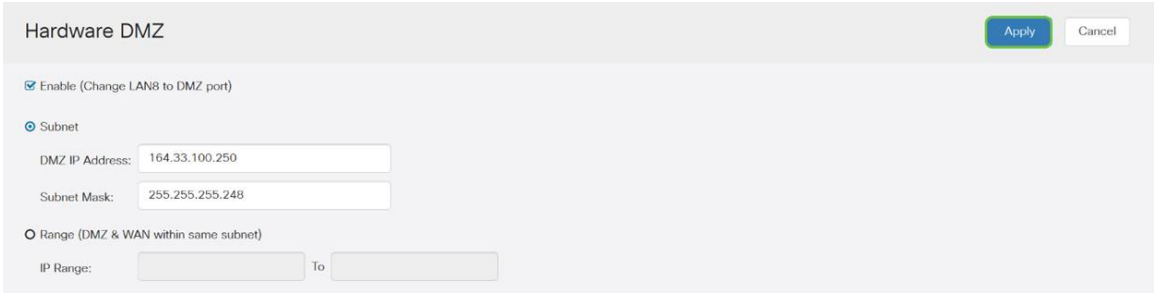


Paso 4. El siguiente paso se divide en dos opciones potenciales, Subred y Rango. En el siguiente ejemplo hemos seleccionado el método **Subnet**.



Nota: Si desea utilizar el método Range, deberá hacer clic en el botón **Range** radial y, a continuación, introducir el intervalo de direcciones IP asignado por el ISP.

Paso 6. Haga clic en **Aplicar** (en la esquina superior derecha) para aceptar la configuración de DMZ.

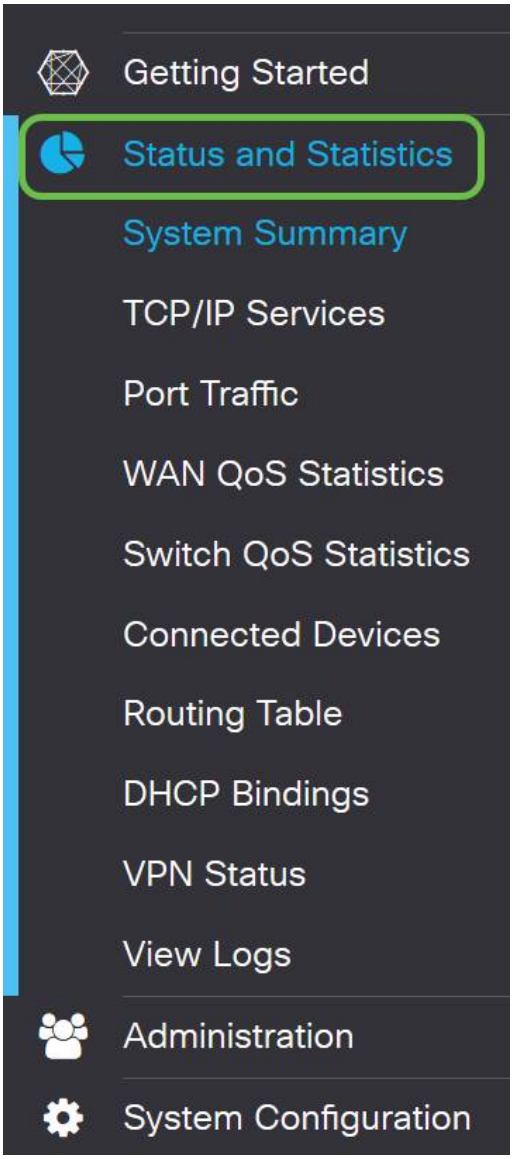


Confirmación de que la DMZ está configurada correctamente

Al verificar que la DMZ esté configurada para aceptar correctamente el tráfico de orígenes fuera de su zona, bastará con una prueba de ping. En primer lugar, pasaremos por la interfaz de

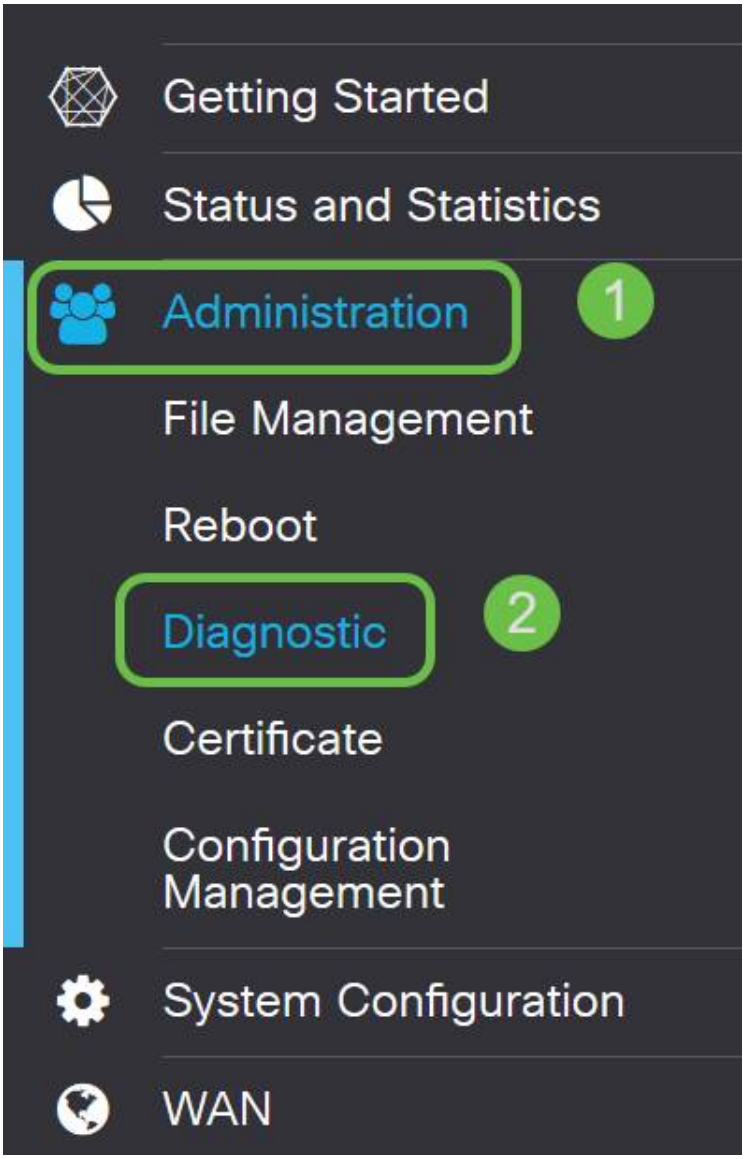
administración para verificar el estado de la DMZ.

Paso 1. Para verificar que su DMZ está configurada, navegue hasta **Estado y estadísticas**, la página cargará automáticamente la página Resumen del sistema**.** El puerto 8 o "Lan 8" enumerarán el estado de la DMZ como "*Conectada*".



Podemos utilizar la función de ping ICMP confiable para probar si la DMZ funciona como se esperaba. El mensaje ICMP o simplemente "ping", intenta llamar a la puerta de la DMZ. Si la DMZ responde diciendo "Hola", el ping se completa.

Paso 2. Para navegar por el explorador hasta la función ping, haga clic en **Administration > Diagnostic**.



Paso 3. Ingrese la **dirección IP de la DMZ** y haga clic en el botón **Ping**.

Si el ping se realiza correctamente, verá un mensaje como el anterior. Si el ping falla, significa que no se puede alcanzar la DMZ. Compruebe los parámetros de DMZ para asegurarse de que están configurados correctamente.

Conclusión

Ahora que ha completado la configuración de la DMZ, debe poder comenzar a acceder a los servicios desde fuera de la LAN.