

Opções DMZ para roteadores RV160/RV260

Objetivo

Este documento abordará as duas opções de configuração de um host de Zona Desmilitarizada - DMZ e de uma sub-rede DMZ nos roteadores da série RV160X/RV260X.

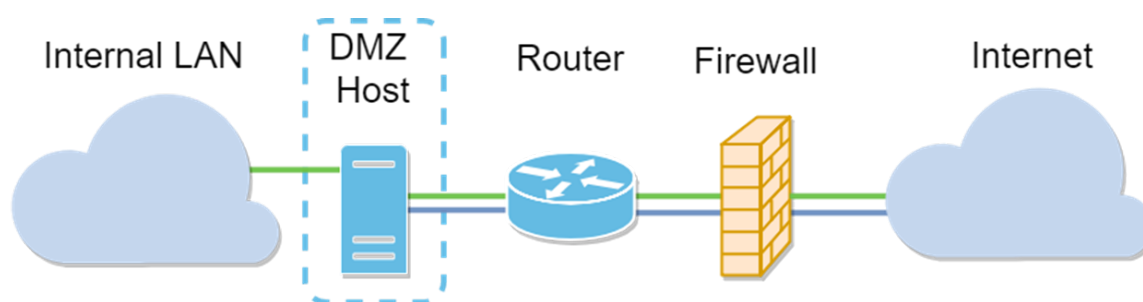
Requirements

- RV160X
- RV260X

Introduction

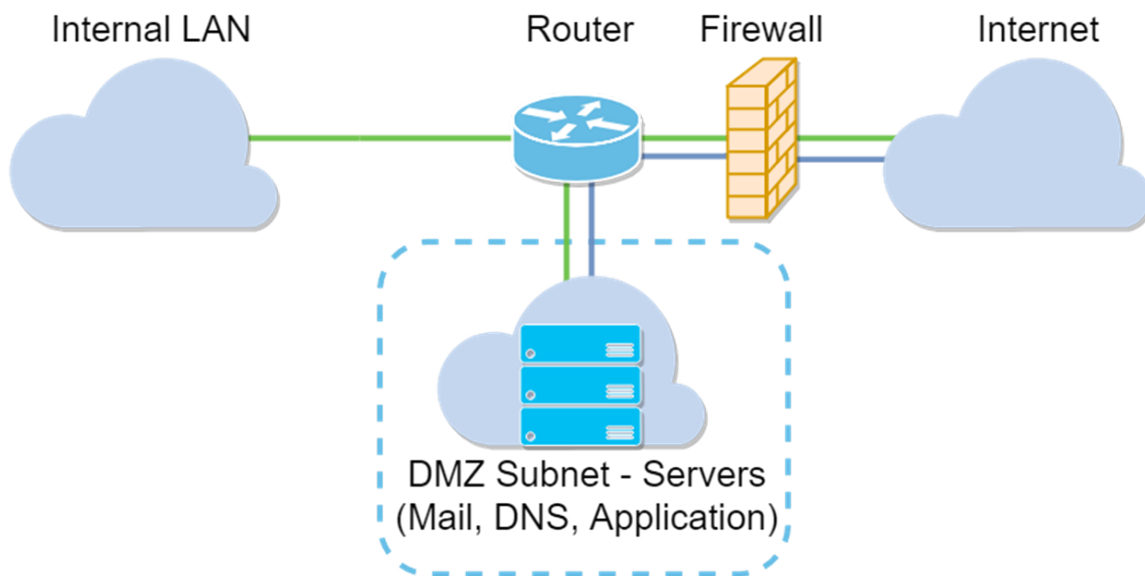
Uma DMZ é um local em uma rede aberta à Internet enquanto protege a rede local (LAN) por trás de um firewall. A separação da rede principal de um único host ou de uma sub-rede inteira, ou "sub-rede", garante que as pessoas que visitam o servidor do seu site através da DMZ, não terão acesso à sua LAN. A Cisco oferece dois métodos de uso de DMZs em sua rede que apresentam distinções importantes na forma como operam. Abaixo estão referências visuais que destacam a diferença entre os dois modos de operação.

Topologia DMZ do host



Note: Ao usar uma DMZ de host, se o host for comprometido por um mau agente, sua LAN interna poderá estar sujeita a mais intrusão de segurança.

Topologia DMZ de sub-rede



Tipo de DMZ	Comparar	Contraste
Host	Segrega o tráfego	Host único, totalmente aberto à Internet
Sub-rede/Intervalo	Segrega o tráfego	Vários dispositivos e tipos, totalmente abertos à Internet. Disponível somente no hardware RV260.

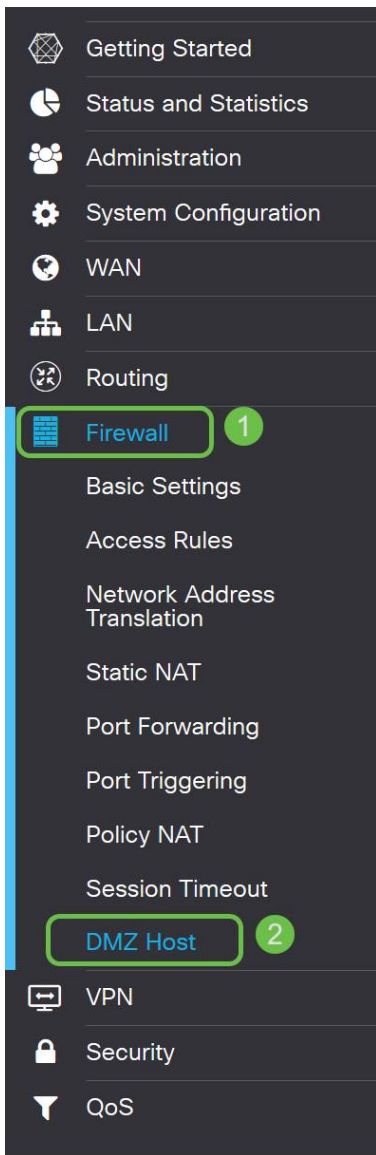
Sobre o endereçamento IP

Este artigo usa esquemas de endereçamento IP que carregam alguma nuance em seu uso. Ao planejar sua DMZ, você pode considerar o uso de um endereço IP privado ou público. Um endereço IP privado será exclusivo para você, somente na LAN. Um endereço IP público será exclusivo da sua organização e será atribuído pelo seu provedor de serviços de Internet. Para adquirir um endereço IP público, você precisará entrar em contato com seu (ISP).

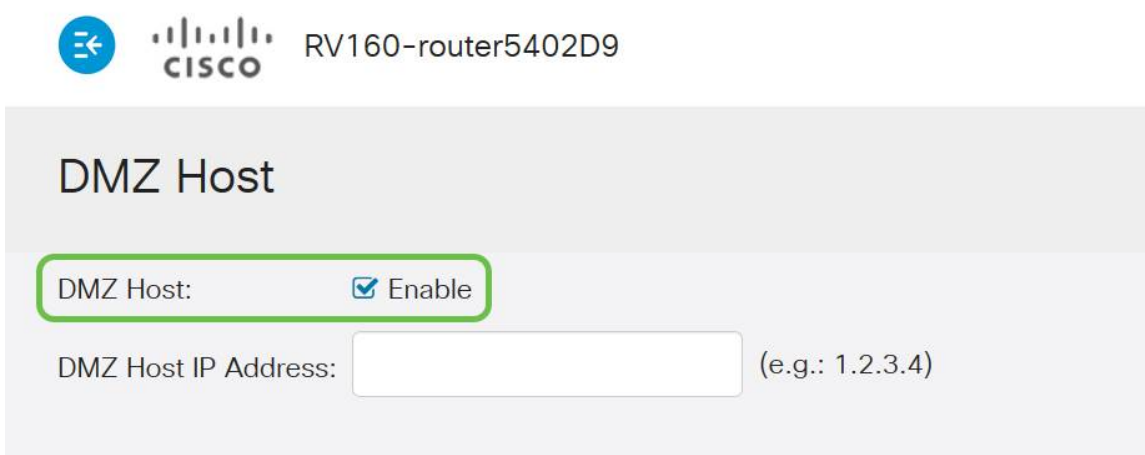
Configurando o host DMZ

As informações necessárias para esse método incluem o endereço IP do host pretendido. O endereço IP pode ser público ou privado, mas o endereço IP público deve estar em uma sub-rede diferente do endereço IP da WAN. A opção DMZ Host está disponível no RV160X e no RV260X. Configure o host DMZ seguindo as etapas abaixo.

Etapa 1. Após fazer login no dispositivo de roteamento, na barra de menus à esquerda, clique em **Firewall > DMZ Host**.



Etapa 2. Clique na caixa de seleção **Habilitar**.



Etapa 3. Insira o endereço IP designado do host que deseja abrir para o acesso à WAN.



RV160-router5402D9

DMZ Host

DMZ Host: Enable

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

Etapa 4. Quando satisfeito com seu endereçamento, clique no botão Aplicar.



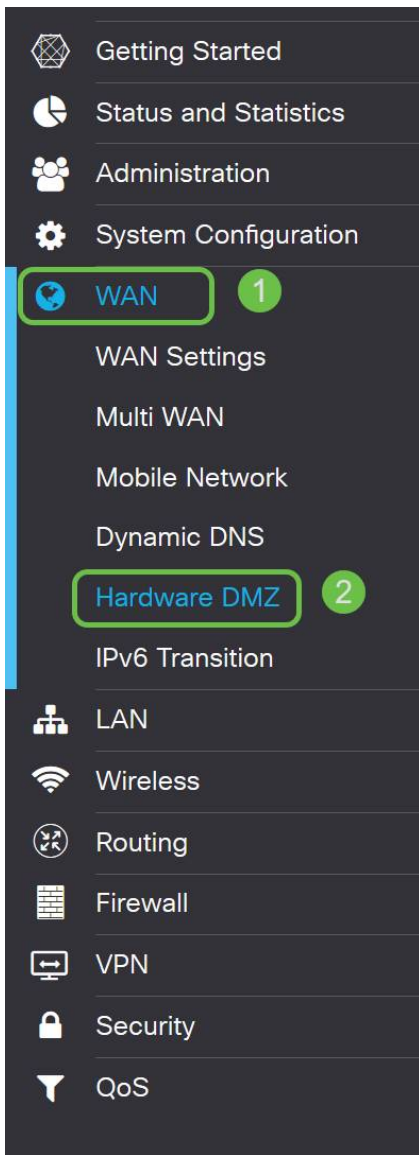
Note: Se estiver trabalhando somente com uma série RV160X e quiser ir para as instruções de verificação, [clique aqui para ir para essa seção deste documento](#).

Configurando DMZ de hardware



Disponível somente para a série RV260X, esse método exige informações de endereçamento IP diferentes com base no método escolhido. Ambos os métodos realmente usam sub-redes para definir a zona, a diferença é quanto da sub-rede é usada para criar a zona desmilitarizada. Neste caso, as opções são - *todas* ou *algumas*. O método Sub-rede (*todos*) exige o endereço IP da própria DMZ, juntamente com a máscara de sub-rede. Esse método ocupa todos os endereços IP pertencentes a essa sub-rede. Enquanto que o método Intervalo (*alguns*) permite definir um intervalo contínuo de endereços IP a serem localizados na DMZ.

Note: Em ambos os casos, você precisará trabalhar com o ISP para definir o esquema de endereçamento IP da sub-rede.

Etapa 1. Depois de fazer login no dispositivo RV260X, clique em **WAN > Hardware DMZ**



Note: As capturas de tela são tiradas da interface de usuário RV260X. Abaixo está a captura de tela das opções DMZ de hardware que serão exibidas nesta página.

  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

Etapa 2. Clique na caixa de seleção **Enable (Change LAN8 to DMZ port) (Habilitar (Alterar porta LAN8 para DMZ))**. Isso converterá a 8ª porta do roteador em uma "janela" somente DMZ para serviços que exigem segurança avançada.

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet


DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

Etapa 3. Depois de clicar em *Ativar*, uma mensagem informativa é exibida abaixo das opções selecionáveis. Revise os detalhes dos pontos que podem afetar sua rede e clique na caixa de seleção **OK, Concordo com a acima**.

 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.

Etapa 4. A próxima etapa se divide em duas opções possíveis, Sub-rede e Intervalo. Em nosso exemplo abaixo selecionamos o método **Sub-rede**.

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address: 164.33.100.250

Subnet Mask: 255.255.255.248

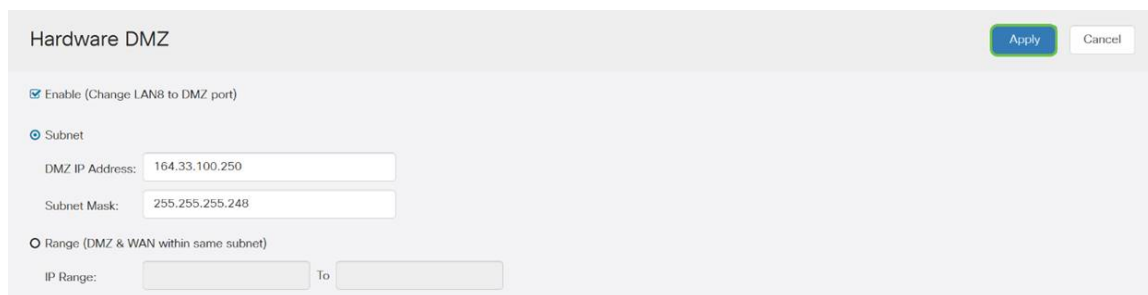
Range (DMZ & WAN within same subnet)

IP Range:

To

Note: Se você pretende usar o método Range (Intervalo), você precisará clicar no botão radial **Range (Intervalo)** e inserir o intervalo de endereços IP atribuídos pelo ISP.

Etapa 6. Clique em **Apply** (no canto superior direito) para aceitar as configurações de DMZ.

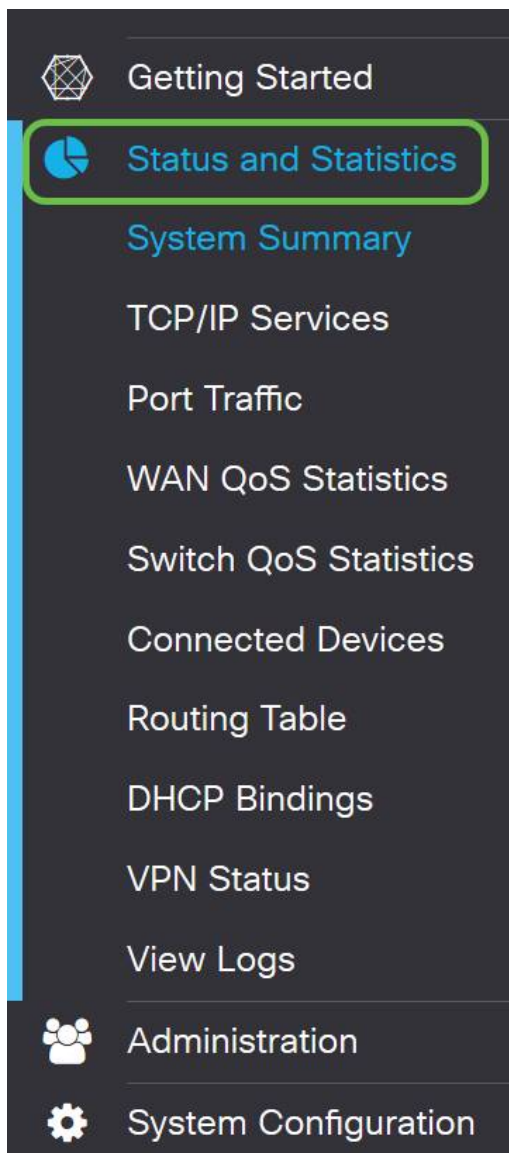


The screenshot shows the 'Hardware DMZ' configuration page. At the top right, there are two buttons: 'Apply' (highlighted in green) and 'Cancel'. The configuration options are the same as in the previous image, with 'Subnet' selected and the IP address and subnet mask entered.

Confirmação de que a DMZ está configurada corretamente

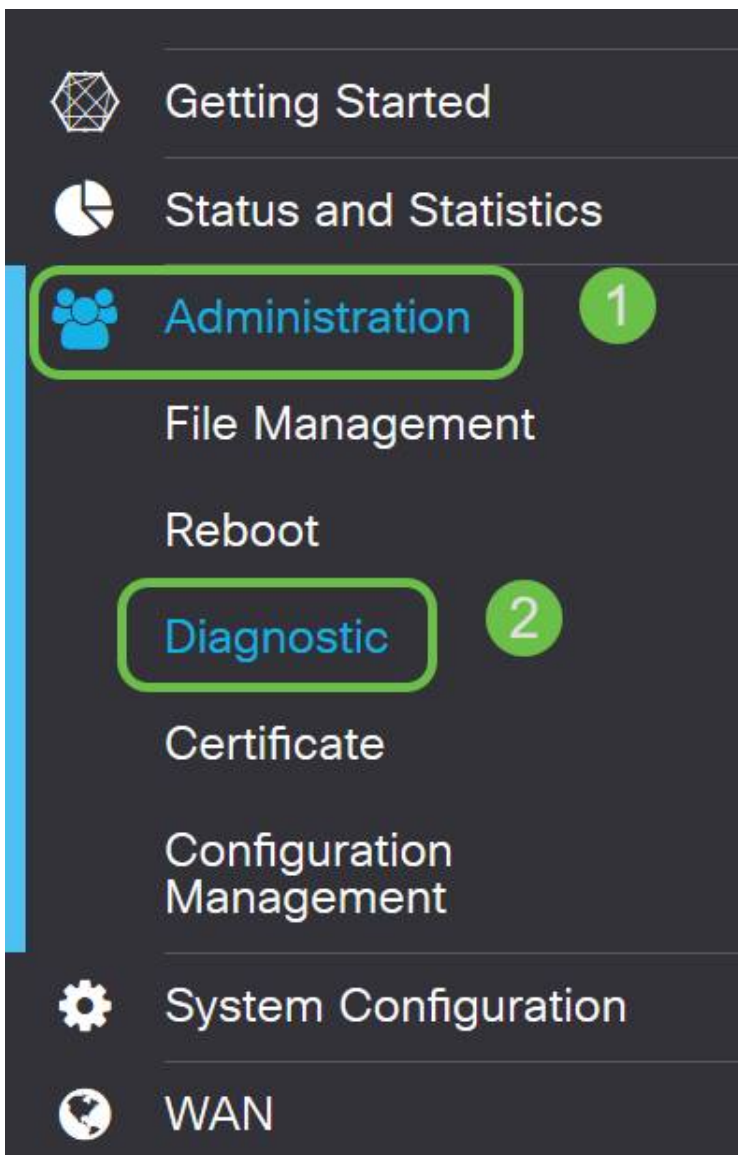
Verificando se a DMZ está configurada para aceitar adequadamente o tráfego de fontes fora de sua zona, um teste de ping será suficiente. Primeiro, porém, passaremos pela interface de administração para verificar o status do DMZ.

Etapa 1. Para verificar se o DMZ está configurado, navegue para **Status & Statistics**, a página carregará a página System Summary automaticamente. A porta 8 ou a "LAN 8" listarão o status da DMZ como "*Conectada*".



Podemos usar o recurso confiável de ping ICMP para testar se a DMZ está funcionando conforme o esperado. A mensagem ICMP ou apenas "ping" tenta bater na porta do DMZ. Se a DMZ responder dizendo "Olá", o ping é concluído.

Etapa 2. Para navegar pelo seu navegador até o recurso ping, clique em **Administration > Diagnostic**.



Etapa 3. Insira o endereço IP da DMZ e clique no botão Ping.



Se o ping tiver êxito, você verá uma mensagem como a acima. Se o ping falhar, significa que a DMZ não pode ser alcançada. Verifique suas configurações de DMZ para garantir que elas estejam configuradas corretamente.

Conclusão

Agora que concluiu a configuração da DMZ, você deve poder começar a acessar os serviços de fora da LAN.