# DMZ-opties voor RV160/RV260-routers

## Doel

Dit document bevat de twee opties voor het instellen van een gedemilitariseerde zone-DMZ host- en DMZ-subsysteem op RV160X/RV260X Series-routers.

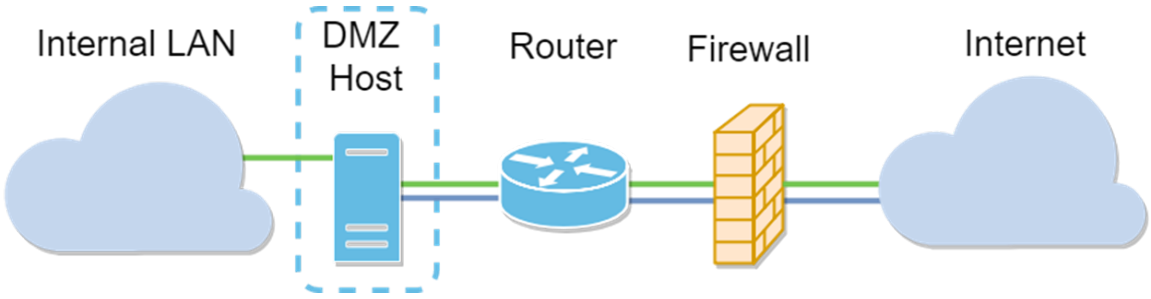
## Vereisten

- RV160X-software
- RV260X-software

## Inleiding

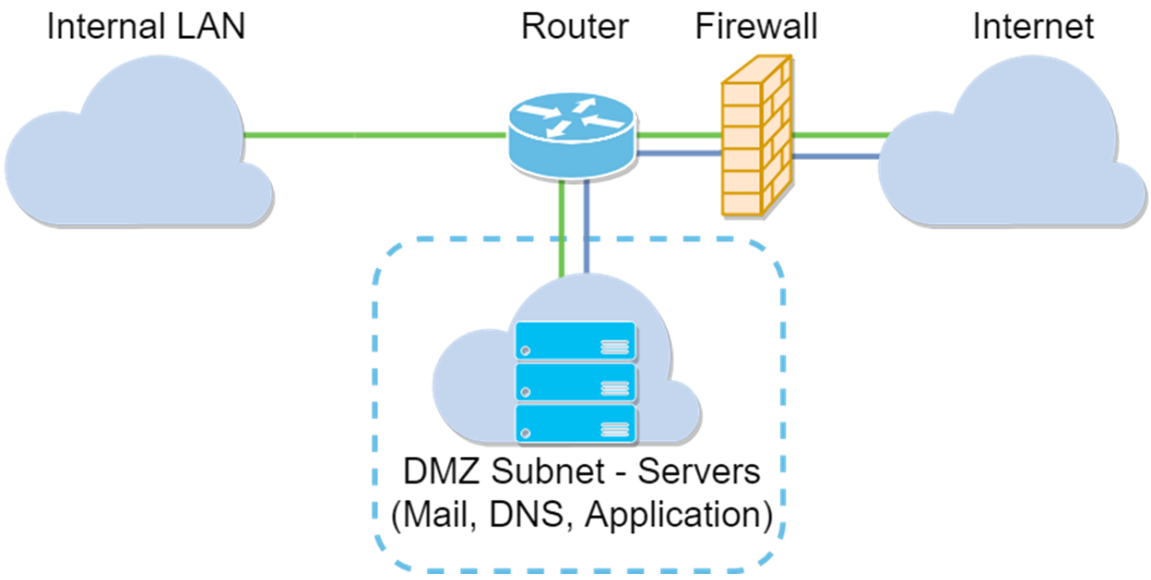
Een DMZ is een locatie op een netwerk die open is voor internet, terwijl u uw LAN (Local Area Network) achter een firewall beveiligen. Als u het hoofdnetwerk van één host of een volledig subnetwerk wilt scheiden, of als u een subnetwerk hebt, zorgt 'net' ervoor dat mensen die uw website server via DMZ bezoeken, geen toegang hebben tot uw LAN. Cisco biedt twee methoden om DMZs in uw netwerk te gebruiken die beiden belangrijke verschillen in hoe zij werken hebben. Hieronder staan visuele referenties die het verschil tussen de twee besturingsmodi markeren.

## Host DMZ-topologie




Opmerking: Wanneer u een host-DMZ gebruikt, kan de host als gevolg van een slecht-actor uw interne LAN opnieuw security inbraak hebben ondergaan.

## Subnet DMZ-topologie




| DMZ-type | Vergelijken | contrast |
|---|---|---|
| Host | Segregs-verkeer | Enkelvoudige host, volledig open voor internet |
| Subnet / bereik | Segregs-verkeer | Meerdere apparaten en typen, volledig open voor internet. **Alleen beschikbaar op RV260-hardware.** |

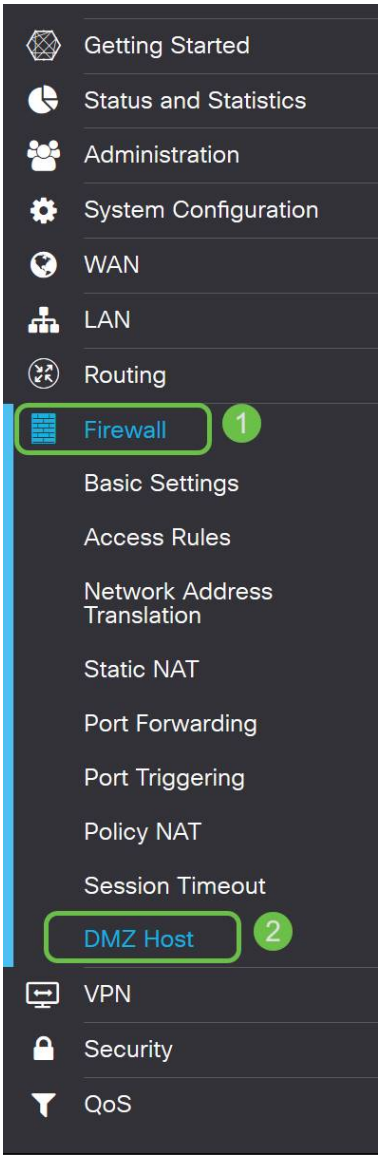
## IP-adressering

In dit artikel wordt gebruik gemaakt van IP-adresseringsschema's die enige nuance in hun gebruik hebben. Bij het plannen van uw DMZ kunt u overwegen een privé of openbaar IP-adres te gebruiken. Een privé IP-adres zal uniek voor u zijn, alleen op uw LAN. Een openbaar IP-adres is uniek voor uw organisatie en wordt toegewezen door uw Internet Service Provider. Om een openbaar IP-adres te verkrijgen moet u contact opnemen met uw (ISP).

## DMZ-host configureren

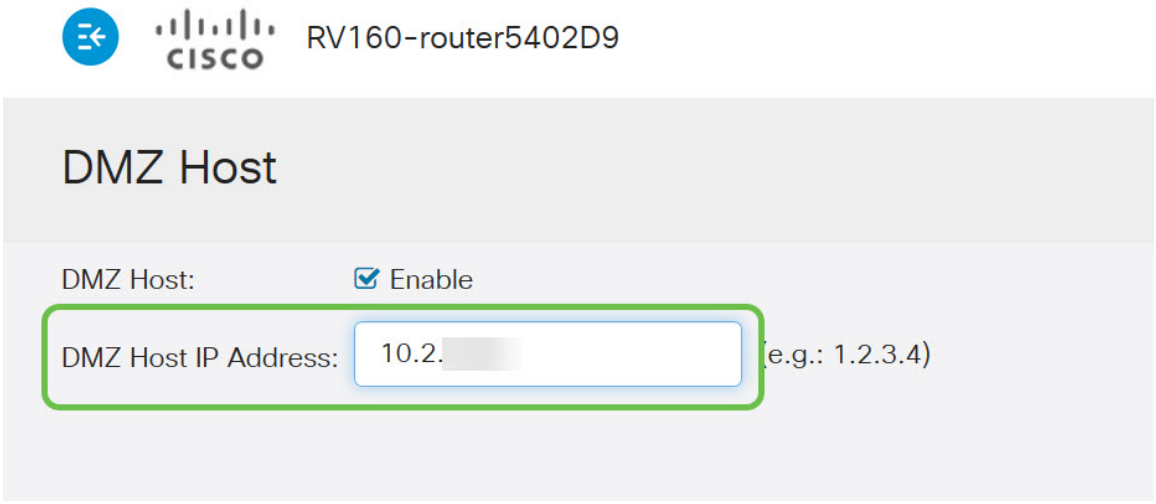
De informatie die voor deze methode vereist is omvat het IP-adres van de bedoelde host. Het IP-adres kan publiek of privaat zijn, maar het openbare IP-adres moet in een ander subnet zijn dan het WAN IP-adres. De DMZ Host optie is beschikbaar in RV160X en RV260X. Configuratie van de DMZ Host volgens de onderstaande stappen.

Stap 1. Na het registreren in uw routingapparaat klikt u in de linkermenu-balk op **Firewall > DMZ Host.**




Stap 2. Klik op het selectieteken **Enable**.


Stap 3. Voer het aangewezen IP-adres in van de host die u wilt openen naar WAN-toegang.




Stap 4. Wanneer u tevreden bent met de adressering, klikt u op de knop toepassen.

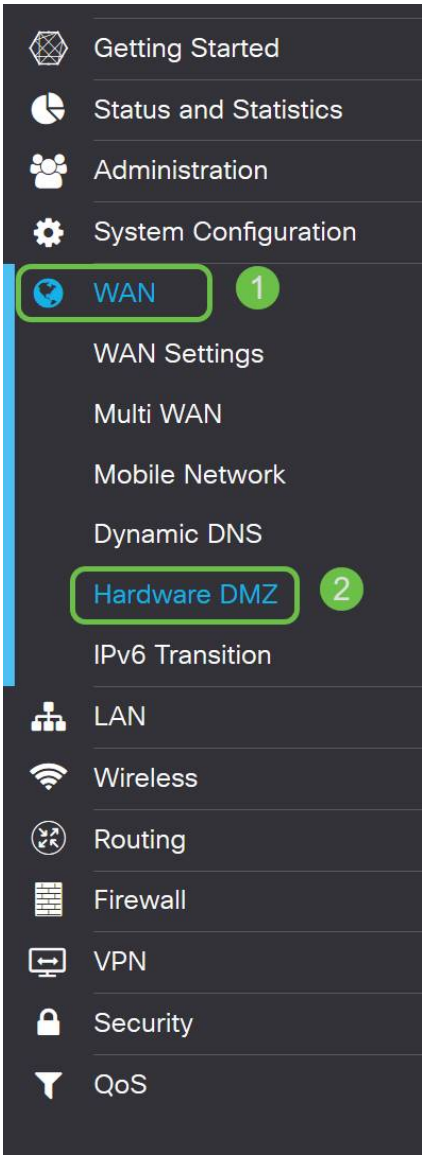

Opmerking: Als u alleen met een RV160X-serie werkt en u naar de verificatie-instructies wilt overslaan, klikt u hier om naar dat gedeelte van dit document te gaan.

## Hardware DMZ configureren

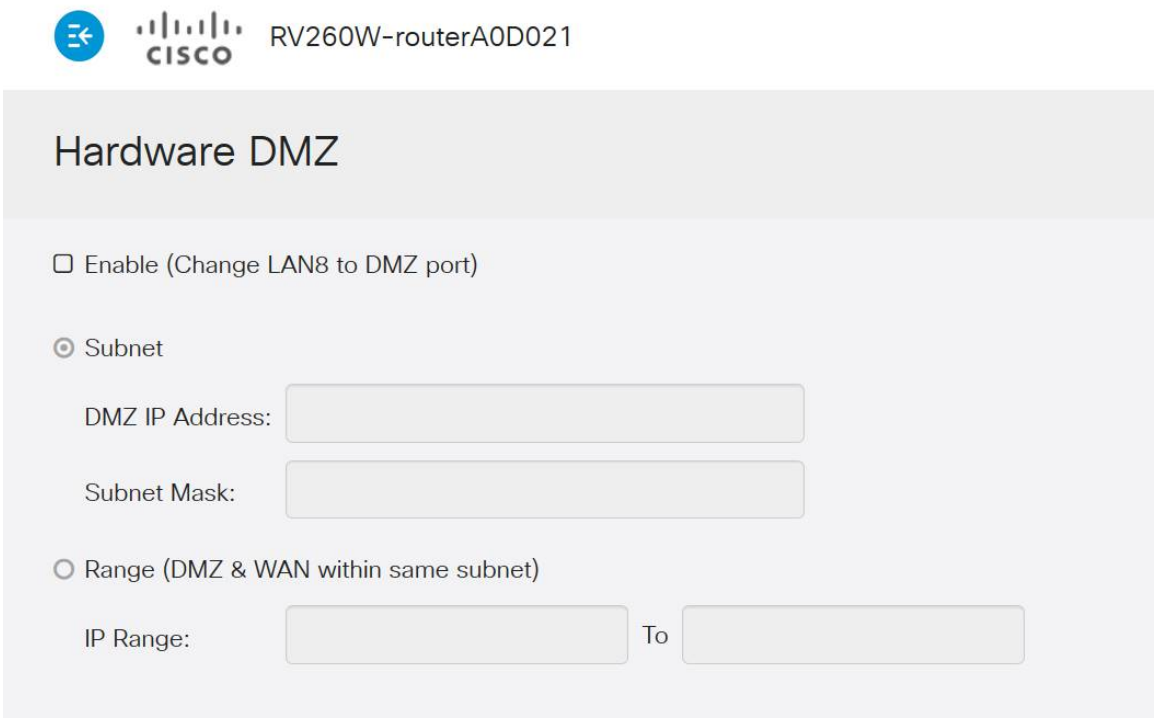
Deze methode is alleen beschikbaar in de RV260X-serie. Voor deze methode is verschillende IP-adresinformatie vereist op basis van de door u gekozen methode. Beide methoden gebruiken inderdaad subnetwerken om de zone te definiëren; het verschil is hoeveel van het subnetwerk wordt gebruikt om de gedemilitariseerde zone te creëren. In dit geval zijn de opties - *allemaal* of *sommige*. De Subnet (*alle*) methode vereist het IP adres van de DMZ zelf, samen met het SUBNET masker. Deze methode bezet alle IP adressen die tot dat subnetwerk behoren. Terwijl de methode van het Bereik (*sommige*) u toestaat om een ononderbroken bereik van IP adressen te bepalen om binnen DMZ te vinden.

Opmerking: In beide gevallen zult u met uw ISP moeten werken om het IP-adresseringsschema van het subnetwerk te definiëren.

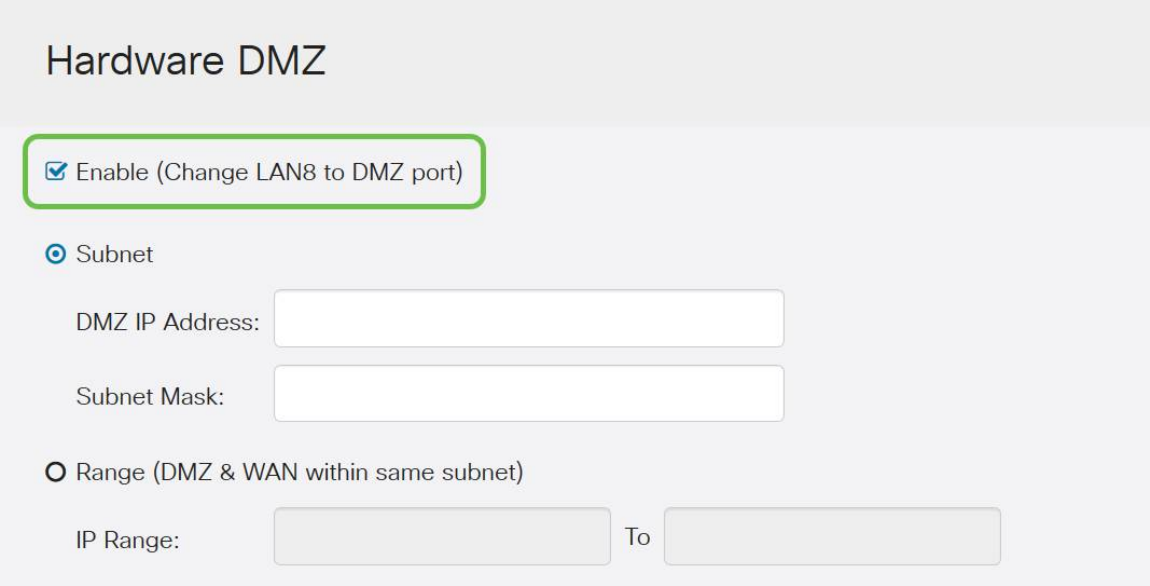
Stap 1. Na het registreren in uw RV260X-apparaat klikt u op **WAN > hardware-DMZ**



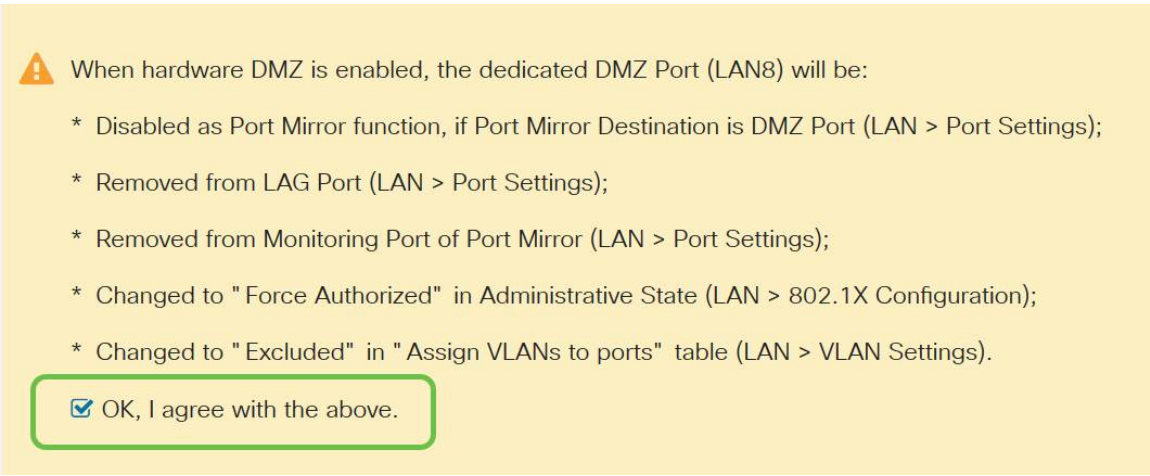

Opmerking: De screenshots worden opgenomen in de RV260X-gebruikersinterface. Hieronder staat het screenshot van de opties voor hardware-DMZ die op deze pagina worden weergegeven.



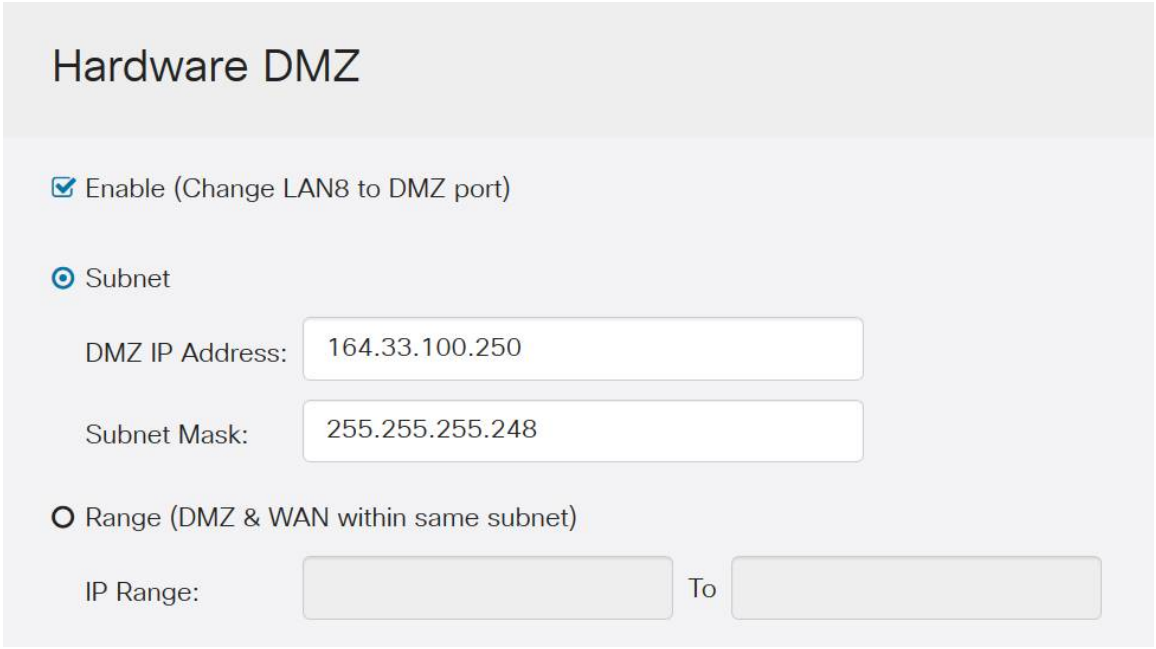
Stap 2. Klik op het selectieteken **Schakel LAN8 in DMZ**. Dit zal de 8e poort op de router in een "venster" alleen "DMZ" naar services converteren die verbeterde beveiliging vereisen.




Stap 3. Na het klikken op Een informatief bericht *inschakelen* geeft u de onderstaande opties weer. Bekijk de details voor punten die uw netwerk kunnen beïnvloeden en klik op **OK, ik ga akkoord met het bovenstaande** selectieteken**.**

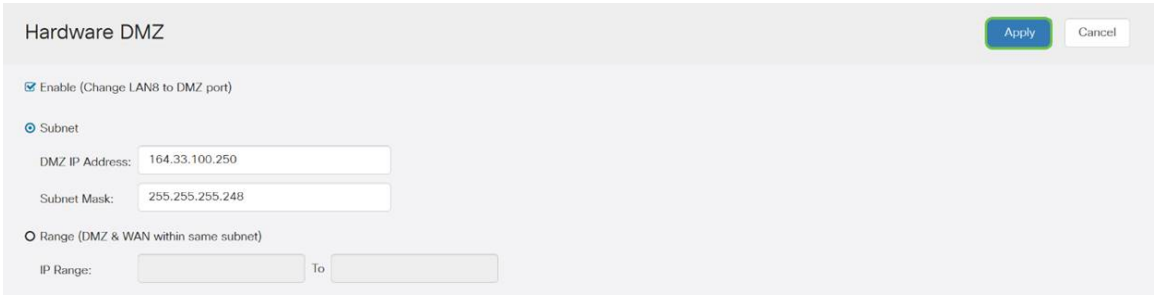



Stap 4. De volgende stap wordt verdeeld in twee mogelijke opties, Subnet en Bereik. In ons voorbeeld hieronder hebben we de **Subnet** methode geselecteerd.




Opmerking: Als u de methode van het Bereik wilt gebruiken, moet u op de radiale knop Bereik klikken en vervolgens het bereik van IP-adressen door uw ISP invoeren.

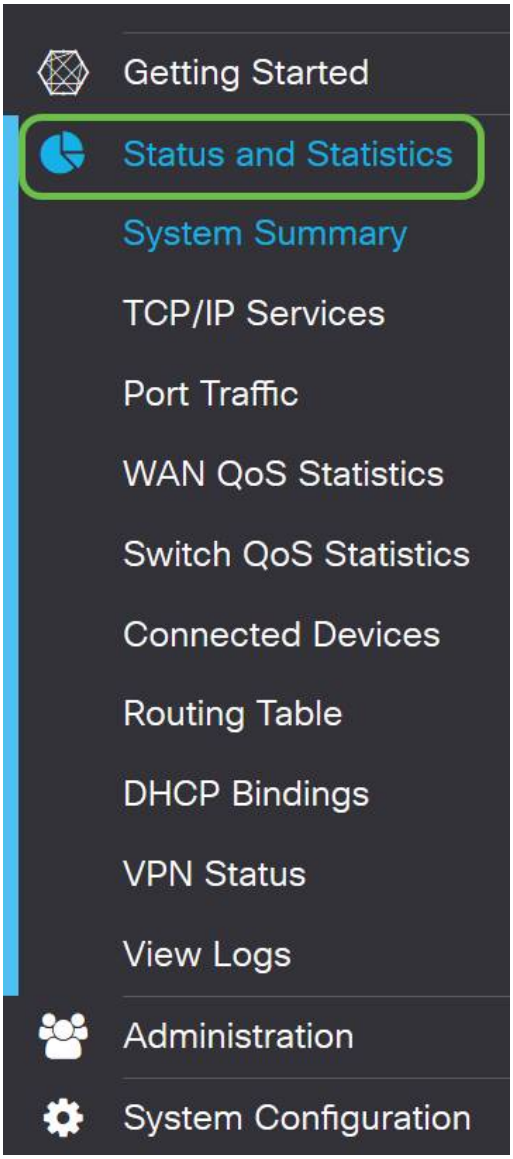
Stap 6. Klik op **Toepassen** (in de rechterbovenhoek) om de DMZ-instellingen te aanvaarden.




# De DMZ-instellingen bevestigen is correct geïnstalleerd

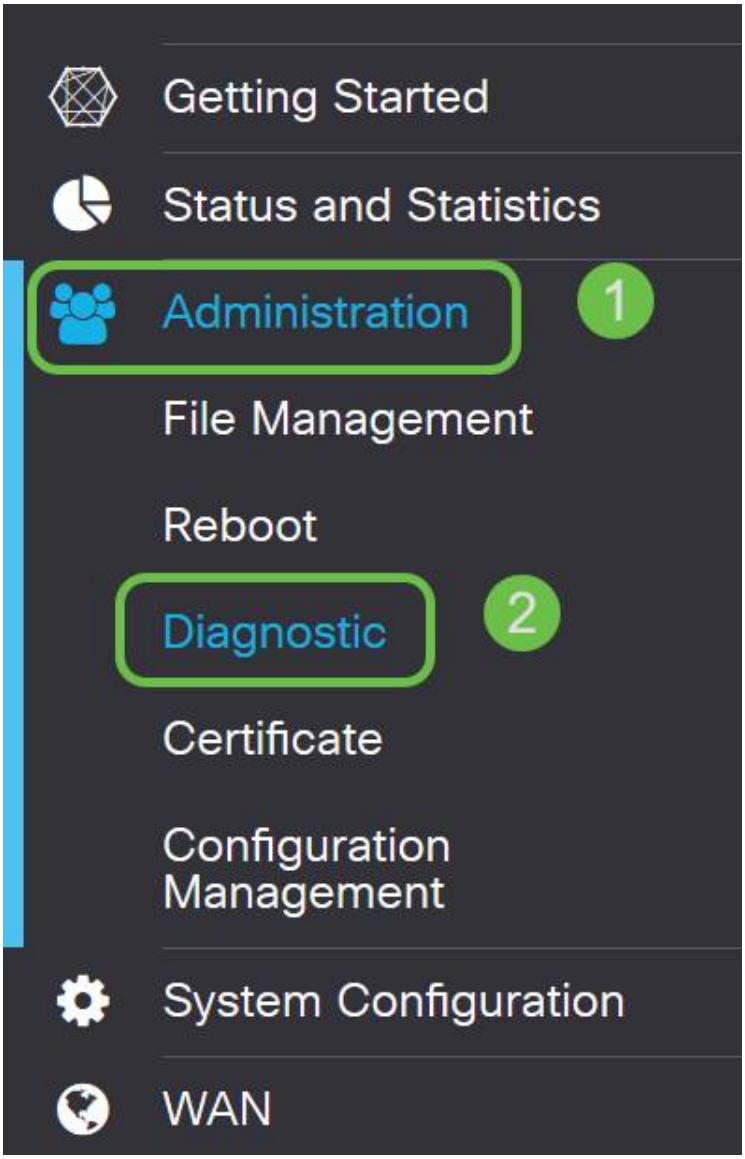
Verifiëren van de DMZ is ingesteld om verkeer vanuit bronnen buiten de zone correct te accepteren. Een ping-test zal volstaan. Eerst stoppen we bij de interface om de status van de DMZ te controleren.

Stap 1. Om te controleren of uw DMZ is ingesteld, navigeer dan naar **Status en Statistieken**. Op de pagina wordt automatisch de pagina met systeemoverzicht geladen. Port 8 of "LAN 8" geven de status van de DMZ op als "*Connected*".




We kunnen de betrouwbare ICMP-ping gebruiken om te testen of de DMZ werkt zoals verwacht. Met het ICMP-bericht of gewoon "ping" probeert u op de deur van de DMZ te kloppen. Als de DMZ reageert met "Hallo", is de ping voltooid.

Stap 2. Als u in uw browser op de ping-functie wilt navigeren, klikt u op **Administration > Diagnostic**.




Stap 3. Voer het **IP-adres van de DMZ in** en klik op de knop **Ping**.


Als de ping is geslaagd, ziet u een bericht zoals hierboven. Als de ping mislukt, betekent dit dat de DMZ niet kan worden bereikt. Controleer uw DMZ-instellingen om er zeker van te zijn dat ze correct zijn geconfigureerd.

## Conclusie

Nu u de instellingen van de DMZ hebt voltooid, kunt u de services beginnen te gebruiken vanaf buiten het LAN.