Options DMZ pour routeurs RV160/RV260

Objectif

Ce document couvre les deux options de configuration d'un hôte DMZ zone démilitarisé et d'un sous-réseau DMZ sur les routeurs de la gamme RV160X/RV260X.

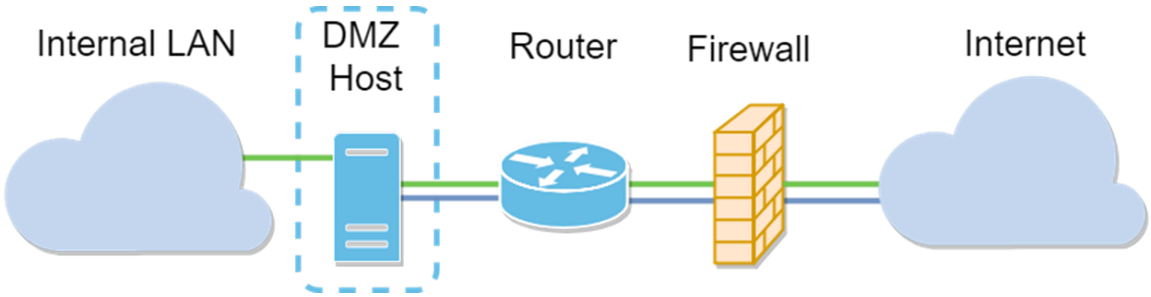
Conditions requises

- RV160X
- RV260X

Introduction

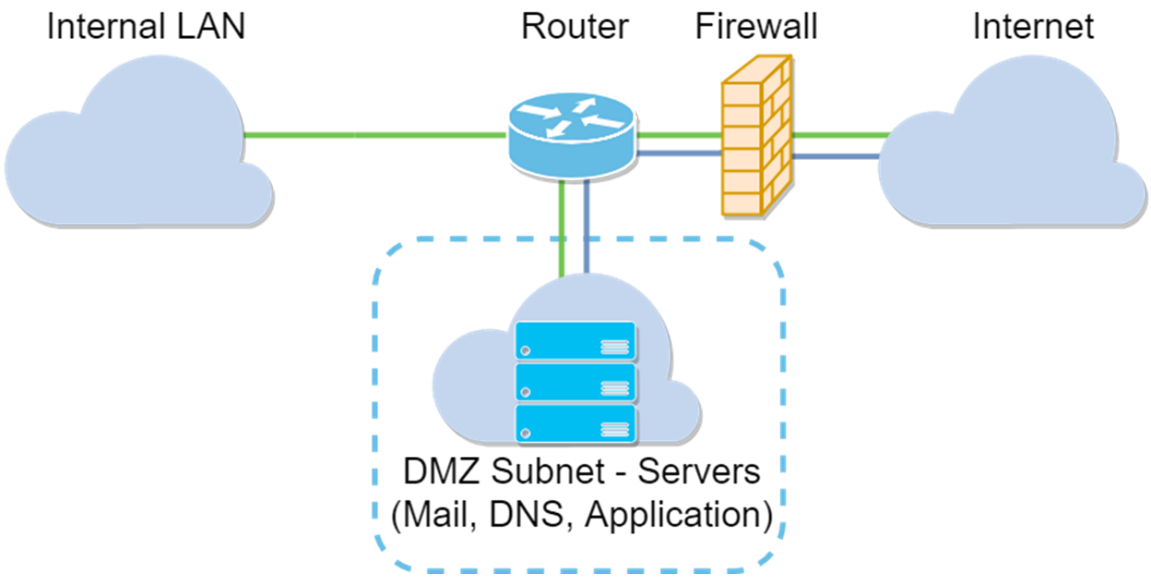
Une zone démilitarisée (DMZ) est un emplacement sur un réseau ouvert à Internet tout en sécurisant votre réseau local (LAN) derrière un pare-feu. La séparation du réseau principal d'un hôte unique ou d'un sous-réseau entier, ou de « sous-réseau », garantit que les personnes qui visitent votre serveur Web via la DMZ n'auront pas accès à votre réseau local. Cisco propose deux méthodes d'utilisation des zones démilitarisées dans votre réseau qui présentent toutes deux des différences importantes dans leur fonctionnement. Les références visuelles ci-dessous mettent en évidence la différence entre les deux modes de fonctionnement.

Topologie DMZ hôte



Note: Lorsque vous utilisez une zone démilitarisée hôte, si l'hôte est compromis par un acteur défectueux, votre réseau local interne peut faire l'objet d'une intrusion de sécurité supplémentaire.

Topologie DMZ de sous-réseau



Type DMZ	Comparer	Contraste
Hôte	Sépare le trafic	Hôte unique, entièrement ouvert sur Internet
Sous-réseau/Plage	Sépare le trafic	Plusieurs périphériques et types, entièrement ouverts à Internet. **Disponible uniquement sur le matériel RV260.**

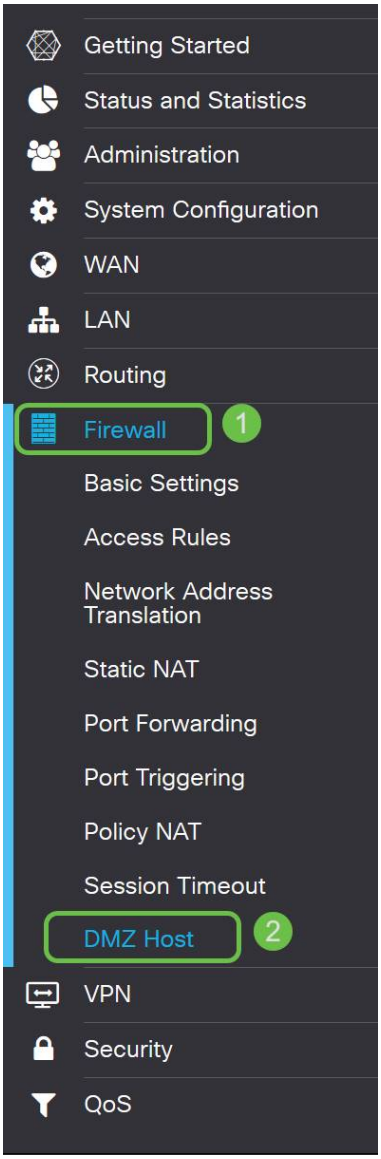
Concernant l’adressage IP

Cet article utilise des schémas d’adressage IP qui présentent certaines nuances dans leur utilisation. Lors de la planification de votre DMZ, vous pouvez envisager d'utiliser une adresse IP privée ou publique. Une adresse IP privée vous sera propre, uniquement sur votre réseau local. Une adresse IP publique sera unique à votre organisation et attribuée par votre fournisseur d'accès Internet. Pour obtenir une adresse IP publique, vous devez contacter votre (FAI).

Configuration de l'hôte DMZ

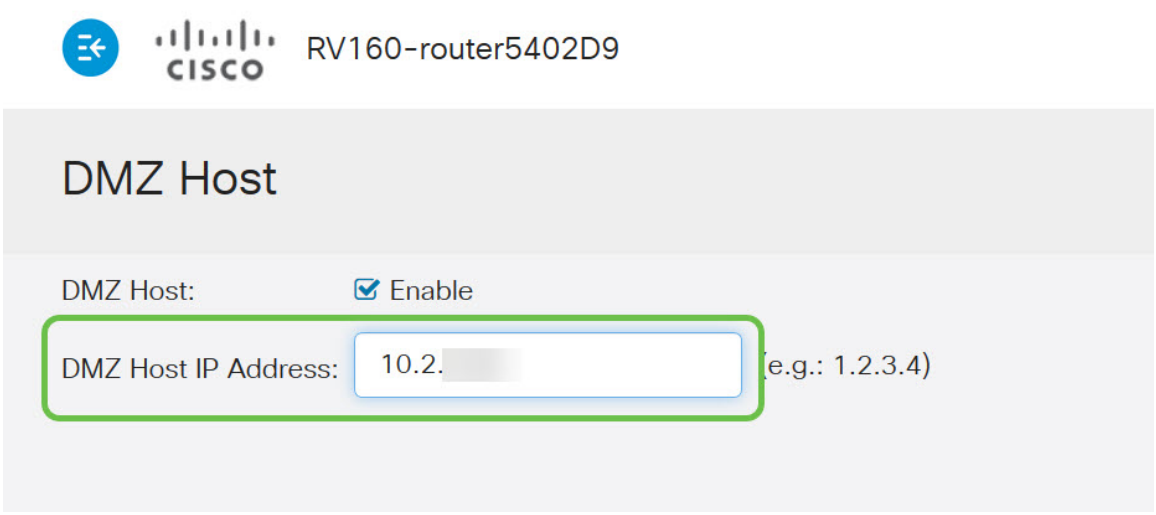
Les informations requises pour cette méthode incluent l'adresse IP de l'hôte souhaité. L'adresse IP peut être publique ou privée, mais l'adresse IP publique doit se trouver dans un sous-réseau différent de l'adresse IP WAN. L'option DMZ Host est disponible sur les modèles RV160X et RV260X. Configurez l’hôte DMZ en procédant comme suit.

Étape 1. Après vous être connecté à votre périphérique de routage, dans la barre de menus de gauche, cliquez sur **Firewall > DMZ Host.**



Étape 2. Cochez la case **Activer**.

Étape 3. Saisissez l'adresse IP désignée de l'hôte que vous souhaitez ouvrir jusqu'à l'accès WAN.



Étape 4. Lorsque vous êtes satisfait de votre adressage, cliquez sur le bouton Apply (Appliquer).

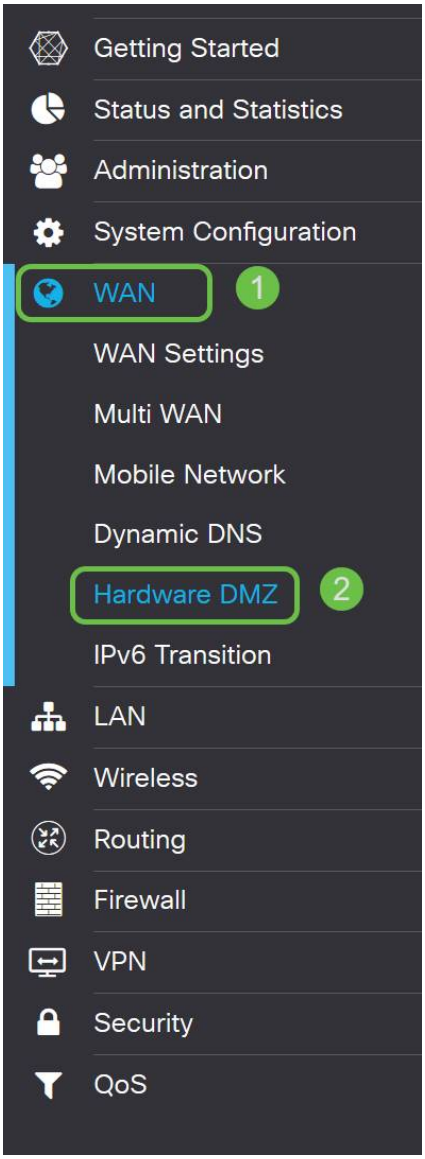
Note: Si vous travaillez avec une gamme RV160X uniquement et que vous voulez passer aux instructions de vérification, cliquez ici pour passer à cette section de ce document.

Configuration de la DMZ matérielle

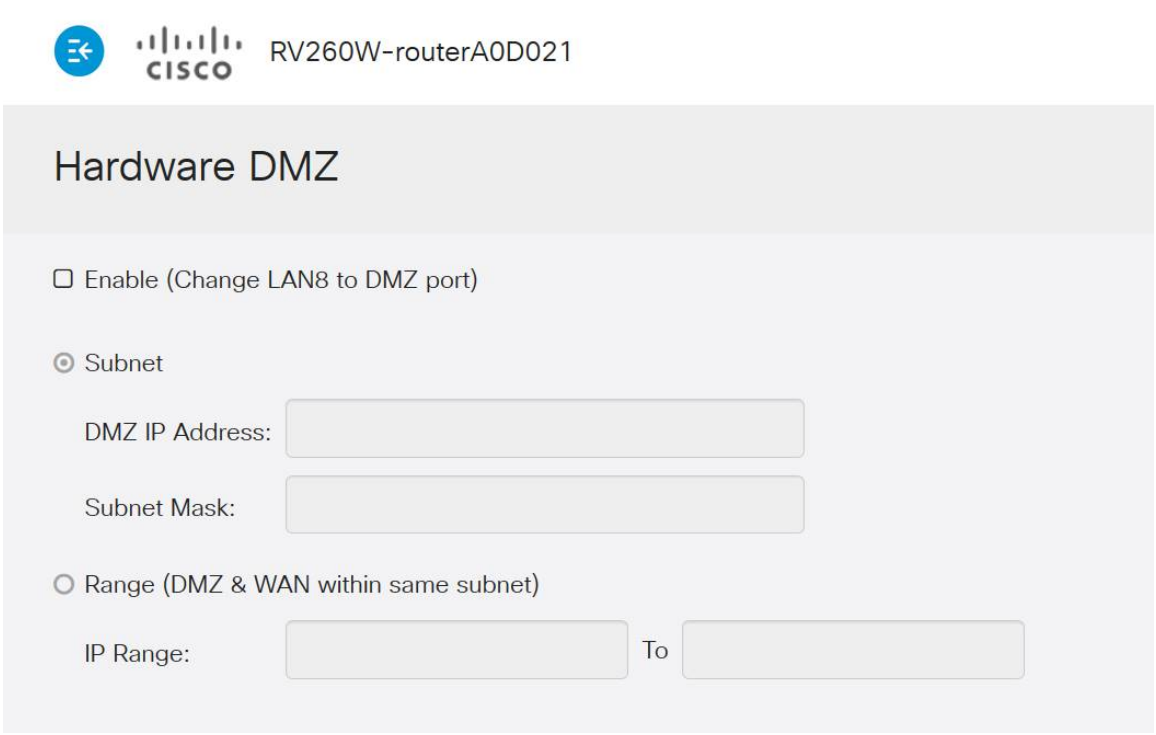
Disponible uniquement pour la gamme RV260X, cette méthode nécessite différentes informations d'adressage IP en fonction de la méthode choisie. Les deux méthodes utilisent en effet des sous-réseaux pour définir la zone, la différence étant la quantité de sous-réseau utilisée pour créer la zone démilitarisée. Dans ce cas, les options sont - *toutes* ou *certaines*. La méthode Subnet (*all*) nécessite l'adresse IP de la DMZ elle-même, ainsi que le masque de sous-réseau. Cette méthode occupe toutes les adresses IP appartenant à ce sous-réseau. Alors que la méthode Range (*certains*) vous permet de définir une plage continue d'adresses IP à trouver dans la zone DMZ.

Note: Dans les deux cas, vous devrez travailler avec votre FAI pour définir le schéma d'adressage IP du sous-réseau.

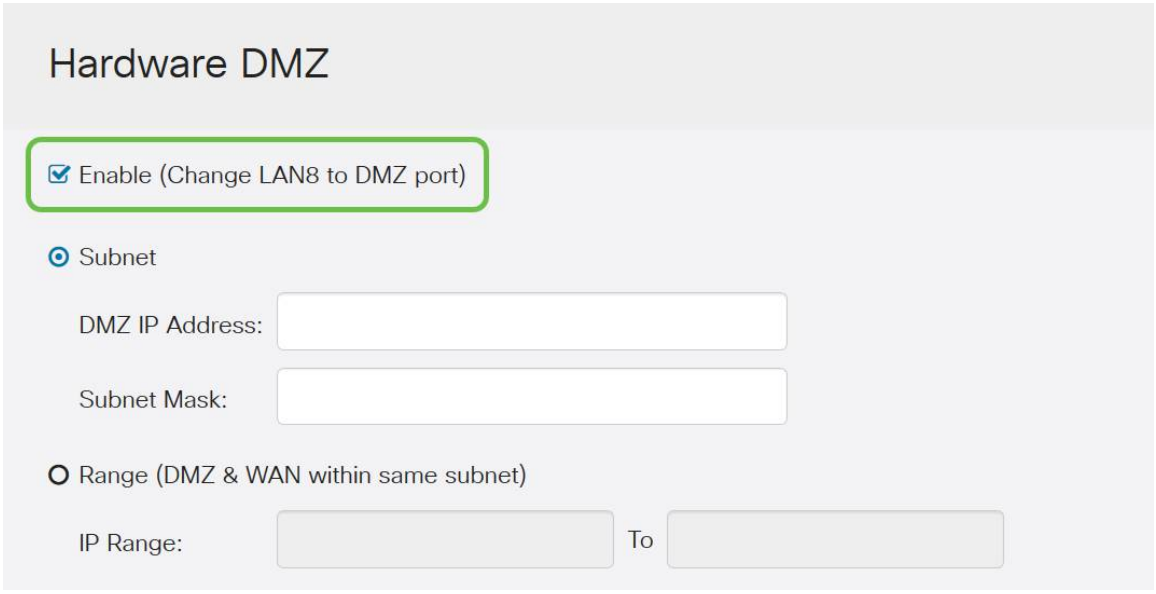
Étape 1. Après vous être connecté à votre périphérique RV260X, cliquez sur **WAN > Hardware DMZ**



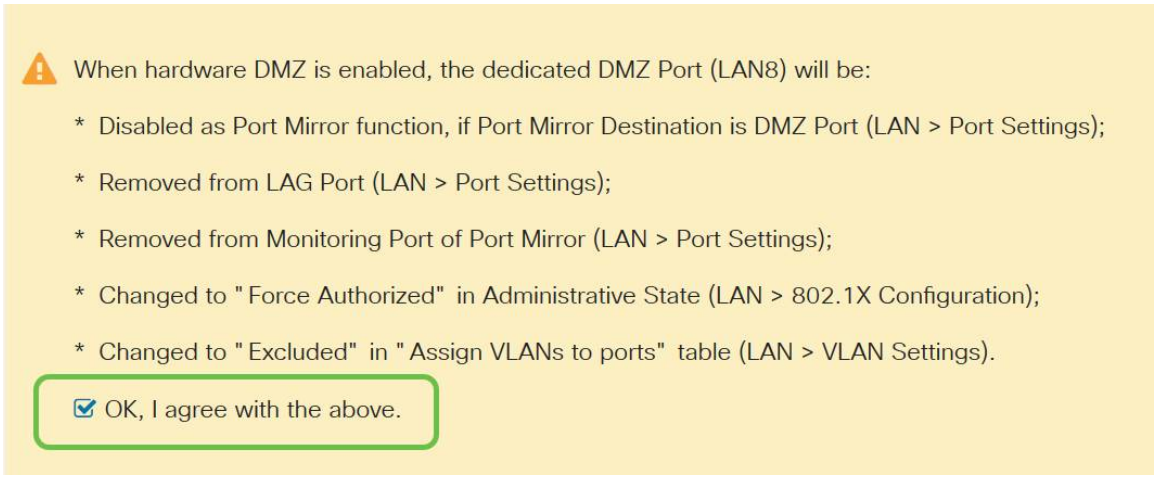
Note: Les captures d'écran proviennent de l'interface utilisateur du RV260X. Vous trouverez ci-dessous la capture d'écran des options DMZ matérielles qui seront affichées sur cette page.



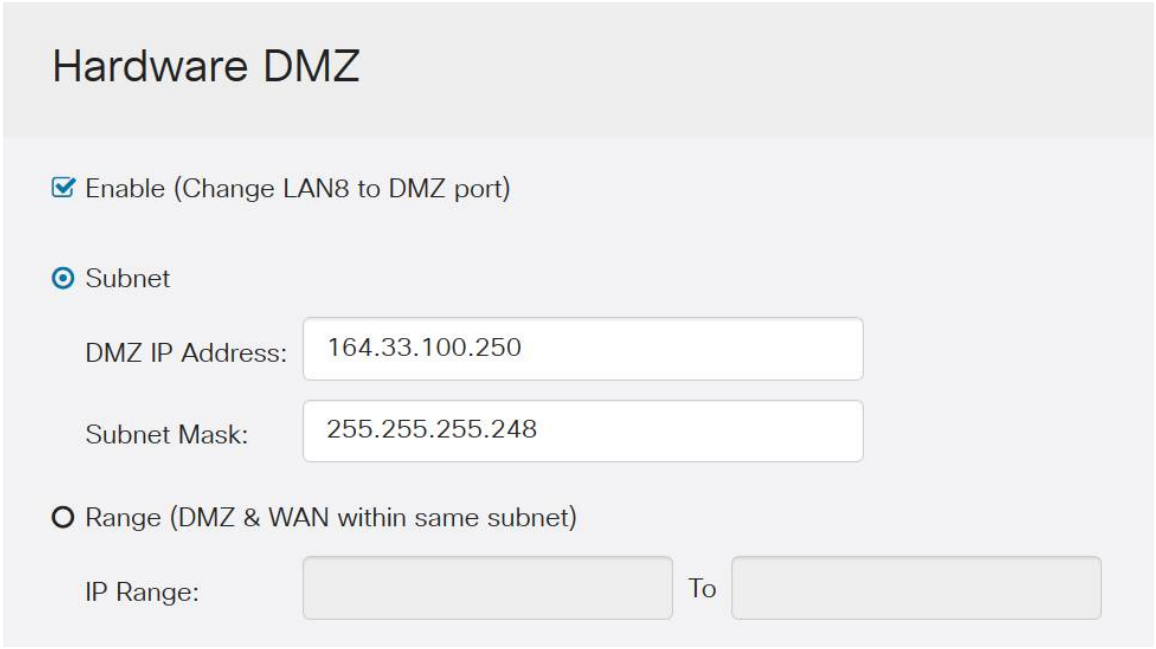
Étape 2. Cochez la case **Enable (Change LAN8 to DMZ port)**. Cela convertira le 8 e port du routeur en une « fenêtre » DMZ uniquement en services nécessitant une sécurité renforcée.



Étape 3. Après avoir cliqué sur *Activer* un message d'information s'affiche sous les options sélectionnables. Vérifiez les détails des points susceptibles d'affecter votre réseau et cliquez sur la case **OK, je suis d'accord avec la** case **ci-dessus.**



Étape 4. L'étape suivante se divise en deux options possibles : Subnet et Range. Dans notre exemple ci-dessous, nous avons sélectionné la méthode **Subnet**.



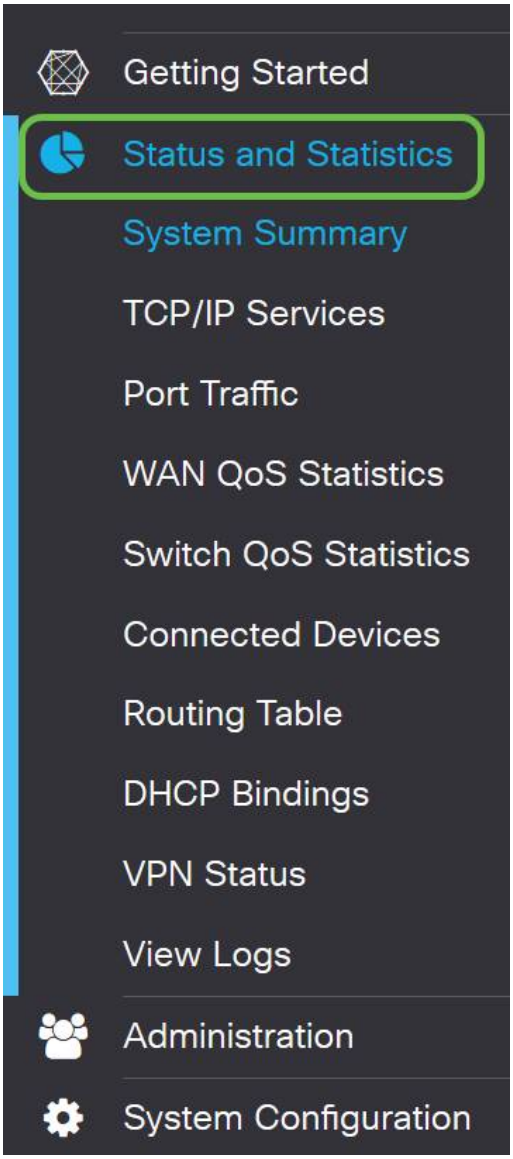
Note: Si vous avez l'intention d'utiliser la méthode Range, vous devez cliquer sur le bouton **Range** radial, puis entrer la plage d'adresses IP attribuée par votre FAI.

Étape 6. Cliquez sur **Apply** (**Appliquer**) (dans le coin supérieur droit) pour accepter les paramètres DMZ.

Confirmation de la configuration correcte de la zone démilitarisée

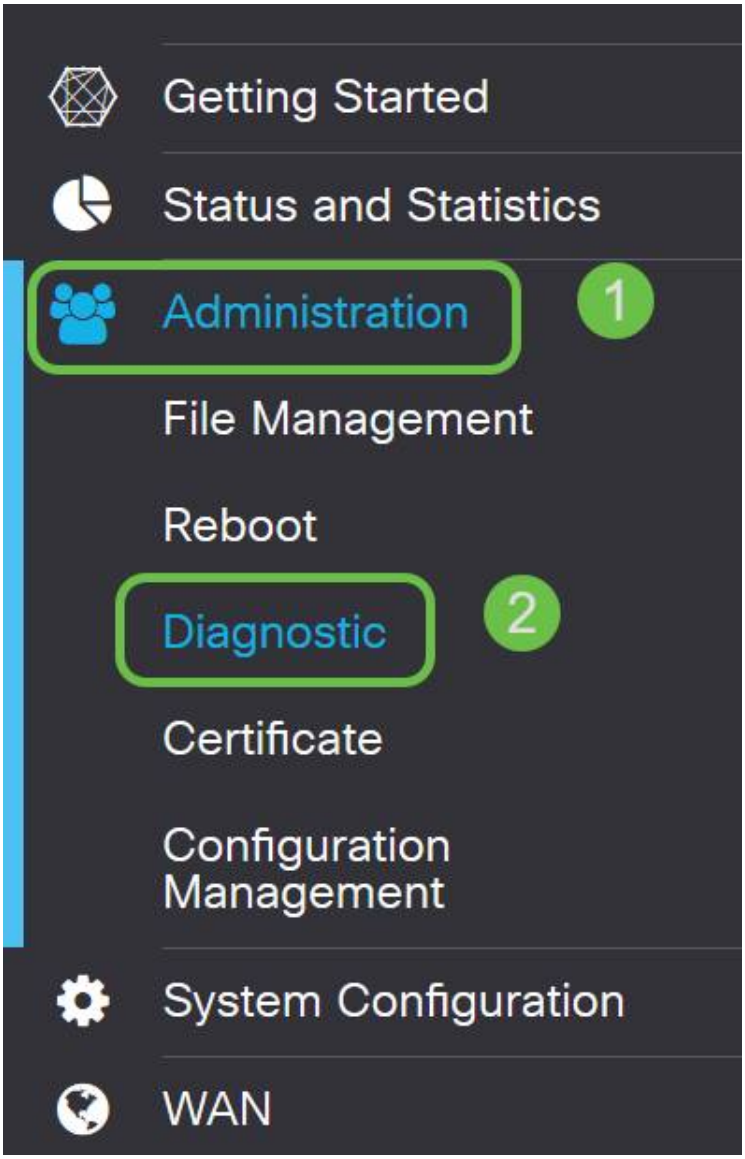
En vérifiant que la DMZ est configurée pour accepter correctement le trafic provenant de sources situées en dehors de sa zone, un test ping sera suffisant. Tout d'abord, nous allons nous arrêter à l'interface d'administration pour vérifier l'état de la DMZ.

Étape 1. Pour vérifier que votre DMZ est configuré, accédez à **Status & Statistics**, la page charge automatiquement la page System Summary**.** Le port 8 ou le port Lan 8 répertorie l'état de la DMZ comme étant "*Connecté*« .



Nous pouvons utiliser la fonctionnalité de requête ping ICMP fiable pour tester si la DMZ fonctionne comme prévu. Le message ICMP ou simplement « ping » tente de frapper à la porte de la DMZ. Si la DMZ répond en disant « Hello », la requête ping est terminée.

Étape 2. Pour accéder à la fonction ping de votre navigateur, cliquez sur **Administration > Diagnostic**.



Étape 3. Entrez l'**adresse IP de la DMZ** et cliquez sur le bouton **Ping**.

Si la requête ping aboutit, un message comme celui ci-dessus s'affiche. Si la requête ping échoue, cela signifie que la DMZ n'est pas accessible. Vérifiez vos paramètres DMZ pour vous assurer qu'ils sont correctement configurés.

Conclusion

Maintenant que vous avez terminé la configuration de la DMZ, vous devez pouvoir commencer à accéder aux services depuis l'extérieur du LAN.