Dépannage sur les routeurs RV160 et RV260

Objectif

D’innombrables problèmes peuvent survenir sur un réseau et entraîner des problèmes de connectivité. Ce document traite de certains aspects à analyser lors du dépannage de la connectivité sur un routeur RV160 ou RV260.

Périphériques pertinents

- RV160
- RV260

Version du logiciel

- 1.0.00.13

Table des matières

Vérifier les problèmes physiques ou environnementaux

Exécuter des tests de connectivité à partir de l'utilitaire Web

Explorer l'état et les statistiques

Explorer les paramètres du pare-feu

Vérifier le WAN par défaut

Modifier l'adresse IP de votre réseau local

Changements d'adresse IP après changement de sous-réseau

Idées de dépannage

Vérifier les problèmes physiques ou environnementaux

Il s'agit de la méthode de dépannage la plus simple, mais elle est souvent négligée. Même si cela peut sembler évident, il est bon de commencer par les bases.

- Tout est-il alimenté ?
- Tout est-il allumé ?
- Les câbles sont-ils correctement connectés ?
- Avez-vous un voyant de liaison allumé de façon constante ?
- Est-ce que c'est un mauvais câble ?
- Le routeur est-il surchauffé ?
- Peut-il y avoir des facteurs environnementaux tels que l'endroit où il se trouve ?
- S'il s'agit d'un routeur sans fil, y a-t-il des interférences, par exemple un micro-ondes, du métal ou des murs épais entre le routeur et l'ordinateur ?

Exécuter des tests de connectivité à partir de l'utilitaire Web

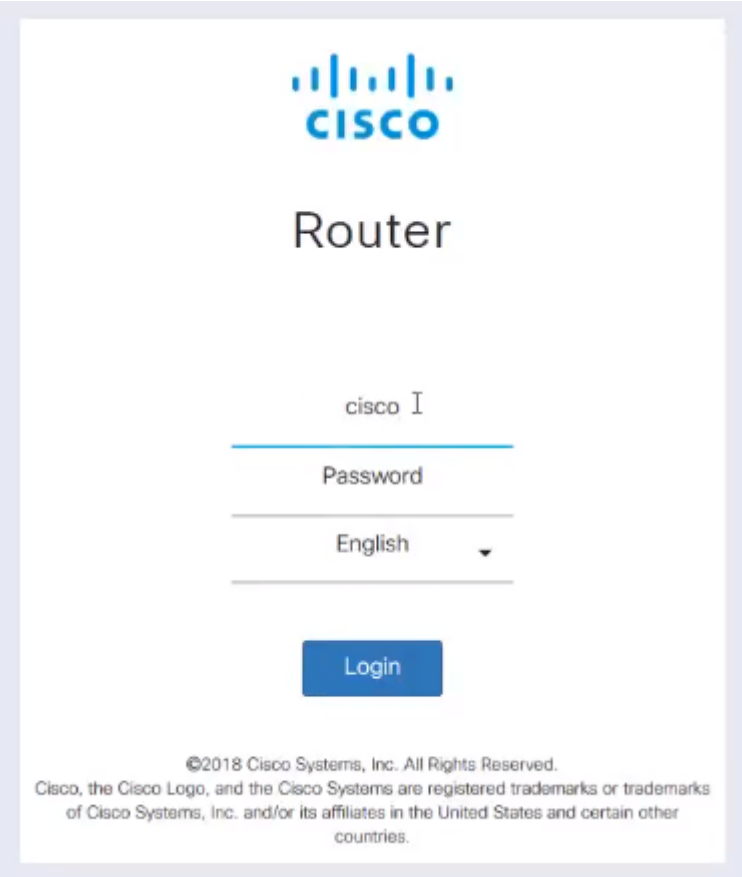
Le routeur doit être capable de communiquer avec d'autres périphériques du réseau et à l'extérieur via Internet pour pouvoir mener à bien ses activités. Il existe plusieurs façons de vérifier la connectivité.

Vous pouvez d'abord vérifier les paramètres d'adresse IP sur l'ordinateur connecté au port LAN (réseau local) du routeur. Par défaut, la fonctionnalité DHCP est activée sur le routeur. Vous pouvez donc conserver les paramètres de votre carte réseau sur votre ordinateur en tant que « Obtenir l'adresse IP automatiquement ». Cela permet à votre ordinateur d'obtenir une adresse IP du routeur. Vérifiez l'accessibilité au réseau local du routeur à l'aide de la commande ping.

Connectez-vous directement à votre routeur et utilisez l'interface utilisateur graphique (GUI). Dans votre navigateur Web, saisissez l'adresse IP du routeur. Saisissez les informations d'identification. Si vous avez réinitialisé les paramètres d'usine ou si vous saisissez pour la première fois des informations d'identification, l'adresse IP par défaut est 192.168.1.1 et les informations d'identification sont cisco pour le nom d'utilisateur et le mot de passe.

Remarque : Si vous avez oublié l'adresse IP du routeur et que vous n'avez pas de configuration spécifique à conserver, vous pouvez rétablir les paramètres d'usine par défaut sur le périphérique physique. Ouvrez un trombone et insérez son extrémité dans le petit bouton de réinitialisation en retrait. Attendez 10 secondes et vous verrez que les voyants du périphérique s'allument. Le redémarrage du système prend au moins quelques minutes. Votre adresse IP reviendra à

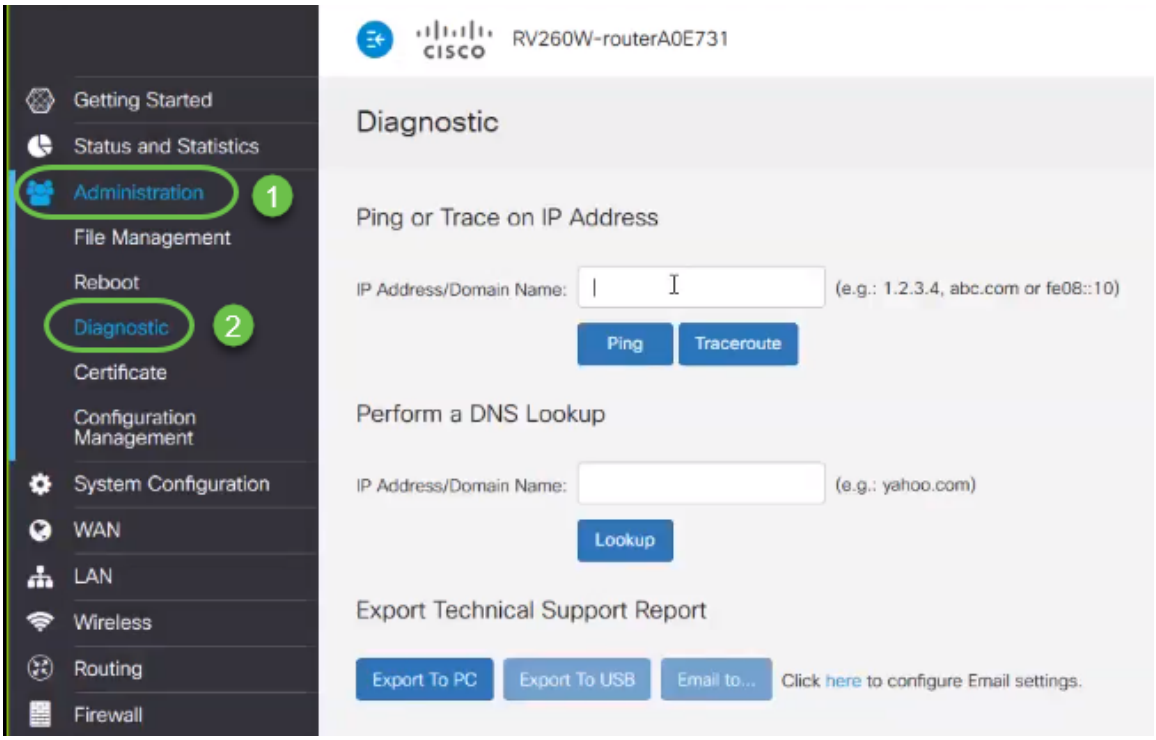
192.168.1.1.



Pour accéder au volet de navigation, cliquez sur l'icône représentant un cercle bleu, comme indiqué ci-dessous.



Dans le volet de navigation, sélectionnez Administration > Diagnostic. À partir de là, vous pouvez effectuer une requête ping, traceroute vers une adresse IP ou effectuer une recherche DNS.



Pour effectuer une requête ping à l'aide de l'interface graphique utilisateur, tapez l'adresse IP qui doit avoir la capacité de communiquer avec votre routeur et cliquez sur Ping. Vous pouvez entrer l'adresse IP d'un autre périphérique connecté de votre réseau ou sélectionner un périphérique fiable que vous connaissez en dehors de votre réseau.

Si votre routeur est capable de communiquer avec l'adresse IP, les paquets sont renvoyés avec des statistiques. L'image ci-dessous montre une requête ping réussie. Par conséquent, la connectivité réseau n'est pas le problème dans ce cas.

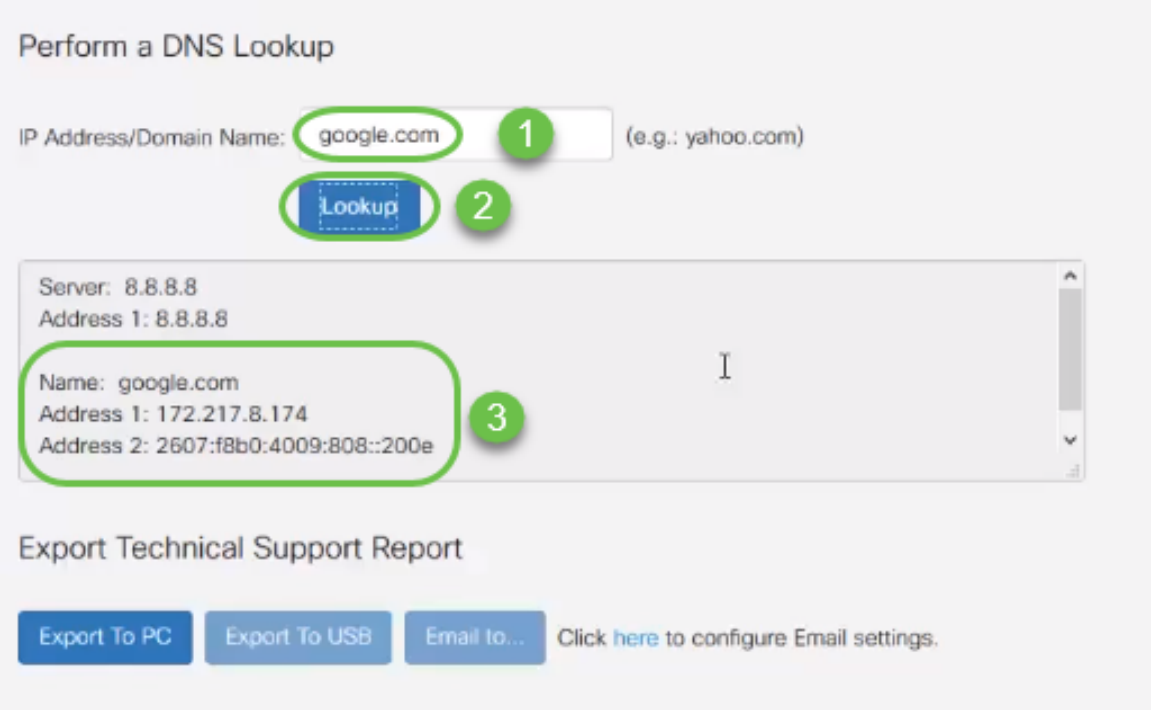


Pour effectuer un suivi sur une adresse IP, cliquez sur Traceroute. Dans le résultat de votre commande traceroute, vous verrez des « sauts » d'un routeur à l'autre. Le « saut » 1 commence par votre routeur local, puis par votre routeur de fournisseur d'accès Internet (FAI). Il « saute » ensuite vers le routeur situé à la périphérie du réseau du FAI, puis à travers d'autres routeurs pour

atteindre la destination. Si les deux ou trois premiers « sauts » sont réussis, le problème se situe en dehors de votre réseau. Essayez une autre adresse IP ou un autre nom de domaine pour recevoir un traceroute réussi.

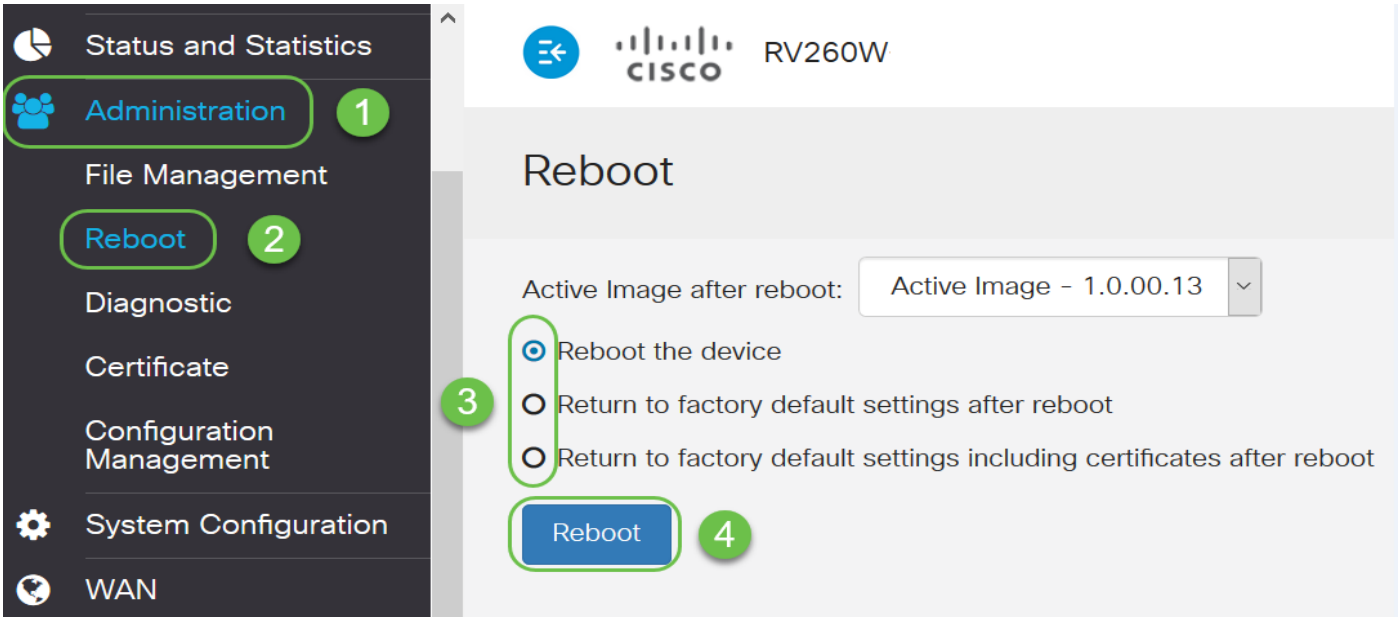


Pour effectuer une recherche DNS (Domain Name Service), vous devez taper une adresse IP ou un nom de domaine et cliquer sur Lookup. Si le serveur DNS renvoie des détails sur l'adresse IP ou le nom de domaine, votre serveur est configuré et connecté.



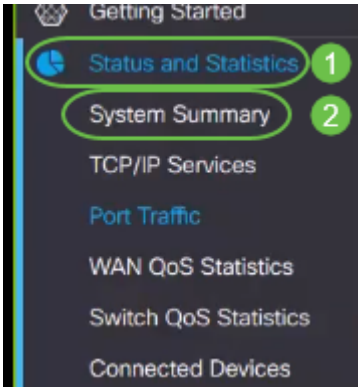
Une autre option est de Redémarrer ou d'effectuer un Retour aux paramètres d'usine par défaut après le redémarrage. Gardez à l'esprit que si vous choisissez Retour aux paramètres d'usine par défaut, toutes les configurations seront perdues. Cela peut parfois résoudre le problème si quelque chose a été modifié par rapport aux paramètres par défaut et a provoqué le problème. Si

vous choisissez Retour aux paramètres d'usine par défaut, y compris les certificats après le redémarrage, vous devrez recharger les certificats.

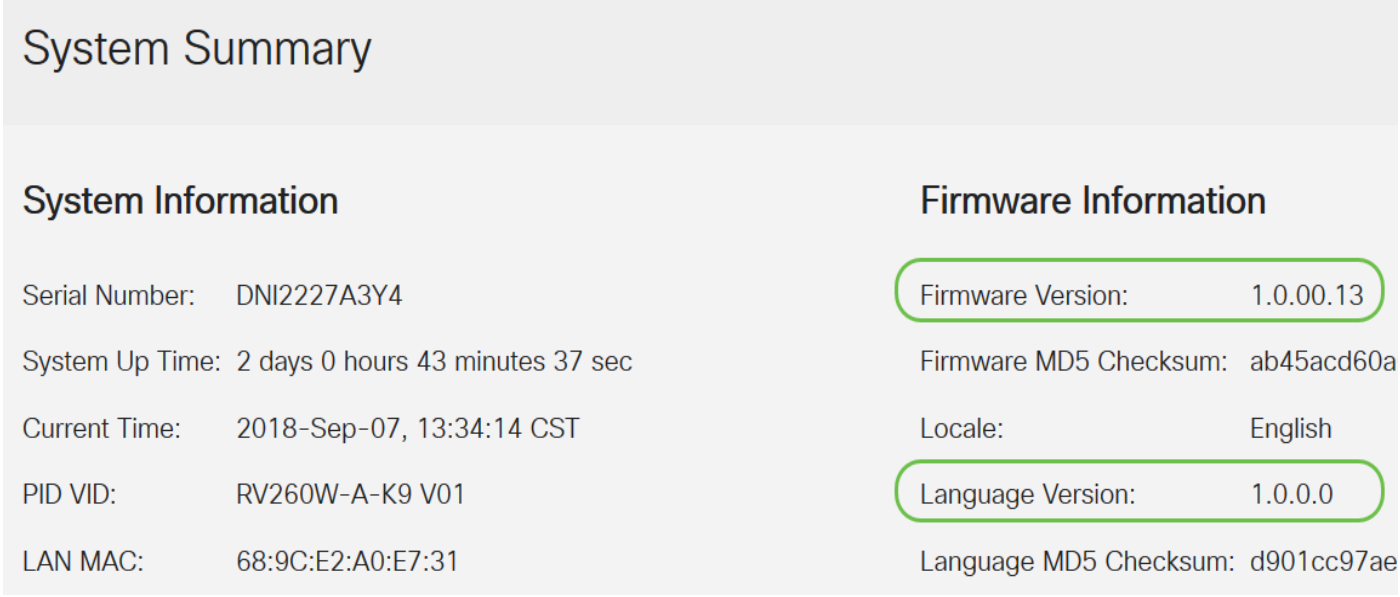


Explorer l'état et les statistiques

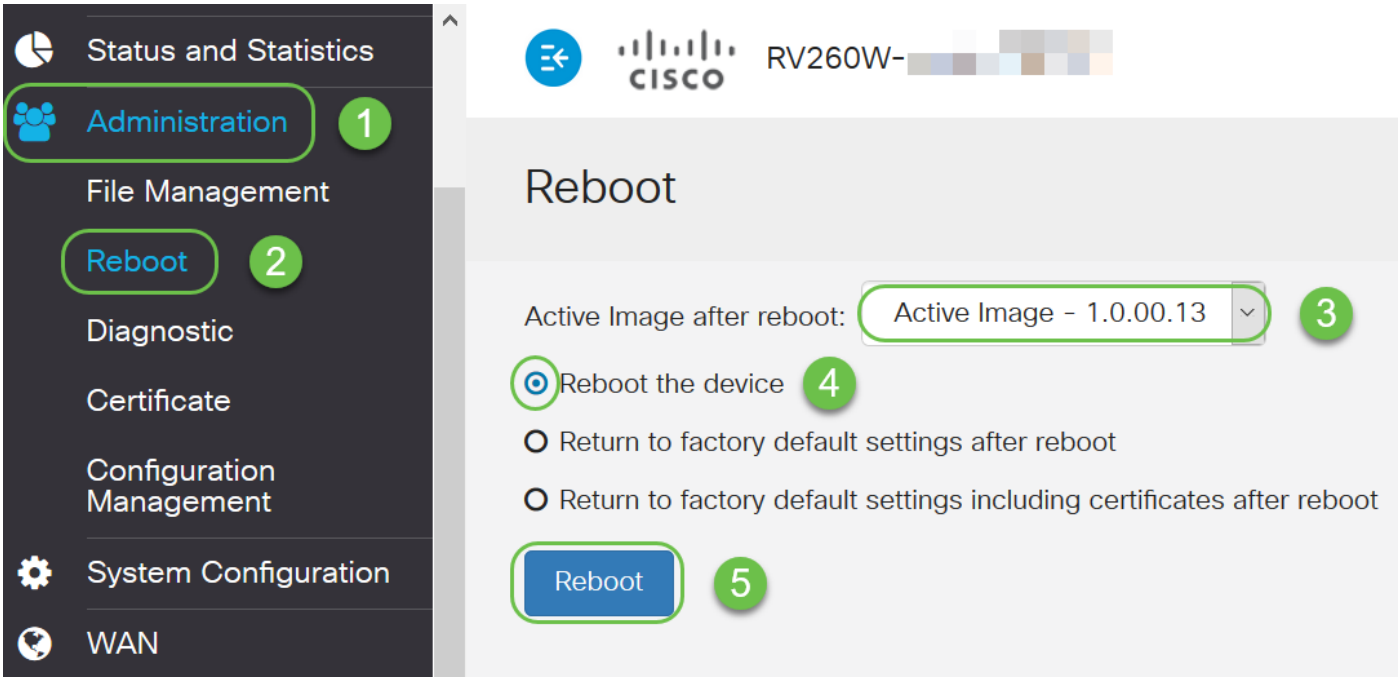
Explorez chacune des autres options État et Statistiques du volet de navigation en commençant par Résumé système.



System Summary affiche votre numéro de série, la durée de fonctionnement de votre routeur, l'heure actuelle, l'état du port, l'état VPN et l'état du pare-feu. Il répertorie également la version actuelle du micrologiciel et de la langue. Si l'une de ces versions n'est pas la plus récente, vous devez aller à Support Cisco et mettre à niveau le micrologiciel ou la version de langue. Cela pourrait potentiellement résoudre votre problème puisque les mises à jour contiennent souvent des correctifs de bogues. Si vous souhaitez être guidé tout au long du processus de mise à niveau du micrologiciel, cliquez ici.

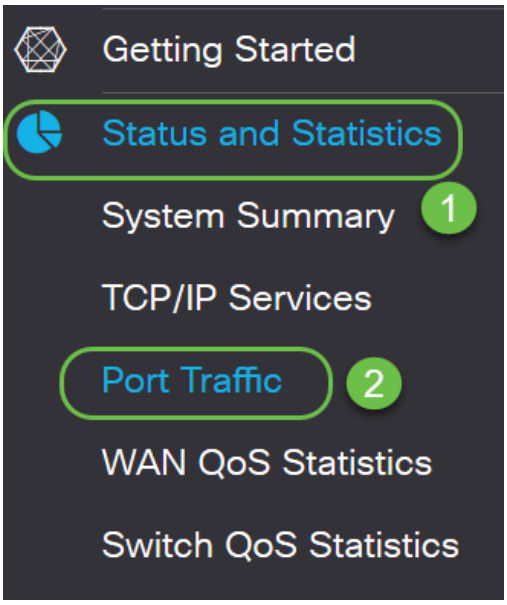


Une fois l'image du micrologiciel mise à niveau, vous devez l'activer et la redémarrer, ce qui entraîne l'inactivité de l'ancienne image du micrologiciel.



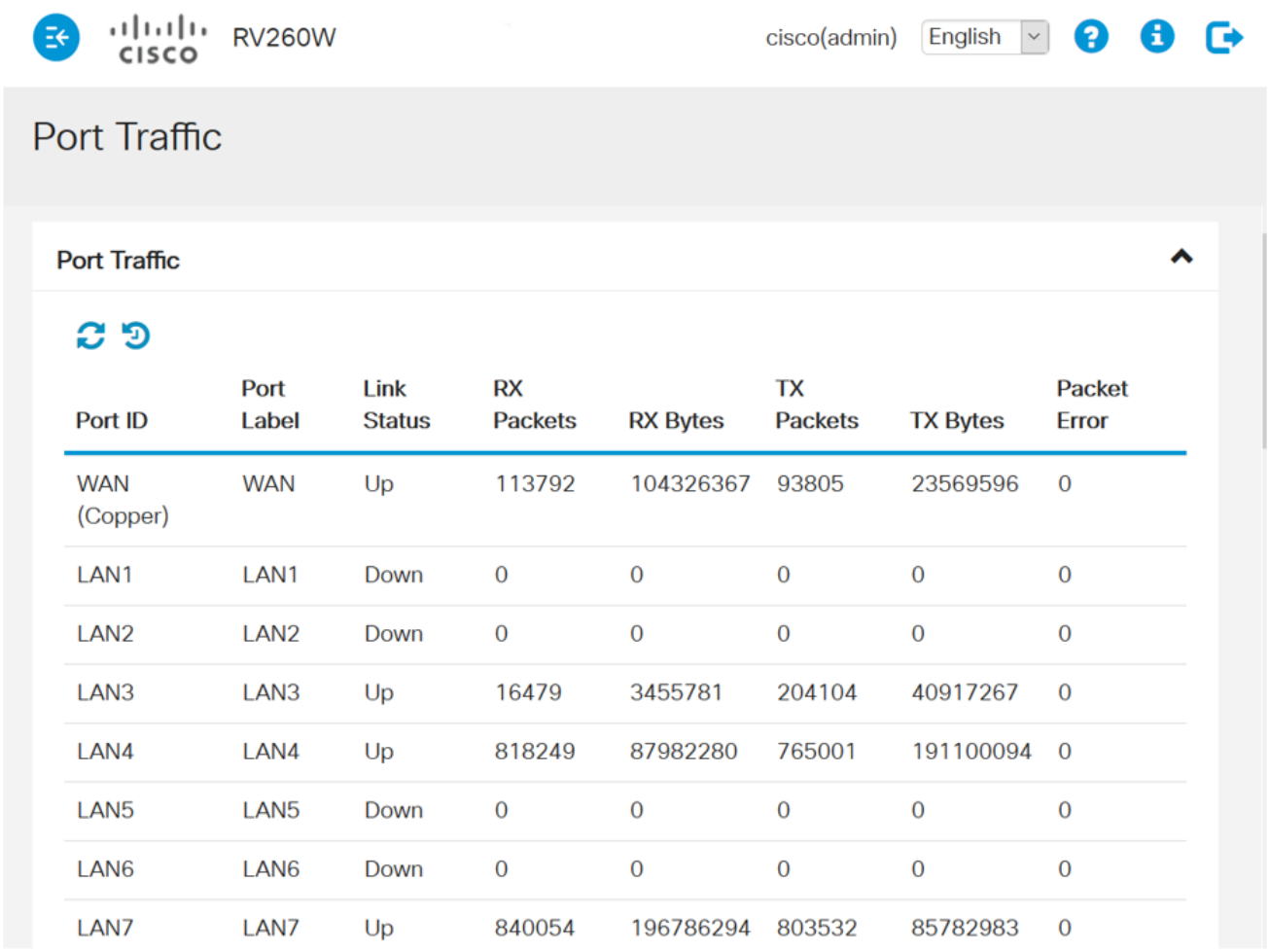
Revenez à System Summary pour vous assurer que le micrologiciel et la langue ont été mis à niveau.

Consultez la section Status and Statistics> Port Traffic pour les problèmes.



La page Port Traffic comprend :

- ID de port - ID de port
- Étiquette de port - étiquette de port
- Link Status : état de la connexion sur chaque port, s'il est actif ou inactif
- Paquets RX - nombre total de paquets reçus via l'interface
- RX Bytes - total des octets reçus
- Paquets TX - nombre total de paquets transmis
- TX Bytes - nombre total d'octets transmis
- Erreur de paquet - erreurs survenues lors de l'envoi ou de la réception de paquets



Port ID	Port Label	Link Status	RX Packets	RX Bytes	TX Packets	TX Bytes	Packet Error
WAN (Copper)	WAN	Up	113792	104326367	93805	23569596	0
LAN1	LAN1	Down	0	0	0	0	0
LAN2	LAN2	Down	0	0	0	0	0
LAN3	LAN3	Up	16479	3455781	204104	40917267	0
LAN4	LAN4	Up	818249	87982280	765001	191100094	0
LAN5	LAN5	Down	0	0	0	0	0
LAN6	LAN6	Down	0	0	0	0	0
LAN7	LAN7	Up	840054	196786294	803532	85782983	0

Cette section de la page Port Traffic, Port Status, comprend :

- État de la liaison - le port est connecté ou non connecté
- Activité des ports - activée ou non
- Speed Status : type de vitesse utilisé par le port
- État du mode bidirectionnel - défini sur Full ou Half. Vous devrez peut-être ajuster ce paramètre si vous utilisez un matériel plus ancien qui ne peut utiliser que le mode bidirectionnel non simultané. Vous devrez peut-être modifier les paramètres pour qu'ils correspondent.
- Négociation automatique : deux périphériques connectés choisissent des paramètres de transmission communs, notamment la vitesse et le contrôle de flux. Il est recommandé d'activer cette option.

Port Status

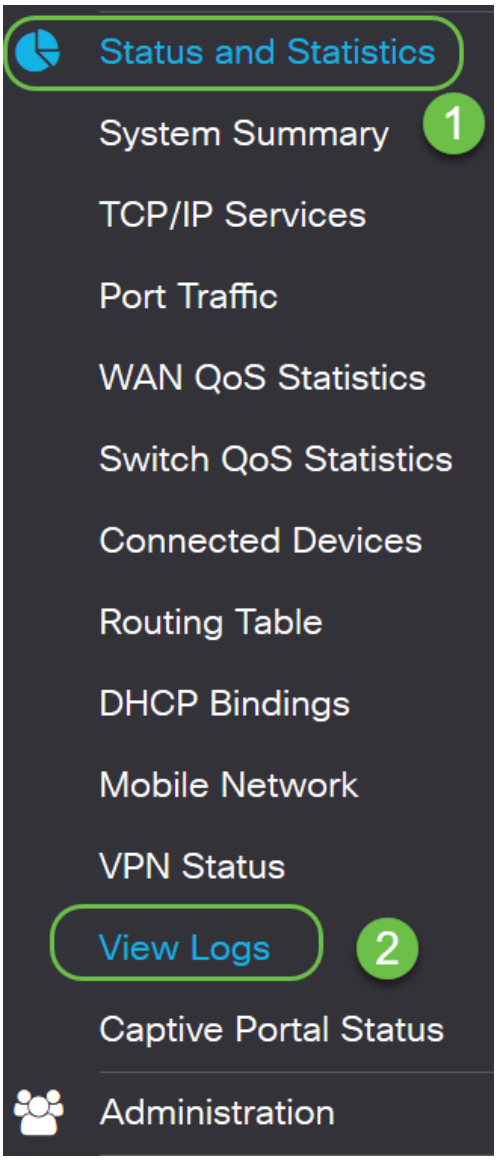
Port ID	Link Status	Port Activity	Speed Status	Duplex Status	Auto Negotiation
WAN (Copper)	Connected	Enabled	100Mbps	Full	Enabled
LAN1	NotConnected	Enabled	N/A	Half	Enabled
LAN2	NotConnected	Enabled	N/A	Half	Enabled
LAN3	Connected	Enabled	100Mbps	Full	Enabled
LAN4	Connected	Enabled	1000Mbps	Full	Enabled
LAN5	NotConnected	Enabled	N/A	Half	Enabled
LAN6	NotConnected	Enabled	N/A	Half	Enabled
LAN7	Connected	Enabled	1000Mbps	Full	Enabled

Si vous utilisez un routeur sans fil, le trafic sans fil fera partie de votre page Port Traffic.

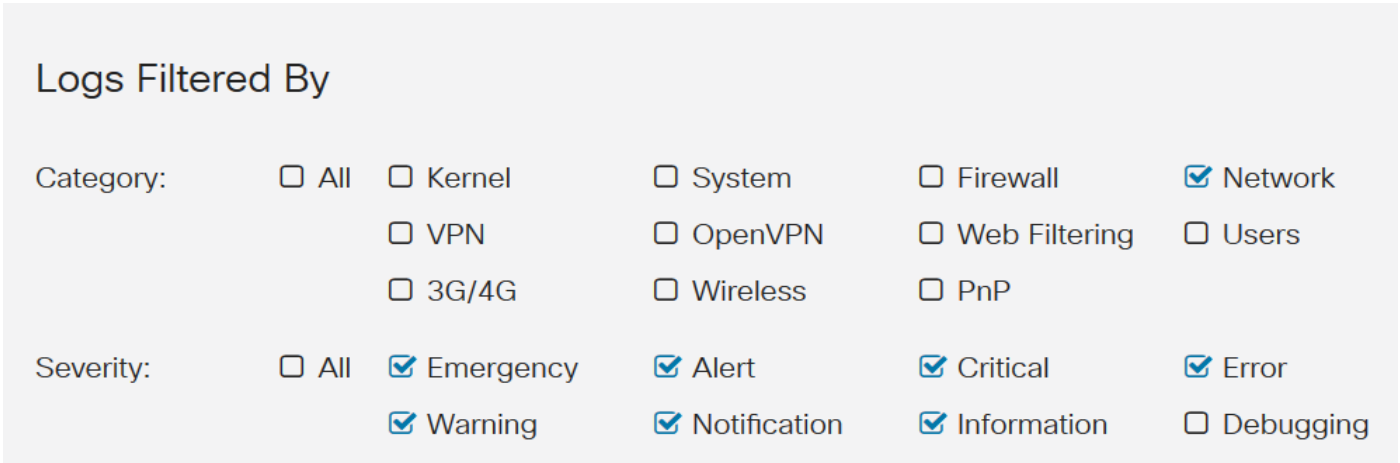
Wireless Traffic

SSID Name	Radio Name	Status	Number of Associated Clients	RX Packets	RX Bytes	TX Packets	TX Bytes	Multicast Packets	Packet Error
RV260W	2.4G	Active	0	0	0	0	0	0	0
RV260-Test	2.4G	Active	1	81439	19610397	87467	21585424	1973	1
RV260W	5G	Active	0	10999	2089434	375848	59451104	181236	5
RV260-Test	5G	Active	0	0	0	3844	841880	1922	6

Consultez Status and Statistics > View Logs pour rechercher les erreurs et les connexions manquantes.



Il existe plusieurs options de ce qu'il faut examiner dans Afficher les journaux. Les journaux étant souvent créés, il peut être difficile de trier les informations dont vous avez besoin sans utiliser la fonction de filtrage.

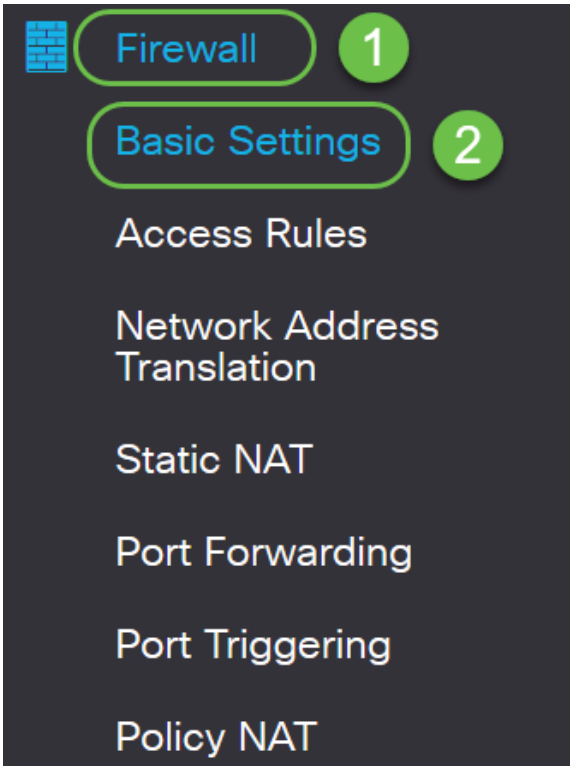


Voici quelques exemples de journaux :

2018-Sep-12, 11:14:10 ALMT	info	network	dnsmasq-dhcp: DHCPACK(br-vlan1) 172.16.1.125 e4:b3:1 :96:0c:b2 ARI
2018-Sep-12, 11:14:10 ALMT	warning	network	dnsmasq-dhcp: Ignoring domain cisco.com for DHCP host name ARI
2018-Sep-12, 16:55:18 ALMT	warning	pnp	PnP: [9713]: pnp.infra.Profile.1 WARNING Config file does not contain 'modified' optionin section 'Profile 1'
2018-Sep-12, 16:56:11 ALMT	error	pnp	PnP: [9713]: pnp.infra.Profile.1 ERROR Failed to send Work-Info request

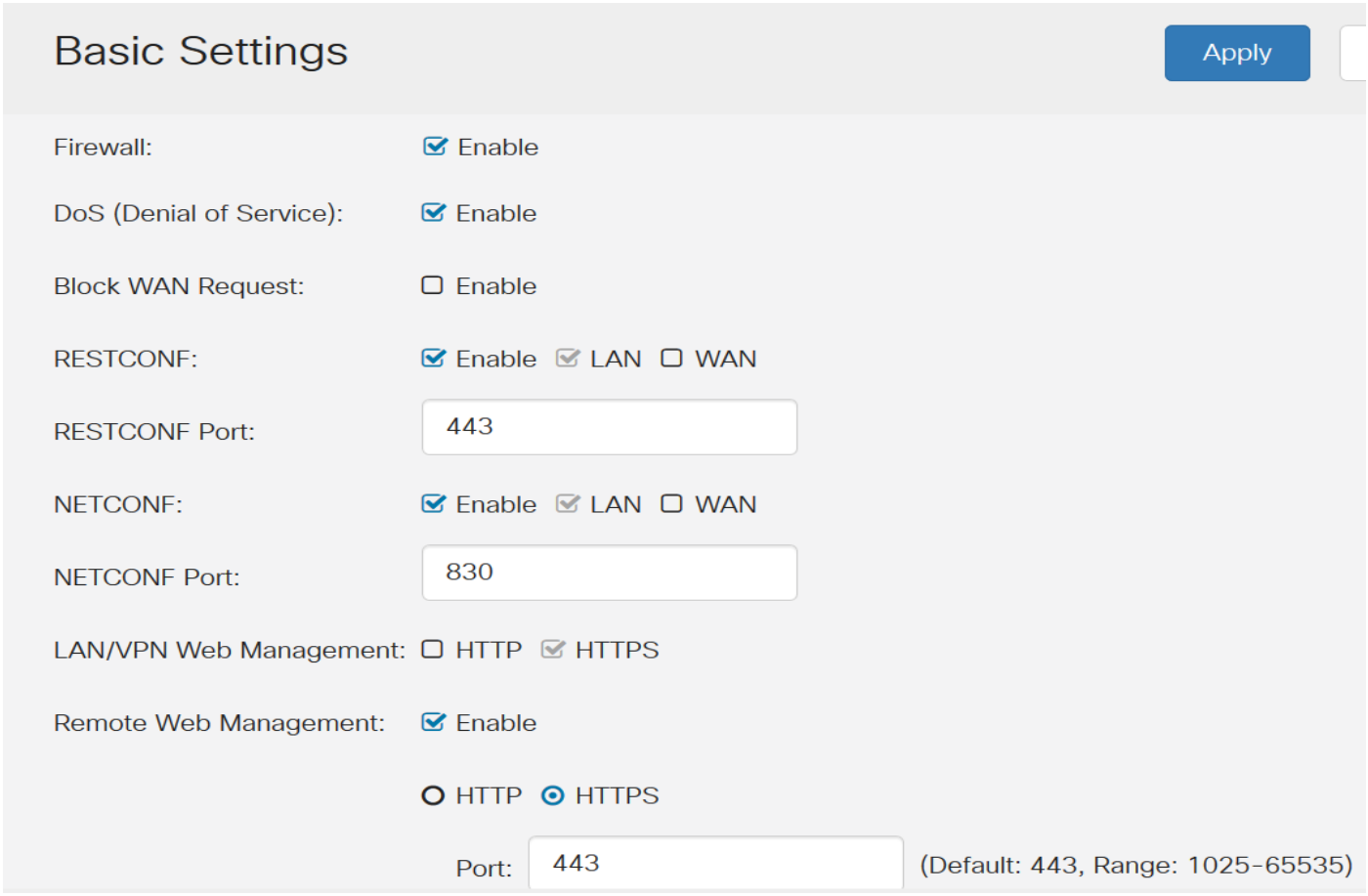
Explorer les paramètres du pare-feu

Explorez Firewall > Basic Settings pour voir si vous avez bloqué tout ce qui pourrait être à l'origine du problème.

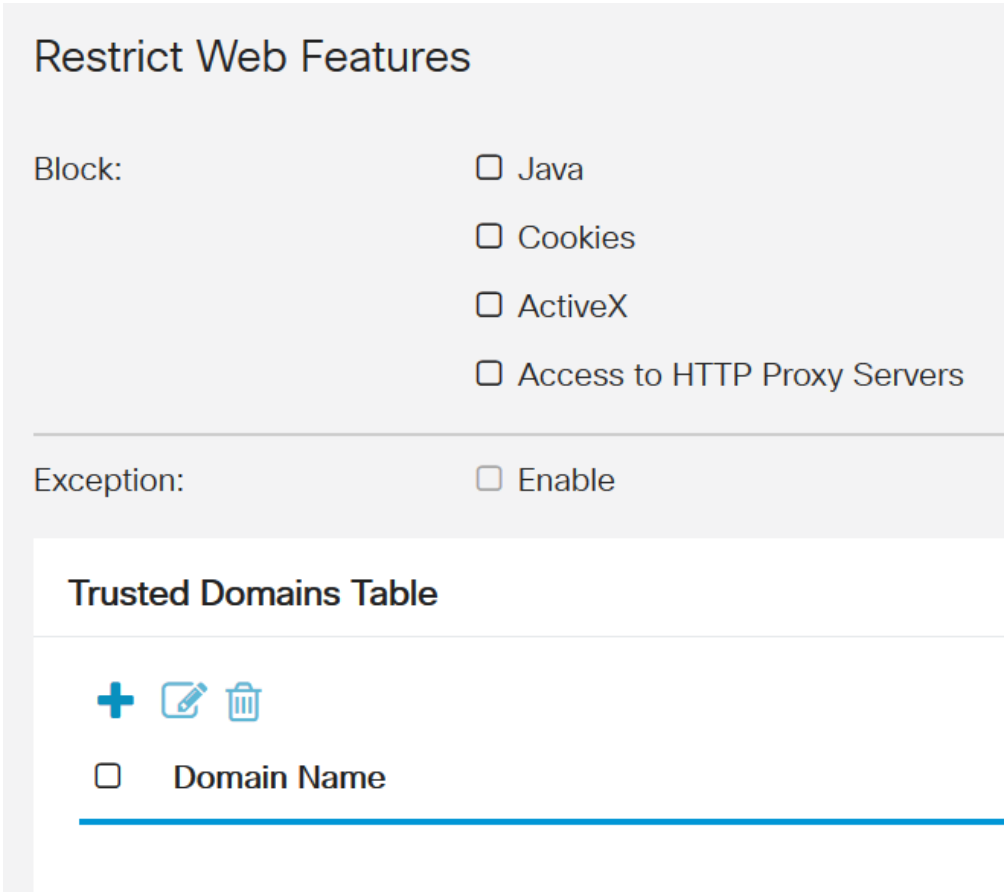


Voici une configuration standard pour les paramètres de base. Si vous ne pouvez pas envoyer de requête ping au réseau étendu (WAN) du routeur, c'est là que vous pouvez vérifier si l'option Block WAN Request est activée. Si vous ne pouvez pas accéder à distance à votre page de configuration Web, le problème est peut-être que vous n'avez pas activé la Gestion Web à

distance.



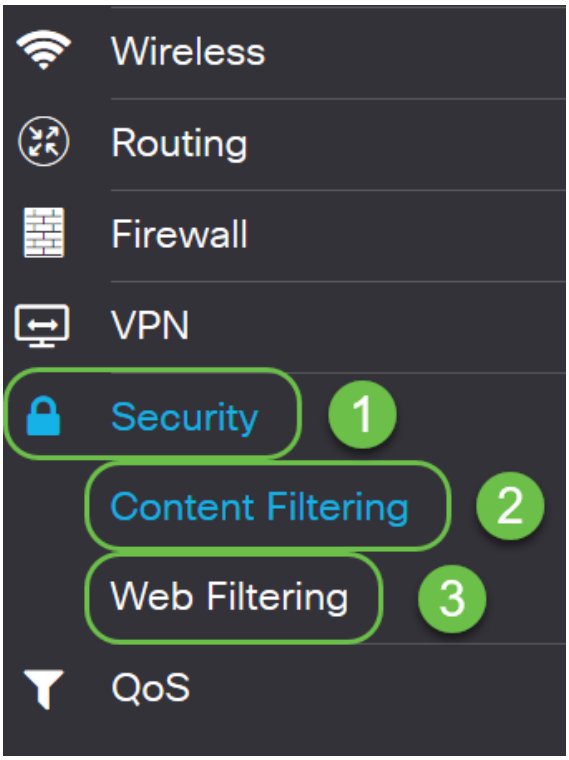
Il est possible qu'un ou plusieurs de ces éléments soient activés, ce qui est à l'origine du problème.



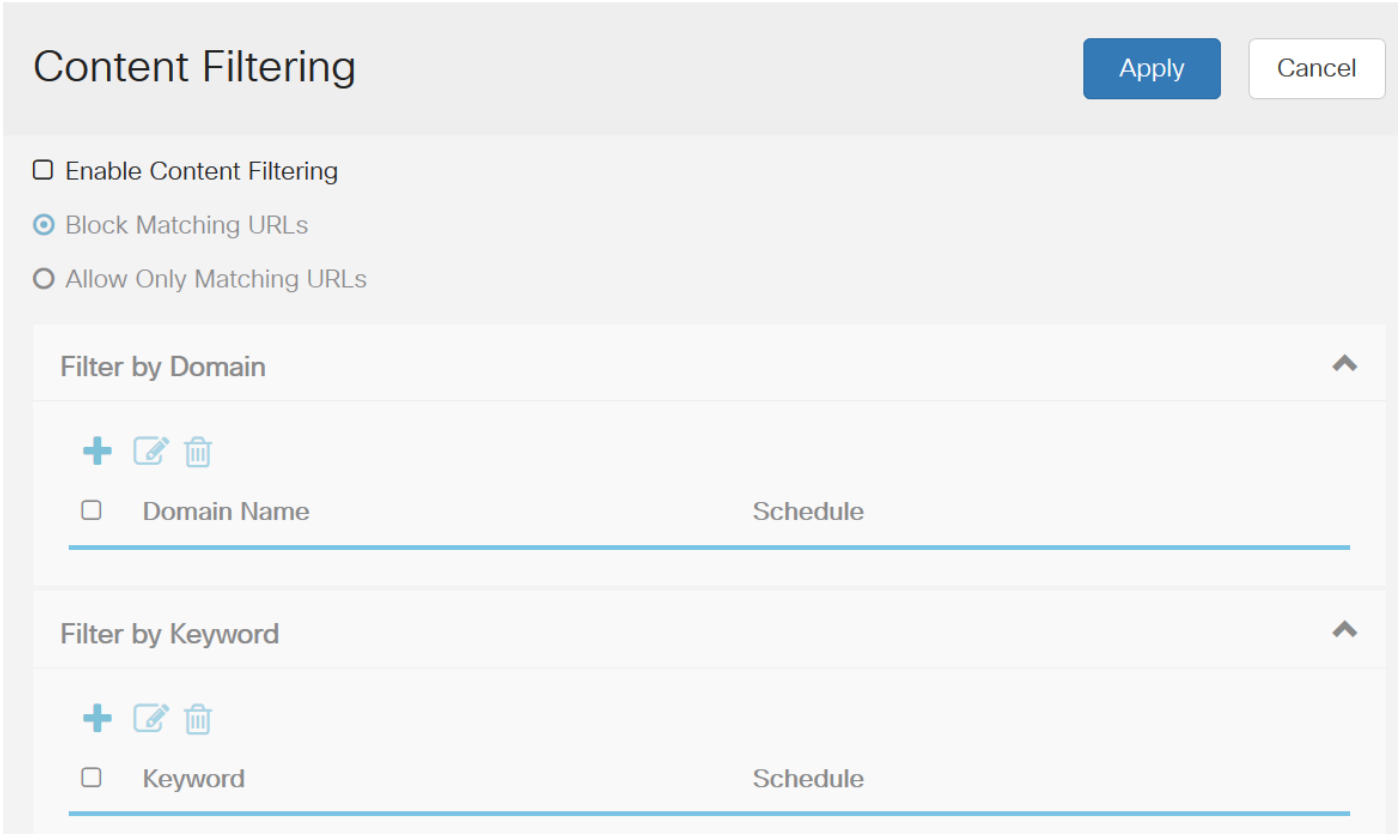
Explorer les paramètres de sécurité

Vérifiez les paramètres de sécurité pour le filtrage de contenu et le filtrage Web. Il est possible que vous ayez configuré un élément qui empêche l'accès au réseau.

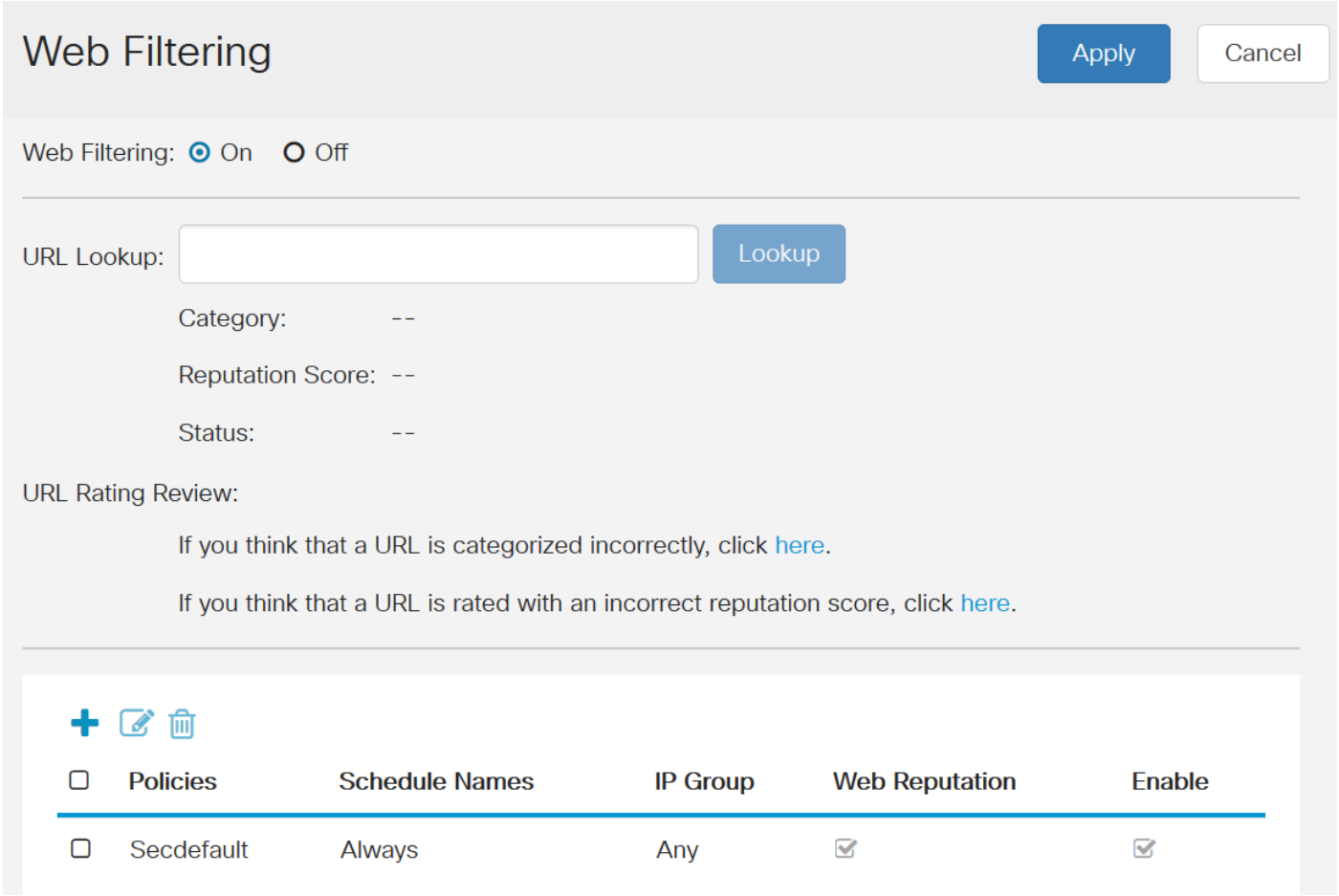
- Le filtrage du contenu vous permet de restreindre l'accès à certains sites Web indésirables en fonction des noms de domaine et des mots clés.
- Le filtrage Web vous permet de gérer l'accès à des sites Web inappropriés. Il peut filtrer la demande d'accès Web d'un client pour déterminer s'il doit autoriser ou refuser ce site Web.



Le filtrage du contenu peut être vérifié pour voir si quelque chose empêche l'accès au réseau. Si vous avez reçu un message indiquant que vous avez été bloqué à partir d'une page spécifique ou si des employés signalent qu'un site spécifique est bloqué, c'est à cet emplacement qu'il faut le vérifier.



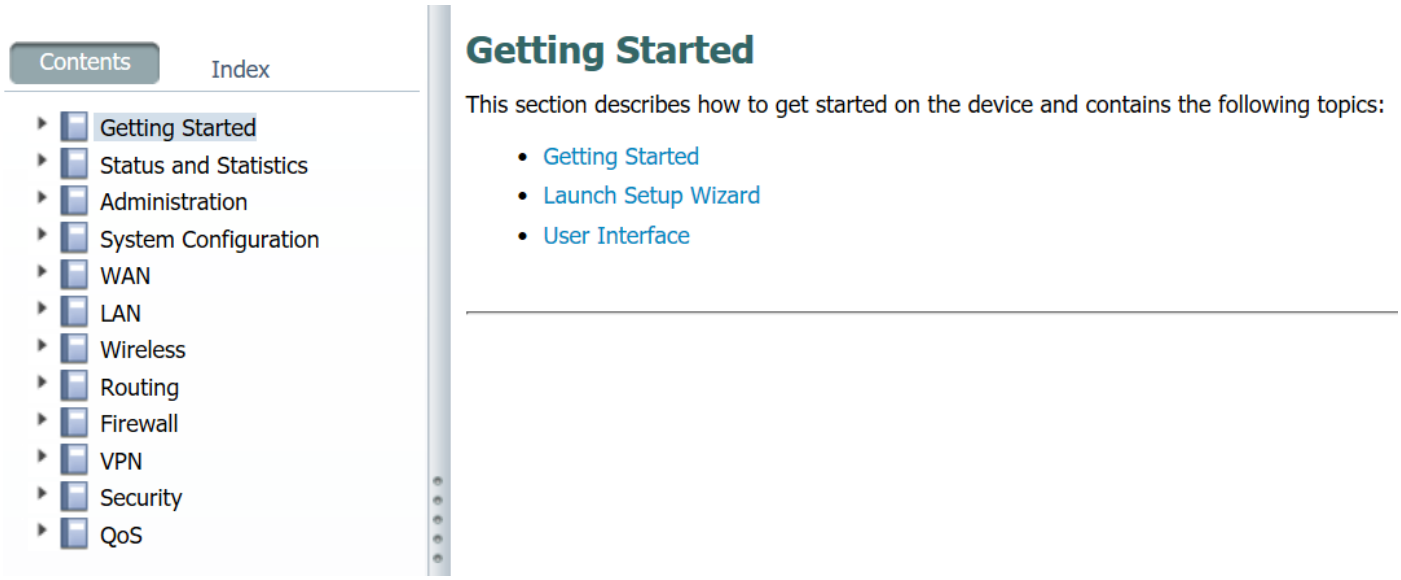
Le filtrage Web est un autre endroit où vous pouvez voir si cela peut être le problème.



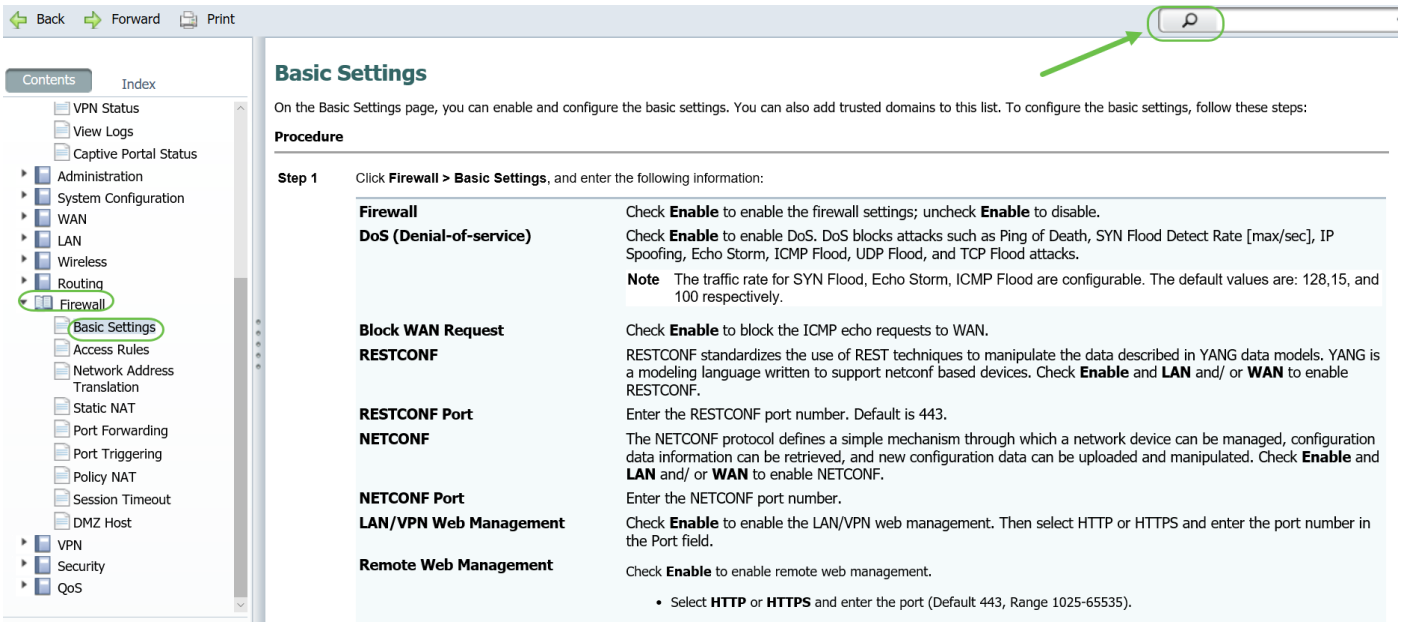
Si vous souhaitez plus de détails sur les options du volet de navigation, cliquez sur le point d'interrogation en haut à droite de votre écran GUI.



Une fois que vous avez sélectionné le point d'interrogation, un nouvel écran s'ouvre et une section extensible apparaît dans le même ordre que le volet de navigation.



Une fois que vous avez cliqué sur l'une des sections, une liste de rubriques s'affiche en dessous. Sélectionnez la zone sur laquelle vous voulez plus d'informations et elle s'ouvrira. Dans cet exemple, Firewall > Basic Settings a été sélectionné. Il y a aussi une fonction de recherche en haut à droite de l'écran si vous ne savez pas où chercher une certaine question.



Vérifiez l'adresse WAN par défaut sur le modem ou la clé

Certains modems et dongles sont fournis avec l'adresse WAN par défaut 192.168.1.1. Les adresses IP commençant par 192.168.x.x sont réservées aux adresses IP privées et ne peuvent pas être de véritables adresses WAN. Ces modems et dongles traduisent l'adresse IP en adresse WAN avant de passer sur Internet, mais 192.168.1.1 est toujours affiché comme adresse IP WAN dans ces réseaux. Cela entraîne des problèmes, car l'adresse IP par défaut du réseau local (LAN) sur les routeurs RV160 et RV260 est également 192.168.1.1.

Si deux périphériques sur un réseau ont la même adresse IP, ils ne peuvent pas communiquer. Si vous rencontrez des problèmes de connectivité, il peut s'agir du problème. Vous avez peut-être même reçu une notification de conflit d'adresse IP. Vous ne pouvez pas modifier l'adresse IP dans le modem ou le dongle. La solution consiste donc à définir l'adresse IP du réseau local sur un sous-réseau différent. Cela devrait résoudre le problème de connectivité.

Pour créer un sous-réseau, le troisième octet, ou le troisième ensemble de nombres dans l'adresse IP, doit être différent d'un 1. Il peut s'agir de n'importe quel nombre compris entre 2 et 254. Par conséquent, VLAN 1 peut être défini sur 192.168.2.x, avec une plage de pool d'adresses IP comprise entre 192.168.2.1 et 192.168.2.254. Dans cet exemple, nous allons modifier l'adresse LAN en 192.168.2.1.

Remarque : Si vous utilisez un ordinateur Mac, vous devez sélectionner l'icône d'engrenage gris pour accéder aux paramètres.

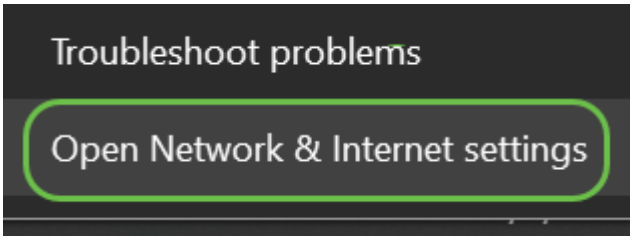
Étape 1. Pour savoir s'il s'agit de votre problème et si vous utilisez un système d'exploitation Windows, vous disposez de deux options simples sur l'interface graphique utilisateur (GUI).

Remarque : Si vous préférez utiliser l'invite de commandes, vous pouvez entrer ipconfig /all.

Option 1 : cliquez avec le bouton droit sur l'icône de l'ordinateur en bas à droite de votre écran.



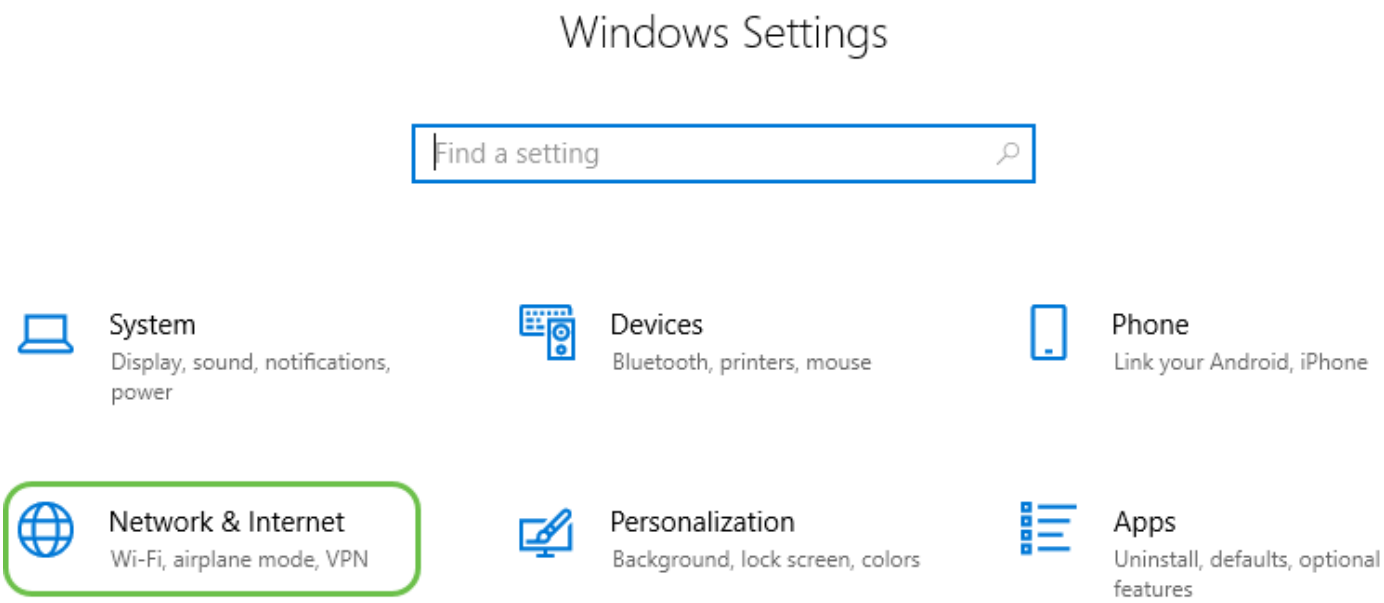
Sélectionnez Open Network and Internet settings.



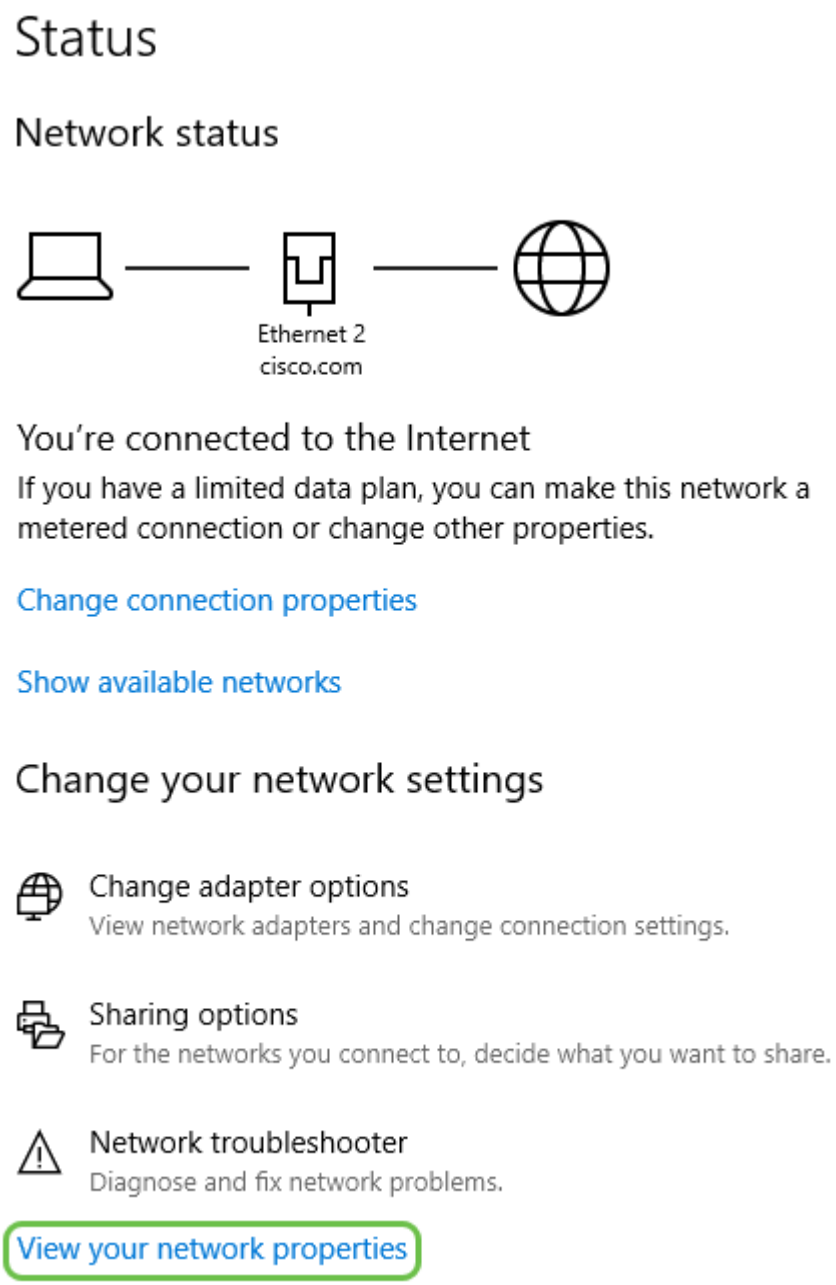
Option 2 : cliquez sur l'icône de la fenêtre, puis sur l'icône de l'engrenage en bas à gauche de votre écran.



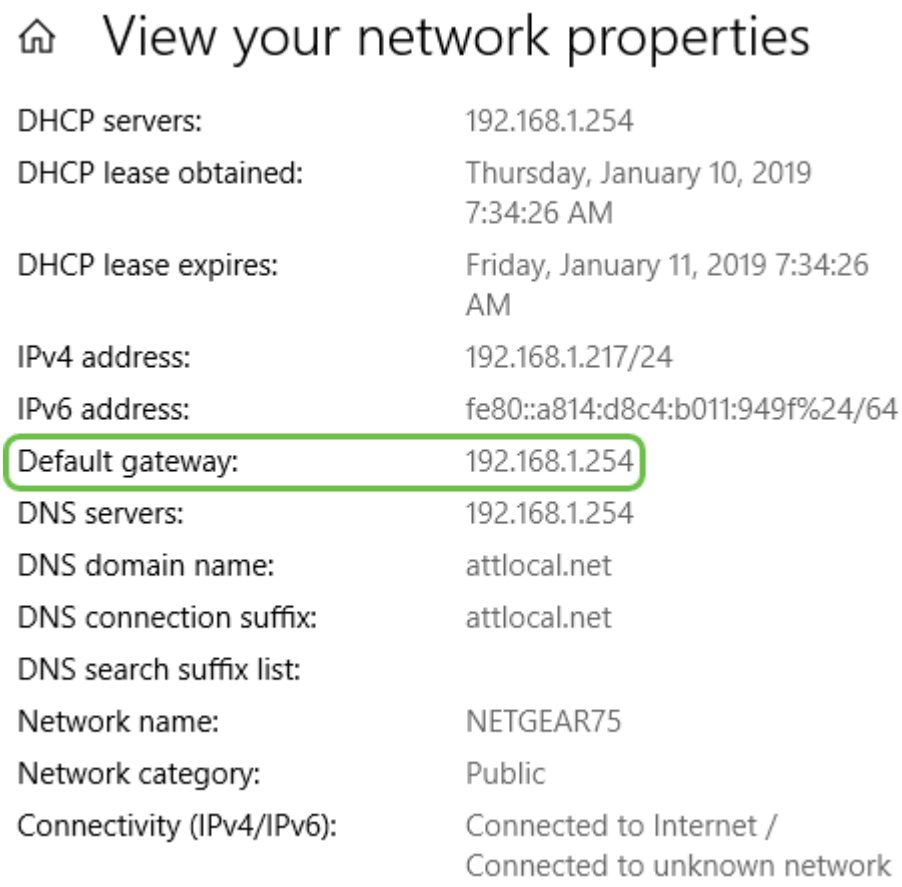
Option 2 (suite) : sélectionnez Réseau et Internet.



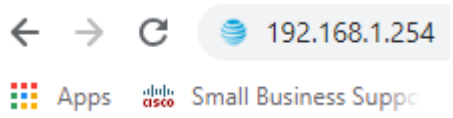
Étape 3. L'une ou l'autre option vous ramène à cet écran. Sélectionnez Afficher les propriétés de votre réseau.



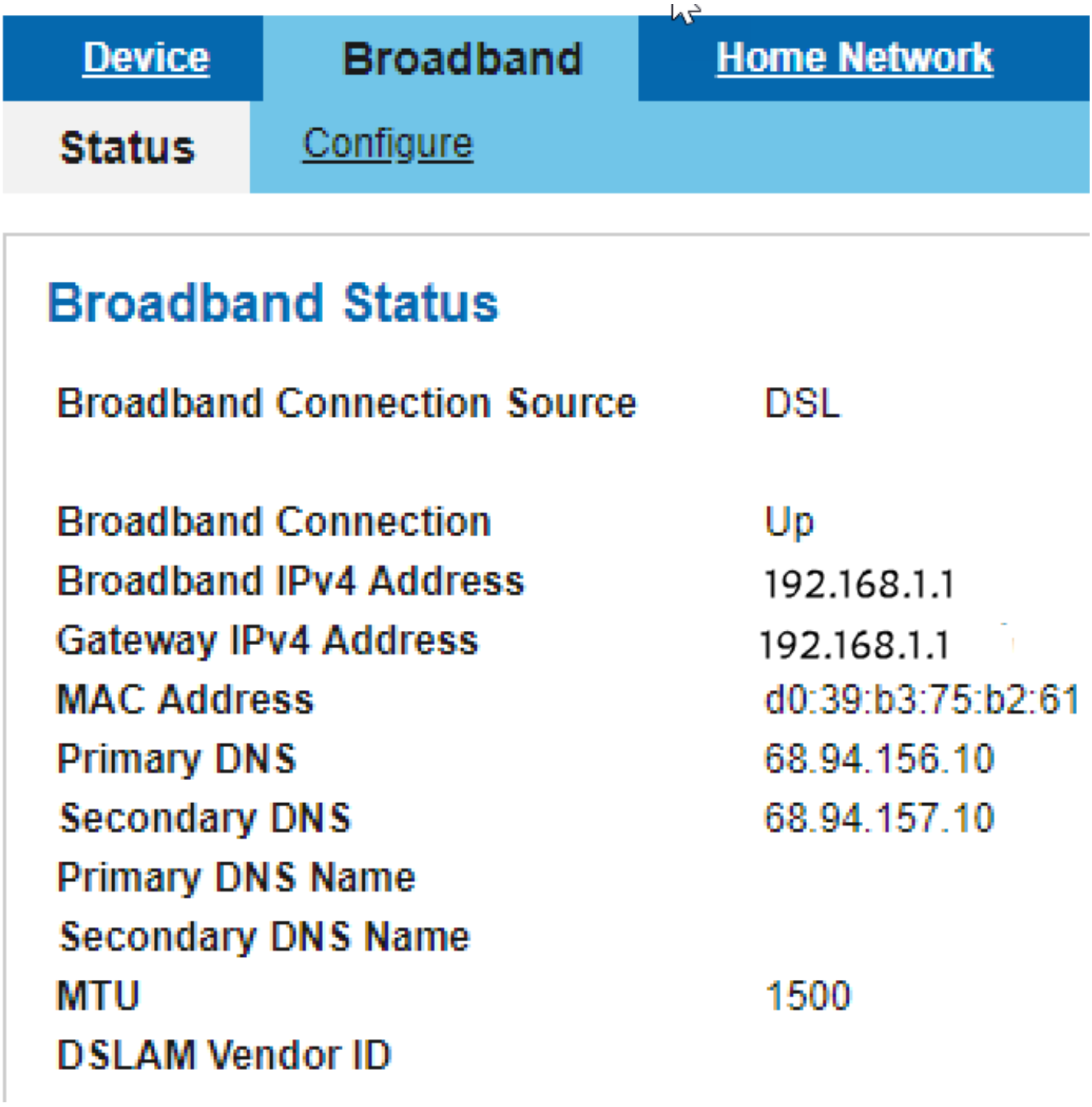
Étape 4. Vous verrez ensuite apparaître la liste Afficher les propriétés de votre réseau. L'adresse de la passerelle par défaut est l'adresse IP du réseau local.



Étape 5. Pour trouver l’adresse IP WAN, accédez au routeur de votre réseau qui se connecte à Internet. Vous devez saisir l'adresse IP du routeur dans votre navigateur Web.



Étape 6. Dans cet exemple, l’adresse IP du réseau étendu est 192.168.1.1. Par conséquent, l’adresse IP du réseau local doit être remplacée par un autre sous-réseau.



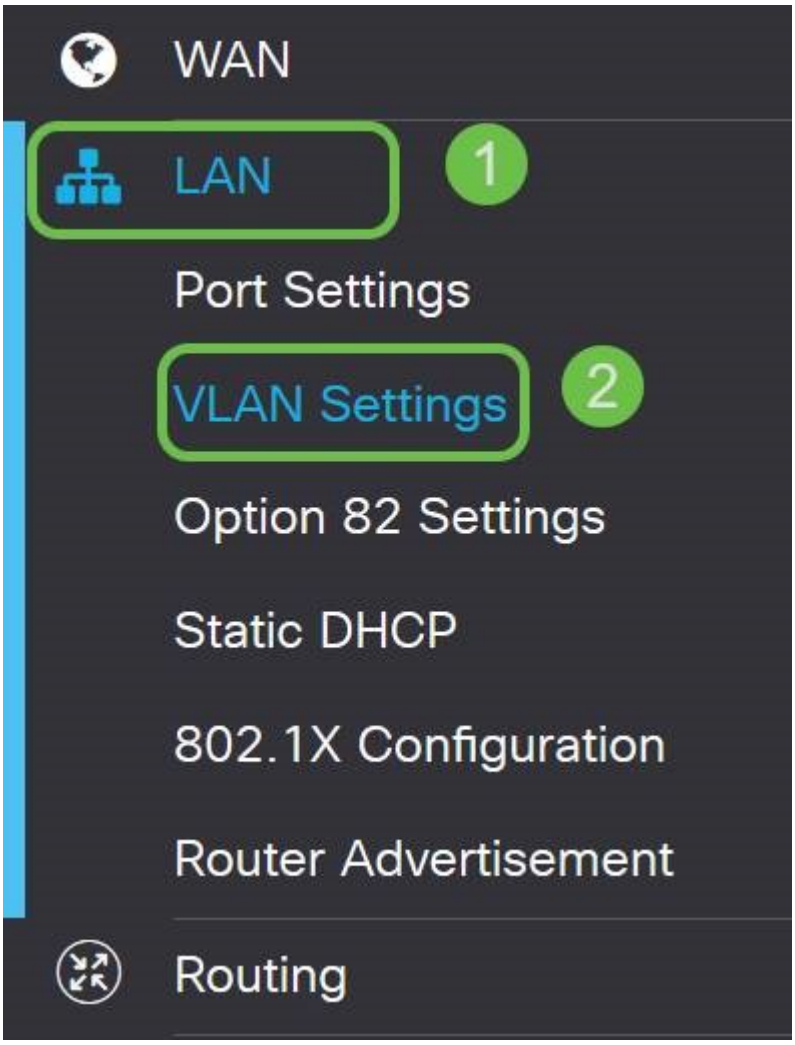
Modifier l'adresse IP de votre réseau local

Cette section n'est généralement pas recommandée, mais elle est nécessaire si votre adresse IP WAN est 192.168.1.x.

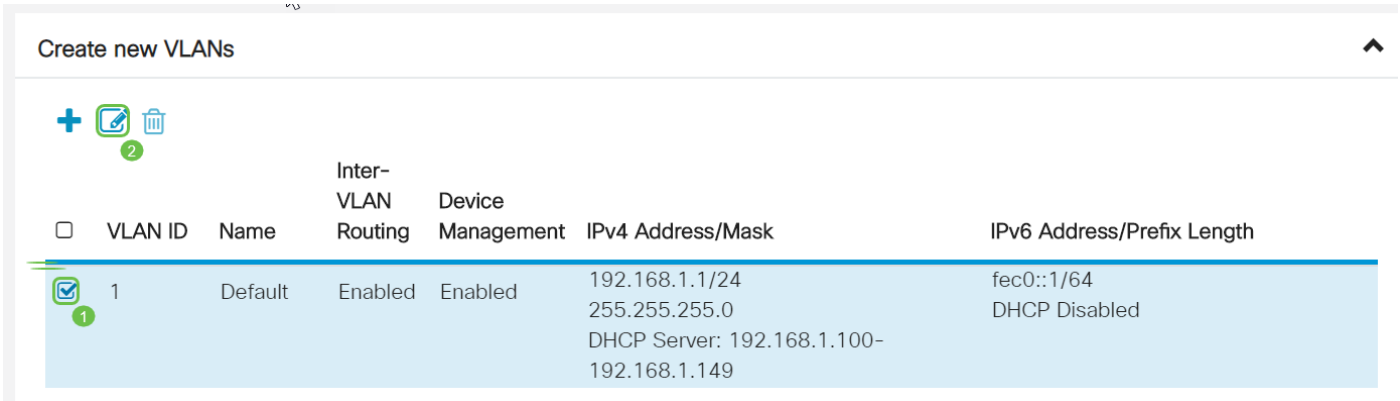
Étape 1 : connexion à votre RV160 ou RV260



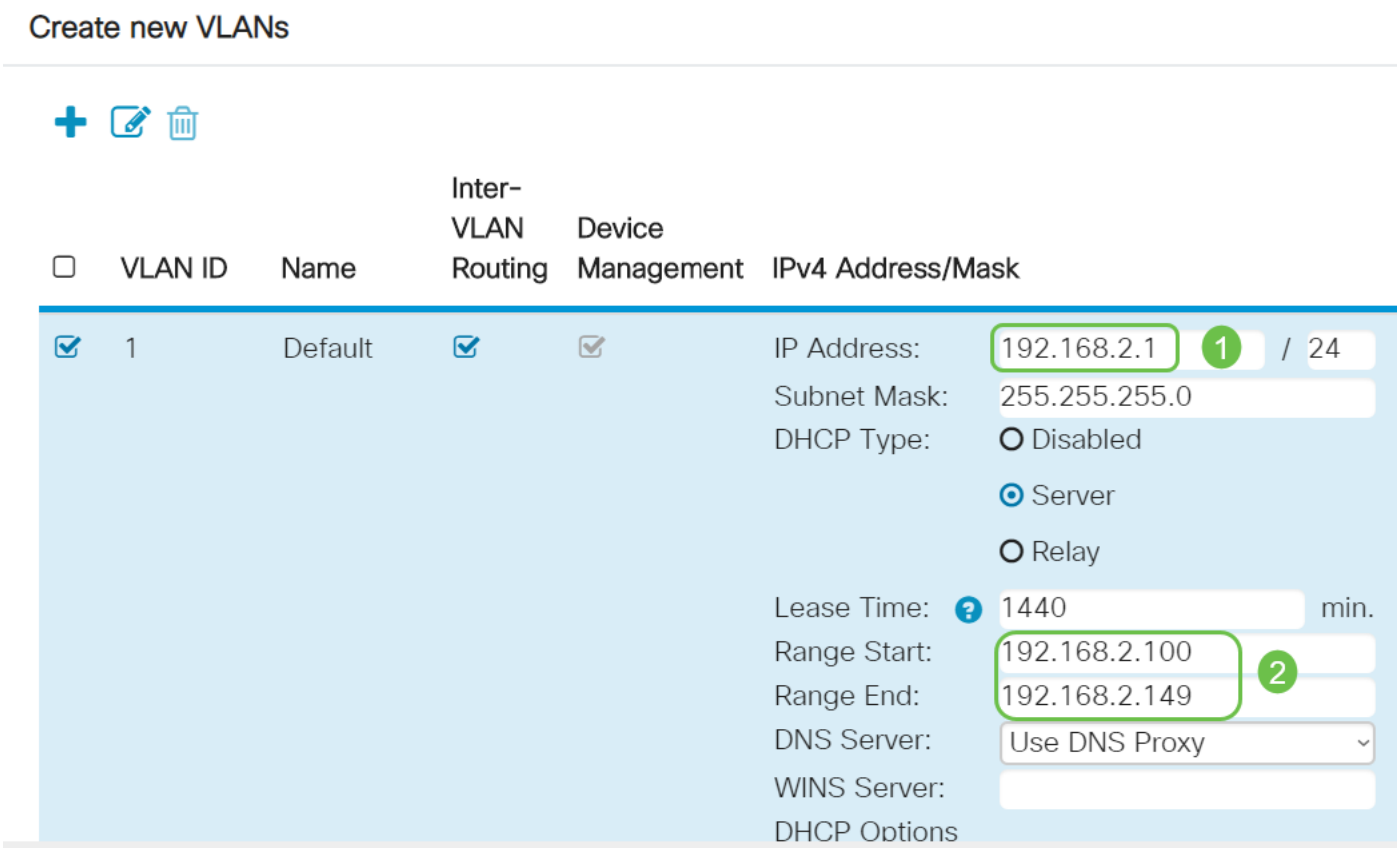
Étape 2. Dans la barre de menus de gauche, cliquez sur le bouton LAN, puis sur VLAN Settings.



Étape 3. Sélectionnez le VLAN qui contient votre périphérique de routage, puis cliquez sur le bouton Edit.



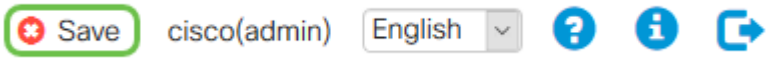
Étape 4. Entrez l’adresse IP statique de votre choix. Vérifiez que le début et la fin de la plage ont été modifiés pour se trouver dans le même sous-réseau que l'adresse IP du VLAN. Si ce n'est pas le cas, vous devrez le modifier pour qu'il se trouve dans le même sous-réseau.



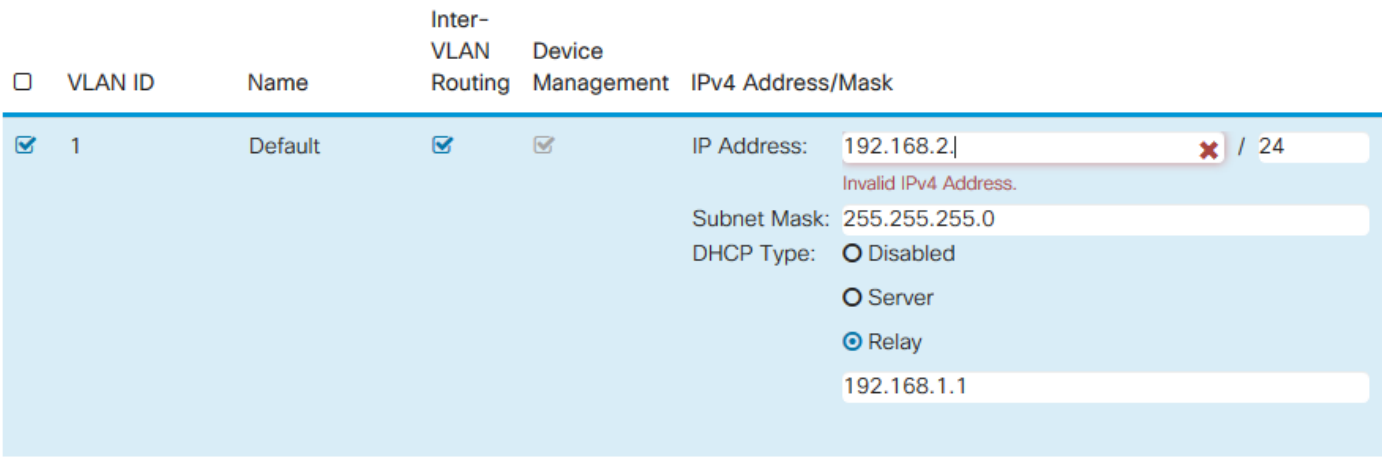
Étape 5. Cliquez sur Apply dans le coin supérieur droit.



Étape 6. Cliquez sur Save.



Étape 7. (Facultatif) Si votre routeur n'est pas le serveur/périphérique DHCP qui attribue des adresses IP, vous pouvez utiliser la fonctionnalité de relais DHCP pour diriger les requêtes DHCP vers une adresse IP spécifique. L'adresse IP est probablement le routeur connecté au WAN/à Internet. Veillez à enregistrer vos modifications.

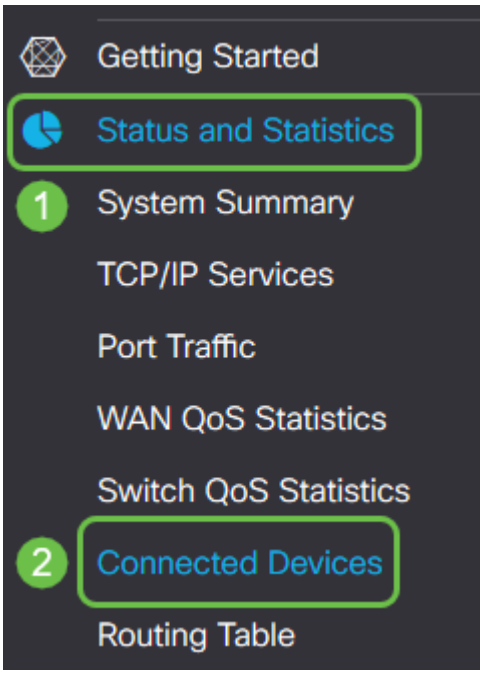


Changements d'adresse IP après changement de sous-réseau

Par défaut, les adresses IP sont attribuées dynamiquement par un serveur DHCP. Par conséquent, votre réseau, par défaut, reçoit une adresse IP attribuée dynamiquement dans le sous-réseau du pool d'adresses LAN local. Une fois que vous avez modifié le sous-réseau, vous devrez peut-être redémarrer les périphériques afin qu'une nouvelle adresse IP leur soit attribuée dans le sous-réseau 192.168.2.x.

Tous les périphériques du réseau doivent se trouver sur le même sous-réseau que le réseau local. Le serveur DHCP doit effectuer cette opération automatiquement. S'il ne change pas automatiquement, débranchez le câble Ethernet et rebranchez-le sur le périphérique. Si un périphérique du réseau n'a toujours pas basculé sur le nouveau sous-réseau 192.168.2.x, vous pouvez le mettre hors tension, puis le remettre sous tension.

Vous pouvez voir les adresses IP et MAC des périphériques connectés en naviguant jusqu'à Status and Statistics, puis Connected Devices.



Pour plus d'informations sur la configuration des paramètres WAN pour votre connexion Internet :

Configuration des paramètres WAN pour votre connexion Internet

Conclusion

Vous disposez maintenant de quelques techniques de dépannage sur votre routeur RV160 ou RV260.

Si l'une des rubriques suivantes vous intéresse, cliquez sur le lien pour afficher l'article :

- Redémarrage et réinitialisation des paramètres d'usine par défaut sur les routeurs RV160 et RV260
- Conseils sur les performances sans fil Périphériques RV160W RV260W
- Configuration Plug-and-Play dans les routeurs RV160 et RV260
- Configuration des assistants de configuration initiale sur les routeurs des gammes RV160X et RV260X

Si vous avez besoin d'aide, voici quelques liens utiles :

- Assistance et téléchargements Cisco
- Informations détaillées sur les routeurs VPN RV160
- Informations détaillées sur les routeurs VPN RV260
- Contacter Cisco
- Contactez l'assistance technique Cisco Small Business

- Créer un dossier

Visionner une vidéo connexe à cet article...

Cliquez ici pour consulter les autres discussions techniques (Tech Talks) de Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.