Configuration de la protection contre les attaques sur le routeur VPN RV132W ou RV134W

Objectif

La protection contre les attaques vous permet de protéger votre réseau contre les types d'attaques les plus courants, telles que la détection, les inondations et les tempêtes d'écho. Bien que la protection contre les attaques soit activée par défaut sur le routeur, vous pouvez ajuster les paramètres pour rendre le réseau plus sensible et plus réactif aux attaques qu'il peut détecter.

Cet article vise à vous montrer comment configurer la protection contre les attaques sur le routeur VPN RV132W et le routeur VPN RV134W.

Périphériques pertinents

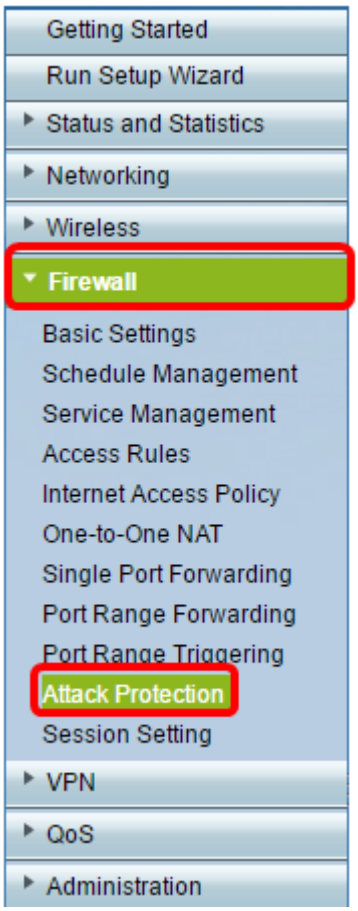
- RV 132 W
- RV134W

Version du logiciel

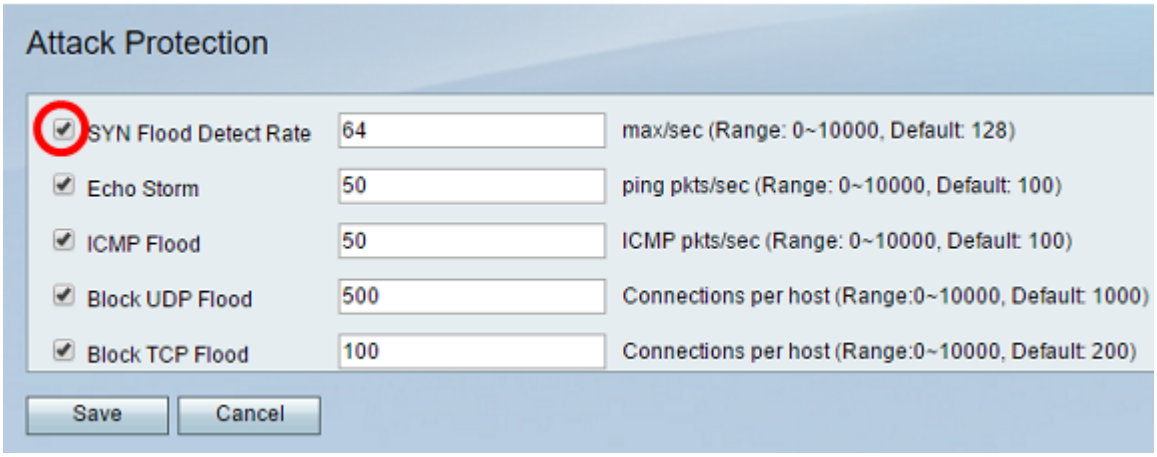
- 1.0.0.17 - RV132W
- 1.0.0.24 — RV134W

Configurer la protection contre les attaques

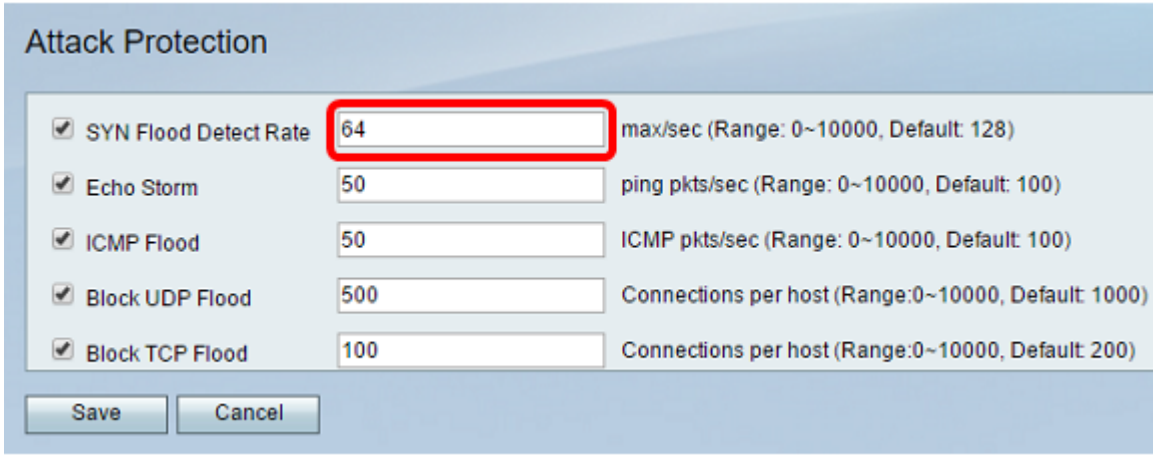
Étape 1. Connectez-vous à l'utilitaire Web et choisissez **Firewall > Attack Protection**.



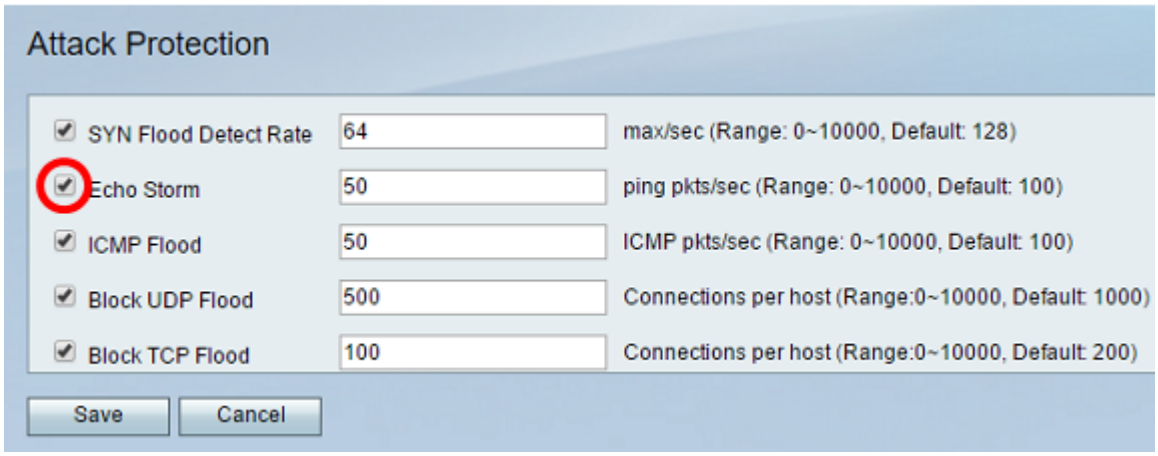
Étape 2. Vérifiez que la case SYN Flood Detect Rate est cochée pour vous assurer que la fonction est active. Cette option est activée par défaut.



Étape 3. Saisissez une valeur dans le champ *SYN Flood Detect Rate*. La valeur par défaut est de 128 paquets SYN par seconde. Vous pouvez entrer une valeur comprise entre 0 et 10000. Il s'agit du nombre de paquets SYN par seconde qui permet à l'appliance de sécurité de déterminer qu'une intrusion d'inondation SYN se produit. Une valeur égale à zéro indique que la fonction de détection de débordement SYN est désactivée. Dans cet exemple, la valeur saisie est 64. Cela signifie que la solution matérielle-logicielle détecterait une intrusion SYN flood à seulement 64 paquets SYN par seconde, ce qui la rendrait plus sensible que la configuration par défaut.

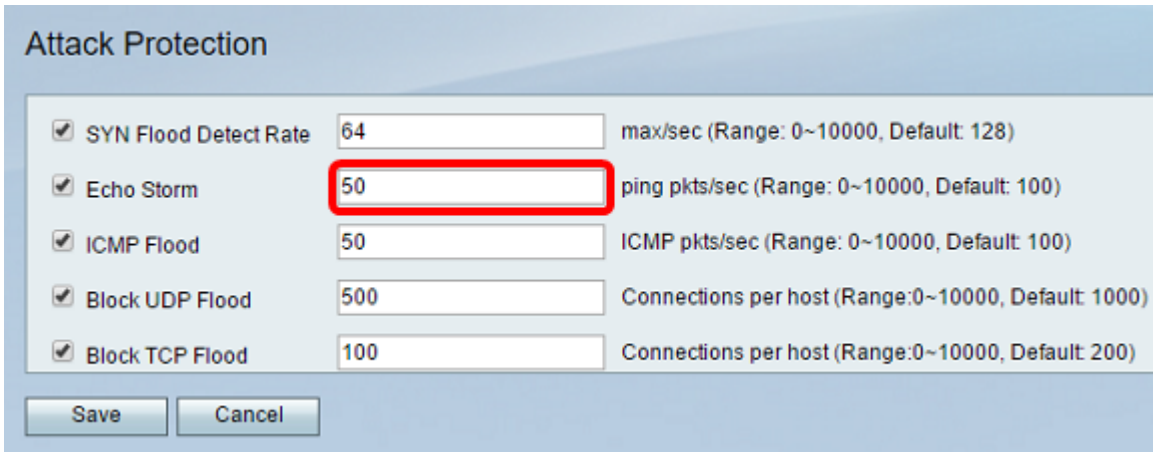


Étape 4. Vérifiez que la case Echo Storm (Tempête d'écho) est cochée pour vous assurer que la fonctionnalité est active. Cette option est activée par défaut.

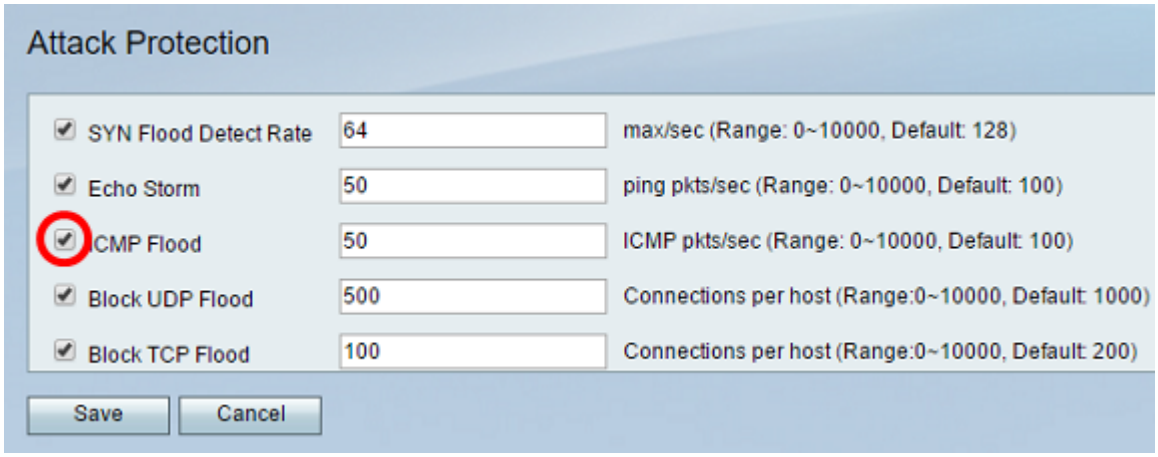


Étape 5. Entrez une valeur dans le champ *Echo Storm*. La valeur par défaut est de 100 requêtes ping par seconde. Vous pouvez entrer une valeur comprise entre 0 et 10000. Il s'agit du nombre de requêtes ping par seconde qui permet à l'appliance de sécurité de déterminer qu'un événement d'intrusion d'écho tempête se produit. Une valeur égale à zéro indique que la fonction Echo Storm est désactivée.

Remarque : dans cet exemple, la solution matérielle-logicielle ne détecte un événement Echo Storm qu'à raison de 50 requêtes ping par seconde.

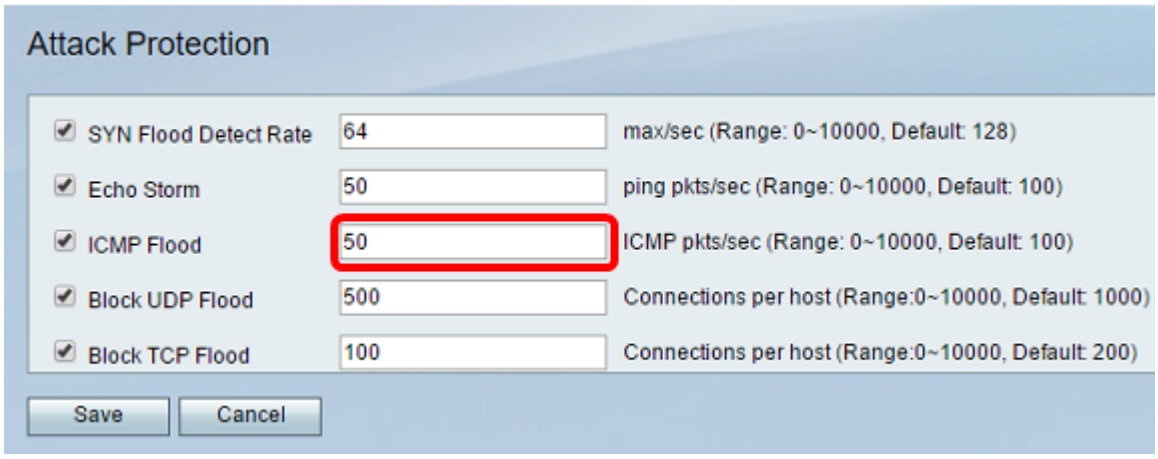


Étape 6. Vérifiez que la case Inondation ICMP (Internet Control Message Protocol) est cochée pour vous assurer que la fonctionnalité est active. Cette fonction est activée par défaut.

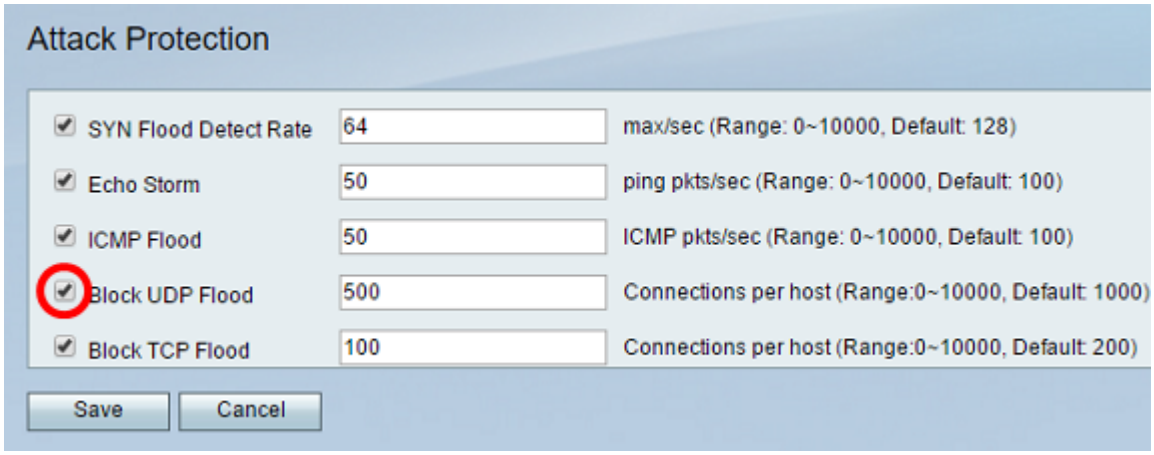


Étape 7. Entrez une valeur numérique dans le champ *Inondation ICMP*. La valeur par défaut est de 100 paquets ICMP par seconde. Vous pouvez entrer une valeur comprise entre 0 et 10000. Il s'agit du nombre de paquets ICMP par seconde qui permet à l'appliance de sécurité de déterminer qu'un événement d'intrusion d'inondation ICMP se produit. Une valeur égale à zéro indique que la fonctionnalité Inondation ICMP est désactivée.

Remarque : dans cet exemple, la valeur entrée est 50, ce qui la rend plus sensible à l'inondation ICMP que son paramètre par défaut.

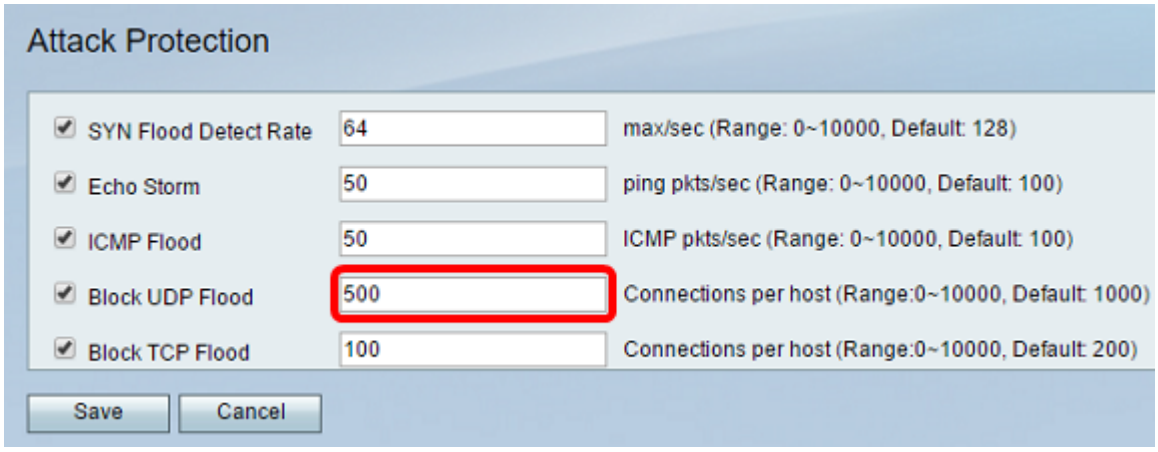


Étape 8. Vérifiez que la case Bloquer le flux UDP est cochée pour vous assurer que la fonctionnalité est active et pour empêcher l'appliance de sécurité d'accepter plus de 150 connexions UDP (User Datagram Protocol) actives simultanées par seconde à partir d'un seul ordinateur sur le réseau local (LAN). Cette option est cochée par défaut.

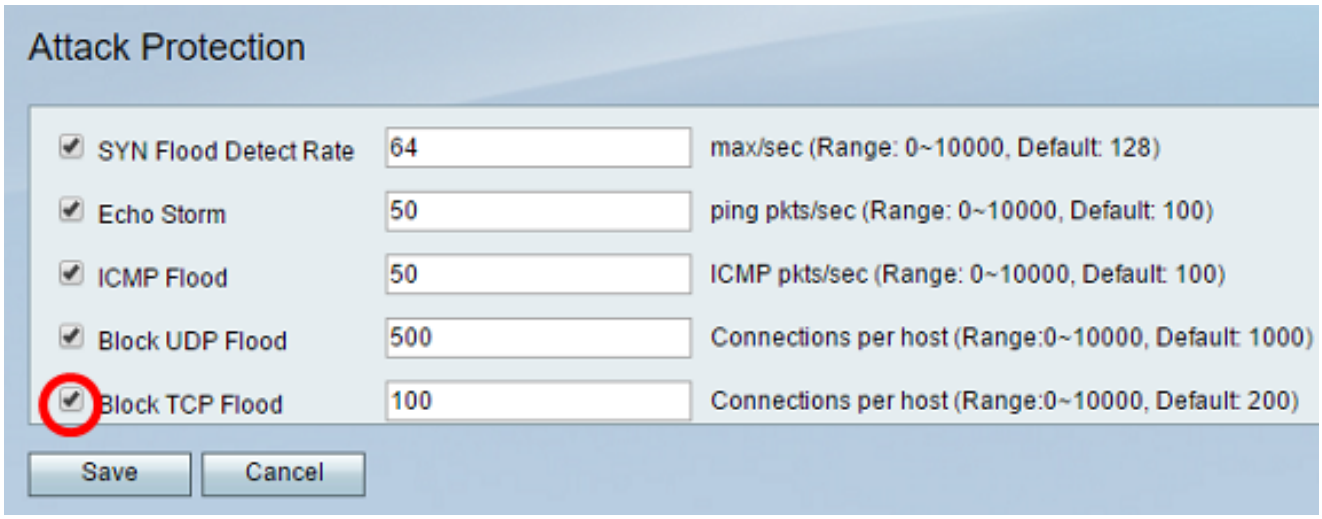


Étape 9. Entrez une valeur comprise entre 0 et 10000 dans le champ *Block UDP Flood*. La valeur par défaut est 1000. Dans cet exemple, la valeur saisie est 500, ce qui la rend plus

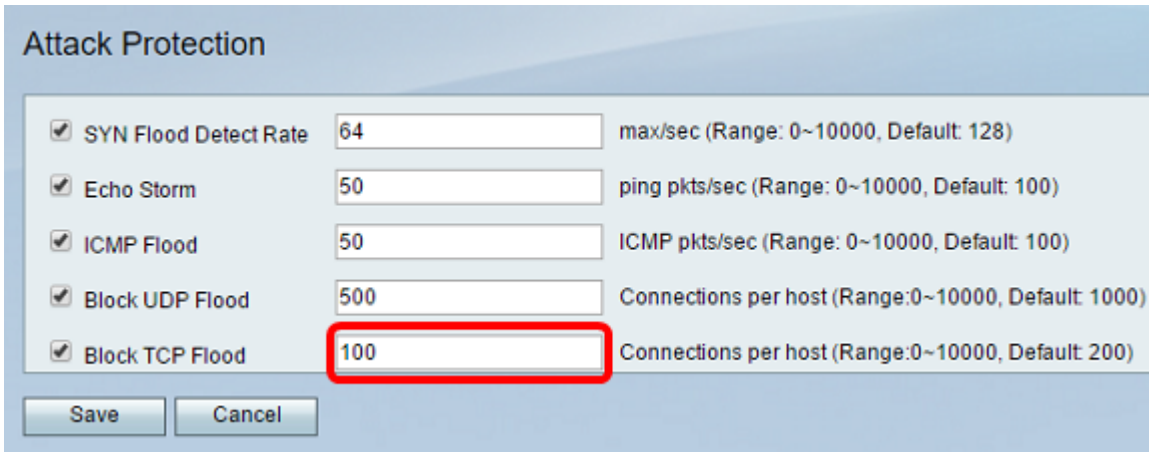
sensible.



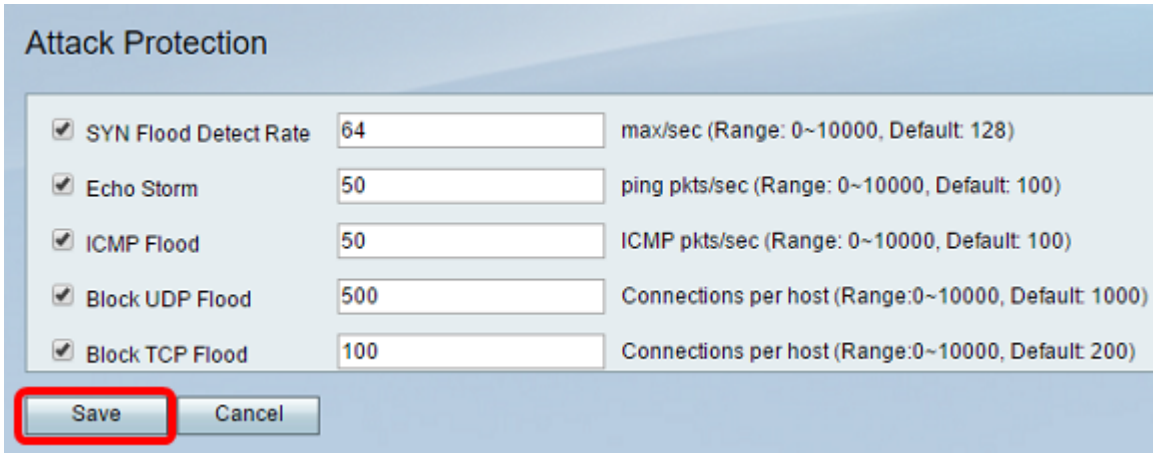
Étape 10. Vérifiez que la case Bloquer le flux TCP est cochée pour supprimer tous les paquets TCP (Transmission Control Protocol) non valides. Cette option est cochée par défaut.



Étape 11. Entrez une valeur comprise entre 0 et 10000 dans le champ *Block TCP Flood* pour protéger votre réseau d'une attaque par inondation SYN. La valeur par défaut est 200. Dans cet exemple, 100 est entré, ce qui le rend plus sensible.



Étape 12. Cliquez sur **Save**.



Vous devez maintenant avoir correctement configuré la protection contre les attaques sur votre routeur RV132W ou RV134W.

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.