Configuration des paramètres de base du pare-feu sur RV215W

Objectif

Un pare-feu est un ensemble de fonctionnalités conçues pour maintenir la sécurité d'un réseau. Un routeur est considéré comme un pare-feu matériel puissant. Ceci est dû au fait que les routeurs sont capables d'inspecter tout le trafic entrant et d'abandonner tout paquet indésirable.

Cet article explique comment configurer les paramètres de pare-feu de base sur le routeur RV215W.

Périphériques pertinents

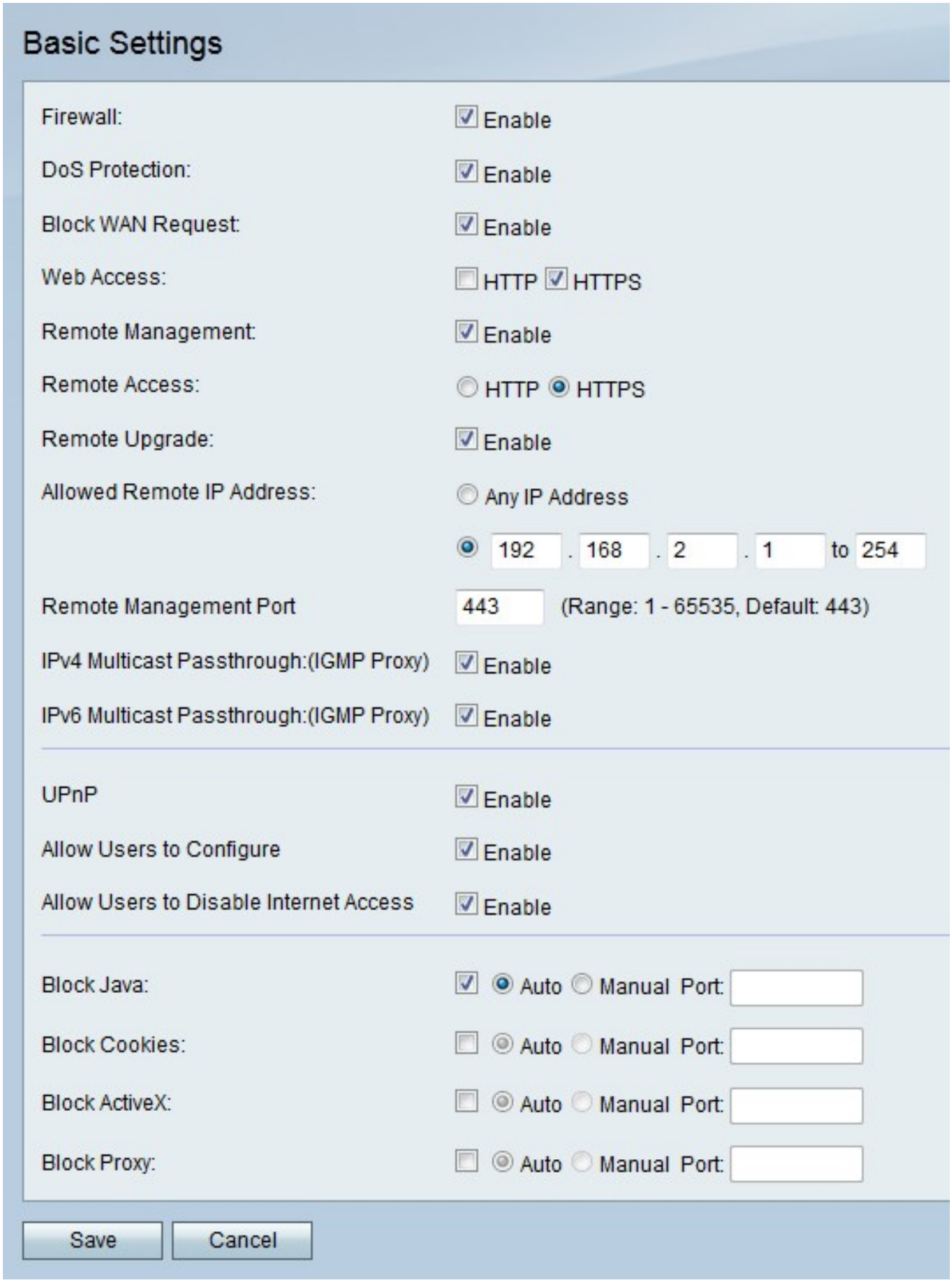
·RV215W

Version du logiciel

•1.1.0.5

Paramètres de base

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Firewall > Basic Settings**. La page *Basic Settings* s'ouvre :



Étape 2. Cochez **Enable** dans le champ Firewall (Pare-feu) pour activer la configuration du pare-feu sur le routeur RV215W.

Étape 3. Cochez **Enable** dans le champ DoS Protection pour activer la protection DoS (Denial of Service) sur le RV215W. La protection par déni de service (DoS) est utilisée pour empêcher un réseau d'être victime d'une attaque par déni de service distribué (DDoS). Les

attaques DDoS sont destinées à inonder un réseau au point où les ressources du réseau deviennent indisponibles. Le RV215W utilise la protection DoS pour protéger le réseau par la restriction et la suppression des paquets indésirables.

Étape 4. Cochez **Enable** dans le champ Block WAN Request pour bloquer toutes les requêtes ping au RV215W à partir du WAN.

Étape 5. Cochez la case correspondant au type d'accès Web souhaité qui peut être utilisé pour se connecter au pare-feu dans le champ Web Access.

Étape 6. Cochez **Activer** dans le champ Gestion à distance. La gestion à distance permet d'accéder au routeur RV215W à partir d'un réseau WAN distant.

Étape 7. Cliquez sur la case d'option correspondant au type d'accès Web souhaité qui peut être utilisé pour se connecter au pare-feu à partir du WAN distant dans le champ Remote Access.

Étape 8. Cochez **Remote Upgrade** pour permettre aux utilisateurs distants de mettre à niveau le RV215W.

Étape 9. Activez la case d'option correspondant aux adresses IP souhaitées qui sont autorisées à accéder au routeur RV215W à distance dans le champ Allowed Remote IP Address (Adresse IP distante autorisée).

·Any IP Address : toutes les adresses IP sont autorisées.

·IP Address : saisissez une plage d'adresses IP autorisées.

Étape 10. Entrez un port sur lequel l'accès à distance est autorisé dans le champ Remote Management Port. Un utilisateur distant doit utiliser le port distant pour accéder au périphérique.

Note: Le format de l'accès distant est https://<*remote-ip*>:<*remote-port*>

Étape 11. Cochez **Enable** dans le champ IPv4 Multicast Passthrough (Passthrough multidiffusion IPv4) pour autoriser le trafic multidiffusion IPv4 à traverser le RV215W à partir d'Internet. La multidiffusion IP est une méthode utilisée pour envoyer des datagrammes IP à un groupe désigné de récepteurs dans une seule transmission.

Étape 12. Cochez **Enable** dans le champ IPv6 Multicast Passthrough (Passthrough multidiffusion IPv6) pour autoriser le trafic de multidiffusion IPv6 à traverser le routeur RV215W à partir d'Internet.

Étape 13. Cochez **Enable** dans le champ UPnP pour activer Universal Plug and Play (UPnP). UPnP permet de détecter automatiquement les périphériques qui peuvent communiquer avec le RV215W.

Étape 14. Cochez la case **Activer** dans le champ Autoriser les utilisateurs à configurer pour permettre aux utilisateurs disposant de périphériques compatibles UPnP de configurer les règles de mappage de port UPnP. Le mappage de port ou le transfert de port est utilisé pour autoriser les communications entre les hôtes externes et les services fournis au sein d'un réseau local privé.

Étape 15. Cochez **Enable** dans le champ Allow Users to Disable Internet Access (Autoriser les utilisateurs à désactiver l'accès à Internet) pour permettre aux utilisateurs de désactiver

l'accès à Internet sur le périphérique.

Étape 16. Cochez **Bloquer Java** pour empêcher le téléchargement des applets java. Les applets Java conçues pour des intentions malveillantes peuvent constituer une menace pour la sécurité d'un réseau. Une fois téléchargé, un applet java hostile peut exploiter les ressources réseau. Sélectionnez la case d'option correspondant à la méthode de blocage souhaitée.

·Auto : bloque automatiquement le Java.

·Manual Port : saisissez un port spécifique sur lequel bloquer java.

Étape 17. Cochez la case **Bloquer les cookies** pour empêcher la création de cookies par un site Web. Les cookies sont créés par les sites Web pour stocker les informations de ces utilisateurs. Les cookies peuvent suivre l'historique Web de l'utilisateur, ce qui peut conduire à une violation de la vie privée. Sélectionnez la case d'option correspondant à la méthode de blocage souhaitée.

·Auto : bloque automatiquement les cookies.

·Manual Port : saisissez un port spécifique sur lequel bloquer les cookies.

Étape 18. Cochez **Bloquer ActiveX** pour empêcher le téléchargement des applets ActiveX. ActiveX est un type d'applet qui manque de sécurité. Une fois qu'une applet ActiveX est installée sur un ordinateur, elle peut faire tout ce qu'un utilisateur peut faire. Il peut insérer du code nuisible dans le système d'exploitation, surfer sur un intranet sécurisé, modifier un mot de passe ou récupérer et envoyer des documents. Sélectionnez la case d'option correspondant à la méthode de blocage souhaitée.

·Auto : bloque automatiquement ActiveX.

·Manual Port : saisissez un port spécifique sur lequel bloquer ActiveX.

Étape 19. Cochez **Bloquer le proxy** pour bloquer les serveurs proxy. Les serveurs proxy sont des serveurs qui fournissent une liaison entre deux réseaux distincts. Les serveurs proxy malveillants peuvent enregistrer toutes les données non chiffrées qui leur sont envoyées, telles que les connexions ou les mots de passe. Sélectionnez la case d'option correspondant à la méthode de blocage souhaitée.

·Auto : bloque automatiquement les serveurs proxy.

·Manual Port : saisissez un port spécifique sur lequel bloquer les serveurs proxy.

Étape 20. Click **Save**.