Configuration des paramètres de base du pare-feu sur les modèles RV130 et RV130W

Objectif

Les paramètres de base du pare-feu peuvent sécuriser votre réseau en créant et en appliquant des règles que le périphérique utilise pour bloquer et autoriser de manière sélective le trafic Internet entrant et sortant.
Des fonctionnalités telles que Universal Plug and Play facilitent la connexion des périphériques entre eux sur votre réseau sans configuration supplémentaire.

La fonctionnalité UPnP (Universal Plug and Play) permet de détecter automatiquement les périphériques qui peuvent communiquer avec le périphérique. Le blocage du contenu peut contribuer à sécuriser votre ordinateur, car certains contenus peuvent être envoyés à votre périphérique, ce qui peut compromettre la sécurité ou infecter votre ordinateur avec des logiciels malveillants. La possibilité de bloquer du contenu spécifique sur les ports de votre choix est utile pour une meilleure sécurité du pare-feu.

L'objectif de ce document est de vous montrer comment configurer les paramètres de base du pare-feu sur les modèles RV130 et RV130W.

Périphériques pertinents

·RV130

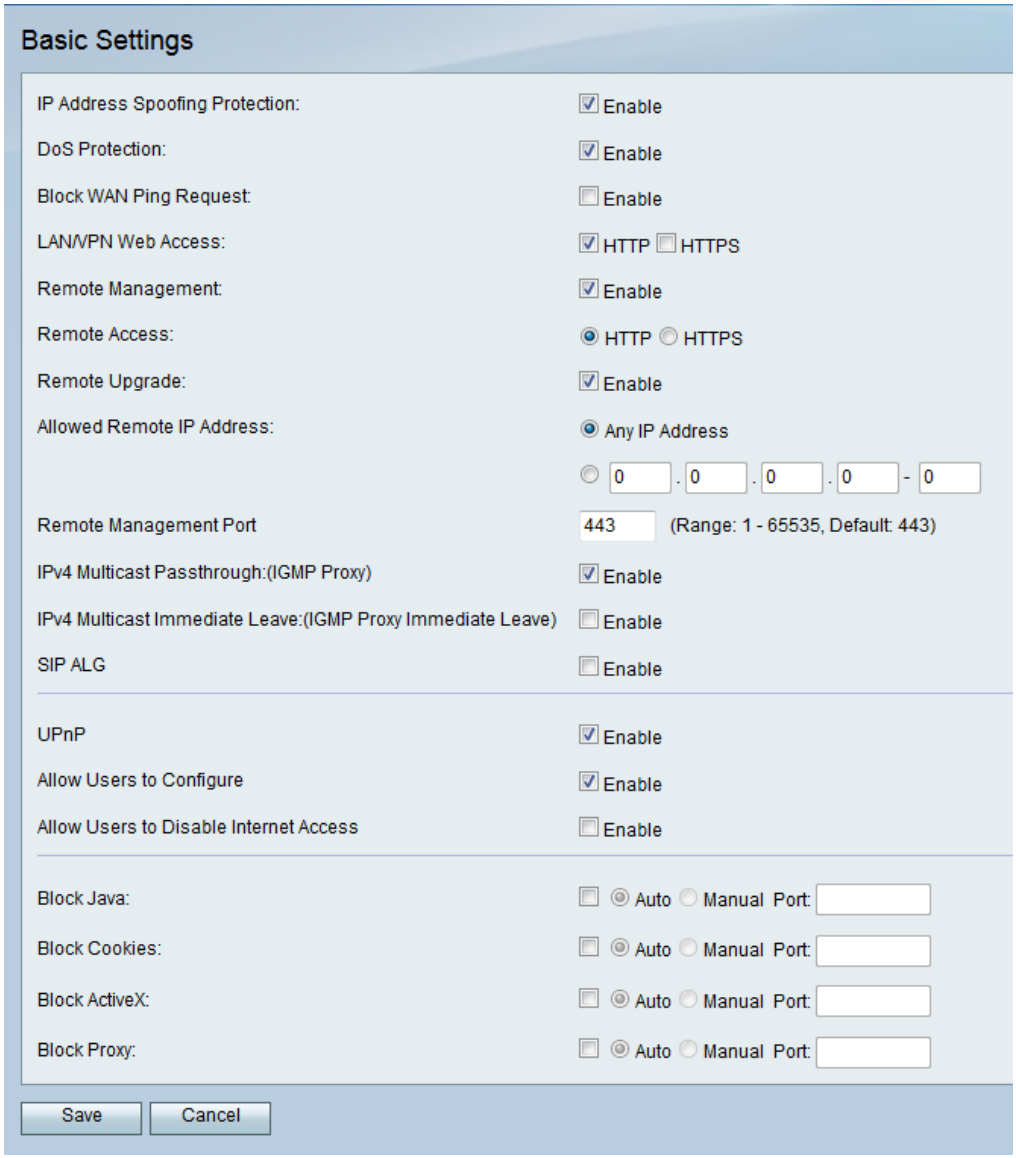
·RV130W

Version du logiciel

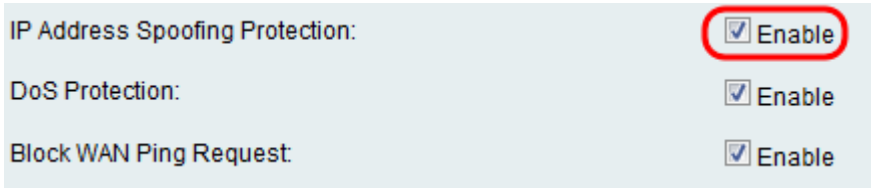
•v 1.0.1.3

Configuration des paramètres de base du pare-feu

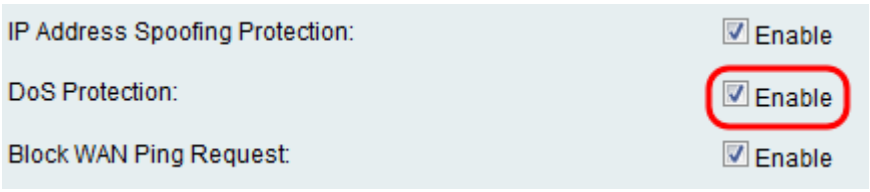
Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Firewall > Basic Settings**. La page Basic Settings s'ouvre :



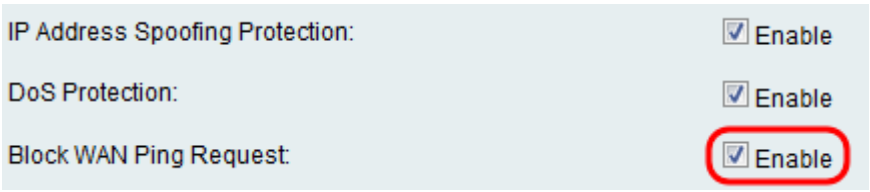
Étape 2. Dans le champ *IP Address Spoofing Protection*, cochez la case **Enable** pour protéger votre réseau contre l'usurpation d'adresse IP. L'usurpation d'adresse IP est une tentative d'accès à un réseau par un utilisateur non autorisé en usurpant l'identité d'un autre périphérique approuvé en utilisant son adresse IP comme sienne. Il est recommandé d'activer *Protection contre la mystification des adresses IP.*



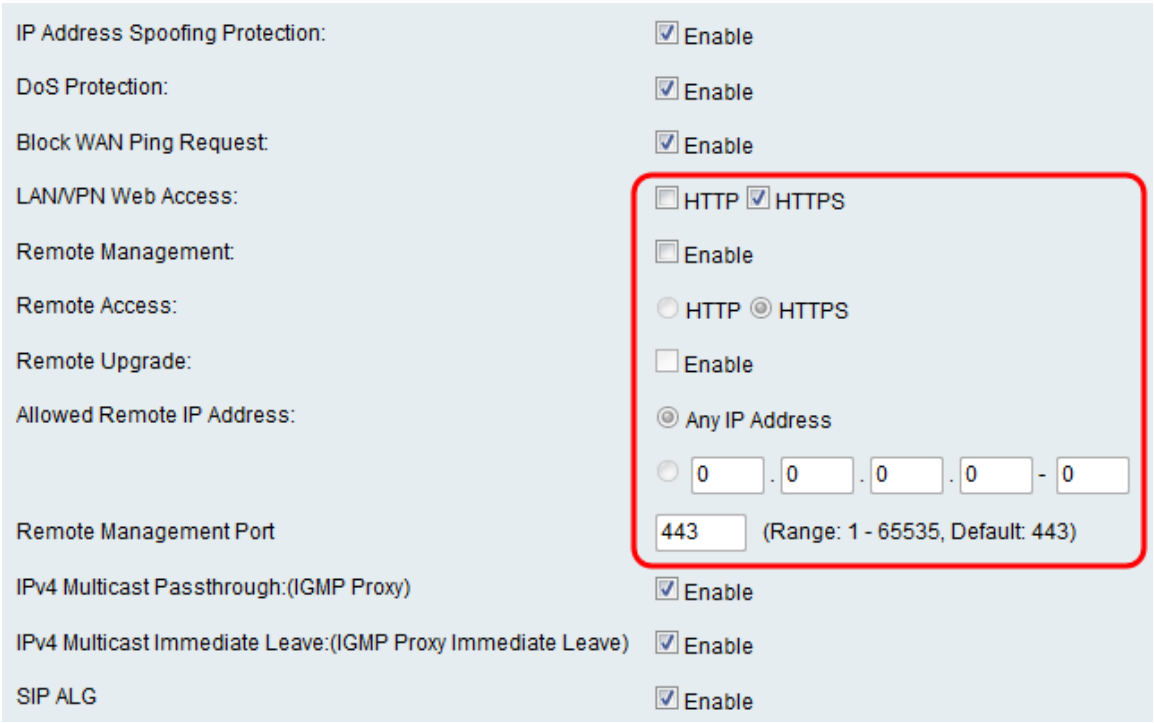
Étape 3. Dans le champ *DoS Protection*, cochez la case **Enable** pour protéger votre réseau contre les attaques par déni de service. La protection par déni de service est utilisée pour protéger un réseau contre une attaque par déni de service distribué (DDoS). Les attaques DDoS visent à inonder un réseau au point où les ressources du réseau deviennent indisponibles.



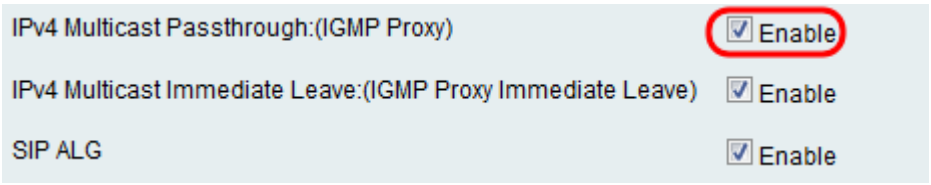
Étape 4. Dans le champ *Block WAN Ping Request*, cochez la case **Enable** pour arrêter les requêtes ping vers votre périphérique à partir du réseau WAN externe.



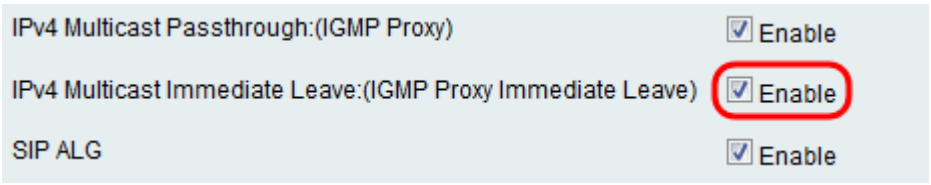
Étape 5. Les champs répertoriés de *LAN/VPN Web Access à Remote Management Port* sont utilisés pour configurer LAN et Remote Management Web Access. Pour en savoir plus sur ces configurations, référez-vous à Configuration de l'accès Web de gestion à distance et de réseau local sur les modèles RV130 et RV130W.



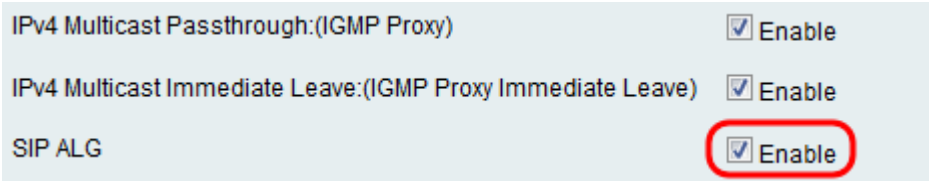
Étape 6. Dans le champ *IPv4 Multicast Passthrough:(IGMP Proxy)*, cochez la case **Enable** pour activer le passage de multidiffusion pour IPv4. Ceci transfère les paquets IGMP de groupe du réseau WAN externe vers votre réseau local interne.



Étape 7. Dans le champ *IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)*, cochez la case **Enable** pour activer le Multicast Immediate Leave. L'activation du congé immédiat garantit une gestion optimale de la bande passante pour les hôtes de votre réseau, même en cas d'utilisation simultanée de groupes de multidiffusion.



Étape 8. Dans le champ *Session Initiation Protocol (SIP) Application Layer Gateway (ALG)*, cochez la case **Enable** pour permettre au trafic SIP (Session Initiation Protocol) de traverser le pare-feu. Le protocole SIP (Session Initiation Protocol) permet aux plates-formes de signaler l'établissement d'appels vocaux et multimédias sur des réseaux IP. La passerelle de couche application (ALG), également appelée passerelle de niveau application, est une application qui traduit les informations d'adresse IP à l'intérieur de la charge utile d'un paquet d'applications.

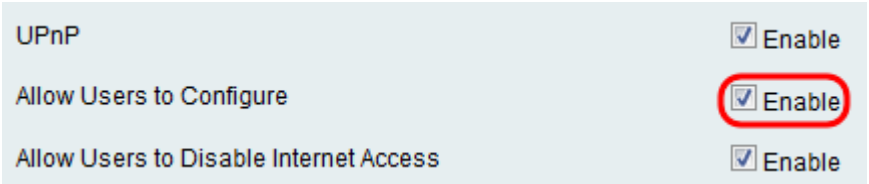


Note: Le périphérique prend en charge un maximum de 256 sessions SIP ALG.

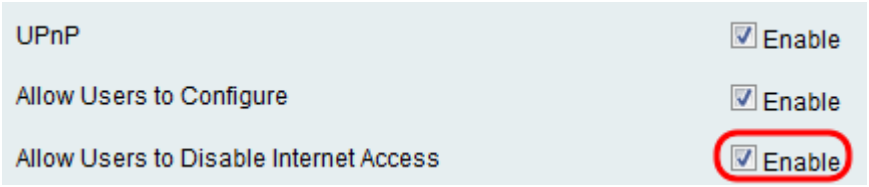
Configuration de Universal Plug and Play

Étape 1. Dans le champ *UPnP*, cochez la case **Enable** pour activer le protocole UPnP (Universal Plug and Play).

Étape 2. Dans le champ *Allow Users to Configure*, cochez la case **Enable** pour autoriser les règles de mappage de port UPnP à être définies par les utilisateurs dont la prise en charge UPnP est activée sur leurs ordinateurs ou d'autres périphériques compatibles UPnP. S'il est désactivé, le périphérique n'autorise pas l'application à ajouter la règle de transfert.



Étape 3. Dans le champ *Allow Users to Disable Internet Access*, cochez la case **Enable** pour permettre aux utilisateurs de désactiver l'accès à Internet.



Blocage du contenu

Étape 1. Cochez la case dans le champ correspondant au contenu que vous souhaitez bloquer à partir du périphérique.

Les options disponibles sont définies comme suit :

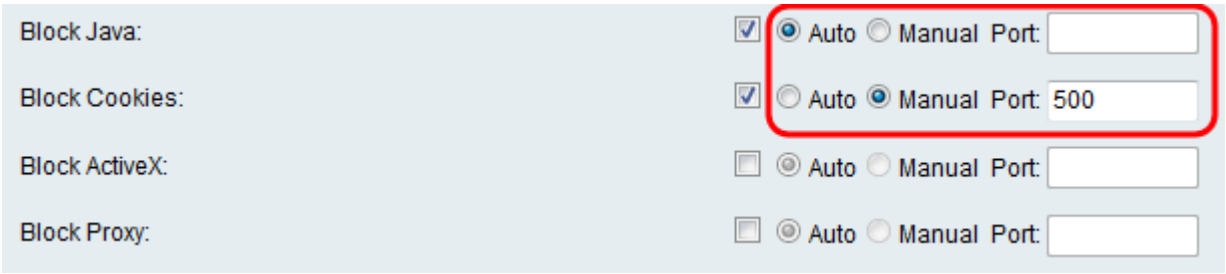
·Block Java : bloque le téléchargement des applets Java.

·Block Cookies : empêche l'appareil de recevoir des informations de cookies à partir de pages Web.

·Block ActiveX : bloque les applets ActiveX qui peuvent être présents lorsque vous utilisez Internet Explorer sur le système d'exploitation Windows.

·Block Proxy : empêche le périphérique de communiquer avec des périphériques externes via un serveur proxy. Cela empêche le périphérique de contourner les règles de pare-feu.

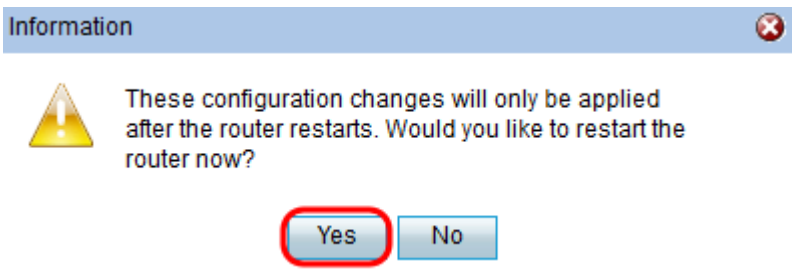
Étape 2. Sélectionnez la case d'option **Auto** pour bloquer automatiquement toutes les instances de ce contenu particulier, ou cliquez sur la case d'option **Manual** et entrez un port spécifique dans le champ correspondant sur lequel le contenu sera bloqué.



Note: Vous pouvez entrer n'importe quel numéro souhaité dans la plage (1-65535) de votre valeur de port.

Étape 3. Cliquez sur **Save** pour enregistrer vos paramètres.

Étape 4. Une fenêtre vous invitant à redémarrer votre routeur s'affiche. Cliquez sur **Yes** pour redémarrer votre routeur et appliquer les modifications.



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.