Configuration des paramètres généraux du pare-feu sur les modèles RV016, RV042, RV042G et RV082

Objectif

Par défaut, le pare-feu intégré pour les routeurs RV016, RV042, RV042G et RV082 bloque certains types de trafic. Les types de trafic bloqués, tels que les requêtes HTTPS, TCP et ICMP et le trafic de gestion à distance, peuvent être ajustés. Le pare-feu lui-même peut également être activé ou désactivé. En outre, certains aspects des sites Web qui peuvent être des vulnérabilités de sécurité peuvent également être bloqués. Lorsqu'elles sont débloquées, ces fonctionnalités du site Web peuvent stocker des données potentiellement dangereuses sur votre ordinateur.

L'objectif de ce document est de vous montrer comment configurer les paramètres généraux du pare-feu sur les routeurs RV016, RV042, RV042G et RV082.

Périphériques pertinents

â€¢RV016

â€¢RV042

â€¢RV042G

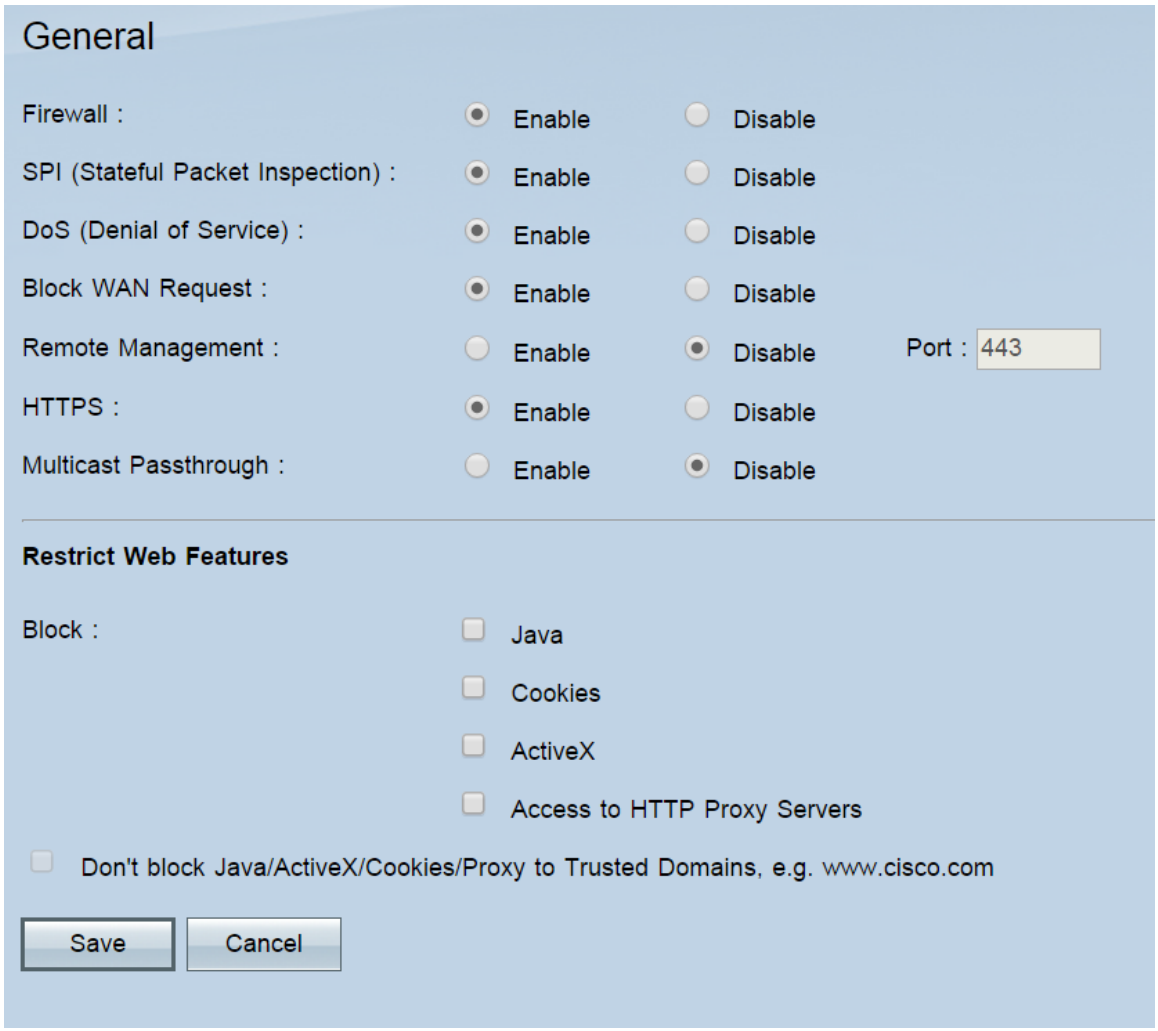
â€¢RV082

Version du logiciel

â€¢v 4.2.3.06

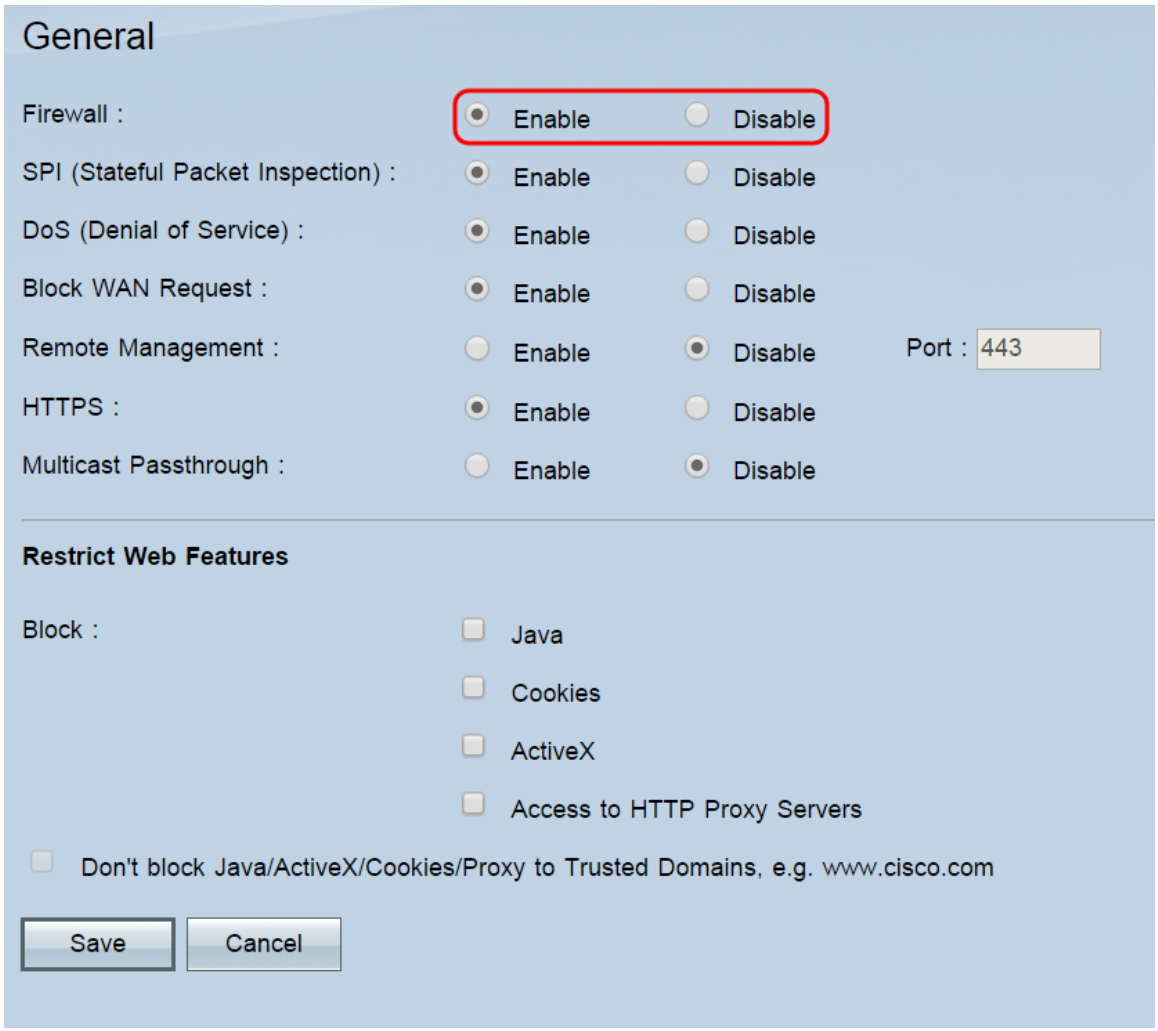
Configuration des paramètres généraux du pare-feu

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



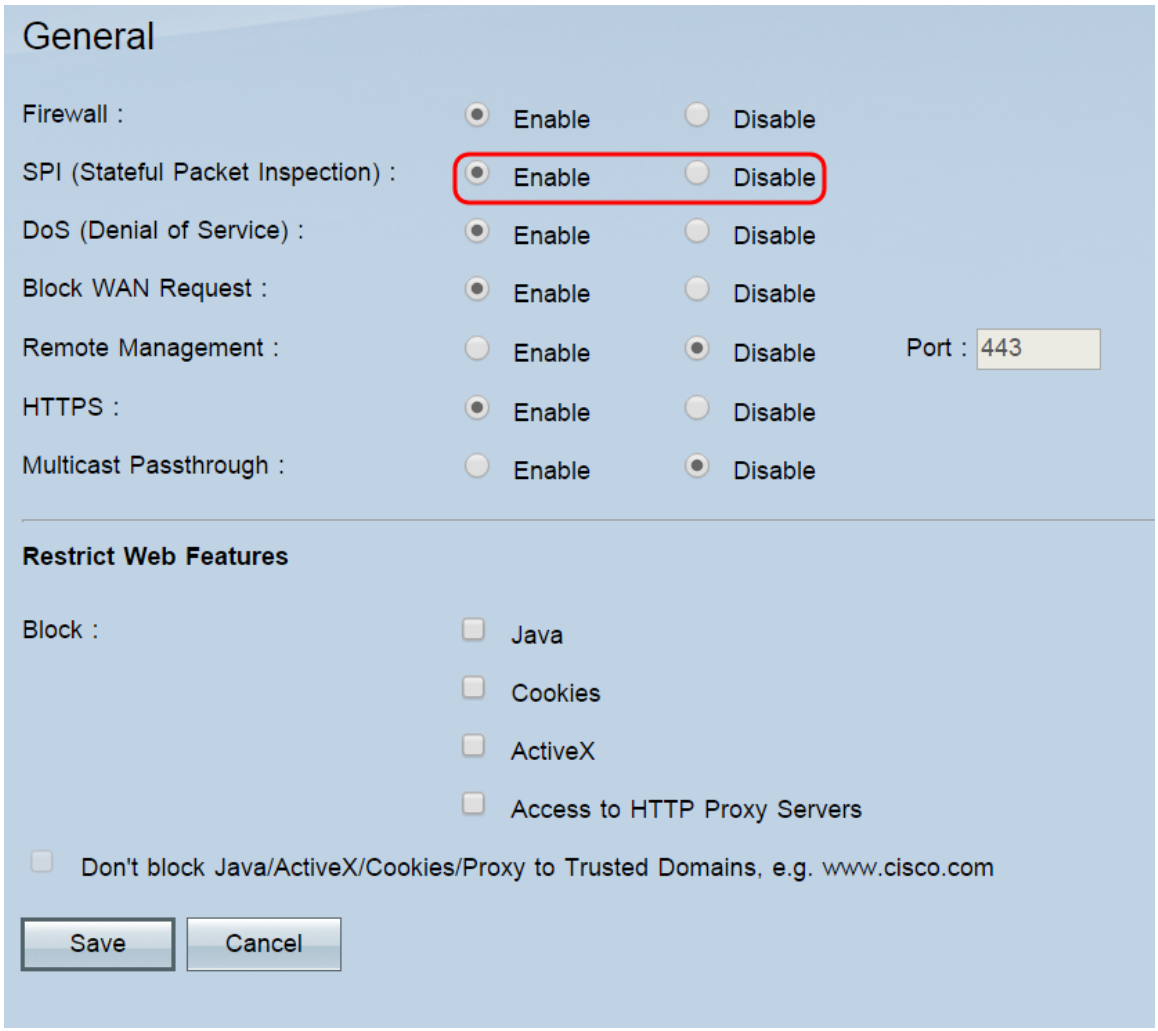
Caractéristiques générales

Étape 1. Dans le champ *Firewall*, sélectionnez une case d'option pour **Enable** ou **Disable** du pare-feu. Le pare-feu est activé par défaut ; sa désactivation n'est pas recommandée. La désactivation du pare-feu désactive également les règles d'accès et les filtres de contenu.

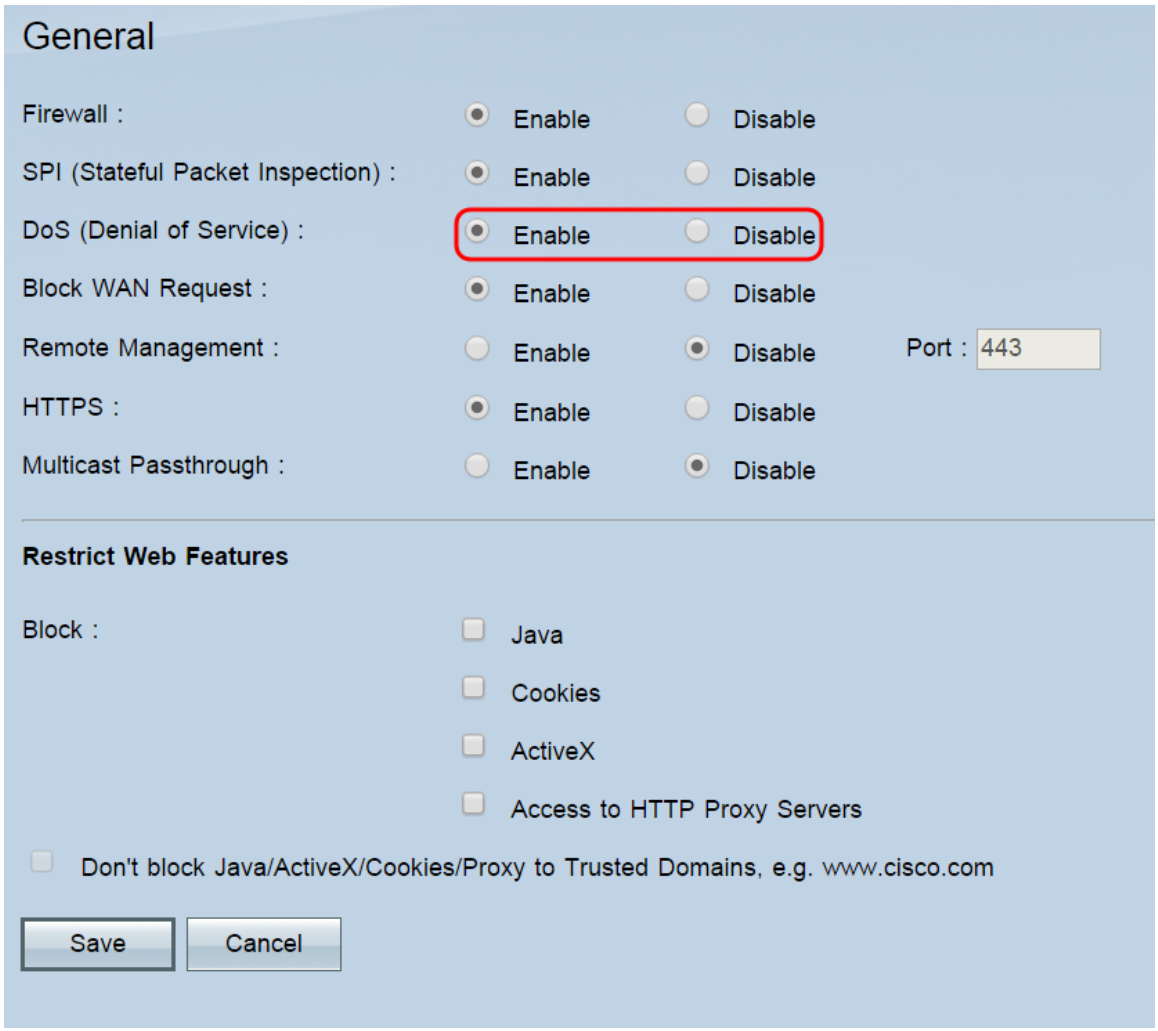


Remarque : si vous souhaitez désactiver le pare-feu et que vous utilisez toujours le mot de passe administrateur par défaut, un message vous avertit que vous devez modifier le mot de passe ; vous ne pourrez pas désactiver le pare-feu tant que vous ne l'aurez pas fait. Cliquez sur **OK** pour passer à la page de mot de passe ou sur **Cancel** pour rester sur cette page.

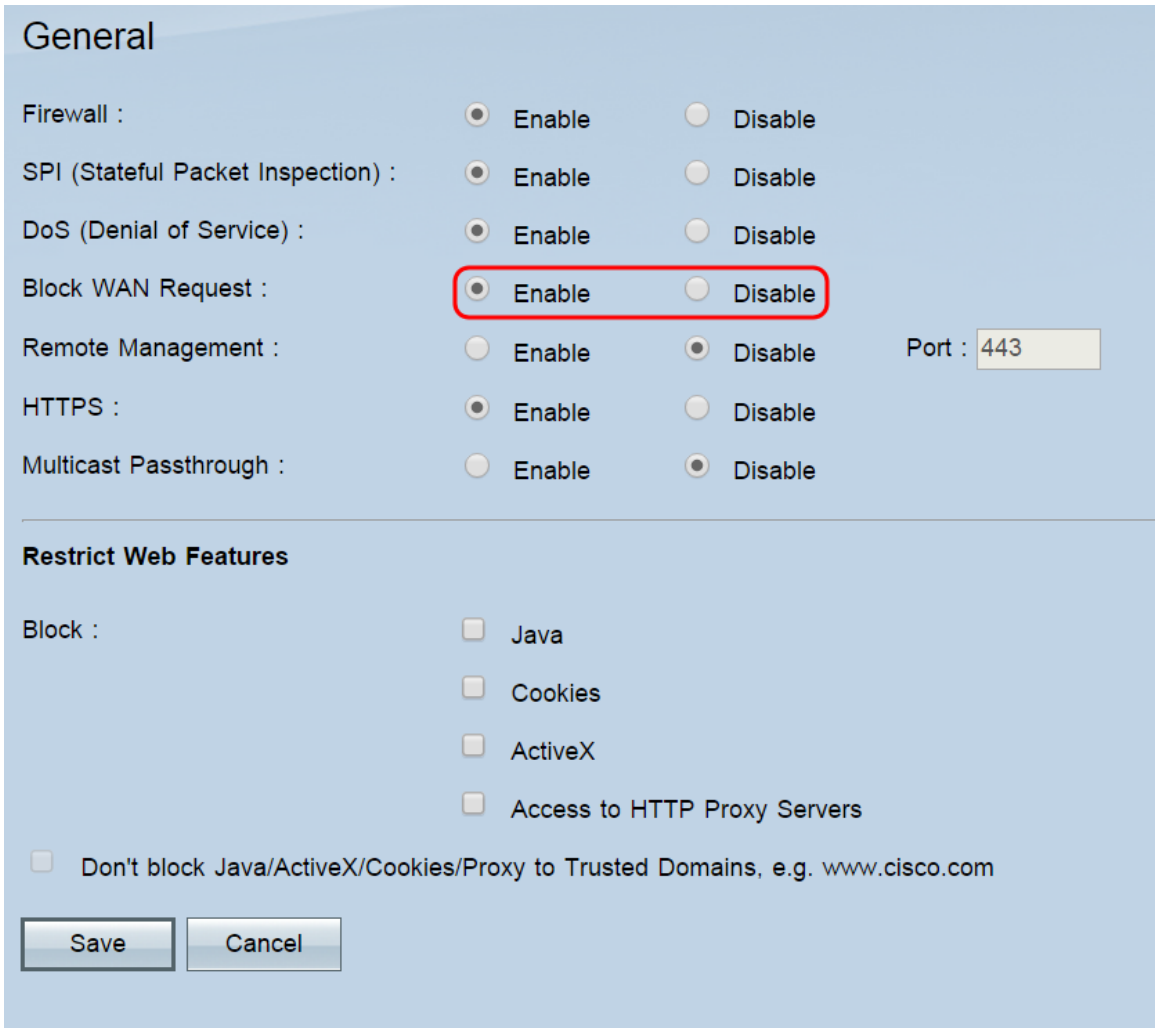
Étape 2. Dans le SPI (Stateful Package Inspection), sélectionnez la case d'option **Enable** ou **Disable**. SPI est activé par défaut. Cette fonctionnalité permet au routeur d'inspecter tous les paquets avant de les envoyer pour traitement. Cette option ne peut être activée que si le pare-feu est activé.



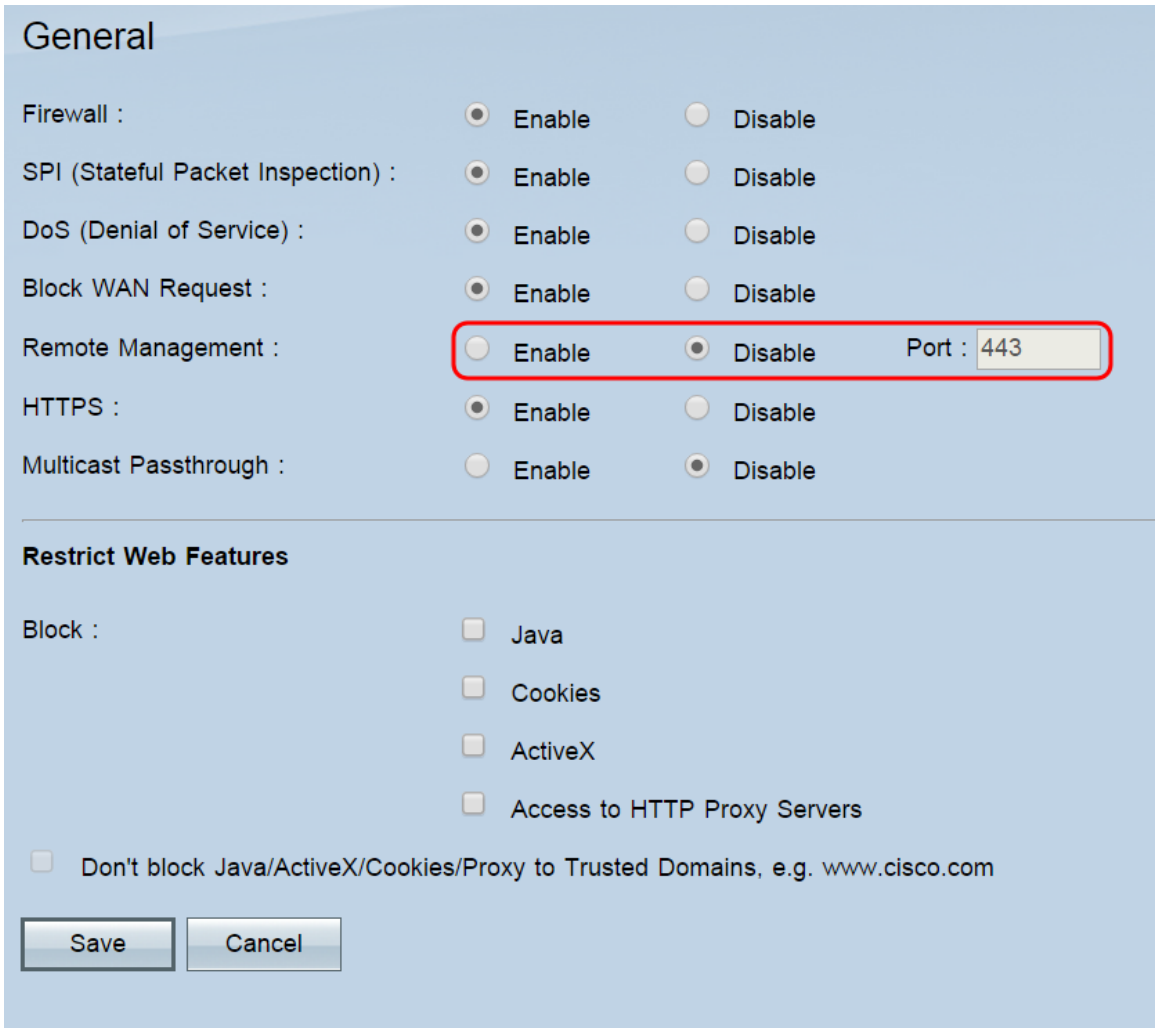
Étape 3. Dans le champ *DoS (Denial of Service)*, sélectionnez la case d'option **Enable** (**Activer)** ou **Disable (Désactiver)**. DoS est activé par défaut. Cette fonctionnalité empêche le réseau interne d'être attaqué par des attaques externes (telles que SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing et les attaques de réassemblage). Cette option ne peut être activée que si le pare-feu est activé.



Étape 4. Dans le champ *Block WAN Request*, sélectionnez la case d'option **Enable** ou **Disable**. L'option Block WAN Request est activée par défaut. Cette fonctionnalité permet au routeur de supprimer les requêtes TCP et ICMP non acceptées du WAN, empêchant ainsi les pirates de trouver le routeur en envoyant une requête ping à l'adresse IP du WAN. Cette option ne peut être activée que si le pare-feu est activé.



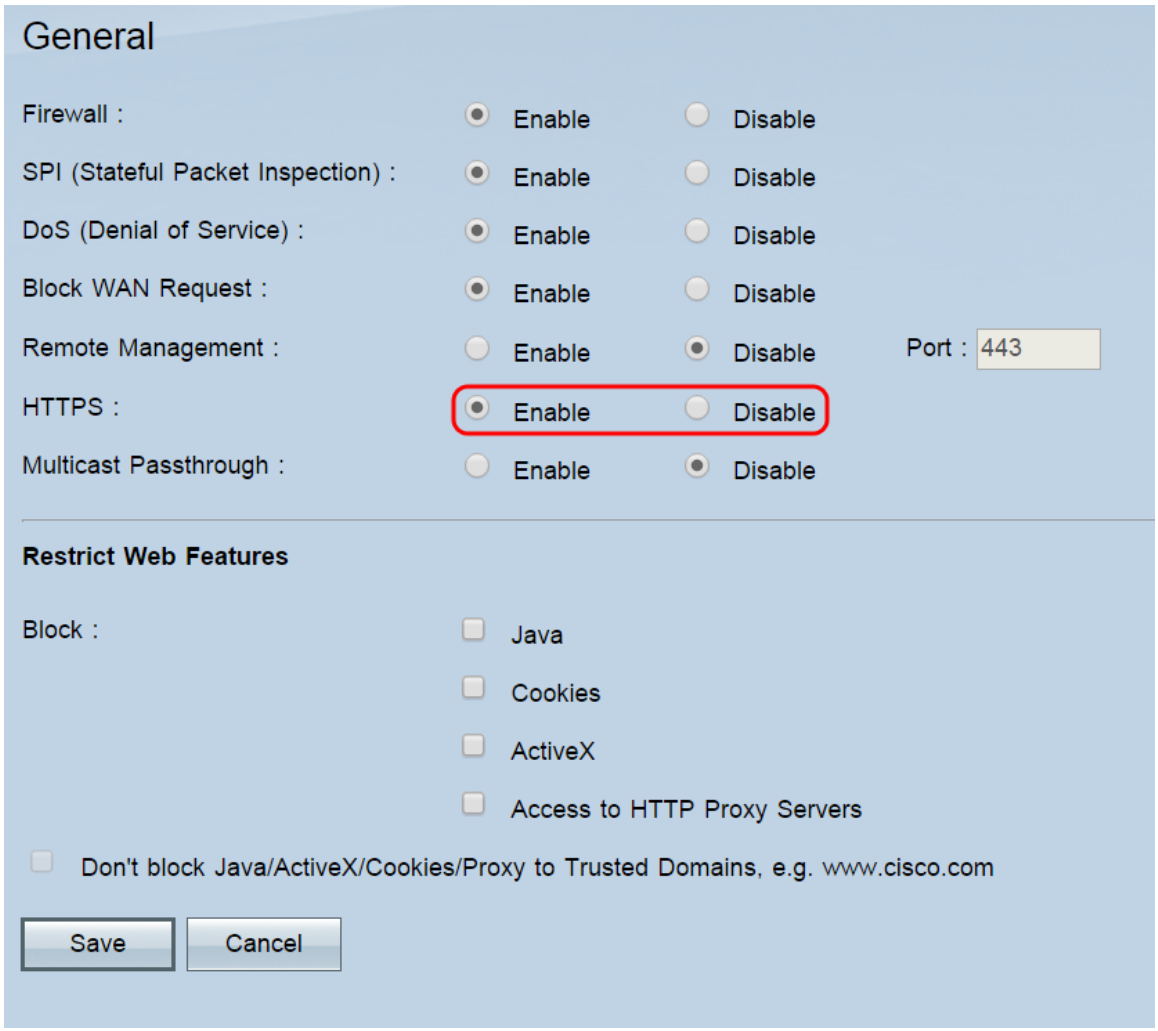
Étape 5. Dans le champ *Remote Management*, sélectionnez la case d'option **Enable** ou **Disable**. La gestion à distance est désactivée par défaut. Cette fonction vous permet de vous connecter à l'utilitaire de configuration Web du routeur depuis n'importe quel emplacement sur Internet. Si vous activez cette fonctionnalité, vous pouvez définir le port utilisé pour les connexions distantes dans le champ Port. Il est défini par défaut à 443.



Remarque : si vous utilisez le mot de passe administrateur par défaut, un message vous avertit que vous devez modifier le mot de passe ; cliquez sur **OK** pour accéder à la page Mot de passe ou sur **Annuler** pour rester sur cette page. La modification du mot de passe est nécessaire pour empêcher les utilisateurs non autorisés dâ€™accéder au routeur avec le mot de passe par défaut.

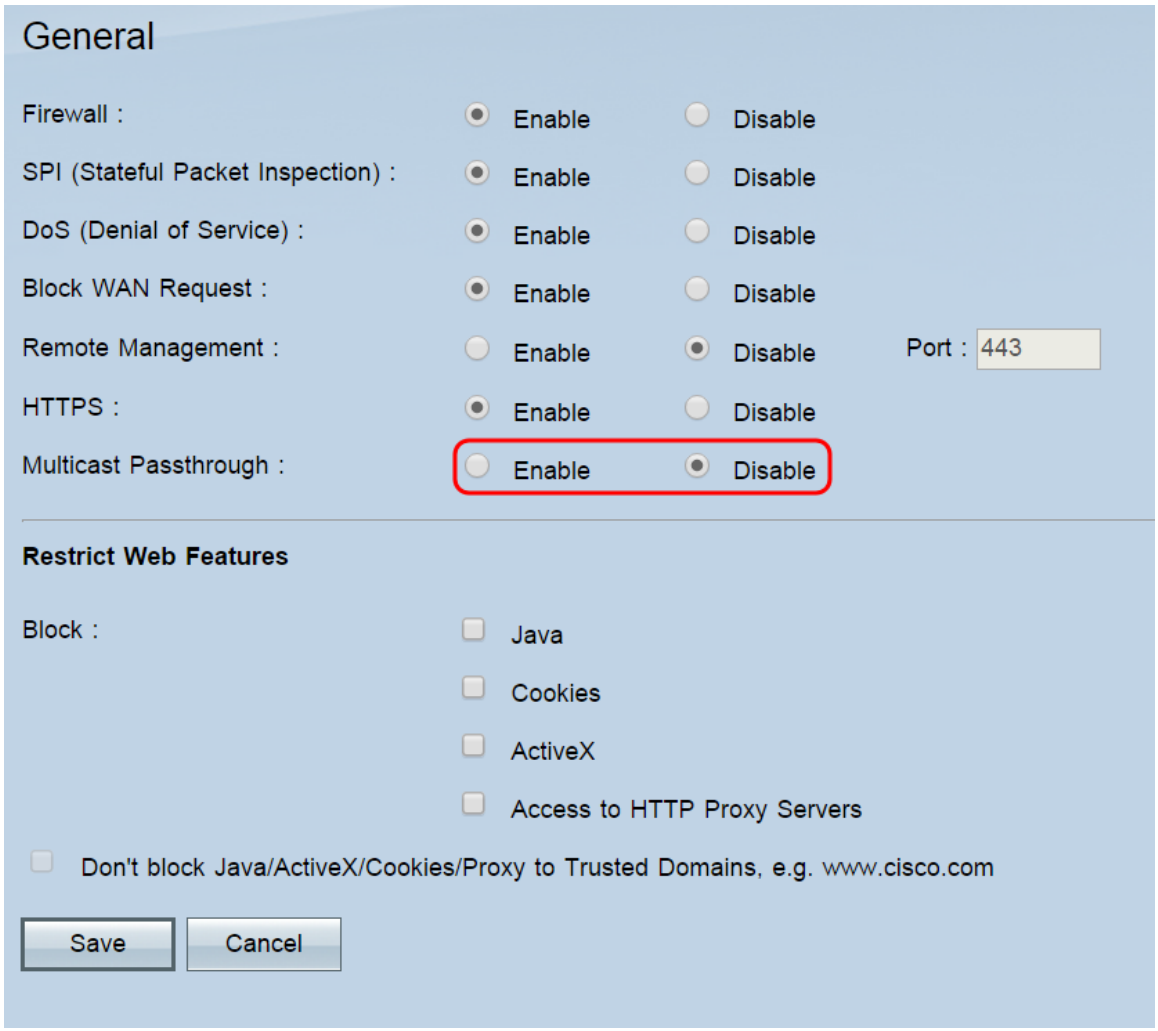
Remarque : lorsque la gestion à distance est activée, vous pouvez accéder à l'utilitaire de configuration Web à partir de n'importe quel navigateur en entrant **http://<adresse IP WAN du routeur>:<port>**. Si HTTPS est activé, entrez **https://<adresse IP WAN du routeur>:<port>** à la place.

Étape 6. Dans le champ *HTTPS*, sélectionnez la case d'option **Enable** (**Activer)** ou **Disable (Désactiver)**. HTTPS est activé par défaut. Cette fonctionnalité permet des sessions HTTP sécurisées.



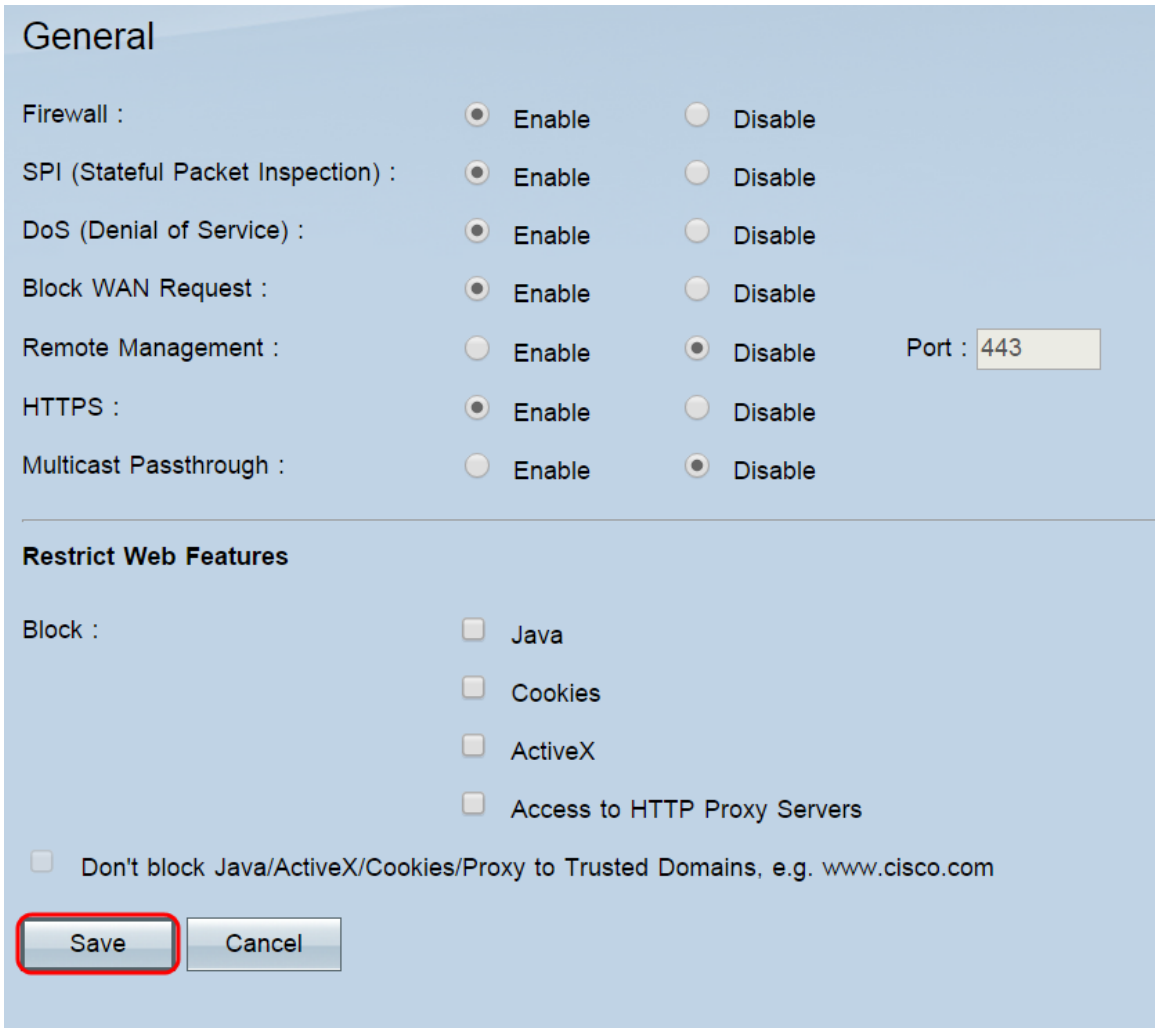
Remarque : si cette fonctionnalité est désactivée, les utilisateurs ne peuvent pas se connecter à l'aide de QuickVPN.

Étape 7. Dans le champ *Multicast Passthrough*, sélectionnez la case d'option **Enable** ou **Disable**. Le mode Passthrough multidiffusion est désactivé par défaut. Cette fonctionnalité permet la diffusion de paquets de multidiffusion IP vers les périphériques LAN correspondants. Elle est utilisée pour les jeux Internet, la vidéoconférence et les applications multimédias.



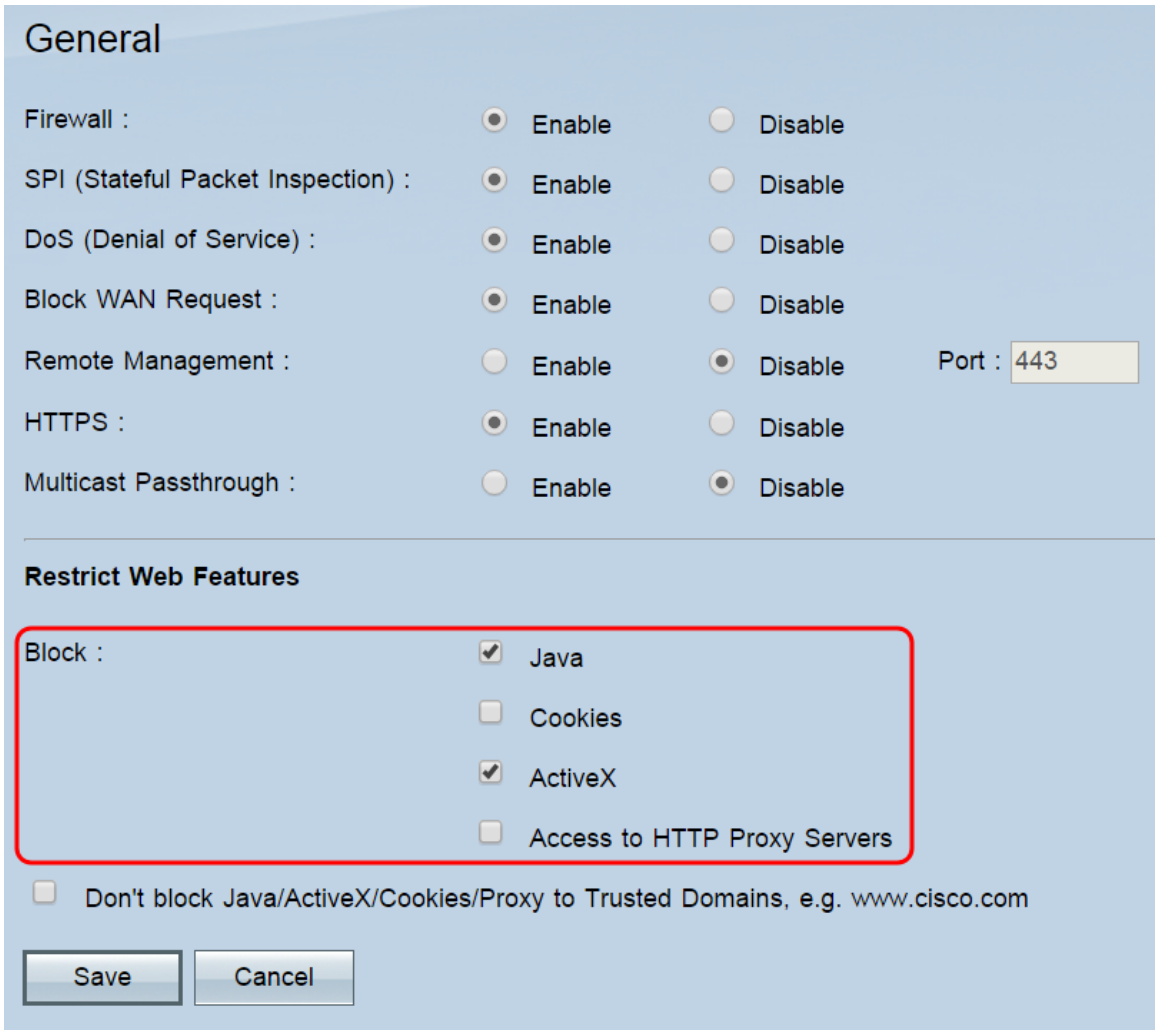
Remarque : les routeurs RV016, RV042, RV042G et RV082 ne prennent pas en charge le passage du trafic de multidiffusion sur un tunnel IPSec.

Étape 8. Cliquez sur **Save**.



Fonctionnalités Web

Étape 1. Dans le champ *Block*, cochez les cases des fonctionnalités Web que vous souhaitez bloquer au niveau du pare-feu. Si vous souhaitez autoriser les fonctionnalités bloquées pour certains domaines, ces domaines peuvent être ajoutés à une liste d'exceptions à l'étape 2. Aucune des fonctionnalités n'est bloquée par défaut.



Les options sont les suivantes :

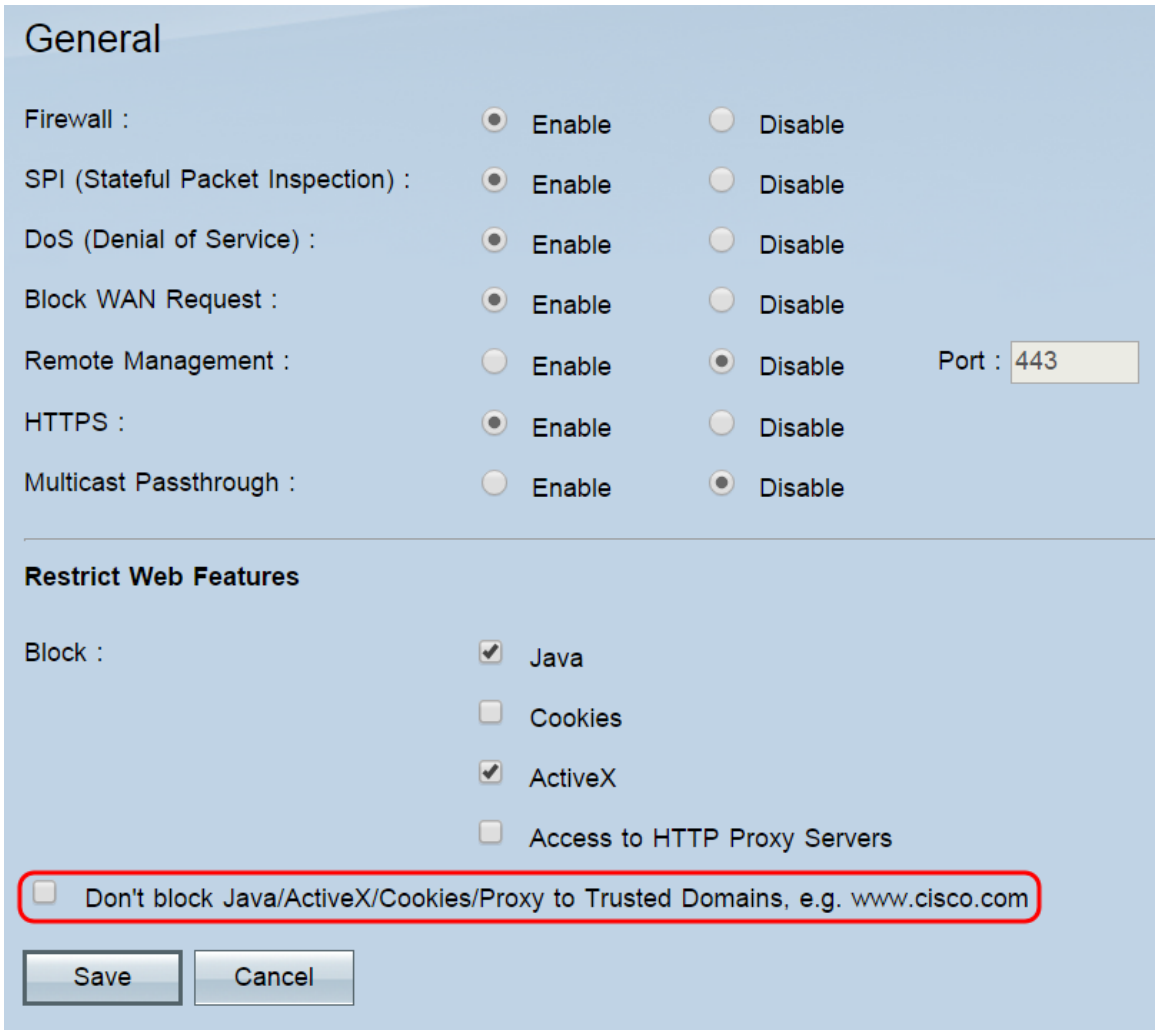
· Java â€" Java est un langage de programmation pour les sites Web. Si vous cochez cette case, les applets Java (petits programmes intégrés dans les pages Web mais exécutés en dehors du navigateur Web) seront bloqués, mais les sites Web qui utilisent cette fonctionnalité risquent de ne pas fonctionner correctement.

· Cookies : un cookie est une donnée qu'un site Web stocke localement sur le PC d'un utilisateur. Le blocage des cookies peut entraîner un comportement incorrect des sites Web qui s'appuient sur eux.

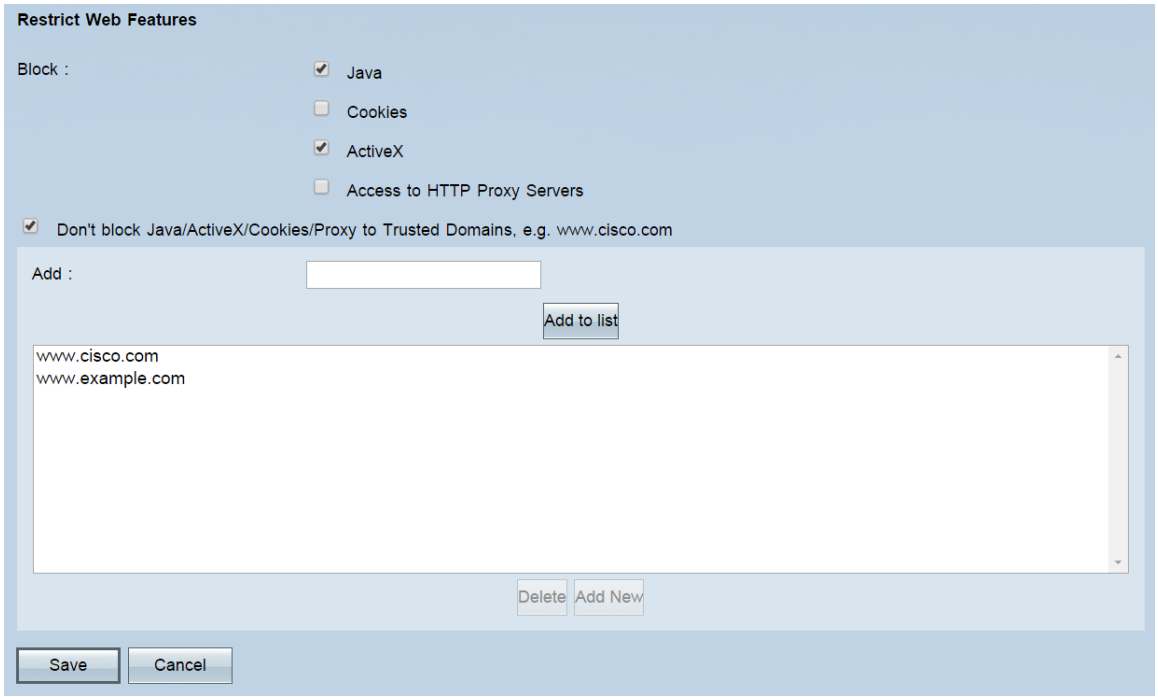
· ActiveX : ActiveX est une infrastructure logicielle développée par Microsoft. Ce cadre peut être utilisé pour exécuter certaines parties de pages Web. Si vous cochez cette case, ces composants seront bloqués, mais les sites Web qui utilisent ActiveX risquent de ne pas fonctionner correctement.

· Access to HTTP Proxy servers : cochez cette case si vous souhaitez bloquer l'accès aux serveurs proxy HTTP. L'utilisation de serveurs proxy WAN peut compromettre la sécurité du routeur.

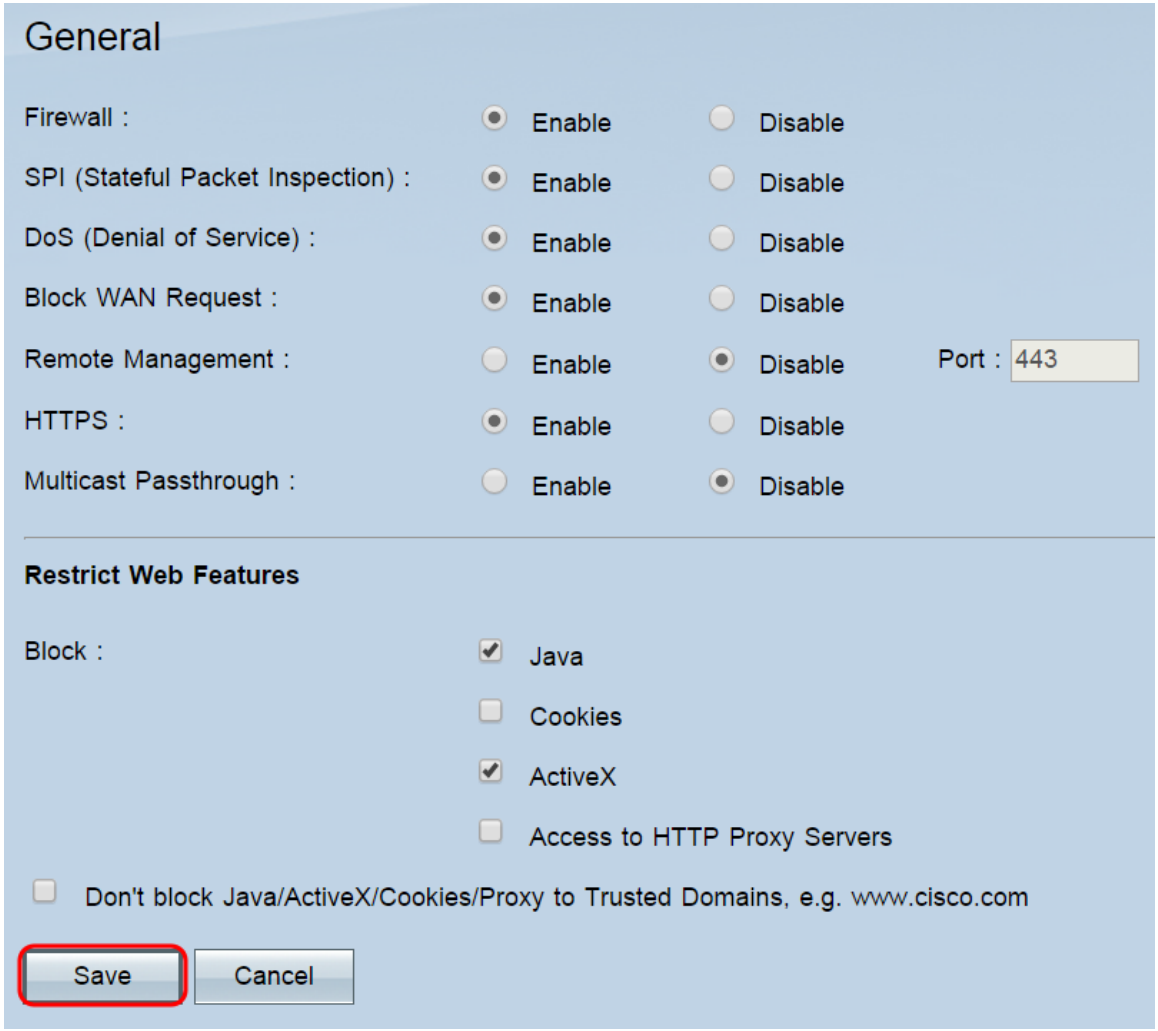
Étape 2. Cochez la case **Ne pas bloquer Java/ActiveX/Cookies/Proxy vers domaines approuvés** pour ouvrir la liste des domaines approuvés, où vous pouvez ajouter ou supprimer des domaines où les fonctionnalités Web bloquées sont autorisées. Ce champ n'est pas coché par défaut et n'est disponible que si vous avez coché une case précédente pour bloquer une fonction. Si cette case n'est pas cochée, les fonctionnalités sont bloquées pour tous les sites Web.



Étape 3. (Facultatif) Si vous avez coché la case **Ne pas bloquer Java/ActiveX/Cookies/Proxy vers les domaines approuvés**, une liste des domaines approuvés s'affiche. Pour ajouter un domaine à la liste, entrez-le dans le champ *Add* et cliquez sur **Add to List**. Si vous voulez modifier un domaine existant, cliquez dessus dans la liste, puis modifiez-le dans le champ *Add*, puis cliquez sur **Update**. Pour supprimer un domaine de la liste, cliquez dessus dans la liste, puis cliquez sur **Supprimer**.



Étape 4. Cliquez sur **Save**.



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.