Paramètres généraux du pare-feu sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Un pare-feu protège un réseau interne d'un réseau externe tel qu'Internet. Les pare-feu sont essentiels à la sécurité du réseau. Plusieurs paramètres différents sont disponibles pour activer ou désactiver des services spécifiques en fonction de vos besoins en matière de sécurité.

L'objectif de cet article est de montrer comment activer ou désactiver les paramètres de pare-feu généraux sur les routeurs VPN RV016, RV042, RV042G et RV082.

Périphériques pertinents

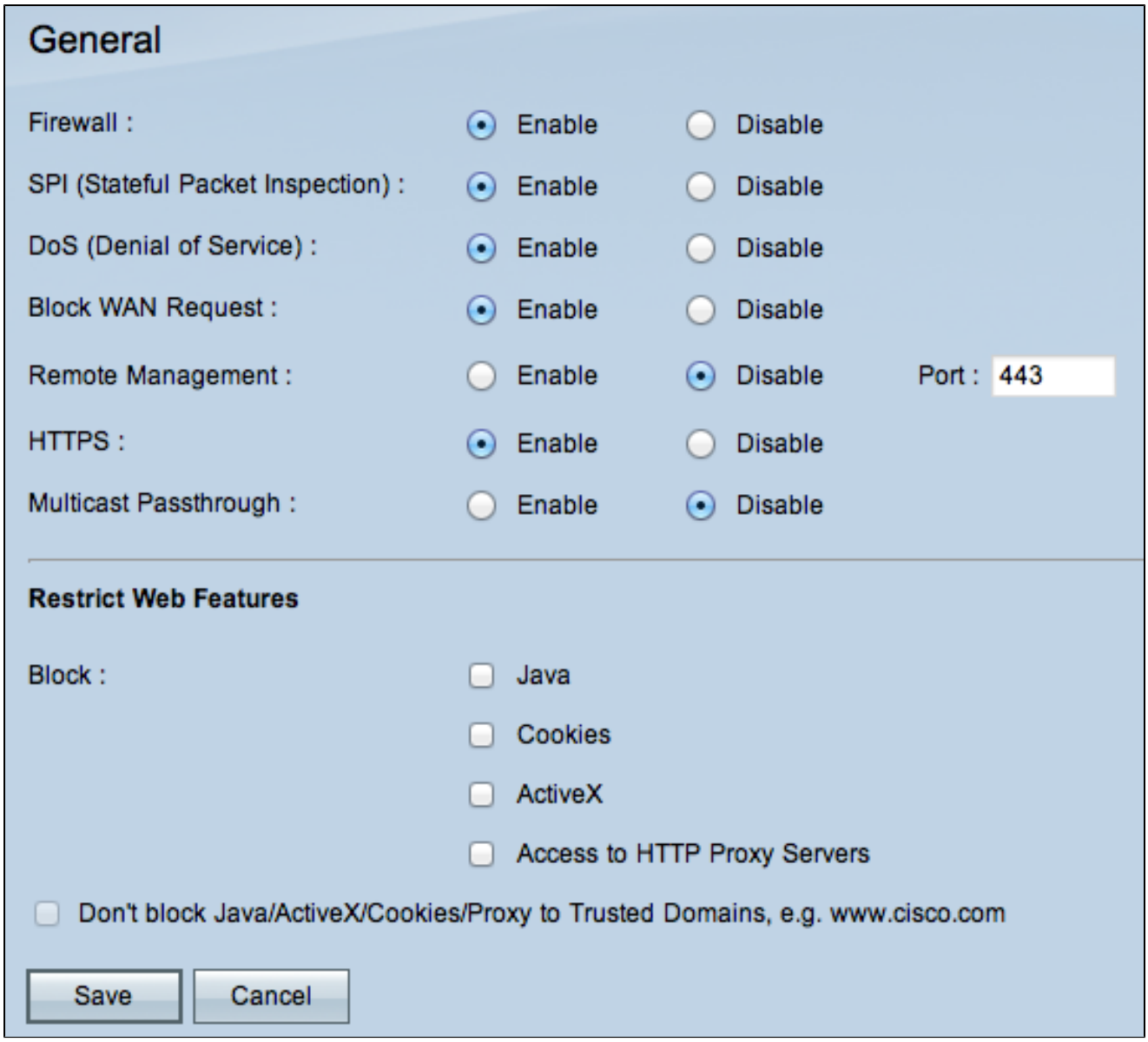
- RV016
- RV042
- RV042G
- RV082

Version du logiciel

- v 4.2.1.02

Paramètres généraux du pare-feu

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



Étape 2. Cliquez sur la case d'option Enable ou Disable pour activer ou désactiver les paramètres disponibles dans le pare-feu selon les besoins de l'utilisateur.

Les champs suivants sont décrits comme suit :

· Pare-feu : lorsque cette fonctionnalité est activée, le routeur effectue une inspection approfondie des paquets sur tout le trafic qui passe par ce routeur et abandonne les paquets qui ne suivent pas le comportement de protocole prédéfini.

· SPI (Stateful Packet Inspection) : le pare-feu du routeur utilise le protocole SPI (Stateful Packet Inspection) pour analyser le trafic au niveau du pare-feu. Il surveille l'état des connexions réseau, telles que les flux TCP et les communications UDP. Le pare-feu distingue les paquets légitimes pour les différents types de connexions et seuls les paquets qui correspondent à une connexion active connue sont autorisés par le pare-feu, tous les autres sont rejetés.

· Dos (Denial of Service) : lorsque cette fonctionnalité est activée, le routeur empêche les attaques DOS (Denial of Service) provenant d'Internet. Les attaques par déni de service (DOS) entraînent une occupation du processeur de votre routeur, qui ne peut donc pas fournir de services au trafic normal.

· Block WAN Request : lorsque cette option est activée, le routeur ignore les requêtes PING provenant d'Internet et semble donc être masqué. Cela permet d'assurer la sécurité en dissimulant les ports réseau de sorte que les intrus n'aient pas facilement accès au réseau.

· Gestion à distance : lorsque cette fonctionnalité est activée, le routeur permet d'accéder à l'utilitaire de configuration Web à partir d'Internet. Saisissez le numéro de port qui sera ouvert aux hôtes côté WAN. Le paramètre par défaut est 443. Ce port doit être spécifié lorsque l'utilisateur établit une connexion à distance.

· HTTPS : lorsqu'il est activé, l'utilitaire de configuration Web est accessible via une session HTTPS côté WAN au lieu du protocole HTTP standard. Votre session Web à distance sera protégée par des algorithmes de chiffrement SSL. Si la fonctionnalité HTTPS est désactivée, les utilisateurs ne peuvent pas se connecter via QuickVPN. Si elle est désactivée, elle utilise une connexion HTTP moins sécurisée.

· Multicast Passthrough : si un proxy IGMP s'exécute actuellement sur le routeur, lorsque Multicast Passthrough est activé, le routeur autorise le trafic IP multidiffusion à entrer à partir d'Internet.

Remarque : pour désactiver le pare-feu, vous devez modifier le mot de passe par défaut de l'administrateur. Les champs SPI (Stateful Packet Inspection), DoS (Denial of Service), Block WAN Request et Remote Management sont grisés.

Étape 3. Dans la zone Restreindre les fonctionnalités Web, cochez une ou toutes les cases pour restreindre la fonctionnalité correspondante.

· Java — Java est un langage de programmation pour les sites Web. Pour bloquer Java, cochez la case Java. Si vous refusez Java, il se peut que vous ne puissiez pas accéder aux sites Internet écrits dans ce langage de programmation. Il est donc plus sûr d'aller de l'avant et de bloquer les applets Java si le périphérique connecté au routeur n'a pas besoin d'accéder aux sites Web créés avec Java. D'autre part, les cybercriminels utilisent Java comme partie intégrante de leur attaque, qui consiste à déterminer le système d'exploitation et à lancer une attaque spécifiée par le système d'exploitation lorsque vous visitez des sites Web infectés par un programme malveillant. Par exemple, lorsque vous visitez un site Web piraté, un fichier JAR (Java Archive) est déclenché qui vous demande d'exécuter sa fonction, mais secrètement il est utilisé pour déterminer le système d'exploitation de l'ordinateur.

· Cookies — Un cookie est une donnée stockée sur le PC et utilisée par les sites Internet lorsque les utilisateurs interagissent avec eux. Pour bloquer les cookies, cochez la case Cookies. Si vous souhaitez bloquer les cookies, les sites Web ne peuvent enregistrer aucune information de visite précédente lorsqu'ils sont accessibles depuis l'appareil. L'avantage est que les cookies malveillants (cookies de suivi tiers) ne sont pas enregistrés, ce qui présente un risque pour la sécurité.

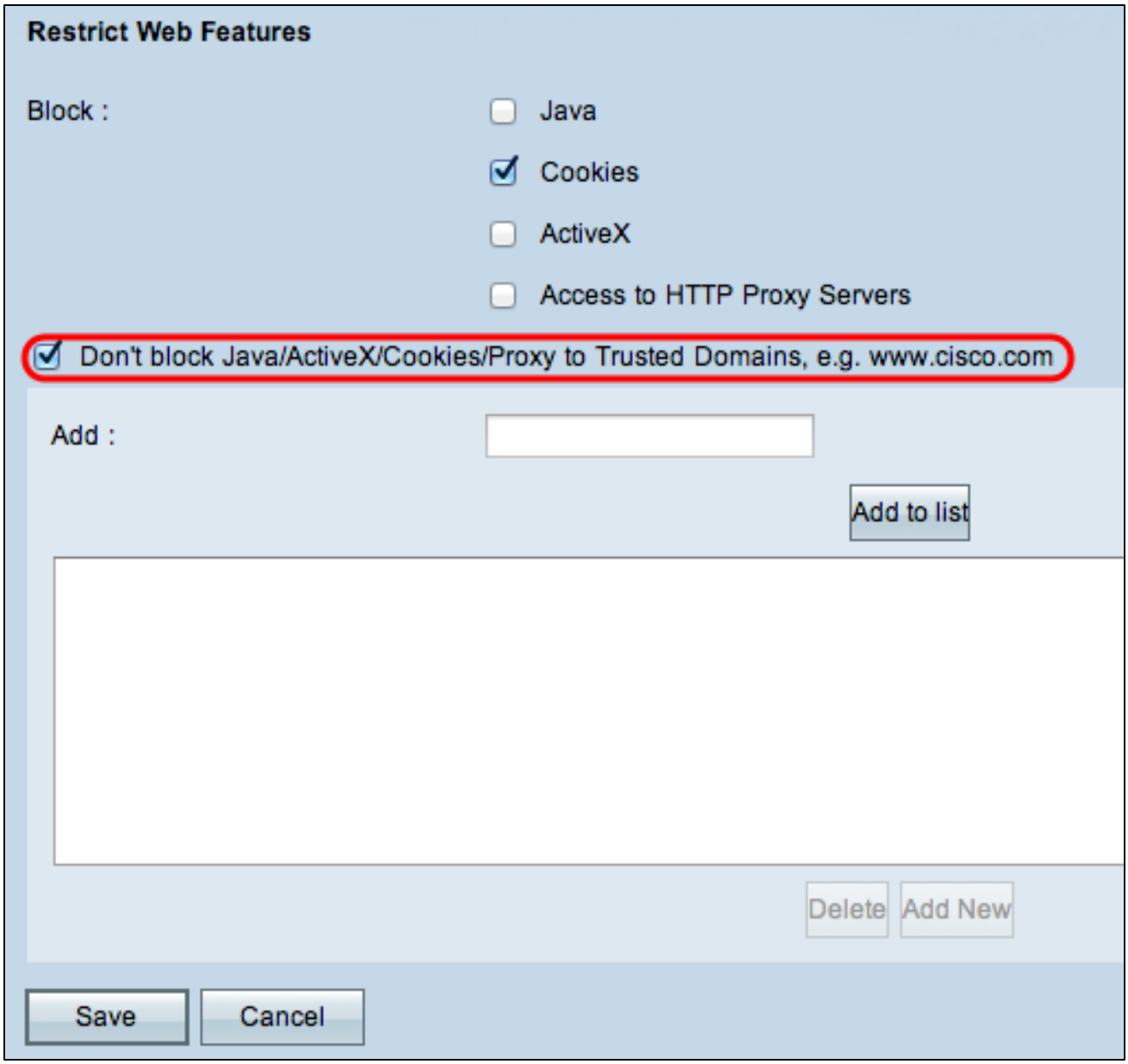
· ActiveX : ActiveX est un composant logiciel de Microsoft Windows qui peut être utilisé pour développer des applications ou contrôler de petits programmes tels que les modules complémentaires utilisés sur des sites Internet. Si vous autorisez ActiveX, il peut vous aider à améliorer votre expérience lorsque vous naviguez ; il permet aux sites Web d'exécuter des animations et d'autres programmes similaires. D'autre part, il y a un risque potentiel si vous visitez des pages Web qui contiennent un logiciel ActiveX malveillant développé par des cybercriminels qui peut causer des dommages à l'ordinateur. Pour bloquer ActiveX, cochez la case ActiveX. Si vous bloquez ActiveX, vous risquez de rencontrer des problèmes si vous souhaitez accéder à certains sites Internet qui utilisent ActiveX pour effectuer des tâches.

· Access to Proxy HTTP Server : si vous souhaitez naviguer anonymement sur un serveur proxy et refuser l'accès au serveur proxy, cochez la case Access to Proxy HTTP Server. Les serveurs proxy HTTP masquent les détails des utilisateurs finaux aux pirates. Ils travaillent comme intermédiaires et vous n'accédez donc pas directement à Internet. Toutefois, si les utilisateurs locaux ont accès aux serveurs proxy WAN, ils peuvent contourner les filtres de contenu sur le routeur et accéder aux sites Internet bloqués par le routeur.

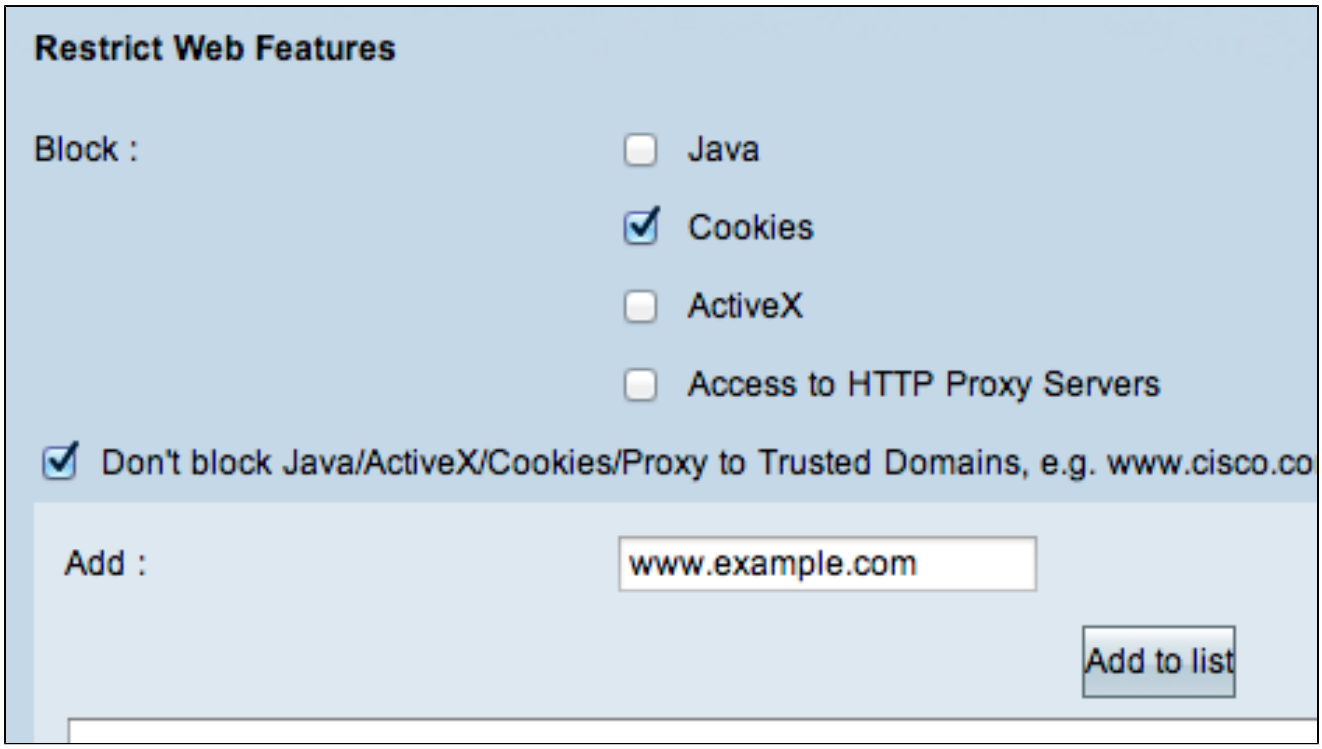
Étape 4. Cliquez sur Save afin d'enregistrer les paramètres.

Ajouter des domaines approuvés

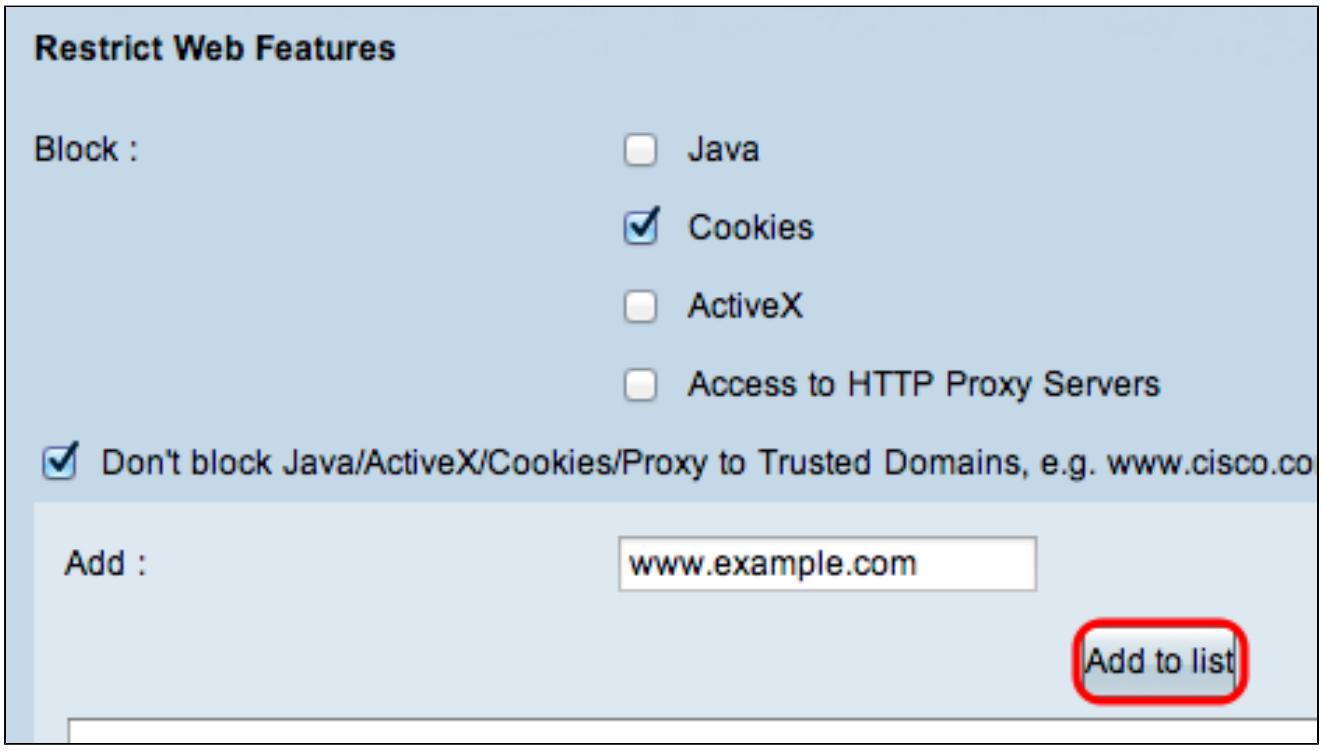
Même si l'une des fonctionnalités Web peut être bloquée, l'utilisateur peut autoriser l'activation de ces fonctionnalités pour des domaines approuvés spécifiés.



Étape 1. Cochez le bouton Ne pas bloquer Java/ActiveX/Cookies/Proxy vers domaines approuvés. Cette option n'est disponible que si l'utilisateur a choisi de bloquer l'une des fonctionnalités Web de l'étape 3 des Paramètres généraux du pare-feu.



Étape 2. Dans le champ Add, saisissez le domaine à ajouter à la liste des domaines approuvés.

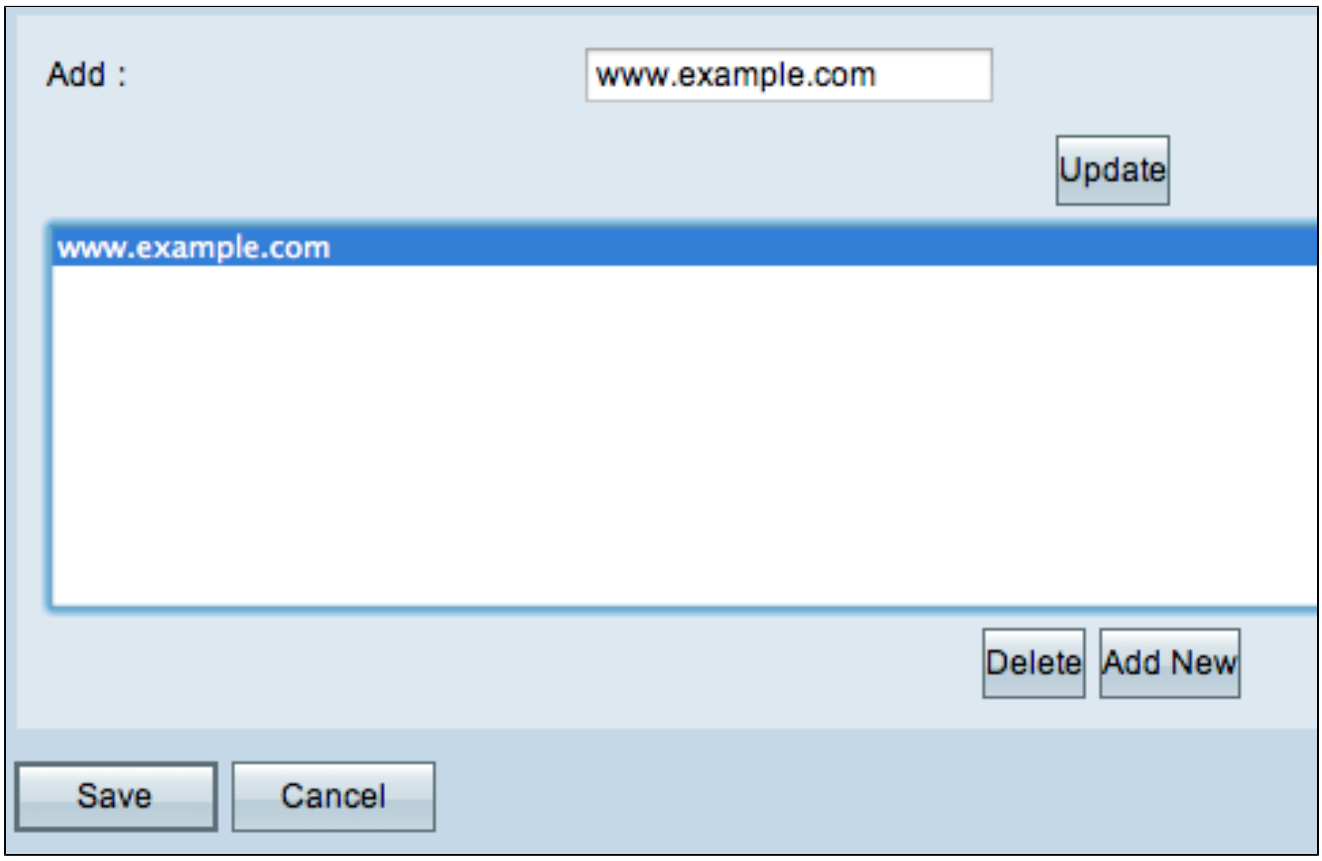


Étape 3. Cliquez sur Ajouter à la liste. Le domaine est ajouté à la liste de confiance.

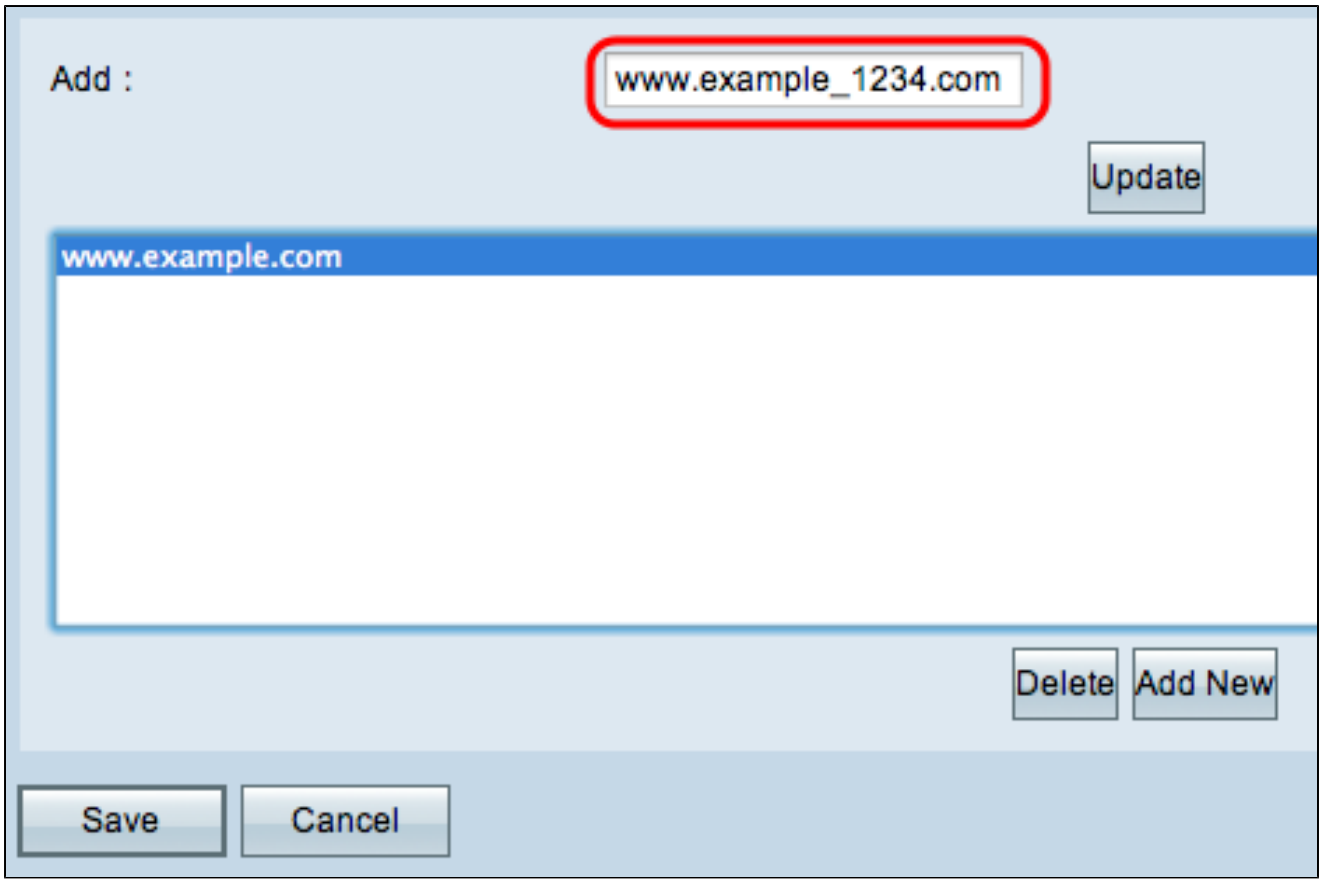
Étape 4. Cliquez sur Save pour enregistrer les modifications.

Mettre à jour un domaine approuvé

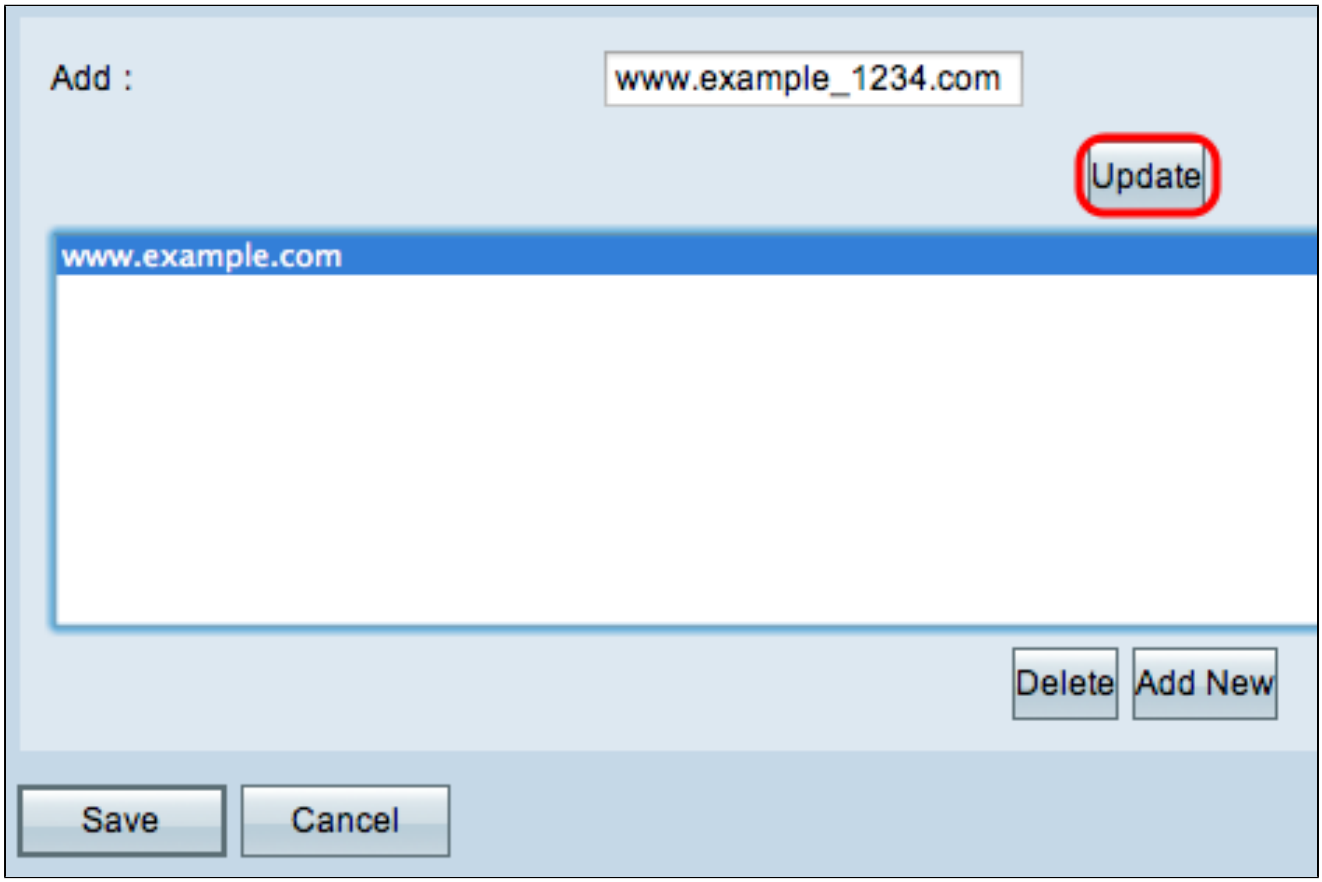
Cette section explique à l'utilisateur comment modifier un domaine approuvé.



Étape 1. Sélectionnez le domaine que vous souhaitez modifier dans la liste des domaines approuvés.



Étape 2. Dans le champ Add, saisissez le nom de domaine mis à jour pour le domaine requis.

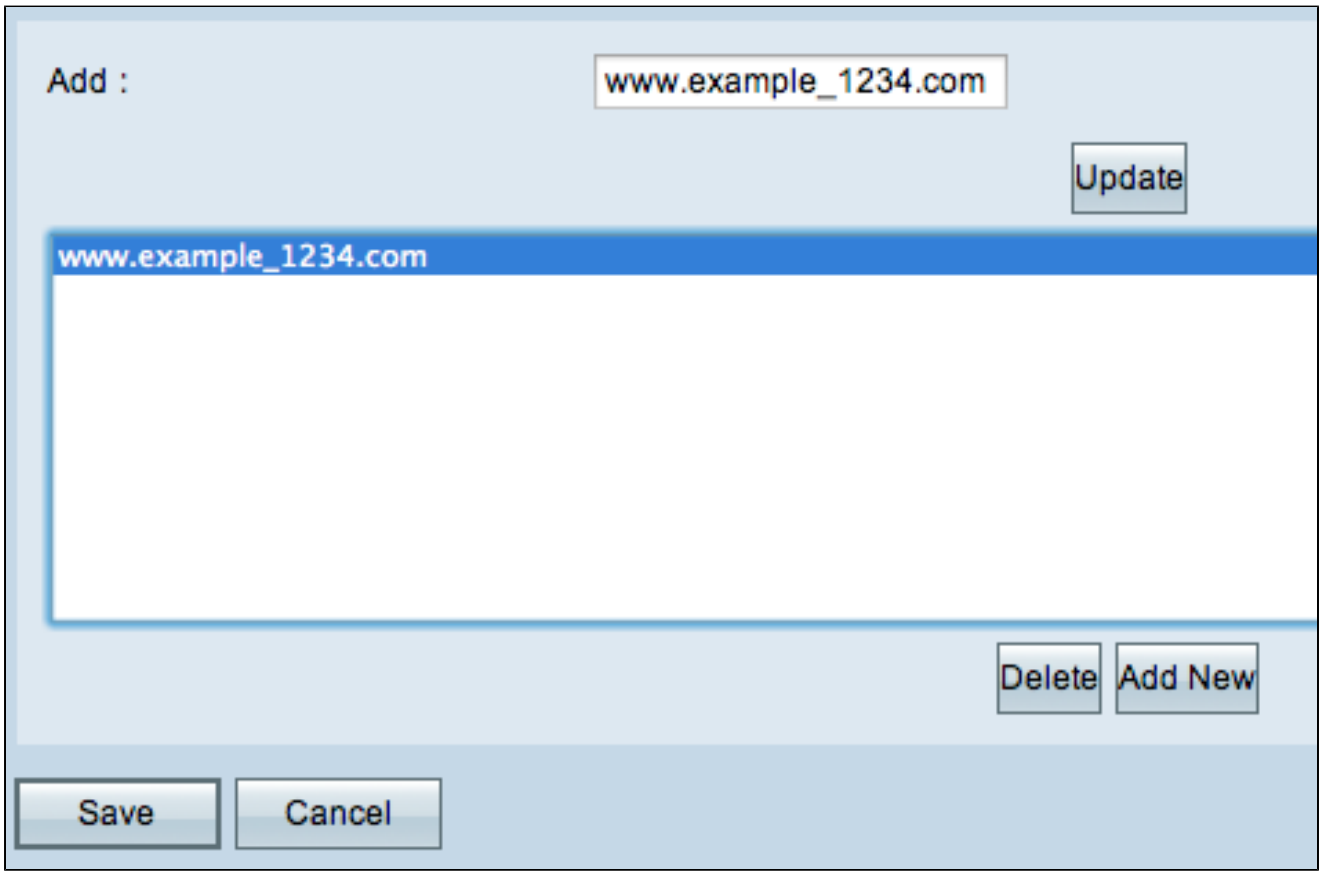


Étape 3. Cliquez sur Update.

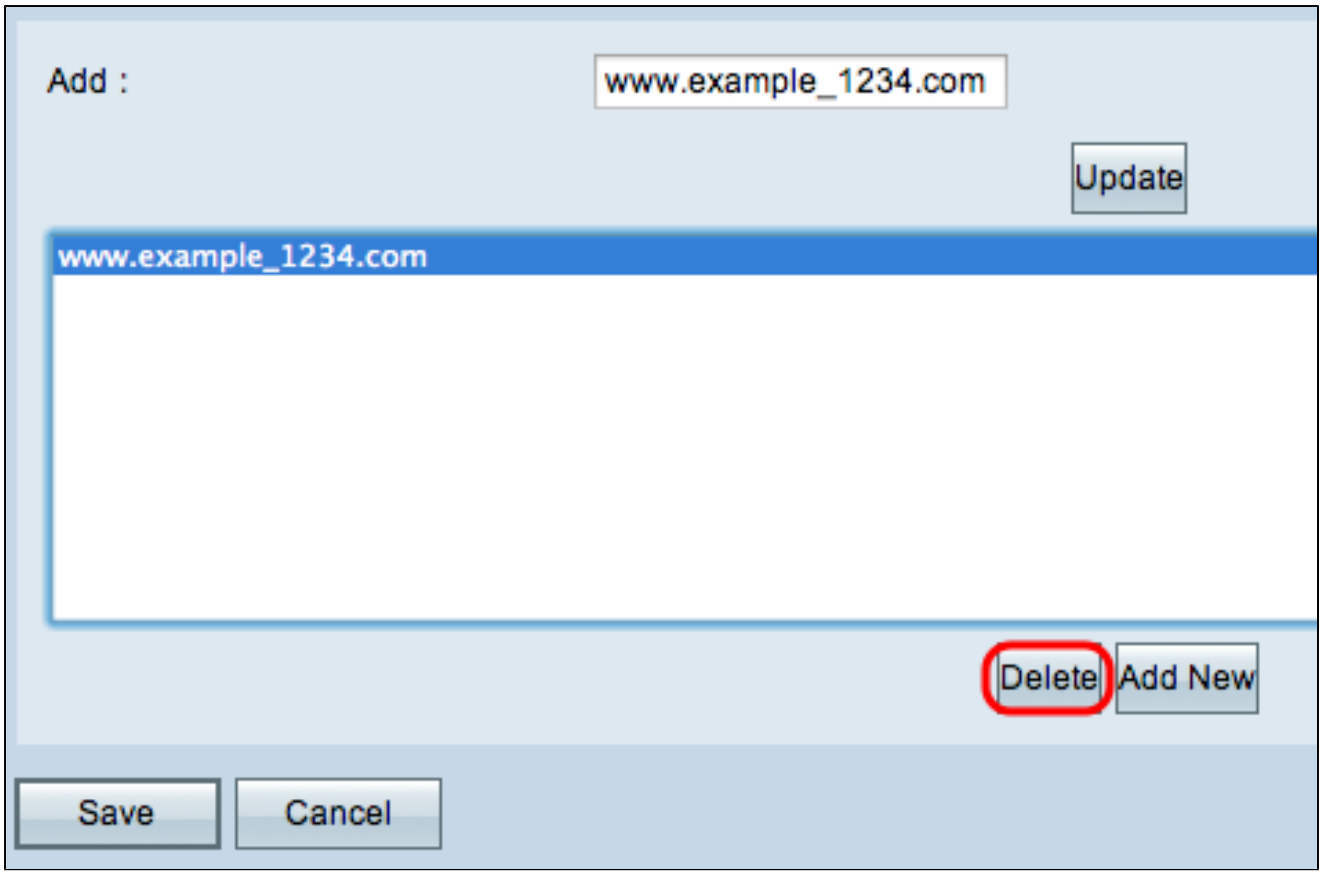
Étape 4. Cliquez sur Save pour enregistrer les modifications.

Supprimer un domaine approuvé

Cette section explique à l'utilisateur comment supprimer un domaine approuvé.



Étape 1. Sélectionnez le domaine que vous souhaitez supprimer.



Étape 2. Cliquez sur Delete. Le domaine est supprimé.

Étape 3. Cliquez sur Save pour enregistrer 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.