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

Objectif

Un Pare-feu protège un réseau interne contre un réseau externe tel que l'Internet. Les Pare-feu sont essentiels à la sécurité des réseaux. Plusieurs différentes configurations sont disponibles que puisse activer ou désactiver des services spécifiques basés sur vos besoins de Sécurité.

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

Périphériques applicables

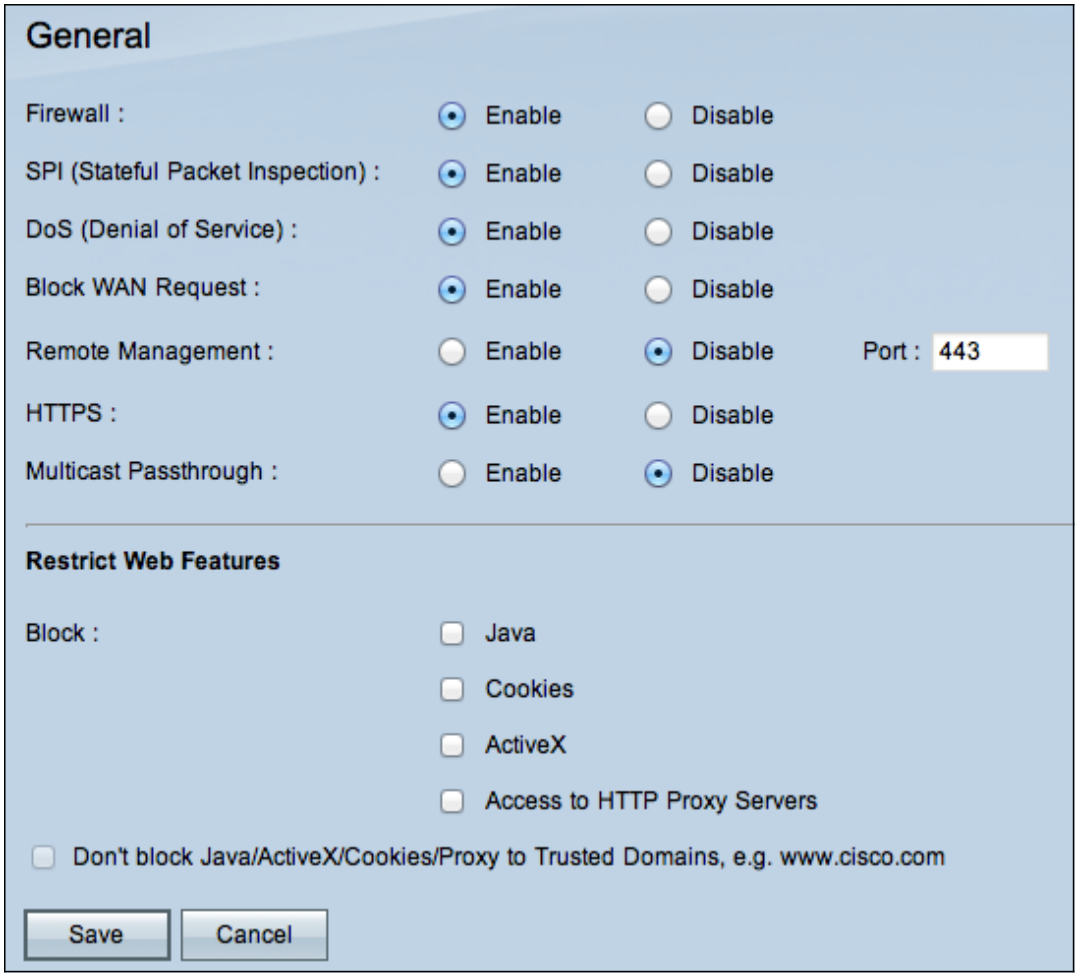
- RV016
- RV042
- RV042G
- RV082

Version de logiciel

- v4.2.1.02

Paramètres du pare-feu généraux

Étape 1. Ouvrez une session l'utilitaire de configuration de routeur et choisissez le **Pare-feu > le général**. La page *générale* s'ouvre :



Étape 2. Cliquez sur l'**enable** ou **désactivez la** case d'option pour activer ou désactiver les configurations disponibles dans le Pare-feu selon des exigences de l'utilisateur.

Les champs suivants sont décrits comme suit :

• Pare-feu — Quand cette caractéristique est activée, le routeur exécutera l'inspection profonde de paquet sur tout le trafic qui passe par ce routeur et relâche les paquets qui ne suivent pas le comportement de protocole de prédéfinis.

• SPI (Stateful Packet Inspection) — Le routeur pare-feu emploie Stateful Packet Inspection (SPI) pour passer en revue le trafic au Pare-feu. Il surveille l'état de connexions réseau telles que des flots de TCP et la transmission d'UDP. Le Pare-feu distingue les paquets légitimes pour différents types de connexions et seulement des paquets qui apparient une connexion active connue sont autorisés par le Pare-feu, tous les autres sont rejetés.

• DOS (Déni de service) — Quand cette caractéristique est activée, le routeur empêchera les attaques DOS (Déni de service) qui proviennent l'Internet. Les attaques DoS rendent la CPU de votre routeur occupée de sorte qu'elle ne puisse pas fournir des services au trafic habituel.

• Demande BLÊME de bloc — Quand ceci est activé, le routeur ignorera des requêtes pings de l'Internet ainsi il semblera être masqué. Ceci aide à fournir la Sécurité en cachant les ports de réseau ainsi les transgresseurs n'ont pas l'accès au réseau facilement.

• Gestion à distance — Quand cette caractéristique est activée, le routeur permet l'utilitaire de configuration Web à accéder à de l'Internet. Introduisez le numéro de port qui sera ouvert aux hôtes du côté WAN. La valeur par défaut est 443. Ce port doit être spécifié quand l'utilisateur établit une connexion distante.

• HTTPS — Une fois activé, l'utilitaire de configuration Web peut être accédé à par une session HTTPS du côté WAN au lieu du HTTP régulier. Ceci aura votre session Web distante protégée par des algorithmes de ssl encryption. Si la caractéristique HTTPS est handicapée les utilisateurs ne peuvent pas se connecter par l'utilisation de QuickVPN. Si désactivé, il utilise moins de connexion de HTTP sécurisé.

• Fonction émulation de Multidiffusion — Si un proxy IGMP fonctionne actuellement sur le routeur, quand la fonction émulation de Multidiffusion est activée le routeur permettra au trafic de Protocole IP Multicast pour entrer de l'Internet.

Remarque: Pour désactiver le Pare-feu, le mot de passe administrateur doit être changé du par défaut. Les champs *BLÊMES SPI* (Stateful Packet Inspection), *DOS* (Déni de service), de *demande de bloc* et de *gestion à distance* sont grisés.

Étape 3. Dans la région de caractéristiques de Web de limiter, vérifiez tout ou une partie des cases pour limiter la caractéristique correspondante.

• Javas — Java est un langage de programmation pour des sites Web. Pour bloquer Javas, cochez la case de **Javas**. Si vous refusez Javas, alors vous ne pouvez pas pouvoir accéder à des sites Internet écrits en ce langage de programmation, ainsi il est sûr d'avancer et de bloquer des applet Java si le périphérique connecté au routeur n'a pas besoin d'accéder aux sites Web créés avec Javas. D'autre part, les Cyber-criminels utilisent Javas en tant que partie intégrante de leur attaque, qui est de déterminer le SYSTÈME D'EXPLOITATION et lance une attaque Système d'exploitation-spécifiée quand vous visitez les sites Web qui sont infectés par malware. Par exemple, quand vous visitez un site Web entaillé, un fichier de POT (archives de Javas) est déclenché qui te demande de remplir sa fonction mais secrètement il est utilisé pour déterminer le SYSTÈME D'EXPLOITATION de l'ordinateur.

• Témoins — Un Témoin est des données enregistrées sur le PC et utilisées par des sites Internet quand les utilisateurs interagissent avec eux. Pour bloquer des Témoins, cochez la case de **Témoins**. Si vous souhaitez bloquer des Témoins, alors les sites Web ne peuvent sauvegarder aucune informations précédentes de visite une fois accédés à du périphérique. L'avantage est que des Témoins malveillants (tiers dépistant des Témoins) ne sont pas enregistrés, qui pose un risque de sécurité.

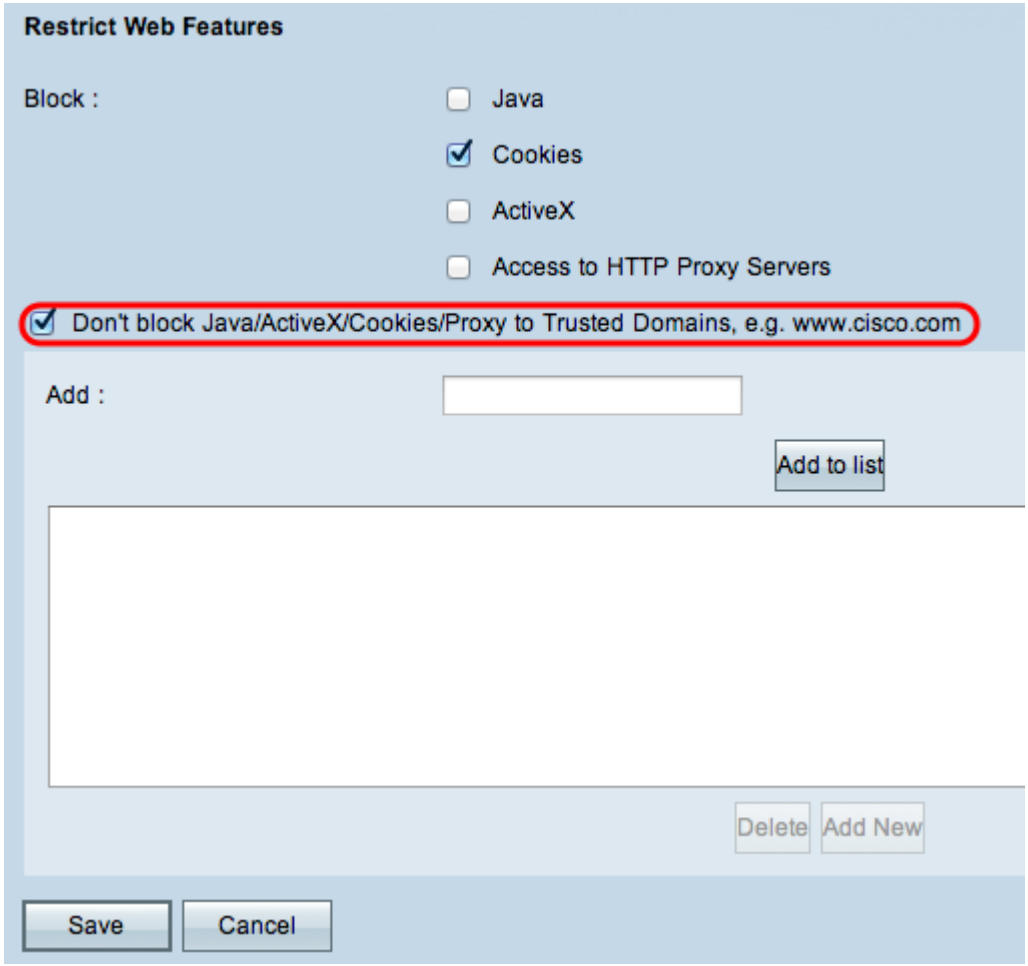
• ActiveX — ActiveX est un composant logiciel de Microsoft Windows qui peut être utilisé pour développer des applications ou pour contrôler de petits programmes comme des adjonctions utilisées sur des sites Internet. Si vous permettez ActiveX, il peut aider à améliorer votre expérience quand vous parcourez ; il permet à des sites Web pour lancer des animations et d'autres programmes semblables. D'autre part, il y a un risque potentiel si vous visitez les pages Web qui contiennent le logiciel malveillant d'ActiveX développé par les cyber-criminels qui peuvent endommager l'ordinateur. Pour bloquer ActiveX, cochez la case d'**ActiveX**. Si vous bloquez ActiveX, vous pouvez avoir des problèmes si vous voulez accéder à certains sites Internet qui emploient ActiveX pour exécuter.

• Access au serveur HTTP de proxy — Si vous souhaitez surfer anonyme par un serveur proxy et refuser l'accès au serveur proxy, cochez **Access dans la** case de **serveur HTTP de proxy**. Les serveurs proxys de HTTP masquent des coordonnées des utilisateurs finaux des pirates informatiques. Ils fonctionnent car les intermédiaires et ainsi vous n'accèdent à pas l'Internet directement. Cependant, si les utilisateurs locaux ont accès aux serveurs proxys BLÊMES, ils peuvent pouvoir trouver une manière autour des filtres satisfaits sur le routeur et accéder à des sites Internet bloqués par le routeur.

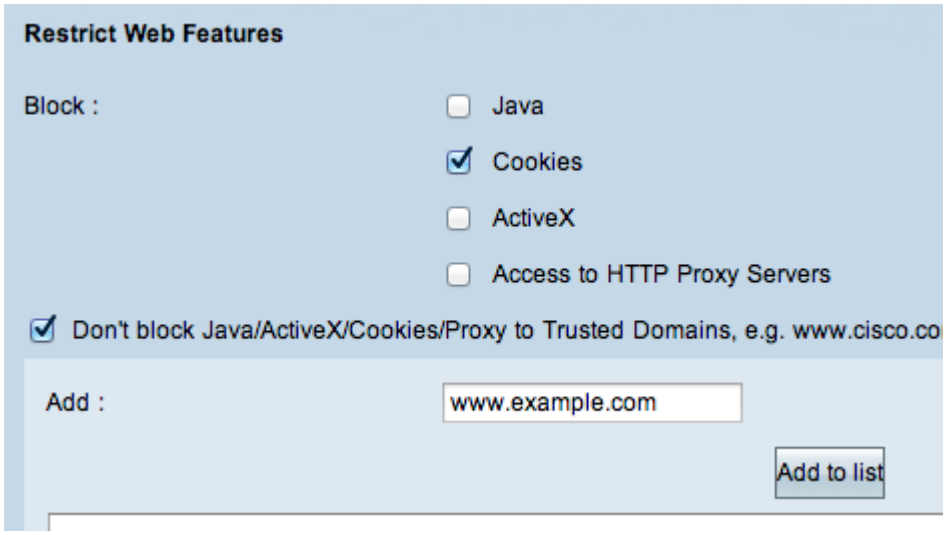
Étape 4. **Sauvegarde de** clic afin de sauvegarder les configurations.

Ajoutez les domaines de confiance

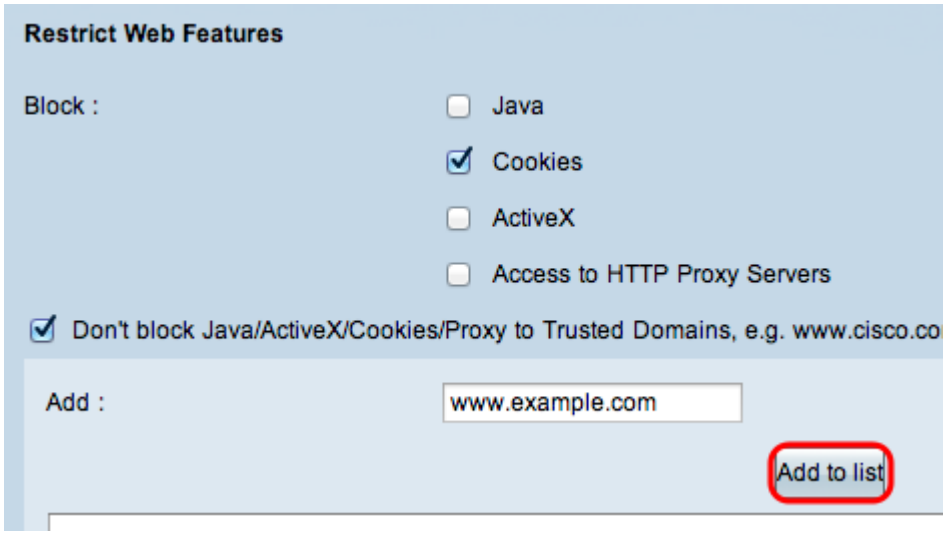
Quoiqu'une des caractéristiques de Web puisse être bloquée, l'utilisateur peut permettre ces caractéristiques à activer pour les domaines de confiance spécifiés.



Étape 1. Vérifiez **ne bloquent pas Javas/ActiveX/Témoins/proxy au** bouton **de confiance de domaines**. Ce sera seulement disponible si l'utilisateur a choisi de bloquer les caractéristiques l'unes des de Web dans l'étape 3 des *paramètres du pare-feu généraux*.



Étape 2. Dans le domaine d'*ajouter*, entrez dans le domaine à ajouter au domain list de confiance.

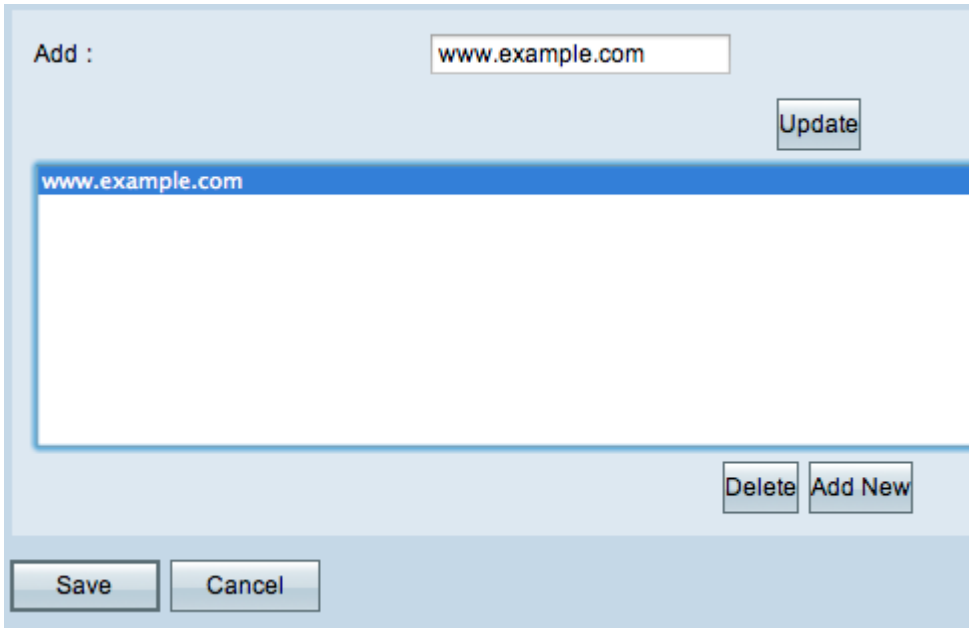


Étape 3. Cliquez sur Add **pour le répertorier.** Le domaine est ajouté à la liste de confiance.

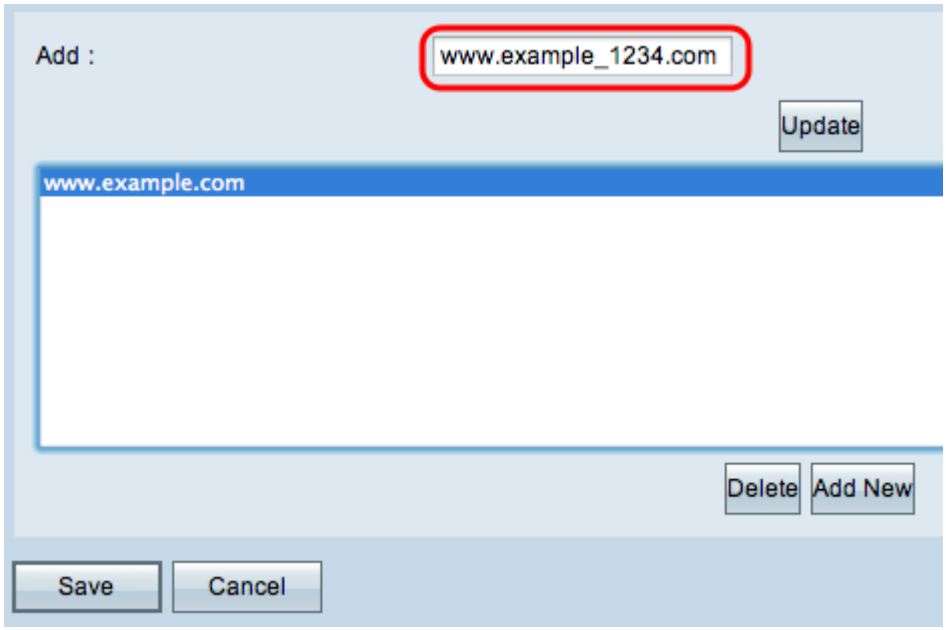
Étape 4. **Sauvegarde de** clic pour sauvegarder les modifications.

Mettez à jour un domaine de confiance

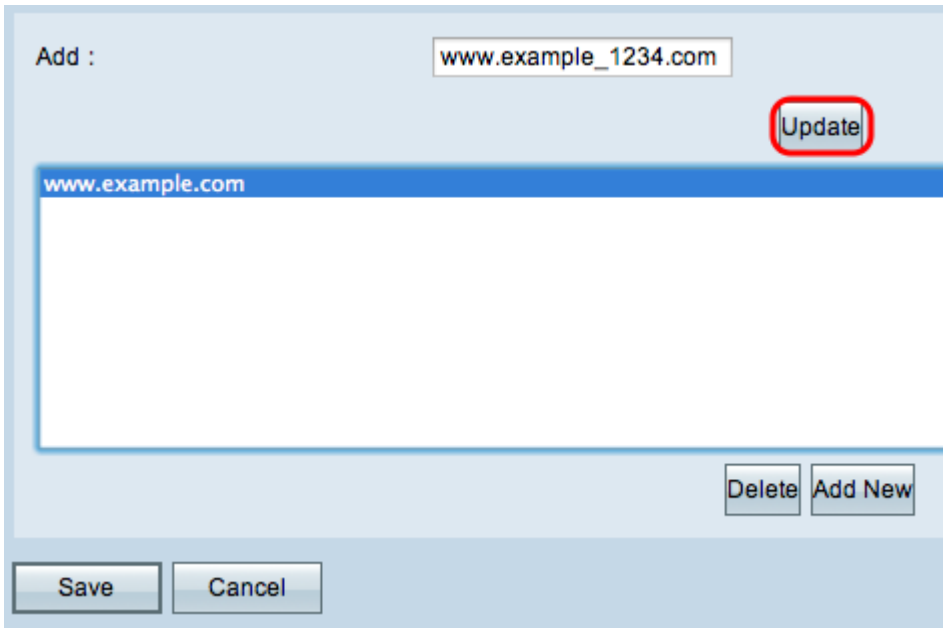
Cette section guide l'utilisateur sur la façon dont éditer un domaine de confiance.



Étape 1. Choisissez le domaine que vous voudriez éditer du domain list de confiance.



Étape 2. Dans le domaine d'*ajouter*, écrivez le nom de domaine mis à jour pour le domaine requis.

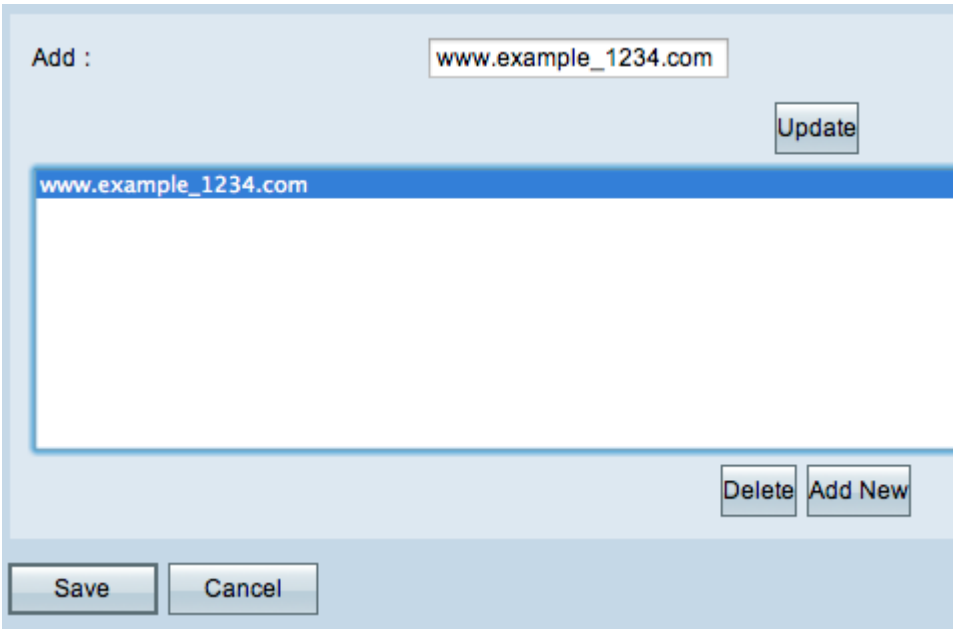


Étape 3. **Mise à jour de** clic.

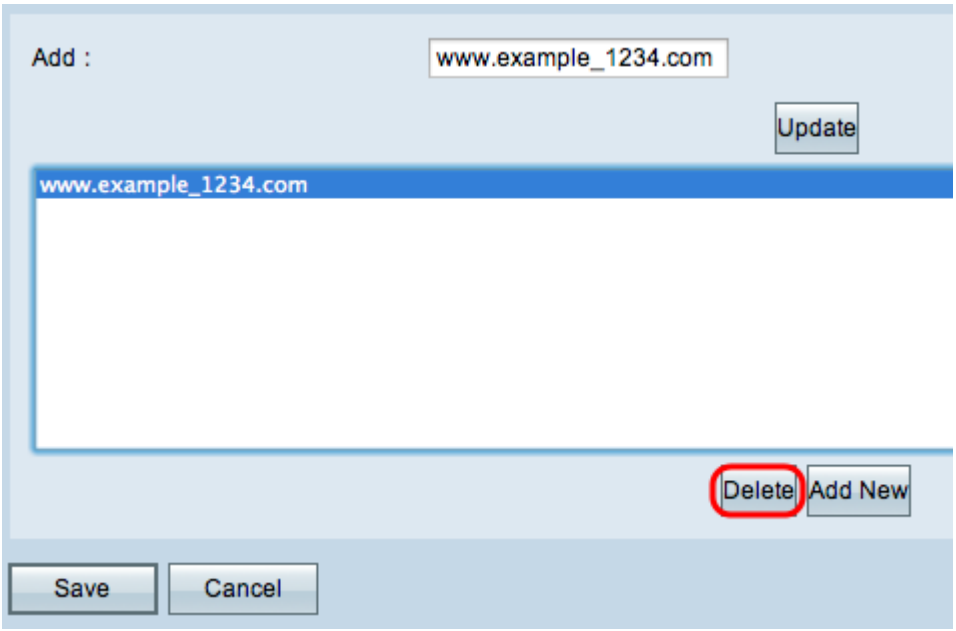
Étape 4. **Sauvegarde de** clic pour sauvegarder les modifications.

Supprimez un domaine de confiance

Cette section guide l'utilisateur sur la façon dont supprimer un domaine de confiance.



Étape 1. Choisissez le domaine que vous voudriez supprimer.



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

Étape 3. **Sauvegarde de** clic pour sauvegarder les modifications.