Filtrage selon le contenu sur des Routeurs RV180 et RV180W

Objectif

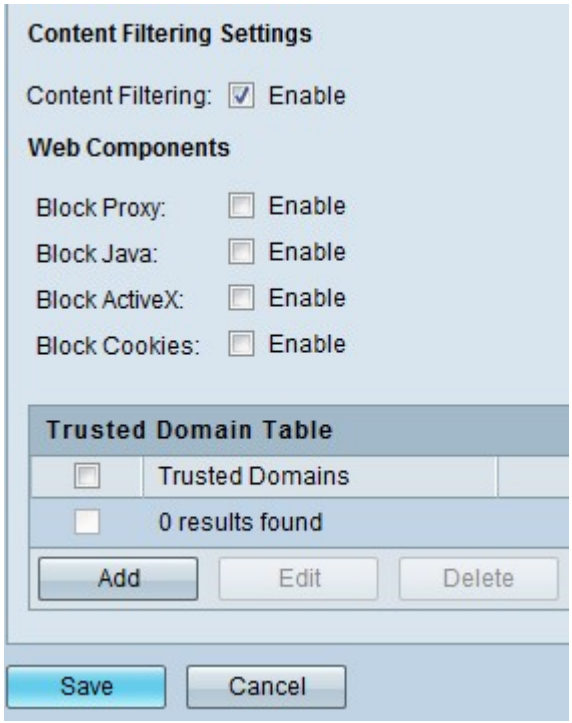
Le filtrage selon le contenu est une méthode dans laquelle on peut être bloqué ou permis le contenu basé sur un examen du type de contenu qui est présent plutôt que la source, la destination, ou d'autres détails d'adresse IP. Cet article explique le filtrage selon le contenu sur des Routeurs RV180 et RV180W.

Périphériques applicables

- RV180
- RV180W

Filtrage selon le contenu en employant le Pare-feu

Étape 1. Employez l'utilitaire de configuration pour choisir le **Pare-feu > le filtrage selon le contenu**. La page de *filtrage selon le contenu* s'ouvre. Vérifiez les cases appropriées pour bloquer le contenu spécifié.



Configurations de filtrage selon le contenu

- Enable de filtrage selon le contenu — Cochez cette case pour activer le filtrage selon le contenu.

Composants Web

- Proxy de bloc — Les paramètres de proxy peuvent aider à conduire des connexions à leurs destinations par les hôtes ou les serveurs intermédiaires connus sous le nom de

proxys. Des proxys peuvent être utilisés de cette façon pour éluder certaines règles de Pare-feu mais peuvent également être essentiels pour certaines connexions. **Enable de** contrôle pour bloquer des serveurs proxys.

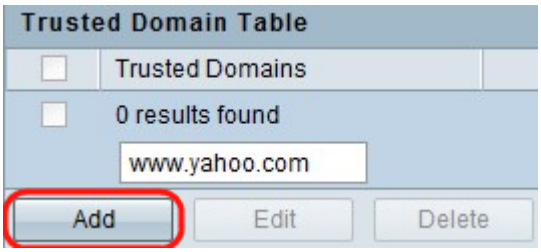
• Javas de bloc — Vérifiez l'**enable** pour bloquer des applet Java d'être téléchargé par des hôtes se connectant par le routeur. Les applet Java tiennent compte de la fonctionnalité dynamique des pages Web mais peuvent également contenir les applet malveillants qui peuvent infecter des ordinateurs.

• Bloc ActiveX — **Enable de** contrôle pour bloquer ActiveX. Les contrôles d'ActiveX sont semblables aux applet Java du fait ils peuvent être utilisés pour certaine fonctionnalité de page Web mais peuvent également infecter des hôtes se connectant par le routeur.

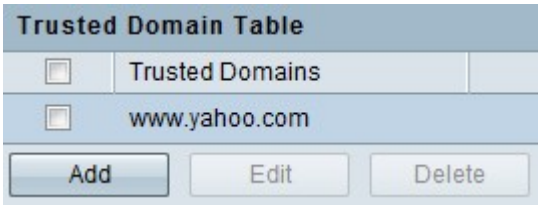
• Témoins de bloc — Vérifiez l'**enable** pour bloquer des Témoins d'être téléchargé par des hôtes se connectant par le routeur. Des Témoins sont utilisés par des sites Web d'Internet pour l'authentification et quelques sites Web ne peuvent pas fonctionner sans eux. Cependant, les sites Web peuvent également utiliser des Témoins pour enregistrer dépister des habitudes de l'information et de furetage d'un hôte.

Tableau de confiance de domaine — Le Tableau de confiance de domaine répertorie tous les domaines qui peuvent sont de confiance et permet toutes les exécutions sur ces domaines.

Remarque: Nomme qui sont dans le domain list de confiance peuvent être sautés par le filtrage de mot clé. par exemple. Si « Yahoo » est ajouté aux mots clé bloqués les répertorient et www.yahoo.com est ajouté au domain list de confiance, alors www.yahoo.com sera permis mais mail.yahoo.com ne sera pas permis.



• Domaine de confiance — Domaine de confiance pour lequel le filtrage selon le contenu est sauté.



• Cliquez sur Add pour joindre la page de la configuration du domaine de confiance.

• Cliquez sur Edit pour apporter des modifications dans le domaine sélectionné.

• Cliquez sur Delete pour supprimer un domaine ou des domaines sélectionnés.

Étape 2. **Sauvegarde de** clic pour sauvegarder les configurations.