Configuration de base du pare-feu sur les routeurs RV320 et RV325

Objectif

Cet article explique comment configurer les paramètres de pare-feu de base sur les routeurs VPN RV32x.

Un pare-feu est un ensemble de fonctionnalités conçues pour maintenir la sécurité d'un réseau. Un routeur est considéré comme un pare-feu matériel puissant. Ceci est dû au fait que les routeurs sont capables d'inspecter tout le trafic entrant et d'abandonner tout paquet indésirable. Les pare-feu réseau protègent un réseau informatique interne (domicile, école, intranet d'entreprise) contre les accès malveillants de l'extérieur. Les pare-feu réseau peuvent également être configurés pour limiter l'accès à l'extérieur des utilisateurs internes.

Périphériques pertinents

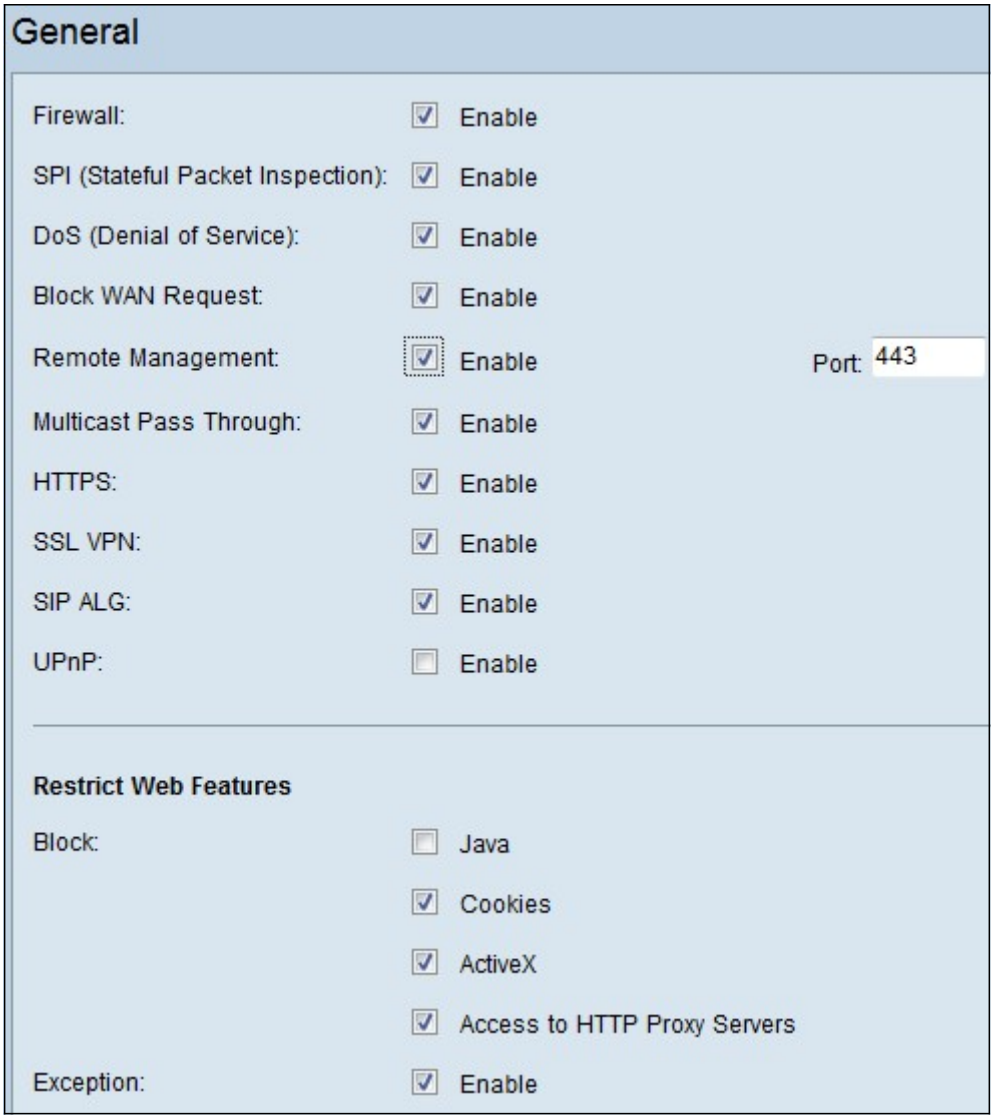
- Routeur VPN double WAN RV320
- Routeur VPN double WAN Gigabit RV325

Version du logiciel

- v 1.1.0.09

Paramètres de base

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



Étape 2. En fonction de vos besoins, cochez la case **Activer** qui correspond aux fonctionnalités que vous souhaitez activer.

- Pare-feu : les pare-feu de routeur peuvent être désactivés (désactivés) ou activés pour filtrer certains types de trafic réseau par le biais de ce qu'on appelle des règles de pare-feu. Un pare-feu peut être utilisé pour filtrer tout le trafic entrant et sortant et basé.
- SPI (Stateful Packet Inspection) : surveille l'état des connexions réseau telles que les flux TCP et la communication UDP. Le pare-feu distingue les paquets légitimes pour différents types de connexions. 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) : utilisé pour protéger un réseau contre une attaque par déni de service distribué (DDoS). Les attaques DDoS sont destinées à inonder un réseau au point où les ressources du réseau deviennent indisponibles. Le RV320 utilise la protection DoS pour protéger le réseau par la restriction et la suppression de paquets indésirables.
- Block WAN Request : bloque toutes les requêtes ping vers le routeur à partir du port WAN.
- Remote Management : permet d'accéder au routeur à partir d'un réseau WAN distant.
  - Port : saisissez un numéro de port à gérer à distance.
- Multicast Pass Through : permet aux messages de multidiffusion IP de traverser le périphérique.
- HTTPS (Hypertext Transfer Protocol Secure) : protocole de communication pour la communication sécurisée sur un réseau informatique. Il fournit un chiffrement bidirectionnel à

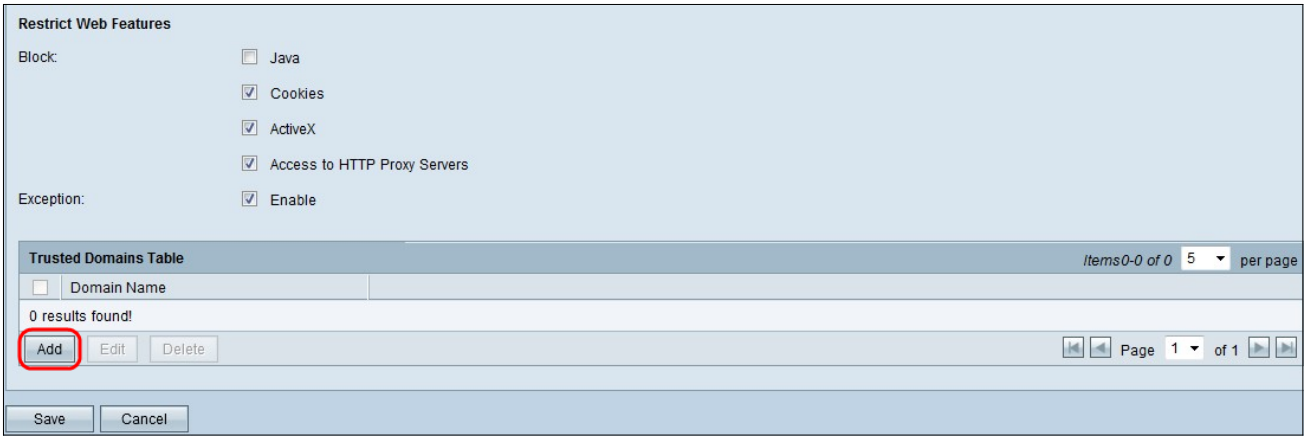
partir du client et du serveur.
- SSL VPN : autorise une connexion VPN SSL établie via le routeur.
- SIP ALG — SIP ALG offre des fonctionnalités qui permettent le trafic voix sur IP qui va du côté privé au côté public et public au côté privé du pare-feu lorsque l'adresse réseau et la traduction de port (NAPT) sont utilisées. NAPT est le type le plus courant de traduction d'adresses réseau.
- UPnP (Universal Plug and Play) : permet de détecter automatiquement les périphériques qui peuvent communiquer avec le routeur.

Étape 3. En fonction de vos besoins, cochez la case **Activer** qui correspond aux fonctionnalités que vous souhaitez bloquer.

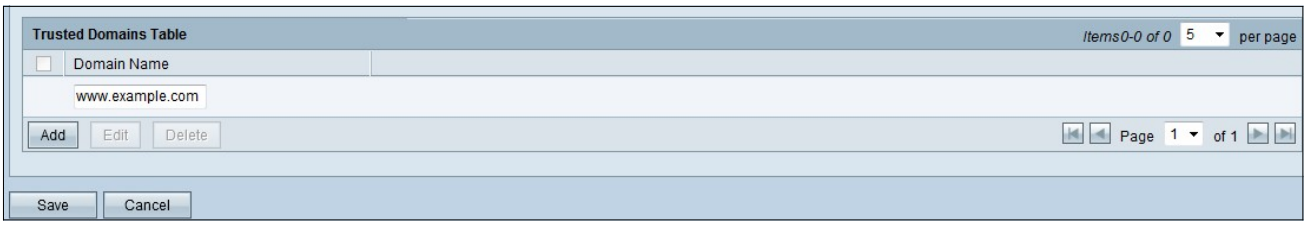
- Java : cochez cette case pour empêcher le téléchargement et l'exécution des applets Java. Java est un langage de programmation courant utilisé par de nombreux sites Web. Cependant, les applets java qui sont conçues pour des intentions malveillantes peuvent constituer une menace pour la sécurité d'un réseau. Une fois téléchargé, un applet java hostile peut exploiter les ressources réseau.
- Cookies : les cookies sont créés par des sites Web pour stocker des informations sur les utilisateurs. Les cookies peuvent suivre l'historique Web de l'utilisateur, ce qui peut conduire à une violation de la vie privée.
- ActiveX — ActiveX est un type d'applet utilisé par de nombreux sites Web. Bien que généralement sûr, une fois qu'un applet ActiveX malveillant est installé sur un ordinateur, il peut faire tout ce qu'un utilisateur peut faire. Il peut insérer du code nuisible dans le système d'exploitation, surfer sur un intranet sécurisé, modifier un mot de passe ou récupérer et envoyer des documents.
- Accès aux serveurs proxy HTTP : les serveurs proxy sont des serveurs qui fournissent une liaison entre deux réseaux distincts. Les serveurs proxy malveillants peuvent enregistrer toutes les données non chiffrées qui leur sont envoyées, telles que les connexions ou les mots de passe.
- Exception : autorise les fonctionnalités sélectionnées (Java, Cookies, ActiveX ou Access to HTTP Proxy Servers), mais limite toutes les fonctionnalités non sélectionnées sur les domaines approuvés configurés. Domaine approuvé et ayant accès au réseau approuvé. Vous pouvez configurer un domaine approuvé qui permet aux utilisateurs d'un domaine externe d'accéder à vos ressources réseau. Si cette option est désactivée, un domaine approuvé autorise toutes les fonctionnalités.

Note: Time Saver : si vous n'avez pas coché la case Exception, ignorez l'étape 4 .

Étape 4. Cliquez sur Ajouter, entrez un nouveau domaine approuvé, puis cliquez sur Enregistrer pour créer un domaine approuvé.

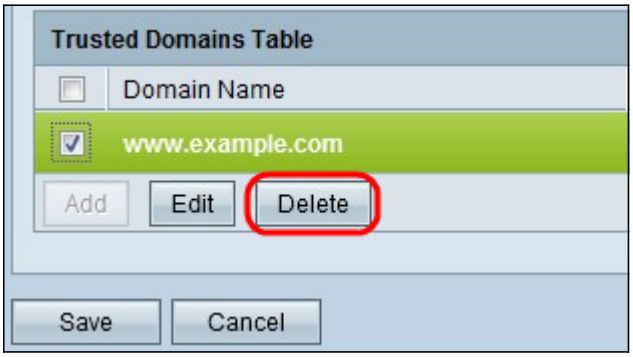


Étape 5. Cliquez sur Enregistrer pour mettre à jour les modifications.



Étape 6. (Facultatif) Pour modifier le nom du domaine approuvé, cochez la case du domaine approuvé que vous souhaitez modifier, cliquez sur Modifier, modifiez le nom de domaine et cliquez sur Enregistrer.

Étape 7. (Facultatif) Pour supprimer un domaine dans la liste Domaine approuvé, cochez la case du domaine approuvé que vous voulez supprimer, puis cliquez sur Supprimer.



Afficher une vidéo relative à cet article...