Configuration des règles d'accès sur RV215W

Objectif

Le routeur RV215W permet de configurer des règles d'accès pour accroître la sécurité. Ces listes de contrôle d'accès (ACL) sont des listes qui bloquent ou autorisent l'envoi du trafic à destination et en provenance de certains utilisateurs. Ils peuvent être configurés pour être en vigueur à tout moment ou en fonction de calendriers définis.

Cet article explique comment configurer les règles d'accès sur le routeur RV215W.

Périphériques pertinents

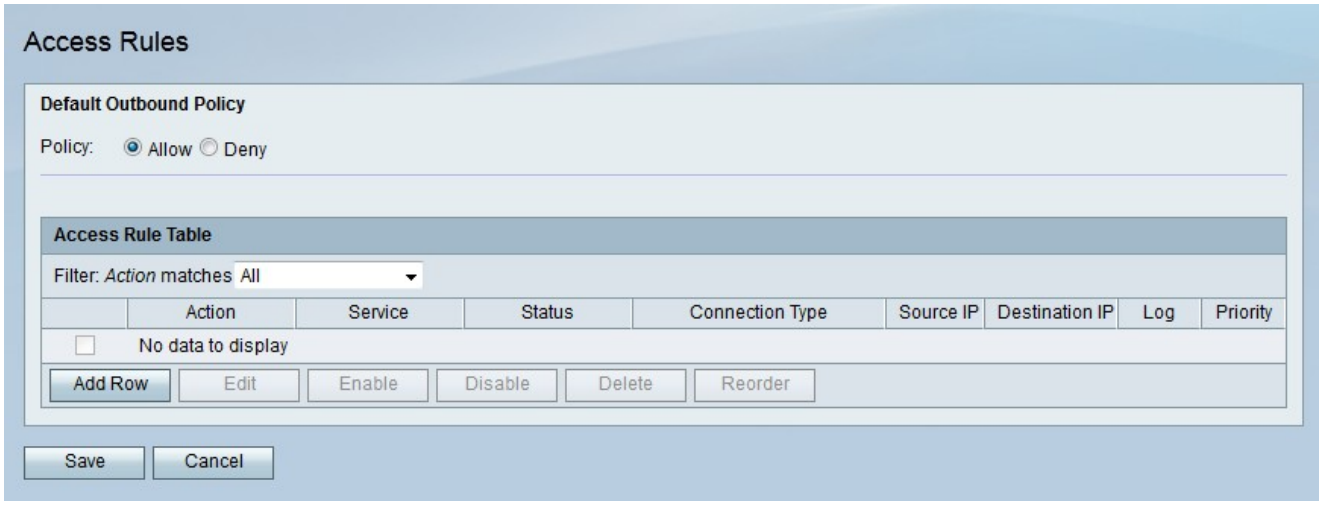
·RV215W

Version du logiciel

•1.1.0.5

Règles d'accès

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Firewall > Access Rules**. La page *Règles d'accès* s'ouvre :

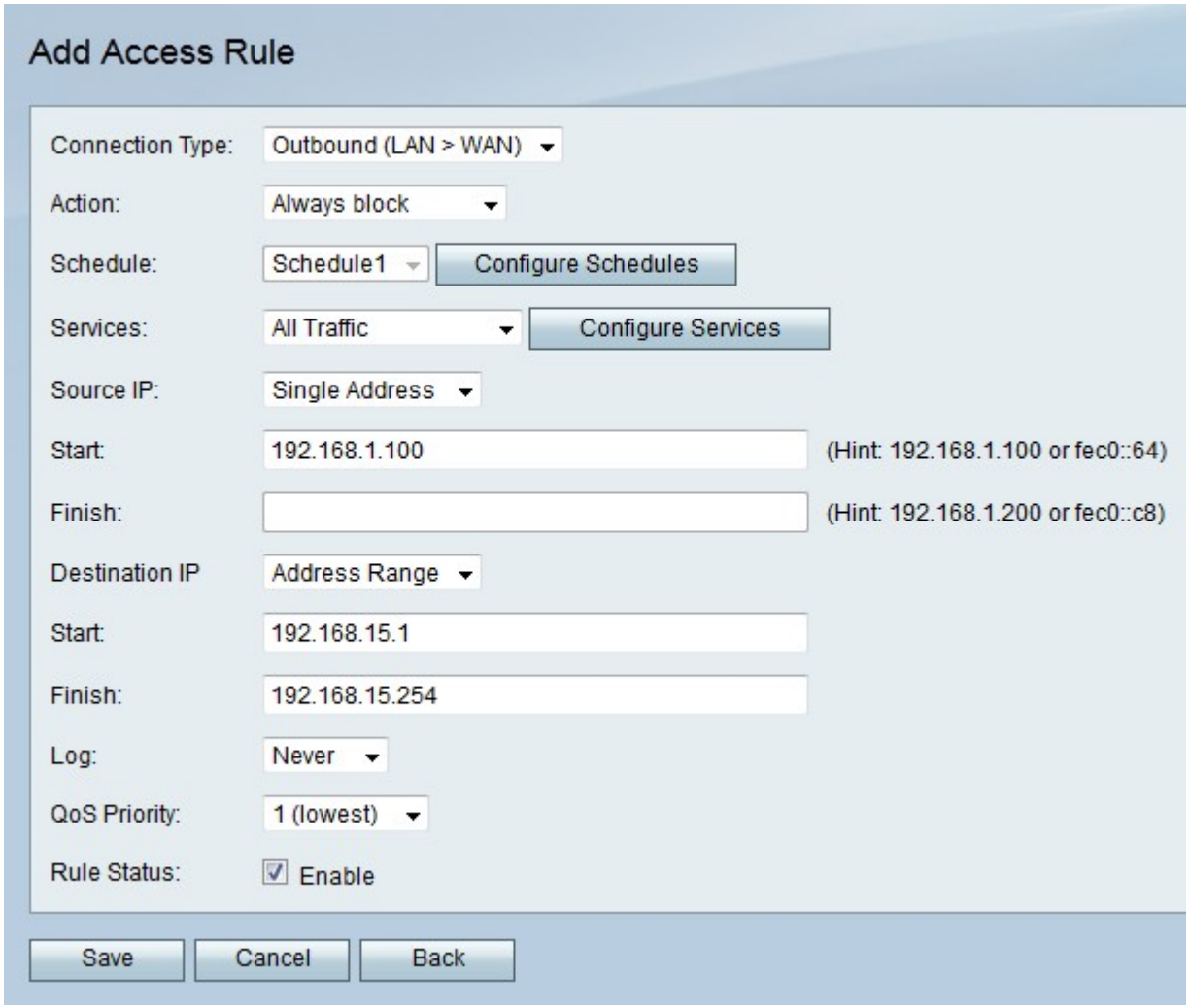


Étape 2. Sélectionnez la case d'option correspondant à la stratégie de sortie par défaut souhaitée dans le champ Stratégie. La stratégie de sortie par défaut détermine si le trafic sortant est autorisé ou refusé. Il est utilisé chaque fois qu'aucune règle d'accès ou stratégie d'accès à Internet n'est configurée sur une adresse IP d'un utilisateur.

Étape 3. Click **Save**.

Ajouter une règle d'accès

Étape 1. Cliquez sur **Ajouter une ligne** pour ajouter une nouvelle règle d'accès. La page Add Access Rule s'ouvre :



Étape 2. Dans la liste déroulante Type de connexion, sélectionnez le type de règle à créer.

·sortant (LAN > WAN) : la règle affecte les paquets qui proviennent du réseau local sécurisé et qui vont au réseau étendu non sécurisé.

·Inbound (WAN > LAN) : la règle affecte les paquets provenant du WAN non sécurisé et transmis au LAN sécurisé.

·Inbound (WAN > DMZ) : la règle affecte les paquets qui proviennent du WAN non sécurisé et qui vont vers la DMZ. Une DMZ est un segment de réseau qui sépare le LAN du WAN pour fournir une couche de sécurité supplémentaire.

Étape 3. Dans la liste déroulante Action, sélectionnez l'action à appliquer à la règle.

·Always Block : bloque toujours les paquets.

·Always Allow : autorise toujours les paquets.

·Bloquer par planning : bloque les paquets en fonction d'un planning spécifié.

·Allow by schedule : autorise les paquets en fonction d'un planning spécifié.

Étape 4. Dans la liste déroulante Planification, sélectionnez un planning à appliquer à la règle.

Étape 5. Dans la liste déroulante Services, sélectionnez un service à autoriser ou à bloquer.

Note: Cliquez sur **Configurer les services** pour configurer les planifications sur la page *Gestion des services*.

Étape 6. Dans la liste déroulante Source IP, sélectionnez les adresses IP source à partir desquelles la règle bloque ou autorise les paquets.

·Any : la règle s'applique à toutes les adresses IP source.

·Single Address : saisissez une adresse IP unique à laquelle la règle s'applique dans le champ Start.

·Address Range : saisissez une plage d'adresses IP auxquelles la règle s'applique dans les champs Start et Finish.

Étape 7. Dans la liste déroulante Destination IP, sélectionnez les adresses IP de destination auxquelles la règle bloque ou autorise les paquets.

·Any : la règle s'applique à toutes les adresses IP de destination.

·Single Address : saisissez une adresse IP unique à laquelle la règle s'applique dans le champ Start.

·Address Range : saisissez une plage d'adresses IP auxquelles la règle s'applique dans les champs Start et Finish.

Étape 8. Dans la liste déroulante Journal, sélectionnez une option de journal. Les journaux sont des enregistrements système générés qui sont utilisés pour la gestion de la sécurité.

·Never : désactive les journaux.

·Always : le routeur RV215W crée un journal chaque fois qu'un paquet correspond à la règle.

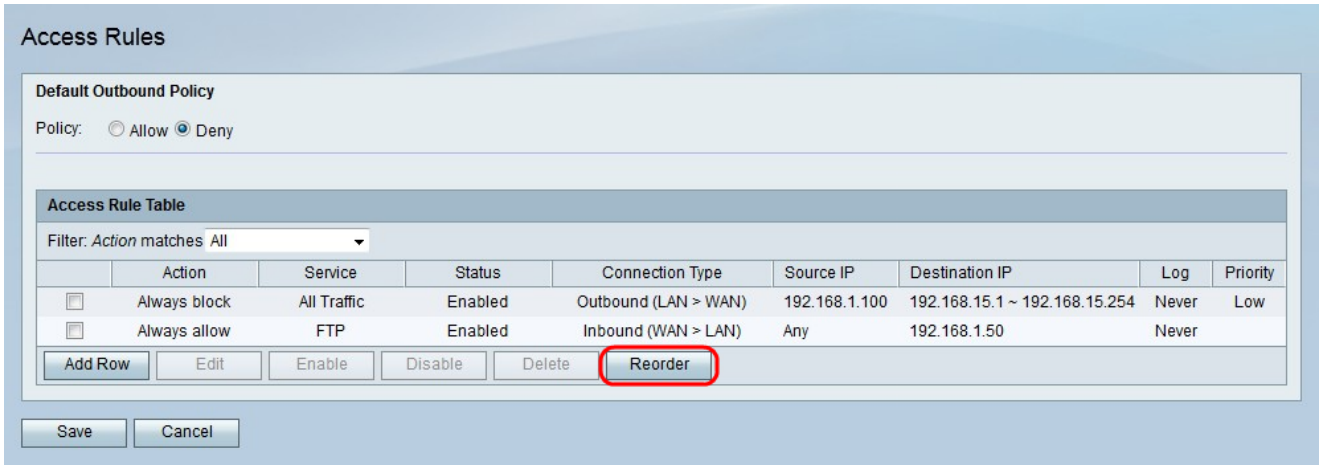
Étape 9. Dans la liste déroulante QoS Priority, sélectionnez une priorité pour les paquets IP sortants de la règle. La priorité 1 est la plus basse, tandis que la priorité 4 est la plus élevée. Les paquets des files d'attente de priorité supérieure seront envoyés avant ceux des files d'attente de priorité inférieure.

Étape 10. Cochez **Enable** dans le champ Rule Status pour activer la règle.

Étape 11. Click **Save**.

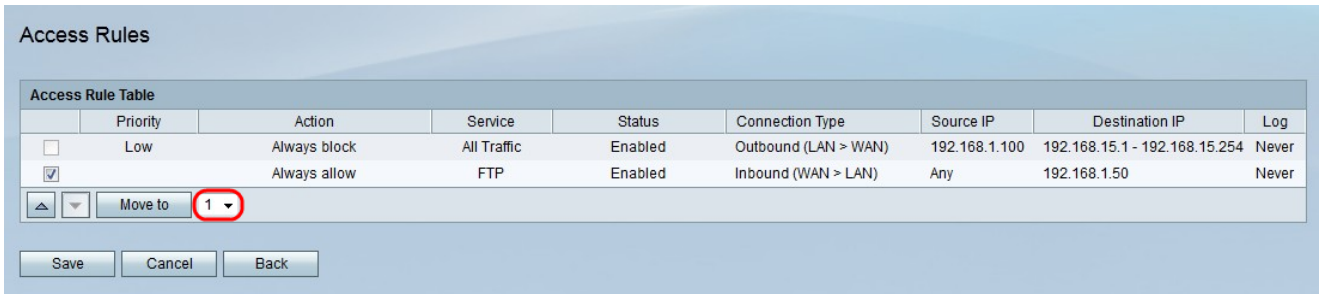
Réorganiser les règles d'accès

La fonction de réorganisation est une option importante sur le RV215W. L'ordre dans lequel les règles d'accès sont affichées dans la table des règles d'accès indique l'ordre dans lequel elles sont appliquées. La première règle du tableau est la première règle à appliquer.



Étape 1. Cliquez sur **Réorganiser** pour réorganiser les règles d'accès.

Étape 2. Cochez la case de la règle d'accès à réorganiser.



Étape 3. Dans la liste déroulante, sélectionnez la position vers laquelle vous souhaitez déplacer la règle spécifiée.

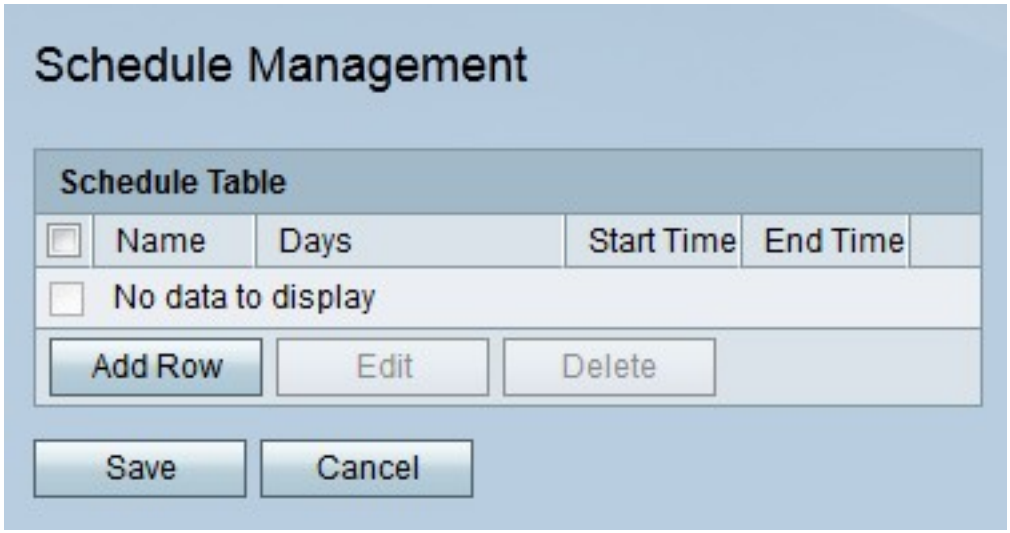
Étape 4. Cliquez sur **Déplacer vers** pour réorganiser la règle. La règle passe à la position spécifiée dans la table.

Note: Les boutons fléchés haut et bas peuvent également être utilisés pour réorganiser les règles d'accès.

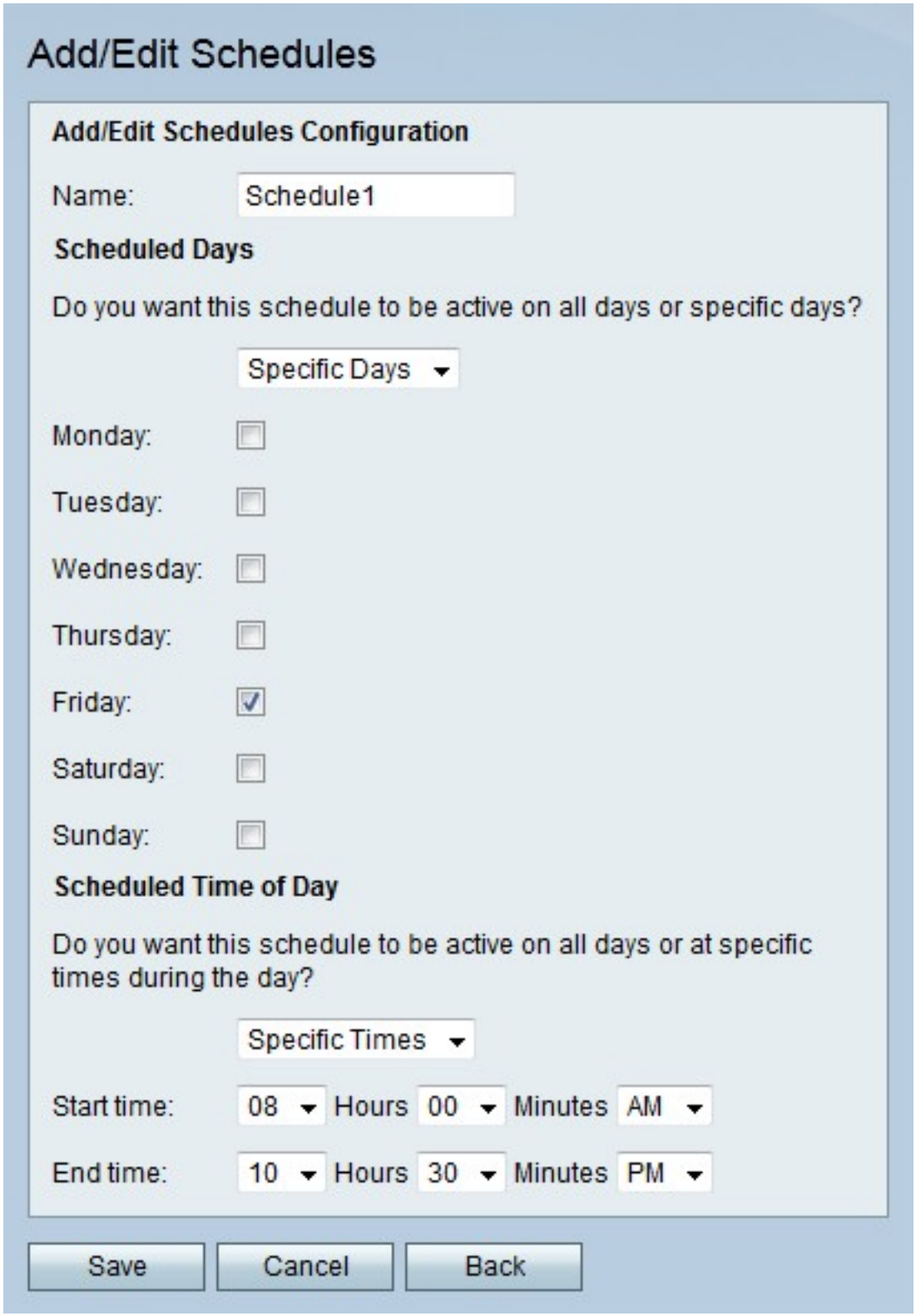
Étape 5. Click **Save**.

Configuration de la gestion des planifications

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



Étape 2. Cliquez sur **Ajouter une ligne** pour ajouter un nouveau planning. La page *Ajouter/modifier des planifications* s'ouvre :



Étape 3. Entrez un nom pour le planning dans le champ Nom.

Étape 4. Dans la liste déroulante Jours planifiés, sélectionnez les jours où le planning est actif.

·Tous les jours : le planning est actif tous les jours de la semaine.

·jours spécifiques : cochez les cases des jours pour que le planning soit actif.

Étape 5. Dans la liste déroulante Heure planifiée du jour, sélectionnez l'heure à laquelle la planification est active.

·Toutes les heures : le planning est actif à tout moment de la journée.

·heures spécifiques — Dans la liste déroulante Heure de début et heure de fin, sélectionnez l'heure de début et de fin du planning.

Étape 6. Click **Save**.