Ajoutez et configurez les règles d'accès sur RV130 et RV130W

Objectif

Les périphériques de réseau fournissent à des capacités de filtrage du trafic de base des règles d'accès. Une règle d'accès est une seule entrée dans une liste de contrôle d'accès (ACL) qui spécifie une autorisation ou refusent la règle (pour expédier ou relâcher un paquet) basée sur le protocole, source et adresse IP de destination, ou configuration réseau.

L'objectif de ce document est de t'afficher comment ajouter et configurer une règle d'accès sur le RV130 et le RV130W.

Périphériques applicables

- RV130
- RV130W

Versions de logiciel

- Version 1.0.1.3

Ajoutez et configurez une règle d'accès

Établissement de la politique sortante par défaut

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez le **Pare-feu > les règles d'accès**. La page de *règles d'accès* s'ouvre :

Étape 2. Dans le secteur de *politique sortante par défaut*, cliquez sur la case d'option désirée pour choisir une stratégie pour le trafic sortant. La stratégie est appliquée toutes les fois qu'il n'y a aucune règle d'accès ou stratégie d'accès Internet configurée. La valeur par défaut est **laissent**, qui permet à tout le trafic à l'Internet pour traverser.

Les options disponibles sont définies comme suit :

- Laissez — Permettez tous les types de trafic sortant du RÉSEAU LOCAL à l'Internet.
- Refusez — Bloquez tous les types de trafic sortant du RÉSEAU LOCAL à l'Internet.

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

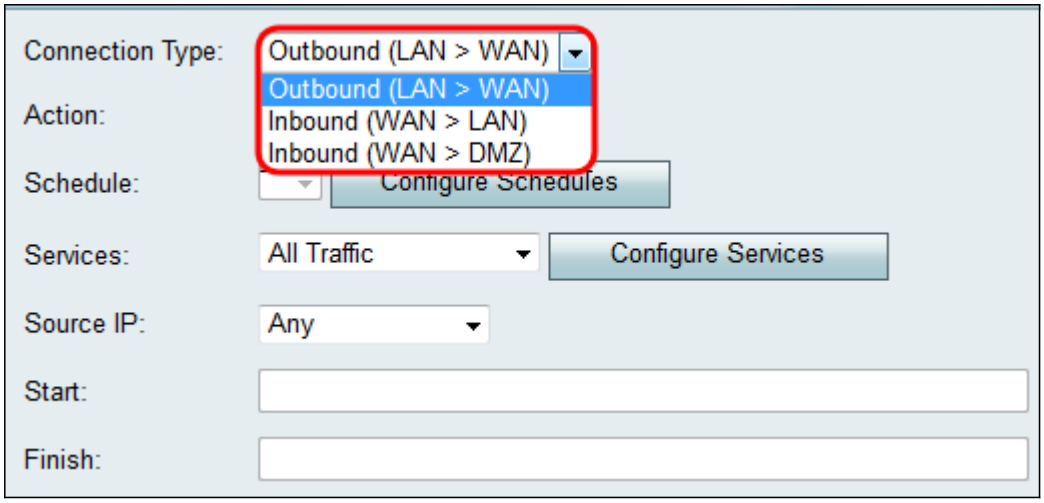
Ajouter une règle d'accès

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez le **Pare-feu > les règles d'accès**. La fenêtre de *règles d'accès* s'ouvre :

Étape 2. Cliquez sur Add la **ligne** dans le *Tableau de règle d'accès* pour ajouter une nouvelle règle d'accès.

La page de *règle d'accès d'ajouter* s'ouvre :

Étape 3. De la liste déroulante de *type de connexion*, choisissez le type de trafic pour lequel la règle s'applique.



Les options disponibles sont définies comme suit :

- Sortant (RÉSEAU LOCAL > WAN) — La règle affecte les paquets qui proviennent le réseau local (RÉSEAU LOCAL) et sortent à l'Internet (WAN).
- D'arrivée (WAN > RÉSEAU LOCAL) — La règle affecte les paquets qui proviennent l'Internet (WAN) et entrent dans le réseau local (RÉSEAU LOCAL).
- D'arrivée (WAN > DMZ) — La règle affecte les paquets qui proviennent l'Internet (WAN) et entrent dans le sous-réseau de la zone démilitarisée (DMZ).

Étape 4. De la liste déroulante d'*action*, choisissez l'action d'être pris quand une règle est appariée.

Les options disponibles sont définies comme suit :

- Toujours bloc — Refusez toujours l'accès si les conditions sont appariées. Saut à l'étape 6.

• Laissez toujours — Permettez toujours l'accès si les conditions sont appariées. Saut à l'étape 6.

• Bloc par programme — Refusez l'accès si les conditions sont appariées pendant un programme préconfiguré.

• Autorisez par programme — Permettez l'accès si les conditions sont appariées pendant un programme préconfiguré.

Étape 5. Si vous choisissiez le **bloc par programme** ou **autorisez par programme** dans l'étape 4, choisissez le programme approprié de la liste déroulante de *programme*.

Remarque: Pour créer ou éditer un programme, cliquez sur Configure les **programmes**. Référez-vous à *configurer des programmes sur le RV130 et* pour en savoir plus et instructions *RV130W*.

Étape 6. Choisissez le type de service que la règle d'accès s'applique pour à partir de la liste déroulante de *services*.

Remarque: Si vous voulez ajouter ou éditer un service, cliquez sur Configure les **services**. Référez-vous à la *configuration de gestion des services sur le RV130 et* pour en savoir plus et instructions *RV130W*.

Configurer l'IP de source et de destination pour le trafic sortant

Suivez les étapes dans cette section si **sortant (RÉSEAU LOCAL > WAN)** était sélectionné comme étape 3 de taper de connexion dedans d'*ajouter une règle d'accès.*

Remarque: Si un type de connexion entrante était sélectionné dans l'étape 3 d'ajouter une règle d'accès, ignorez à la section suivante : *Configurer l'IP de source et de destination pour le trafic d'arrivée*.

Étape 1. Choisissez comment vous voudriez définir le source ip de la liste déroulante de *source ip*. Pour le trafic sortant, le source ip se rapporte à l'adresse ou aux adresses (dans le RÉSEAU LOCAL) auxquelles la règle de Pare-feu s'appliquerait.

Les options disponibles sont définies comme suit :

• Quels — S'applique pour trafiquer provenir de n'importe quelle adresse IP du réseau local. , Blanc quittez par conséquent de *début* et de *finition* champs. Ignorez à l'étape 4 si vous choisissez cette option.

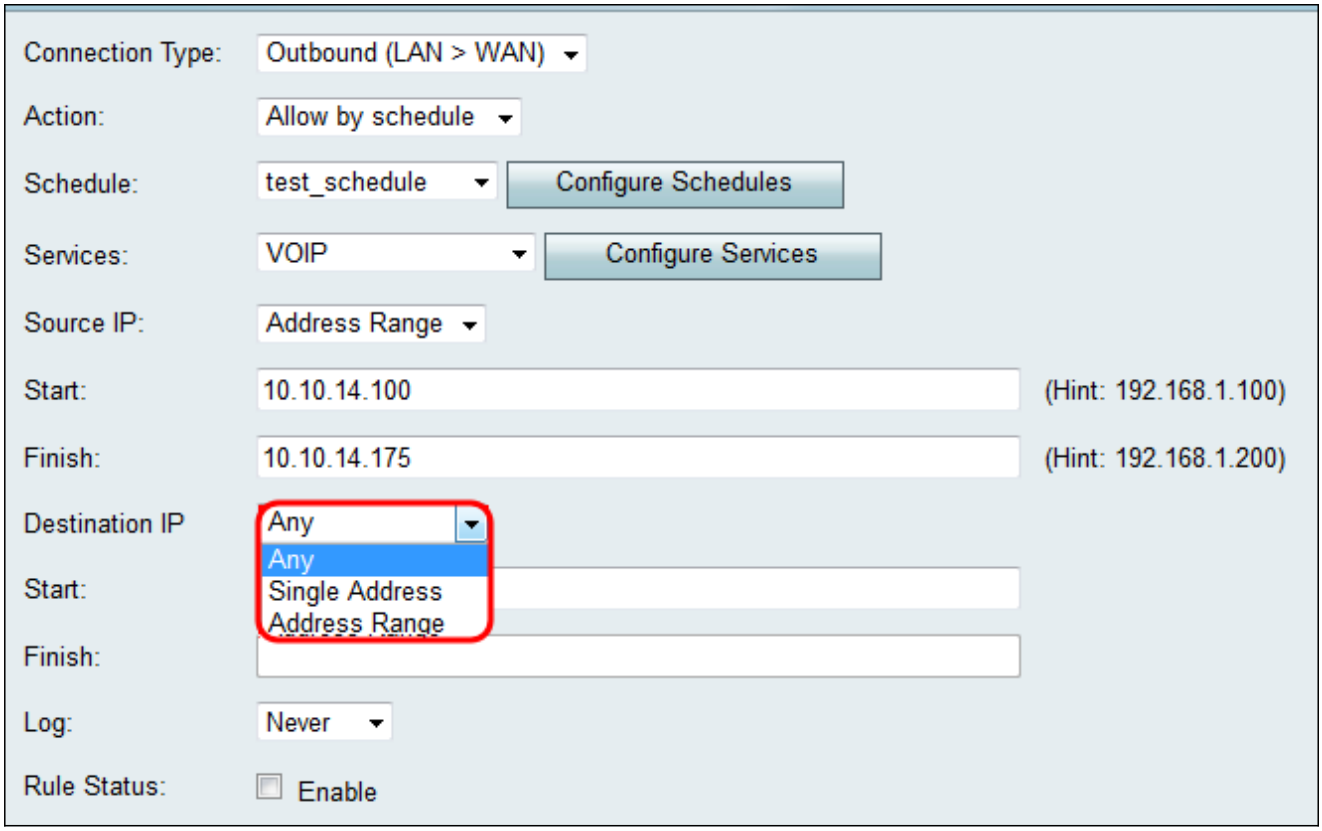
• Adresse unique — S'applique pour trafiquer provenir d'une adresse IP simple du réseau local. Écrivez l'adresse IP dans le domaine de *début*.

• Plage d'adresses — S'applique pour trafiquer provenir d'une plage des adresses IP du réseau local. Écrivez l'adresse IP commençante de la plage dans le domaine de *début* et l'adresse IP de fin dans le domaine de *finition* afin de placer la plage.

Étape 2. Si vous choisissiez l'**adresse unique** dans l'étape 1, écrivez l'adresse IP qui sera appliquée à la règle d'accès dans le domaine de *début*, et puis ignorez à l'étape 4. Si vous choisissiez la **plage d'adresses** dans l'étape 1, écrivez une adresse IP commençante qui sera appliquée à la règle d'accès dans le domaine de *début*.

Étape 3. Si vous choisissiez la **plage d'adresses** dans l'étape 1, écrivez l'adresse IP de fin qui encapsulera la plage d'adresses IP pour la règle d'accès dans le domaine de *finition*.

Étape 4. Choisissez comment vous voudriez définir l'IP de destination de la liste déroulante *IP de destination*. Pour le trafic sortant, l'IP de destination se rapporte à l'adresse ou aux adresses (dans le WAN) auxquelles le trafic est permis ou refusé du réseau local.



Les options disponibles sont définies comme suit :

- Quels — S'applique pour trafiquer dirigé vers n'importe quelle adresse IP en Internet public. , Blanc quittez par conséquent de *début* et de *finition* champs.
- Adresse unique — S'applique pour trafiquer dirigé vers une adresse IP simple en Internet public. Écrivez l'adresse IP dans le domaine de *début*.
- Plage d'adresses — S'applique pour trafiquer dirigé vers une plage des adresses IP en Internet public. Écrivez l'adresse IP commençante de la plage dans le domaine de *début* et l'adresse IP de fin dans le domaine de *finition* afin de placer la plage.

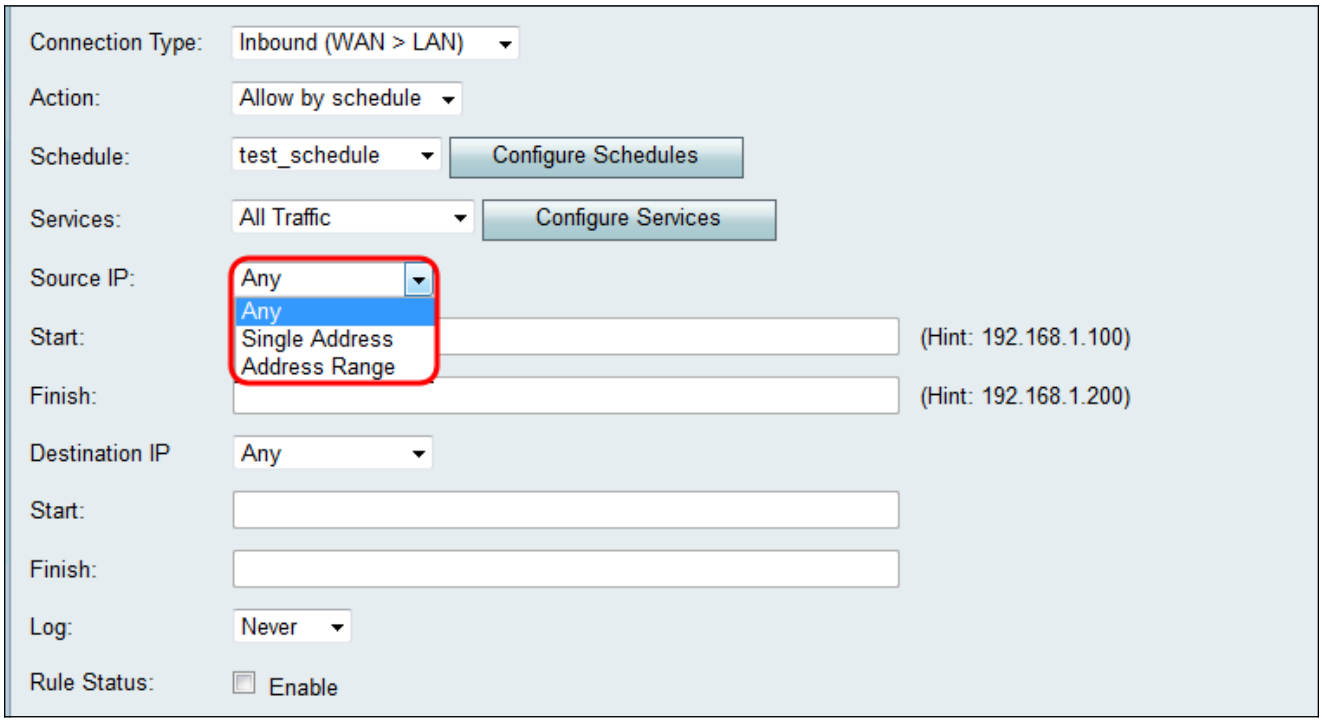
Étape 5. Si vous choisissiez l'**adresse unique** dans l'étape 4, écrivez l'adresse IP qui sera appliquée à la règle d'accès dans le domaine de *début*. Si vous choisissiez la **plage d'adresses** dans l'étape 4, écrivez une adresse IP commençante qui sera appliquée à la règle d'accès dans le domaine de *début*.

Étape 6. Si vous choisissiez la **plage d'adresses** dans l'étape 4, écrivez l'adresse IP de fin qui encapsulera la plage d'adresses IP pour la règle d'accès dans le domaine de *finition*.

Configurer l'IP de source et de destination pour le trafic d'arrivée

Suivez les étapes dans cette section si **d'arrivée (WAN > RÉSEAU LOCAL)** ou **d'arrivée (WAN > DMZ)** a été sélectionné comme étape 3 de taper de connexion dedans d'*ajouter une règle d'accès*.

Étape 1. Choisissez comment vous voudriez définir le source ip de la liste déroulante de *source ip*. Pour le trafic d'arrivée, le source ip se rapporte à l'adresse ou aux adresses (dans le WAN) auxquelles la règle de Pare-feu s'appliquerait.



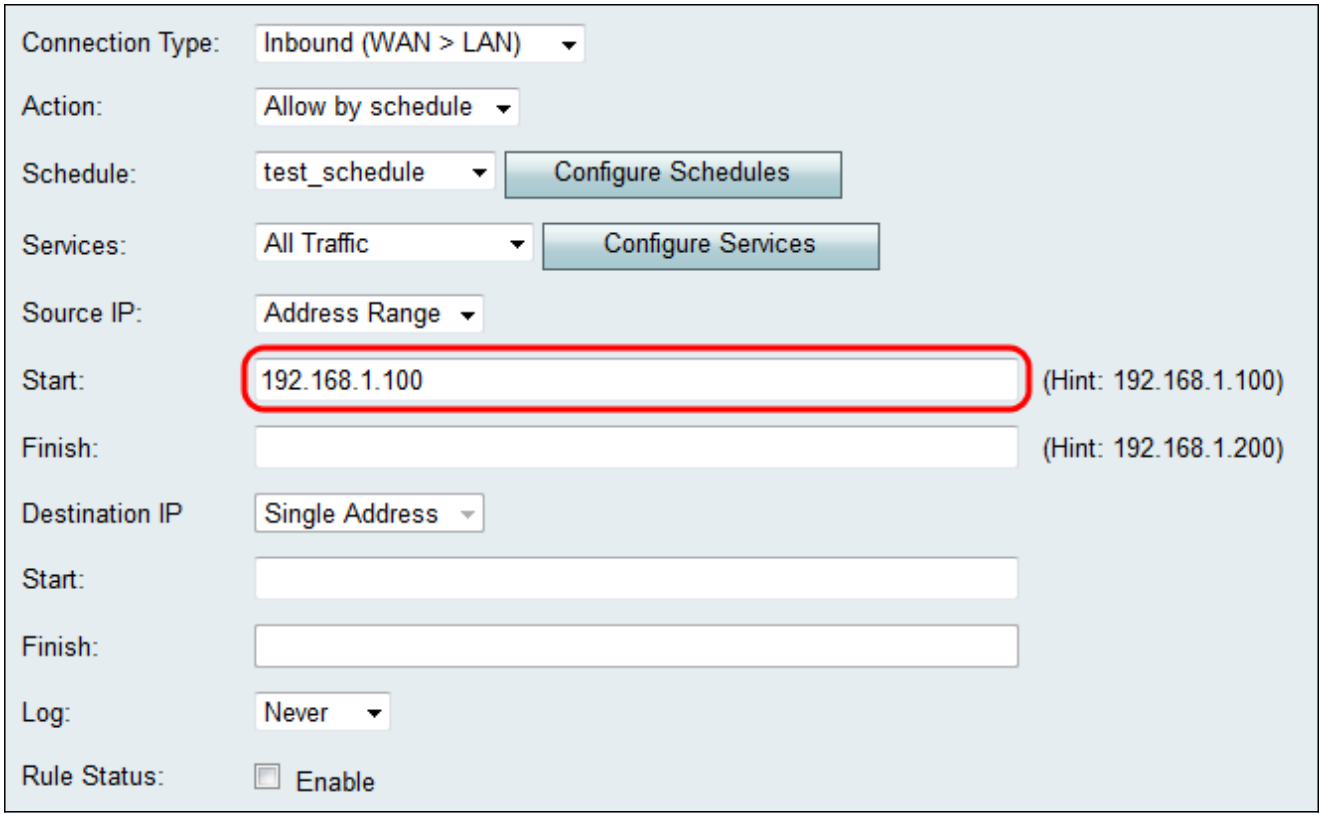
Les options disponibles sont définies comme suit :

• Quels — S'applique pour trafiquer provenir de n'importe quelle adresse IP en Internet public. , Blanc quittez par conséquent de *début* et de *finition* champs. Ignorez à l'étape 4 si vous choisissez cette option.

• Adresse unique — S'applique pour trafiquer provenir d'une adresse IP simple en Internet public. Écrivez l'adresse IP dans le domaine de *début*.

• Plage d'adresses — S'applique pour trafiquer provenir d'une plage des adresses IP en Internet public. Écrivez l'adresse IP commençante de la plage dans le domaine de *début* et l'adresse IP de fin dans le domaine de *finition* afin de placer la plage.

Étape 2. Si vous choisissiez l'**adresse unique** dans l'étape 1, écrivez l'adresse IP qui sera appliquée à la règle d'accès dans le domaine de *début*, et puis ignorez à l'étape 4. Si vous choisissiez la **plage d'adresses** dans l'étape 1, écrivez une adresse IP commençante qui sera appliquée à la règle d'accès dans le domaine de *début*.



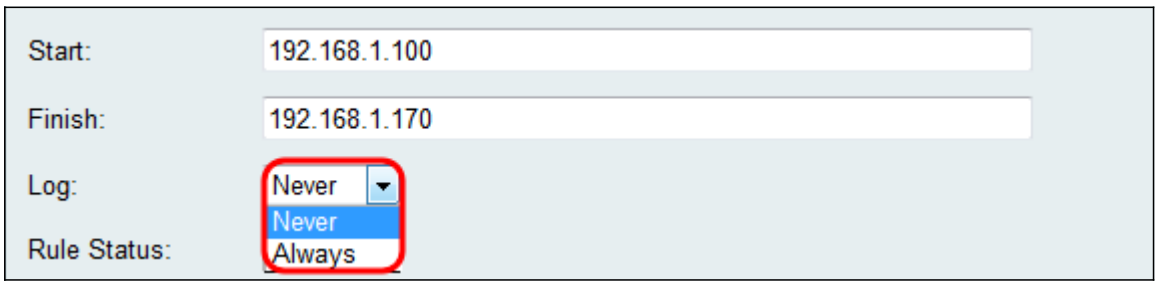
Étape 3. Si vous choisissiez la **plage d'adresses** dans l'étape 1, écrivez l'adresse IP de fin qui encapsulera la plage d'adresses IP pour la règle d'accès dans le domaine de *finition*.

Étape 4. Introduisez une adresse unique pour l'IP de destination dans le domaine de *début* au-dessous de la liste déroulante *IP de destination*. Pour le trafic d'arrivée, l'IP de destination se rapporte à l'adresse (dans le RÉSEAU LOCAL) à laquelle le trafic est permis ou refusé de l'Internet public.

Remarque: Si **d'arrivée (WAN > DMZ)** était sélectionné comme étape 3 de taper de connexion dedans d'*ajouter une règle d'accès*, l'adresse unique pour l'IP de destination est automatiquement configurée avec l'adresse IP de l'hôte DMZ activé.

Se connectant et activant la règle d'accès

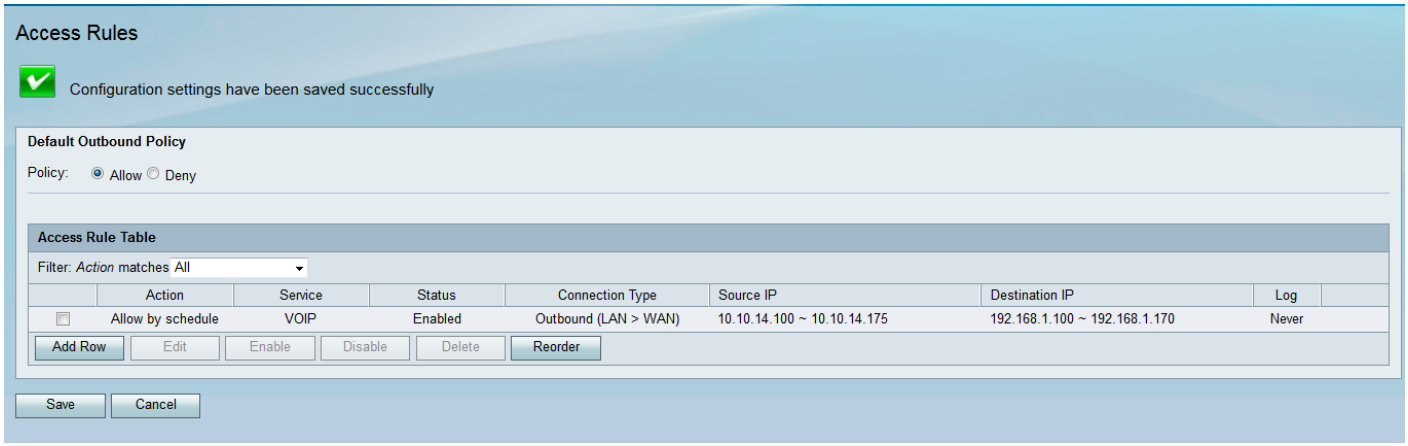
Étape 1. Sélectionnez **toujours** dans la liste déroulante de *log* si vous voulez que le routeur crée des logs toutes les fois qu'un paquet apparie une règle. Ne sélectionnez jamais si voulez se connecter à ne jamais se produire quand une règle est appariée.



Étape 2. Vérifiez la case à cocher d'**enable** pour activer la règle d'accès.

Étape 3. **Sauvegarde de** clic pour sauvegarder vos configurations.

Le Tableau de règle d'accès est mis à jour avec la règle d'accès nouvellement configurée.


Access Rules
Configuration settings have been saved successfully
Default Outbound Policy
Policy: Allow Deny
Access Rule Table
Filter: Action matches All
Action
Service
Status
Connection Type
Source IP
Destination IP
Log
Allow by schedule
VOIP
Enabled
Outbound (LAN > WAN)
10.10.14.100 ~ 10.10.14.175
192.168.1.100 ~ 192.168.1.170
Never
Add Row
Edit
Enable
Disable
Delete
Reorder
Save
Cancel