Ajouter et configurer des règles d'accès sur RV130 et RV130W

Objectif

Les périphériques réseau fournissent des fonctionnalités de filtrage de trafic de base avec des règles d'accès. Une règle d'accès est une entrée unique dans une liste de contrôle d'accès (ACL) qui spécifie une règle d'autorisation ou de refus (pour transférer ou abandonner un paquet) basée sur le protocole, une adresse IP source et de destination ou la configuration du réseau.

L'objectif de ce document est de vous montrer comment ajouter et configurer une règle d'accès sur les routeurs RV130 et RV130W.

Périphériques pertinents

•RV130

· RV130W

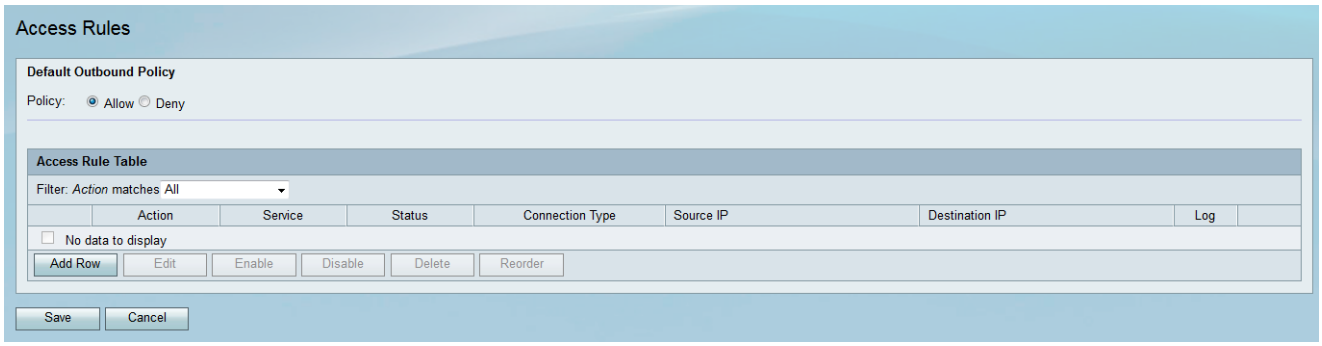
Versions logicielles

· Version 1.0.1.3

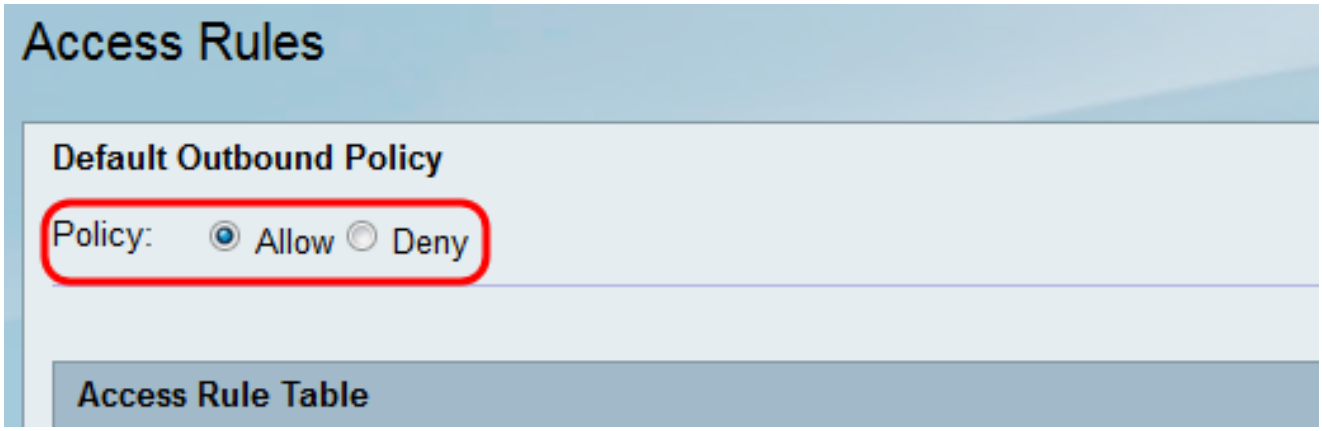
Ajouter et configurer une règle d'accès

Définition de la stratégie sortante par défaut

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



Étape 2. Dans la zone Default Outbound Policy, cliquez sur la case d'option souhaitée pour choisir une stratégie pour le trafic sortant. La stratégie est appliquée chaque fois qu'aucune règle d'accès ou stratégie d'accès à Internet n'est configurée. Le paramètre par défaut est Allow, qui permet à tout le trafic vers Internet de passer.

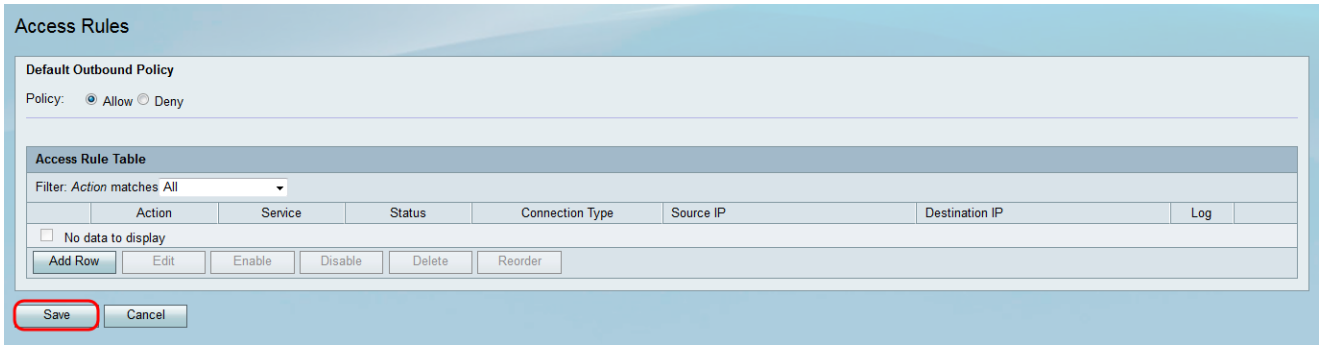


Les options disponibles sont définies comme suit :

· Allow : autorise tous les types de trafic sortant du réseau local vers Internet.

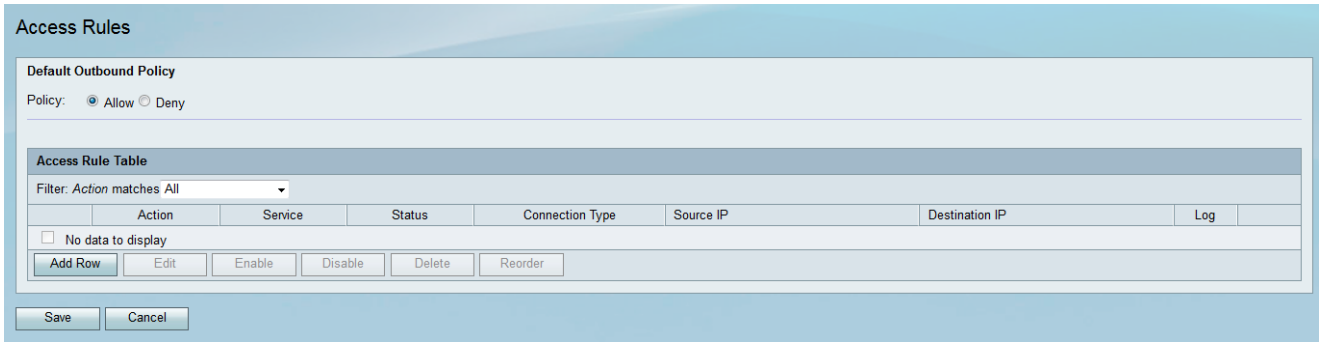
· Deny : bloque tous les types de trafic sortant du LAN vers Internet.

Étape 3. Cliquez sur Save pour enregistrer les paramètres.

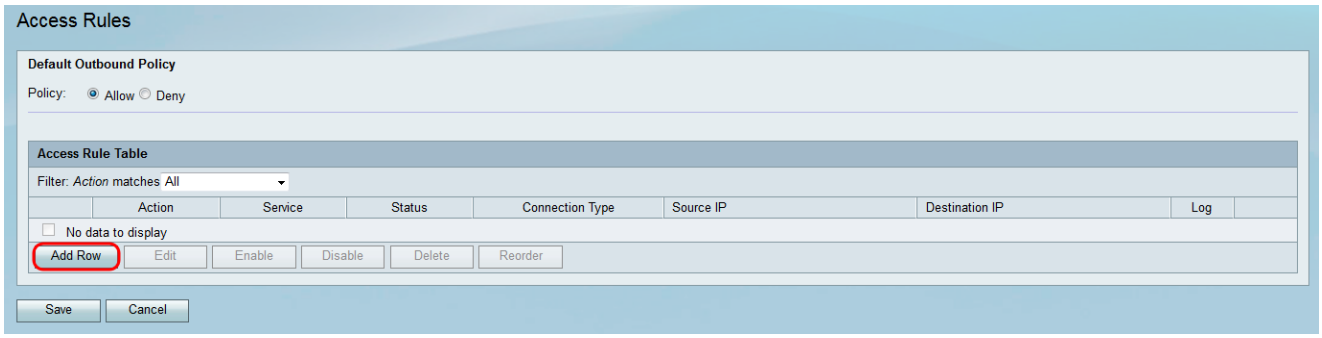


Ajout d'une règle d'accès

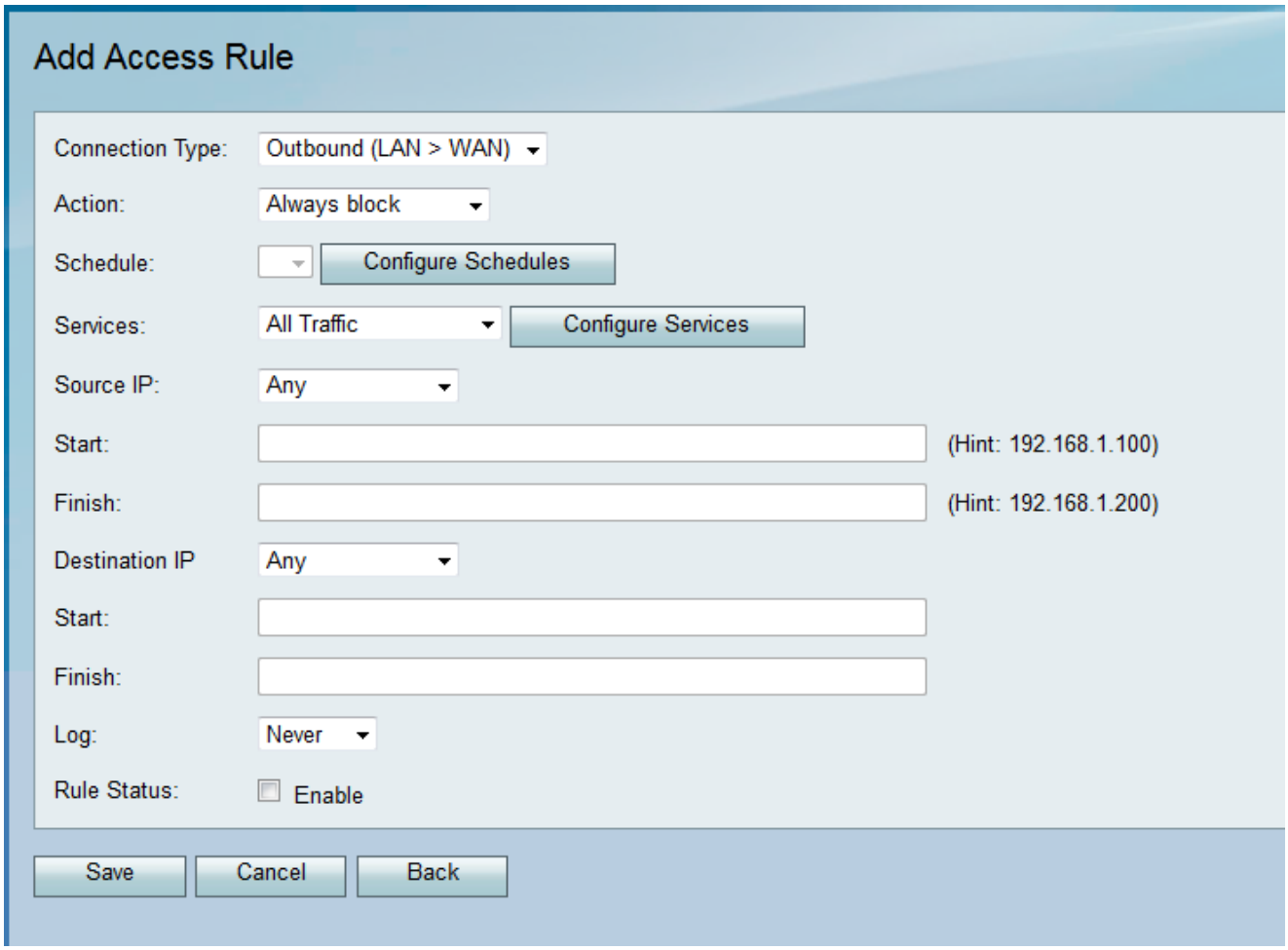
Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Firewall > Access Rules. La fenêtre Access Rules s'ouvre :



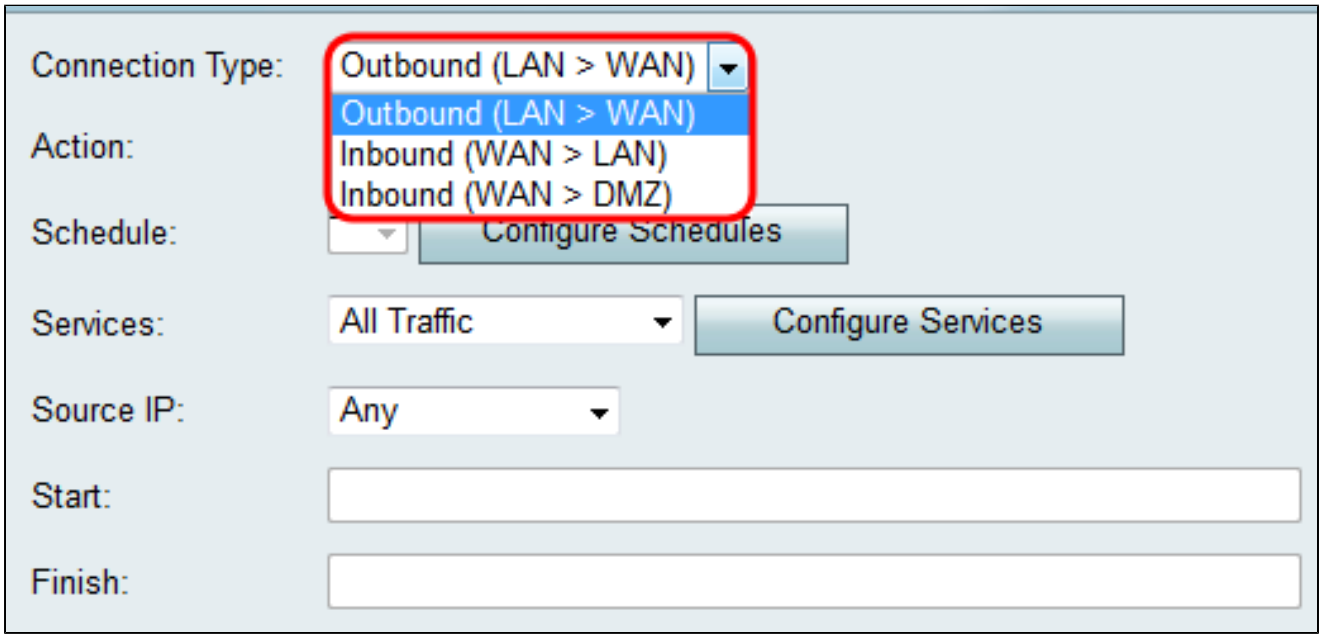
Étape 2. Cliquez sur Add Row dans le tableau Access Rule pour ajouter une nouvelle règle d'accès.



La page Ajouter une règle d'accès s'ouvre :



Étape 3. Dans la liste déroulante Type de connexion, sélectionnez le type de trafic auquel la règle s'applique.



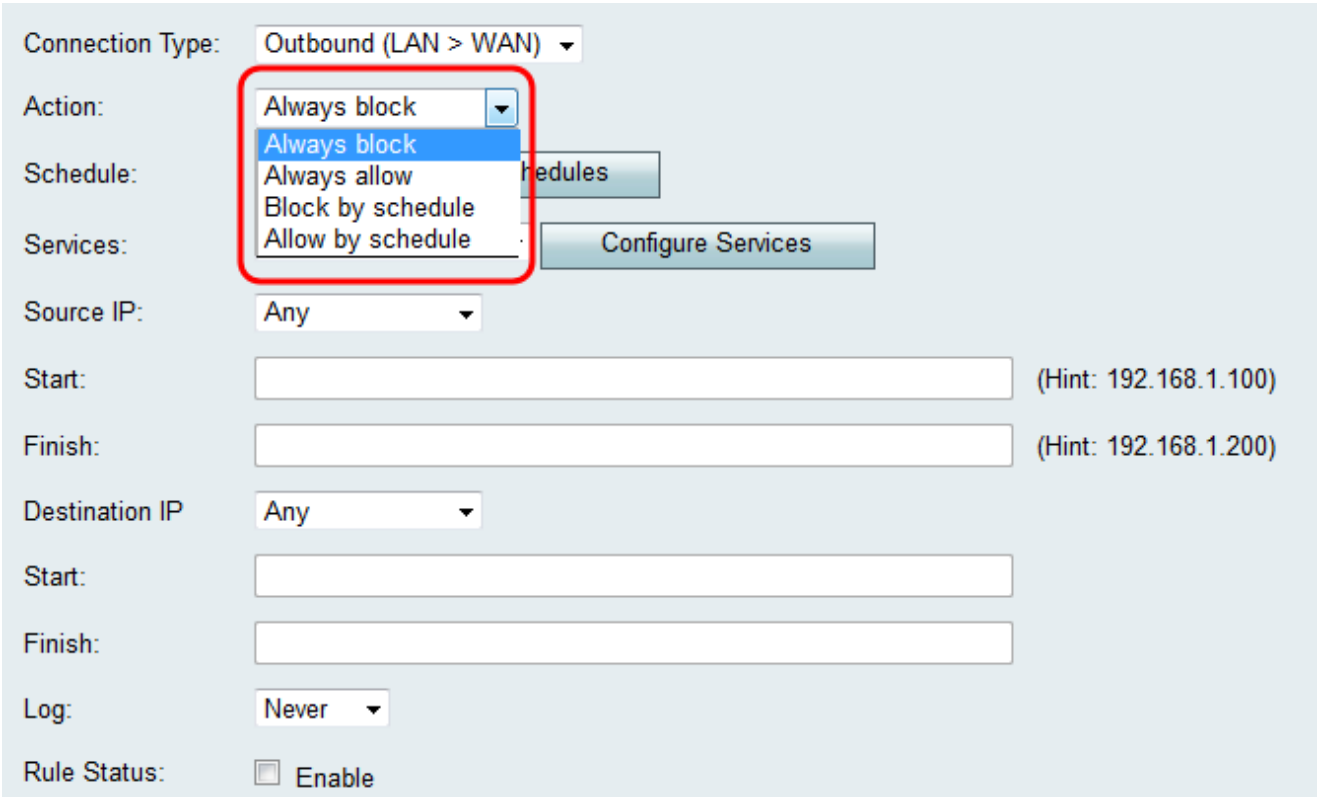
Les options disponibles sont définies comme suit :

· Sortant (LAN > WAN) - La règle affecte les paquets qui proviennent du réseau local (LAN) et qui vont sur Internet (WAN).

· Entrant (WAN > LAN) - La règle affecte les paquets qui proviennent d'Internet (WAN) et qui vont dans le réseau local (LAN).

· Entrant (WAN > DMZ) : la règle affecte les paquets qui proviennent d'Internet (WAN) et qui entrent dans le sous-réseau de la zone démilitarisée (DMZ).

Étape 4. Dans la liste déroulante Action, sélectionnez l'action à entreprendre lorsqu'une règle est mise en correspondance.



Les options disponibles sont définies comme suit :

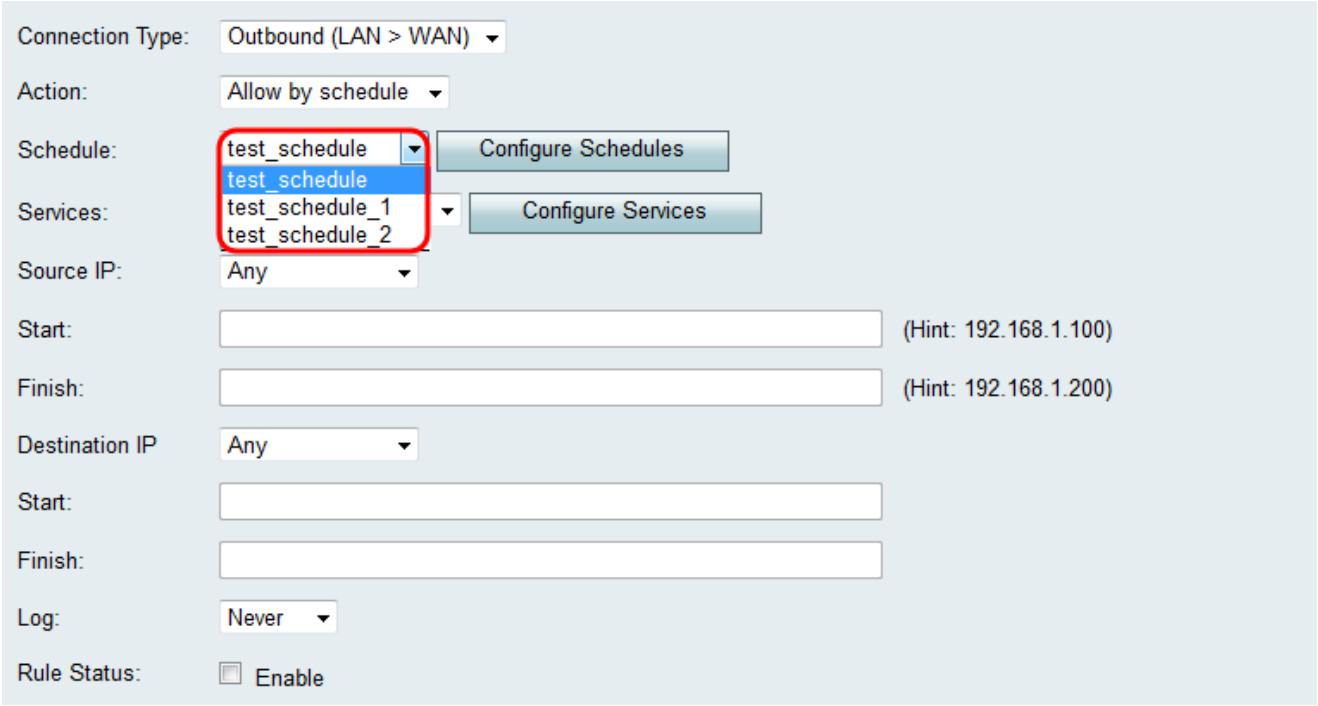
· Always Block : refusez toujours l'accès si les conditions sont remplies. Passez à l'étape 6.

· Toujours autoriser — Toujours autoriser l'accès si les conditions sont respectées. Passez à l'étape 6.

· Block by schedule : refusez l'accès si les conditions sont respectées lors d'un planning préconfiguré.

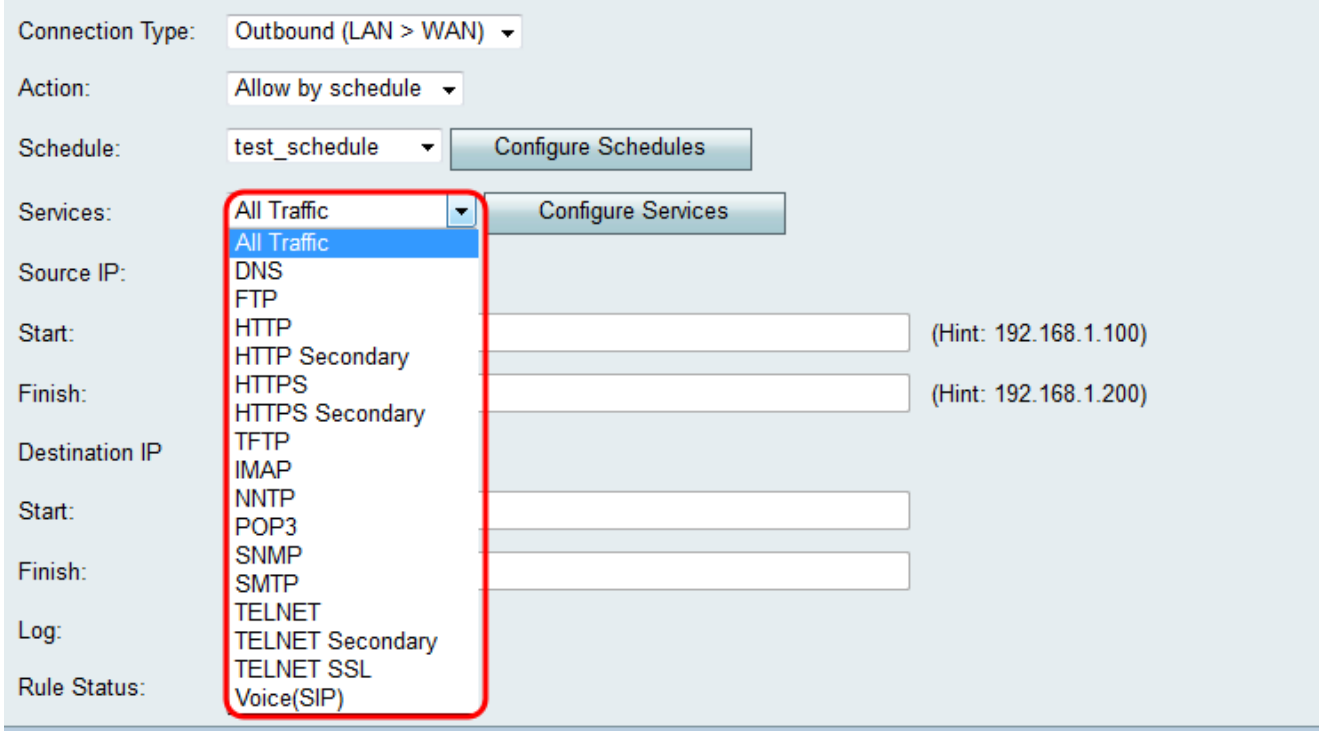
· Allow by schedule : autorise l'accès si les conditions sont respectées lors d'un planning préconfiguré.

Étape 5. Si vous avez choisi Bloquer par planification ou Autoriser par planification à l'étape 4, choisissez la planification appropriée dans la liste déroulante Planification.



Remarque : pour créer ou modifier une planification, cliquez sur Configurer les planifications. Référez-vous à Configuration des plannings sur les RV130 et RV130W pour plus d'informations et de directives.

Étape 6. Choisissez le type de service auquel la règle d'accès s'applique dans la liste déroulante Services.



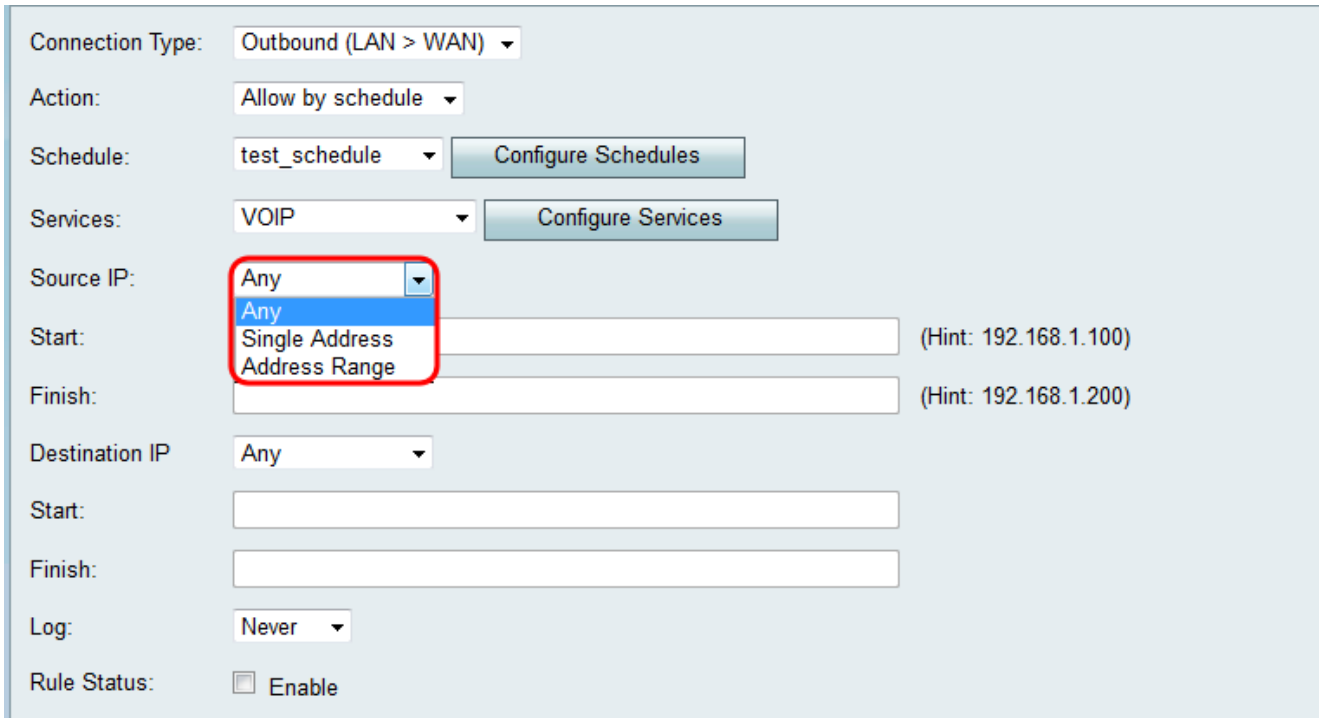
Remarque : si vous souhaitez ajouter ou modifier un service, cliquez sur Configurer les services. Référez-vous à Configuration de la gestion des services sur les RV130 et RV130W pour plus d'informations et de directives.

Configuration des adresses IP source et de destination pour le trafic sortant

Suivez les étapes de cette section si Outbound (LAN > WAN) a été sélectionné comme type de connexion à l'étape 3 de Adding an Access Rule.

Remarque : si un type de connexion entrante a été sélectionné à l'étape 3 de l'ajout d'une règle d'accès, passez à la section suivante : Configuration des adresses IP source et de destination pour le trafic entrant.

Étape 1. Choisissez la manière dont vous souhaitez définir l'IP source dans la liste déroulante Source IP. Pour le trafic sortant, l'adresse IP source fait référence à la ou aux adresses (dans le réseau local) auxquelles la règle de pare-feu s'appliquerait.



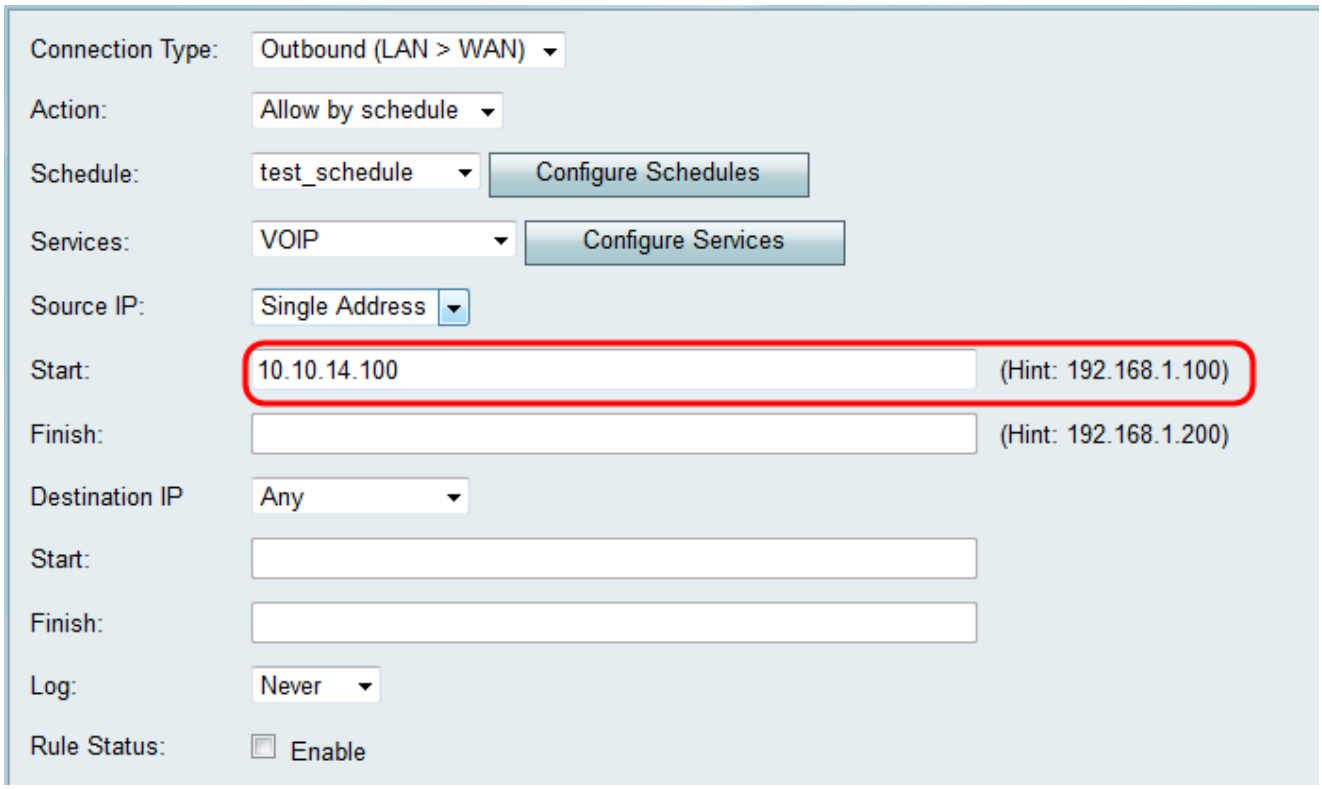
Les options disponibles sont définies comme suit :

· Any : s'applique au trafic provenant de toute adresse IP du réseau local. Par conséquent, laissez les champs Start et Finish vides. Passez à l'étape 4 si vous choisissez cette option.

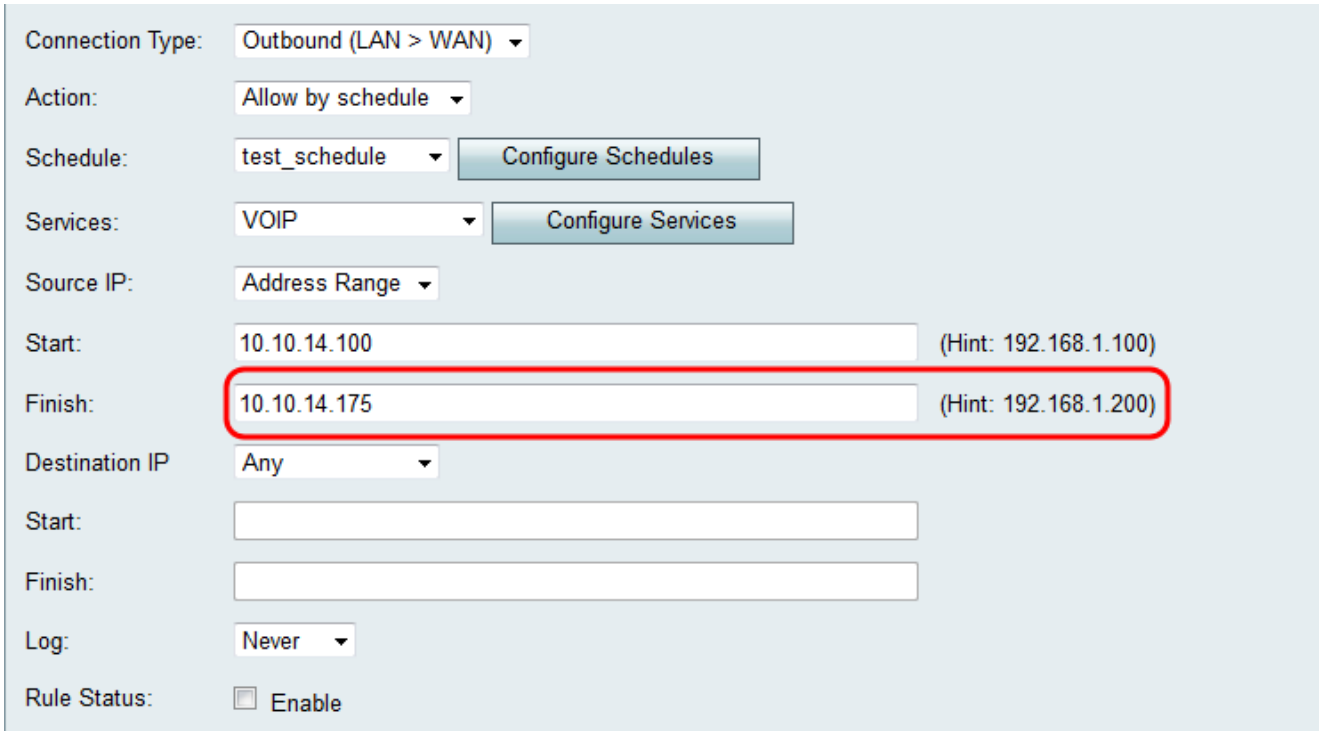
· Single Address : s'applique au trafic provenant d'une adresse IP unique sur le réseau local. Saisissez l'adresse IP dans le champ Start.

· Address Range : s'applique au trafic provenant d'une plage d'adresses IP sur le réseau local. Entrez l'adresse IP de début de la plage dans le champ Start et l'adresse IP de fin dans le champ Finish afin de définir la plage.

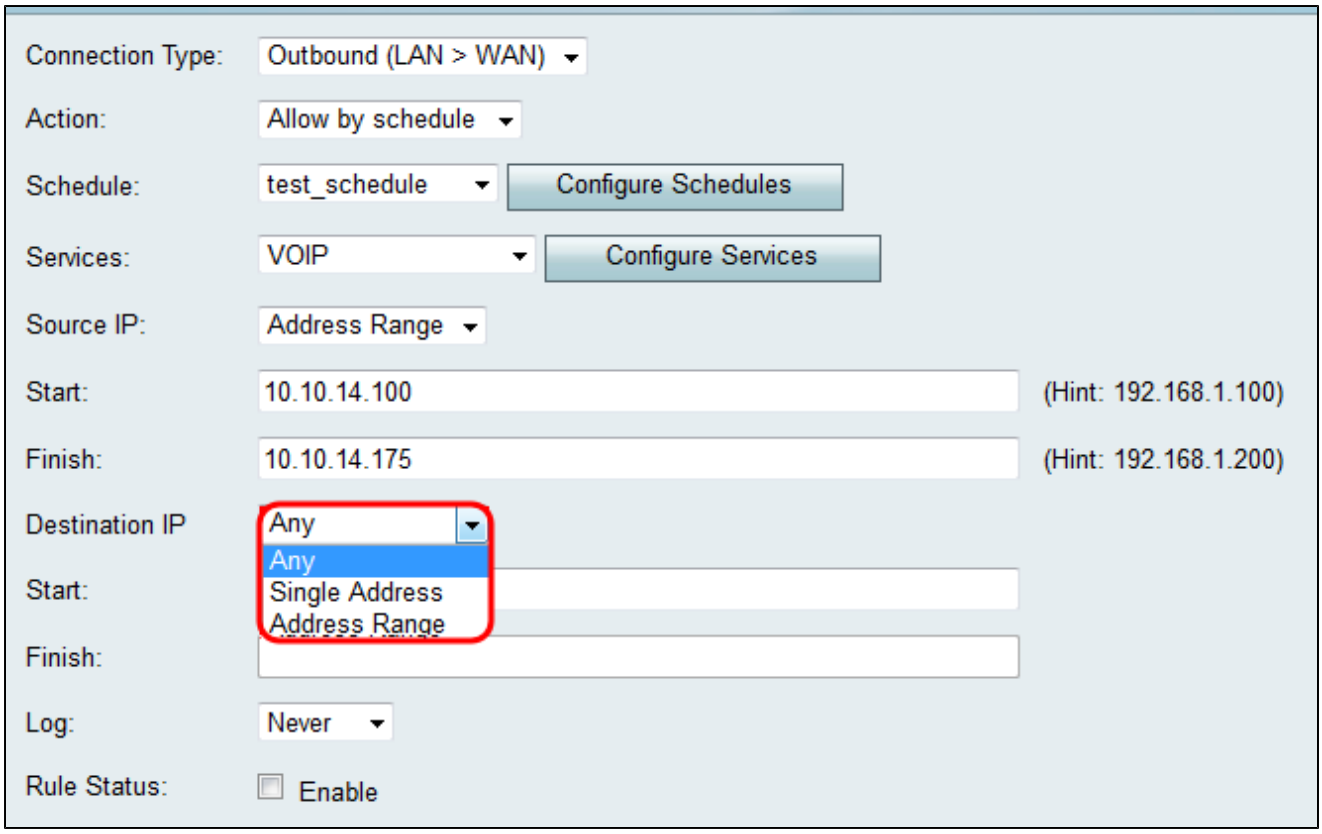
Étape 2. Si vous avez choisi Single Address à l'étape 1, entrez l'adresse IP qui sera appliquée à la règle d'accès dans le champ Start , puis passez à l'étape 4. Si vous avez choisi Plage d'adresses à l'étape 1, entrez une adresse IP de début qui sera appliquée à la règle d'accès dans le champ Début.



Étape 3. Si vous avez choisi Address Range à l'étape 1, entrez l'adresse IP de fin qui encapsulera la plage d'adresses IP pour la règle d'accès dans le champ Finish.



Étape 4. Choisissez le mode de définition de l'adresse IP de destination dans la liste déroulante Destination IP. Pour le trafic sortant, l'adresse IP de destination fait référence à l'adresse ou aux adresses (dans le réseau étendu) auxquelles le trafic est autorisé ou refusé à partir du réseau local.



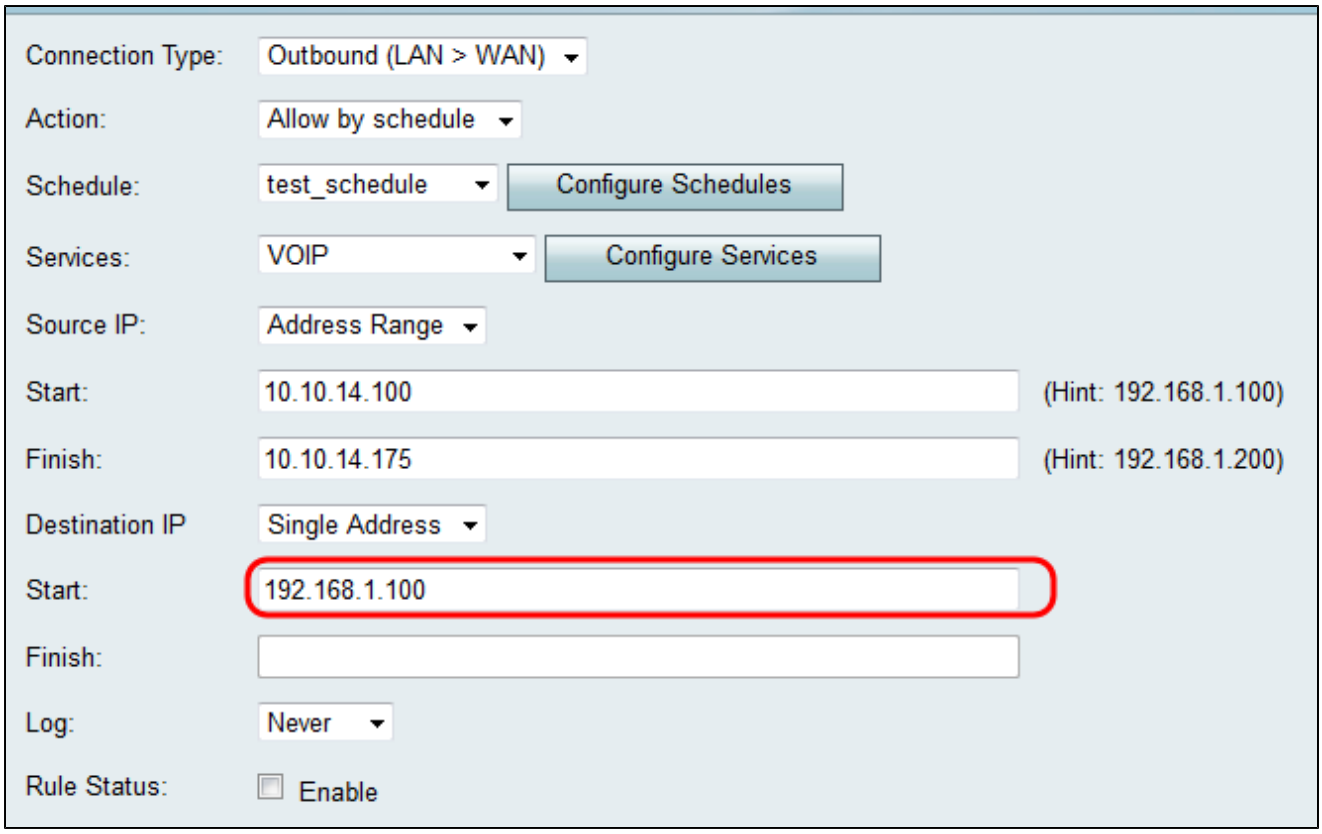
Les options disponibles sont définies comme suit :

· Any : s'applique au trafic dirigé vers n'importe quelle adresse IP sur l'Internet public. Par conséquent, laissez les champs Start et Finish vides.

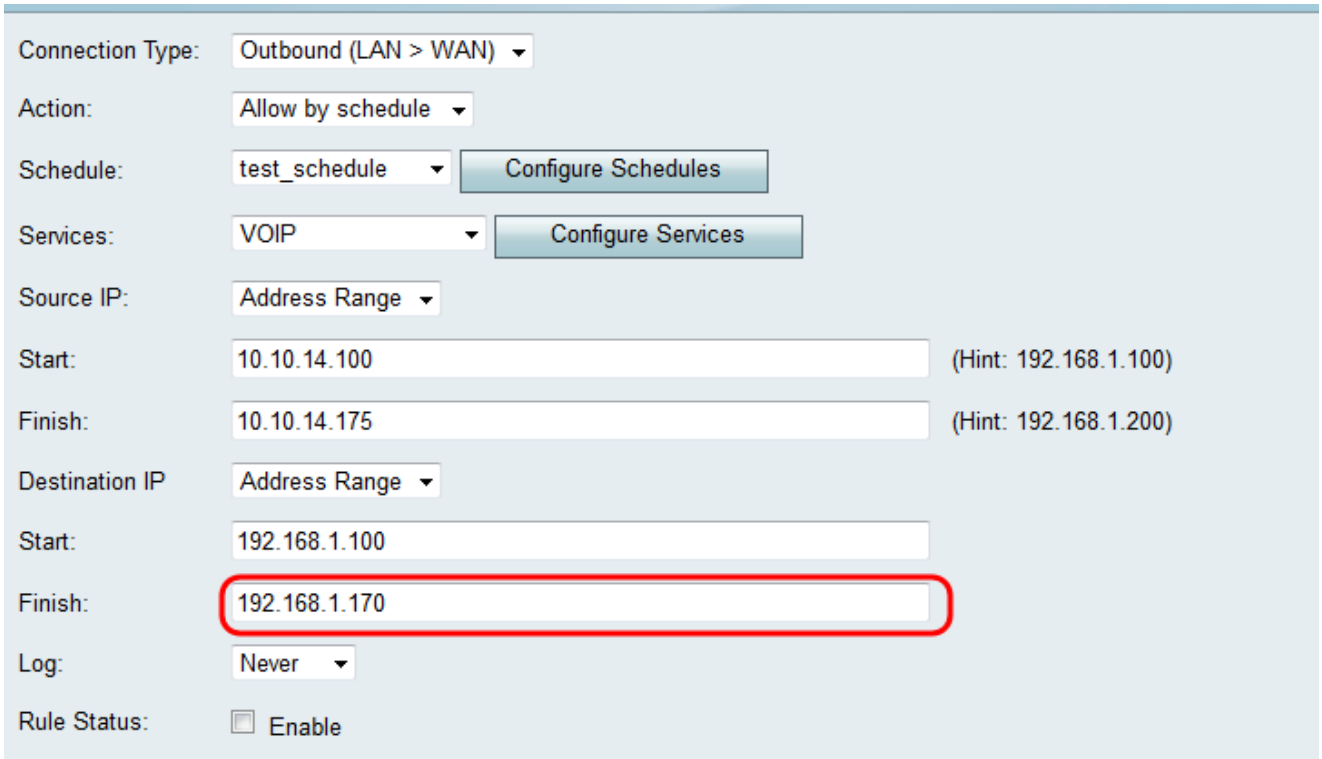
· Single Address : s'applique au trafic acheminé vers une adresse IP unique sur l'Internet public. Saisissez l'adresse IP dans le champ Start.

· Plage d'adresses : s'applique au trafic dirigé vers une plage d'adresses IP sur l'Internet public. Entrez l'adresse IP de début de la plage dans le champ Start et l'adresse IP de fin dans le champ Finish afin de définir la plage.

Étape 5. Si vous avez choisi Single Address à l'étape 4, entrez l'adresse IP qui sera appliquée à la règle d'accès dans le champ Start. Si vous avez choisi Plage d'adresses à l'étape 4, entrez une adresse IP de début qui sera appliquée à la règle d'accès dans le champ Début.



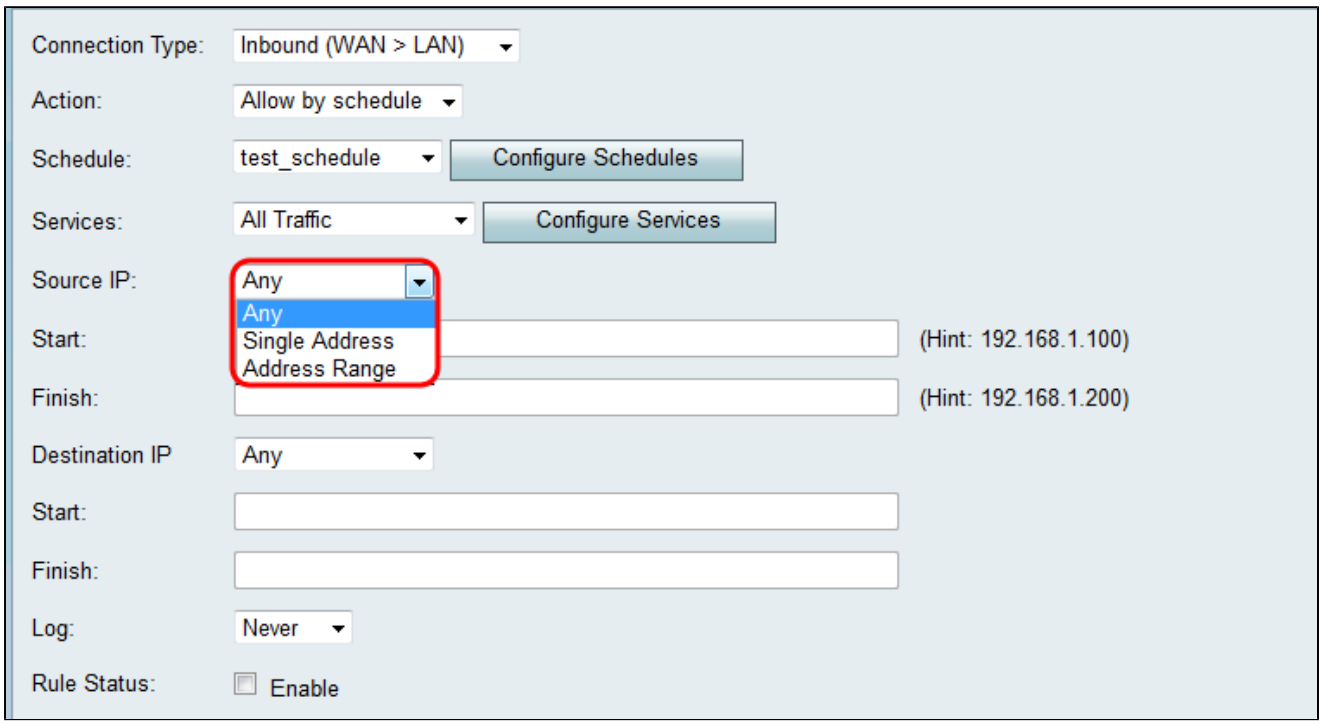
Étape 6. Si vous avez choisi Address Range à l'étape 4, entrez l'adresse IP de fin qui encapsulera la plage d'adresses IP pour la règle d'accès dans le champ Finish.



Configuration des adresses IP source et de destination pour le trafic entrant

Suivez les étapes de cette section si le type de connexion entrant (WAN > LAN) ou entrant (WAN > DMZ) a été sélectionné à l'étape 3 de l'ajout d'une règle d'accès.

Étape 1. Choisissez la manière dont vous souhaitez définir l'IP source dans la liste déroulante Source IP. Pour le trafic entrant, l'adresse IP source fait référence à la ou aux adresses (dans le réseau étendu) auxquelles la règle de pare-feu s'appliquerait.



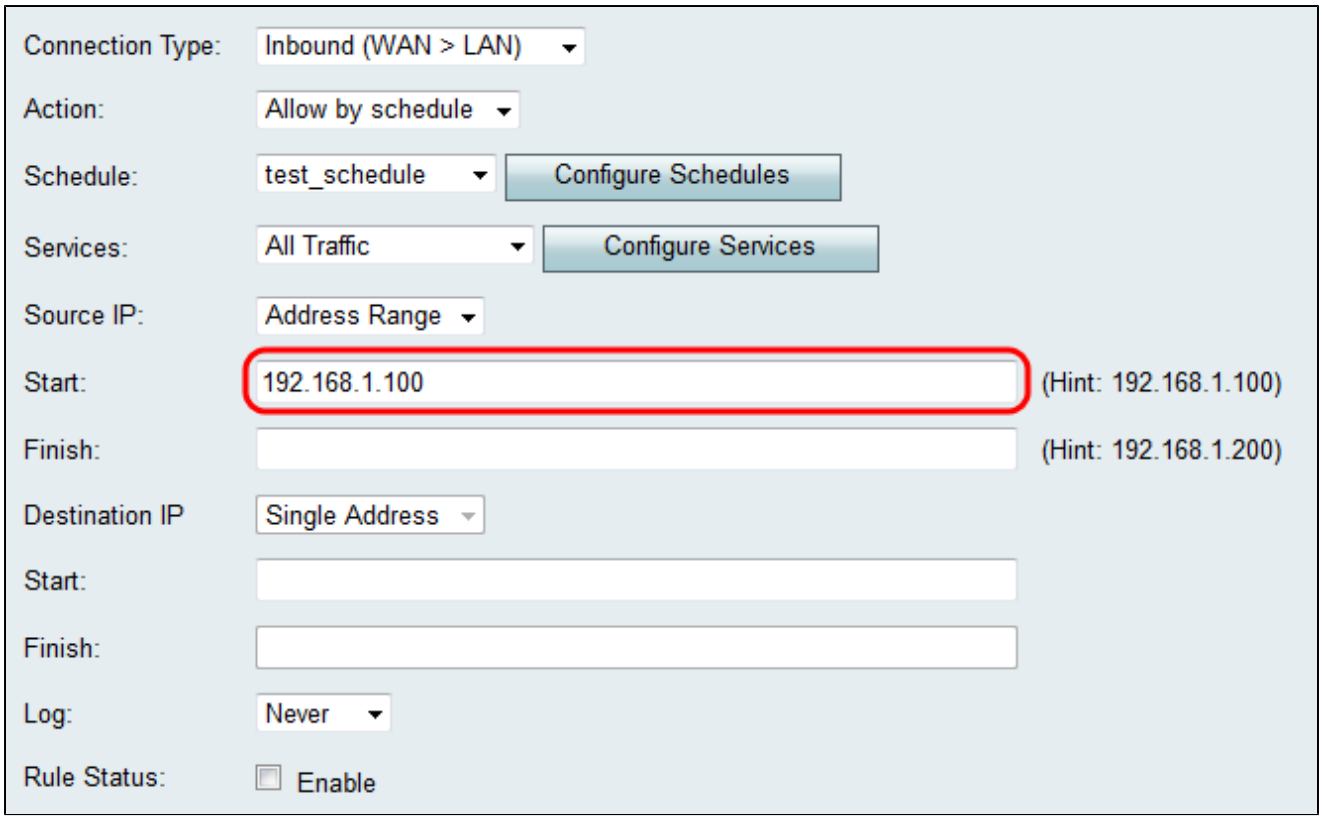
Les options disponibles sont définies comme suit :

· Any : s'applique au trafic provenant de n'importe quelle adresse IP sur l'Internet public. Par conséquent, laissez les champs Start et Finish vides. Passez à l'étape 4 si vous choisissez cette option.

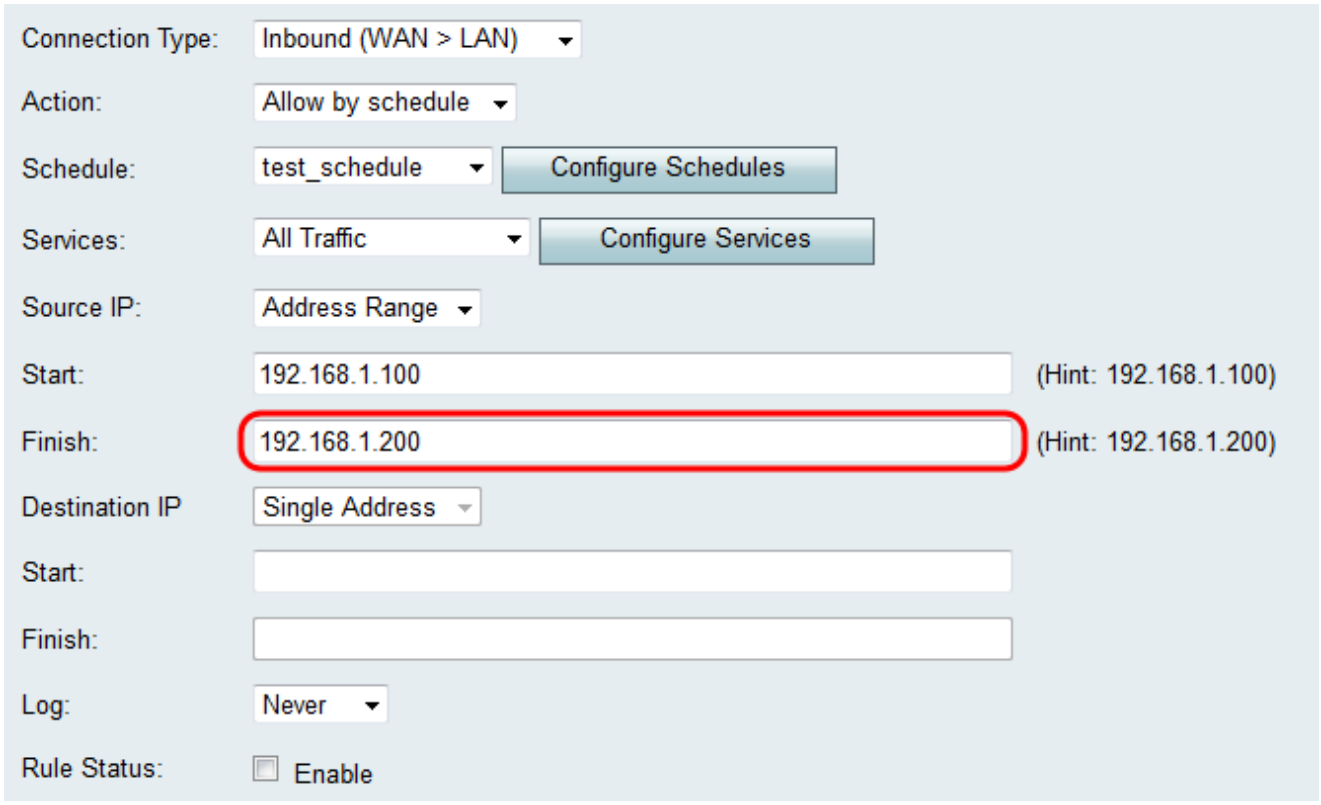
· Single Address : s'applique au trafic provenant d'une adresse IP unique sur l'Internet public. Saisissez l'adresse IP dans le champ Start.

· Address Range : s'applique au trafic provenant d'une plage d'adresses IP sur l'Internet public. Entrez l'adresse IP de début de la plage dans le champ Start et l'adresse IP de fin dans le champ Finish afin de définir la plage.

Étape 2. Si vous avez choisi Single Address à l'étape 1, entrez l'adresse IP qui sera appliquée à la règle d'accès dans le champ Start , puis passez à l'étape 4. Si vous avez choisi Address Range à l'étape 1, entrez une adresse IP de début qui sera appliquée à la règle d'accès dans le champ Start.

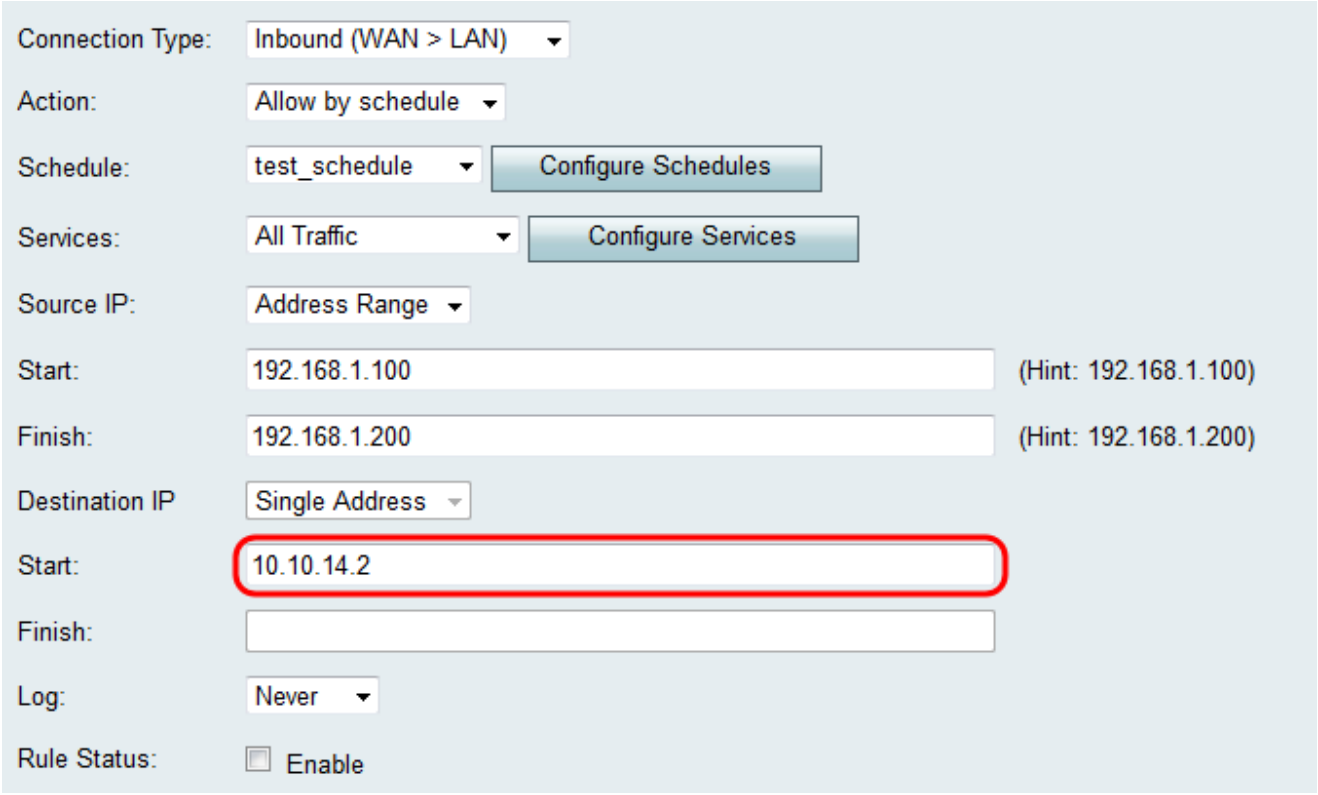


Étape 3. Si vous avez choisi Address Range à l'étape 1, entrez l'adresse IP de fin qui encapsulera la plage d'adresses IP pour la règle d'accès dans le champ Finish.



Étape 4. Entrez une adresse unique pour l'adresse IP de destination dans le champ Start sous la liste déroulante Destination IP. Pour le trafic entrant, l'adresse IP de destination fait

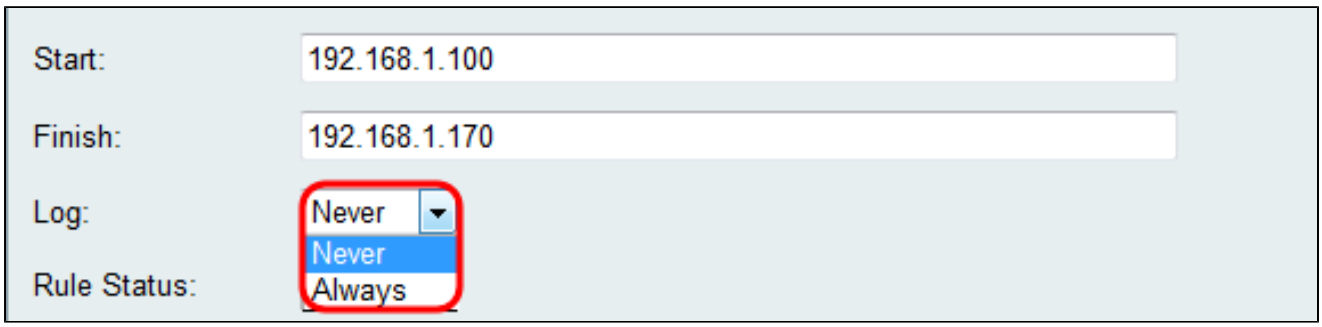
référence à l'adresse (dans le réseau local) à laquelle le trafic est autorisé ou refusé à partir de l'Internet public.



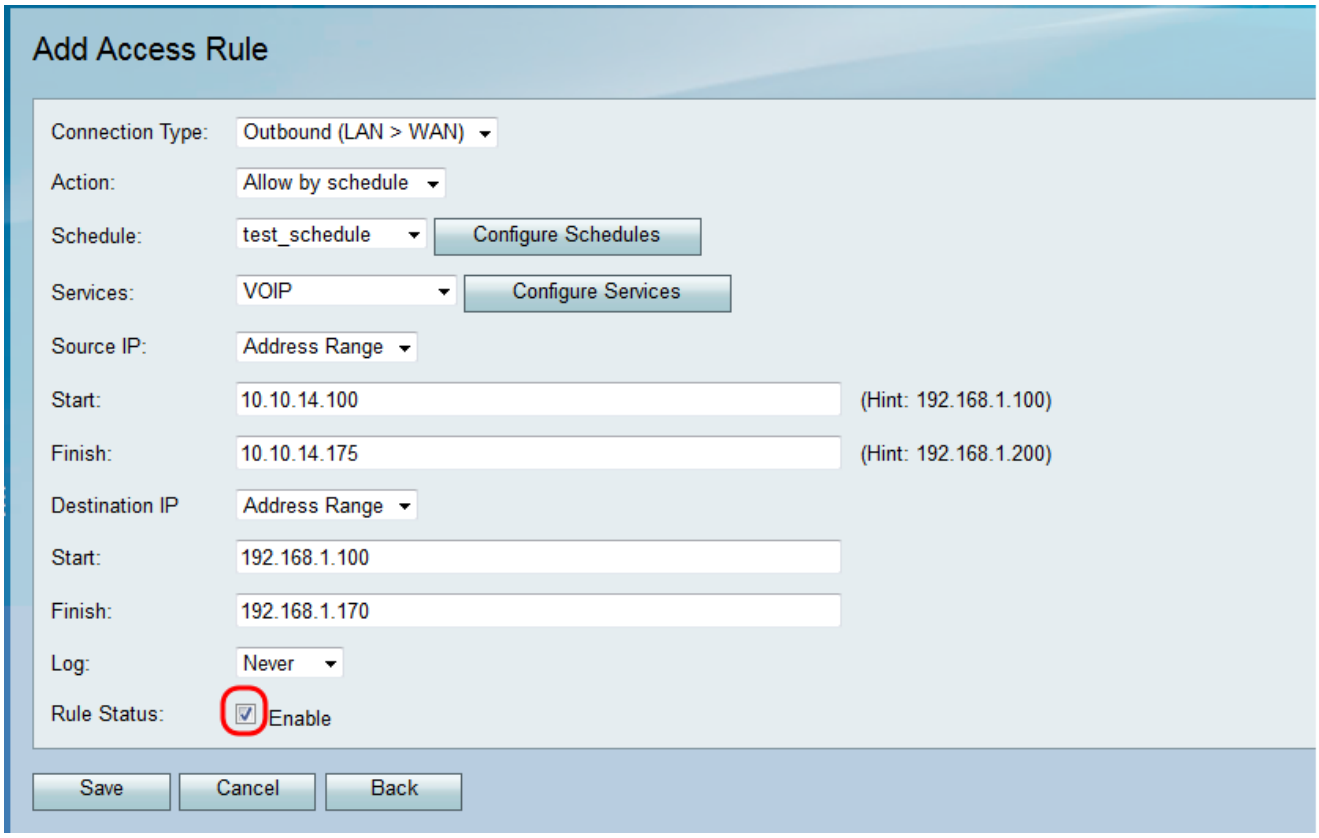
Remarque : si le type de connexion entrant (WAN > DMZ) a été sélectionné à l'étape 3 de l'ajout d'une règle d'accès, l'adresse unique de l'adresse IP de destination est automatiquement configurée avec l'adresse IP de l'hôte DMZ activé.

Journalisation et activation de la règle d'accès

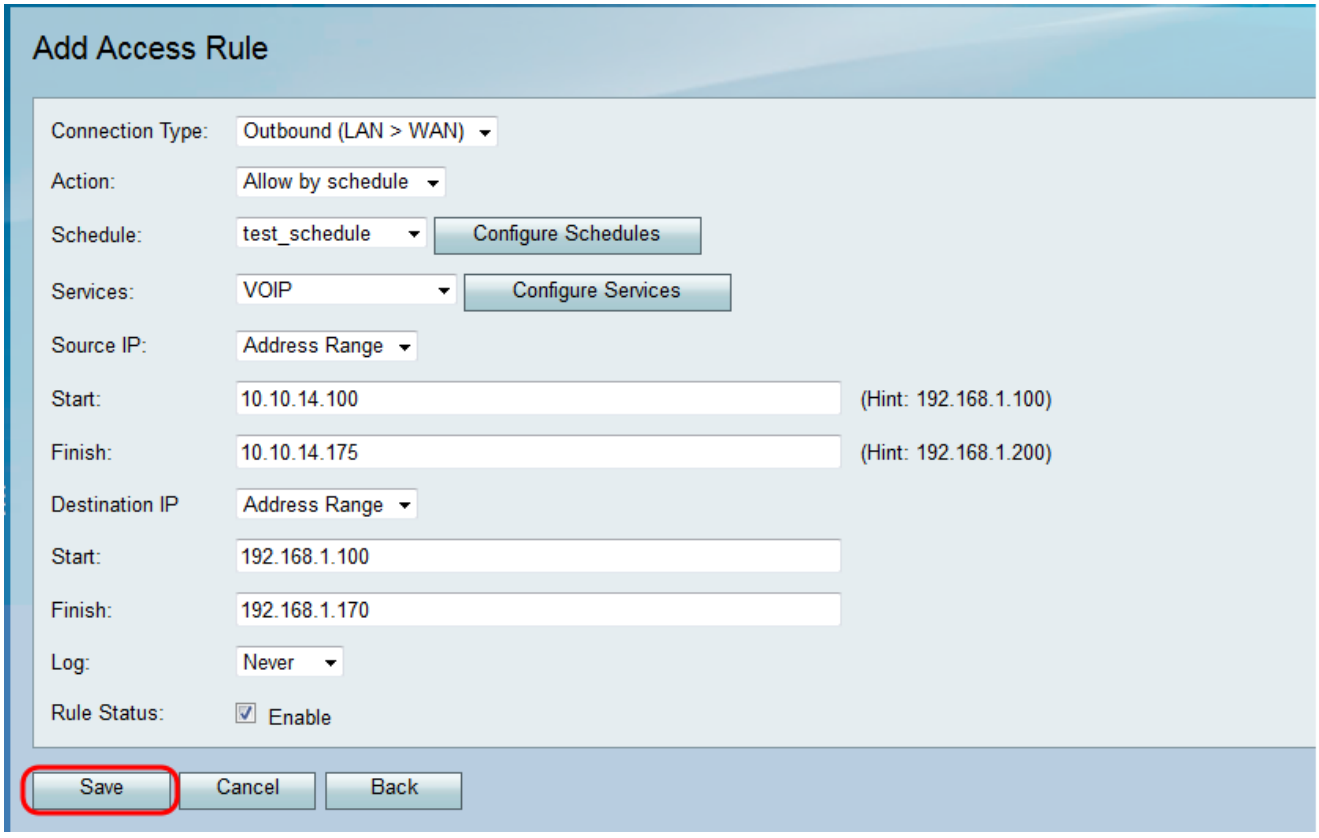
Étape 1. Sélectionnez Always dans la liste déroulante Log si vous souhaitez que le routeur crée des journaux chaque fois qu'un paquet correspond à une règle. Sélectionnez Jamais si vous souhaitez que la journalisation n'ait jamais lieu lorsqu'une règle est mise en correspondance.



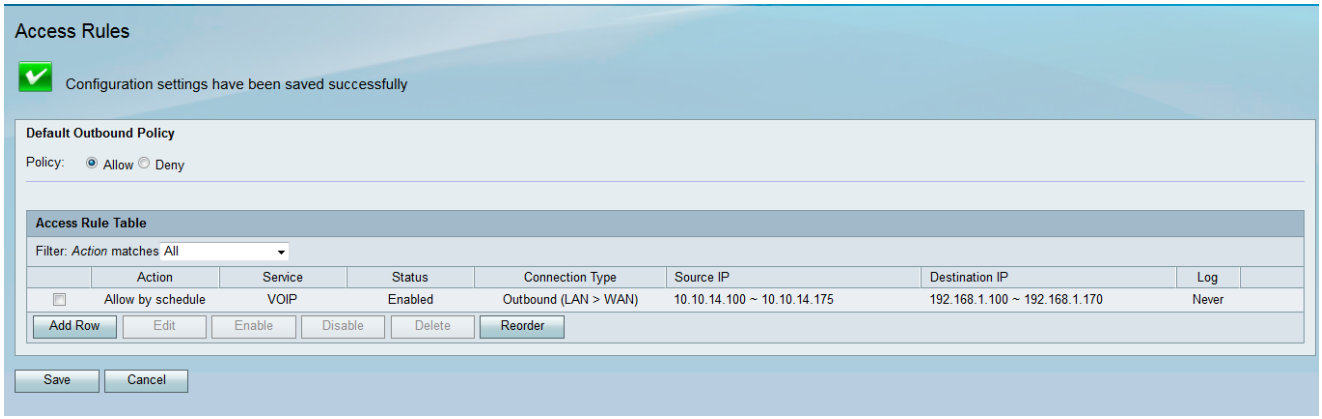
Étape 2. Cochez la case Enable pour activer la règle d'accès.



Étape 3. Cliquez sur Save pour enregistrer vos paramètres.



La table de règles d'accès est mise à jour avec la règle d'accès nouvellement configurée.



À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.