# Configurez les règles d'accès sur des Routeurs de gammes RV160 et RV260

## Objectif

Votre routeur est responsable de recevoir des données du réseau extérieur et est la première ligne de défense quand il s'agit de votre Sécurité de réseau local. En activant des règles d'accès sur votre routeur, vous pouvez filtrer des paquets basés sur des paramètres spécifiques tels que l'adresse IP ou le numéro de port. Avec les étapes a fourni ci-dessous, des objectifs de ce document pour vous guider sur la façon dont configurer des règles d'accès de contrôler mieux les paquets qui entrent dans votre réseau. Ce document mettra en valeur également quelques pratiques recommandées pour l'usage des règles d'accès à leur plein potentiel pour la meilleure Sécurité.

## Périphériques applicables

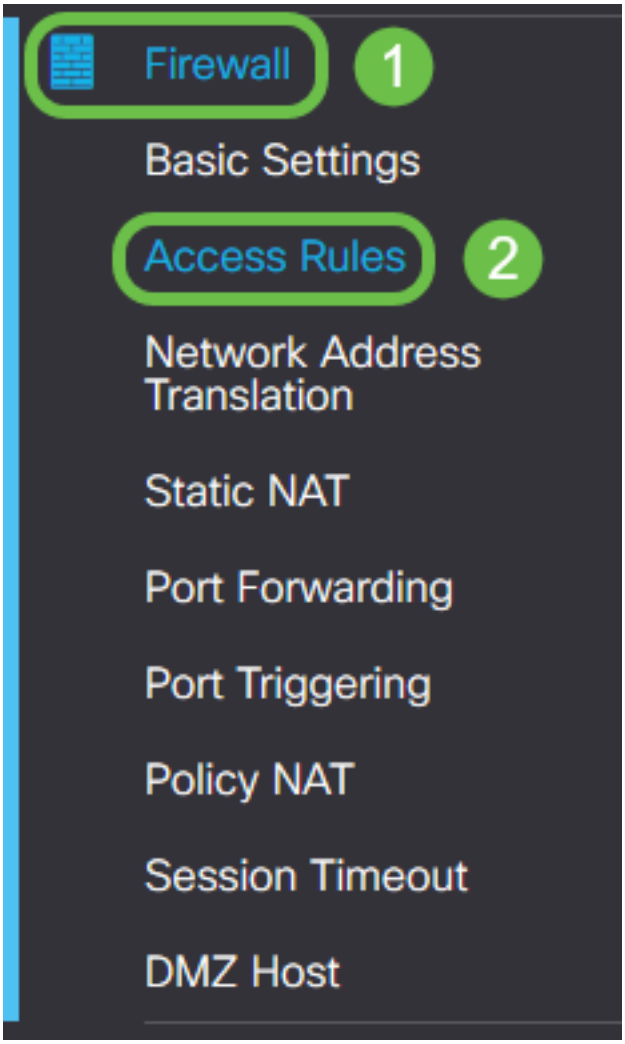
- RV160x
- RV260x

## Version de logiciel

- 1.0.00.13

## Configurez les règles d'accès

Étape 1. Du volet de navigation du côté gauche de l'utilitaire de configuration, **Pare-feu > règles d'accès** choisis.

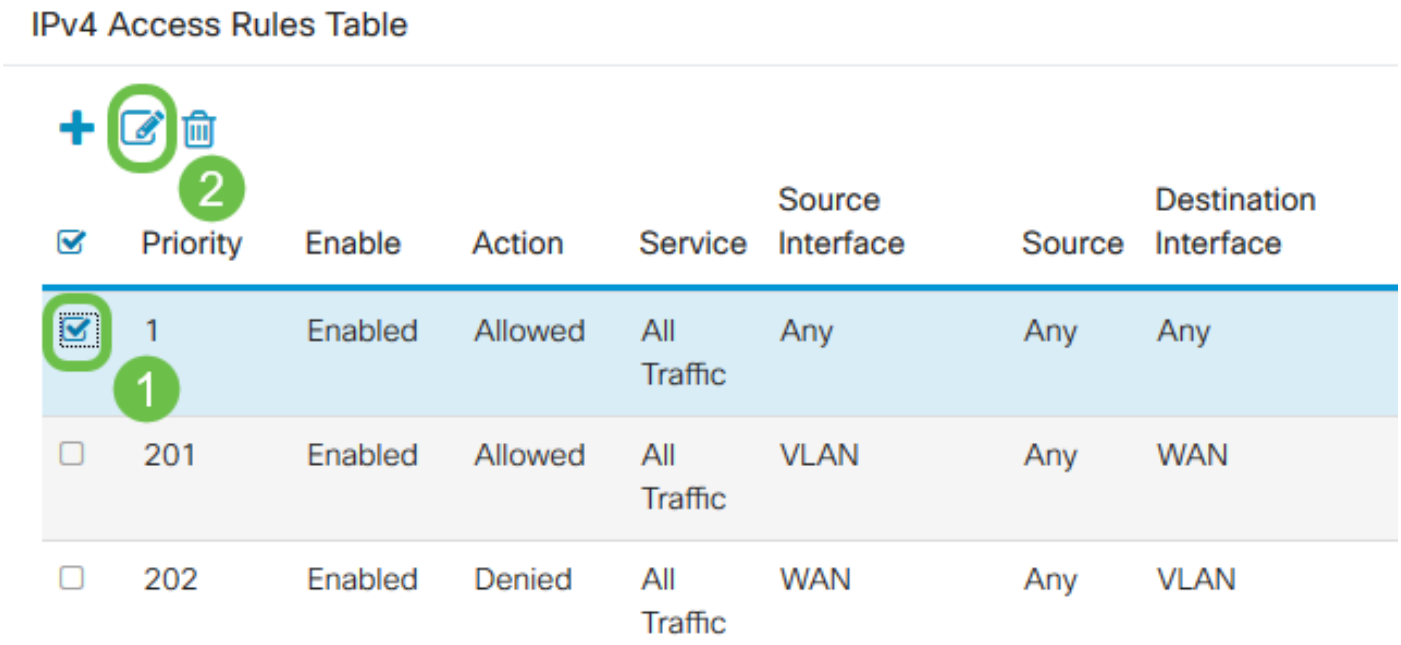



La page de règles d'accès paraît. À cette page il y a des tables contenant des listes de règles d'accès et de leurs attributs pour l'ipv4 et l'IPv6 respectivement. D'ici vous pouvez ajouter une nouvelle règle d'accès, éditer une règle existante, ou retirer une règle existante.

## Add/Edit une règle d'accès

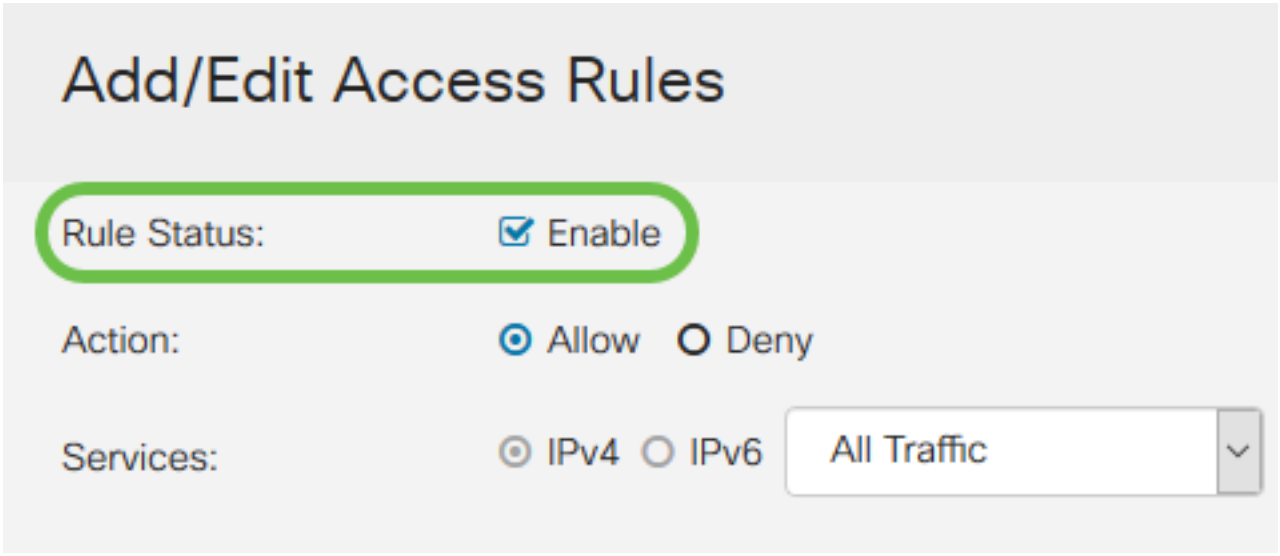
**Étape 2.** Pour ajouter une nouvelle règle d'accès, cliquez sur l'icône bleue pour ajouter dans la table de règles d'accès d'ipv4 ou de règles d'accès d'IPv6 selon à quel protocole vous comme la règle de s'appliquer. Dans ce cas, l'ipv4 est utilisé.


Pour éditer une entrée existante, sélectionnez la case à cocher à côté de la règle d'accès que vous voudriez modifier. Sélectionnez alors le bleu éditent l'icône en haut de la table correspondante. Seulement une règle peut être sélectionnée à la fois pour éditer.

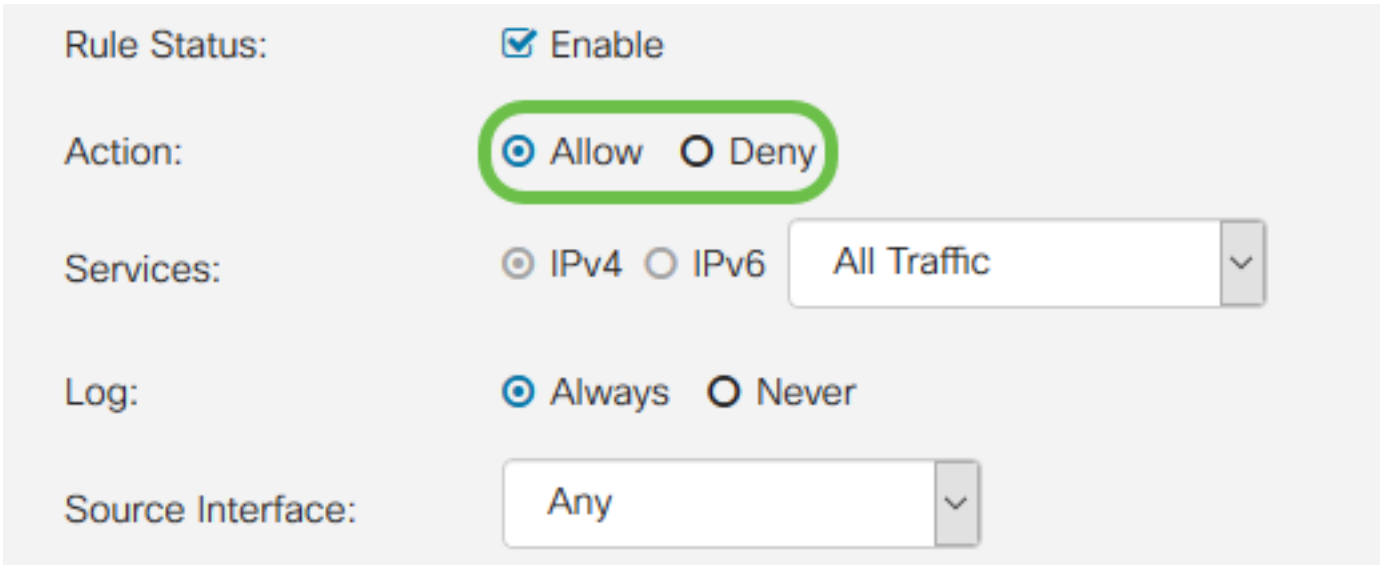



La page de *règles d'accès d'Add/Edit* paraît.

Étape 3. Vérifiez/décochez la case à cocher pour que l'état de règle active ou pour désactive la règle d'accès lors du fonctionnement. C'est utile quand vous avez une règle d'accès que vous voudriez sauvegarder pour s'appliquer à une date ultérieure.

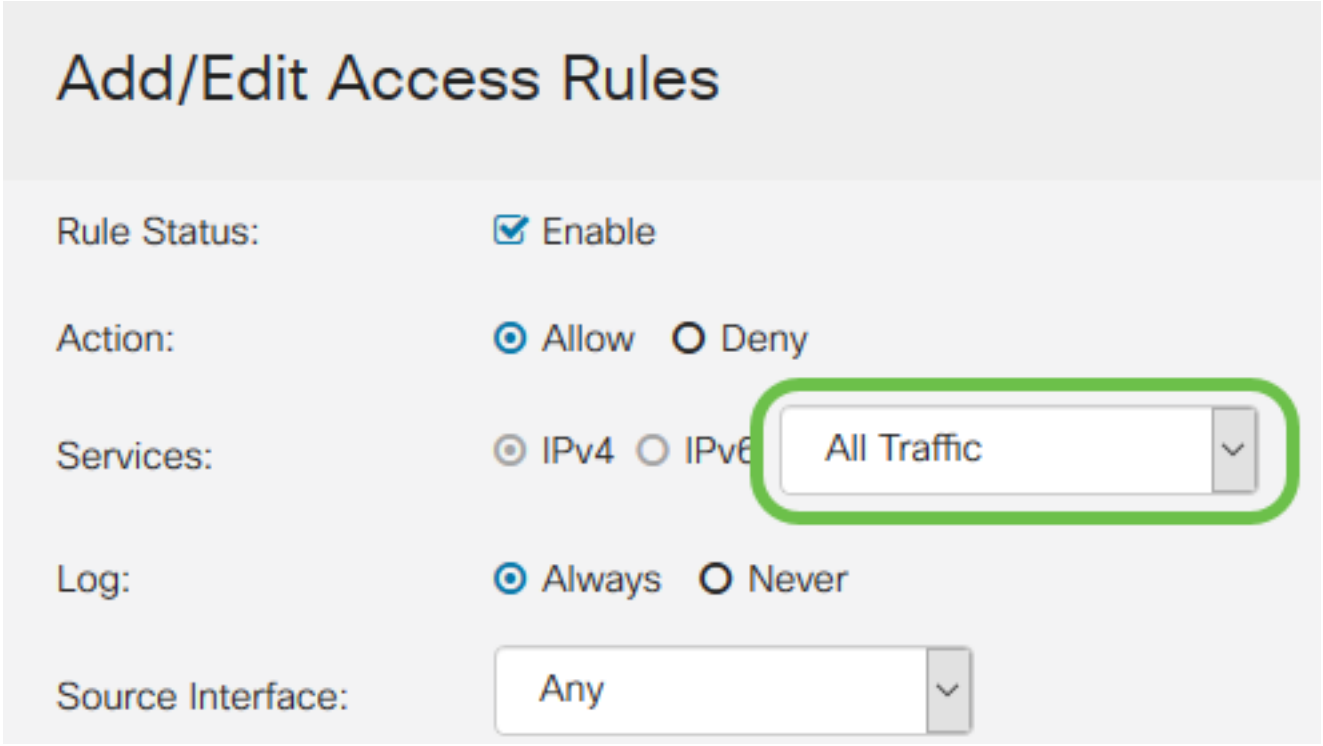



Étape 4. Du champ action, sélectionnez si la règle devrait permettre ou refuser l'accès au trafic réseau entrant à spécifier.



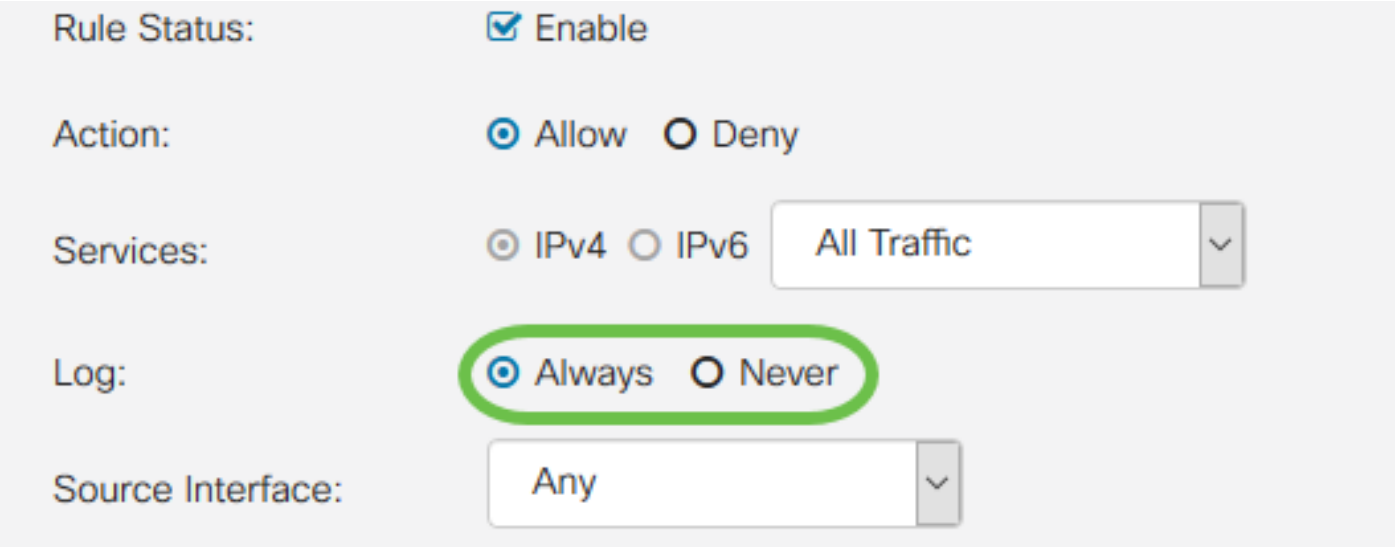

**Remarque:** Il est recommandé pour que la meilleure Sécurité place les règles d'accès qui permettent seulement le trafic que vous comptez recevoir, plutôt qu'essayant de refuser seulement le trafic indésirable. Ceci protégera mieux votre réseau contre des menaces inconnues.

Étape 5. Dans le domaine de *services*, choisi du menu déroulant le type de service réseau que vous comme la règle d'accès de s'appliquer à.

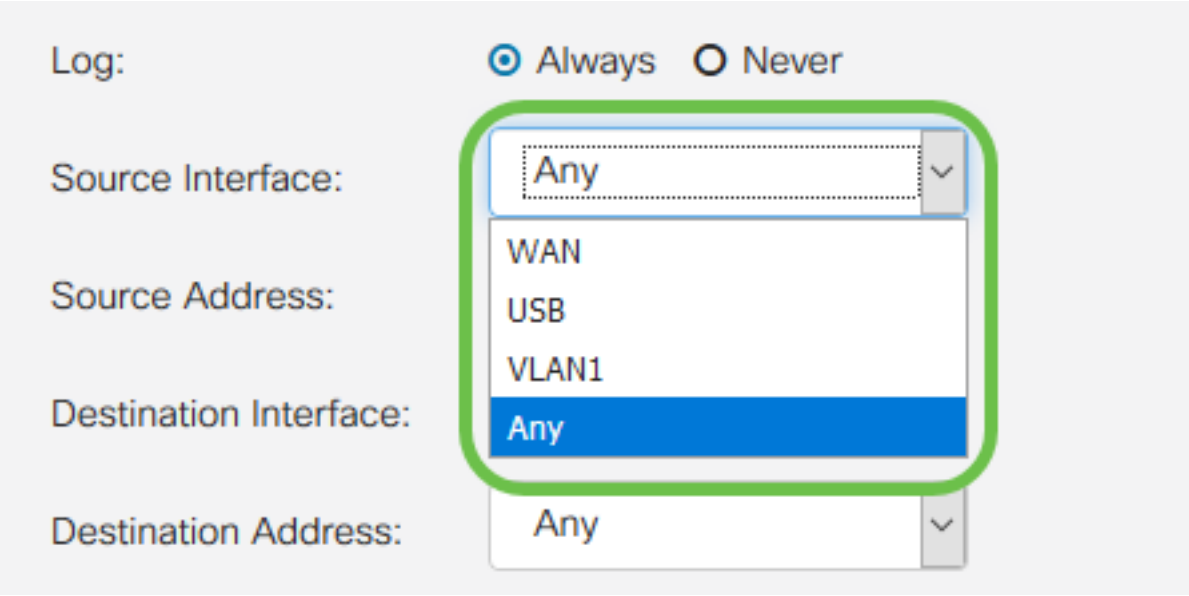



**Remarque:** La case d'option d'ipv4 ou d'IPv6 est automatiquement sélectionnée basée sur la table que vous avez choisi de s'appliquer la règle d'accès à de la page de *règles d'accès*.

Étape 6. Choisissez parmi le champ de *log* si vous comme le routeur génèreriez des paquets d'un message de log une fois écrivant votre réseau appariez les règles appliquées.



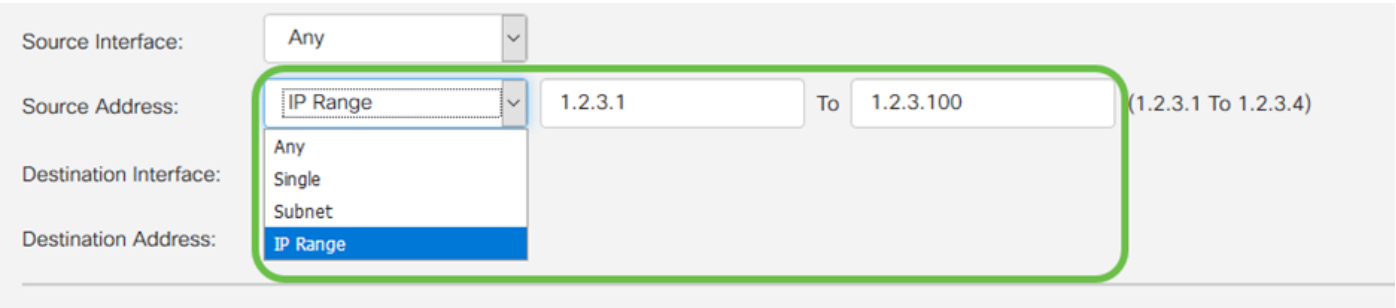

Étape 7. De la liste déroulante d'*interface de source*, sélectionnez l'interface réseau pour les paquets entrant vers lesquels la règle d'accès s'appliquera.




Étape 8. Choisissez parmi la liste déroulante d'*adresse source le* type d'adresse entrante que la règle d'accès s'appliquera à. Les options sont comme suit :

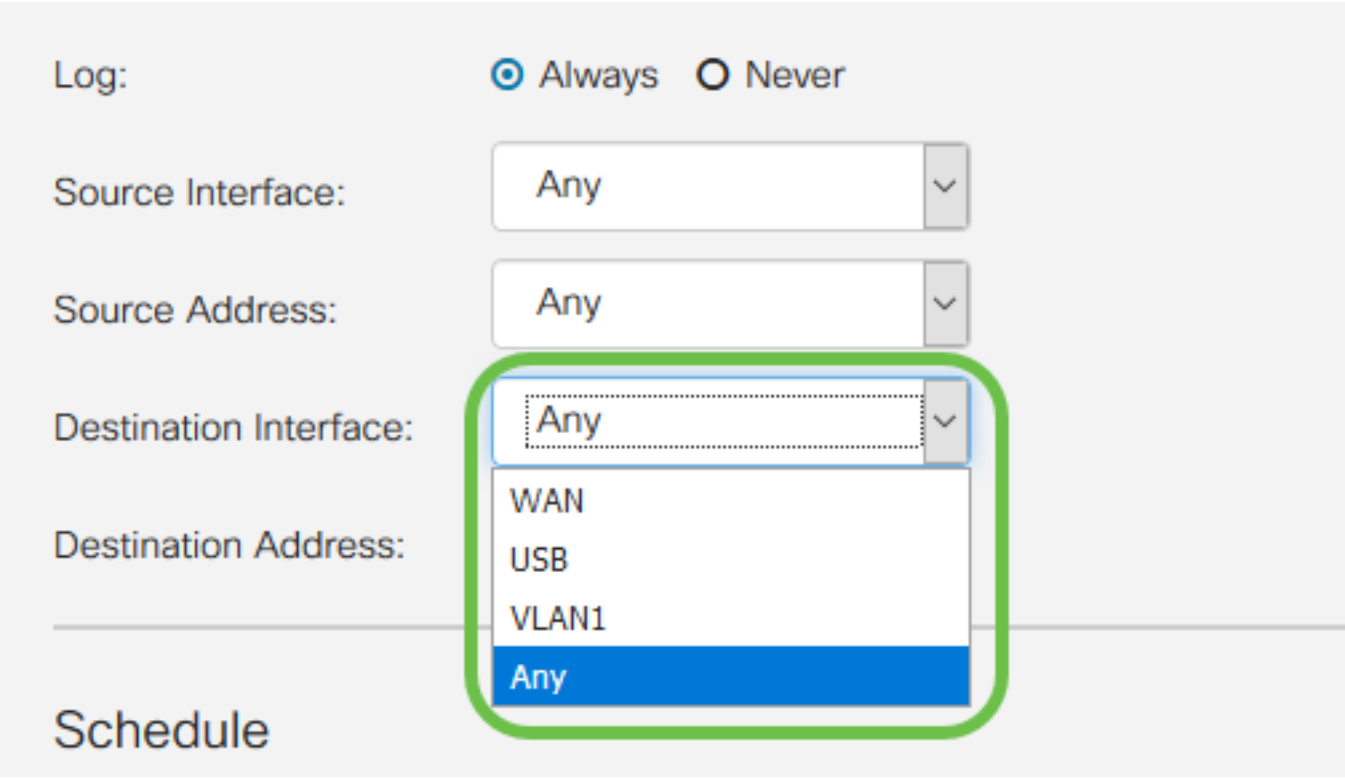
- Quels - La règle s'appliquera à toutes les adresses IP entrantes
- Simple - La règle s'appliquera à une adresse IP définie simple
- Sous-réseau - La règle s'appliquera à un sous-réseau défini d'un réseau
- Plage IP - La règle s'appliquera à une plage définie des adresses IP

**Remarque:** Si vous sélectionnez simple, le sous-réseau, ou la plage IP, des champs correspondants apparaîtra à la droite du menu déroulant où vous pouvez écrire des détails d'adresse. Dans cet exemple une plage IP est écrite pour expliquer.




Étape 9. De la liste déroulante d'*interface de destination*, sélectionnez l'interface réseau pour les

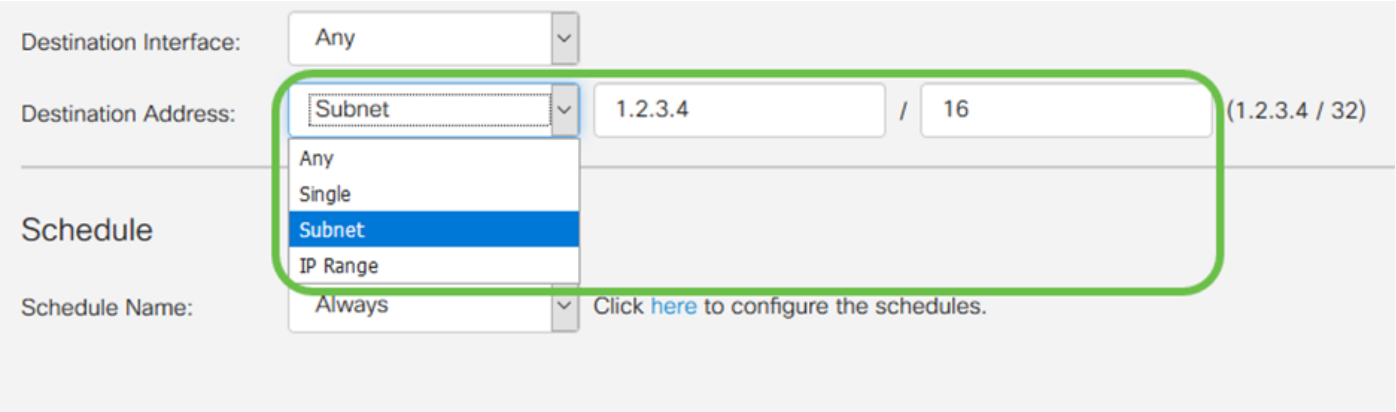
paquets sortants vers lesquels la règle d'accès s'appliquera.



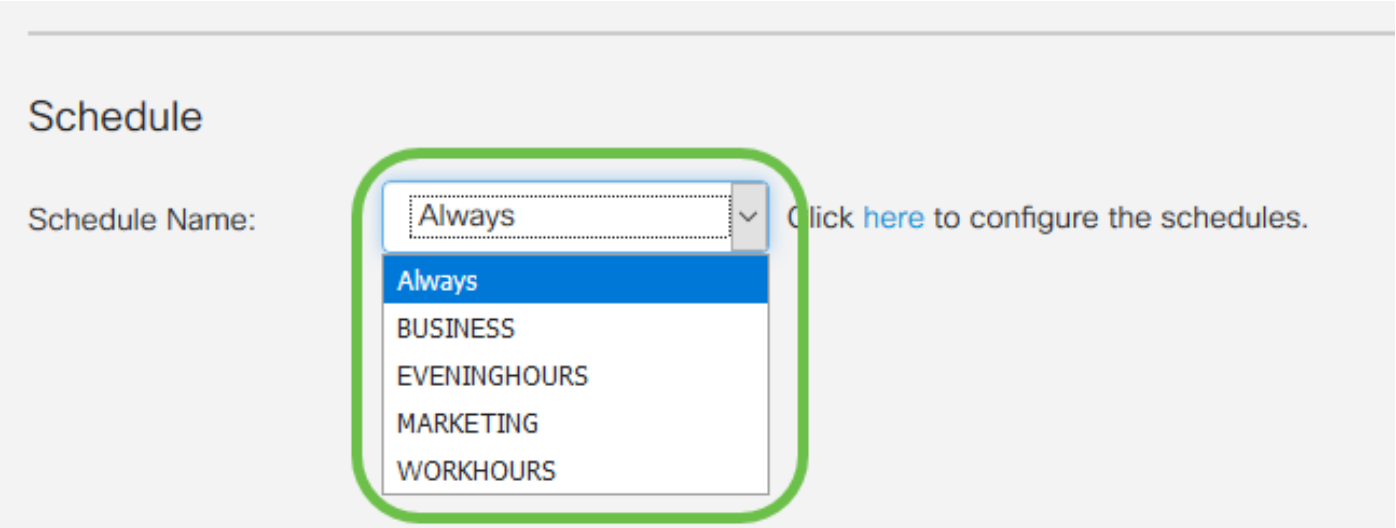

Étape 10. Choisissez parmi la liste déroulante d'*adresse de destination le* type d'adresse sortante que la règle d'accès s'appliquera à. Les options sont comme suit :

- Quels - La règle s'appliquera à toutes les adresses IP sortantes
- Simple - La règle s'appliquera à une adresse IP définie simple
- Sous-réseau - La règle s'appliquera à un sous-réseau défini d'un réseau
- Plage IP - La règle s'appliquera à une plage définie des adresses IP

**Remarque:** Si vous sélectionnez simple, le sous-réseau, ou la plage IP, des champs correspondants apparaîtra à la droite du menu déroulant où vous pouvez écrire des détails d'adresse. Dans cet exemple un sous-réseau est écrit pour expliquer.




Étape 11. De la liste déroulante de *nom de programme*, sélectionnez le calendrier où vous comme la règle d'accès de s'appliquer à.



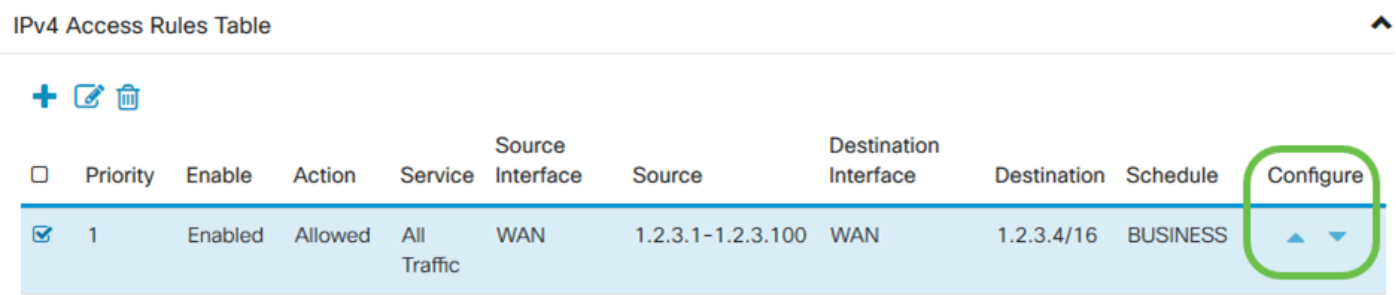

**Remarque:** Pour la Sécurité accrue, il est dans une pratique recommandée de limiter l'accès au réseau non critique aux heures de travail pour s'assurer que des connexions non désirées sont refusées quand votre entreprise n'est pas en fonction.

**Remarque:** Cliquez sur le lien à la droite du déroulant de *nom de programme* si vous voudriez configurer les temps de programme pour des règles d'accès. Plus d'informations peuvent être trouvées sur la façon dont configurer ces programmes ici.

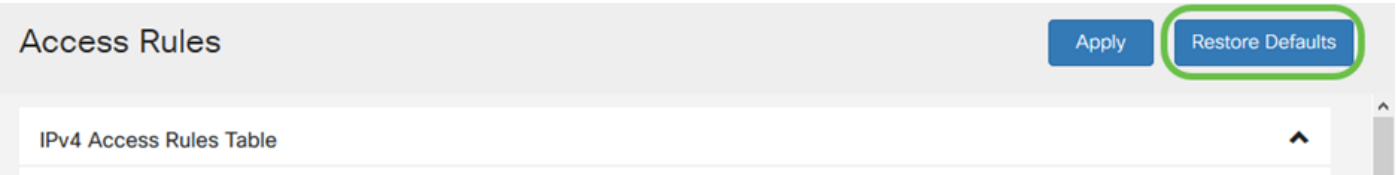
Étape 12. Quand vous êtes satisfait avec la configuration de règle d'accès, cliquez sur Apply pour confirmer.


Vous serez maintenant retourné à la page principale de *règles d'accès*.

**Remarque:** Quand une nouvelle règle d'accès est créée, sa priorité est placée au bas de la liste. Ceci signifie que si une règle d'accès est en conflit avec des autres sur un paramètre spécifique, les restrictions de la règle plus prioritaire auront la priorité. Pour déplacer une règle en haut ou en bas dans la priorité, vous pouvez utiliser les flèches bleues situées dans la colonne de configurer.

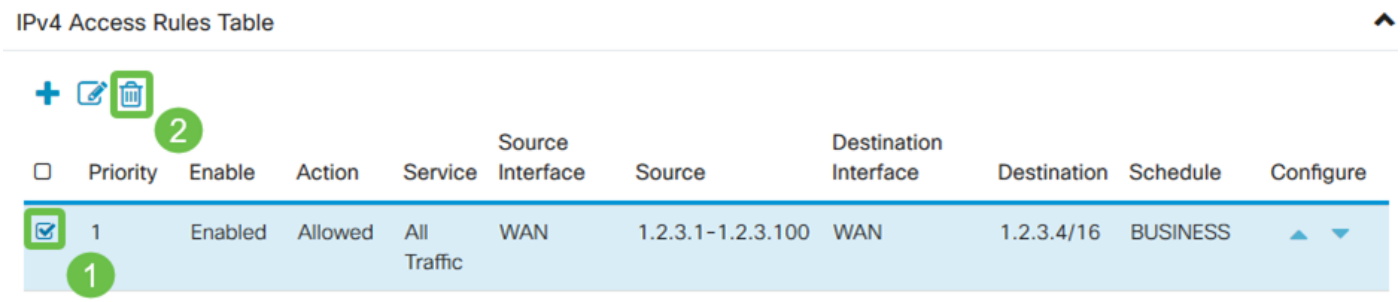



Étape 13 (facultative). Si vous voudriez retourner les règles d'accès les répertorient pour se transférer, cliquer sur des **par défaut de restauration** dans l'angle supérieur droit de la page.



### Retirez une règle d'accès

Étape 14. Pour retirer une règle d'accès de la liste, sélectionnez simplement la case à cocher pour la règle correspondante que vous voudriez retirer. Sélectionnez alors l'icône bleue de poubelle en haut de la liste. De plusieurs entrées de règle d'accès peuvent être retirées immédiatement.




### Gestion des services

La gestion des services te permet pour ajouter ou éditer des services de réseau existant par leur numéro de port, protocole, et d'autres détails. Ces le servicescwill de réseau soit disponible dans le déroulant de services en configurant les règles d'accès. Par le menu de configuration de la liste de gestion des services, vous pouvez créer le service des douanes qui peut alors être appliqué aux règles d'accès pour le contrôle plus précis au-dessus du trafic entrant votre réseau. Pour se renseigner plus sur la façon configurer la gestion des services, a cliquez ici.

## Conclusion

Les règles d'accès si convenablement appliquées sont un outil utile pour sécuriser votre connexion WAN. Avec le guide ci-dessus et les pratiques discutées, vous devriez avoir tout que vous devez configurer correctement des règles d'accès sécurisé pour votre routeur RV160x ou RV260x.