# Configuration des règles d'accès sur les routeurs des gammes RV160 et RV260

## Objectif

Votre routeur est responsable de la réception des données du réseau externe et constitue la première ligne de défense en matière de sécurité de votre réseau local. En activant les règles d'accès sur votre routeur, vous pouvez filtrer les paquets en fonction de paramètres spécifiques tels que l'adresse IP ou le numéro de port. Avec les étapes ci-dessous, ce document vise à vous guider sur la façon de configurer les règles d'accès pour mieux contrôler les paquets qui entrent dans votre réseau. Ce document met également en évidence certaines meilleures pratiques d'utilisation des règles d'accès pour optimiser leur potentiel de sécurité.

## Périphériques pertinents

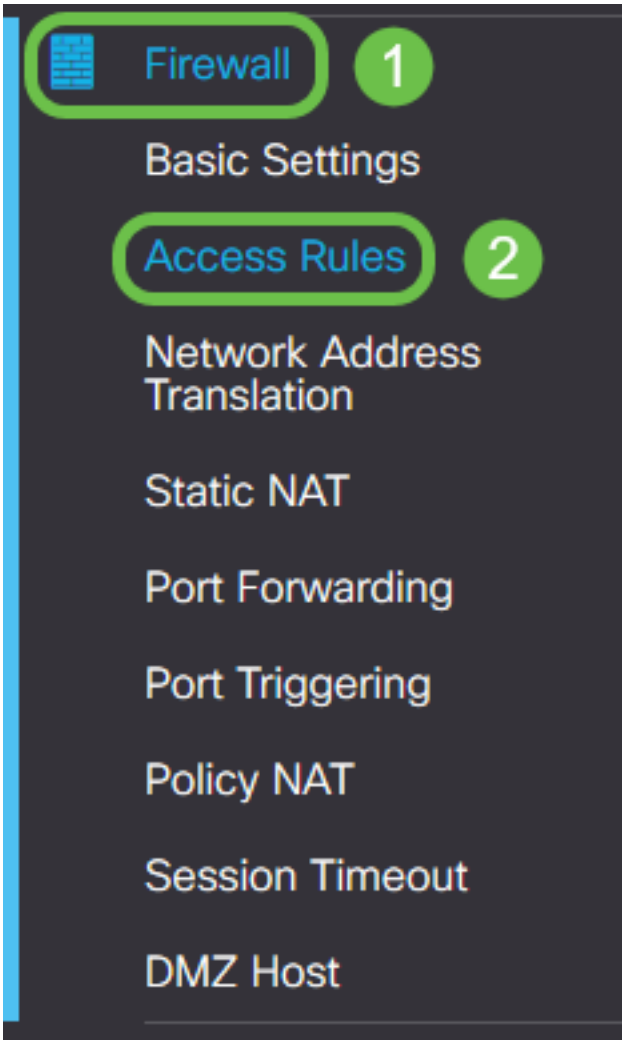
- RV160x
- RV260x

## Version du logiciel

- 1.0.00.13

## Configurer les règles d'accès

Étape 1. Dans le volet de navigation situé à gauche de l'utilitaire de configuration, sélectionnez **Firewall > Access Rules.**

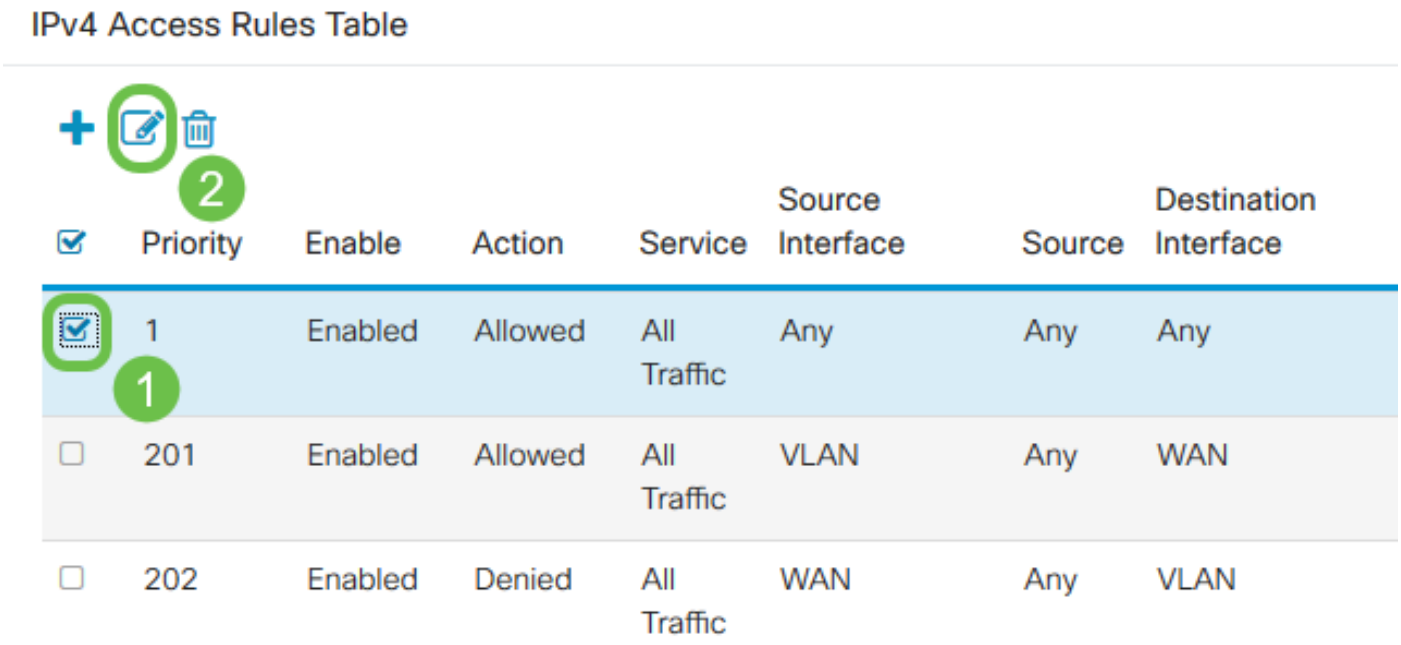



La page Access Rules s'affiche. Sur cette page, il existe des tableaux contenant des listes de règles d'accès et leurs attributs pour IPv4 et IPv6 respectivement. À partir de là, vous pouvez ajouter une nouvelle règle d'accès, modifier une règle existante ou supprimer une règle existante.

## Ajouter/modifier une règle d'accès

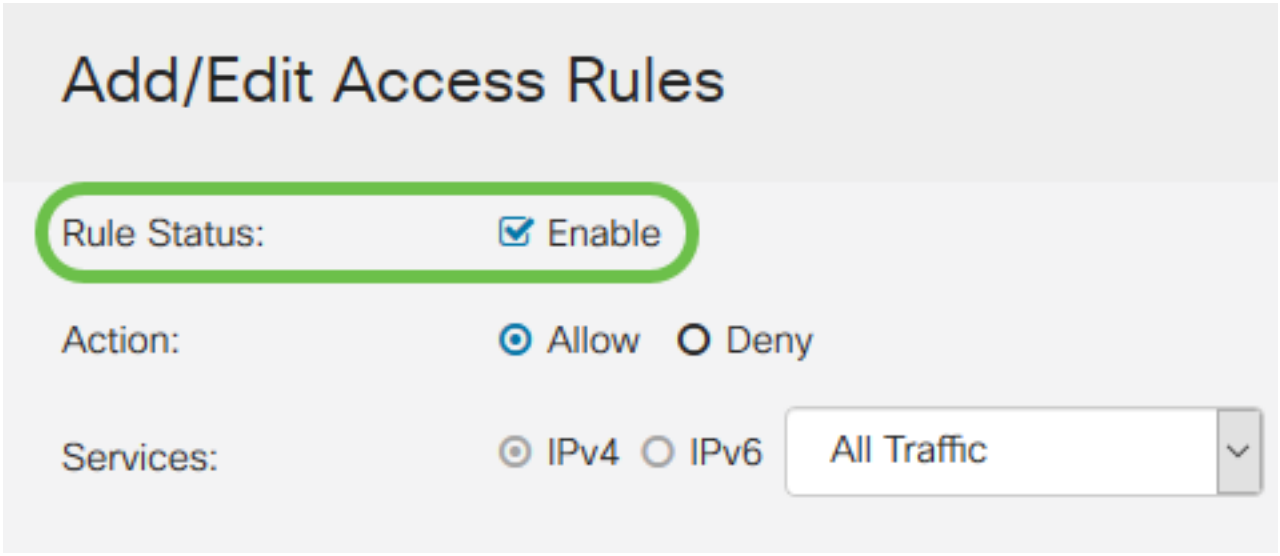
Étape 2. Pour ajouter une nouvelle règle d'accès, cliquez sur l'icône bleue à ajouter dans le tableau Règles d'accès IPv4 ou Règles d'accès IPv6 en fonction du protocole auquel vous souhaitez appliquer la règle. Dans ce cas, IPv4 est utilisé.


Pour modifier une entrée existante, cochez la case en regard de la règle d'accès que vous souhaitez modifier. Sélectionnez ensuite l'icône de modification bleue en haut du tableau correspondant. Une seule règle peut être sélectionnée à la fois pour modification.

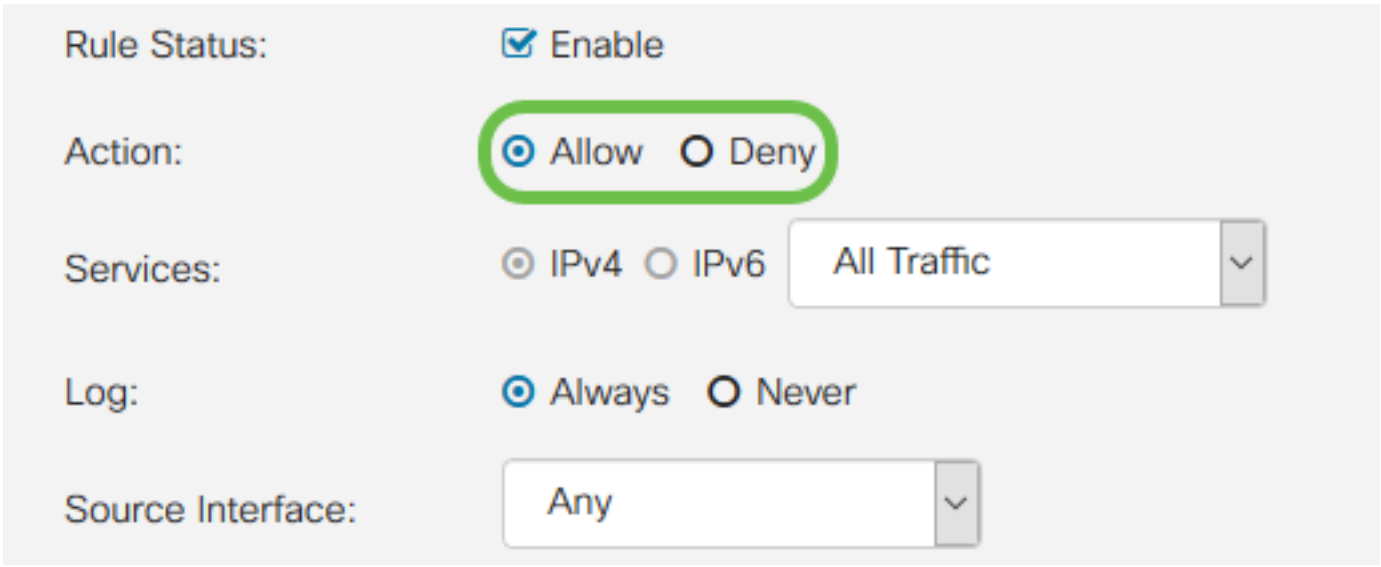



La page *Ajouter/modifier des règles d'accès* apparaît.

Étape 3. Cochez/décochez la case État de la règle pour activer ou désactiver la règle d'accès pendant le fonctionnement. Cela est utile lorsque vous avez une règle d'accès que vous souhaitez enregistrer pour appliquer ultérieurement.

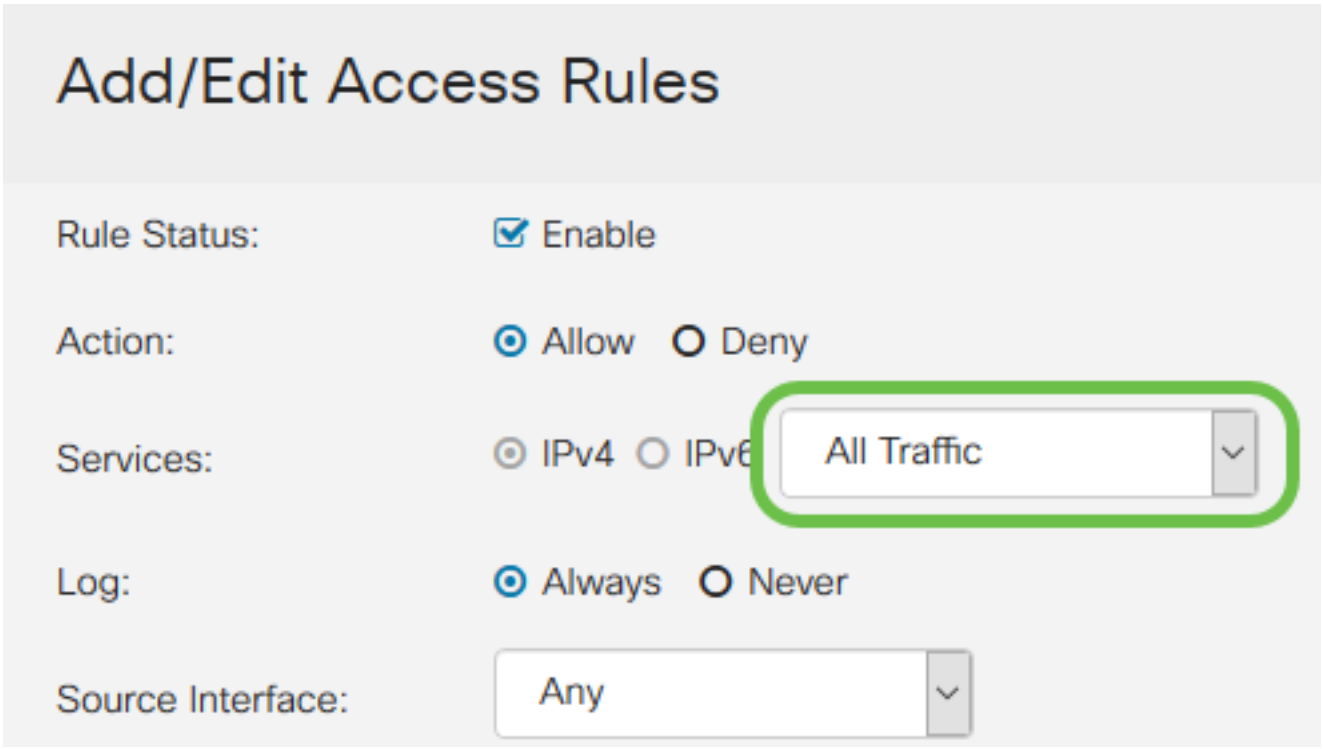



Étape 4. Dans le champ *Action*, sélectionnez si la règle doit autoriser ou refuser l'accès au trafic réseau entrant à spécifier.



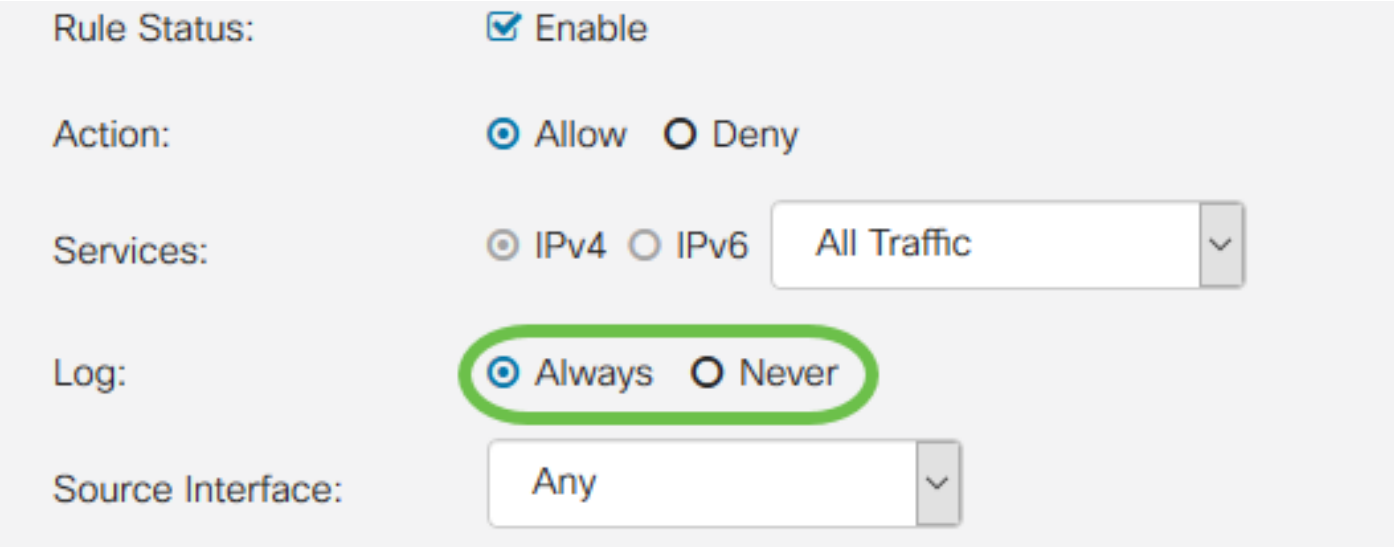

**Note:** Il est recommandé pour la meilleure sécurité de définir des règles d'accès qui autorisent uniquement le trafic que vous prévoyez recevoir, plutôt que d'essayer de refuser uniquement le trafic indésirable. Votre réseau sera ainsi mieux protégé contre les menaces inconnues.

Étape 5. Dans le champ *Services*, sélectionnez dans le menu déroulant le type de service réseau auquel vous souhaitez appliquer la règle d'accès.

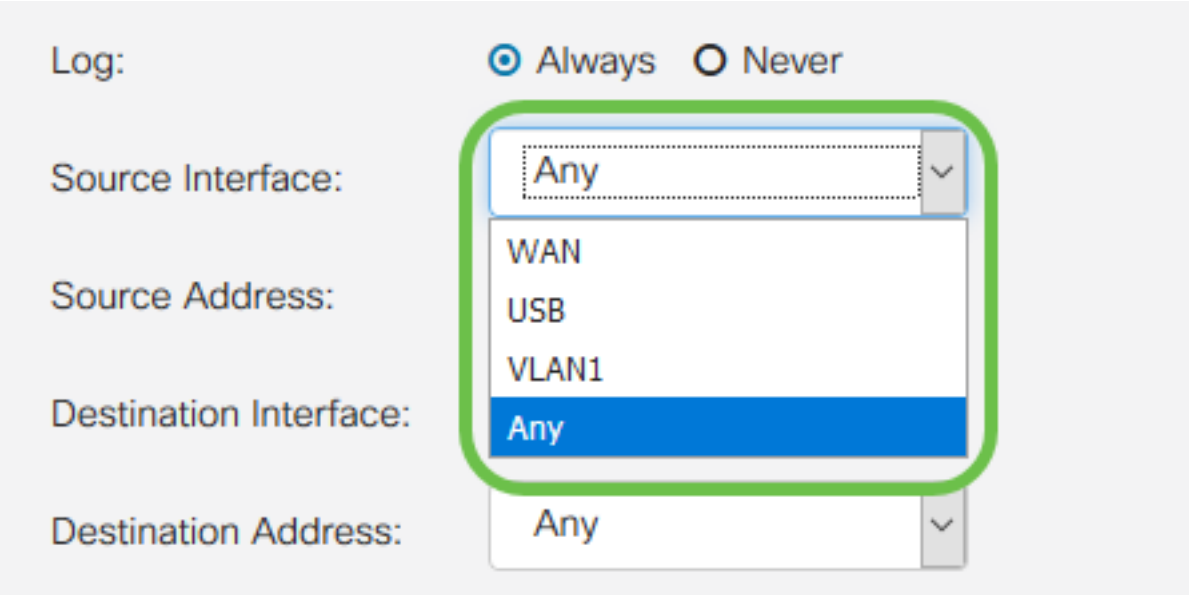



**Note:** La case d'option IPv4 ou IPv6 est automatiquement sélectionnée en fonction du tableau auquel vous avez choisi d'appliquer la règle d'accès à partir de la page *Règles d'accès*.

Étape 6. Sélectionnez dans le champ *Journal* si vous souhaitez que le routeur génère un message de journal une fois que les paquets qui entrent dans votre réseau correspondent aux règles appliquées.



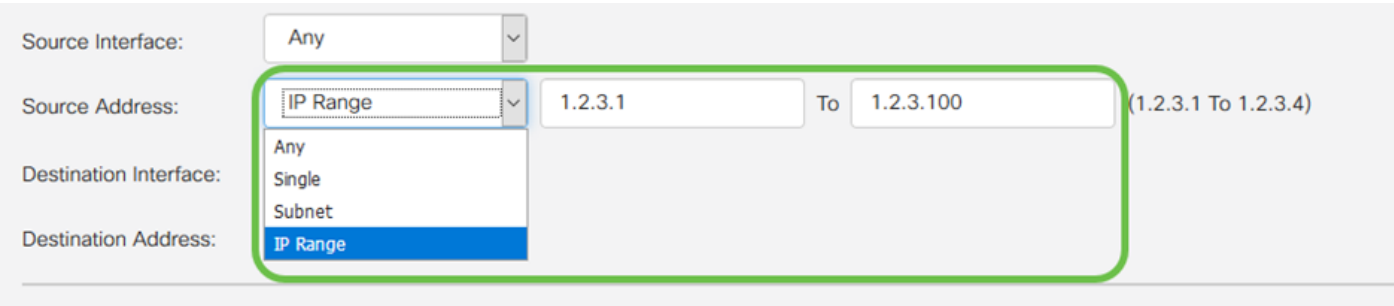

Étape 7. Dans la liste déroulante *Interface source*, sélectionnez l'interface réseau pour les paquets entrants auxquels la règle d'accès s'appliquera.




Étape 8. Sélectionnez dans la liste déroulante *Adresse source* le type d'adresse entrante auquel la règle d'accès s'appliquera. Les options sont les suivantes :

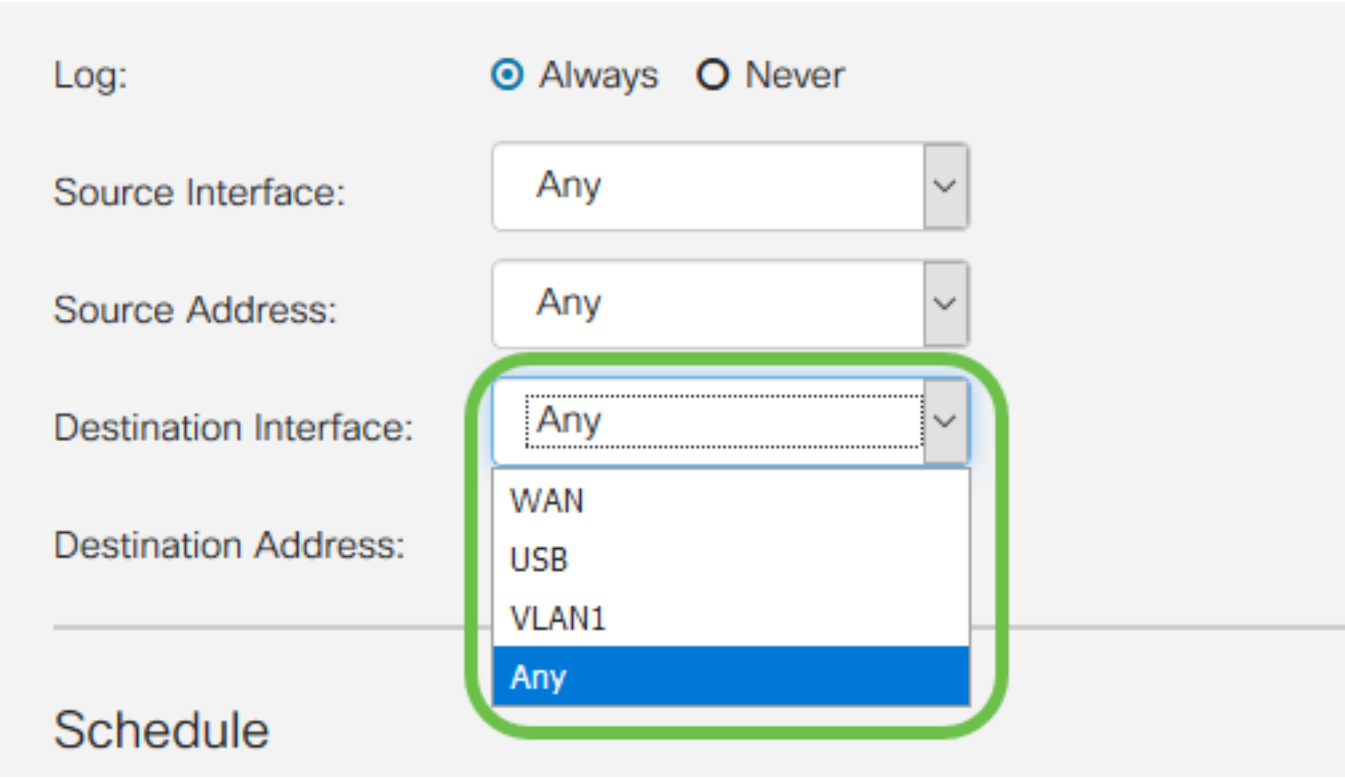
- Any : la règle s'applique à toutes les adresses IP entrantes.
- Single : la règle s'applique à une adresse IP définie unique.
- Sous-réseau : la règle s'applique à un sous-réseau défini d'un réseau.
- Plage d'adresses IP : la règle s'applique à une plage d'adresses IP définie.

**Note:** Si vous sélectionnez Single, Subnet ou IP Range, les champs correspondants s'affichent à droite du menu déroulant, où vous pouvez saisir les détails de l'adresse. Dans cet exemple, une plage IP est entrée pour illustrer.




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

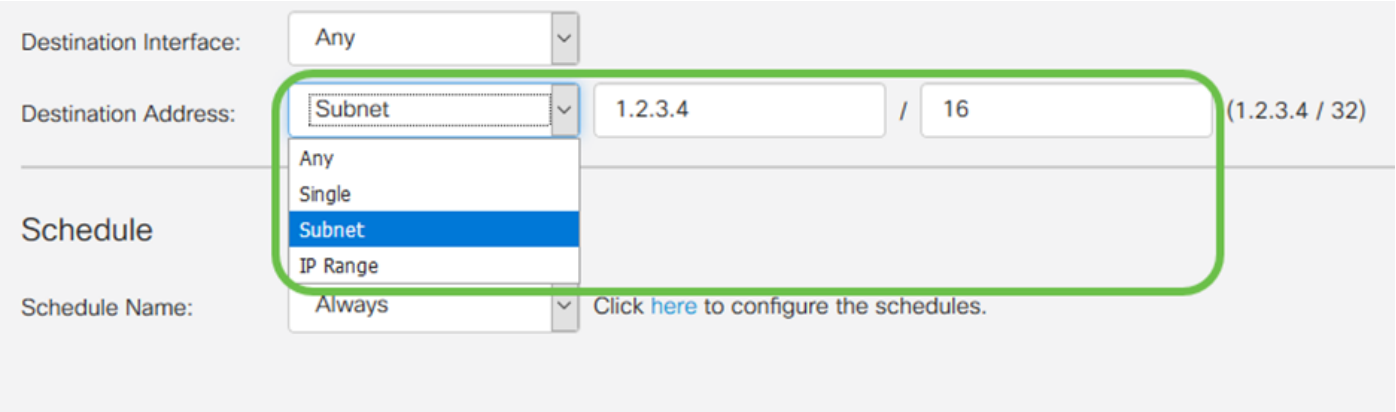
paquets sortants auxquels la règle d'accès s'appliquera.



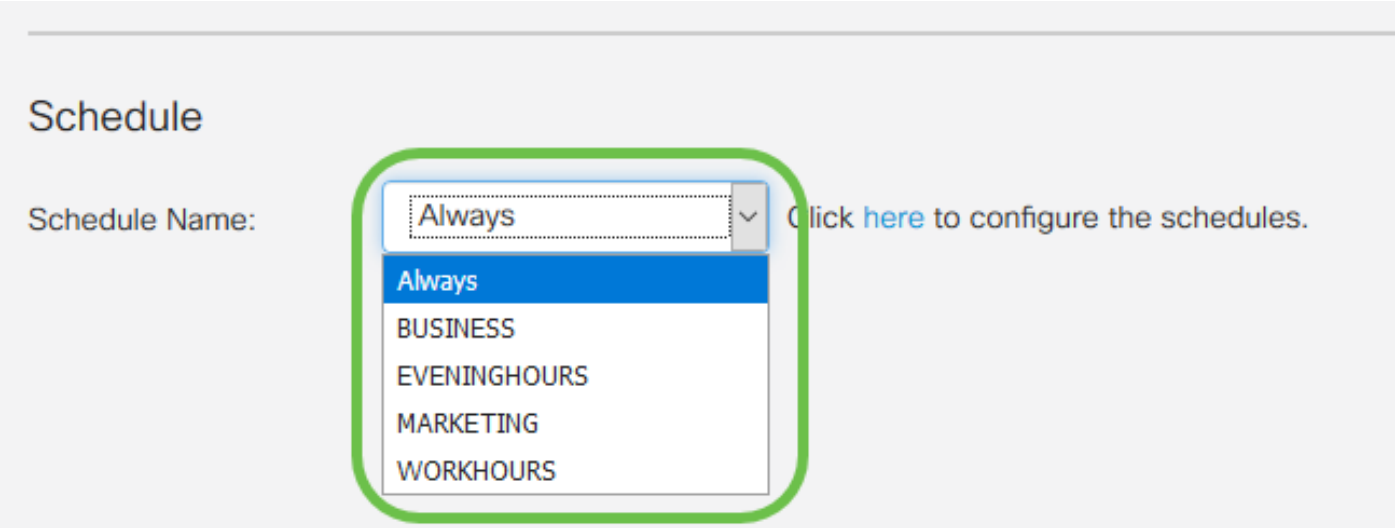

Étape 10. Sélectionnez dans la liste déroulante *Adresse de destination* le type d'adresse sortante auquel la règle d'accès s'appliquera. Les options sont les suivantes :

- Any : la règle s'applique à toutes les adresses IP sortantes.
- Single : la règle s'applique à une adresse IP définie unique.
- Sous-réseau : la règle s'applique à un sous-réseau défini d'un réseau.
- Plage d'adresses IP : la règle s'applique à une plage d'adresses IP définie.

**Note:** Si vous sélectionnez Single, Subnet ou IP Range, les champs correspondants s'affichent à droite du menu déroulant, où vous pouvez saisir les détails de l'adresse. Dans cet exemple, un sous-réseau est entré pour illustrer.




Étape 11. Dans la liste déroulante *Nom du programme*, sélectionnez le calendrier auquel vous souhaitez appliquer la règle d'accès.



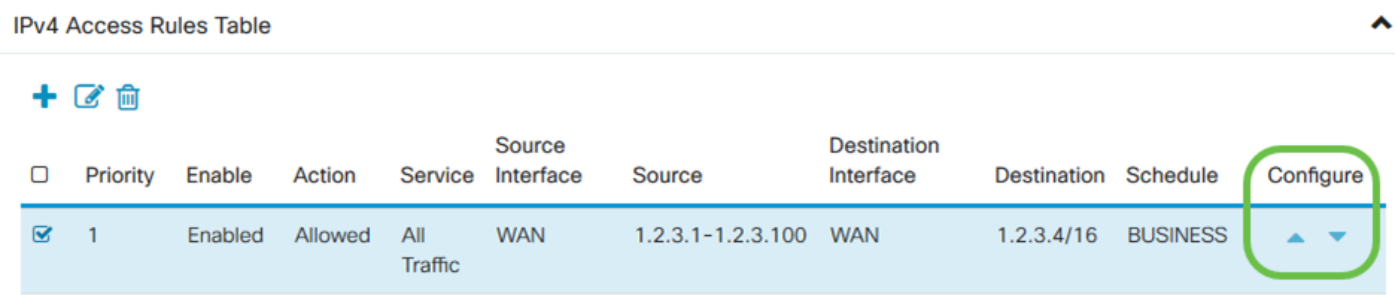

**Note:** Pour améliorer la sécurité, il est recommandé de limiter l'accès réseau non essentiel aux heures d'ouverture afin de s'assurer que les connexions indésirables sont refusées lorsque votre entreprise n'est pas en service.

**Note:** Cliquez sur le lien situé à droite de la liste déroulante *Nom de la planification* si vous souhaitez configurer les heures de planification pour les règles d'accès. Vous trouverez plus d'informations sur la façon de configurer ces planifications ici.

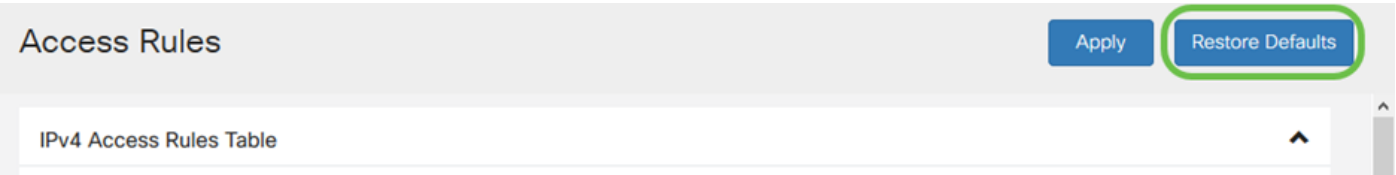
Étape 12. Lorsque vous êtes satisfait de la configuration de la règle d'accès, cliquez sur **Appliquer** pour confirmer.


Vous revenez maintenant à la page principale *Règles d'accès*.

**Note:** Lorsqu'une nouvelle règle d'accès est créée, sa priorité est placée en bas de la liste. Cela signifie que si une règle d'accès est en conflit avec une autre sur un paramètre spécifique, les restrictions de la règle de priorité supérieure auront priorité. Pour déplacer une règle vers le haut ou le bas en priorité, vous pouvez utiliser les flèches bleues situées dans la colonne Configurer.

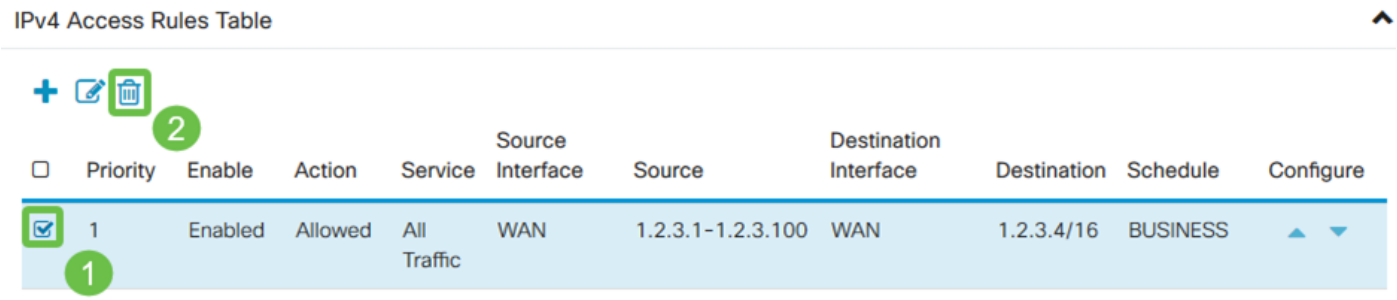



Étape 13 (Facultatif). Si vous souhaitez rétablir la liste des règles d'accès par défaut, cliquez sur **Restaurer les valeurs par défaut** dans le coin supérieur droit de la page.



### Supprimer une règle d'accès

Étape 14. Pour supprimer une règle d'accès de la liste, cochez simplement la case correspondant à la règle correspondante que vous souhaitez supprimer. Sélectionnez ensuite l'icône représentant une poubelle bleue en haut de la liste. Plusieurs entrées de règle d'accès peuvent être supprimées simultanément.




### Gestion des services

La gestion des services vous permet d'ajouter ou de modifier des services réseau existants en fonction de leur numéro de port, de leur protocole et d'autres détails. Ces services réseau seront disponibles dans la liste déroulante Services lors de la configuration des règles d'accès. Dans le menu de configuration de la liste de gestion des services, vous pouvez créer des services personnalisés qui peuvent ensuite être appliqués aux règles d'accès pour un contrôle plus précis du trafic entrant sur votre réseau. Pour en savoir plus sur la configuration de la gestion des services, cliquez ici.

## Conclusion

Les règles d'accès, lorsqu'elles sont appliquées de manière appropriée, constituent un outil précieux pour sécuriser votre connexion WAN. Avec le guide ci-dessus et les pratiques décrites ci-dessus, vous devez disposer de tout ce dont vous avez besoin pour configurer correctement les règles d'accès sécurisé pour votre routeur RV160x ou RV260x.