Configuration des règles d'accès sur un routeur de la gamme RV34x

Objectif

Le routeur VPN double WAN RV340 est un périphérique hautes performances, flexible et facile à utiliser, adapté aux petites entreprises. Avec des fonctions de sécurité supplémentaires, telles que le filtrage Web, le contrôle des applications et la protection de la source IP. Le nouveau routeur RV340 offre une connectivité filaire haut débit hautement sécurisée aux petits bureaux et aux employés distants. Ces nouvelles fonctions de sécurité facilitent également le réglage précis de l'activité autorisée sur le réseau.

Les règles d'accès ou les stratégies sur le routeur de la gamme RV34x permettent de configurer les règles pour accroître la sécurité du réseau. Une combinaison de règles et vous avez une liste de contrôle d'accès (ACL). Les listes de contrôle d'accès sont des listes qui bloquent ou autorisent l'envoi du trafic à destination et en provenance de certains utilisateurs. Les règles d'accès peuvent être configurées pour être en vigueur à tout moment ou en fonction de calendriers définis.

Les listes de contrôle d'accès ont un refus implicite à la fin de la liste. Par conséquent, à moins que vous ne l'autorisiez explicitement, le trafic ne peut pas passer. Par exemple, si vous voulez autoriser tous les utilisateurs à accéder à un réseau via le routeur, à l'exception des adresses particulières, vous devez refuser ces adresses et autoriser toutes les autres.

L'objectif de cet article est de vous montrer comment configurer les règles d'accès sur un routeur de la gamme RV34x.

Périphériques pertinents

- Gamme RV34x

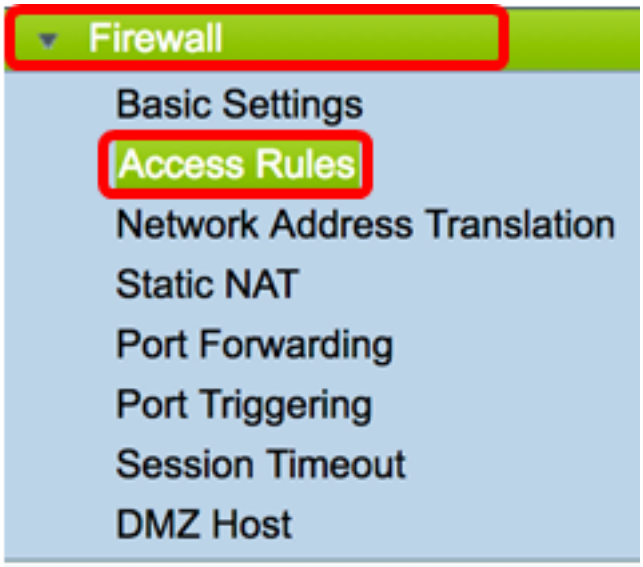
Version du logiciel

- 1.0.1.16
  - Un micrologiciel mettant à jour l'interface utilisateur est disponible depuis la publication de cet article, cliquez ici pour accéder à la page de téléchargement, localisez votre produit spécifique là.

Configurer une règle d'accès sur un routeur de la gamme RV34x

Créer une règle d'accès

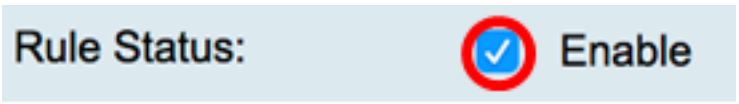
Étape 1. Connectez-vous à l'utilitaire Web du routeur et choisissez **Firewall > Access Rules**.



Étape 2. Dans le tableau Règles d'accès IPv4 ou IPv6, cliquez sur **Ajouter** pour créer une nouvelle règle.

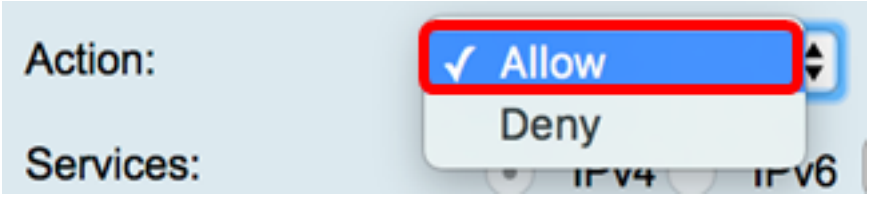
Note: Sur le routeur de la gamme RV34x, il est possible de configurer jusqu'à 202 règles. Dans cet exemple, IPv4 est utilisé.

Étape 3. Cochez la case **Activer l'état de la règle** pour activer la règle.



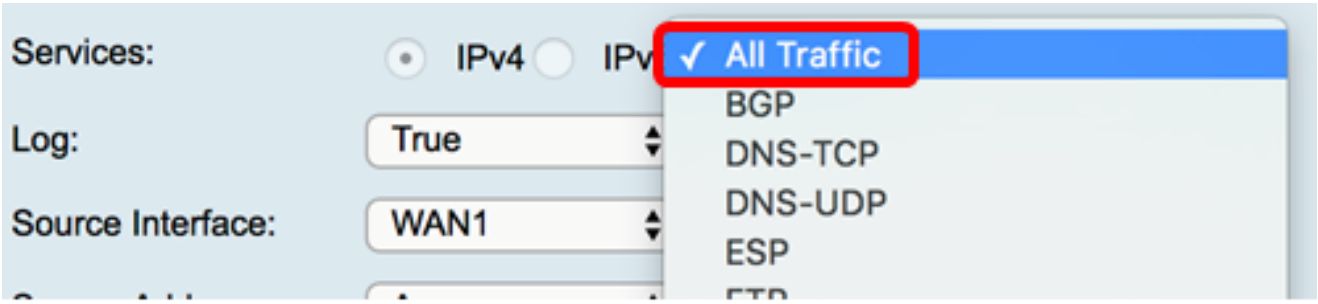
Étape 4. Dans le menu déroulant Action, choisissez si la stratégie autorise ou refuse les données.

Note: Dans cet exemple, Allow est sélectionné.



Étape 5. Dans le menu déroulant Services, sélectionnez le type de trafic que le routeur autorise ou refuse.

Note: Dans cet exemple, tout le trafic est sélectionné. Tout le trafic sera autorisé.



Étape 6. Dans le menu déroulant Log (Journal), sélectionnez une option pour déterminer si le routeur enregistre le trafic autorisé ou refusé. Les options sont les suivantes :

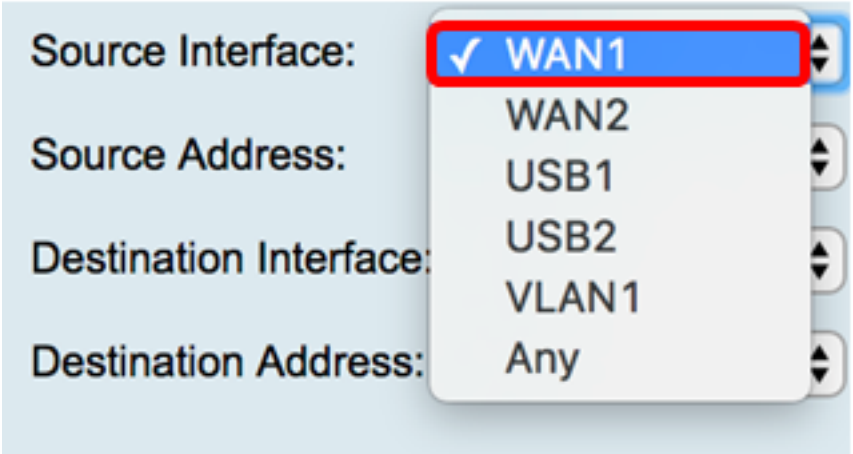
- Jamais : le routeur ne consigne jamais le trafic autorisé et refusé.
- True : le routeur enregistre le trafic correspondant à la stratégie.

Note: Dans cet exemple, Jamais est sélectionné.

Étape 7. Dans le menu déroulant Interface source, sélectionnez une interface pour le trafic entrant ou entrant où la stratégie d'accès doit être appliquée. Les options sont les suivantes

- WAN1 : la stratégie s'applique uniquement au trafic provenant du WAN1.
- WAN2 : la stratégie s'applique uniquement au trafic provenant du WAN2.
- USB1 : la stratégie s'applique uniquement au trafic provenant d'USB1.
- USB2 — La stratégie s'applique uniquement au trafic provenant d'USB2.
- VLAN1 : la stratégie s'applique uniquement au trafic VLAN1.
- Any : la stratégie s'applique à n'importe quelle interface.

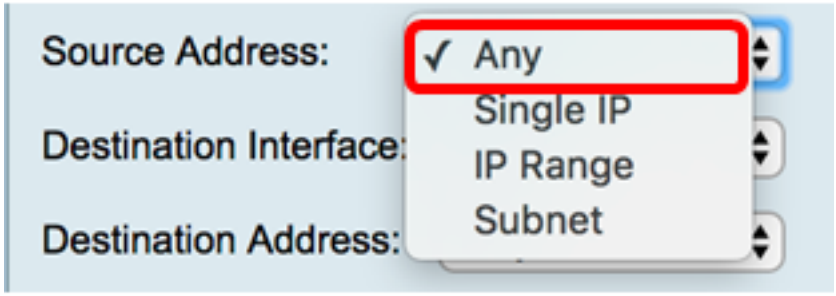
Note: Si un réseau local virtuel (VLAN) supplémentaire a été configuré, l'option VLAN apparaît dans la liste. Dans cet exemple, WAN1 est choisi.



Étape 8. Dans le menu déroulant Adresse source, sélectionnez une source pour appliquer la stratégie. Les options sont les suivantes :

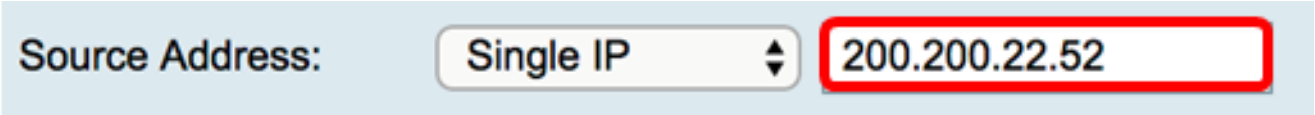
- Any : la stratégie s'applique à toute adresse IP du réseau. Si cette option est sélectionnée, passez à l'étape 12.
- Single IP : la stratégie s'applique à un seul hôte ou adresse IP. Si cette option est sélectionnée, passez à l'étape 9.
- IP Range : la stratégie s'applique à un ensemble ou une plage d'adresses IP. Si cette option est sélectionnée, passez à l'étape 10.
- Sous-réseau : la stratégie s'applique à un sous-réseau entier. Si cette option est sélectionnée, passez à l'étape 11.

Note: Dans cet exemple, Any est sélectionné.



Étape 9. (Facultatif) Une adresse IP unique a été choisie à l'étape 8, saisissez une adresse IP unique pour la stratégie à appliquer, puis passez à l'étape 12.

Note: Pour cet exemple, 200.200.22.52 est utilisé.



Étape 10. (Facultatif) Si la plage IP a été choisie à l'étape 8, saisissez les adresses IP de début et de fin dans les champs d'adresse IP respectifs.

Note: Dans cet exemple, 200.200.22.22 est utilisé comme adresse IP de début et 200.200.22.34 comme adresse IP de fin.

Étape 11. (Facultatif) Si le sous-réseau a été choisi à l'étape 8, saisissez l'ID réseau et son masque de sous-réseau respectif pour appliquer la stratégie.

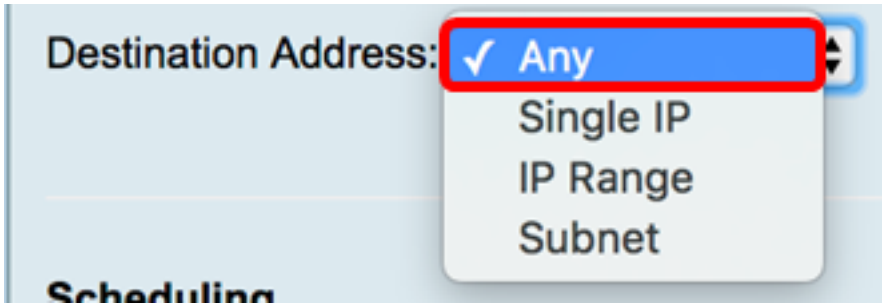
Note: Dans cet exemple, 200.200.22.1 est utilisé comme ID de sous-réseau et 24 comme masque de sous-réseau.

Étape 12. Dans le menu déroulant Interface de destination, sélectionnez une interface pour le trafic sortant ou sortant où la stratégie d'accès doit être appliquée. Les options disponibles sont WAN1, WAN2, USB1, USB2, VLAN1 et Any.

Note: Dans cet exemple, WAN1 est choisi.

Étape 13. Dans le menu déroulant Adresse de destination, sélectionnez une destination pour appliquer la stratégie. Les options sont Any, Single IP, IP Range, Subnet.

Note: Dans cet exemple, Any est sélectionné. Passez à l'étape 17.



Étape 14. (Facultatif) Si une adresse IP unique a été choisie à l'étape 13, saisissez une adresse IP unique pour la stratégie à appliquer.

Note: Dans cet exemple, 210.200.22.52 est utilisé.

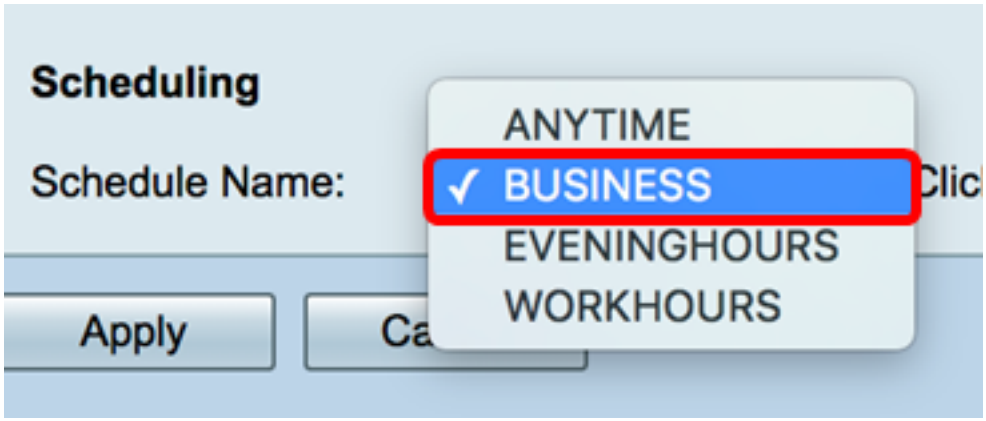
Étape 15. (Facultatif) Si vous avez choisi IP Range à l'étape 13, saisissez les adresses IP de début et de fin dans les champs d'adresse IP respectifs.

Note: Dans cet exemple, 210.200.27.22 est utilisé comme adresse IP de début et 210.200.27.34 comme adresse IP de fin. Passez à l'étape 17.

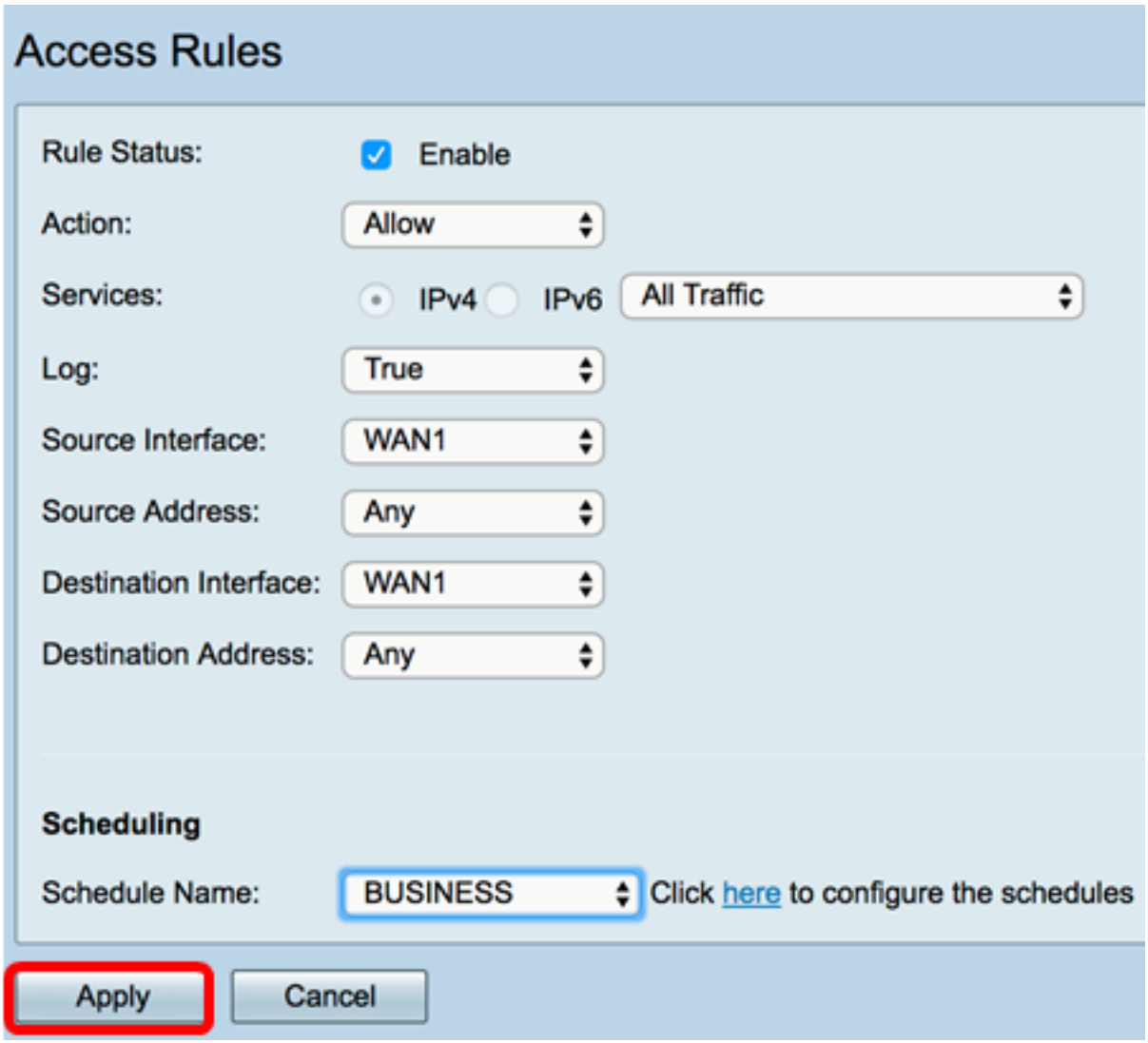
Étape 16. (Facultatif) Si Subnet a été sélectionné à l'étape 13, saisissez l'adresse réseau et son masque de sous-réseau respectif pour appliquer la stratégie.

Note: Dans cet exemple, 210.200.27.1 est utilisé comme adresse de sous-réseau et 24 comme masque de sous-réseau.

Étape 17. Dans la liste déroulante Nom du programme, sélectionnez un programme pour appliquer cette stratégie. Pour savoir comment configurer un planning, cliquez ici.



Étape 18. Cliquez sur Apply.

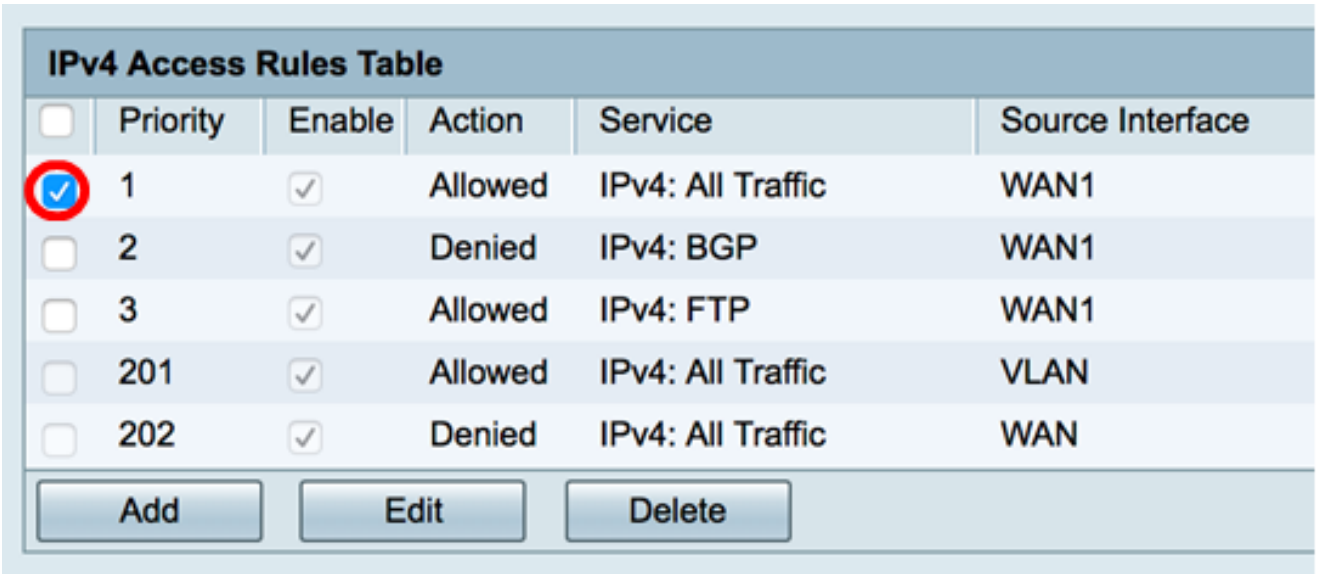


Vous devez maintenant avoir créé une règle d'accès sur un routeur de la gamme RV.

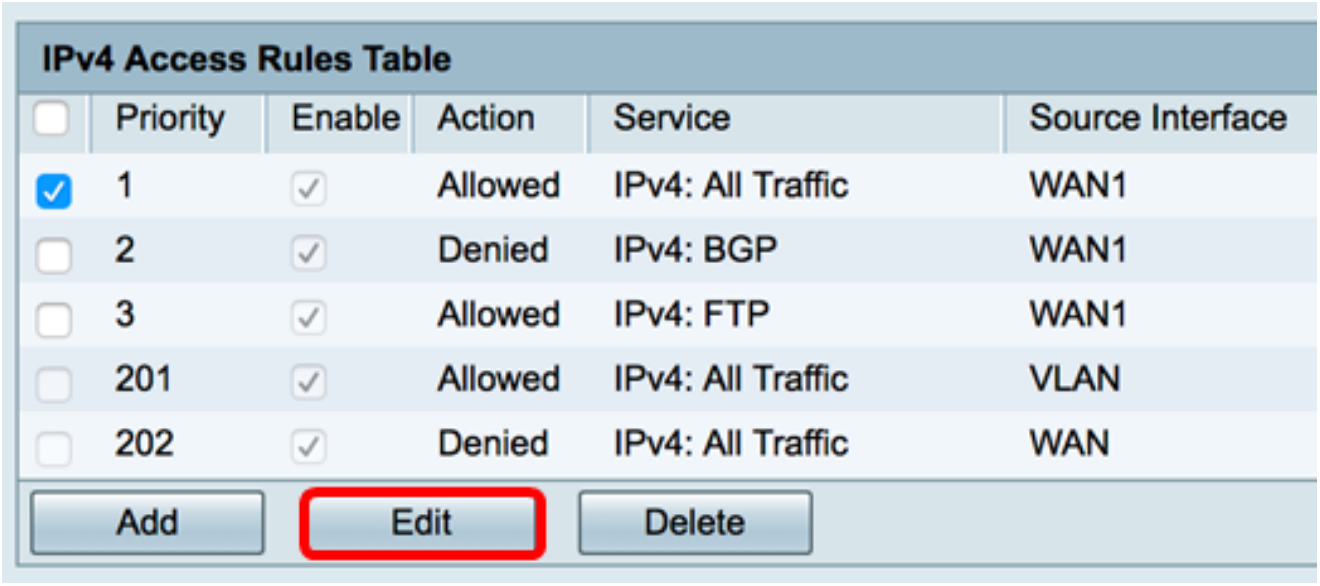
Modifier une règle d'accès

Étape 1. Dans le tableau des règles d'accès IPv4 ou IPv6, cochez la case en regard de la règle d'accès que vous voulez configurer.

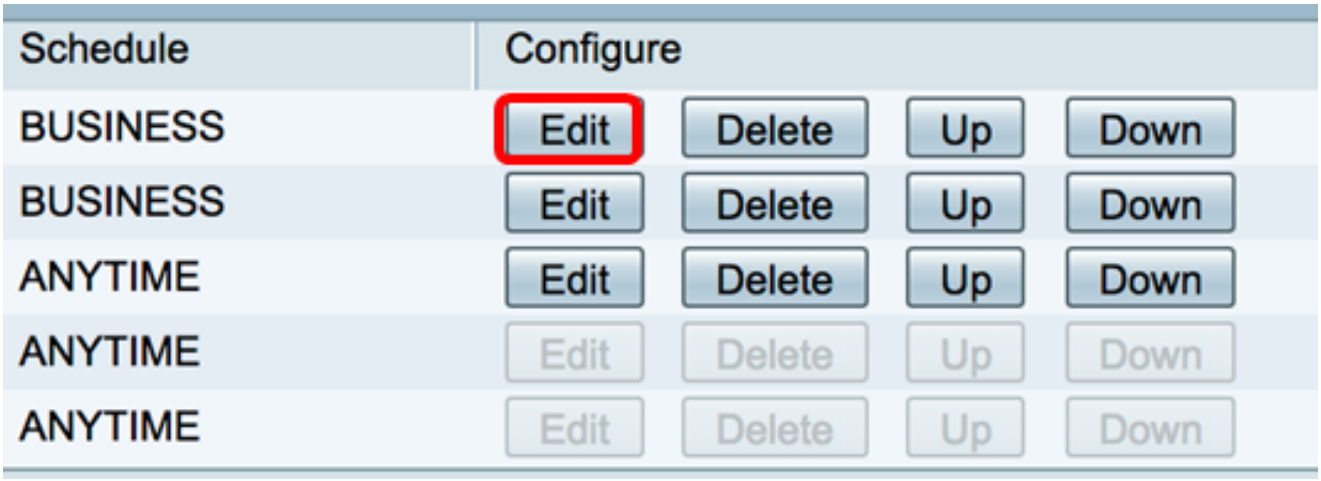
Note: Dans cet exemple, dans le tableau des règles d'accès IPv4, la priorité 1 est choisie.



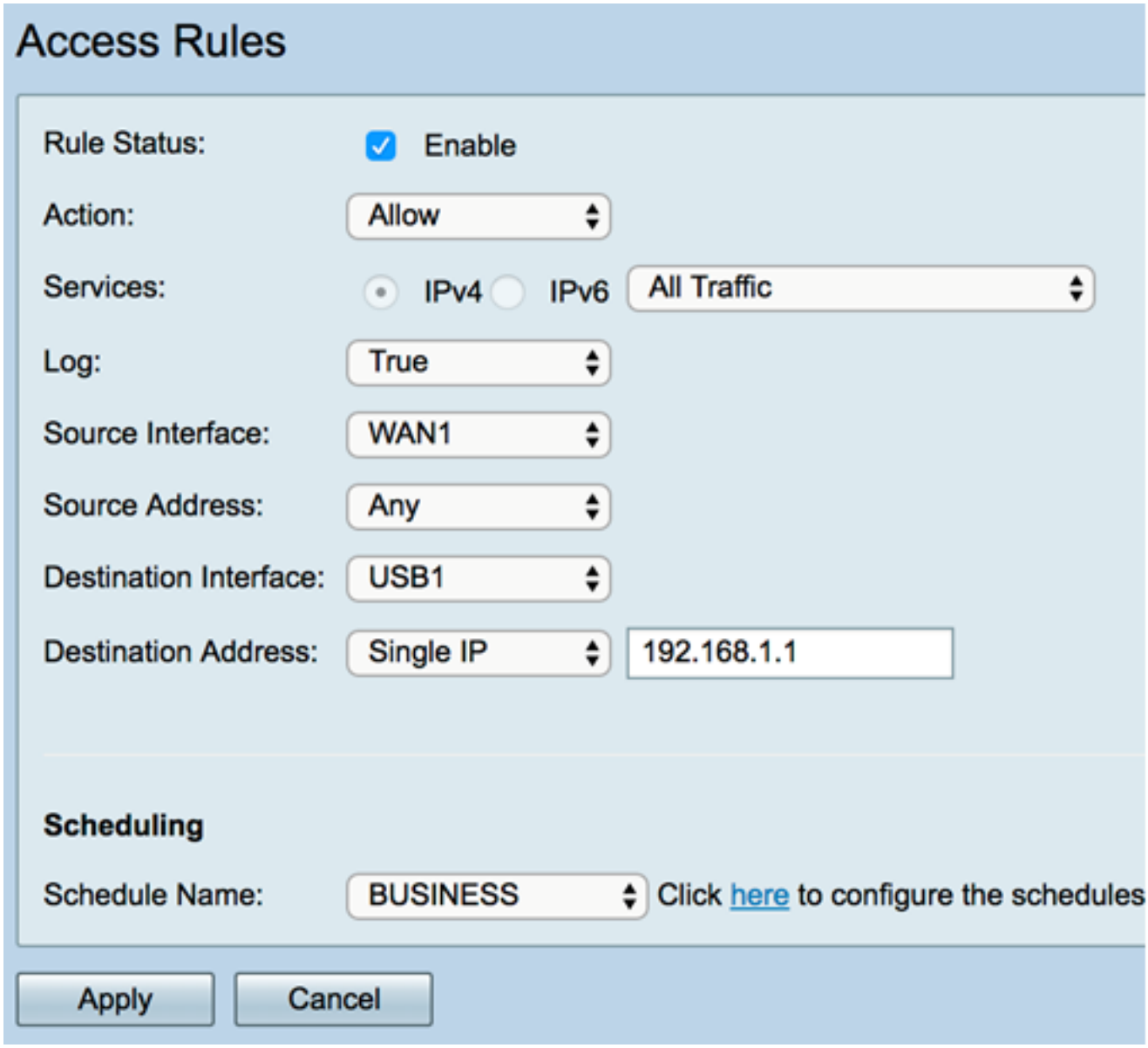
Étape 2. Cliquez sur **Edit**.



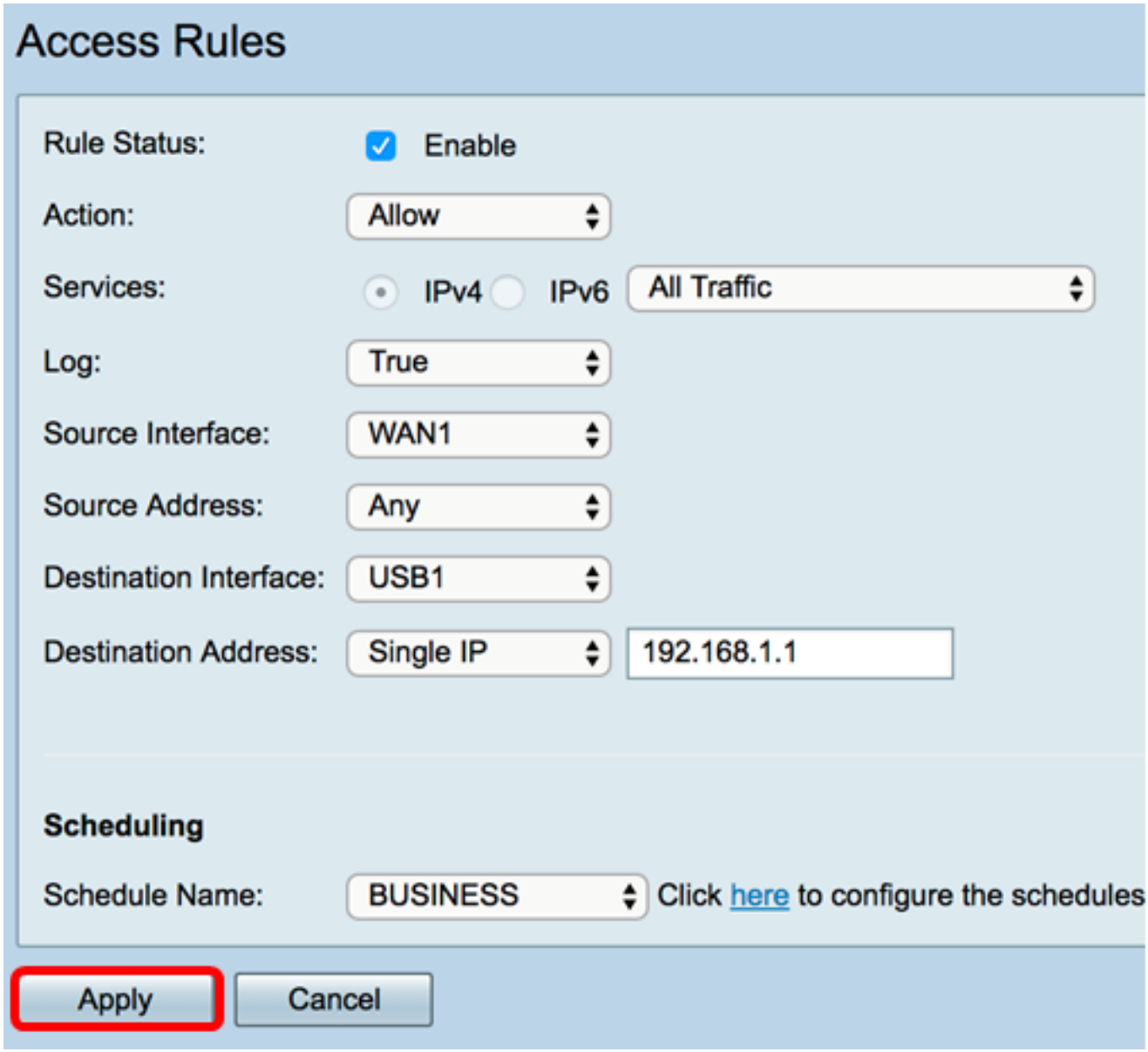
Étape 3. (Facultatif) Dans la colonne Configure, cliquez sur le bouton **Edit** dans la ligne de la règle d'accès souhaitée.



Étape 4. Mettre à jour les paramètres nécessaires.



Étape 5. Cliquez sur Apply.



Étape 6. (Facultatif) Pour modifier la priorité d'une règle d'accès dans la colonne Configurer, cliquez sur le bouton **Haut** ou **Bas** de la règle d'accès à déplacer.

Note: Lorsqu'une règle d'accès est déplacée vers le haut ou vers le bas, elle déplace une étape au-dessus ou au-dessous de son emplacement d'origine. Dans cet exemple, la priorité 1 sera déplacée vers le bas.

Note: Dans cet exemple, la priorité 1 est désormais la priorité 2.

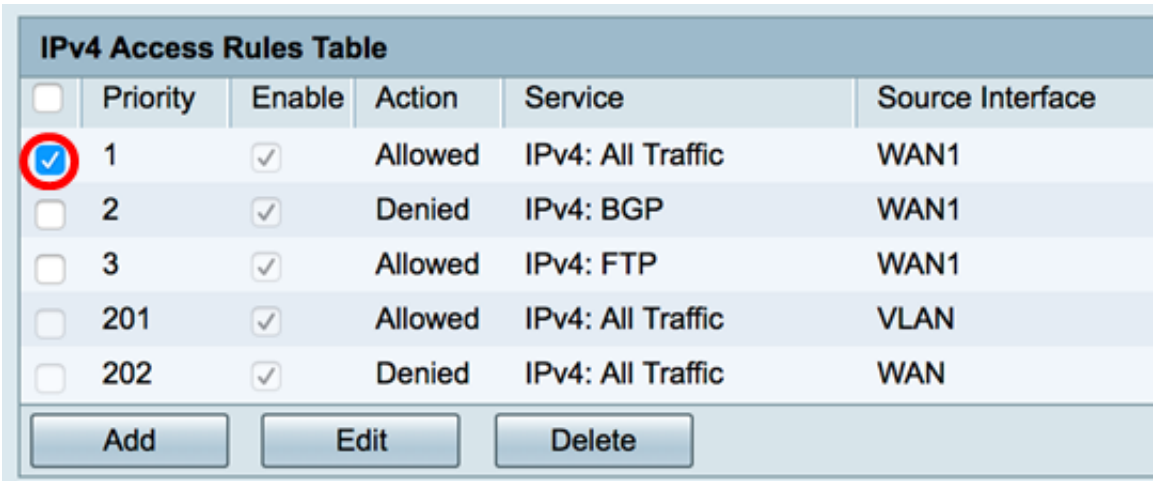
Étape 7. Cliquez sur Apply.

Vous devez maintenant avoir correctement modifié une règle d'accès sur un routeur de la gamme RV34x.

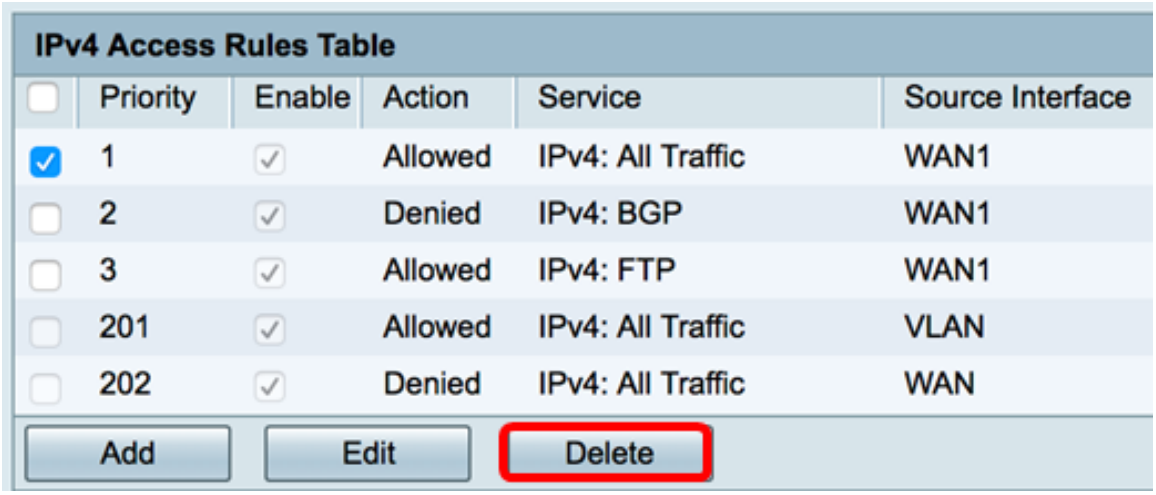
Supprimer une règle d'accès

Étape 1. Dans le tableau Règles d'accès IPv4 ou IPv6, cochez la case en regard de la règle d'accès que vous voulez supprimer.

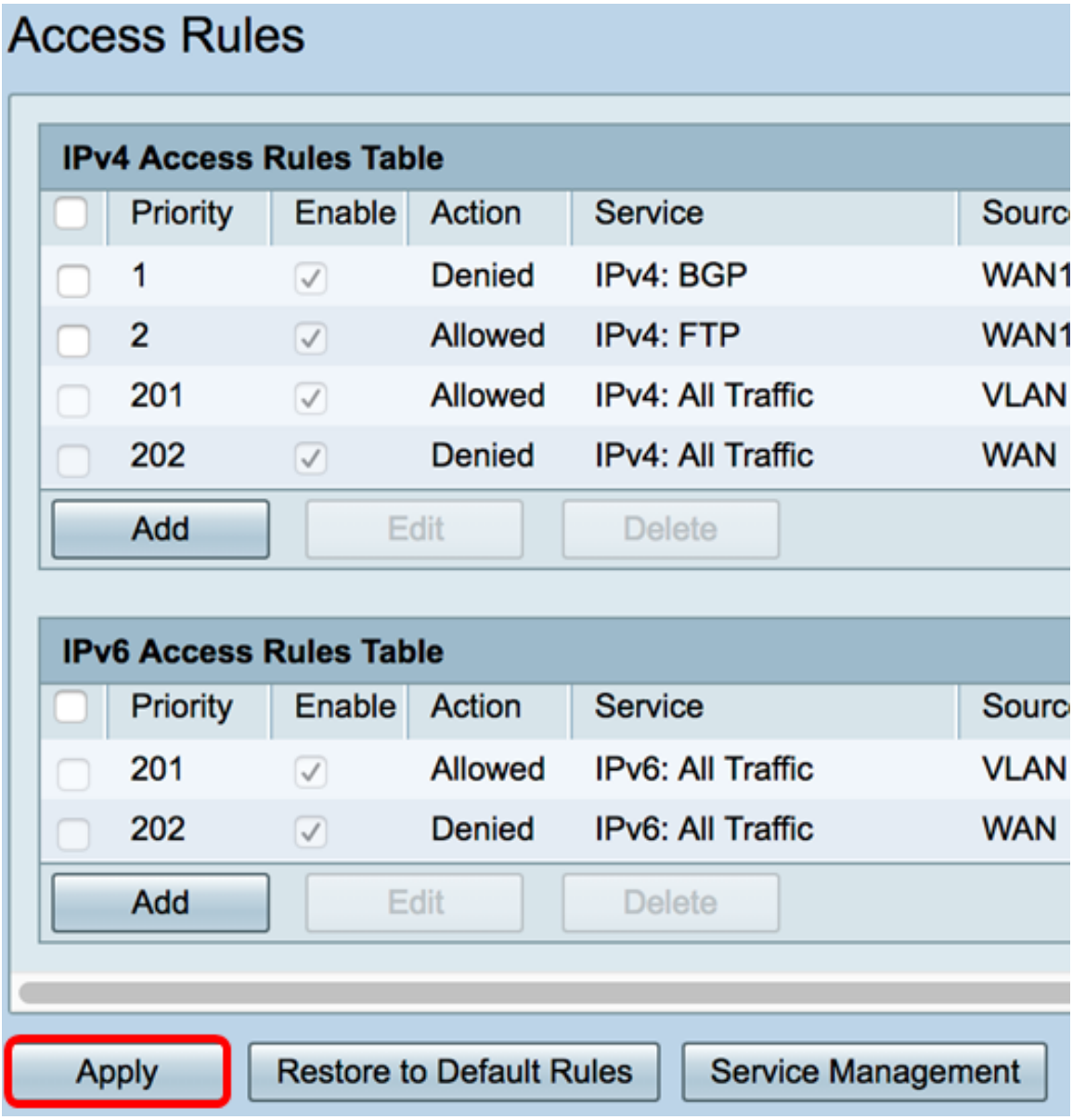
Note: Dans cet exemple, dans le tableau des règles d'accès IPv4, la priorité 1 est choisie.



Étape 2. Cliquez sur **Supprimer** situé sous le tableau ou cliquez sur le bouton Supprimer dans la colonne Configurer.



Étape 3. Cliquez sur Apply.



Vous devez maintenant avoir supprimé une règle d'accès sur le routeur de la gamme RV34x.

Afficher une vidéo relative à cet article...

Cliquez ici pour afficher d'autres présentations techniques de Cisco