Configuration d'une règle d'accès IPv4 sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Une règle dâ€™accès aide le routeur à déterminer, en fonction des besoins de lâ€™utilisateur, le trafic autorisé à passer et le trafic à refuser via le pare-feu. Cela permet d'ajouter de la sécurité au routeur.

Ce document explique la procédure à suivre pour ajouter ou supprimer une règle d'accès sur les routeurs VPN RV016, RV042, RV042G et RV082.

Périphériques pertinents

â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

Version du logiciel

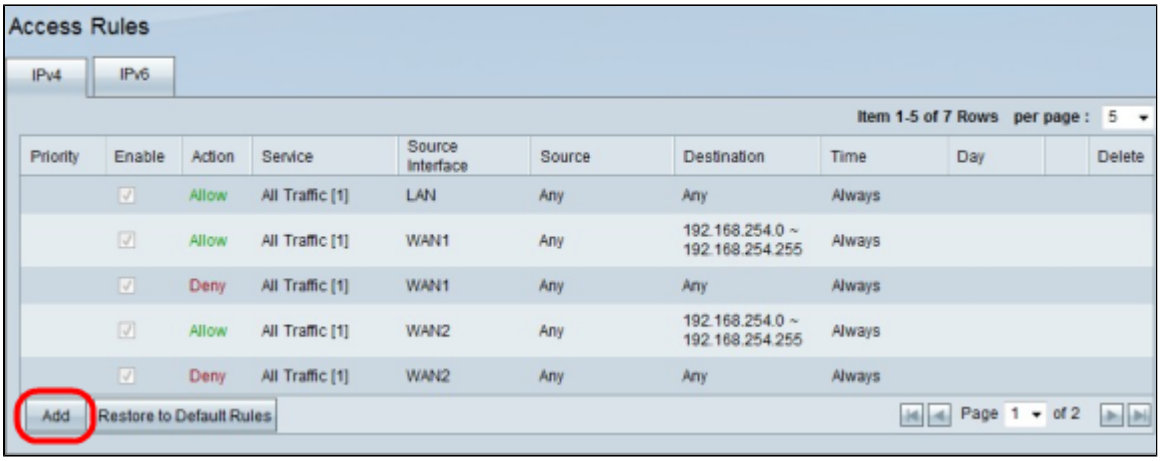
â€¢4.2.1.02

Gérer les règles d'accès IPv4

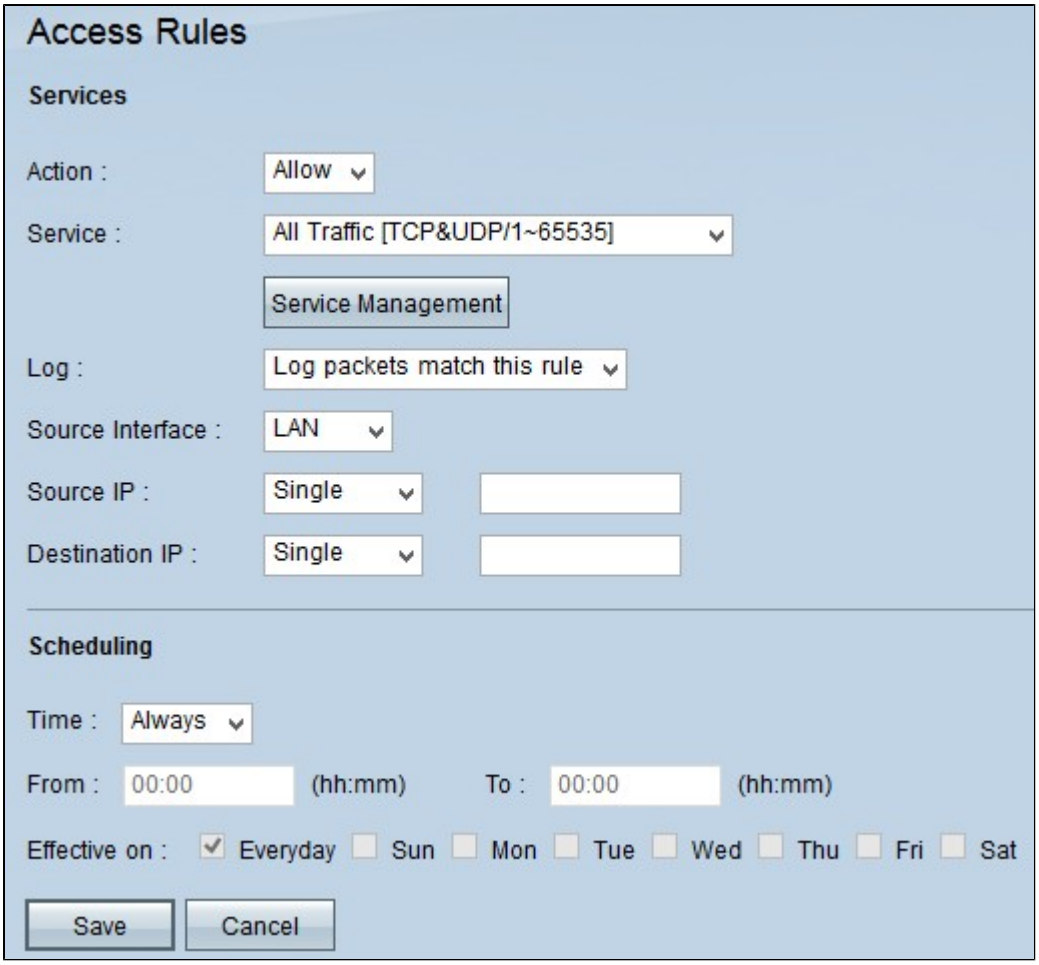
La planification des règles d'accès IPv4 est une configuration facultative.

Ajouter ou supprimer des règles d'accès IPv4

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Firewall > Access Rules**. La page *IPv4 Access Rules* s'ouvre. Cliquez sur **Add**.

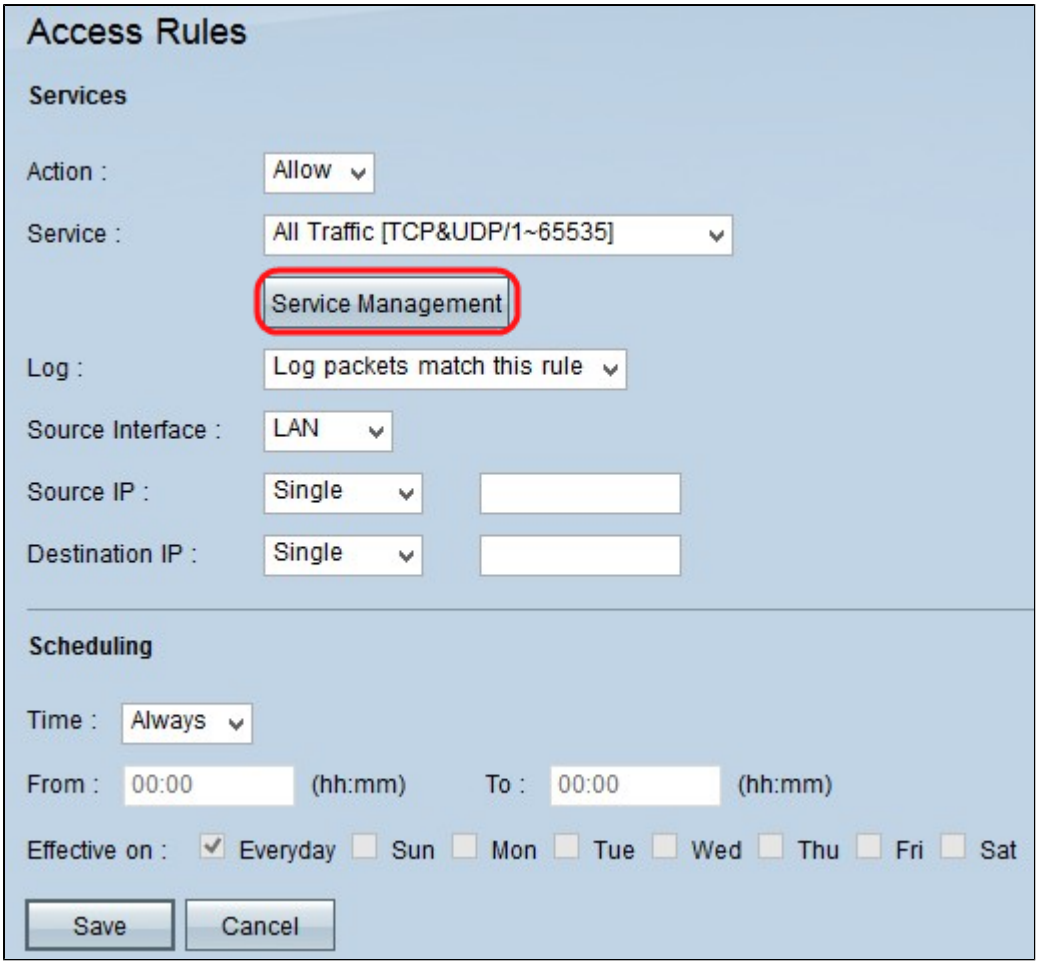


Étape 2. La page *Access Rules Service* s'ouvre. Dans la liste déroulante Action, sélectionnez **Allow** pour autoriser le trafic. Sinon, choisissez **Deny** pour refuser le trafic.



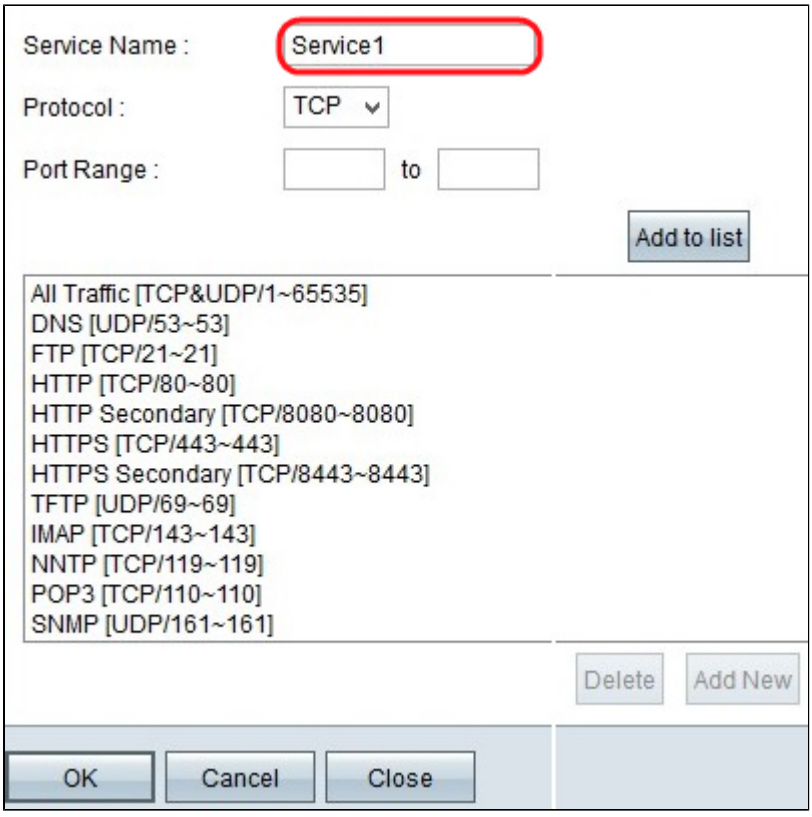
Étape 3. Sélectionnez le service approprié dans la liste déroulante Service. Si le service approprié n'est pas disponible, cliquez sur **Gestion des services.**

Remarque : si le service souhaité est disponible, passez à l'étape 6.



Étape 4.

Une nouvelle fenêtre s'affiche. Saisissez un nom de service dans le champ Nom de service.

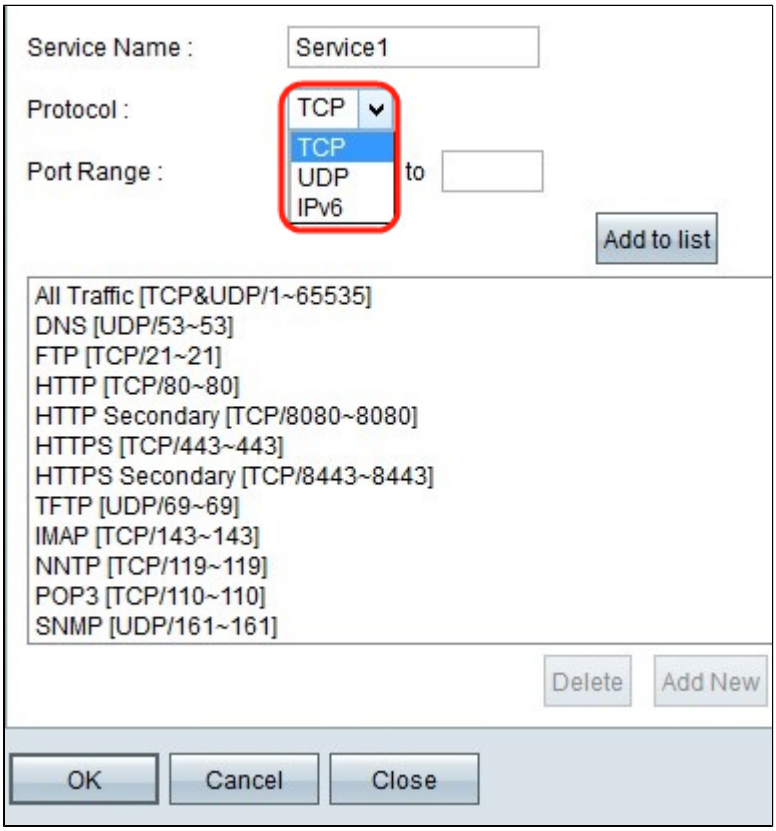


Étape 5. Sélectionnez le type de protocole approprié dans la liste déroulante Protocole.

· TCP (Transmission Control Protocol) : protocole de couche transport utilisé par les applications qui nécessitent une livraison garantie.

· UDP (User Datagram Protocol) : utilise des sockets de datagramme pour établir des communications entre hôtes. Il est plus rapide que le protocole TCP, mais il est moins susceptible de fonctionner correctement.

· IPv6 (Internet Protocol version 6) - Dirige le trafic Internet entre les hôtes dans des paquets qui sont routés sur des réseaux spécifiés par des adresses de routage.

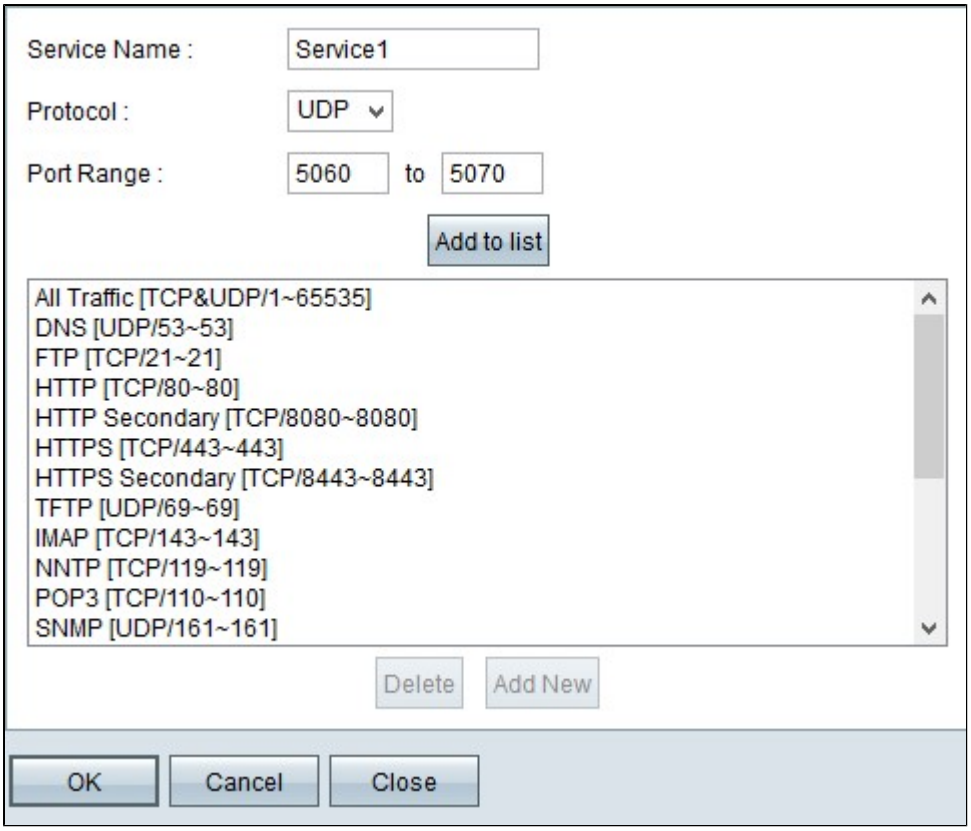


Étape 6. Saisissez la plage de ports dans les champs Port Range. Cette plage dépend du protocole choisi.

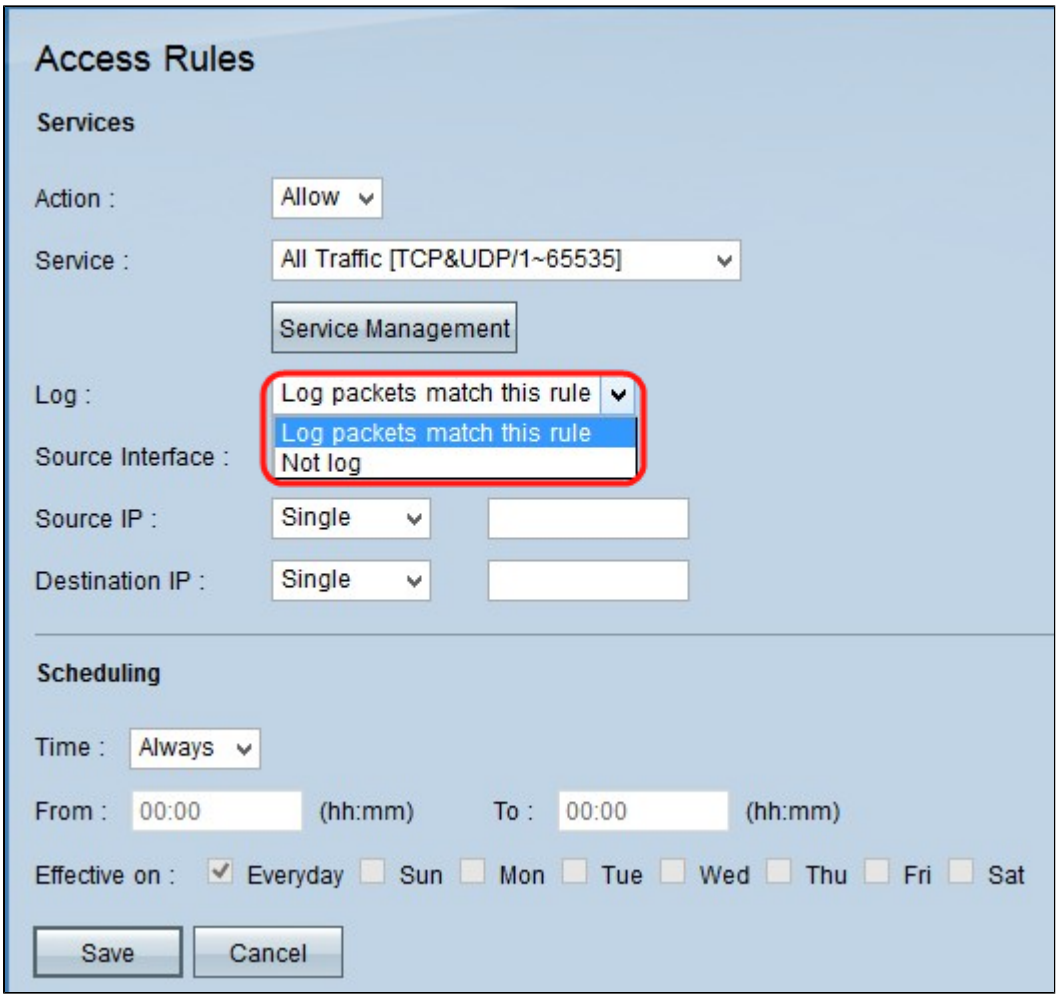
Cliquez sur **Add to List**. Le service est ajouté à la liste déroulante Service.

Les autres options disponibles ici sont **Supprimer**, **Mettre à jour** ou **Ajouter nouveau**.

Click OK. Cette opération ferme la fenêtre et ramène l'utilisateur à la page *Access Rule Service*.



Étape 7. Dans la liste déroulante Log, sélectionnez **Log packets match this rule** pour consigner les paquets entrants correspondant à la règle d'accès. Sinon, choisissez **Not Log**.



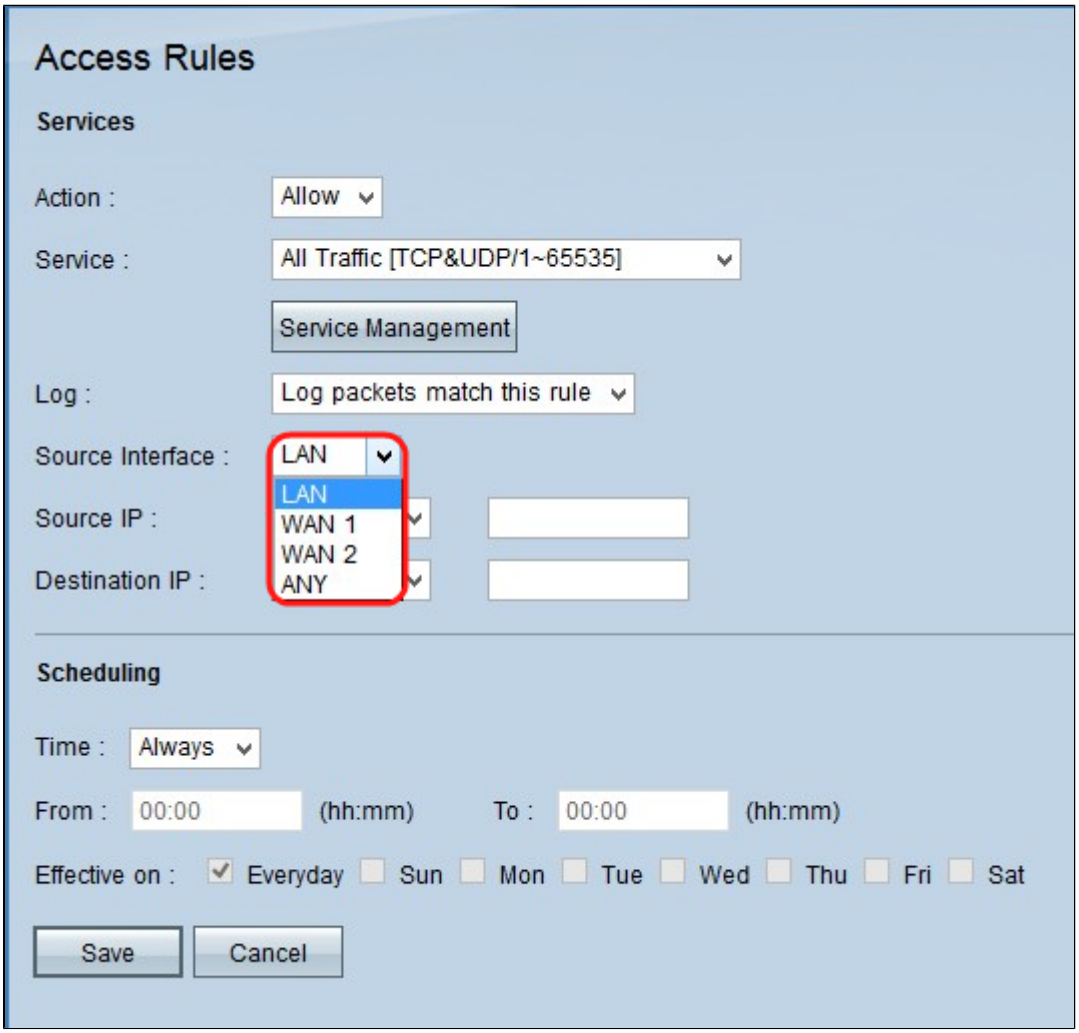
Étape 8. Sélectionnez l'interface affectée par cette règle dans la liste déroulante Interface source. Lâ€™interface source est lâ€™interface à partir de laquelle le trafic est initié.

· LAN : réseau local du routeur.

· WAN1 : réseau étendu ou réseau à partir duquel le routeur obtient Internet du FAI ou du routeur de tronçon suivant.

· WAN2 : identique à WAN1, à ceci près qu'il s'agit d'un réseau secondaire.

· ANY : permet d'utiliser n'importe quelle interface.

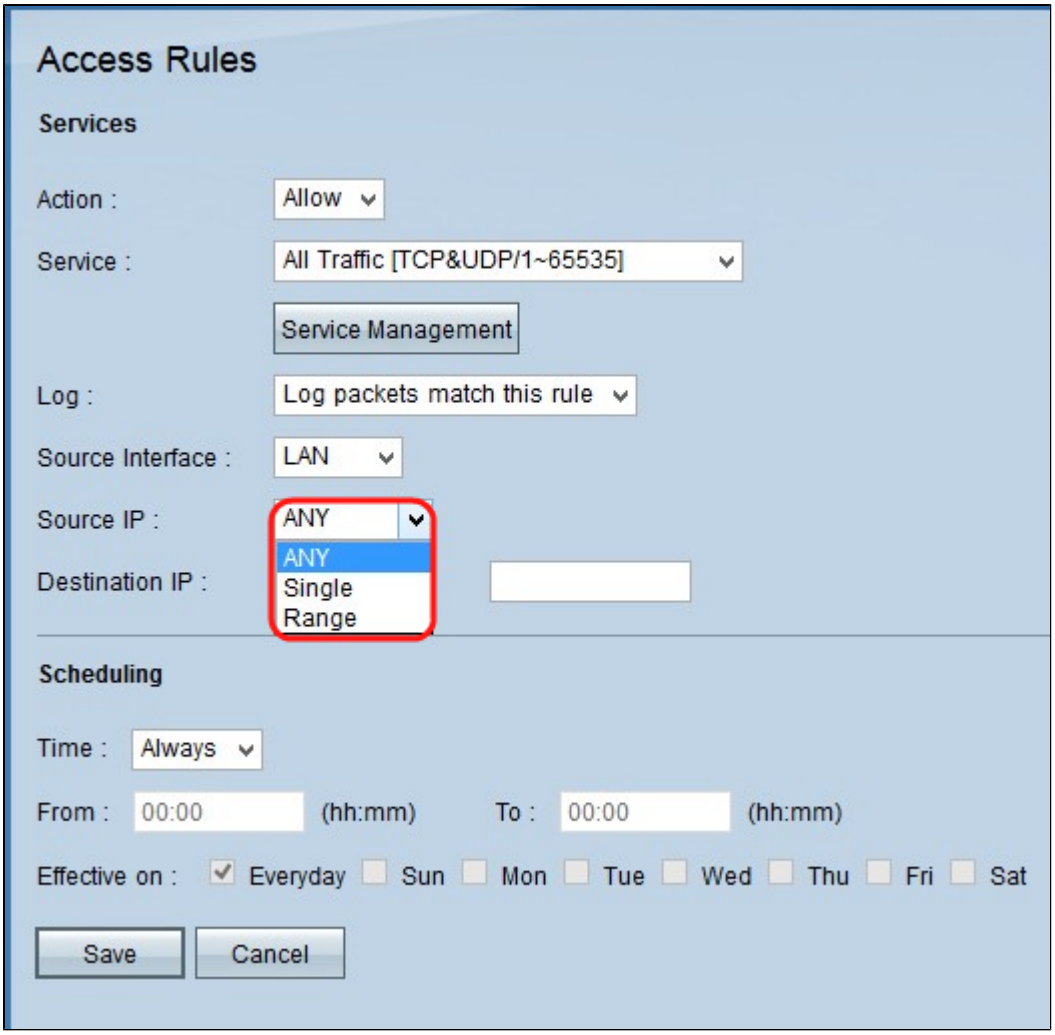


Étape 9. Dans la liste déroulante Adresse IP source, choisissez une option pour spécifier la plage d'adresses IP source qui doivent être autorisées ou refusées par l'interface. Les paquets qui arrivent sur lâ€™interface sont vérifiés par lâ€™IP source et lâ€™IP de destination.

· Any : la règle d'accès sera appliquée à tout le trafic provenant de l'interface source. Aucun champ n'est disponible à droite de la liste déroulante.

· Single : la règle d'accès sera appliquée à une adresse IP unique à partir de l'interface source. Saisissez l'adresse IP souhaitée dans le champ d'adresse.

· Plage : la règle d'accès sera appliquée sur un réseau de sous-réseau à partir de l'interface source. Saisissez l'adresse IP et la longueur du préfixe.



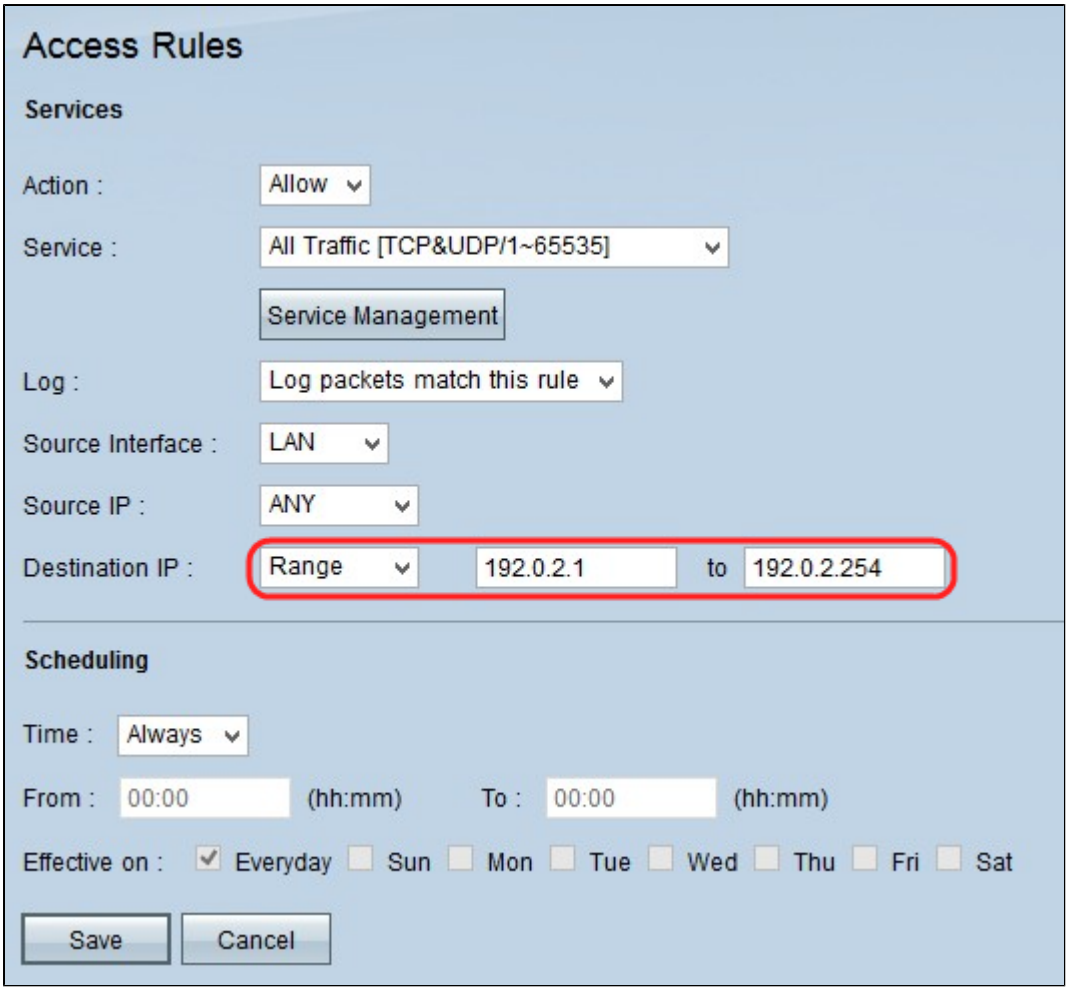
Étape 9. Dans la liste déroulante Destination, choisissez une option pour spécifier la plage d'adresses de destination qui doivent être autorisées ou refusées par l'interface. Les paquets qui arrivent sur lâ€™interface sont vérifiés par lâ€™IP source et lâ€™IP de destination.

· Any : la règle d'accès sera appliquée à tout le trafic vers l'interface de destination. Aucun champ n'est disponible à droite de la liste déroulante.

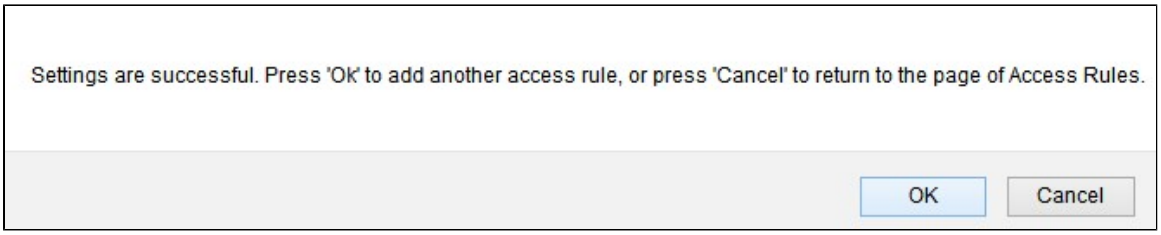
· Single : la règle d'accès sera appliquée sur une adresse IP unique à l'interface de destination. Saisissez l'adresse IP souhaitée dans le champ d'adresse.

· Plage : la règle d'accès sera appliquée sur un réseau de sous-réseau à l'interface de destination. Saisissez l'adresse IP et la longueur du préfixe.

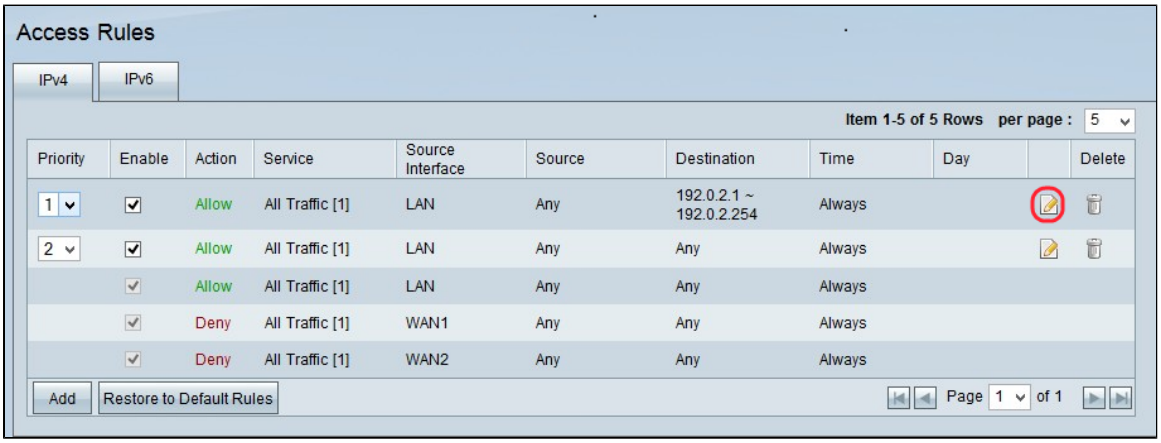
Cliquez sur **Save** pour enregistrer toutes les modifications apportées à la règle d'accès. Une fenêtre de confirmation s'affiche et indique l'état des modifications apportées au périphérique.



Étape 10. Cliquez sur **OK** pour ajouter une autre règle d'accès. Cliquez sur **Cancel** pour revenir à la page *Access Rules*.

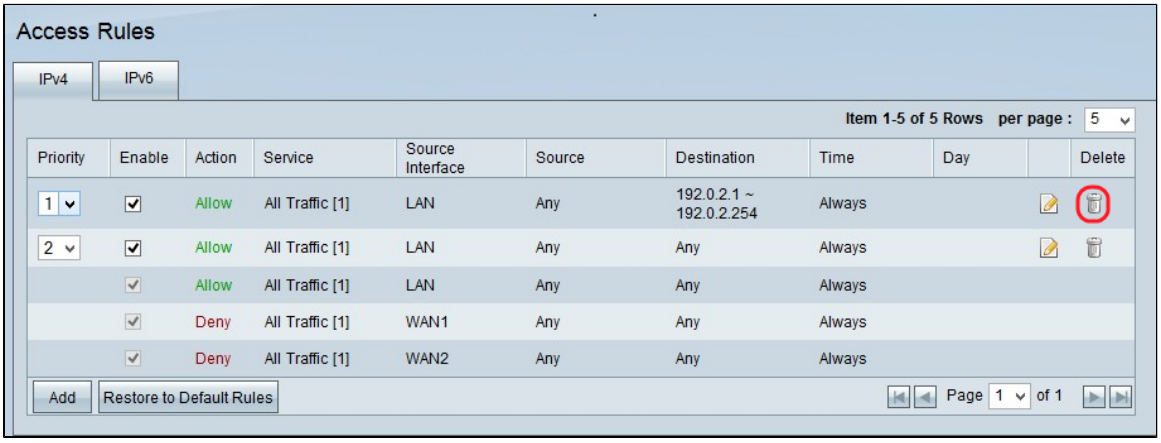


Étape 11 (facultatif). Choisissez la règle d'accès souhaitée dans la liste, puis cliquez sur **Modifier bouton** pour modifier la configuration de la règle d'accès.



Étape 12 (facultatif). Choisissez les règles d'accès souhaitées dans la liste, puis cliquez sur **Supprimer**

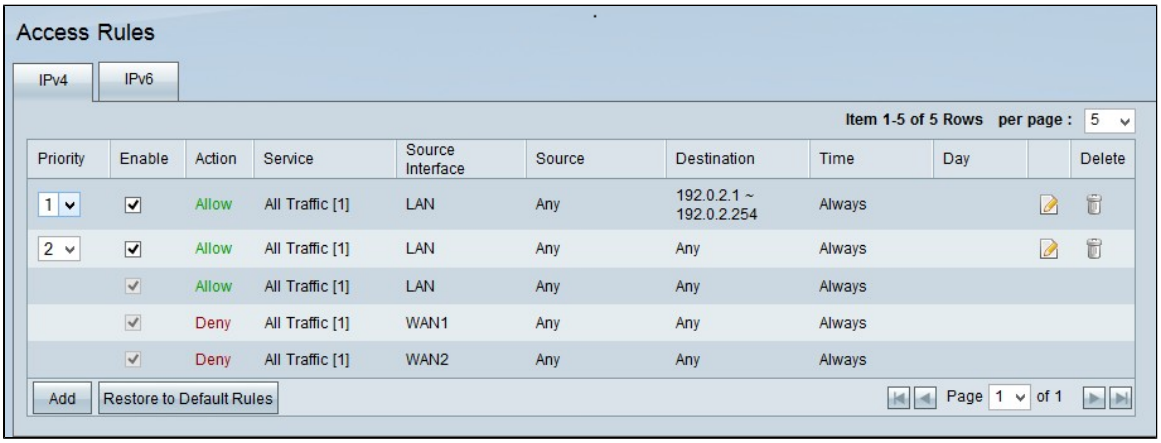
bouton pour supprimer la règle d'accès de la liste des règles d'accès.



Planifier des règles d'accès IPv4

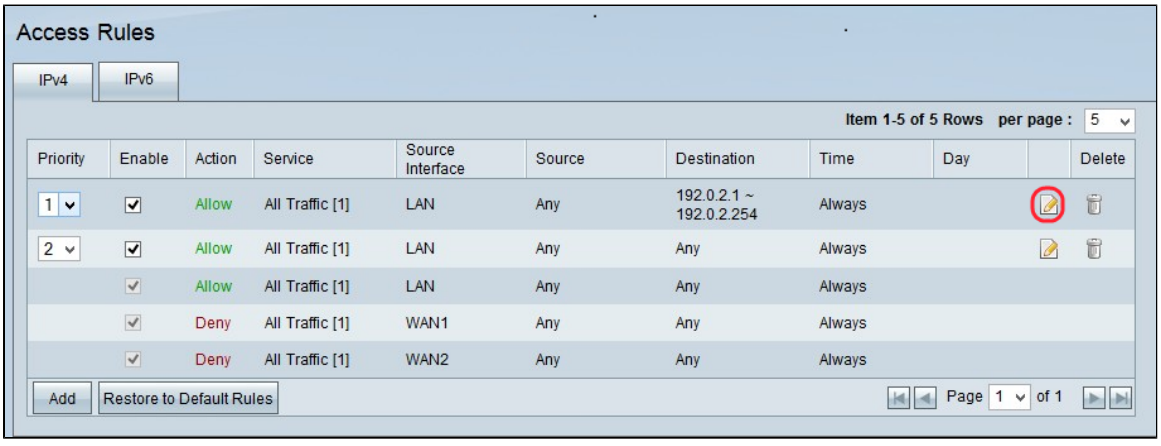
La planification des règles d'accès permet de spécifier une planification lorsque ces règles d'accès sont actives en termes de jour et d'heure. Il fonctionne uniquement avec IPv4.

Étape 1. Utilisez l'utilitaire de configuration Web et choisissez **Firewall > Access Rules**. La page *IPv4 Access Rules* s'ouvre :



Étape 2. Choisissez la règle d'accès dans le tableau et cliquez sur l'icône **Modifier** pour ajouter la fonctionnalité de planification à cette règle d'accès.

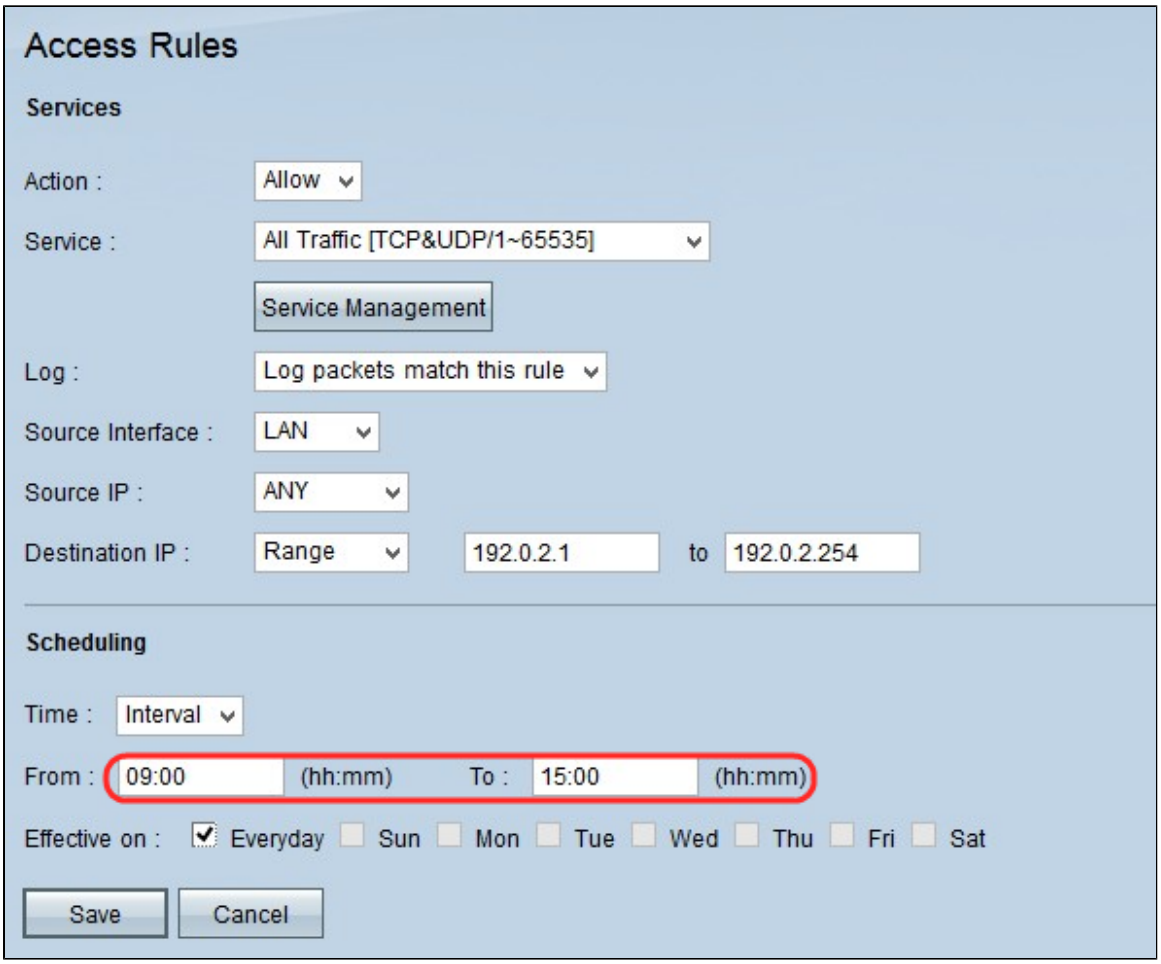
Remarque : vous pouvez également ajouter la fonction de réservation lorsque vous ajoutez une nouvelle règle d'accès.



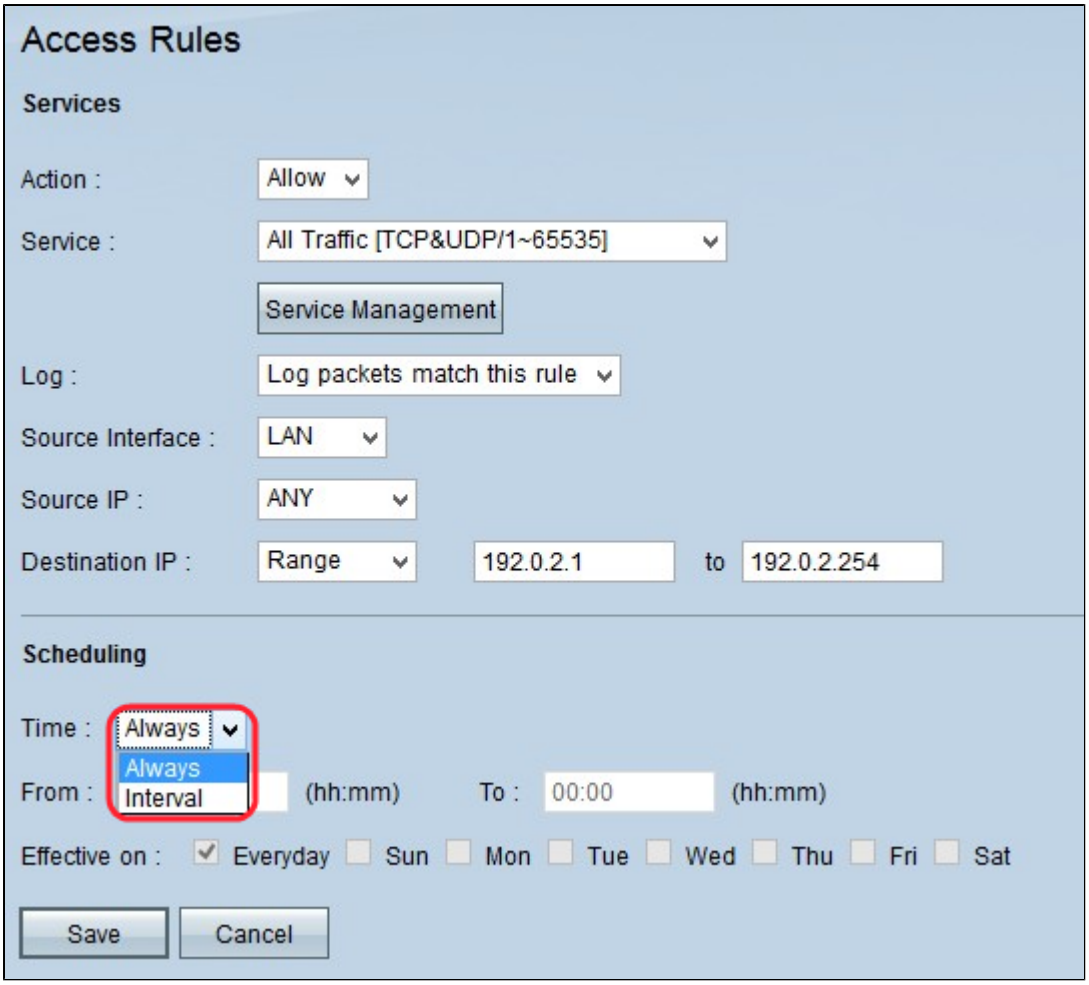
Étape 3. Sélectionnez l'heure dans la liste déroulante Heure. Elle indique quand utiliser la planification.

· Toujours - La règle d'accès s'applique à tout moment et tous les jours de la semaine. Il est sélectionné par défaut. Si vous choisissez cette option, cliquez sur *Save* et passez à l'étape 6.

· Interval : en fonction de l'intervalle de temps donné par l'utilisateur, la règle d'accès est appliquée.

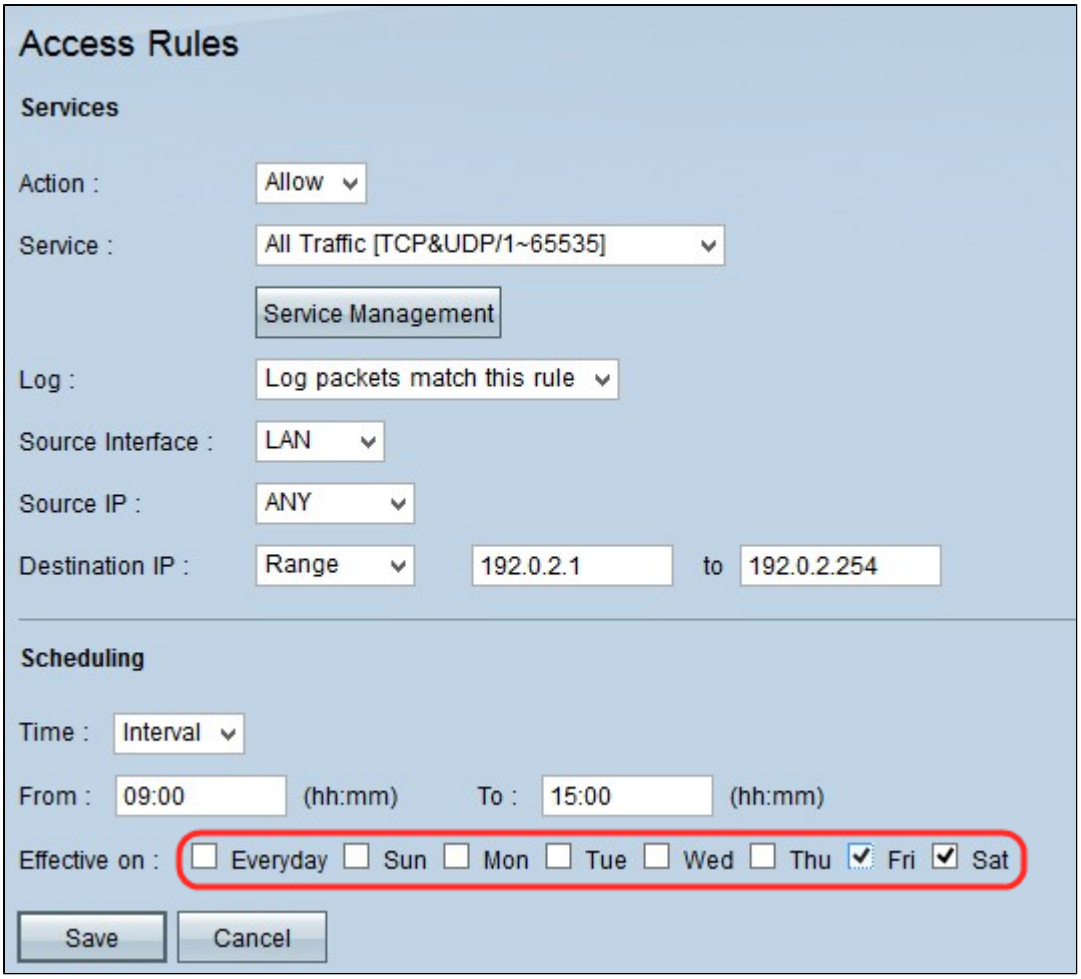


Étape 4. Saisissez l'intervalle de temps au format 24 heures pendant lequel la règle d'accès est appliquée dans les champs *De* et *A*.

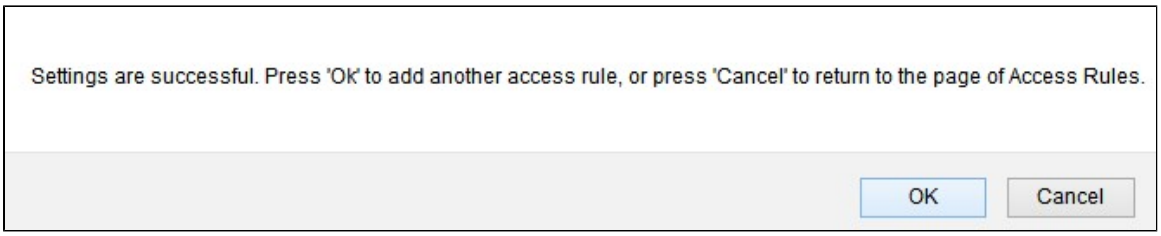


Étape 5. Cochez les cases en regard des jours auxquels vous souhaitez appliquer la règle d'accès. La règle d'accès ne sera effective que les jours vérifiés. Par défaut, *Everyday* est sélectionné.

Cliquez sur **Save** pour enregistrer toutes les modifications apportées à la règle d'accès. Des fenêtres de confirmation s'affichent, indiquant l'état des modifications apportées au périphérique.



Étape 6. Cliquez sur **OK** pour ajouter une autre règle d'accès. Cliquez sur **Cancel** pour revenir à la page de la règle d'accès.



Conclusion

Vous venez de configurer des règles d'accès IPv4 sur votre routeur VPN RV016, RV042, RV042G ou RV082.

Si vous souhaitez accéder à toute la prise en charge de ces routeurs, consultez la page produit en cliquant ici.

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.