Configuration d'une règle d'accès IPv6 sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Une règle d’accès aide le routeur à déterminer le trafic autorisé à traverser le pare-feu. Cela permet d'ajouter de la sécurité au routeur.

Cet article explique comment ajouter une règle d'accès IPv6 sur les routeurs VPN RV016, RV042, RV042G et RV082.

Périphériques pertinents

- RV016
- RV042
- RV042G
- RV082

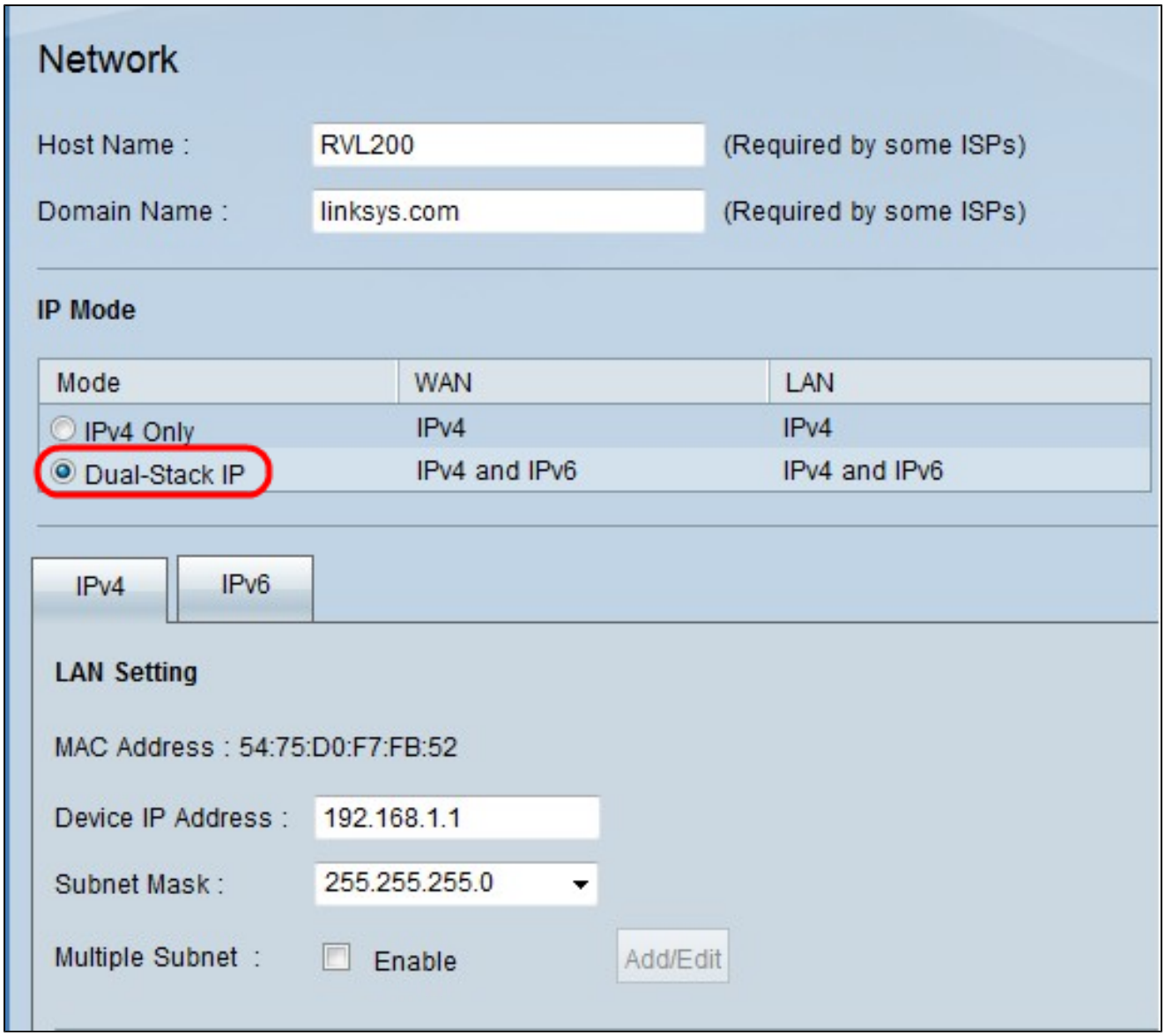
Version du logiciel

- v 4.2.1.02

Configuration d'une règle d'accès IPv6

Activer le mode IPv6

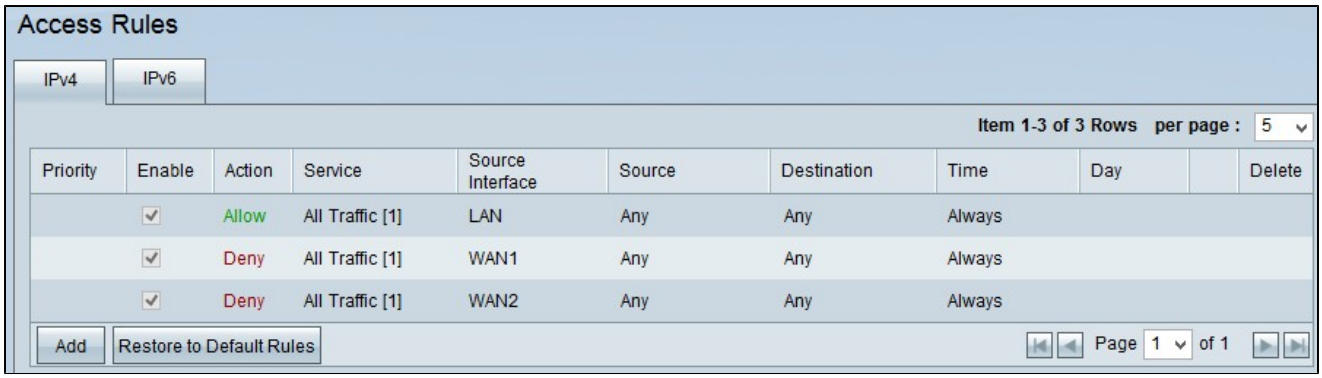
Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Setup > Network. La page Réseau s'ouvre :



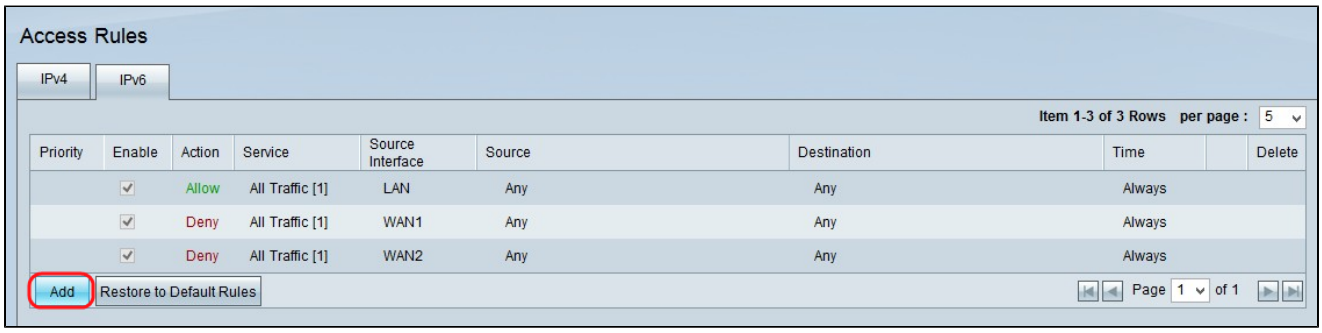
Étape 2. Cliquez sur la case d'option Dual-Stack IP. Cela permet aux protocoles IPv4 et IPv6 de s'exécuter simultanément. Si la communication IPv6 est possible, il s'agit de la communication préférée.

Configuration des règles d'accès IPv6

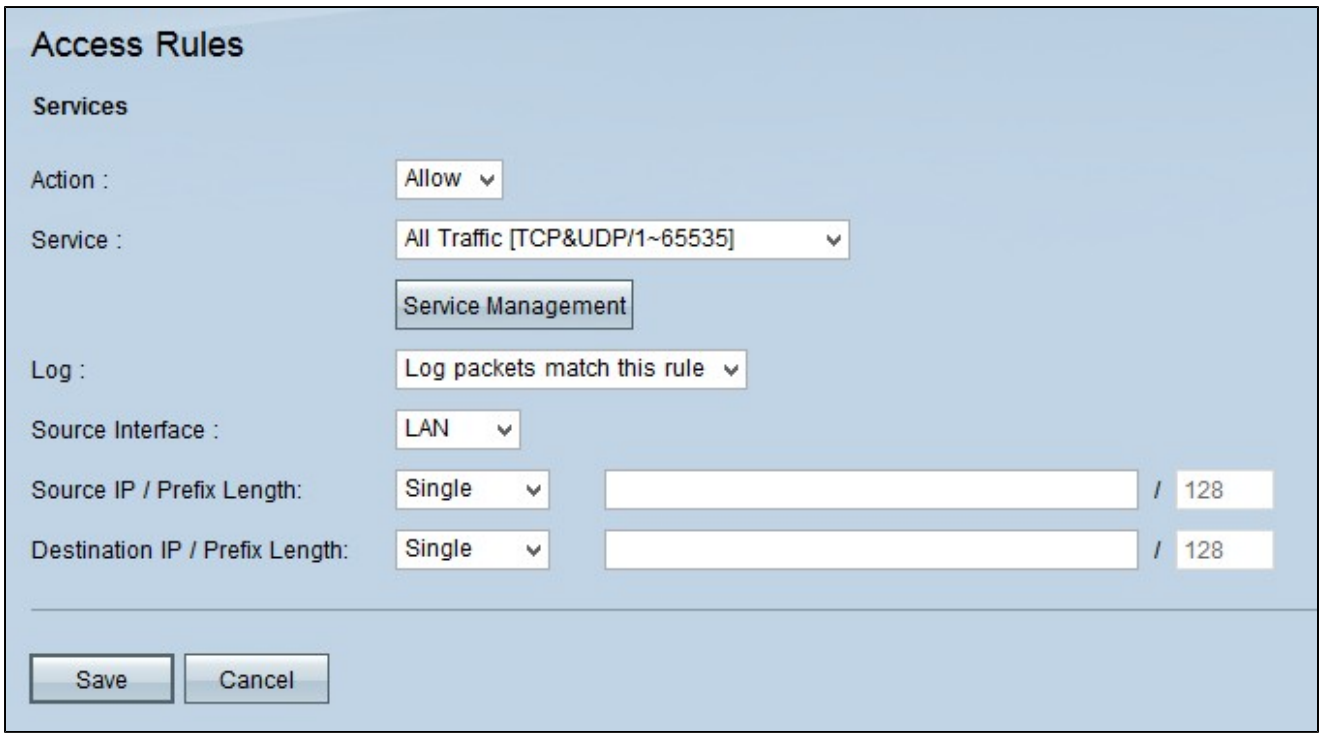
Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Firewall > Access Rules. La page Access Rules s'ouvre :



Étape 2. Cliquez sur l'onglet IPv6. La page Règles d'accès IPv6 s'ouvre.



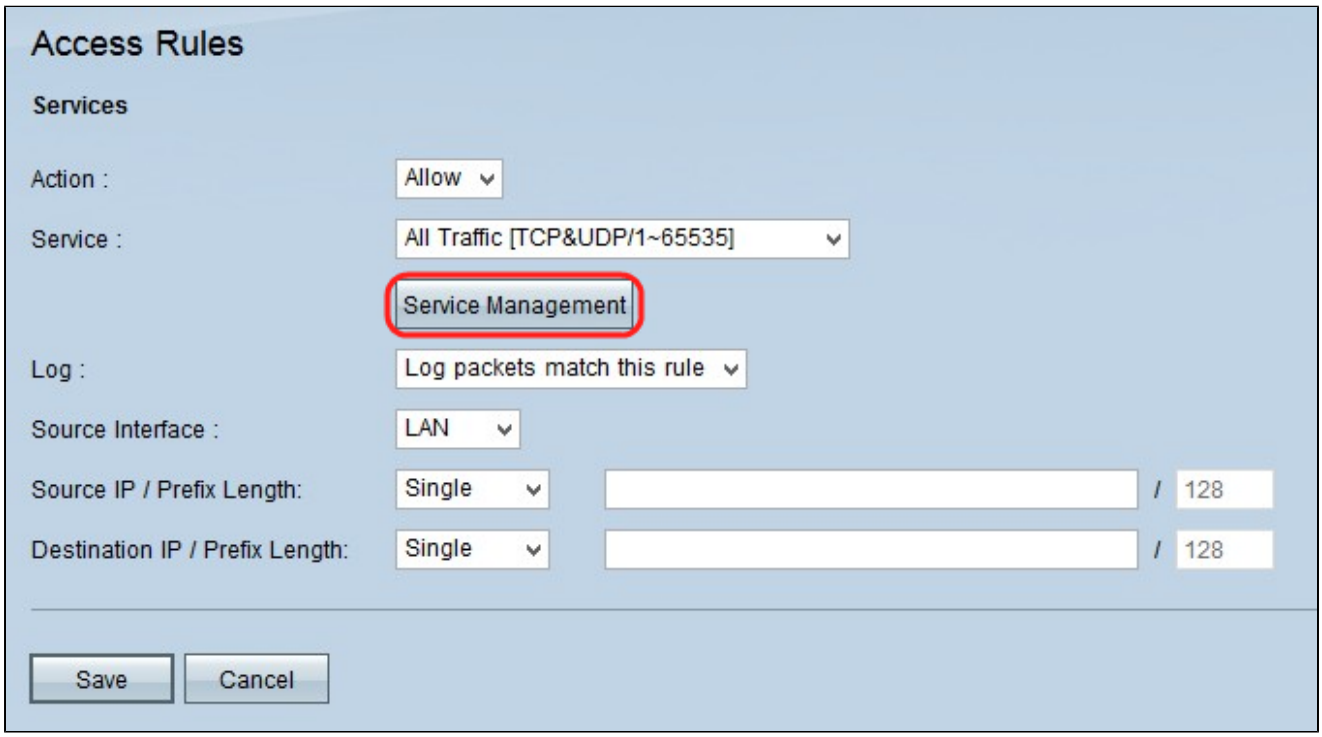
Étape 3. Cliquez sur Add pour ajouter les règles d'accès. La page Access Rules s'affiche pour configurer les règles d'accès pour IPv6.



Étape 4. Choisissez Allow dans la liste déroulante Action si le trafic doit être autorisé. Choisissez Deny pour refuser le trafic.

Étape 5. Sélectionnez le service approprié dans la liste déroulante Service.

Gain de temps : si le service souhaité est disponible, passez à l'étape 12.



Étape 6. Si le service approprié n'est pas disponible, cliquez sur Gestion des services. La fenêtre Gestion des services s'affiche.

Service Name :

Protocol : TCP

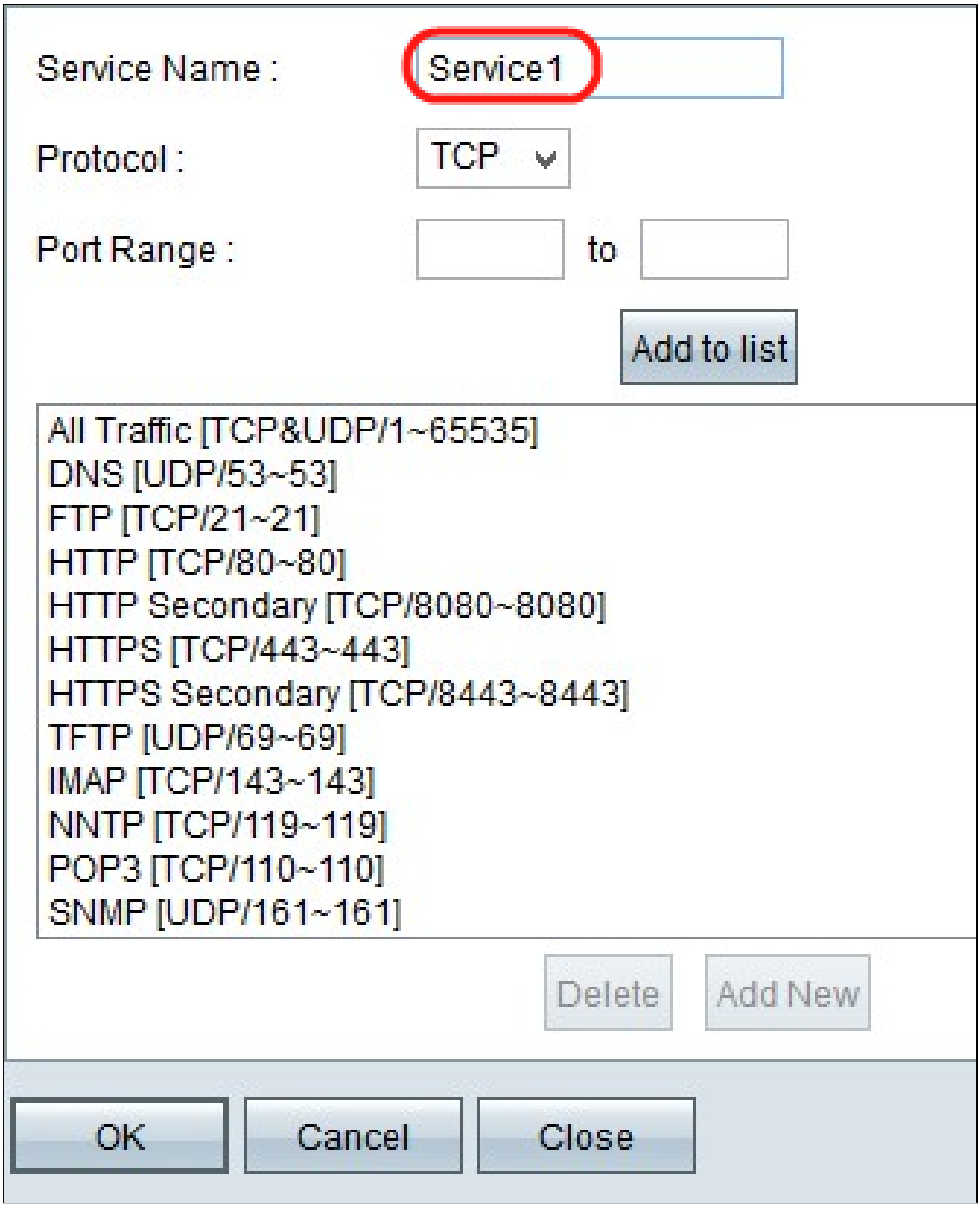
Port Range : to

Add to list

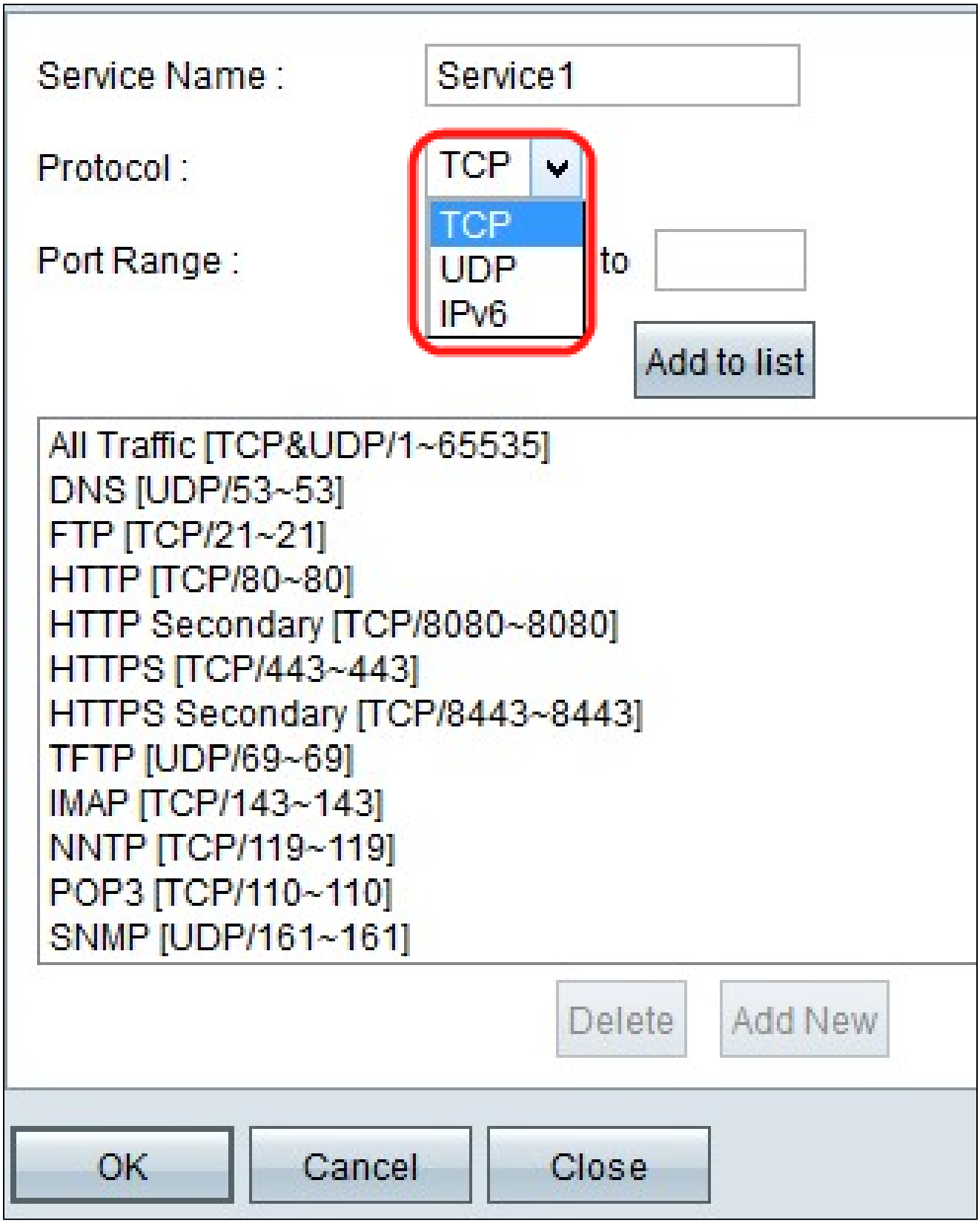
All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]

Delete Add New

OK Cancel Close



Étape 7. Saisissez le nom du nouveau service dans le champ Nom du service.

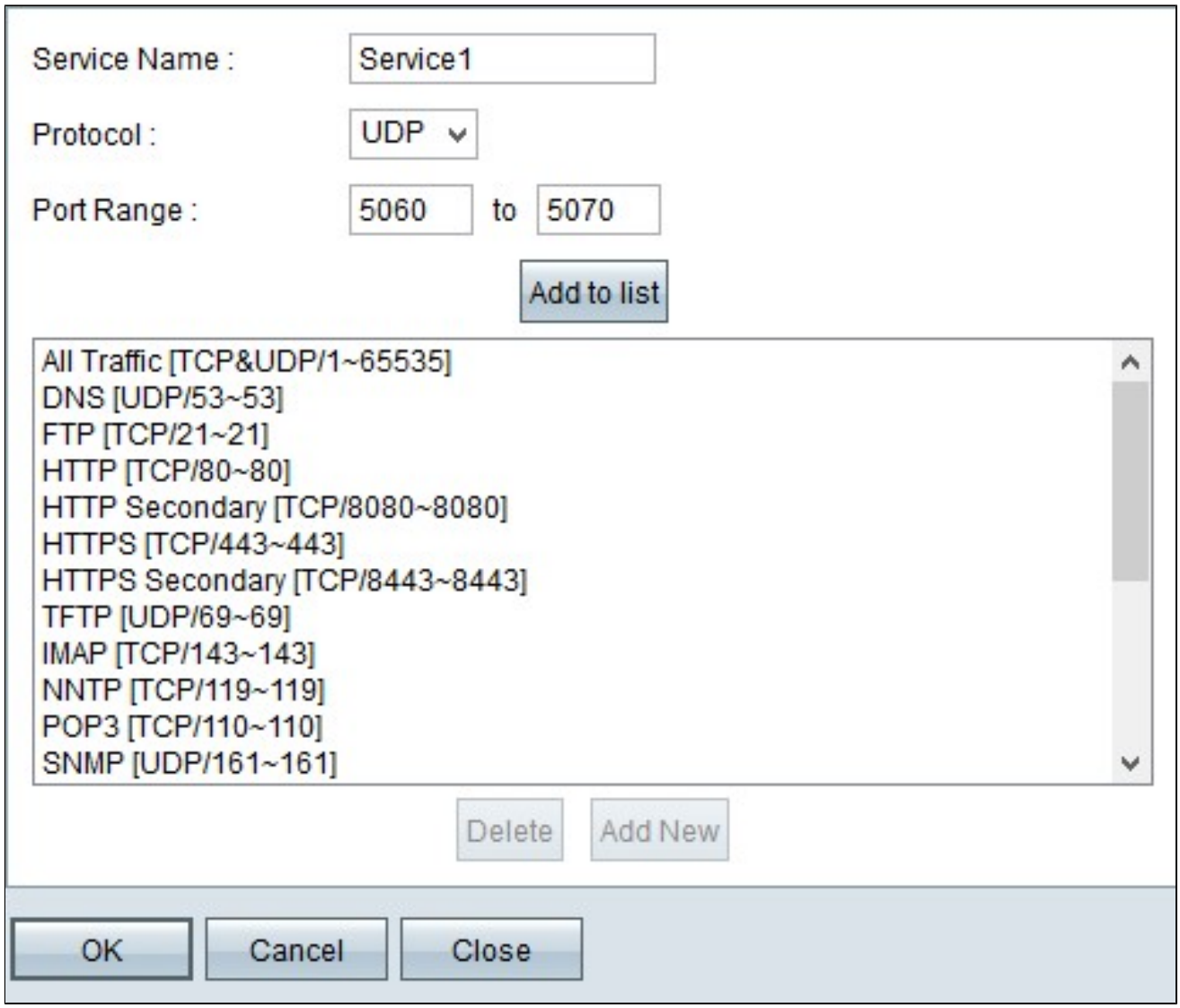


Étape 8. Sélectionnez le type de protocole approprié dans la liste déroulante Protocole.

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

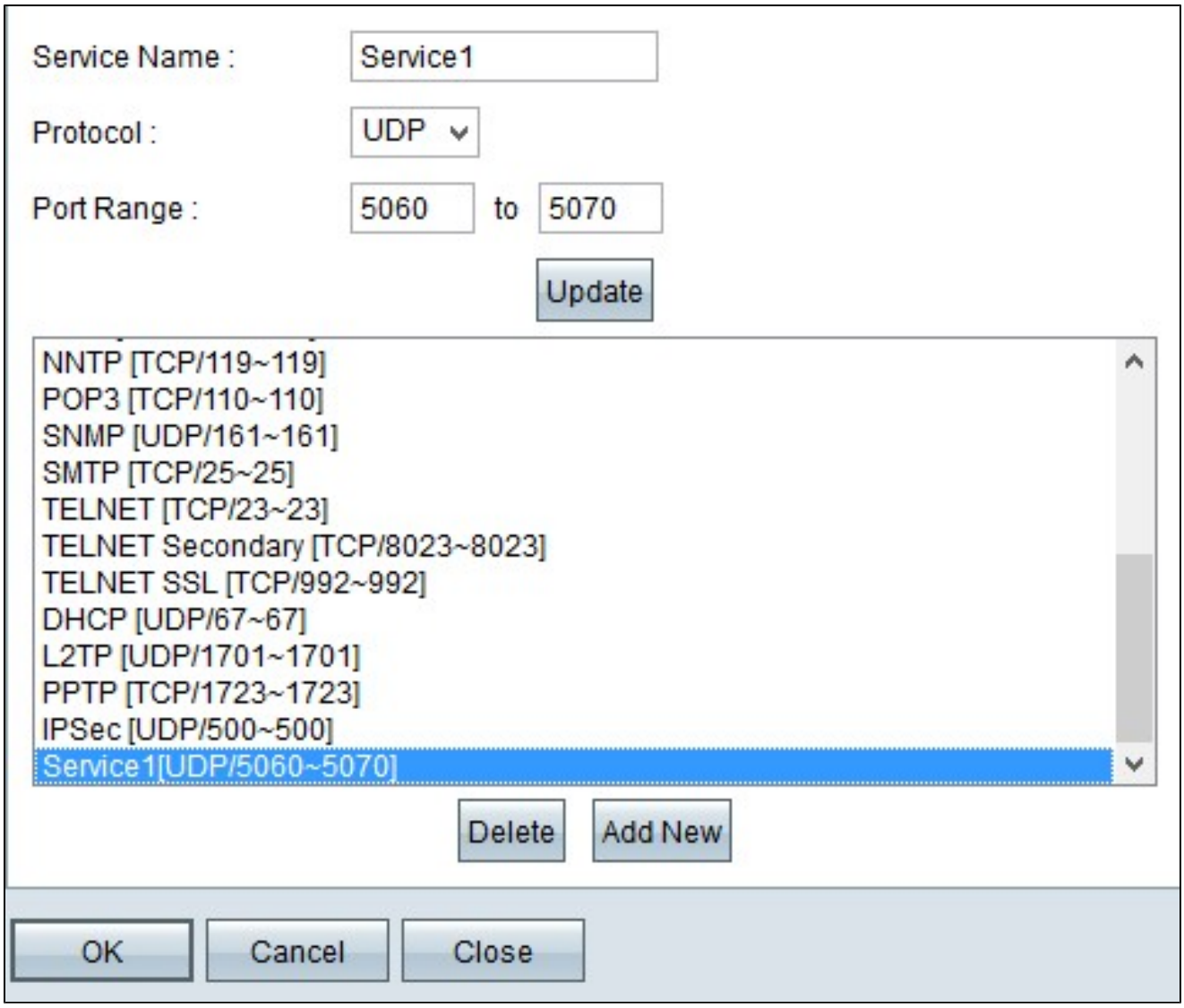
· UDP (User Datagram Protocol) : utilise des sockets de datagramme pour établir des communications entre hôtes. La livraison UDP n'est pas garantie.

· 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 9. Saisissez la plage de ports dans le champ Port Range. Cette plage dépend du protocole choisi à l'étape précédente.

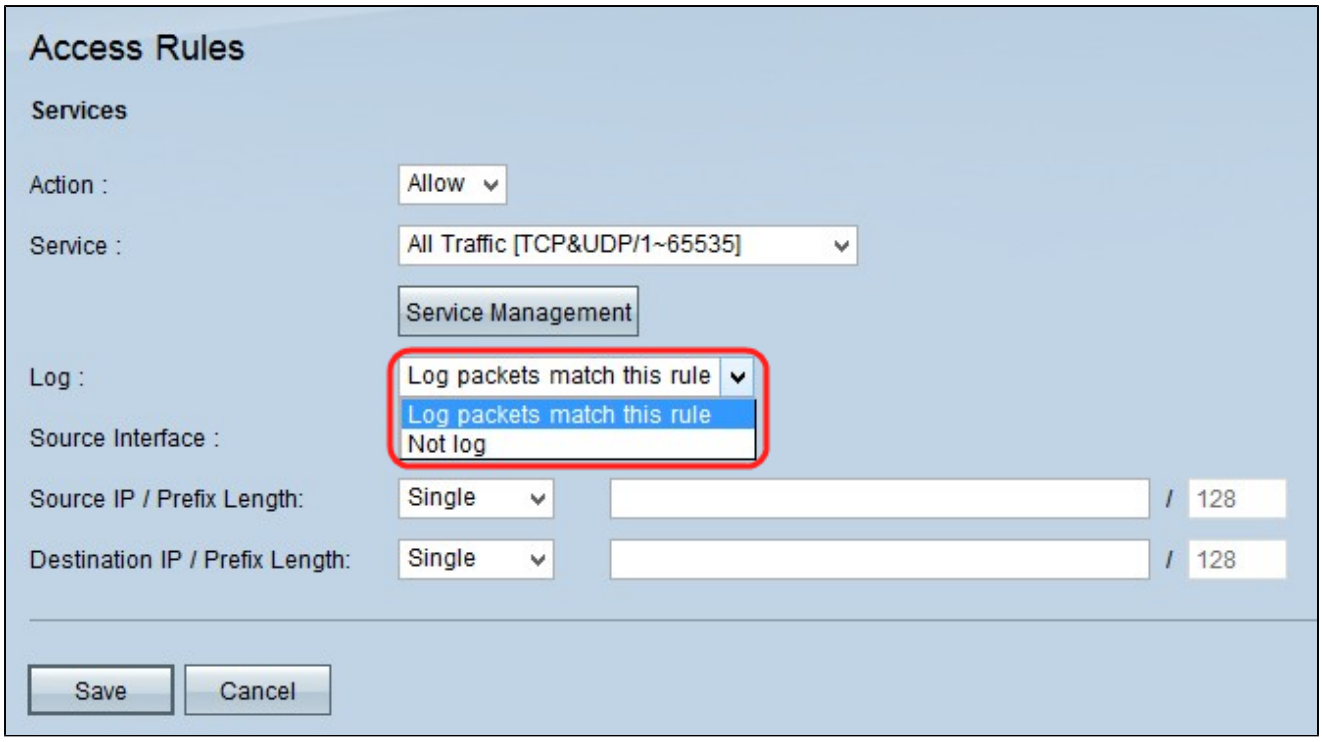
Étape 10. Cliquez sur Add to List. Le service est ajouté à la liste déroulante Service.



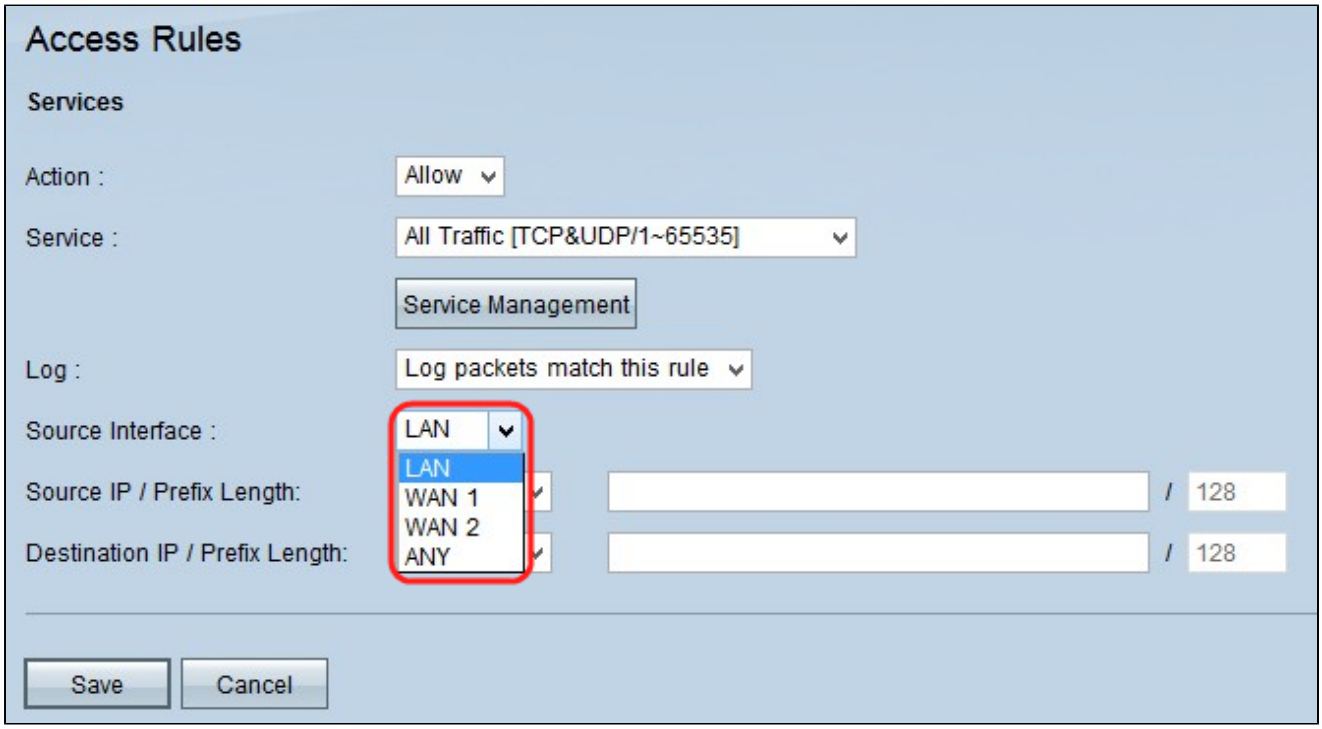
Remarque : si vous souhaitez supprimer un service de la liste des services, sélectionnez-le dans la liste et cliquez sur Supprimer. Si vous souhaitez mettre à jour l'entrée de service, sélectionnez le service à mettre à jour dans la liste des services, puis cliquez sur Mettre à jour. Pour ajouter un autre nouveau service à la liste, cliquez sur Add New.

Étape 11. Click OK. Cela ferme la fenêtre et ramène l'utilisateur à la page Règle d'accès.

Remarque : si vous cliquez sur Add New, suivez les étapes 7 à 11.



Étape 12. Si vous voulez consigner les paquets qui correspondent à la règle d'accès, choisissez Consigner les paquets qui correspondent à cette règle dans la liste déroulante Consigner. Sinon, choisissez Not Log.



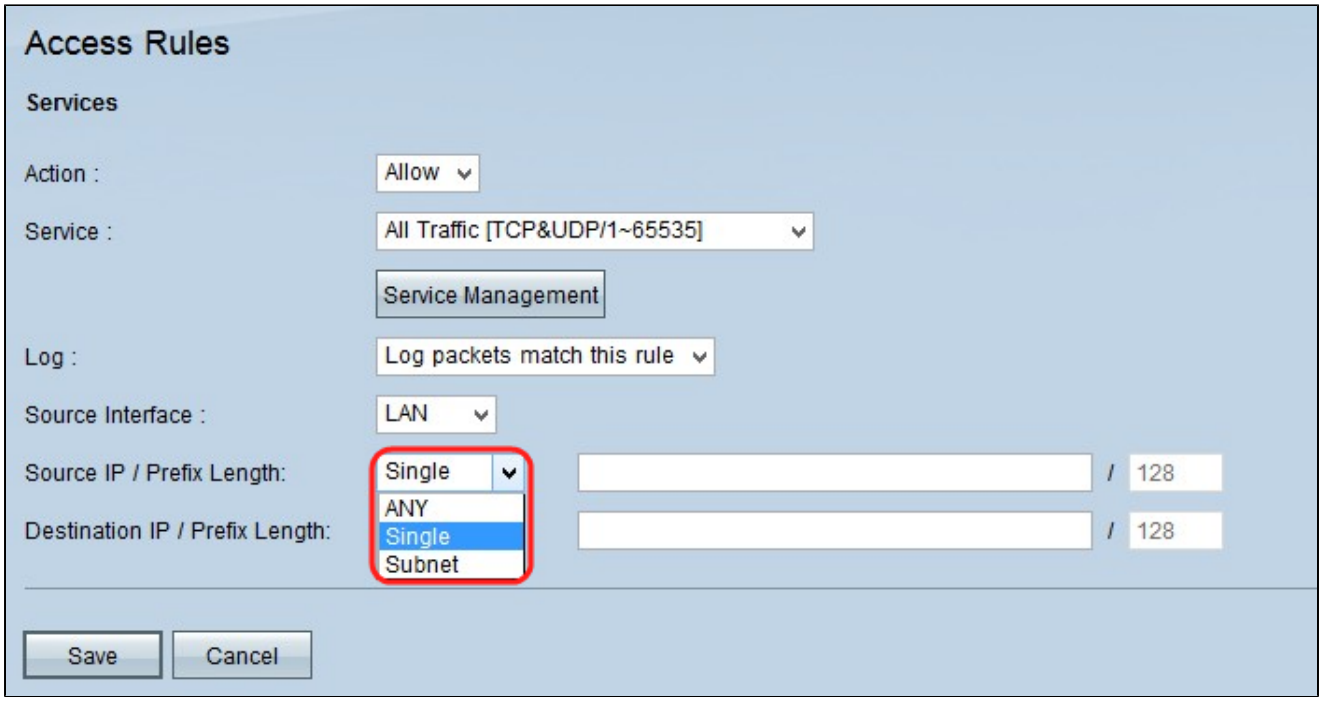
Étape 13. Sélectionnez l'interface affectée par cette règle dans la liste déroulante Interface source. L'interface source est l'interface à partir de laquelle le trafic est initié.

· 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.

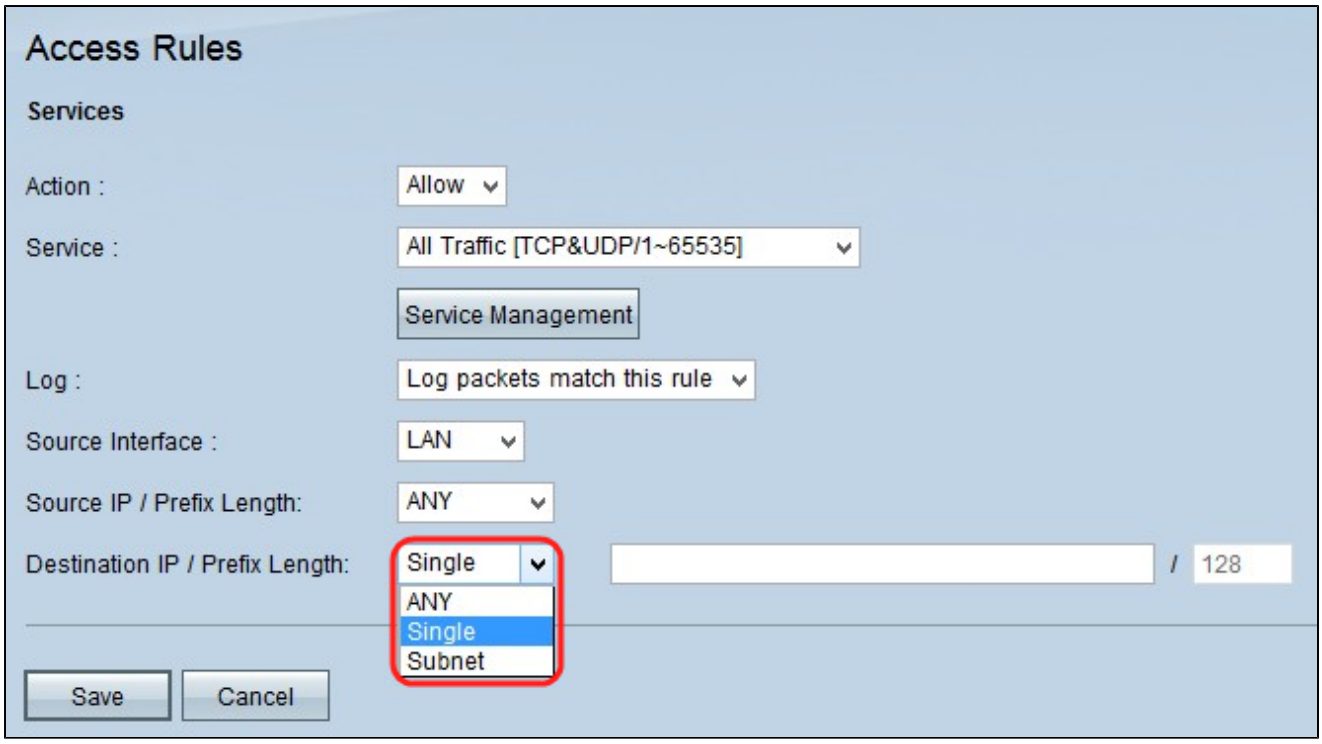


Étape 14. Dans la liste déroulante Source IP, choisissez une option pour spécifier l'adresse IP source à laquelle la règle d'accès est appliquée.

· 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.

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



Étape 15. Dans la liste déroulante Destination IP, choisissez une option pour spécifier l'adresse IP de destination à laquelle la règle d'accès est appliquée.

· 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.

· Subnet : 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.

Étape 16. Cliquez sur Save pour enregistrer toutes les modifications apportées à la règle d'accès IPv6.

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.