Configuration d'une règle d'accès de pare-feu pour bloquer les paquets Ping de deux réseaux différents sur les routeurs VPN RV016, RV042, RV042G et RV082

Objectif

Deux réseaux différents peuvent être nécessaires sur un routeur pour fournir un accès Internet à des périphériques qui ne se trouvent pas sur le même réseau que le routeur. Cela peut être réalisé par une règle d'accès basée sur divers critères afin d'autoriser ou de refuser l'accès à n'importe quel réseau ou plage d'adresses IP. Une règle d’accès aide le routeur à déterminer le trafic autorisé à traverser le pare-feu et à renforcer la sécurité du routeur.

Cet article explique comment bloquer les paquets ping de deux réseaux différents sur les routeurs VPN RV016, RV042, RV042G et RV082 par le biais d'une règle d'accès.

Périphériques pertinents

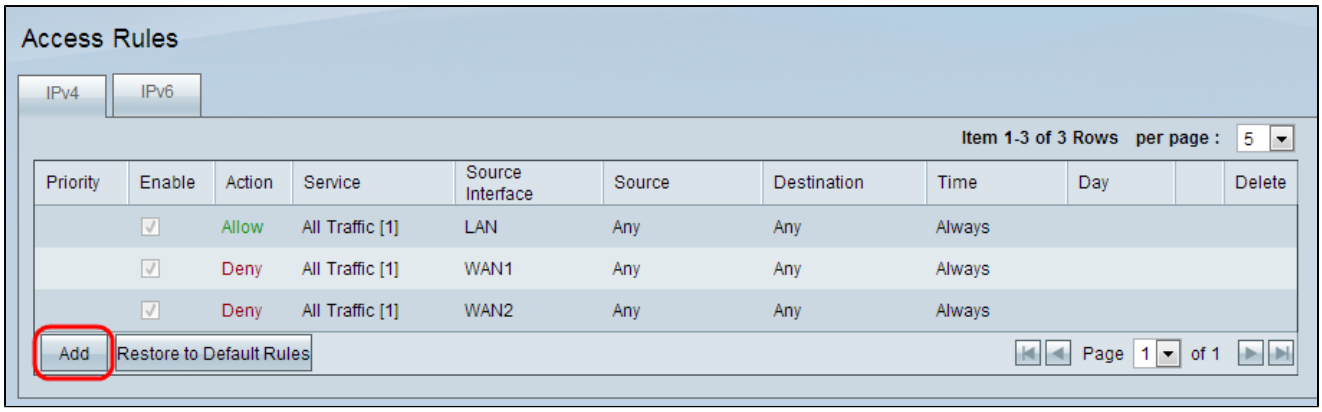
- RV016
- RV042
- RV042G
- RV082

Version du logiciel

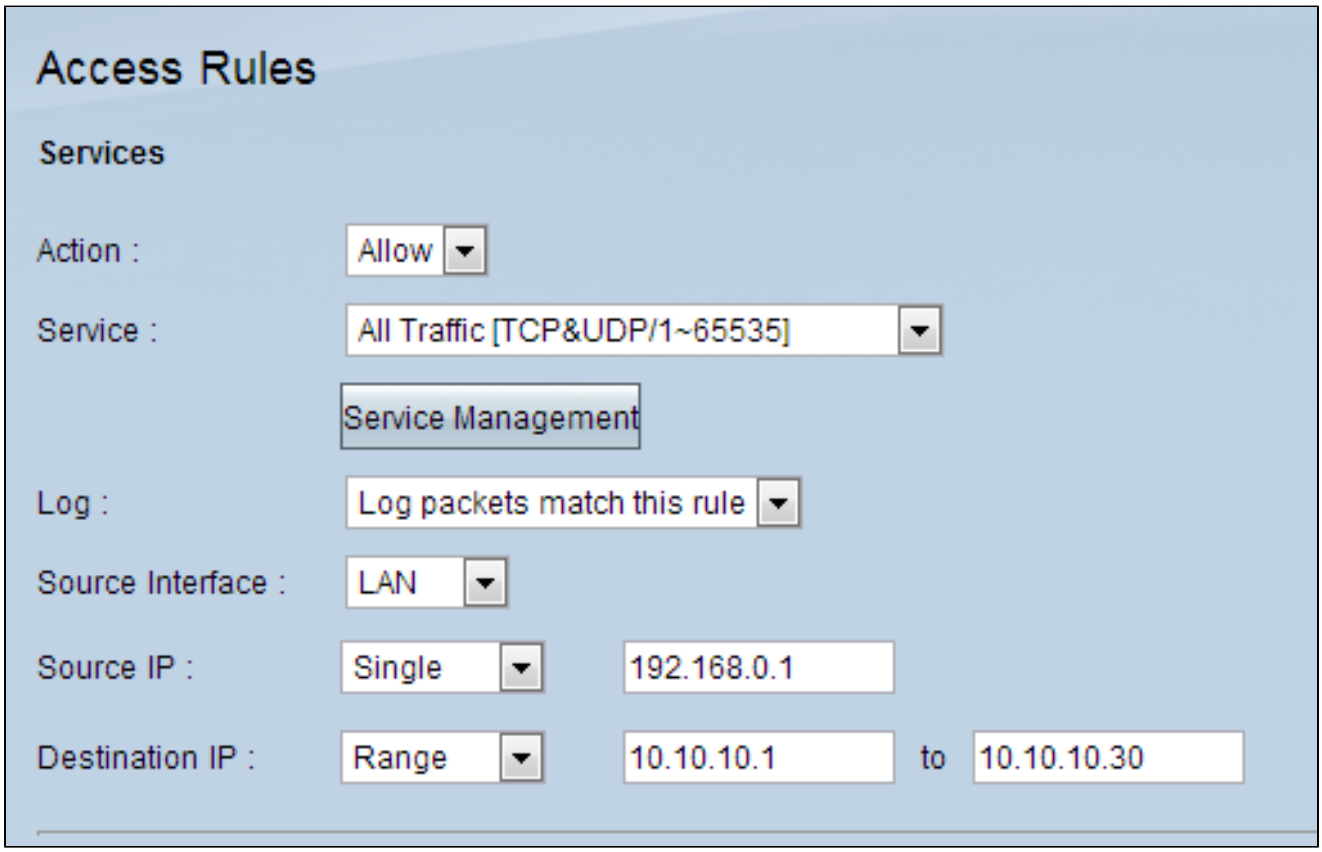
- v 4.2.1.02

Configuration des règles d'accès

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 Add pour ajouter une règle d'accès. La page Access Rules Services s'ouvre :

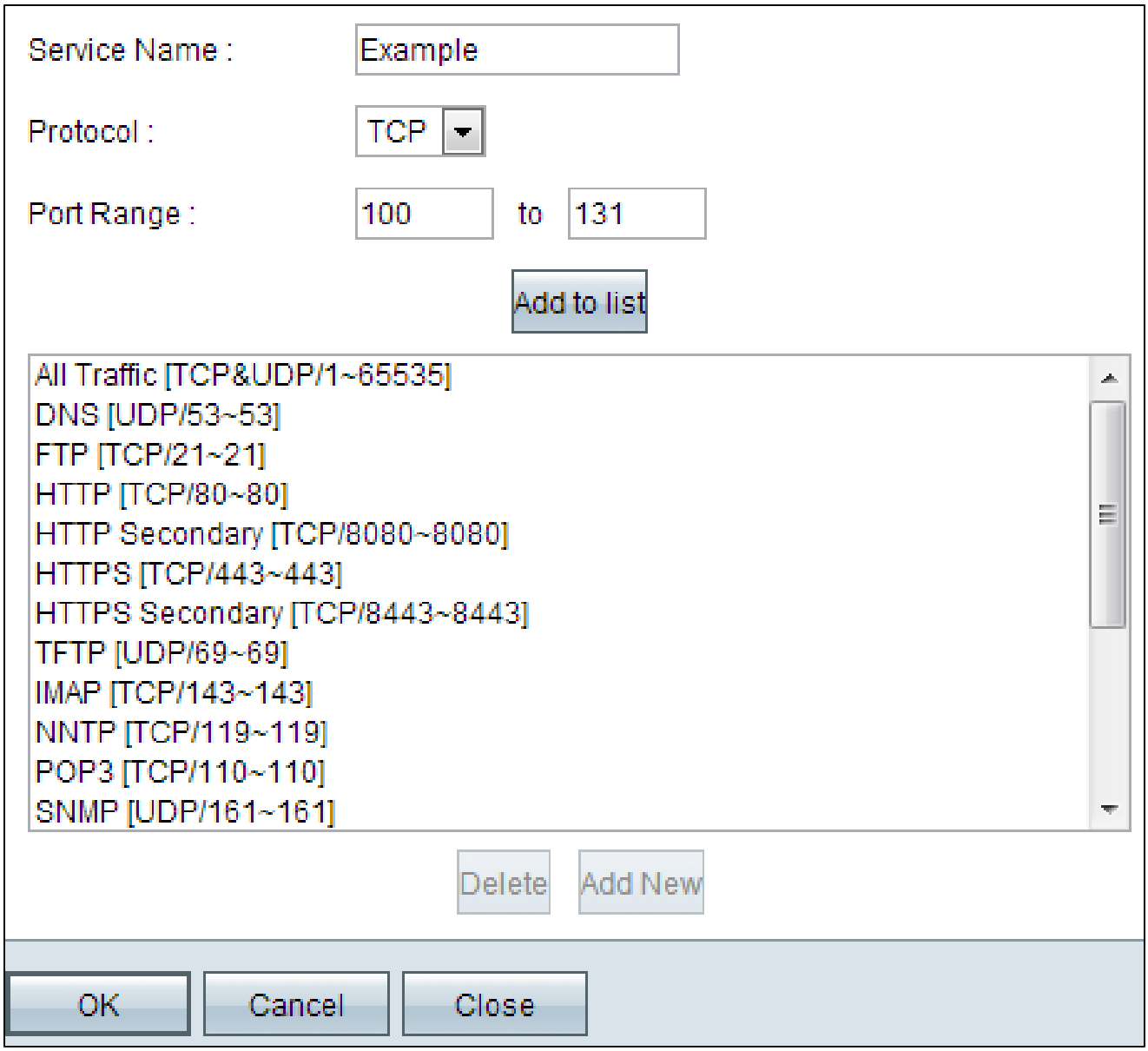


Étape 3. Choisissez l'action appropriée dans la liste déroulante Action qui permettra au trafic de passer si l'option Allow est sélectionnée. Sinon, choisissez Deny pour refuser le trafic.

Étape 4. Sélectionnez le service approprié dans la liste déroulante Service.

Remarque : si le service souhaité est disponible, passez à l'étape 10.

Étape 5. Si le service approprié n'est pas disponible, cliquez sur Service Management et la fenêtre Service Management s'affiche :



Étape 6. Saisissez un nom de service souhaité dans le champ Nom de service.

Étape 7. Sélectionnez un type de protocole approprié dans la liste déroulante Protocole :

· TCP — Transmission Control Protocol est un protocole utilisé par les applications qui nécessitent une livraison garantie.

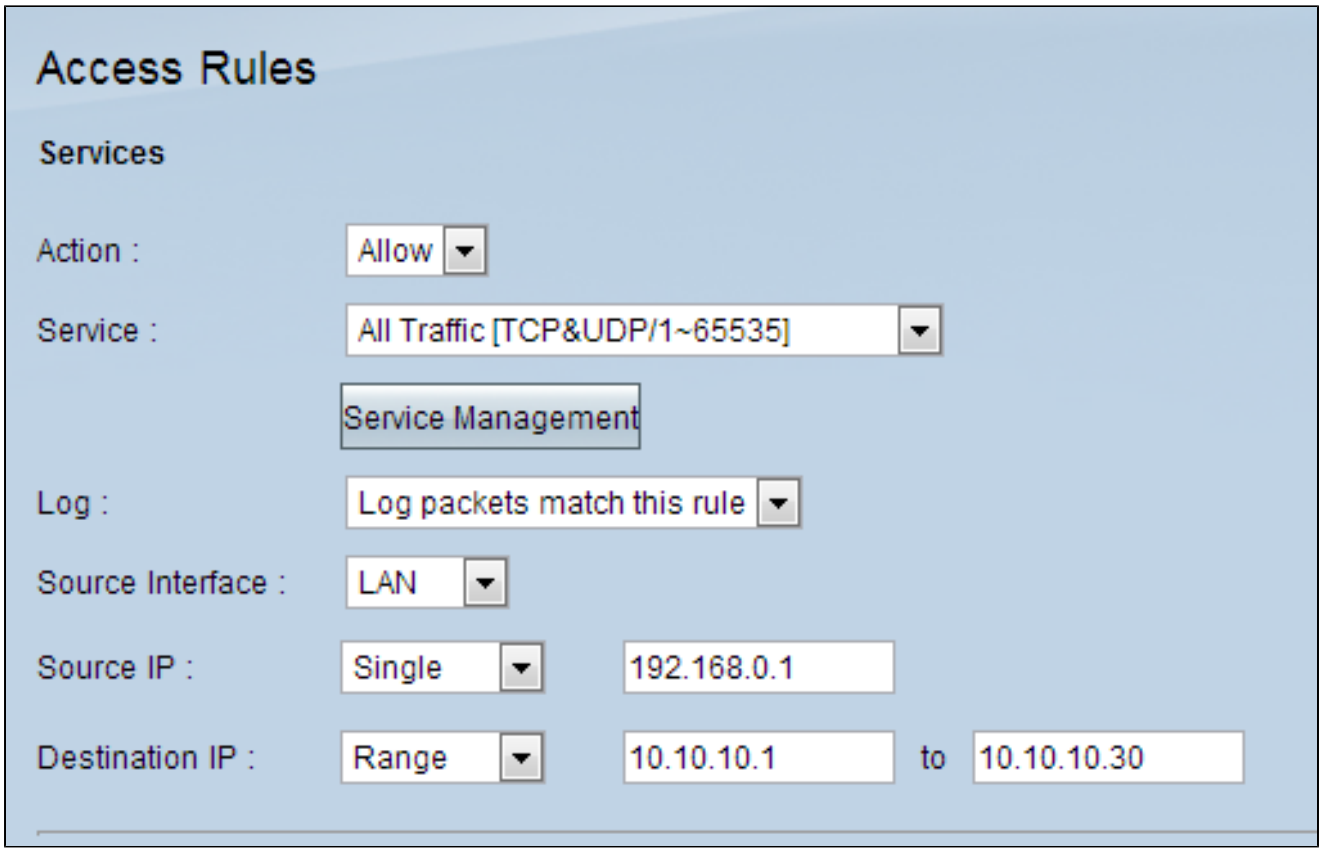
· UDP — User Datagram Protocol utilise des sockets de datagramme pour établir des communications hôte à hôte.

· IPv6 — Dirige le trafic Internet entre les hôtes dans des paquets qui sont routés sur des réseaux spécifiés par des adresses de routage.

Étape 8. Saisissez la plage de ports qui s'appliquera au service dans le champ Port Range.

Étape 9. Cliquez sur Add to List pour ajouter le service à la liste déroulante Service de la page Access Rules.

Étape 10. Cliquez sur OK pour fermer la fenêtre, ce qui ramène l'utilisateur à la page Access Rules.



Étape 11. Choisissez Log packets match this rule pour consigner les paquets entrants correspondant à la règle d'accès dans la liste déroulante Log.

Étape 12. Choisissez une interface dans la liste déroulante Interface source qui est affectée par cette règle. L'interface source est l'interface à partir de laquelle le trafic est initié.

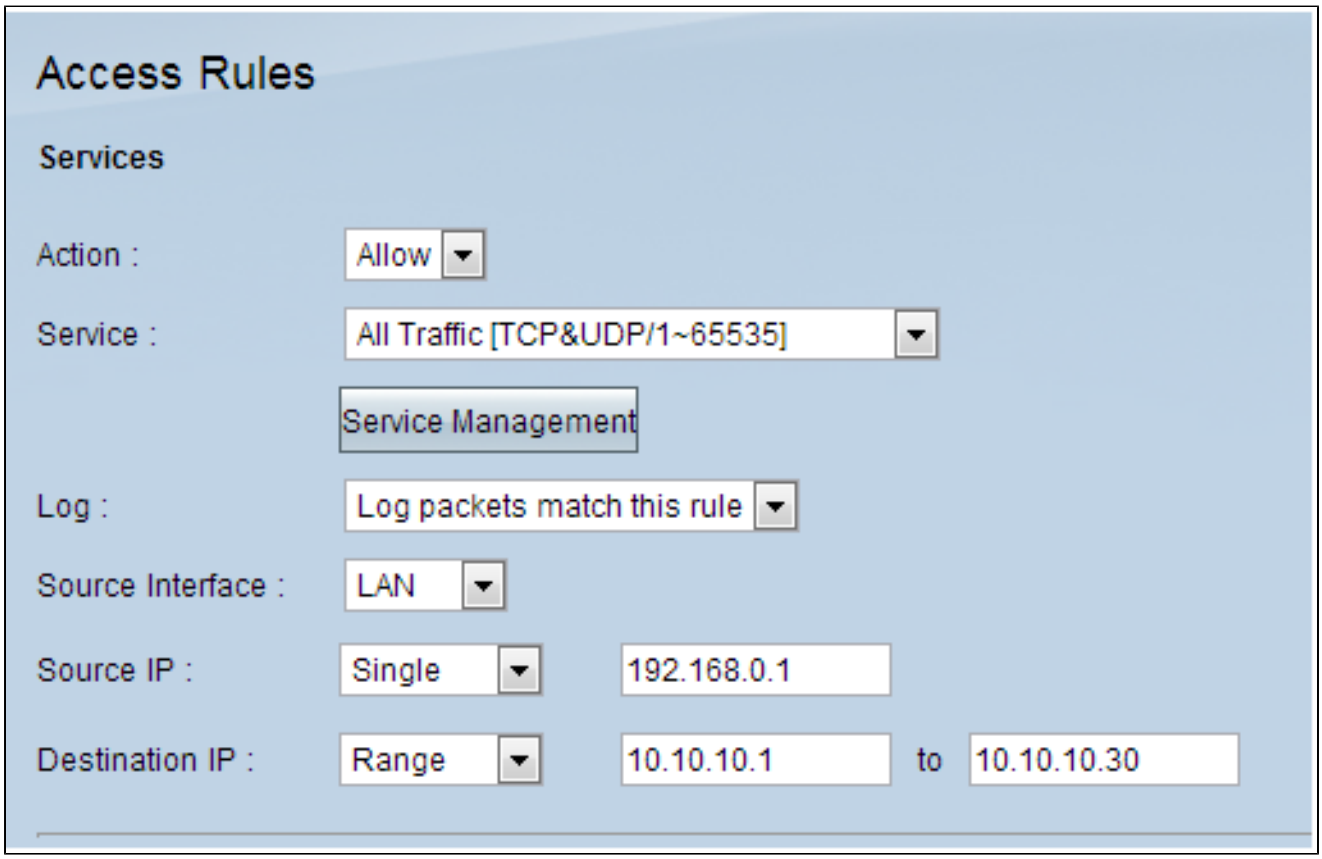
· Réseau local : le port réseau local connecte les ordinateurs à proximité d'un réseau tel qu'un immeuble de bureaux ou une école.

· WAN1 : le port WAN connecte les ordinateurs d'une zone étendue d'un réseau. Il peut s'agir de n'importe quel réseau reliant une région ou même un pays. Il est utilisé par les entreprises et le gouvernement pour se connecter à d'autres sites.

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

· DMZ — Permet au trafic externe d'accéder à un ordinateur sur le réseau sans exposer le réseau local.

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



Étape 13. Choisissez une option pour spécifier l'adresse IP source que le réseau utilisera pour le trafic via l'interface dans la liste déroulante Source IP :

· Any : toute adresse IP sera utilisée pour transférer le trafic. Aucun champ n'est disponible à droite de la liste déroulante.

· Single : une seule adresse IP sera utilisée pour transférer le trafic. Saisissez l'adresse IP souhaitée dans le champ situé à droite de la liste déroulante.

· Range : une plage d'adresses IP sera utilisée pour transférer le trafic. Saisissez la plage d'adresses IP souhaitée dans les champs à droite de la liste déroulante.

Étape 14. Choisissez une option pour spécifier l'adresse IP de destination que le réseau utilisera pour le trafic via l'interface dans la liste déroulante Destination IP :

· Any : toute adresse IP sera utilisée pour transférer le trafic. Aucun champ n'est disponible

à droite de la liste déroulante.

· Single : une seule adresse IP sera utilisée pour transférer le trafic. Saisissez l'adresse IP souhaitée dans le champ situé à droite de la liste déroulante.

· Range : une plage d'adresses IP sera utilisée pour transférer le trafic. Saisissez la plage d'adresses IP souhaitée dans les champs à droite de la liste déroulante.

Étape 15. Cliquez sur Save pour appliquer les paramètres.

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.