Configuration de listes d'accès basées sur IPv4 sur les commutateurs gérés de la gamme 200/300

Objectif

Les listes d'accès sont des règles que vous pouvez appliquer pour autoriser ou refuser un flux de trafic spécifique sur votre réseau, ce qui renforce la sécurité et améliore les performances globales de votre réseau.

L'objectif de ce document est de vous montrer comment configurer des listes d'accès basées sur IPv4 sur les commutateurs gérés de la gamme 200/300.

Périphériques pertinents

· Commutateurs administrables des gammes SF/SG 200 et SF/SG 300

Version du logiciel

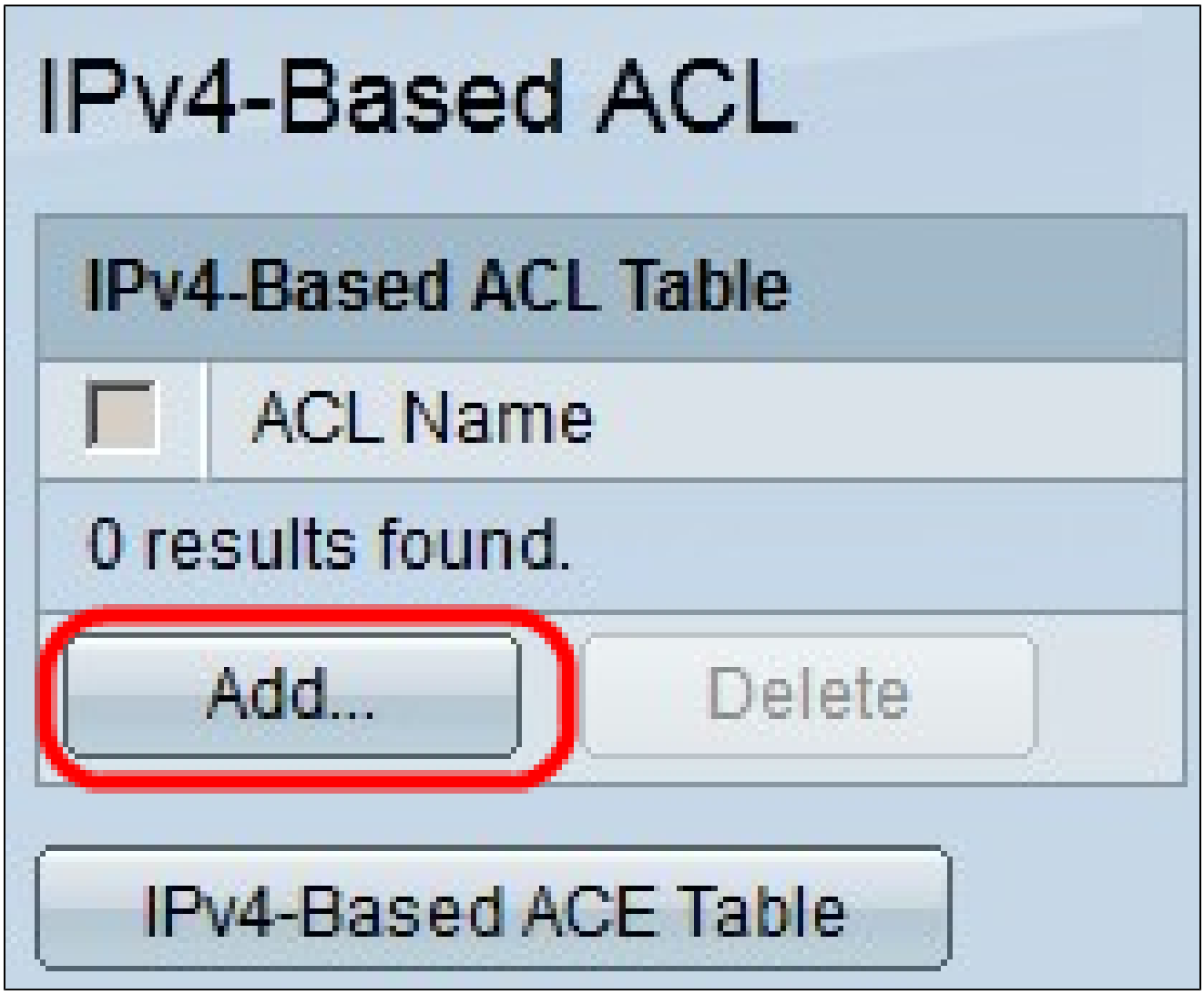
•1.3.0.62

Configuration des listes de contrôle d'accès et des ACE basées sur IPv4

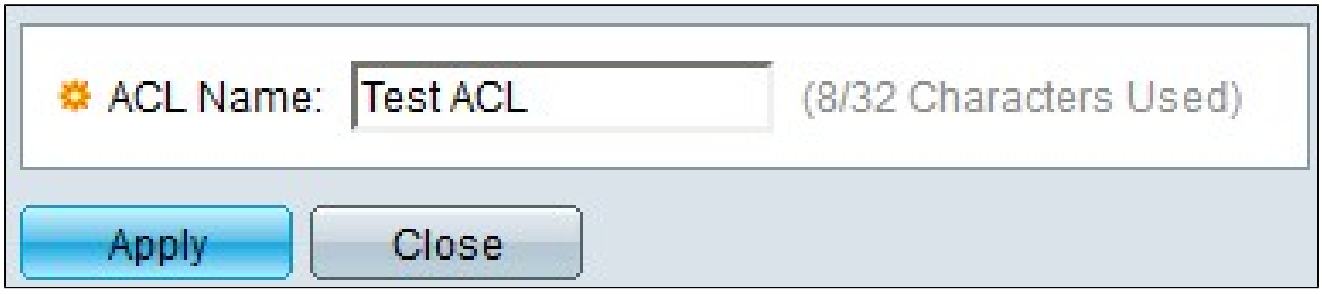
ACL basées sur IPv4

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Access Control > IPv4-Based ACL. La page IPv4-Based ACL s'ouvre.

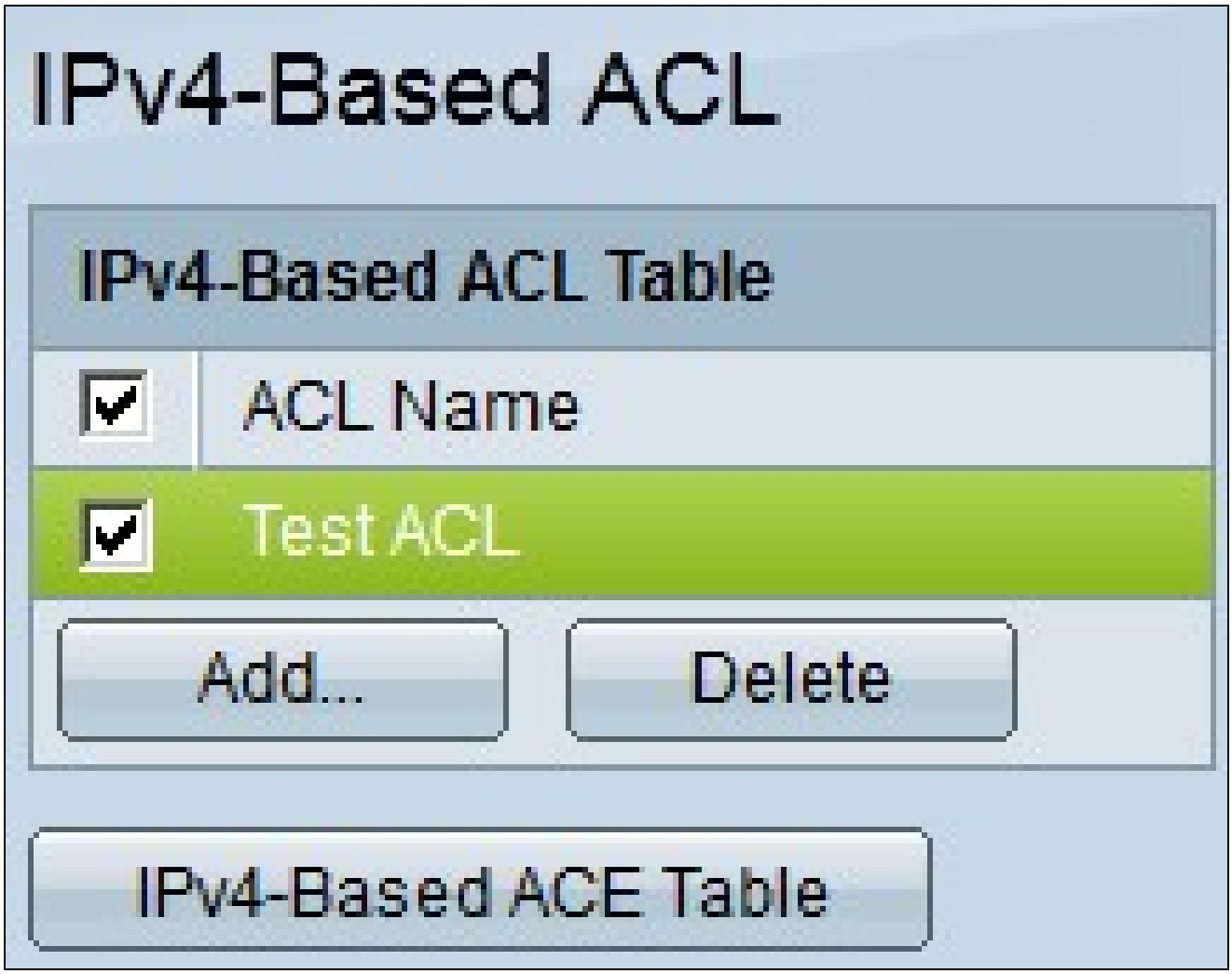
Étape 2. Cliquez sur Add pour ajouter une nouvelle liste d'accès.



Étape 3. Dans le champ ACL Name, saisissez un nom pour la nouvelle liste de contrôle d'accès.



Étape 4. Cliquez sur Apply pour enregistrer la liste d'accès.

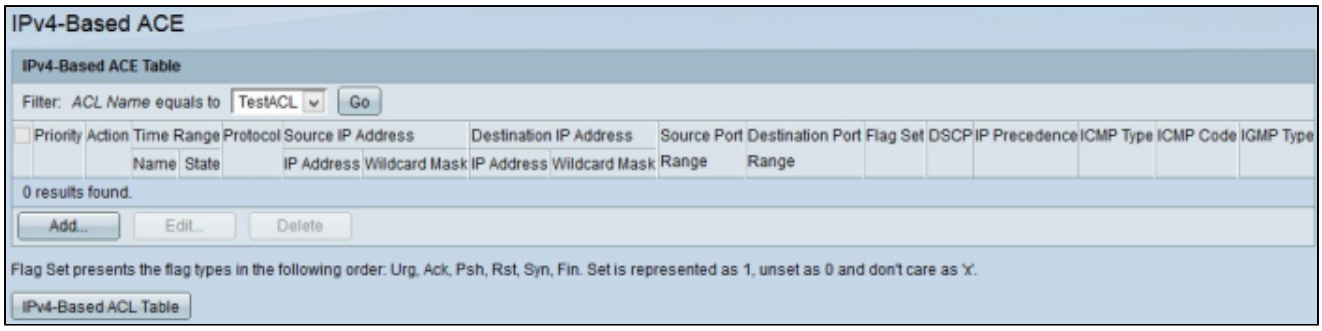


Étape 5. (Facultatif) Pour supprimer une liste d'accès, cochez la case de la liste que vous souhaitez supprimer, puis cliquez sur Supprimer.

ACE basés sur IPv4

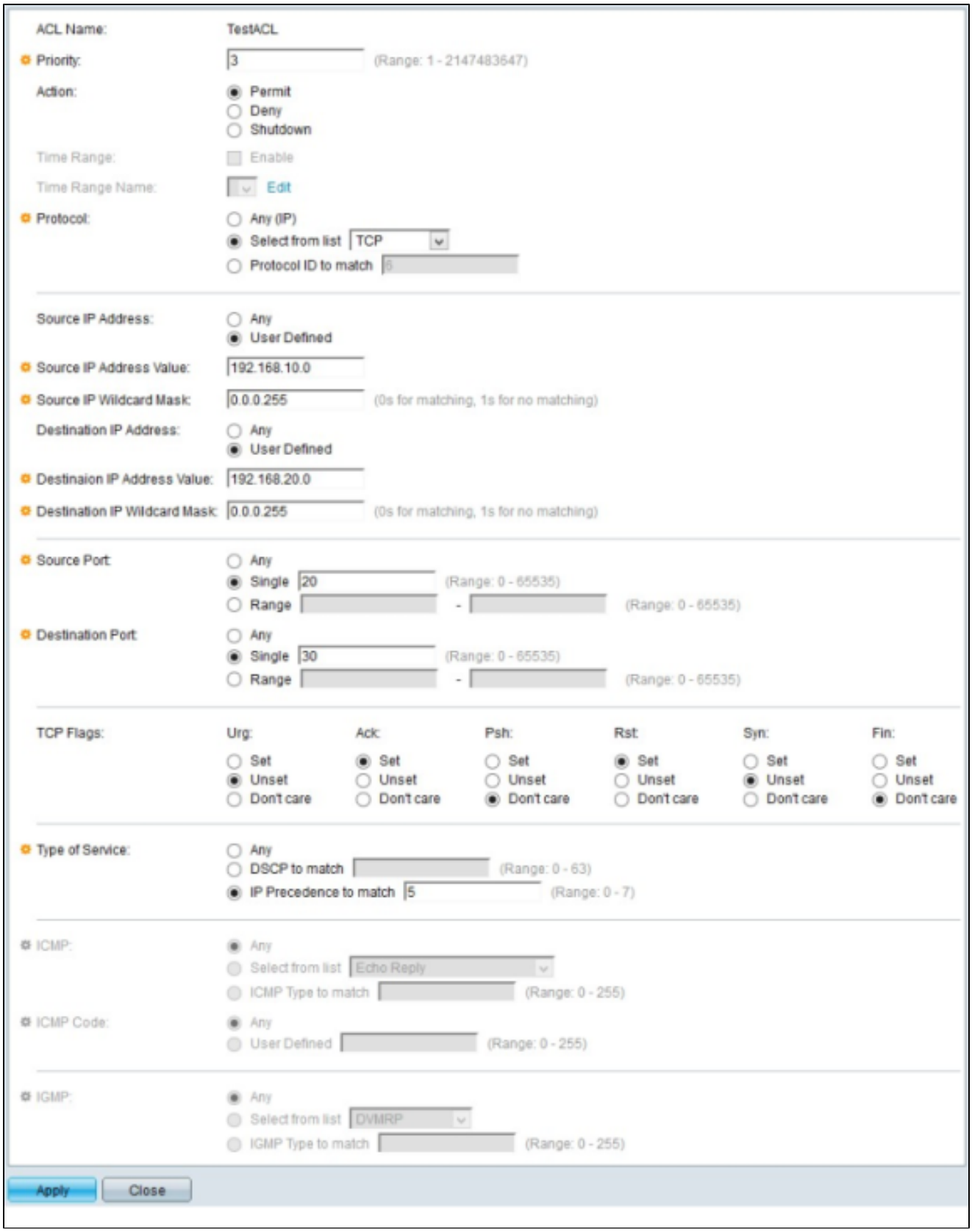
Pour gérer une entrée ACE vers une liste de contrôle d'accès, les étapes suivantes doivent être suivies.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Access Control > IPv4-Based ACE. La page IPv4-Based ACE s'ouvre.



Étape 2. Dans la liste déroulante Filter: ACL Name equal to, sélectionnez la liste d'accès à laquelle vous souhaitez attribuer une règle d'accès.

Étape 3. Cliquez sur Add. La fenêtre Add IP-Based ACE apparaît.



Étape 4. Entrez la priorité de l'ACE dans le champ Priorité. L'ACE ayant la priorité la plus élevée est traitée en premier. La priorité la plus élevée est 1. Sa plage est comprise entre 1 et 2147483647.

Étape 5. Dans le champ Action, cliquez sur la case d'option de l'action que cette règle

d'accès doit exécuter. Les options disponibles sont les suivantes :

· Permit : transfère les paquets filtrés par l'ACE actuel.

· Deny : abandonne les paquets qui sont filtrés par l'ACE actuel.

· Shutdown : supprime les paquets qui sont filtrés par l'ACE actuel et désactive le port d'où les paquets ont été reçus.

Étape 6. Dans le champ Protocol, cliquez sur la case d'option du protocole que vous souhaitez ajouter dans l'ACE. L'ACE est configuré pour tous les protocoles réseau routés afin de filtrer les paquets au fur et à mesure qu'ils traversent un routeur. Les options disponibles sont les suivantes :

· Any : sélectionne l'un des protocoles ACE basés sur IPv4.

· Select from list : sélectionnez le protocole souhaité dans la liste déroulante.

· Protocol ID to match : cette option vous permet d'entrer l'ID de protocole que vous souhaitez utiliser.

Étape 7. Dans le champ Source IP Address, cliquez sur l'une des options disponibles en tant qu'adresse IP source :

· Any : cette option applique la règle d'accès à n'importe quelle adresse IP disponible dans un segment de réseau spécifique.

· Défini par l'utilisateur : cette option vous permet d'entrer une adresse IP spécifique.

- Source IP Address Value : dans ce champ, saisissez l'adresse IP source.

- Source IP Wildcard Mask : dans ce champ, saisissez le masque générique de l'adresse IP source. Le masque générique vous permet de spécifier à quel hôte de l’adresse IP source cette liste d’accès est appliquée.

Étape 8. Dans le champ Destination IP Address, cliquez sur l'une des options disponibles comme adresse IP de destination :

· Any : cette option applique la règle d'accès à n'importe quelle adresse IP disponible dans

un segment de réseau spécifique.

· Défini par l'utilisateur — Cette option vous permet d'entrer une adresse IP spécifique pour appliquer la règle d'accès :

- Destination IP Address Value : dans ce champ, saisissez l'adresse IP de destination.

- Destination IP Wildcard Mask : dans ce champ, saisissez le masque générique de l'adresse IP de destination. Le masque générique vous permet de spécifier à quels hôtes de l'adresse IP de destination cette liste d'accès est appliquée.

Étape 9. Le champ Port source est activé uniquement lorsque vous sélectionnez TCP ou UDP à l'étape 5. Cliquez sur la case d'option de l'une des options disponibles pour choisir le port source :

· Any : cette option accepte n'importe quel port source.

· Single : cette option vous permet d'entrer une seule valeur de port source.

· Range : cette option vous permet d'entrer une plage de ports source disponibles.

Étape 10. Le champ Port de destination est activé uniquement lorsque vous sélectionnez TCP ou UDP à l'étape 5. Cliquez sur la case d'option de l'une des options disponibles pour choisir le port de destination :

· Any : cette option accepte tout port de destination.

· Single : cette option vous permet d'entrer une seule valeur de port de destination.

· Range : cette option vous permet d'entrer une plage de ports de destination disponibles.

Étape 11. Le champ TCP flags n'est activé que si vous sélectionnez TCP à l'étape 5. Cliquez sur l'une des cases d'option pour chaque indicateur afin de choisir l'état que vous souhaitez déclencher la règle d'accès :

· Urg : cet indicateur identifie les données entrantes comme étant urgentes.

· Ack : cet indicateur est utilisé pour accuser réception des paquets.

· Psh — Cet indicateur est utilisé pour s'assurer que les données reçoivent la priorité correcte et sont traitées à l'extrémité émettrice ou réceptrice.

· Rst : cet indicateur est utilisé lorsqu'une connexion reçoit un segment incorrect.

· Syn : cet indicateur est utilisé pour les communications TCP.

· Fin — Cet indicateur est utilisé lorsque la communication ou le transfert de données est terminé.

Étape 12. Dans le champ Type of Service, cliquez sur l'une des cases d'option disponibles pour choisir un type de service pour le paquet IP :

· Tout — Cette option permet de choisir n'importe quel type de service.

· DSCP to match : choisissez cette option pour implémenter le DSCP (Differentiated Service Code Point) en tant que type de service. DSCP est un mécanisme de classification et de gestion du trafic réseau. Saisissez la valeur DSCP que vous souhaitez appliquer à la règle d'accès.

· Priorité IP à mettre en correspondance : ce type de service est utilisé par le réseau actuel pour fournir la qualité de service (QoS) correcte. Saisissez la valeur que vous souhaitez appliquer à la règle d'accès.

Étape 13. Le champ ICMP (Internet Control Message Protocol) est activé uniquement lorsque vous sélectionnez ICMP à l'étape 5. Le protocole ICMP est utilisé pour envoyer des messages d'erreur lorsqu'un service n'est pas disponible ou pour tester la connectivité. Cliquez sur l'une des cases d'option disponibles pour filtrer les types de message ICMP :

· Any : il peut s'agir de n'importe quel message d'erreur ou de requête.

· Select from list : sélectionnez l'un des messages de contrôle autorisés dans la liste déroulante.

· ICMP type to match : cette option vous permet d'entrer le nombre de types ICMP que vous souhaitez filtrer.

Étape 14. Le champ ICMP Code est activé uniquement lorsque vous sélectionnez ICMP à l'étape 5. Les codes ICMP sont utilisés pour fournir des informations plus spécifiques sur les messages de contrôle. Cliquez sur l'une des options disponibles :

· Any : il peut s'agir de n'importe quelle valeur correspondant au message de contrôle.

· Défini par l'utilisateur — Saisissez le code ICMP que vous souhaitez filtrer.

Étape 15. Le champ IGMP (Internet Group Management Protocol) est activé uniquement lorsque vous sélectionnez IGMP à l'étape 5. Le protocole IGMP gère l'appartenance des hôtes aux groupes de multidiffusion IP sur un segment de réseau. Cliquez sur l'une des cases d'option disponibles pour filtrer les types de message IGMP :

· Any — Cette option accepte tous les types de messages IGMP.

· Select from list : choisissez l'une des options disponibles dans la liste déroulante pour filtrer :

- DVMRP - Il utilise une technique d'inondation de chemin inverse, qui envoie une copie d'un paquet reçu par chaque interface, à l'exception de celle à laquelle le paquet est arrivé.

- Host-Query : envoie régulièrement des messages de requête d'hôte généraux sur chaque réseau connecté pour obtenir des informations

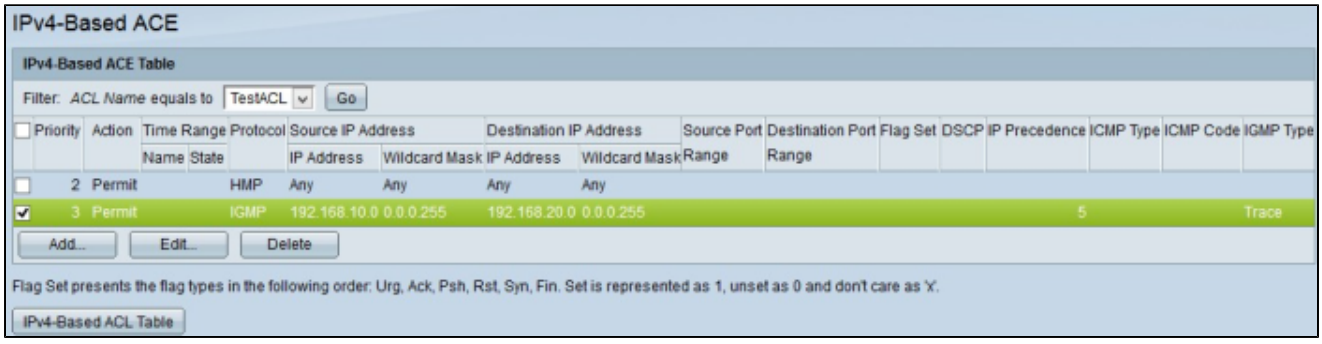
- Host-Reply : répond à la requête .

- PIM - Il est utilisé entre les routeurs de multidiffusion locaux et distants pour diriger le trafic de multidiffusion du serveur de multidiffusion vers de nombreux clients de multidiffusion.

- Trace : fournit des informations pour rejoindre et quitter un groupe de multidiffusion IGMP.

· IGMP type of match : cette option vous permet d'entrer le nombre de types IGMP que vous souhaitez filtrer.

Étape 16. Cliquez sur Apply pour enregistrer votre configuration.



Étape 17. (Facultatif) Pour modifier une règle d’accès actuelle, cochez la case de la règle d’accès que vous souhaitez modifier, puis cliquez sur Modifier.

Étape 18. (Facultatif) Pour supprimer une règle d’accès actuelle, cochez la case de la règle d’accès que vous souhaitez supprimer, puis cliquez sur Supprimer.

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.