Configurer la liste de contrôle d'accès (ACL) et l'entrée de contrôle d'accès (ACE) IPv4 sur un commutateur

Objectif

Une liste de contrôle d’accès (ACL) est une liste de filtres de trafic réseau et d’actions corrélées utilisées pour améliorer la sécurité. Il bloque ou permet aux utilisateurs d'accéder à des ressources spécifiques. Une liste de contrôle d’accès contient les hôtes auxquels l’accès au périphérique réseau est autorisé ou refusé.

La liste de contrôle d'accès IPv4 est une liste d'adresses IPv4 source qui utilisent les informations de couche 3 pour autoriser ou refuser l'accès au trafic. Les listes de contrôle d'accès IPv4 limitent le trafic lié à l'IP en fonction des filtres IP configurés. Un filtre contient les règles permettant de faire correspondre un paquet IP, et si le paquet correspond, la règle stipule également si le paquet doit être autorisé ou refusé.

Une entrée de contrôle d'accès (ACE) contient les critères de règle d'accès réels. Une fois l'ACE créée, elle est appliquée à une liste de contrôle d'accès.

Vous devez utiliser des listes d'accès pour fournir un niveau de sécurité de base pour accéder à votre réseau. Si vous ne configurez pas de listes d'accès sur vos périphériques réseau, tous les paquets passant par le commutateur ou le routeur peuvent être autorisés sur toutes les parties de votre réseau.

Cet article explique comment configurer la liste de contrôle d'accès et l'ACE IPv4 sur votre commutateur géré.

Périphériques pertinents

- Gamme Sx350
- Gamme SG350X
- Série Sx500
- Gamme Sx550X

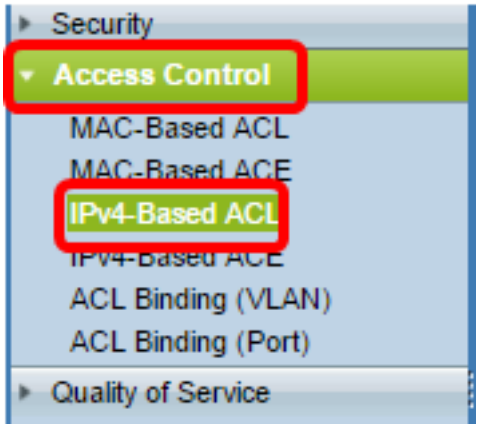
Version du logiciel

- 1.4.5.02 - Série Sx500
- 2.2.5.68 - Série Sx350, Série SG350X, Série Sx550X

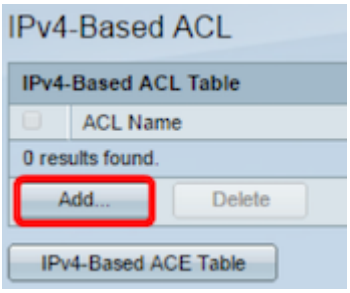
Configuration de la liste de contrôle d'accès et de l'ACE IPv4

Configurer une liste de contrôle d'accès IPv4

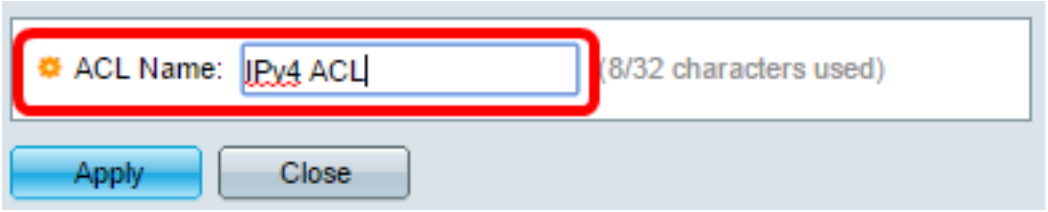
Étape 1. Connectez-vous à l'utilitaire Web, puis accédez à **Access Control > IPv4-Based ACL**.



Étape 2. Cliquez sur le bouton **Add.**

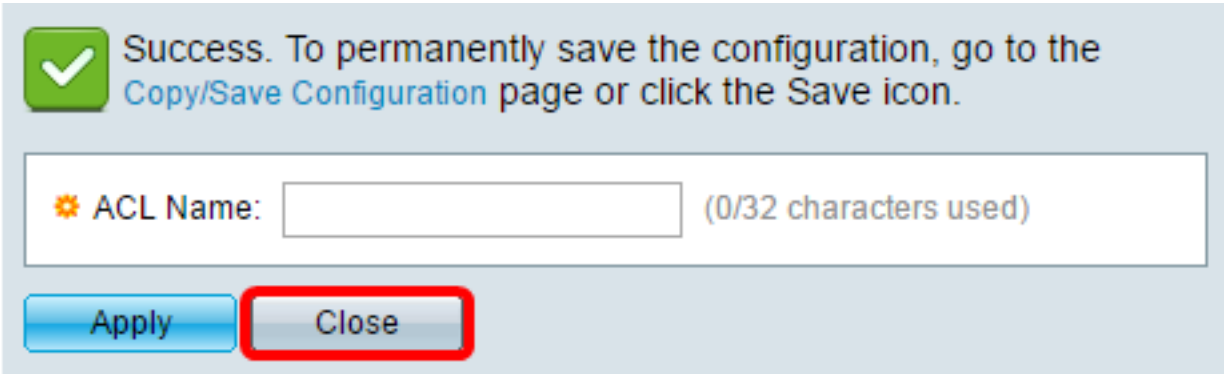


Étape 3. Entrez le nom de la nouvelle liste de contrôle d'accès dans le champ *Nom de la liste de contrôle d'accès*.



Note: Dans cet exemple, la liste de contrôle d'accès IPv4 est utilisée.

Étape 4. Cliquez sur **Appliquer** puis sur **Fermer**.



Étape 5. (Facultatif) Cliquez sur **Enregistrer** pour enregistrer les paramètres dans le fichier de configuration initiale.

Vous devez maintenant avoir configuré une liste de contrôle d'accès IPv4 sur votre commutateur.

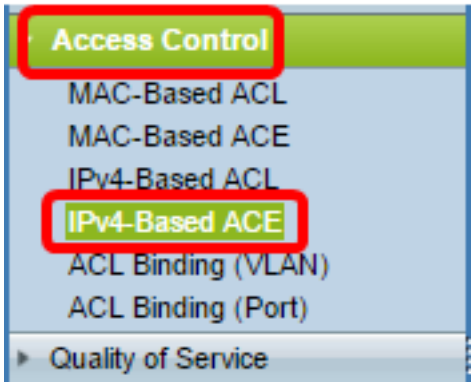
Configuration de l'ACE IPv4

Lorsqu'un paquet est reçu sur un port, le commutateur traite le paquet via la première liste de contrôle d'accès. Si le paquet correspond à un filtre ACE de la première liste de contrôle d'accès, l'action ACE a lieu. Si le paquet ne correspond à aucun des filtres ACE, la liste de contrôle d'accès suivante est traitée. Si aucune correspondance n'est trouvée avec une ACE dans toutes les listes de contrôle d'accès pertinentes, le paquet est abandonné par défaut.

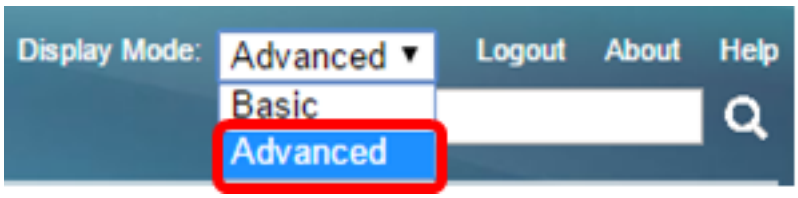
Dans ce scénario, une ACE sera créée pour refuser le trafic qui est envoyé d'une adresse IPv4 source définie par l'utilisateur à n'importe quelle adresse de destination.

Note: Cette action par défaut peut être évitée par la création d'une ACE de faible priorité qui autorise tout le trafic.

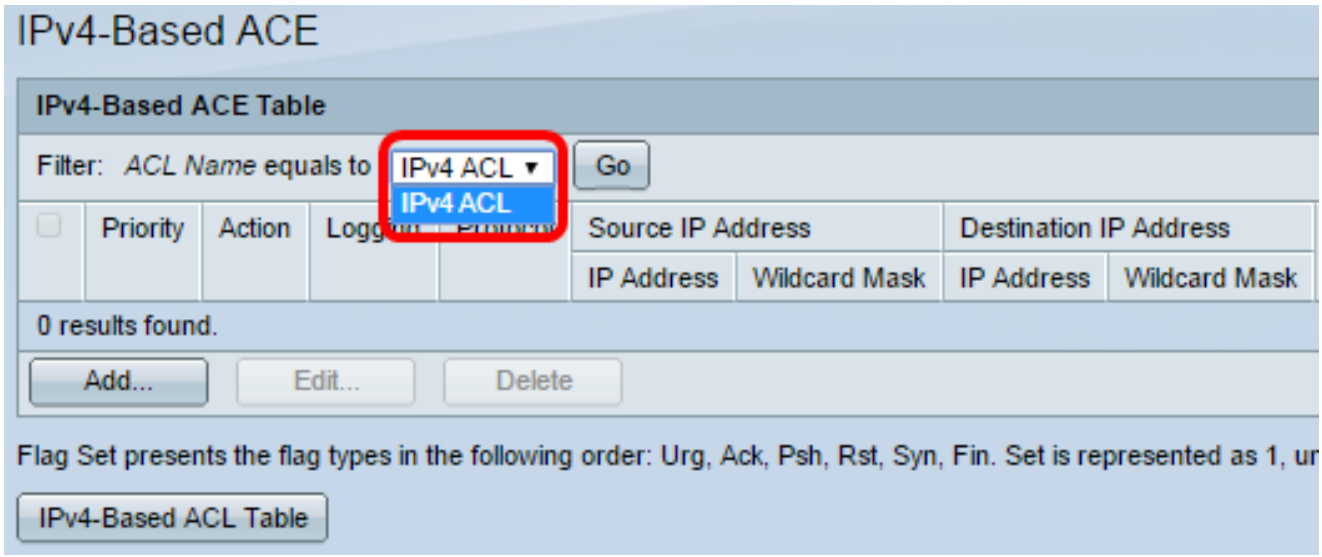
Étape 1. Dans l'utilitaire Web, accédez à **Access Control > IPv4-Based ACE**.



Important : Pour utiliser pleinement les fonctions et fonctions disponibles du commutateur, passez en mode Avancé en sélectionnant **Avancé** dans la liste déroulante Mode Affichage dans le coin supérieur droit de la page.



Étape 2. Choisissez une liste de contrôle d'accès dans la liste déroulante Nom de la liste de contrôle d'accès, puis cliquez sur **Go**.

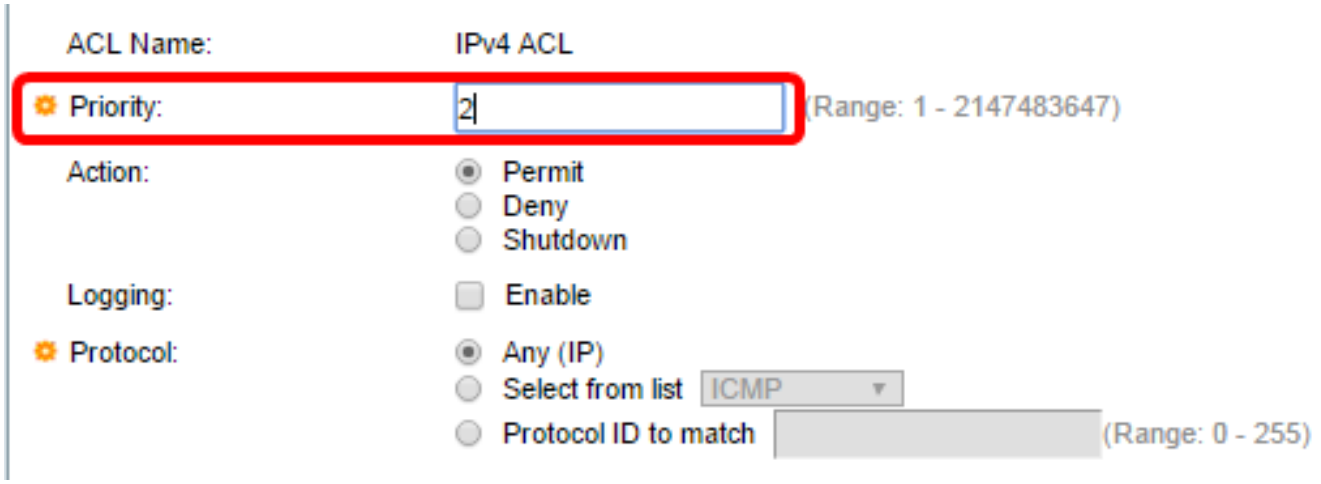


Note: Les ACE déjà configurés pour la liste de contrôle d'accès s'affichent dans le tableau.

Étape 3. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle à la liste de contrôle d'accès.

Note: Le champ *Nom de la liste de contrôle d'accès* affiche le nom de la liste de contrôle d'accès.

Étape 4. Entrez la valeur de priorité de l'ACE dans le champ *Priorité*. Les ACE ayant une valeur de priorité supérieure sont traités en premier. La valeur 1 est la priorité la plus élevée. Il a une plage de 1 à 2147483647.



Note: Dans cet exemple, 2 est utilisé.

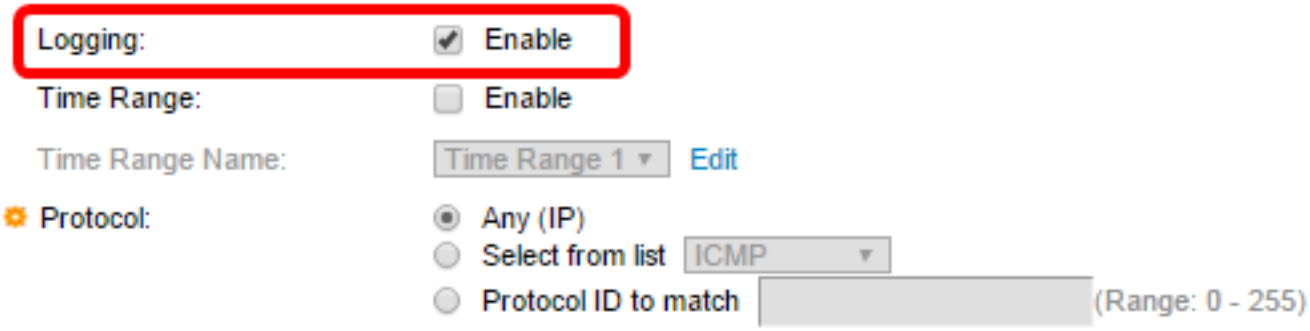
Étape 5. Sélectionnez la case d'option correspondant à l'action souhaitée qui est effectuée lorsqu'une trame répond aux critères requis de l'ACE.

Note: Dans cet exemple, Permit est sélectionné.

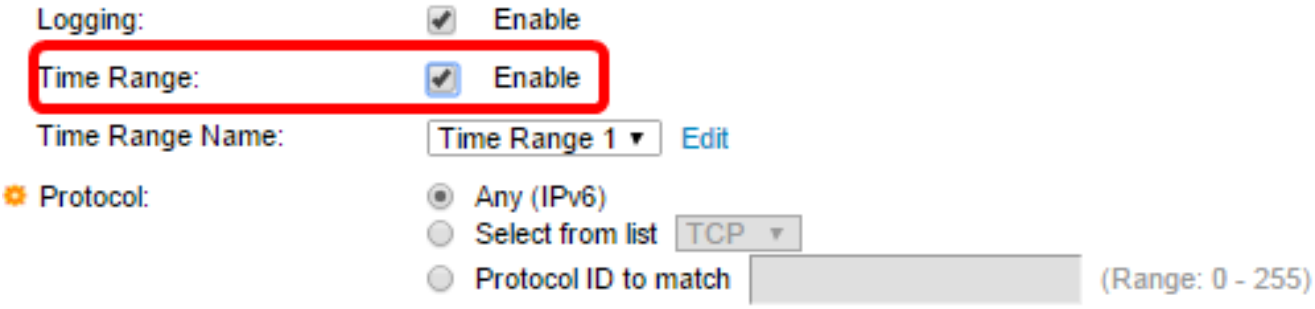
- Permit : le commutateur transfère les paquets qui répondent aux critères requis de l'ACE.
- Deny : le commutateur abandonne les paquets qui répondent aux critères requis de l'ACE.
- Arrêt : le commutateur abandonne les paquets qui ne répondent pas aux critères requis de l'ACE et désactive le port où les paquets ont été reçus.

Note: Les ports désactivés peuvent être réactivés sur la page Port Settings.

Étape 6. (Facultatif) Cochez la case **Activer la** journalisation pour activer la journalisation des flux ACL qui correspondent à la règle ACL.

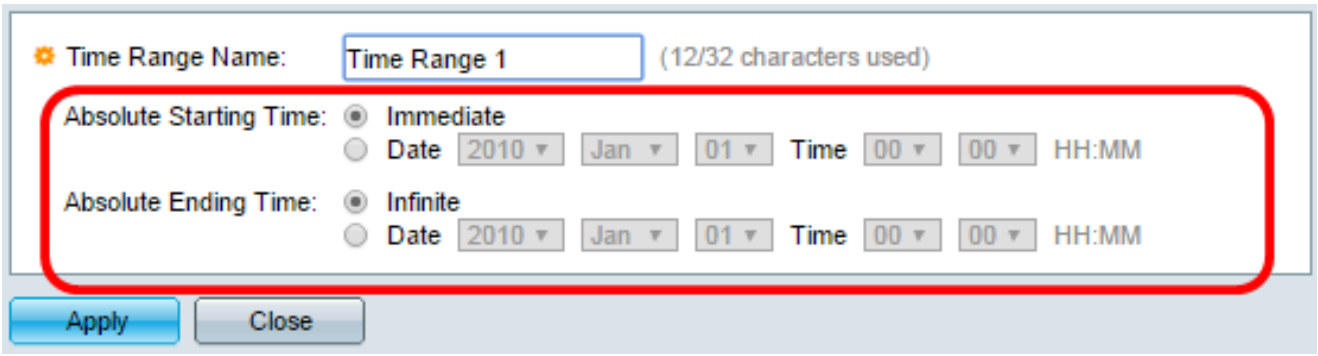


Étape 7. (Facultatif) Cochez la case **Activer** la plage de temps pour autoriser la configuration d'une plage de temps à l'ACE. Les plages de temps sont utilisées pour limiter la durée de validité d'une ACE.

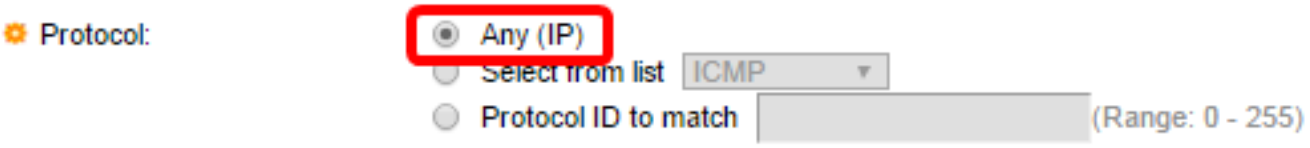


Étape 8. (Facultatif) Dans la liste déroulante Nom de la plage de temps, sélectionnez une plage de temps à appliquer à l'ACE.

Note: Vous pouvez cliquer sur **Modifier** pour naviguer et créer une plage de temps sur la page Plage de temps.



Étape 9. Sélectionnez un type de protocole dans la zone Protocole. L'ACE sera créé en fonction d'un protocole ou d'un ID de protocole spécifique.

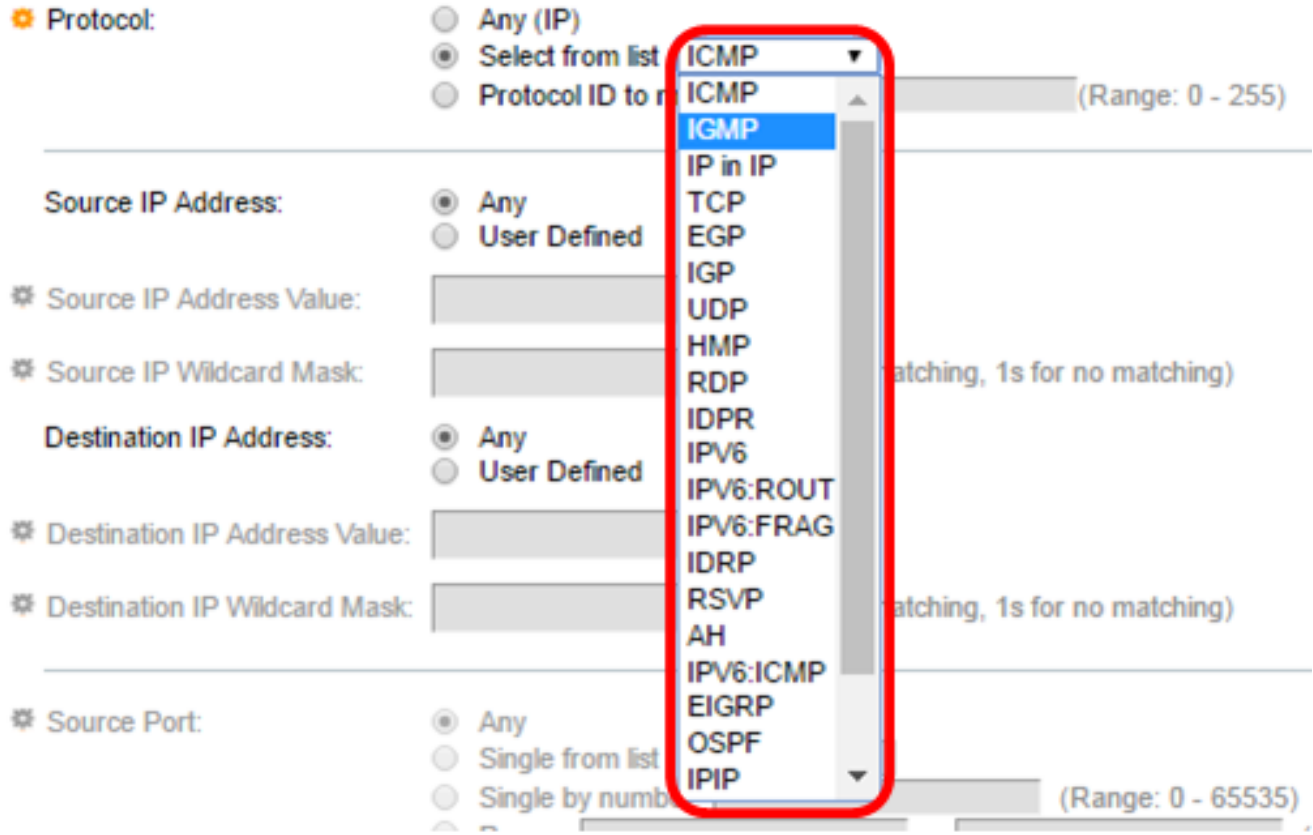


Les options sont les suivantes :

- Any (IP) : cette option configure l'ACE pour accepter tous les protocoles IP.
- Sélectionner dans la liste — Cette option vous permet de choisir un protocole dans une liste déroulante. Si vous préférez cette option, passez à l'étape 10.
- Protocol ID to match : cette option vous permet d'entrer un ID de protocole. Si vous préférez cette option, passez à l'étape 11.

Note: Dans cet exemple, Any (IP) est sélectionné.

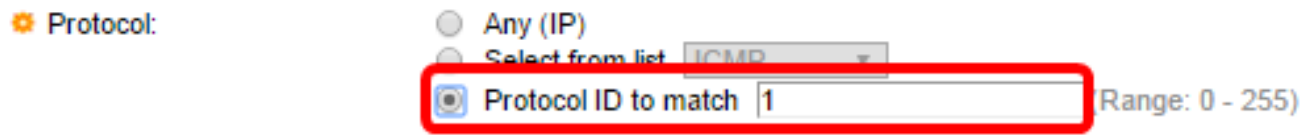
Étape 10. (Facultatif) Si vous avez sélectionné Sélectionner dans la liste de l'étape 9, sélectionnez un protocole dans la liste déroulante.



Les options sont les suivantes :

- ICMP — Protocole de message de contrôle Internet
- IP in IP - IP in IP encapsulation
- TCP : protocole de contrôle de transmission
- EGP - Protocole de passerelle externe
- IGP - Interior Gateway Protocol
- UDP - Protocole de datagramme utilisateur
- HMP - Host Mapping Protocol
- RDP - Protocole de datagramme fiable
- IDPR — Routage de stratégie interdomaine
- IPV6 - Tunneling IPv6 sur IPv4
- IPV6:ROUT — Correspond aux paquets appartenant à la route IPv6 sur IPv4 via une passerelle
- IPV6:FRAG — Correspond aux paquets appartenant à l'en-tête de fragment IPv6 sur IPv4
- IDRP — protocole de routage interdomaine IS-IS
- RSVP — Protocole ReSerVation
- AH — En-tête d'authentification
- IPV6:ICMP — ICMP pour IPv6
- EIGRP - Enhanced Interior Gateway Routing Protocol
- OSPF - Ouvrir le chemin le plus court d'abord
- IPIP - IP dans IP
- PIM — Multidiffusion indépendante du protocole
- L2TP : protocole de tunnellisation de couche 2

Étape 11. (Facultatif) Si vous avez choisi l'ID de protocole à faire correspondre à l'étape 9, saisissez l'ID de protocole dans le champ *ID de protocole à faire correspondre*.



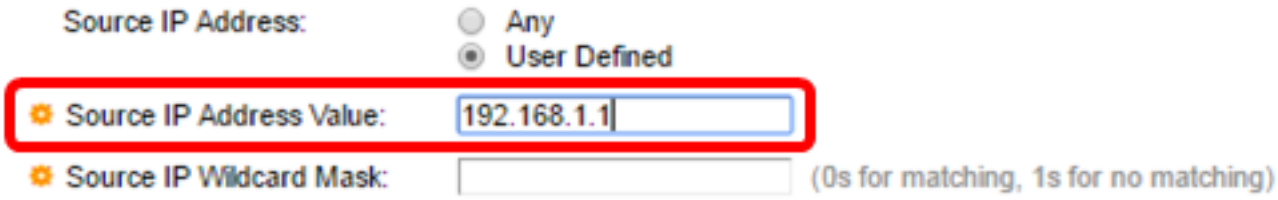
Étape 12. Cliquez sur la case d'option qui correspond aux critères souhaités de l'ACE dans la zone Adresse IP source.

Les options sont les suivantes :

- Any : toutes les adresses IPv4 source s'appliquent à l'ACE.
- User Defined : saisissez une adresse IP et un masque générique IP qui doivent être appliqués à l'ACE dans les champs *Source IP Address Value* et *Source IP Wildcard Mask*. Les masques génériques sont utilisés pour définir une plage d'adresses IP.

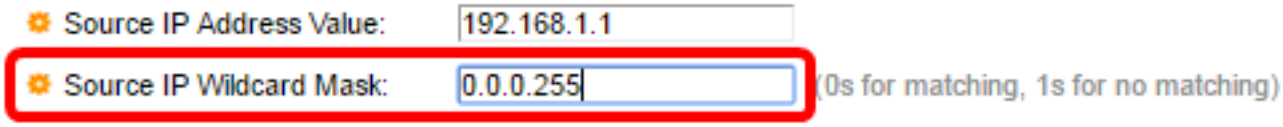
Note: Dans cet exemple, User Defined est sélectionné. Si vous avez sélectionné Any (Tous), passez à l'étape 15.

Étape 13. Entrez l'adresse IP source dans le champ *Valeur de l'adresse IP source*.



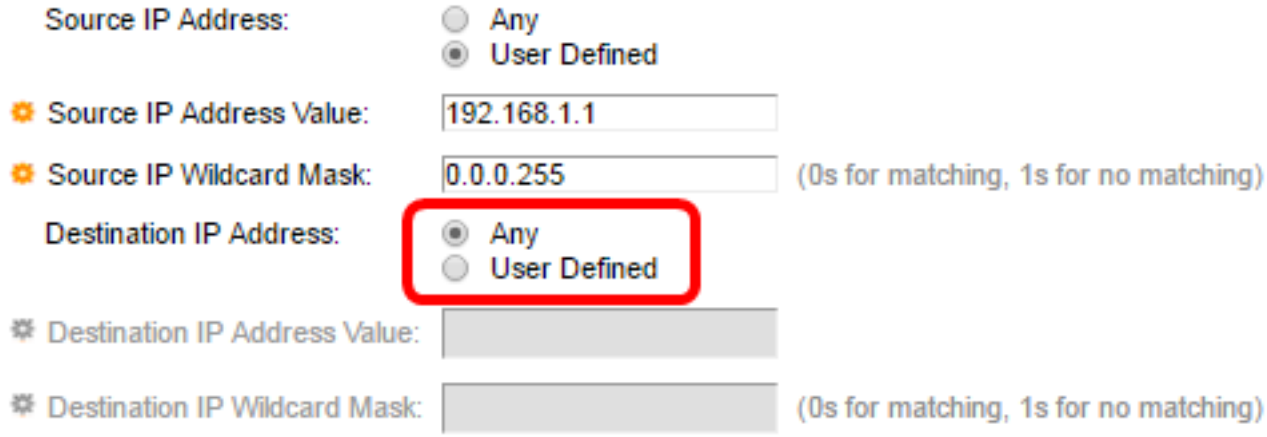
Note: Dans cet exemple, 192.168.1.1 est utilisé.

Étape 14. Entrez le masque générique source dans le champ *Masque générique IP source*.



Note: Dans cet exemple, 0.0.0.255 est utilisé.

Étape 15. Cliquez sur la case d'option qui correspond aux critères souhaités de l'ACE dans la zone Adresse IP de destination.

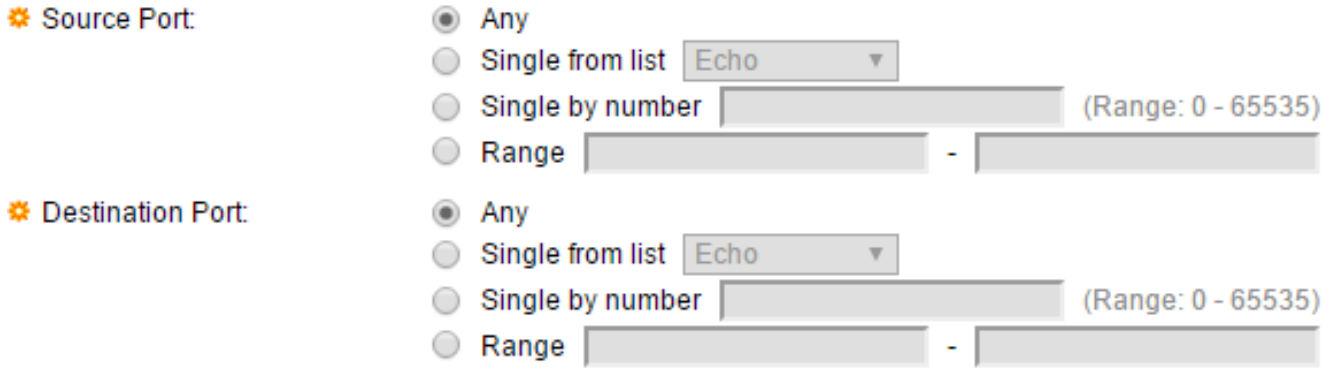


Les options sont les suivantes :

- Any : toutes les adresses IPv4 de destination s'appliquent à l'ACE.
- User Defined : saisissez une adresse IP et un masque générique IP qui doivent être appliqués à l'ACE dans les champs *Destination IP Address Value* et *Destination IP Wildcard Mask*. Les masques génériques sont utilisés pour définir une plage d'adresses IP.

Note: Dans cet exemple, Any est sélectionné. Si vous choisissez cette option, l'ACE à créer autorisera le trafic ACE provenant de l'adresse IPv4 spécifiée vers n'importe quelle destination.

Étape 16. (Facultatif) Cliquez sur une case d'option dans la zone Port source. La valeur par défaut est Any.



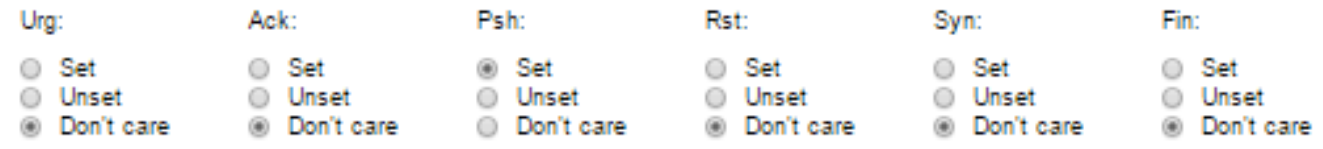
- Any : fait correspondre tous les ports source.
- Single from list : vous pouvez choisir un seul port source TCP/UDP auquel les paquets sont mis en correspondance. Ce champ est actif uniquement si 800/6-TCP ou 800/17-UDP est sélectionné dans le menu déroulant Sélectionner dans la liste.
- Single by number : vous pouvez choisir un seul port source TCP/UDP auquel les paquets sont associés. Ce champ est actif uniquement si 800/6-TCP ou 800/17-UDP est sélectionné dans le menu déroulant Sélectionner dans la liste.
- Range : vous pouvez choisir une plage de ports sources TCP/UDP auxquels le paquet correspond. Il existe huit plages de ports différentes qui peuvent être configurées (partagées entre les ports source et de destination). Les protocoles TCP et UDP ont chacun huit plages de ports.

Étape 17. (Facultatif) Cliquez sur une case d'option dans la zone Port de destination. La valeur par défaut est Any.

- Any — Correspondance avec tous les ports source
- Single from list : vous pouvez choisir un seul port source TCP/UDP auquel les paquets sont mis en correspondance. Ce champ est actif uniquement si 800/6-TCP ou 800/17-UDP est sélectionné dans le menu déroulant Sélectionner dans la liste.
- Single by number : vous pouvez choisir un seul port source TCP/UDP auquel les paquets sont associés. Ce champ est actif uniquement si 800/6-TCP ou 800/17-UDP est sélectionné dans le menu déroulant Sélectionner dans la liste.
- Range : vous pouvez choisir une plage de ports sources TCP/UDP auxquels le paquet correspond. Il existe huit plages de ports différentes qui peuvent être configurées (partagées entre les ports source et de destination). Les protocoles TCP et UDP ont chacun huit plages de ports.

Étape 18. (Facultatif) Dans la zone Indicateurs TCP, sélectionnez un ou plusieurs indicateurs TCP avec lesquels filtrer les paquets. Les paquets filtrés sont transférés ou abandonnés. Le filtrage des paquets par des indicateurs TCP augmente le contrôle des paquets, ce qui augmente la sécurité du réseau.

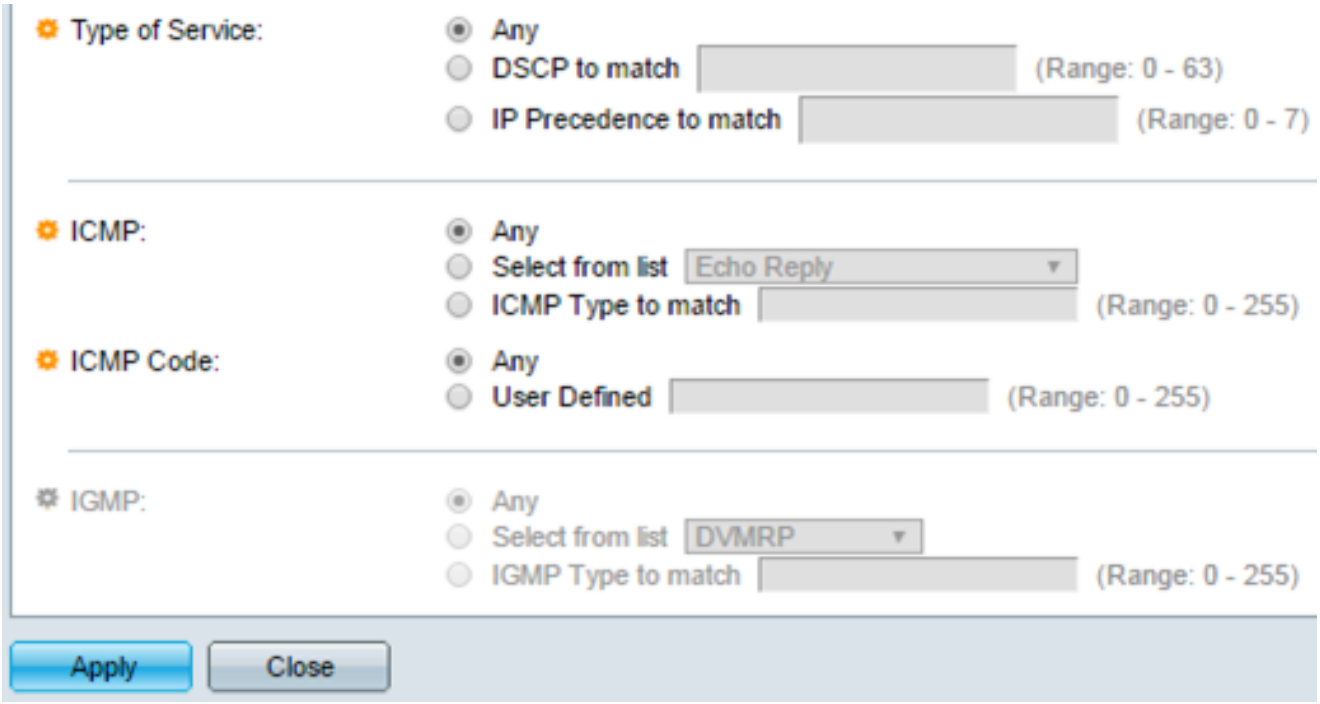
- Set : fait correspondre si l'indicateur est défini.
- Unset : correspond si l'indicateur n'est pas défini.
- Ne vous en souciez pas : ignorez l'indicateur TCP.



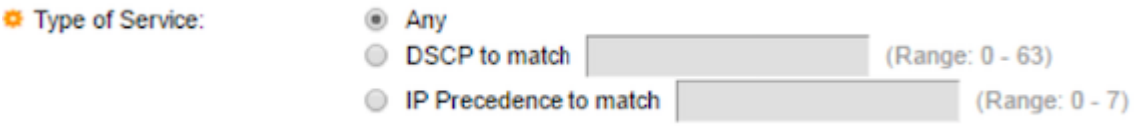
Les indicateurs TCP sont les suivants :

- Urg : cet indicateur est utilisé pour identifier les données entrantes comme 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 (qu'elles méritent) et qu'elles sont traitées à l'extrémité d'envoi ou de réception.
- Rst : cet indicateur est utilisé lorsqu'un segment arrive qui n'est pas destiné à la connexion actuelle.
- 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 19. (Facultatif) Cliquez sur le type de service du paquet IP dans la zone Type de service.



Les options sont les suivantes :



- Any : il peut s'agir de n'importe quel type de service pour la congestion du trafic.
- DSCP to Match — DSCP est un mécanisme de classification et de gestion du trafic réseau. Six bits (0-63) permettent de sélectionner le comportement par saut d'un paquet au niveau de chaque noeud.
- Priorité IP à respecter : la priorité IP est un modèle de type de service (TOS) que le réseau utilise pour fournir les engagements de qualité de service (QoS) appropriés. Ce modèle utilise les trois bits les plus significatifs de l'octet de type de service dans l'en-tête IP, comme décrit dans les documents RFC 791 et RFC 1349. Le mot clé avec la valeur de préférence IP est le suivant :

  - 0 — pour la routine

- 1 — par priorité

- 2 — pour immédiat

- 3 — pour la mémoire flash

- 4 — pour le remplacement de mémoire flash

- 5 - pour les

- 6 — pour Internet

- 7 — pour le réseau

Étape 20. (Facultatif) Si le protocole IP de la liste de contrôle d'accès est ICMP, cliquez sur le type de message ICMP utilisé à des fins de filtrage. Choisissez le type de message par nom ou saisissez le numéro du type de message :

- Any : tous les types de message sont acceptés.
- Sélectionner dans la liste — Vous pouvez choisir le type de message par nom.
- ICMP Type to match : nombre de types de message à utiliser à des fins de filtrage. Il a une plage de 0 à 255.

Étape 21. (Facultatif) Les messages ICMP peuvent avoir un champ de code qui indique comment gérer le message. Cliquez sur l'une des options suivantes pour configurer le filtrage de ce code :

- Any : acceptez tous les codes.
- Défini par l'utilisateur : vous pouvez entrer un code ICMP à des fins de filtrage. Il a une plage de 0 à 255.

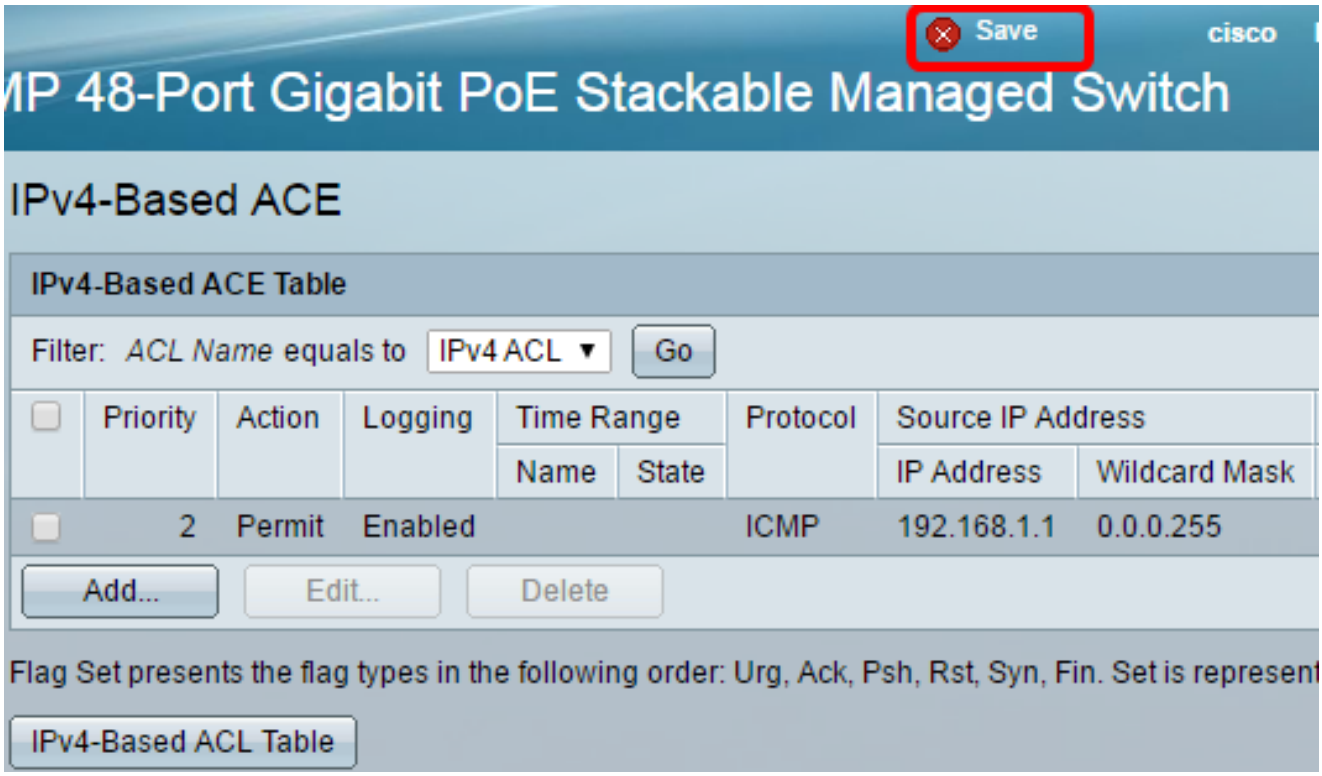
Étape 22. (Facultatif) Si la liste de contrôle d'accès est basée sur IGMP, cliquez sur le type de message IGMP à utiliser à des fins de filtrage. Choisissez le type de message par nom ou saisissez le numéro du type de message :

- Any : tous les types de message sont acceptés.
- Sélectionner dans la liste — Vous pouvez choisir l'une des options de la liste déroulante :
- DVMRP : utilise une technique d'inondation de chemin inverse, qui envoie une copie d'un paquet reçu par l'intermédiaire de chaque interface, à l'exception de celle à laquelle le paquet est arrivé.
- Host-Query : envoie périodiquement des messages de requête hôte généraux sur chaque réseau connecté pour obtenir des informations.
- Host-Reply : répond à la requête.
- PIM : le protocole PIM (Protocol Independent Multicast) 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 sur la jointure et la sortie des groupes de multidiffusion IGMP.
- IGMP Type to match : nombre de types de message à utiliser à des fins de filtrage. Il a une plage de 0 à 255.

Étape 23. Cliquez sur **Appliquer**, puis sur **Fermer**. L'ACE est créée et associée au nom de la

liste de contrôle d'accès.

Étape 24. Cliquez sur **Save** pour enregistrer les paramètres dans le fichier de configuration initiale.



Vous devez maintenant avoir configuré un ACE IPv4 sur votre commutateur.