Configurer la liste de contrôle d'accès (ACL) et l'entrée de contrôle d'accès (ACE) IPv6 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 fonctionnalité de liste de contrôle d'accès classique dans IPv6 est similaire aux listes de contrôle d'accès dans IPv4. Les listes de contrôle d’accès déterminent le trafic à bloquer et le trafic à transmettre sur les interfaces du commutateur. Les listes de contrôle d’accès permettent le filtrage en fonction des adresses source et de destination, entrantes et sortantes vers des interfaces spécifiques. Chaque liste de contrôle d’accès comporte une instruction de refus implicite à la fin. Les règles des listes de contrôle d'accès sont configurées dans les entrées de contrôle d'accès (ACE).

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 IPv6 sur un commutateur.

Périphériques pertinents

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

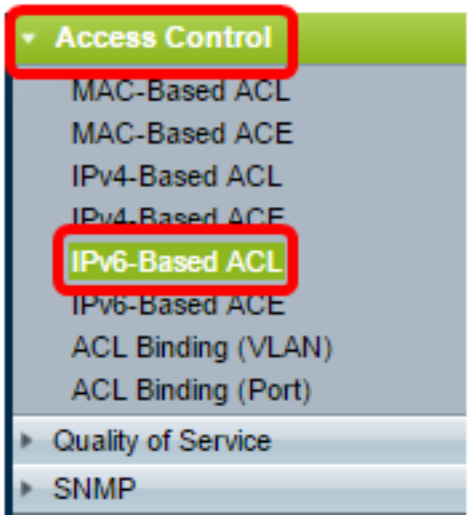
Version du logiciel

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

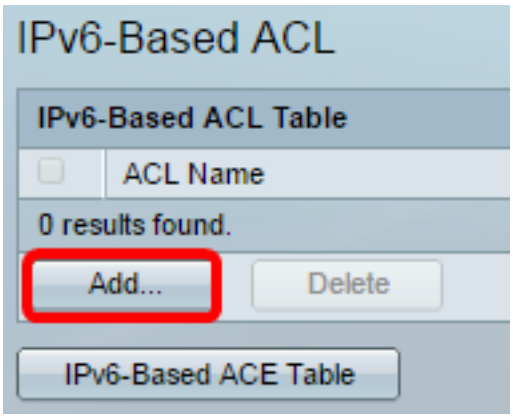
Configuration de la liste de contrôle d'accès et de l'ACE IPv6

Configurer une liste de contrôle d'accès IPv6

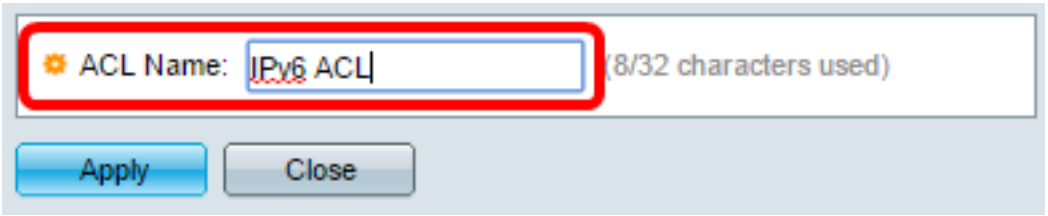
Étape 1. Connectez-vous à l'utilitaire Web, puis accédez à **Access Control > IPv6-Based ACL**.



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

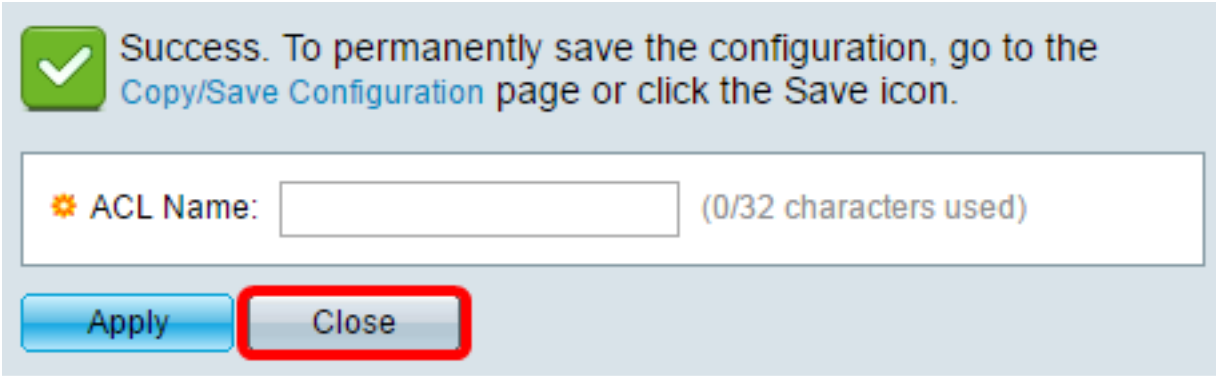


Étape 3. Entrez le nom de la nouvelle liste de contrôle d'accès dans le champ *Nom de la liste de contrôle d'accès*.



Note: Dans cet exemple, la liste de contrôle d'accès IPv6 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 IPv6 sur votre commutateur.

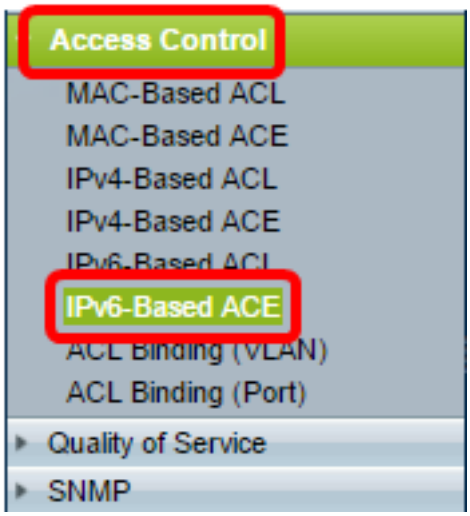
Configuration de l'ACE IPv6

Lorsqu'un paquet est reçu sur un port, le commutateur traite la trame 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.

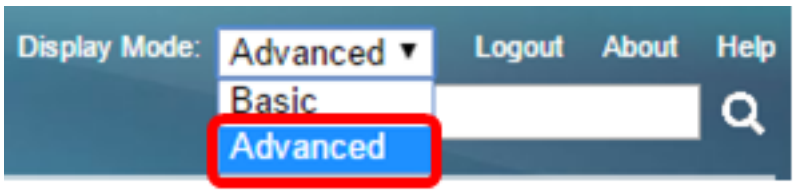
Dans ce scénario, une ACE sera créée pour refuser le trafic envoyé à partir d'une adresse IPv6 source spécifique définie par l'utilisateur vers n'importe quelle adresse de destination.

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

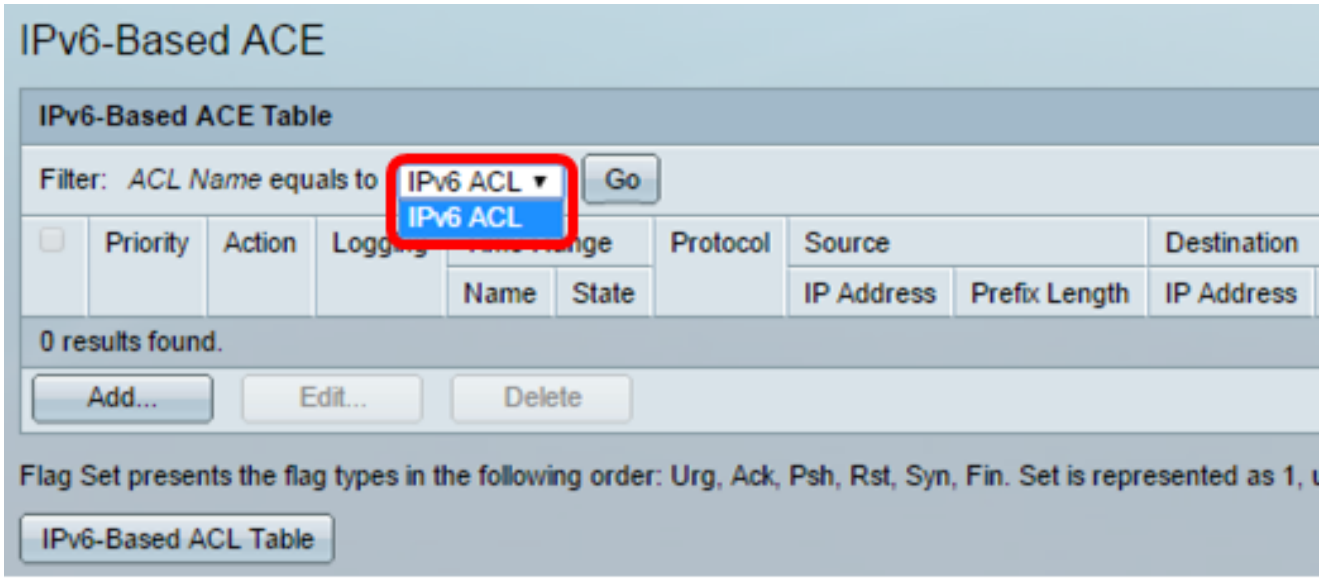
Étape 1. Sur l'utilitaire Web, accédez à **Access Control > IPv6-Based ACE**.



Important : Si vous disposez d'un commutateur Sx350, SG350X et Sx550X, passez en mode avancé en sélectionnant **Advanced** dans la liste déroulante Display Mode dans le coin supérieur droit de la page.

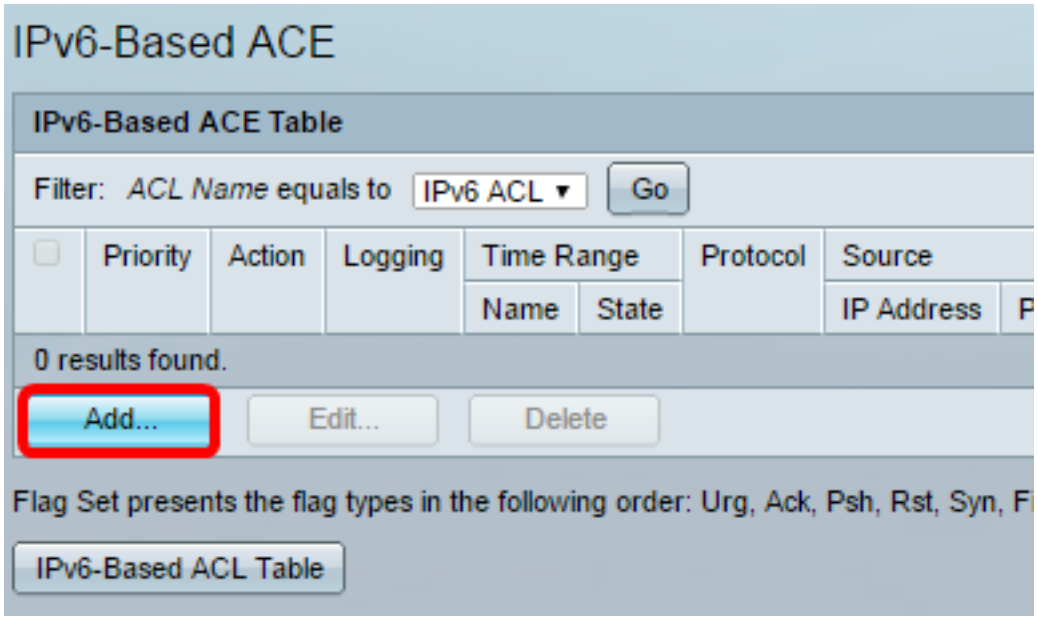


Étape 2. Choisissez une liste de contrôle d'accès dans la liste déroulante Nom de la liste de contrôle d'accès, puis cliquez sur **Go**.



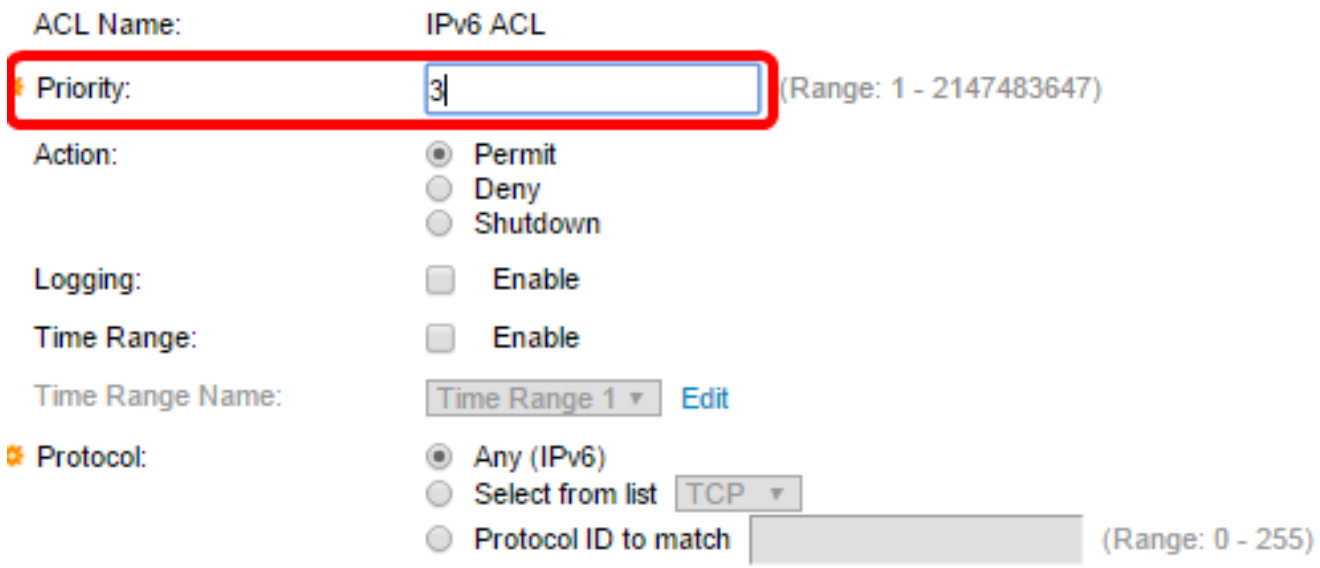
Note: Les ACE déjà configurés pour la liste de contrôle d'accès s'affichent dans le tableau.

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, 3 est utilisé.

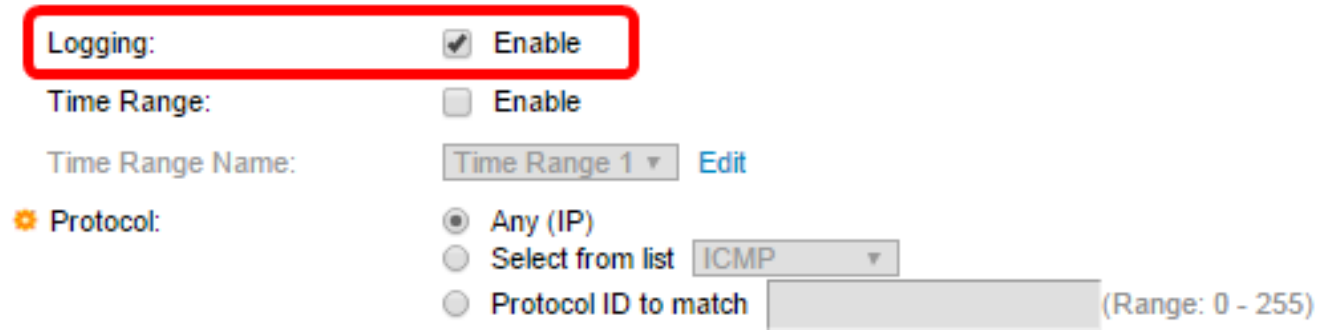
Étape 5. Sélectionnez la case d'option correspondant à l'action souhaitée qui est effectuée lorsqu'une trame répond aux critères requis de l'ACE.

Note: Dans cet exemple, Permit est sélectionné.

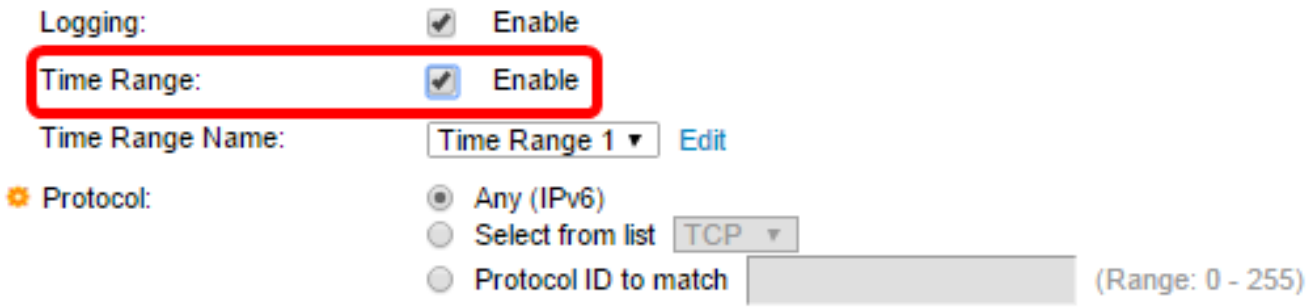
- Permit : le commutateur transfère les paquets qui répondent aux critères requis de l'ACE.
- Deny : le commutateur abandonne les paquets qui répondent aux critères requis de l'ACE.

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

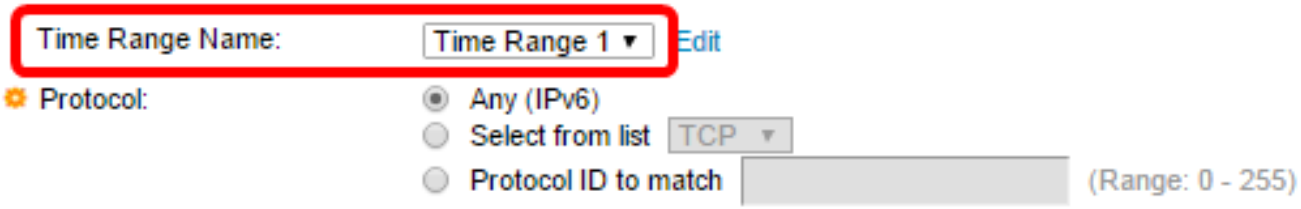
Étape 6. (Facultatif) Cochez la case **Activer la** journalisation pour activer la journalisation des flux ACL qui correspondent à la règle ACL.



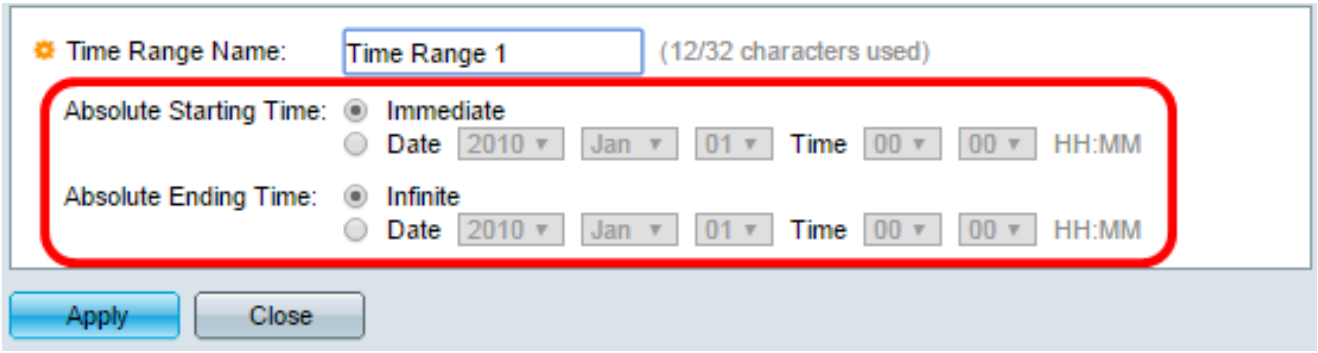
Étape 7. (Facultatif) Cochez la case **Activer** la plage de temps pour autoriser la configuration d'une plage de temps à l'ACE. Les plages de temps sont utilisées pour limiter la durée de validité d'une ACE. Si cette option est désactivée, l'ACE fonctionne à tout moment.



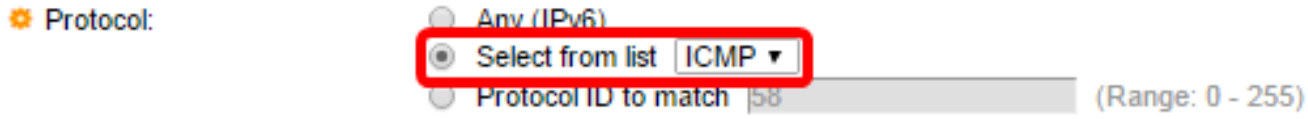
Étape 8. (Facultatif) Dans la liste déroulante Nom de la plage de temps, sélectionnez une plage de temps à appliquer à l'ACE.



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.

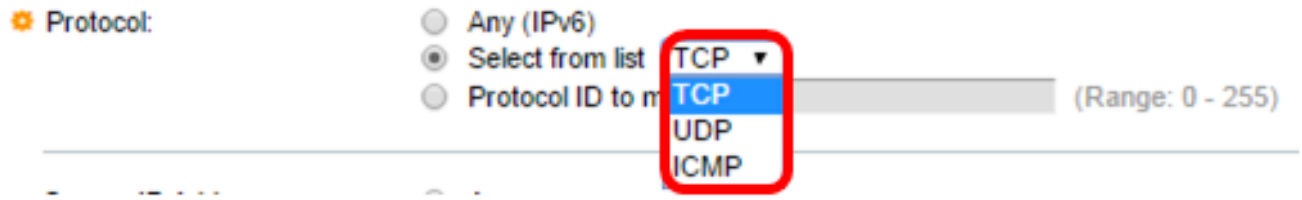


Les options sont les suivantes :

- 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, sélectionnez Sélectionner dans la liste.

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

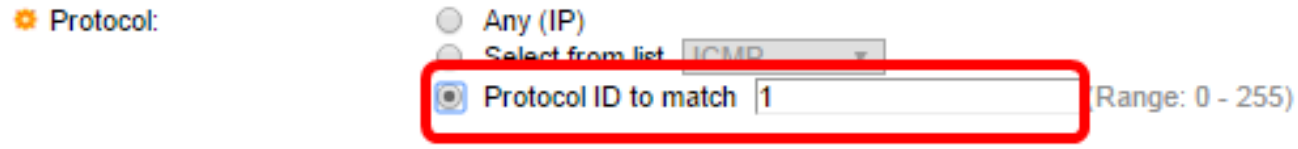


Les options sont les suivantes :

- TCP : le protocole TCP (Transmission Control Protocol) permet à deux hôtes de communiquer et d'échanger des flux de données. Le protocole TCP garantit la livraison des paquets et garantit que les paquets sont transmis et reçus dans l'ordre dans lequel ils ont été envoyés.
- UDP : le protocole UDP (User Datagram Protocol) transmet les paquets mais ne garantit pas leur livraison.
- ICMP : fait correspondre les paquets au protocole ICMP (Internet Control Message Protocol).

Note: Dans cet exemple, TCP est utilisé.

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



Note: Dans cet exemple, 1 est utilisé.

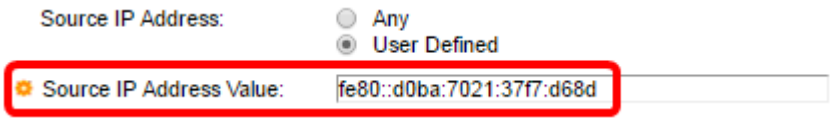
Étape 12. Cliquez sur la case d'option qui correspond aux critères souhaités de l'ACE dans la zone Adresse IP source.

Les options sont les suivantes :

- Any : toutes les adresses IPv6 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 Prefix Length*.

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

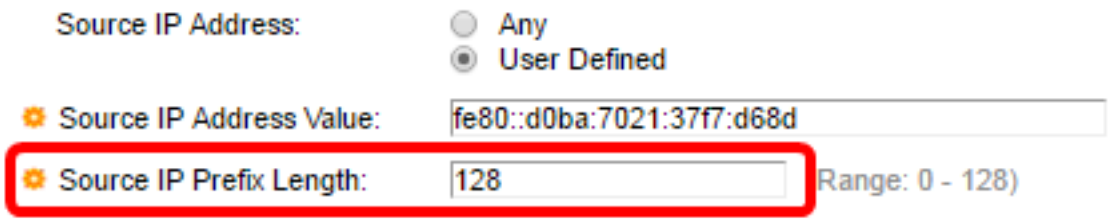
Étape 13. Entrez l'adresse IP source dans le champ *Valeur de l'adresse IP source*.



Note: Dans cet exemple, fe80::d0ba:7021:37f7:d68d est utilisé.

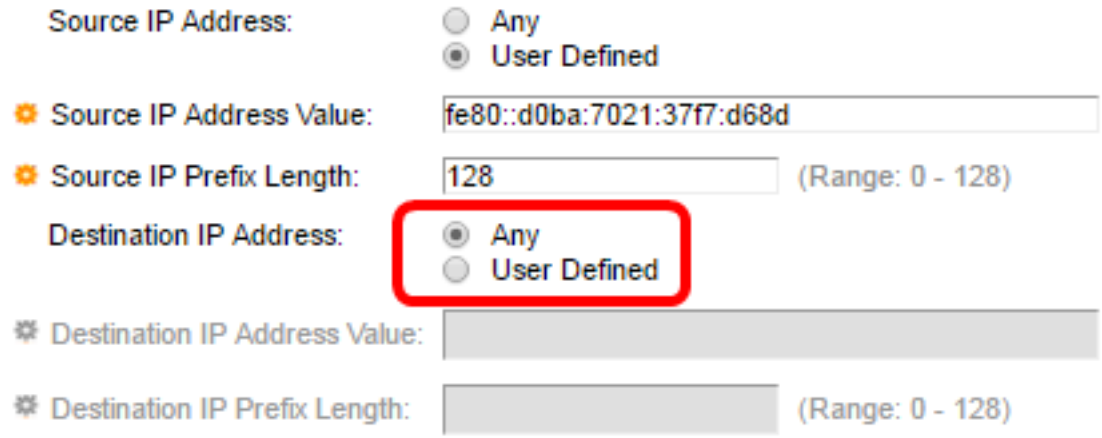
Étape 14. Entrez la longueur du préfixe IP source dans le champ *Longueur du préfixe IP*

source.



Note: Dans cet exemple, 128 est utilisé.

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

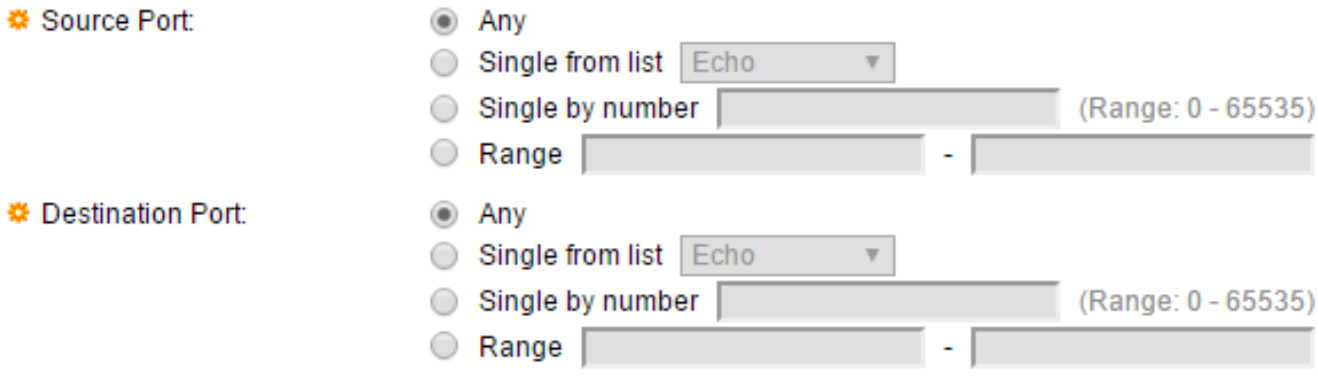


Les options sont les suivantes :

- Any : toutes les adresses IPv6 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 IPPrefix Length*.

Note: Dans cet exemple, Any est sélectionné. Si vous choisissez cette option, l'ACE à créer autorisera le trafic ACE provenant de l'adresse IPv6 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.

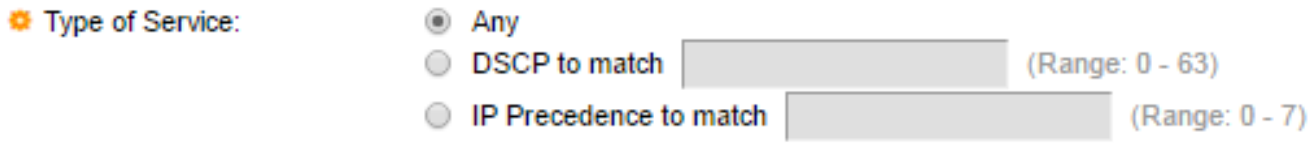
Étape 18. (Facultatif) Dans la zone Indicateurs TCP, sélectionnez un ou plusieurs indicateurs TCP avec lesquels filtrer les paquets. Les paquets filtrés sont transférés ou abandonnés. Le filtrage des paquets par des indicateurs TCP augmente le contrôle des paquets, ce qui augmente la sécurité du réseau.

- 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 — Differentiated Services Code Point 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 les valeurs 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

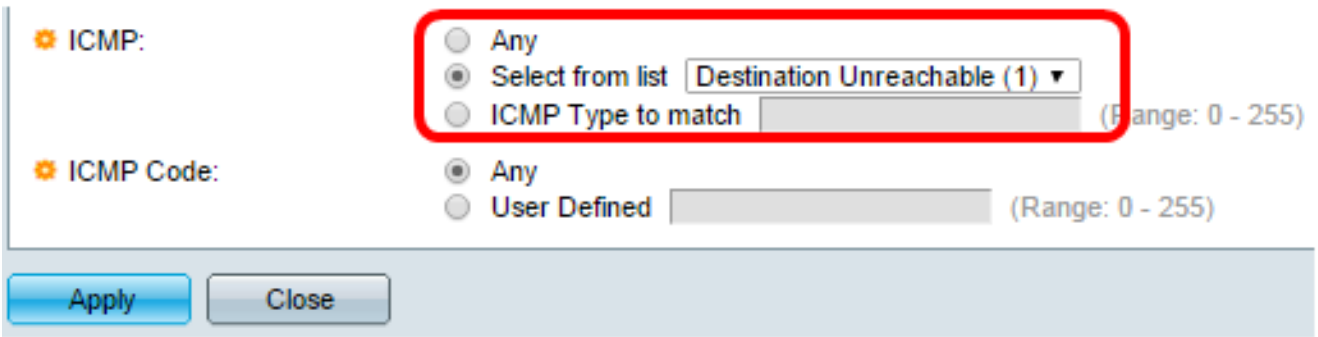
    - 5 - pour les

    - 6 — pour Internet

    - 7 — pour le réseau

Note: Dans cet exemple, Any est sélectionné.

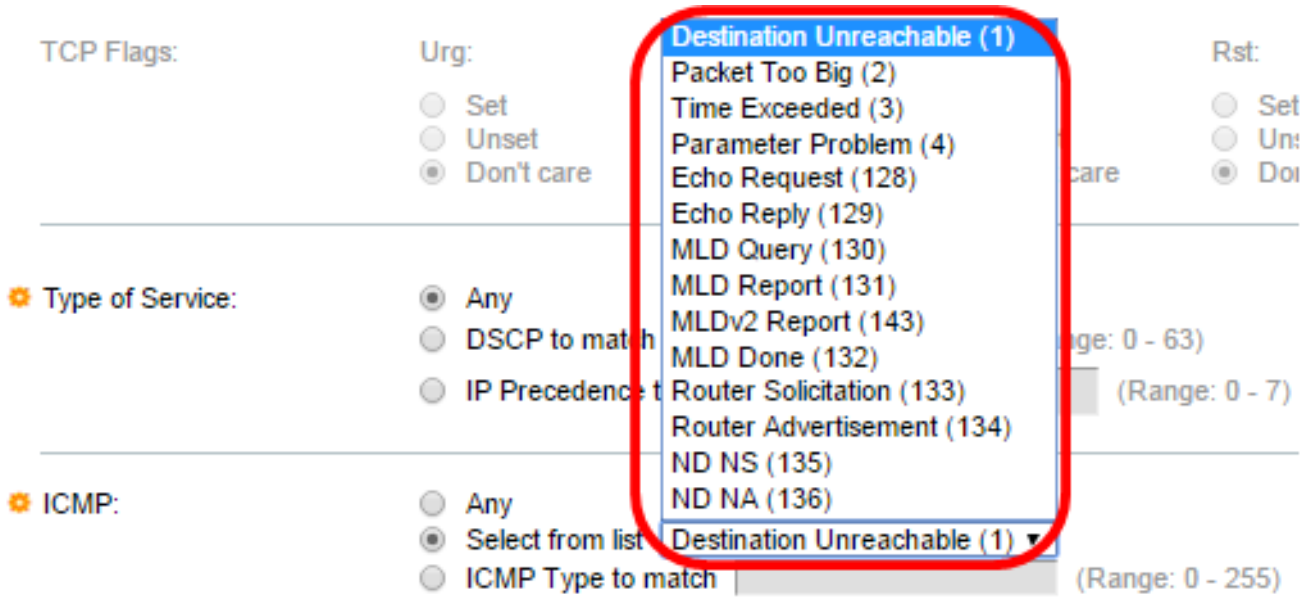
Étape 20. (Facultatif) Si le protocole IP de la liste de contrôle d'accès est ICMP, cliquez sur le type de message ICMP utilisé à des fins de filtrage. Choisissez le type de message par nom ou saisissez le numéro du type de message :



- 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.

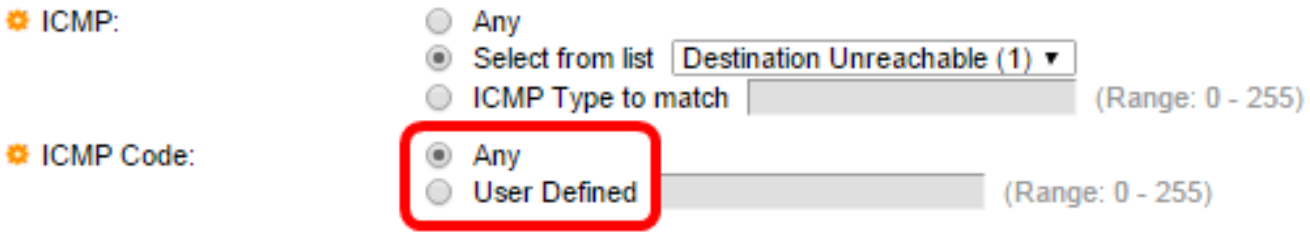
Note: Dans cet exemple, sélectionnez Sélectionner dans la liste.

Étape 21. (Facultatif) Si vous choisissez Sélectionner dans la liste à l'étape 20, choisissez les messages de contrôle à filtrer dans les options possibles de la liste déroulante :



- Destination inaccessible (1) : elle est générée par l'hôte ou sa passerelle pour informer le client que la destination est inaccessible pour une raison quelconque (Exemple : Erreur réseau ou hôte inaccessible).
- Packet Too Big (2) : la taille du datagramme dépasse la MTU donnée.
- Temps dépassé (3) : il est généré par une passerelle pour informer la source d'un datagramme ignoré en raison du temps nécessaire pour que le champ actif atteigne zéro.
- Problème de paramètre (4) : il est généré en réponse à toute erreur non spécifiquement couverte par un autre message ICMP.
- Demande d'écho (128) : il s'agit d'une requête ping dont les données doivent être reçues dans une réponse d'écho.
- Réponse d'écho (129) : elle est générée en réponse à une demande d'écho.
- Requête MLD (130) : elle permet d'apprendre quelles adresses de multidiffusion ont des écouteurs sur une liaison connectée. Tapez 130 en notation décimale.
- Rapport MLD (131) : il est généré lorsque l'adresse de multidiffusion IPv6 à laquelle l'expéditeur du message écoute.
- Rapport MLD v2 (143) — Il est identique à Rapport MLD avec la version 2.
- MLD Done (132) : lorsque l'hôte quitte un groupe, il envoie un message d'écoute de multidiffusion aux routeurs de multidiffusion du réseau.
- Sollicitation de routeur (133) : message de découverte de routeur. Les hôtes découvrent les adresses de leurs routeurs voisins simplement lorsqu'ils écoutent des annonces. La valeur par défaut est 224.0.0.2 pour la multidiffusion, sinon elle est 255.255.255.255.
- Router Advertisement (134) : le routeur diffuse périodiquement une annonce de routeur à partir de chacune de ses interfaces de multidiffusion et annonce les adresses IP de cette interface.
- ND NS (135) - Les messages sont émis par des noeuds pour demander l'adresse de couche liaison d'un autre noeud, ainsi que pour des fonctions telles que la détection des adresses en double et la détection de l'inaccessibilité des voisins.
- ND NA (136) : les messages sont envoyés en réponse aux messages NS. Si un noeud modifie son adresse de couche liaison, il peut envoyer une adresse de réseau non sollicitée pour annoncer la nouvelle adresse.

Étape 22. (Facultatif) Les messages ICMP peuvent avoir un champ de code qui indique comment gérer le message. Cette option est activée si vous choisissez le protocole ICMP à l'étape 10. Cliquez sur l'une des options suivantes pour configurer le filtrage de ce code :

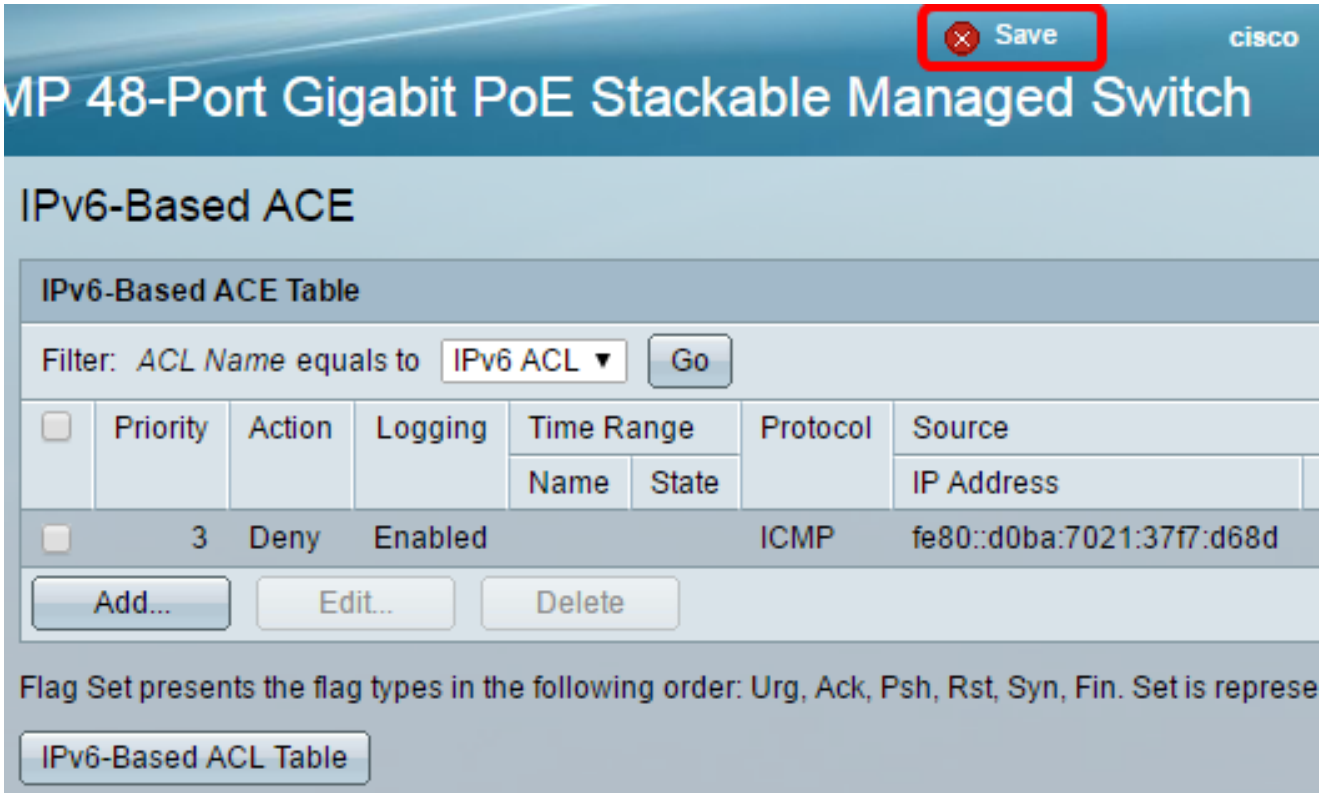


- Any : acceptez tous les codes.
- Défini par l'utilisateur : vous pouvez entrer un code ICMP à des fins de filtrage.

Note: Dans cet exemple, Any est sélectionné.

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 IPv6 sur votre commutateur.