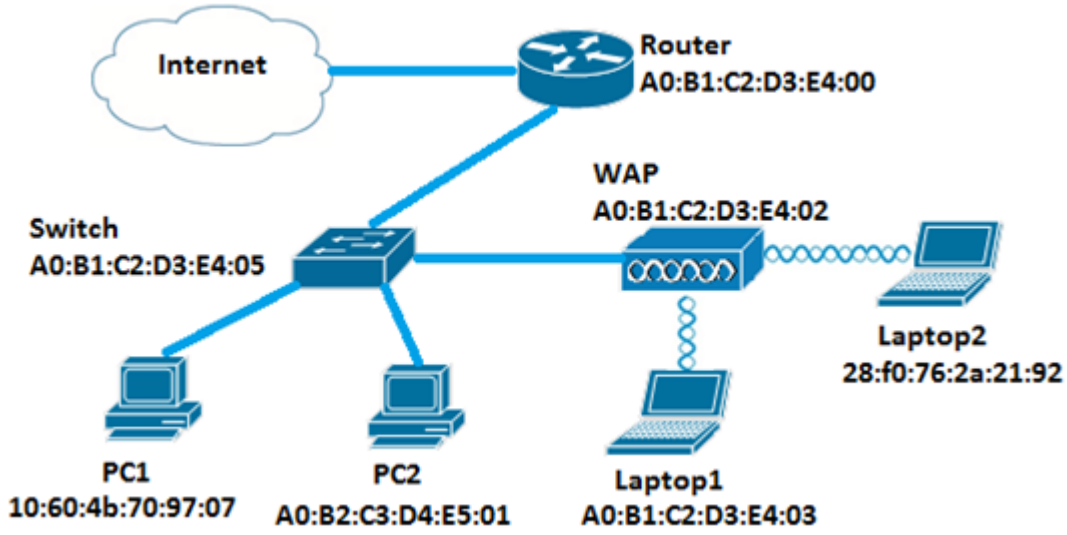
Configurez un ACL de MAC sur un WAP125 et un WAP581

Introduction

Le Listes de contrôle d'accès (ACL) de Contrôle d'accès au support (MAC) sont couche 2 ACLs. Chaque ACL est un ensemble de règles appliquées pour trafiquer reçu par le point d'accès sans fil (WAP). La règle spécifie si le contenu d'un champ donné devrait être utilisé pour permettre ou refuser l'accès au réseau. L'ACLs peut être configuré pour examiner des champs d'une trame comme la source ou l'adresse MAC de destination, l'identifiant virtuel du réseau local (VLAN) (ID), ou le Classe de service (Cos). Quand une trame entre dans le port de périphérique WAP, elle examine la trame et vérifie les règles d'ACL contre le contenu de la trame. Si les règles l'unes des apparient le contenu, une autorisation ou refusent l'action est prise sur la trame. Configurant le MAC ACLs est typiquement utilisé pour autoriser l'accès aux ressources de réseau pour sélectionner des périphériques dans le réseau.

Remarque: Il y a un implicite refusent à la fin de chaque règle créée.



Dans ce scénario, on permettra à tous les périphériques dans le réseau pour avoir accès à Laptop2 derrière le WAP excepté PC1.

Objectif

Ce buts de l'article de t'afficher comment configurer un ACL basé sur MAC sur un Point d'accès WAP125 ou WAP581 afin d'empêcher PC1 d'accéder à Laptop2 derrière le WAP.

Périphériques applicables

- WAP125
- WAP581

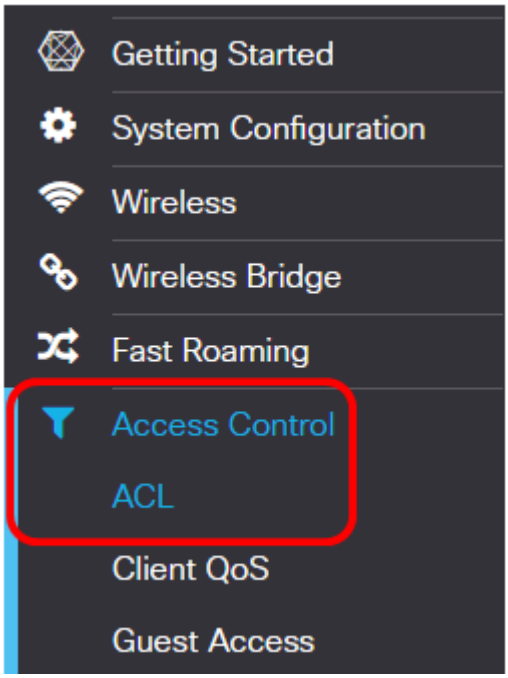
Version de logiciel

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

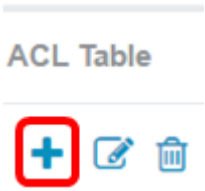
Configurez une liste de filtre de client

Remarque: Les options du menu peuvent varier selon le modèle exact du WAP que vous utilisez. Les images ci-dessous sont prises du WAP125.

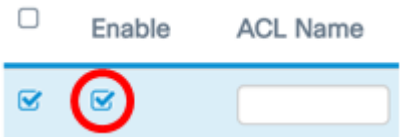
Étape 1. Ouvrez une session à l'utilitaire basé sur le WEB du WAP et choisissez le **contrôle d'accès > l'ACL**.



Étape 2. Cliquez sur le bouton.



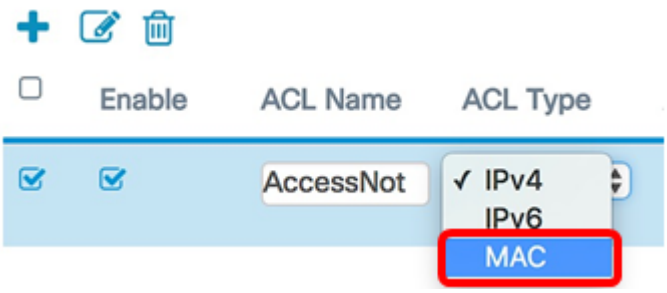
Étape 3. Vérifiez que la case à cocher d'**enable** est vérifiée pour s'assurer que l'ACL est en activité. Cette option est vérifiée par défaut.



Étape 4. Écrivez un nom pour l'ACL dans la zone d'*identification d'ACL* pour identifier l'ACL.

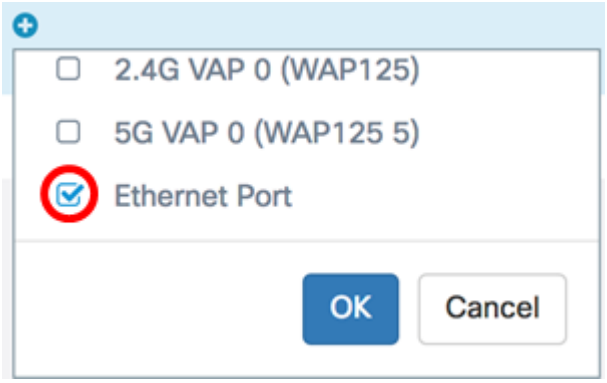
Remarque: Dans cet exemple, AccessNot est entré.

Étape 5. Choisissez le **MAC de la** liste déroulante de type d'ACL.



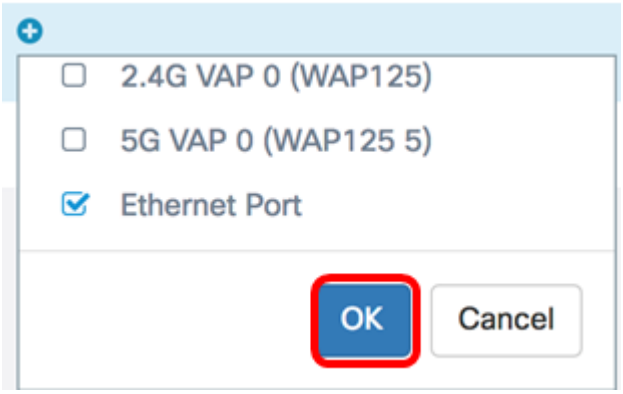
Étape 6. Cliquez sur le bouton et choisissez une interface de la liste déroulante associée d'interface. Les options sont :

- 2.4G VAP 0 (nom SSID) — cette option appliquera l'ACL de MAC au Point d'accès virtuel 2.4 gigahertz (VAP). La section de nom SSID peut changer selon le nom SSID configuré sur le WAP.
- 5G VAP0 (nom SSID) — Cette option s'appliquera l'ACL de MAC aux 5 gigahertz VAP.
- Port Ethernet — Cette option s'appliquera l'ACL de MAC à l'interface Ethernet du WAP.

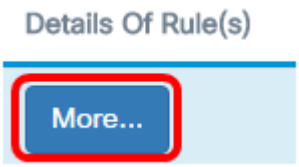


Remarque: Des plusieurs interfaces peuvent être associées à un ACL. Cochez la case de l'interface correspondante pour associer l'interface à l'ACL. Décochez la case pour dissocier l'interface de l'ACL. Dans cet exemple, le port Ethernet est associé à l'ACL.

Étape 7. Cliquez sur OK.



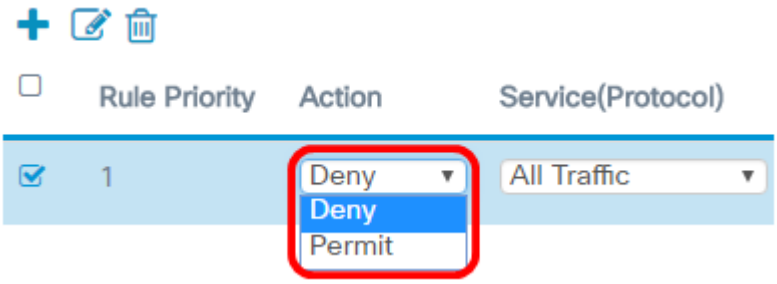
Étape 8. Cliquez sur **davantage… le** bouton pour configurer les paramètres de l'ACL.



Étape 9. Cliquez sur le bouton pour ajouter une nouvelle règle.

Étape 10. Choisissez une action de la liste déroulante d'action. Les options sont :

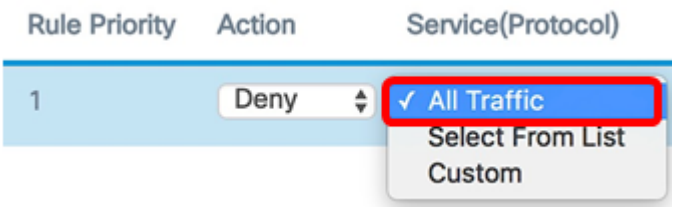
- Autorisation — Cette option permettra les paquets qui apparient les critères d'ACL pour se connecter au réseau.
- Refusez — Cette option empêchera les paquets qui apparient les critères d'ACL de se connecter au réseau.



Remarque: Dans cet exemple, Deny est choisi.

Étape 11. Choisissez un service ou un protocole à filtrer de la liste déroulante de service (Protocol). Les options sont :

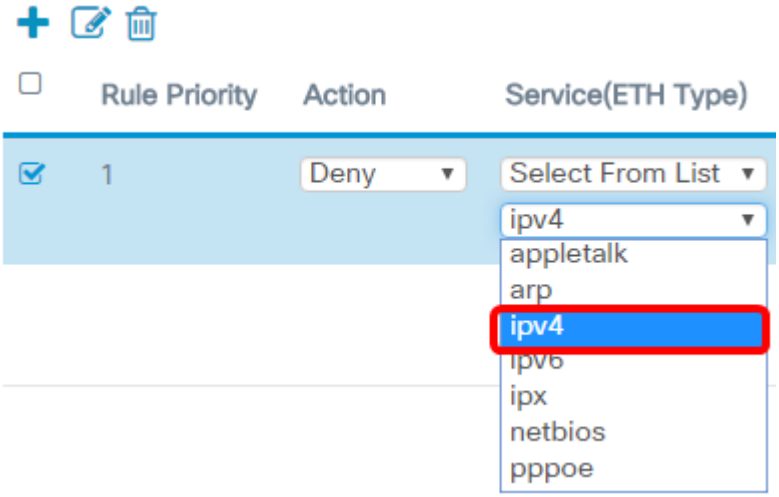
- Tous trafiquent — Cette option traitera tous les paquets comme correspondance au filtre d'ACL.
- Choisissez parmi la liste — Cette option te permettra pour choisir l'AppleTalk, l'ARP, l'ipv4, l'IPv6, l'IPX, le Netbios, et le PPPoE comme filtres pour l'ACL. Si vous choisissez cette option, ignorez à l'étape 12.
- Coutume — Cette option te permettra pour écrire un identificateur de protocole fait sur commande comme filtre pour les paquets. La valeur est un nombre hexadécimal à quatre chiffres. La plage est 0600 à FFFF.



Remarque: Dans cet exemple, **tout le trafic** est choisi.

Étape 12. (Facultatif) si vous choisissiez choisi de la liste, choisissez l'un des après des options :

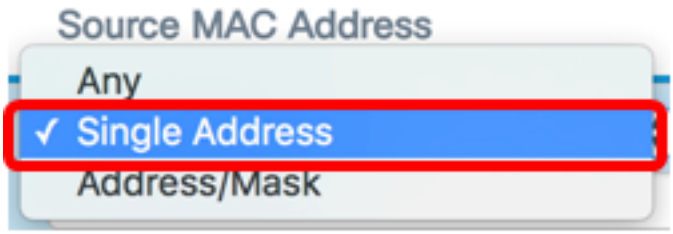
- AppleTalk — Cette option filtre des paquets d'AppleTalk basés sur la déclaration de l'ACL. L'AppleTalk est un ensemble de protocoles de réseau développés par Apple pour leurs ordinateurs de MAC. Une des caractéristiques permettent des réseaux locaux (réseaux locaux) à connecter sans besoin d'un routeur ou d'un serveur central.
- ARP — Cette option filtre des paquets de Protocole ARP (Address Resolution Protocol) basés sur la déclaration de l'ACL. L'ARP met à jour une table en laquelle des adresses MAC sont tracées aux adresses IP.
- ipv4 — Cette option filtre des paquets d'ipv4 basés sur la déclaration de l'ACL.
- IPv6 — Cette option filtre des paquets d'IPv6 basés sur la déclaration de l'ACL. L'IPv6 est le successeur de l'IPv6 dans l'adressage réseau.
- IPX — Cette option filtre des paquets de l'Internetwork Packet Exchange (IPX) basés sur la déclaration de l'ACL. Comme l'AppleTalk, l'IPX est également un protocole de réseau de propriété industrielle. Il connecte les réseaux qui utilisent des clients Novell et des serveurs.
- Netbios — Cette option filtre les paquets de base de système d'entrée et sortie de réseau (Netbios) basés sur la déclaration de l'ACL. Netbios permet à des applications sur les ordinateurs distincts pour communiquer en fournissant les services pour qu'ils puissent communiquer.
- PPPoE — Cette option filtre des paquets de Protocole PPPoE (PPP sur Ethernet) basés sur la déclaration de l'ACL. Il est principalement utilisé dans des services de la ligne d'abonné numérique (DSL).



Remarque: Dans cet exemple, l'ipv4 est choisi.

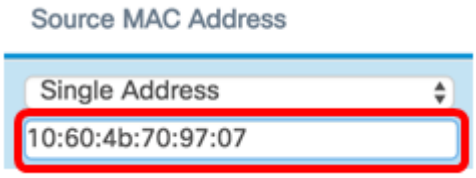
Étape 13. Définissez l'adresse MAC source de la liste déroulante d'adresse MAC source. Les options sont :

- Quels — Cette option permettra le WAP d'appliquer le filtre aux paquets à partir de n'importe quelle adresse MAC.
- Adresse unique — Cette option permettra le WAP d'appliquer le filtre aux paquets à partir d'une adresse MAC spécifiée.
- Adresse/masque — Cette option permettra le WAP d'appliquer le filtre aux paquets à une adresse MAC et au masque du WAP.



Remarque: Dans cet exemple, l'adresse unique est choisie.

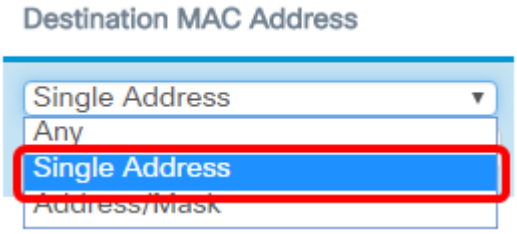
Étape 14. Introduisez l'adresse MAC source dans la zone adresse d'*adresse MAC source*.



Remarque: Dans cet exemple, 10:60:4b:70:97:07 est écrit. C'est l'adresse MAC de PC1.

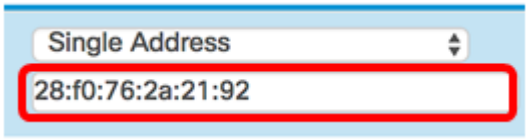
Étape 15. Définissez l'adresse MAC de destination de la liste déroulante d'adresse MAC de destination. Les options sont :

- Quels — Cette option permettra le WAP d'appliquer le filtre aux paquets à partir de n'importe quelle adresse MAC.
- Adresse unique — Cette option permettra le WAP d'appliquer le filtre aux paquets à partir d'une adresse MAC spécifiée.
- Adresse/masque — Cette option permettra le WAP d'appliquer le filtre aux paquets à une adresse MAC et au masque du WAP.



Remarque: Dans cet exemple, l'adresse unique est choisie.

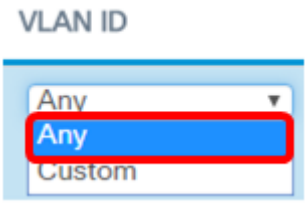
Étape 16. Écrivez l'adresse MAC de destination dans le domaine d'**adresse MAC de destination**.



Remarque: Dans cet exemple, 28:f0:76:2a:21:92 est écrit. C'est l'adresse MAC de Laptop2.

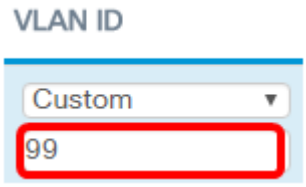
Étape 17. Choisissez un ID DE VLAN de la liste déroulante.

- Quels — Cette option permet n'importe quel ID DE VLAN par le réseau.
- Coutume — Cette option te permettra pour écrire un ID DE VLAN spécifique. Si vous choisissez cette option, ignorez à l'étape 18.



Remarque: Dans cet exemple, en est choisi.

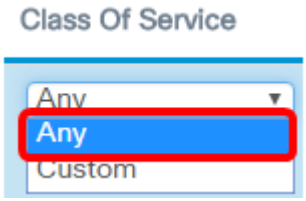
Étape 18. (Facultatif) si vous choisissiez la coutume, écrivez l'ID DE VLAN dans le domaine d'*ID DE VLAN*.



Remarque: Dans cet exemple, 99 est écrits.

Étape 19. (Facultatif) choisissez une classe de service de la liste déroulante. Les options sont :

- Quels — Cette option permet au paquet avec n'importe quel niveau de priorité pour se connecter au réseau.
- Coutume — Cette option te permettra pour filtrer des paquets à un niveau de priorité spécifique.



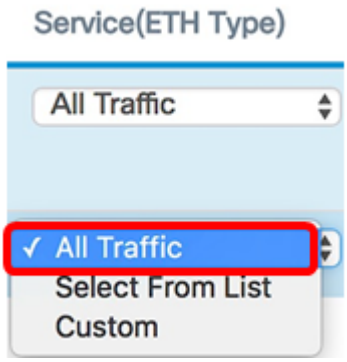
Remarque: Dans cet exemple, en est choisi. Si vous choisissiez la coutume, écrivez la priorité dans le domaine de *classe de service*.

Étape 20. Cliquez sur le bouton de nouveau pour ajouter une règle d'autorisation.

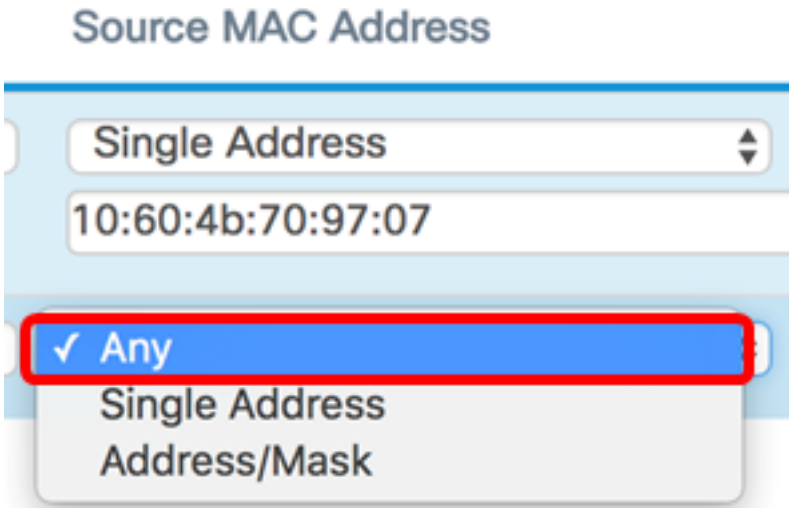
Remarque: Puisqu'il y a un implicite refusez à la fin de chaque règle créée, il est fortement recommandé d'ajouter une règle d'autorisation à l'ACL de permettre le trafic d'autres périphériques dans le réseau.

Étape 21. Cliquez sur la flèche déroulante d'action et choisissez l'**autorisation**.

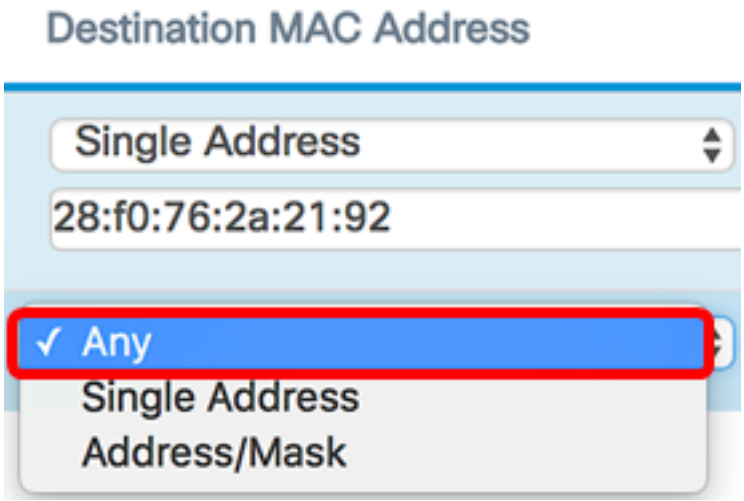
Étape 22. Cliquez sur la flèche déroulante de service (type ETH) et choisissez **tout le trafic**.



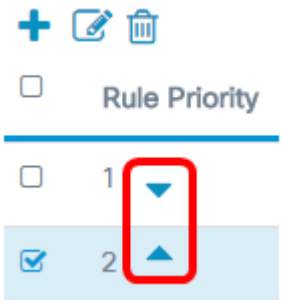
Étape 23. En cliquez sur le menu déroulant d'adresse MAC source et choisissez. Ceci permettrait le trafic de toutes les autres adresses MAC dans le réseau excepté l'adresse MAC PC1 indiquée dans la première règle.



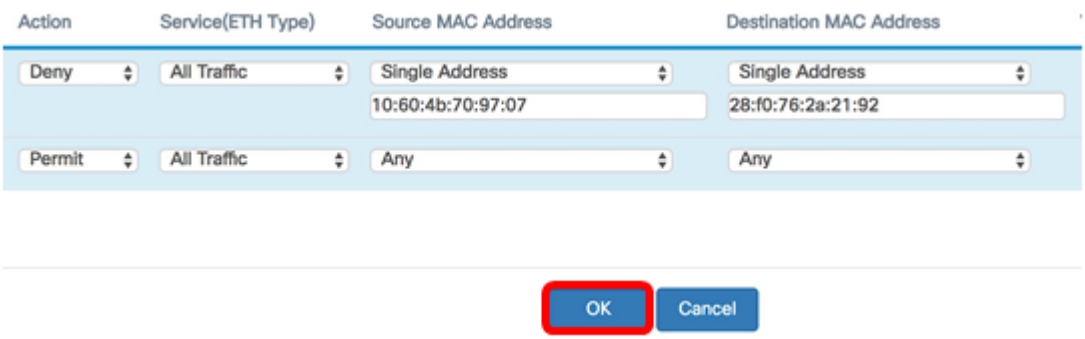
Étape 24. En cliquez sur le menu déroulant d'adresse MAC de destination et choisissez. Ceci permettrait le trafic allant à toutes les adresses MAC dans le réseau.



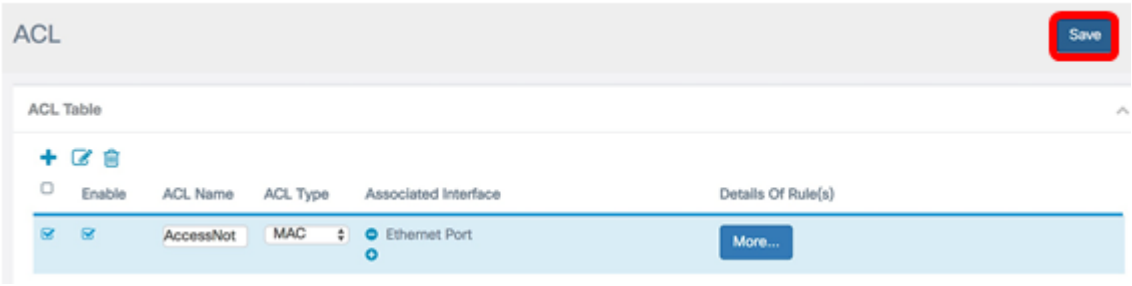
Étape 25.(Optional) Changez la priorité de la règle en cliquant sur en haut et en bas les flèches jusqu'à ce que la règle soit en place.



Étape 26. Cliquez sur **OK**.



Étape 27. Cliquez sur **Save**.



Vous devriez maintenant avoir configuré l'ACL de MAC sur le Point d'accès WAP125 ou WAP581.

Visualisez un vidéo lié à cet article…

[A cliquez ici pour visualiser d'autres entretiens de tech de Cisco]