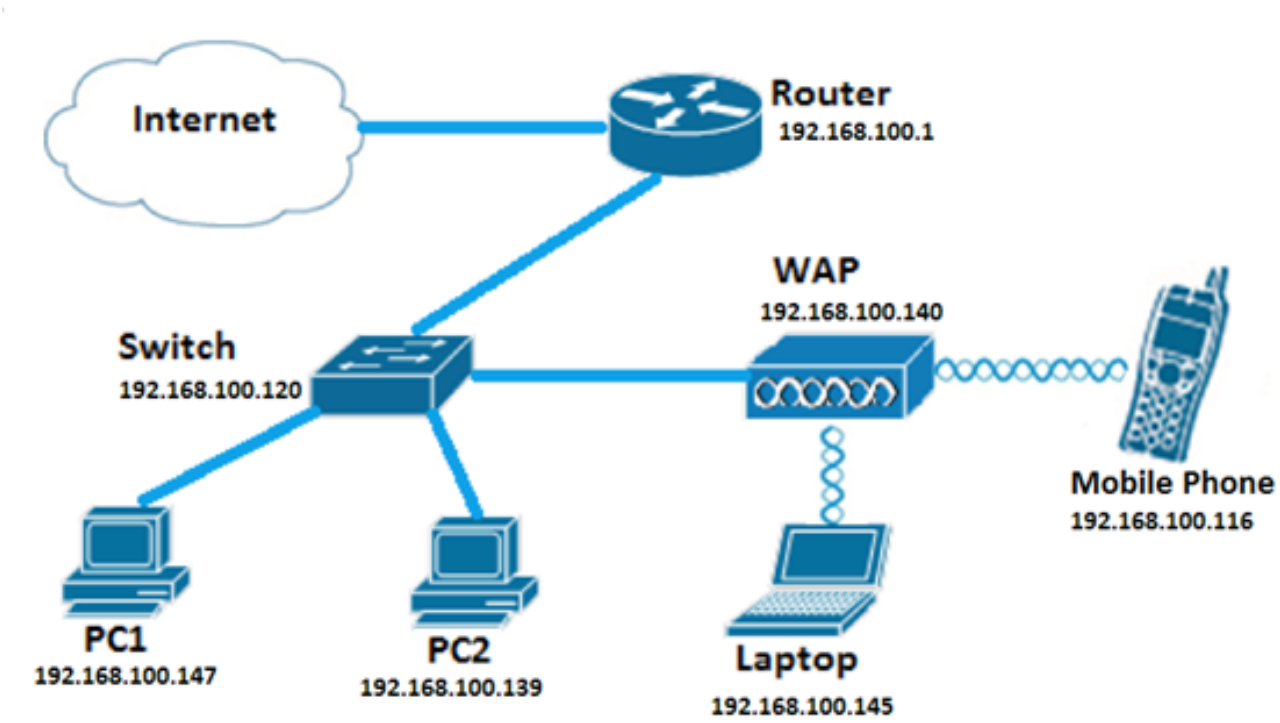
Configurez l'ACL d'ipv4 sur le WAP125 et le WAP581

Introduction

La version 4 (ipv4) d'Internet Protocol et Listes de contrôle d'accès (ACL) de la version 6 d'Internet Protocol (IPv6) sont un ensemble de règles appliquées aux paquets reçus par le point d'accès sans fil (WAP). Chaque règle est utilisée de déterminer si l'accès au réseau devrait être permis ou refusé. L'ACLs peut être configuré pour examiner des champs d'une trame comme la source ou l'adresse IP 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 l'ipv4 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.



Remarque: Dans ce scénario, on permettra au tout le trafic de PC2 pour accéder au réseau. Tout autre trafic d'autres hôtes sera refusé.

Objectif

Ce buts de l'article de t'afficher comment configurer un ACL d'ipv4 sur un Point d'accès WAP125 et WAP581.

Périphériques applicables

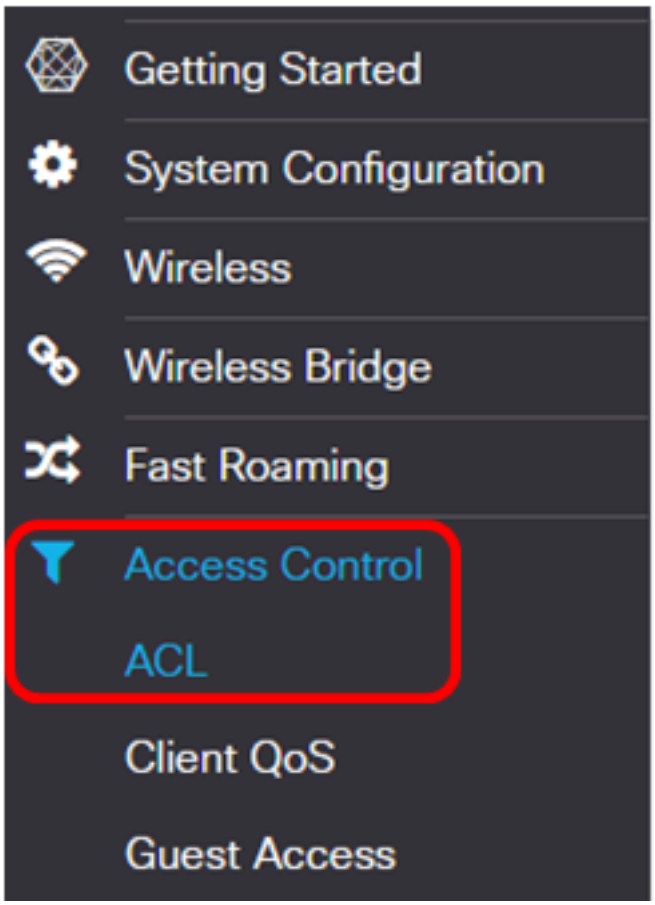
- WAP125
- WAP581

Version de logiciel

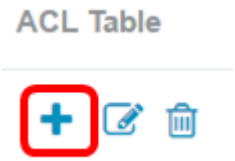
- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

Configurez un ACL d'ipv4

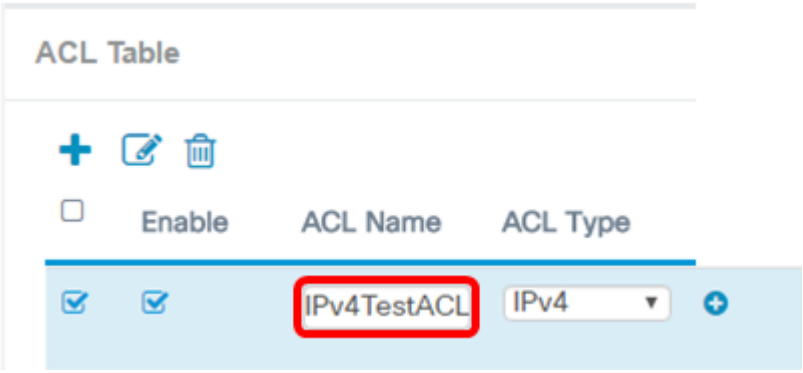
Étape 1. Ouvrez une session à l'utilitaire basé sur le WEB du WAP et choisissez le **contrôle d'accès > l'ACL**.



Étape 2. Cliquez sur + le bouton pour créer un nouvel ACL.

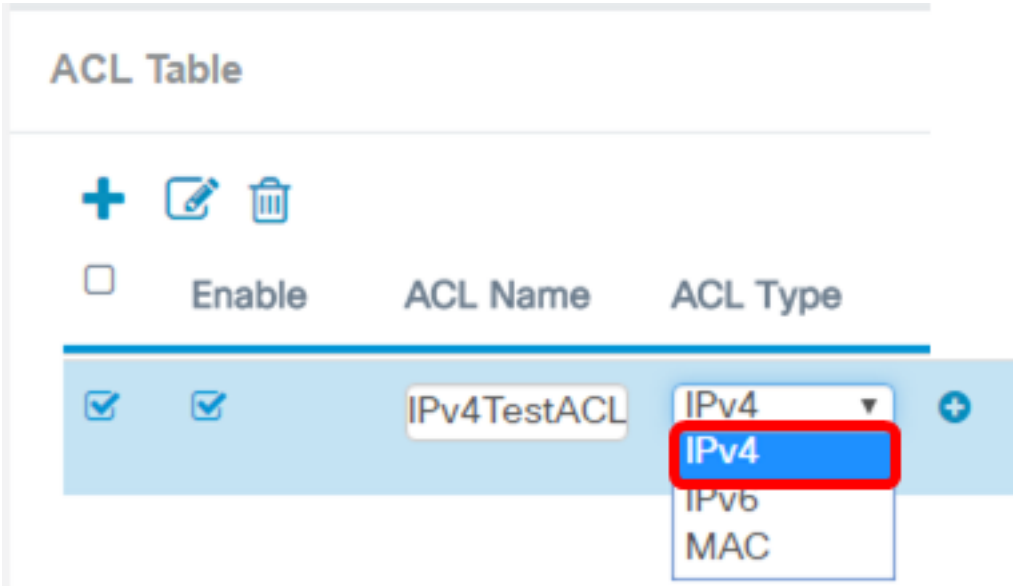


Étape 3. Écrivez un nom pour l'ACL dans la zone d'*identification d'ACL*.



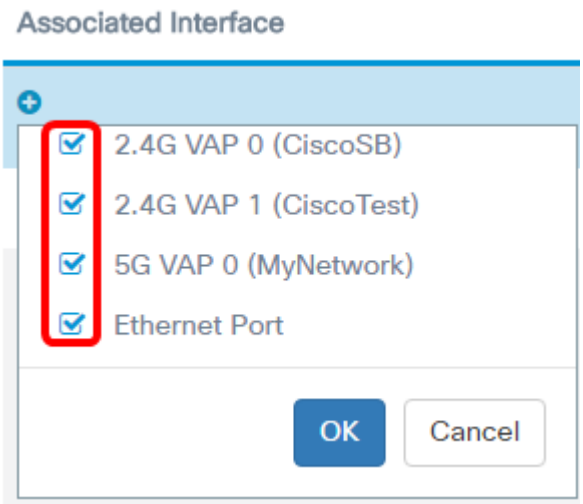
Remarque: Dans cet exemple, IPv4TestACL est écrit.

Étape 4. Choisissez l'ipv4 de la liste déroulante de type d'ACL.



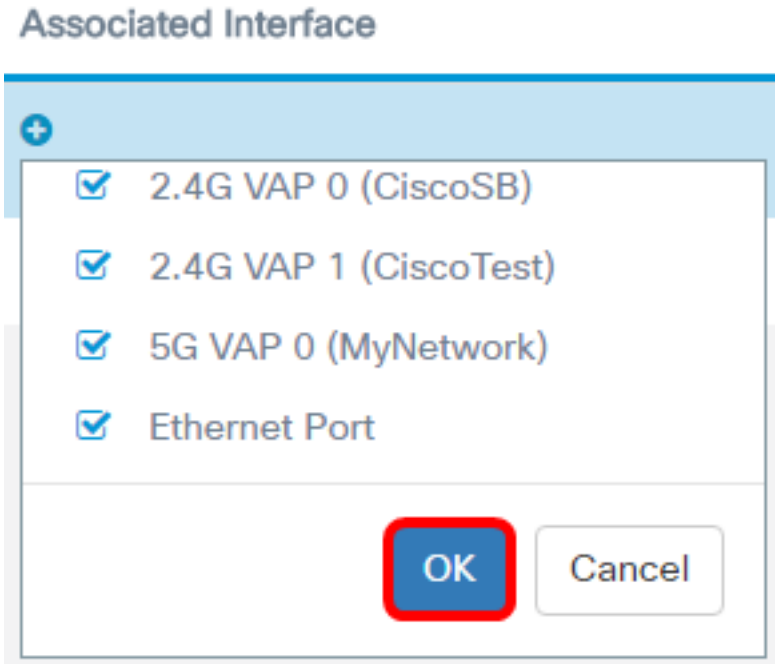
Étape 5. Cliquez sur le bouton et choisissez une interface de la liste déroulante associée d'interface. Les options sont :

- 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. Cependant, il ne peut pas être associé à un ACL quand il a été déjà associé à un autre ACL. Dans cet exemple, toutes les interfaces sont associées à IPv4TestACL. Décochez la case pour dissocier l'interface de l'ACL.

Étape 6. Cliquez sur OK.

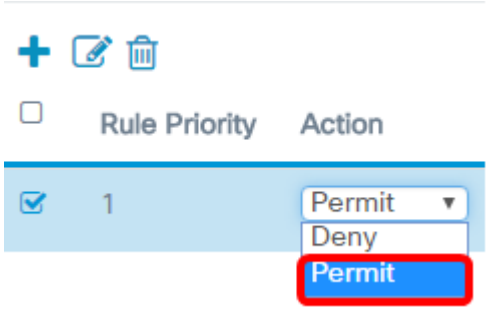


Étape 7. Cliquez sur **davantage… le** bouton pour configurer les paramètres de l'ACL.

Étape 8. Cliquez sur + le bouton pour ajouter une nouvelle règle.

Étape 9. Choisissez une action de la liste déroulante d'action. Les options sont :

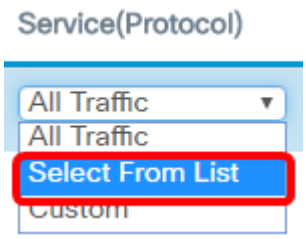
- Autorisation — Cette option permettra les paquets qui apparient les critères d'ACL pour se connecter au réseau.
- Refusez — Cette option empêchera les paquets qui apparient les critères d'ACL de se connecter au réseau.



Remarque: Dans cet exemple, l'autorisation est choisie.

Étape 10. Choisissez un service ou un protocole à filtrer de la liste déroulante de service (Protocol). Les options sont :

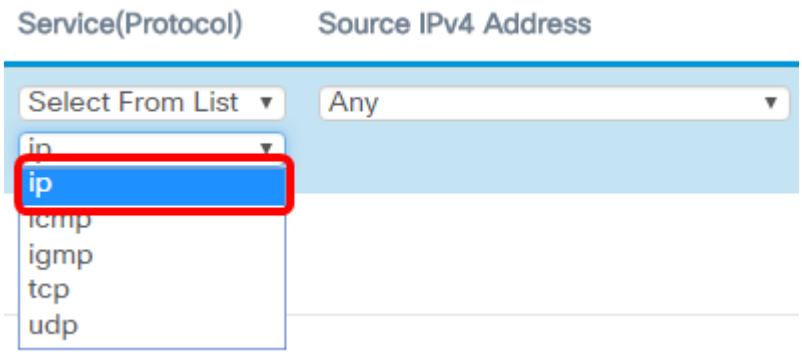
- Tous trafiquent — Cette option traitera tous les paquets comme correspondance au filtre d'ACL.
- Choisissez parmi la liste — Cette option te permettra pour choisir l'IP, l'ICMP, l'IGMP, le TCP, ou l'UDP comme filtres pour l'ACL. Si cette option est choisie, passez à l'étape 11.
- Coutume — Cette option 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 de 0 à 255.



Remarque: Dans cet exemple, choisi de la liste est choisi.

Étape 11. Définissez Protocol qui doit être permis pour se connecter au réseau. Les options sont :

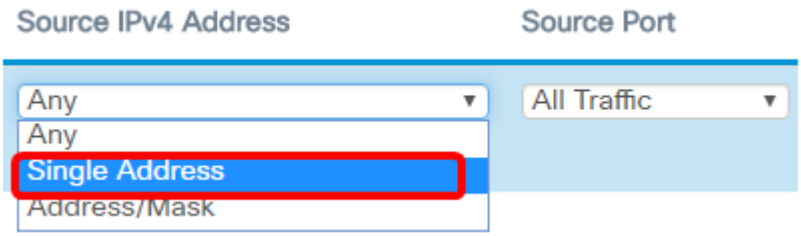
- IP — Cette option permettra le Point d'accès de filtrer les hôtes accédant au réseau utilisant leur adresse IP comme filtre.
- ICMP — Cette option permettra le Point d'accès de filtrer des paquets de Protocole ICMP (Internet Control Message Protocol) écrivant le réseau à l'aide du Point d'accès.
- igmp — Cette option permettra le Point d'accès de filtrer des paquets de Protocole IGMP (Internet Group Management Protocol) écrivant le réseau à l'aide du Point d'accès.
- TCP — Cette option permettra le Point d'accès de filtrer des paquets de Protocole TCP (Transmission Control Protocol) écrivant le réseau à l'aide du Point d'accès.
- UDP — Cette option permettra le Point d'accès de filtrer des paquets de Protocole UDP (User Datagram Protocol) écrivant le réseau à l'aide du Point d'accès.



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

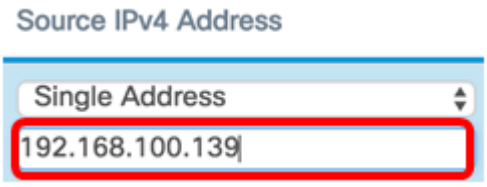
Étape 12. Définissez l'ipv4 addres de source de la liste déroulante d'ipv4 addres de source. Les options sont :

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



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

Étape 13. Écrivez l'adresse IP de l'hôte qui doit être permis en accédant au réseau.



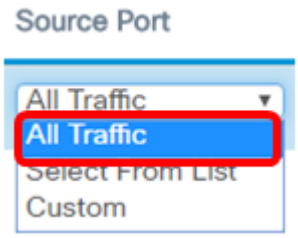
Remarque: Dans cet exemple, 192.168.100.139 est entré. C'est l'adresse IP de PC2.

Étape 14. Choisissez un port de source pour la condition. Les options sont :

- Tous trafiquent — Cette option permettra tous les paquets du port de source qui répond aux critères.
- Choisissez parmi la liste — Cette option te permet pour choisir le FTP, le ftpdata, le HTTP, le SMTP, le SNMP, le telnet, le tftp, et le WWW.
- Coutume — Cette option te permettra pour introduire un numéro de port IANA pour apparier le port de source identifié dans l'en-tête de datagramme. La plage de port est de 0 à 65535 et inclut ce qui suit :

- 0 à 1023 — Ports connus

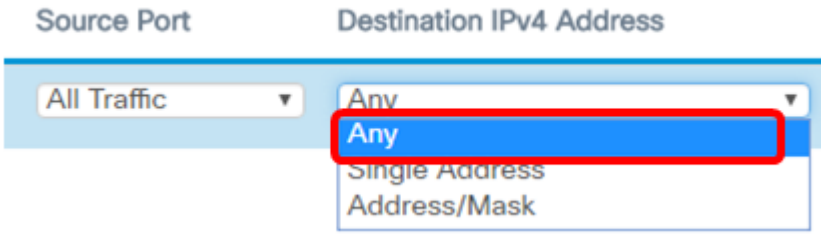
- 1024 — 49151 — ports enregistrés
- 49152 — 65535 — dynamiques et/ou ports privés



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

Étape 15. Choisissez une adresse de destination de la liste déroulante d'ipv4 addres de destination. Les options sont :

- Quels — Cette option traite n'importe quelle adresse IP comme correspondance à la déclaration d'ACL.
- Adresse unique — Cette option vous permet d'écrire une adresse IP spécifique pour l'état d'ACL.
- Adresse/masque — Cette option vous permet d'écrire une plage d'adresses IP ou un masque.



Remarque: Dans cet exemple, en est choisi.

Étape 16. Choisissez une destination port de la liste déroulante de destination port. Les options sont :

- Quels — Cette option traite toutes les destinations port des paquets comme correspondance à la déclaration dans l'ACL.
- Choisissez parmi la liste — Cette option vous permet de choisir un mot clé associé avec la destination port pour apparier. Les options sont : FTP, ftpdata, HTTP, SMTP, SNMP, telnet, tftp, et WWW. Ces mots clé se traduisent à leurs nombres de port correspondant.
- Coutume — Cette option te permettra pour introduire un numéro de port IANA pour apparier le port de source identifié dans l'en-tête de datagramme. La plage de port est de 0 à 65535 et inclut ce qui suit :

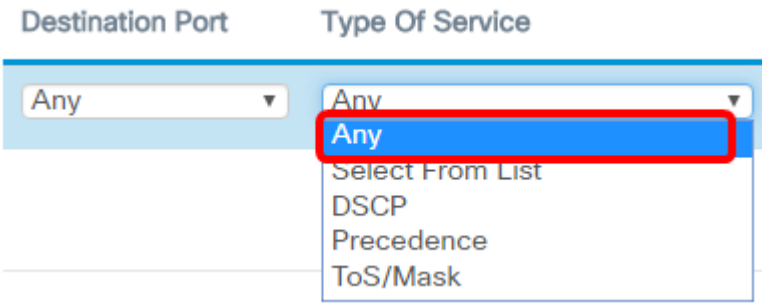
  - 0 à 1023 — Ports connus
  - 1024 — 49151 — ports enregistrés
  - 49152 — 65535 — dynamiques et/ou ports privés

Étape 17. Choisissez un type de service pour apparier le type de paquet du type de liste déroulante de service. Les options sont :

- Quels — Cette option traite n'importe quel service comme correspondance pour les paquets.
- Choisissez parmi la liste — Cette option apparie les paquets basés sur leur

Differentiated Services Code Point, (DSCP), Classe de service (Cos), ou valeurs (E-F) expédiées d'expédition.

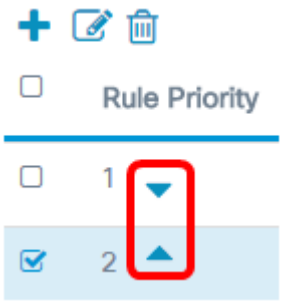
- DSCP — L'option apparie les paquets basés sur leur valeur DSCP faite sur commande. En choisissant cette option, écrivez une valeur de 0 à 63 dans le domaine de valeur DSCP.
- Priorité — Cette option apparie les paquets basés sur leur valeur de priorité IP. Quand cette option est choisie, entrez dans une valeur de priorité IP de 0 à 7.
- Tos/masque — Cette option vous permet d'écrire un masque de tos IP pour identifier les positions binaires en valeur de bits de tos IP qui sont utilisées pour la comparaison contre le tos IP mettent en place dans un paquet.



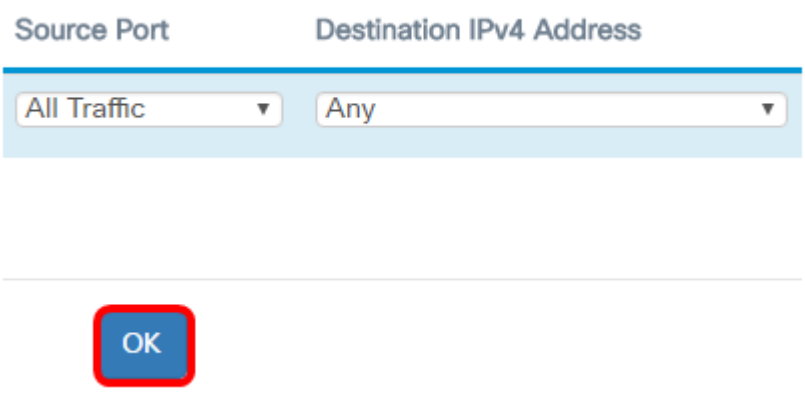
Étape 18. (Facultatif) répétez l'étape 8 à l'étape 17 jusqu'à ce que l'ACL soit complet.

Remarque: Puisqu'il y a un implicite refusez à la fin de chaque règle créée, là n'est aucun besoin d'ajouter une règle de refuser à l'ACL d'empêcher l'accès d'autres périphériques dans le réseau.

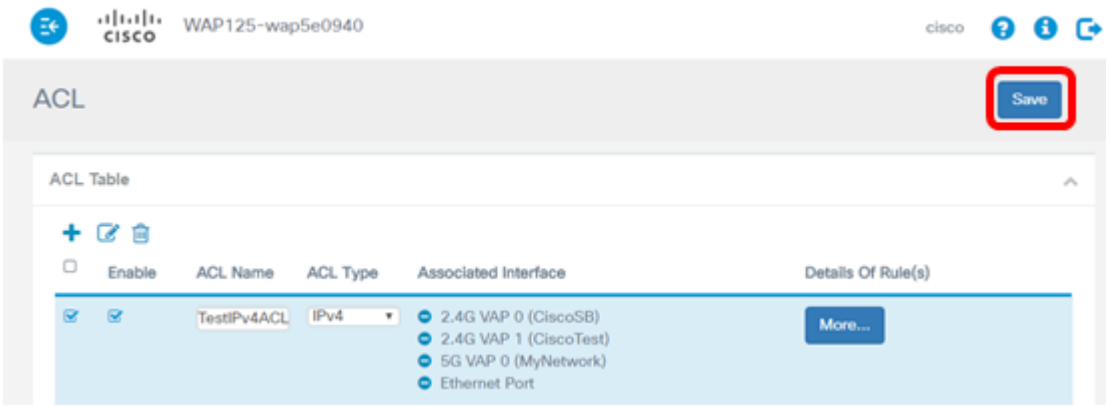
Étape 19. (Facultatif) changez la commande des conditions sur l'ACL en cliquant sur en haut et en bas les boutons jusqu'à ce qu'ils soient dans l'ordre approprié.



Étape 20. Cliquez sur **OK**.



Étape 21. Cliquez sur **Save**.



Vous devriez maintenant s'être terminé installant un ACL d'ipv4 qui permettrait à seulement un hôte pour accéder au réseau une fois connecté au WAP.