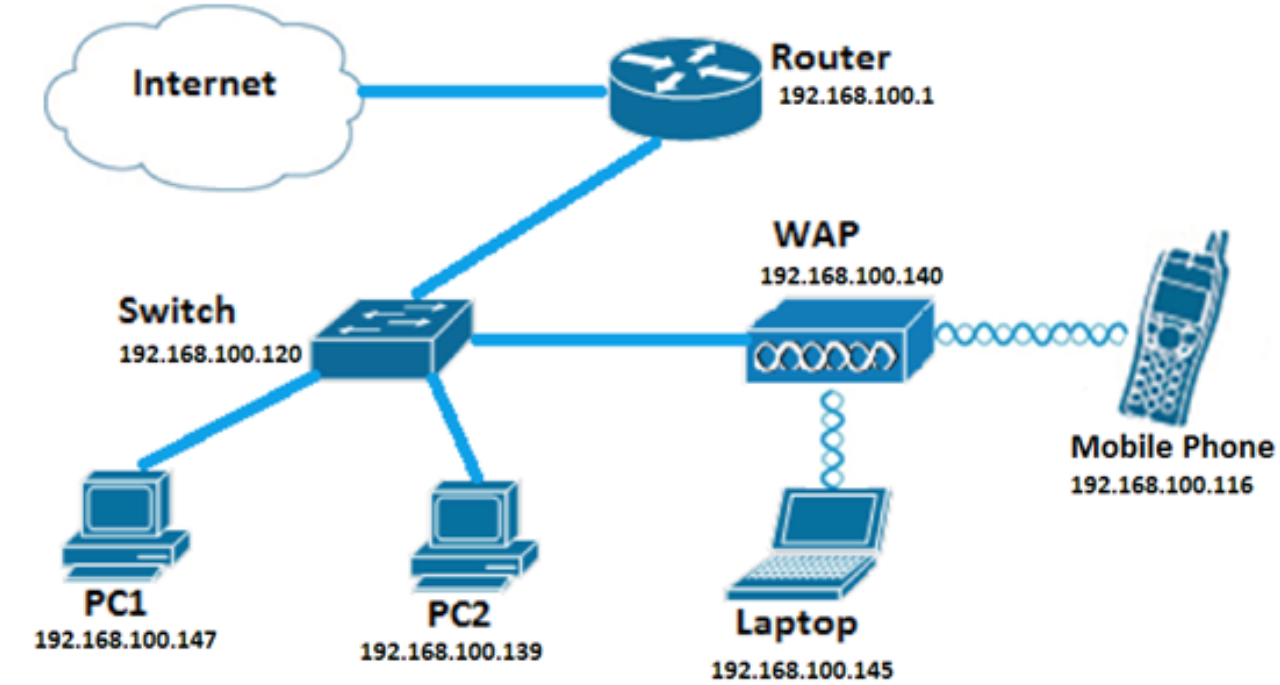
IPv4 ACL's configureren op WAP125 en WAP581

Inleiding

Internet Protocol, versie 4 (IPv4) en Internet Protocol, versie 6 (IPv6) Toegangscontrolelijsten (ACL's) zijn een reeks regels die worden toegepast op pakketten die worden ontvangen door WAP (Wireless Access Point). Elke regel wordt gebruikt om te bepalen of toegang tot het netwerk toegestaan of geweigerd moet worden. U kunt ACL's (ACL's) configureren om velden van een kader te inspecteren, zoals het IP-adres van de bron of bestemming, het VLAN-id (Virtual Local Area Network) of de CoS-serviceklasse (CoS). Wanneer een kader de poort van het WAP apparaat ingaat, inspecteert het het kader en controleert de ACL regels tegen de inhoud van het kader. Als een van de regels overeenkomt met de inhoud, wordt een vergunning afgegeven of ontkende actie ondernomen op het frame.

Het configureren van IPv4 ACL's wordt doorgaans gebruikt om toegang tot netwerkbronnen te verlenen om apparaten in het netwerk te selecteren.

Opmerking: Er is een impliciet ontkennen aan het eind van elke gecreëerde regel.



Opmerking: In dit scenario zal al het verkeer van PC2 toegang tot het netwerk worden verleend. Al het andere verkeer van andere hosts wordt ontkend.

Doel

Dit artikel heeft als doel u te tonen hoe u een IPv4 ACL op een WAP125 en WAP581 access point kunt configureren.

Toepasselijke apparaten

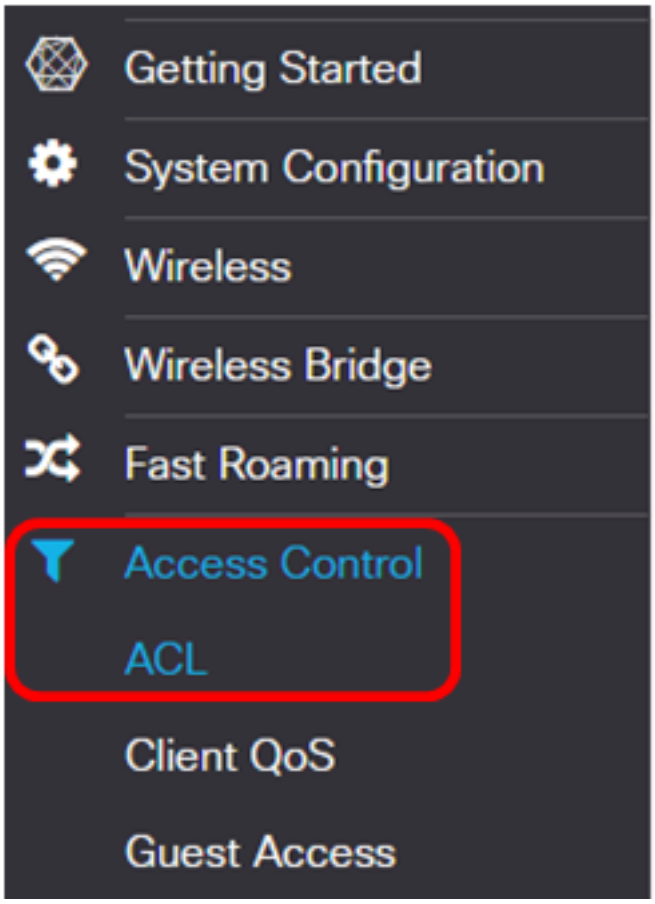
- WAP125
- WAP581

Softwareversie

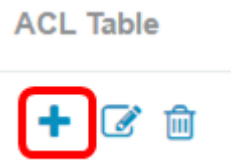
- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

Een IPv4 ACL configureren

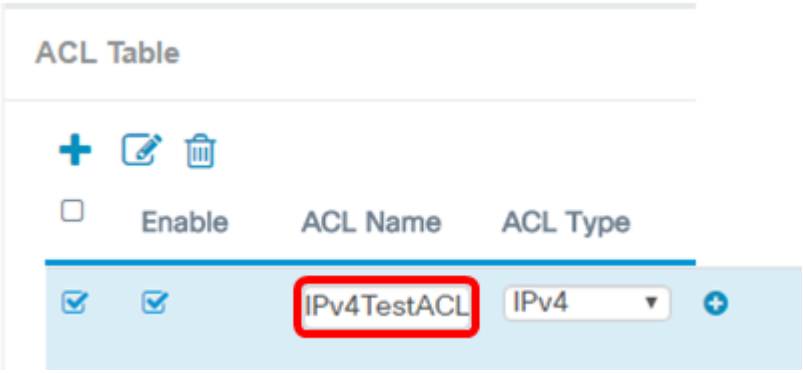
Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van WAP en kies **toegangscontrole > ACL**.



Stap 2. Klik op de + knop om een nieuwe ACL te maken.

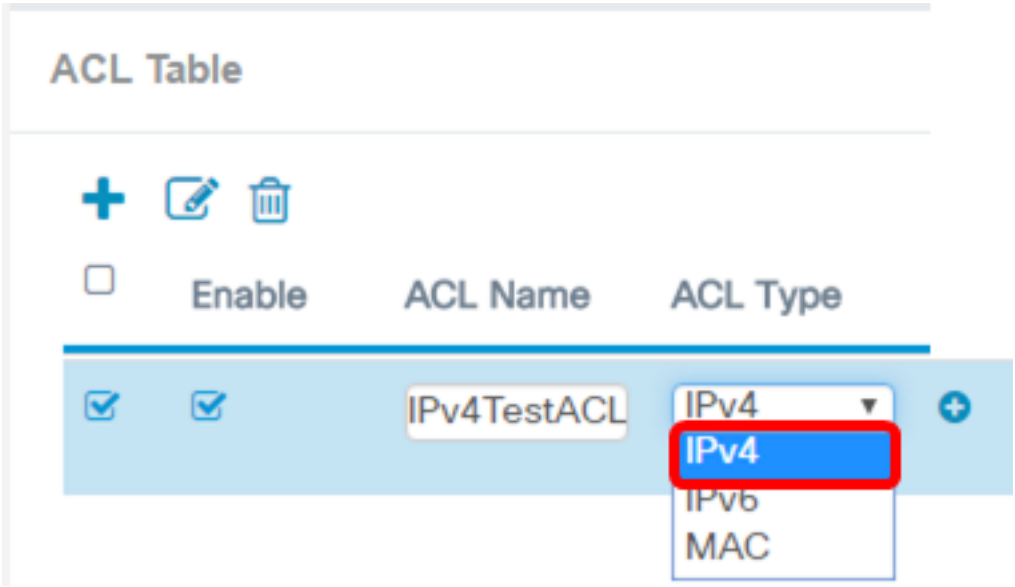


Stap 3. Voer een naam voor ACL in het veld *ACL-naam* in.



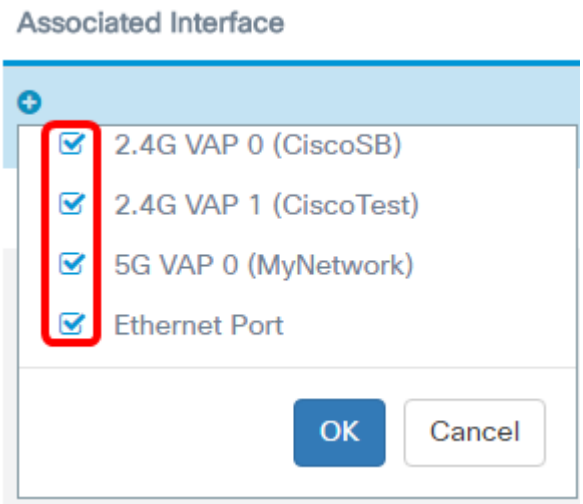
Opmerking: In dit voorbeeld wordt IPv4TestACL ingevoerd.

Stap 4. Kies IPv4 uit de vervolgkeuzelijst ACL-type.



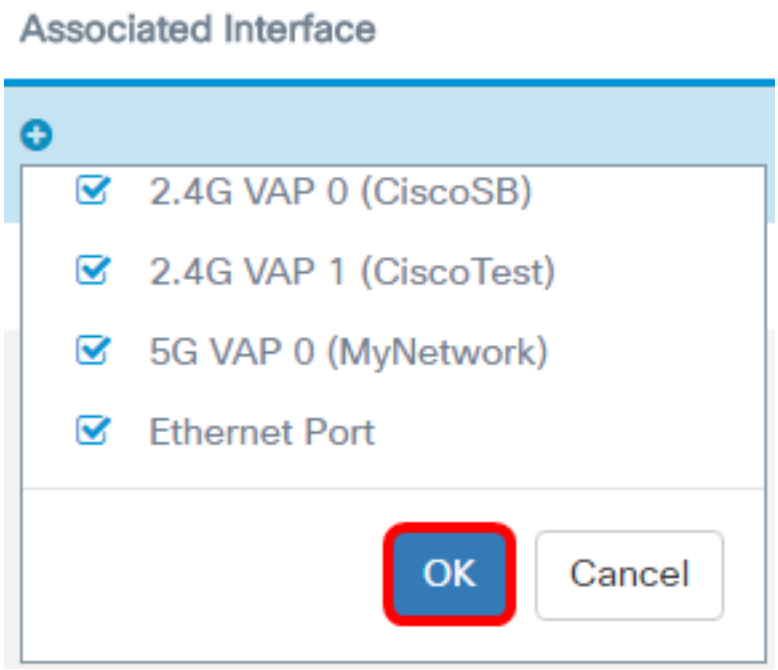
Stap 5. Klik op de knop en kies een interface in de vervolgkeuzelijst Geassocieerde interface. De opties zijn:

- 2.4G VAP 0 (SSID Name) — Deze optie zal MAC ACL toepassen op het 2.4 GHz Virtual Access Point (VAP). Het gedeelte SSID Name kan afhankelijk van de SSID naam in de WAP worden ingesteld.
- 5G VAP0 (SSID Name) — Deze optie zal MAC ACL toepassen op de 5 GHz VAP.
- Ethernet Port - Deze optie zal MAC ACL op de Ethernet-interface van WAP toepassen.



Opmerking: Meervoudige interfaces kunnen aan een ACL worden gekoppeld. Dit kan echter niet worden gekoppeld aan een ACL wanneer deze al is gekoppeld aan een andere ACL. In dit voorbeeld worden alle interfaces gekoppeld aan IPv4TestACL. Schakel het vakje uit om de interface van de ACL te verwijderen.

Stap 6. Klik op **OK**.

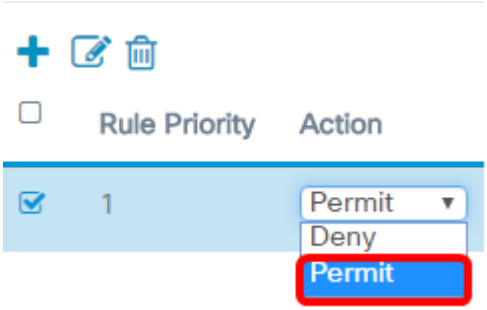


Stap 7. Klik op de knop **Meer...** om de parameters van ACL te configureren.

Stap 8. Klik op de + knop om een nieuwe regel toe te voegen.

Stap 9. Kies een actie uit de vervolgkeuzelijst Actie. De opties zijn:

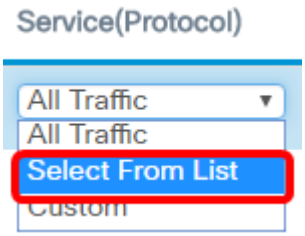
- Toestemming - Deze optie laat pakketten toe die overeenkomen met de ACL-criteria om aan het netwerk te verbinden.
- Jeans: deze optie voorkomt dat pakketten die overeenkomen met de ACL-criteria, op het netwerk worden aangesloten.



Opmerking: In dit voorbeeld wordt de Vergunning gekozen.

Stap 10. Kies een service- of protocol dat moet worden gefilterd uit de vervolgkeuzelijst Service (Protocol). De opties zijn:

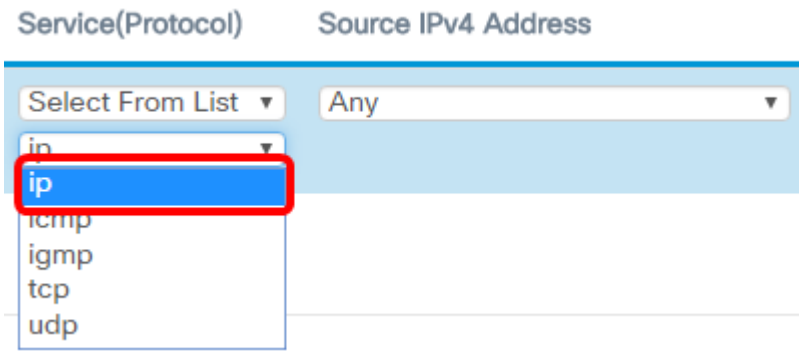
- Alle verkeer - Deze optie behandelt alle pakketten als een overeenkomst met het ACL-filter.
- Selecteer vanuit Lijst - Met deze optie kunt u IP, ICMP, IGMP, TCP of UDP als filters voor ACL kiezen. Als deze optie is geselecteerd, gaat u naar Stap 11.
- Aangepast - met deze optie kunt u een aangepaste protocol-ID als een filter voor de pakketten invoeren. De waarde is een viercijferig hexadecimaal nummer. Het bereik is 0 tot 255.



Opmerking: In dit voorbeeld wordt Select Van List geselecteerd.

Stap 1. Bepaal het protocol dat op het netwerk moet kunnen worden aangesloten. De opties zijn:

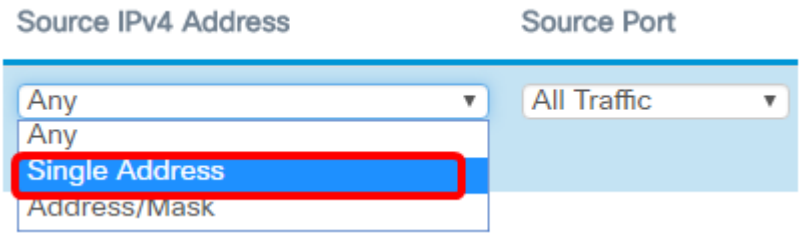
- ip — Met deze optie laat de filter van het toegangspunt de hosts die toegang tot het netwerk hebben, gebruik maken van hun IP-adres als filter.
- ICMP —Deze optie laat de pakketten Internet Control Message Protocol (ICMP), het toegangspoint, dat het netwerk via het toegangspunt invoert, in.
- igmp — Deze optie laat de pakketten Internet Group Management Protocol (IGMP) van het toegangspunt filter binnen in het netwerk via het access point.
- TCP — Deze optie laat de TCP-pakketten (Access Point Filter Transmission Control Protocol) die het netwerk via het access point invoeren.
- udp — Deze optie laat de pakketten met het toegangsknooppunt en het toegangsknooppunt van het filter User Datagram Protocol (UDP) invoeren die het netwerk via het access point invoeren.



Opmerking: In dit voorbeeld wordt ip gekozen.

Stap 12. Defineer het Bron IPv4-adres uit de vervolgkeuzelijst Bron IPv4-adres. De opties zijn:

- Alle — Met deze optie kan WAP het filter op pakketten van een IP-adres toepassen.
- Eén adres - met deze optie kan WAP het filter op pakketten van een bepaald IP-adres toepassen.
- Adres/masker - Deze optie laat WAP het filter op pakketten op een IP-adres en het masker van de IP toepassen.



Opmerking: In dit voorbeeld wordt één adres gekozen.

Stap 13. Voer het IP-adres van de host in dat moet worden toegestaan bij de toegang tot het netwerk.

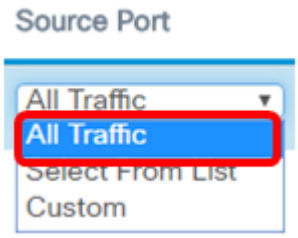
Opmerking: In dit voorbeeld wordt 192.168.100.139 opgenomen. Dit is het IP adres van PC2.

Stap 14. Kies een bronpoort voor de voorwaarde. De opties zijn:

- Alle verkeer - Deze optie staat alle pakketten van de bronpoort toe die aan de criteria voldoen.
- Selecteer vanuit Lijst — Met deze optie kun je ftp, ftpdata, http, smtp, snmp, telnet, tftp en www kiezen.
- Aangepast - met deze optie kunt u een IANA-poortnummer invoeren dat overeenkomt met de bronpoort die in de datagram-kop is geïdentificeerd. Het poortbereik loopt van 0 tot 65535 en omvat het volgende:

- 0 tot 1023 — bekende havens

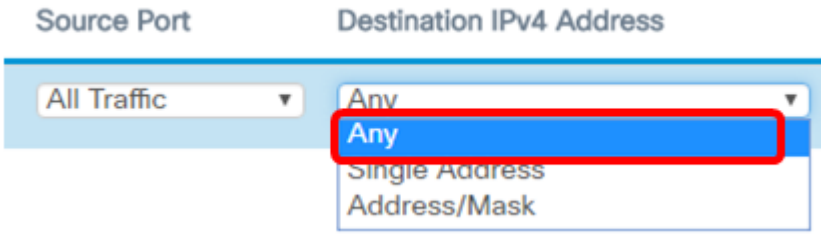
- 1024-49151 — geregistreerde poorten
- 49152 — 65535 — Dynamische en/of particuliere havens



Opmerking: In dit voorbeeld wordt al het verkeer geselecteerd.

Stap 15. Kies een doeladres in de vervolgkeuzelijst IPv4-adres van de bestemming. De opties zijn:

- Om het even welk — Deze optie behandelt om het even welk IP adres als overeenkomend met de ACL verklaring.
- Single Address — Met deze optie kunt u een specifiek IP-adres voor de ACL-voorwaarde invoeren.
- Adres/masker - Met deze optie kunt u een IP-adresbereik of -masker invoeren.



Opmerking: In dit voorbeeld wordt AnyRes gekozen.

Stap 16. Kies een doelpoort in de vervolgkeuzelijst Doelpoort. De opties zijn:

- Om het even welk - Deze optie behandelt alle bestemmingspoorten van de pakketten als een overeenkomst met de verklaring in ACL.
- Selecteer vanuit lijst — Met deze optie kunt u een trefwoord kiezen dat gekoppeld is aan de doelpoort. De opties zijn: ftp , ftpdata , http, smtp, snmp, telnet, tftp en www. Deze zoekwoorden vertalen naar hun corresponderende poortnummers.
- Aangepast - met deze optie kunt u een IANA-poortnummer invoeren dat overeenkomt met de bronpoort die in de datagram-kop is geïdentificeerd. Het poortbereik loopt van 0 tot 65535 en omvat het volgende:

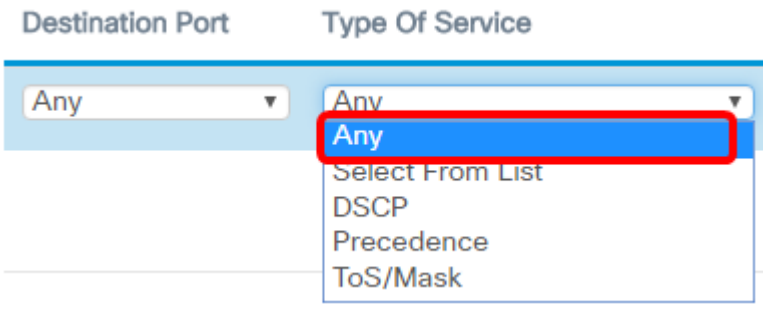
  - 0 tot 1023 — bekende havens
  - 1024-49151 — geregistreerde poorten
  - 49152 — 65535 — Dynamische en/of particuliere havens

Stap 17. Kies een type service dat overeenkomt met het pakkettype in de vervolgkeuzelijst Type service. De opties zijn:

- Alle — Deze optie behandelt elke service als een overeenkomst voor de pakketten.
- Selecteer vanuit Lijst - Deze optie komt overeen met de pakketten die zijn gebaseerd op hun waarden voor Gedifferentieerde Services Code Point, (DSCP), Class of Service (CoS) of Extended Forwarding (EF).
- DSCP - De optie komt overeen met de pakketten die zijn gebaseerd op hun aangepaste

DSCP-waarde. Wanneer u deze optie kiest, voert u een waarde van 0 tot 63 in het veld DSCP-waarde in.

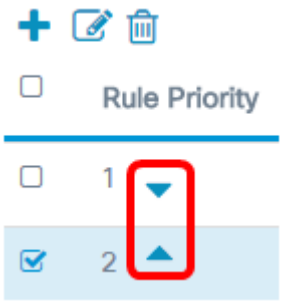
- voorrang - Deze optie komt overeen met de pakketten die zijn gebaseerd op hun IP-prioriteitswaarde. Als deze optie is geselecteerd, voert u een IP-voorrang in van 0 tot 7.
- ToS/masker - Met deze optie kunt u een IP ToS-masker invoeren om de bitposities in de waarde van IP Tos Bits te identificeren die voor vergelijking tegen het veld IP ToS in een pakket worden gebruikt.



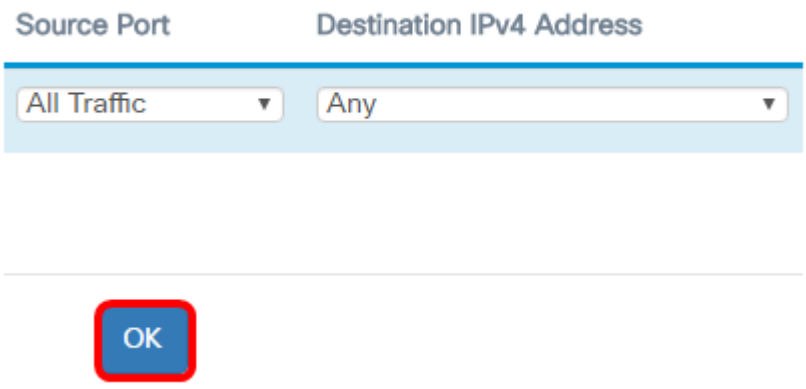
Stap 18. (Optioneel) Herhaal Stap 8 naar Stap 17 totdat de ACL is voltooid.

Opmerking: Aangezien er een impliciet ontkennen is aan het eind van elke gecreëerd regel, is er geen behoefte om een ontkenningsregel aan ACL toe te voegen om toegang van andere apparaten in het netwerk te verhinderen.

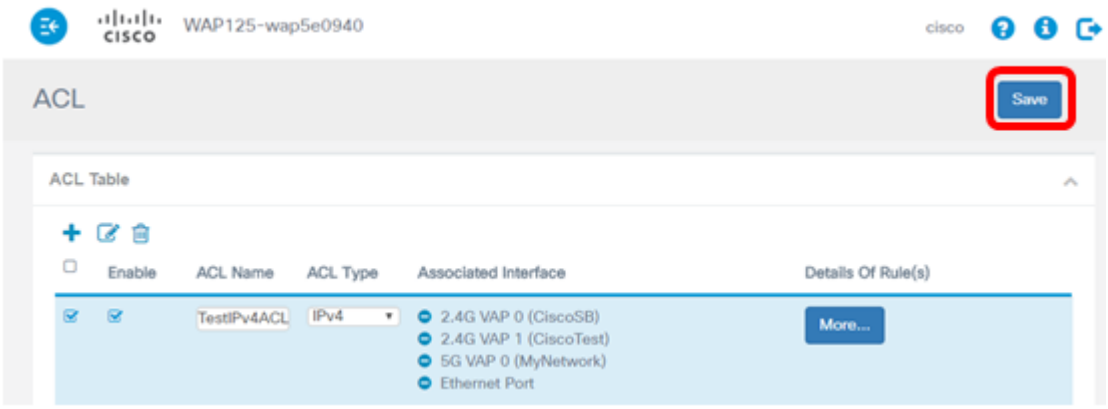
Stap 19. (Optioneel) Verander de volgorde van de voorwaarden op de ACL door op de knoppen omhoog en omlaag te klikken totdat deze in de juiste volgorde zijn.



Stap 20. Klik op **OK**.



Stap 21. Klik op **Opslaan**.



U dient nu een IPv4 ACL te hebben ingesteld die slechts één host in staat zou stellen om het netwerk te bereiken wanneer het wordt aangesloten op WAP.