ACL-lijnconfiguratie op WAP371

Doel

Een controlelijst voor netwerktoegang (ACL) is een optionele laag beveiliging die fungeert als een firewall voor het besturen van verkeer in en uit een netwerk. Toegangslijsten zijn collecties van vergunningen en ontkenningsvoorwaarden, of regels, die om een aantal redenen veiligheid bieden. Deze regels kunnen bijvoorbeeld niet-geautoriseerde gebruikers blokkeren, geautoriseerde gebruikers toegang geven tot specifieke bronnen en ongerechtvaardigde pogingen blokkeren om netwerkbronnen te bereiken.

Het doel van dit document is om u te tonen hoe u ACL-regels op WAP 371 moet configureren.

Toepasselijke apparaten

- WAP371

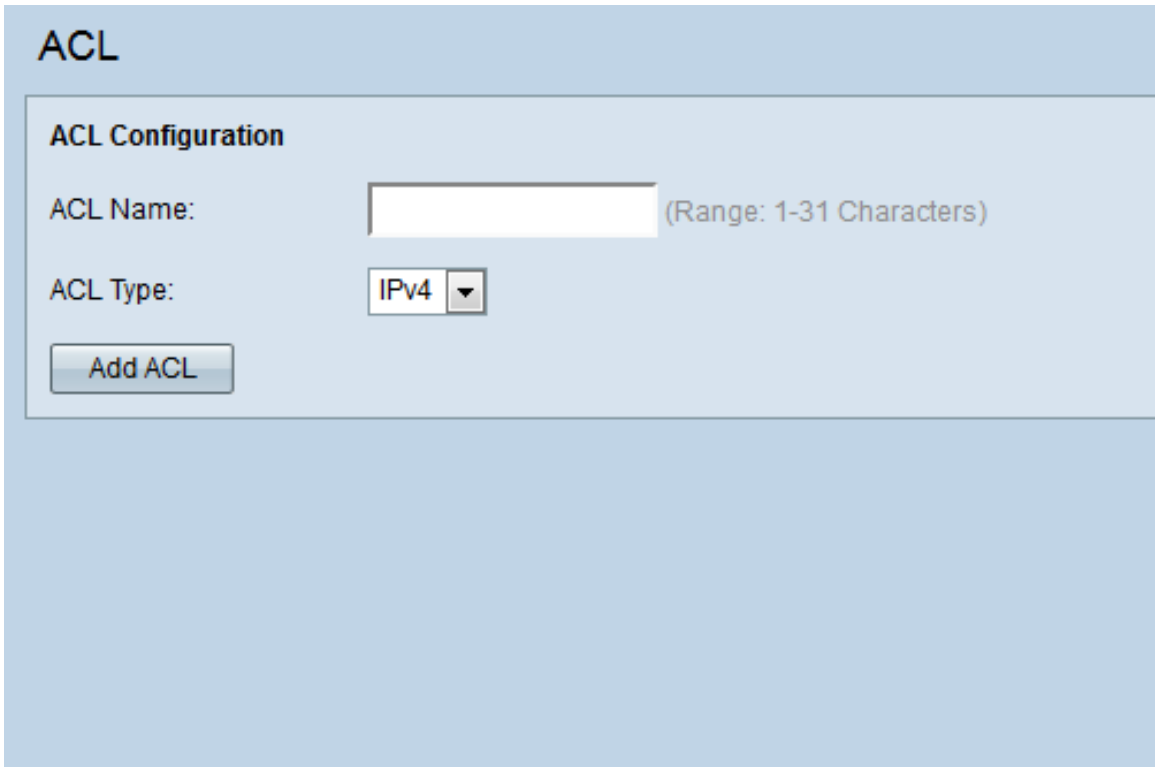
Softwareversie

- v1.2.0.2

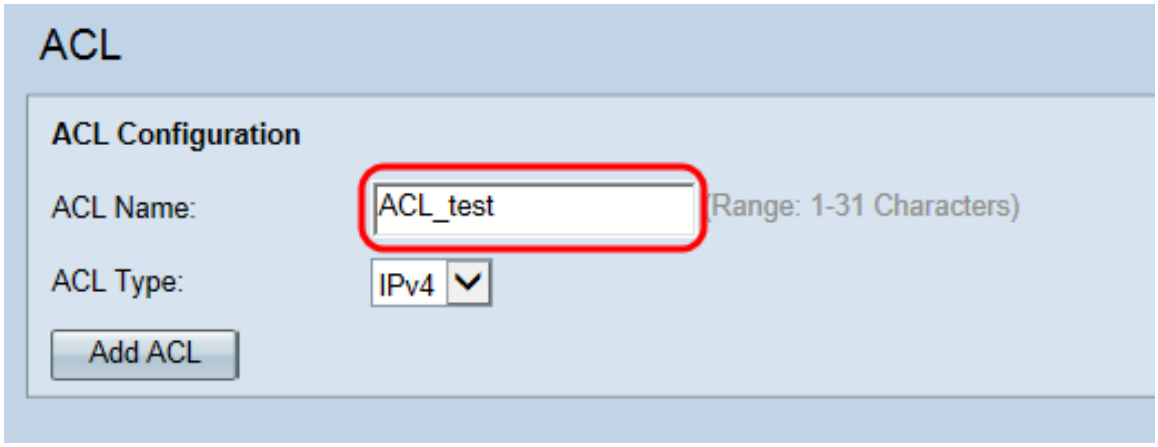
Configuratie van ACL-regels

ACL-configuratie

Stap 1. Meld u aan bij het web configuratieprogramma en kies **client-QoS > ACL**. De *ACL*-pagina wordt geopend:

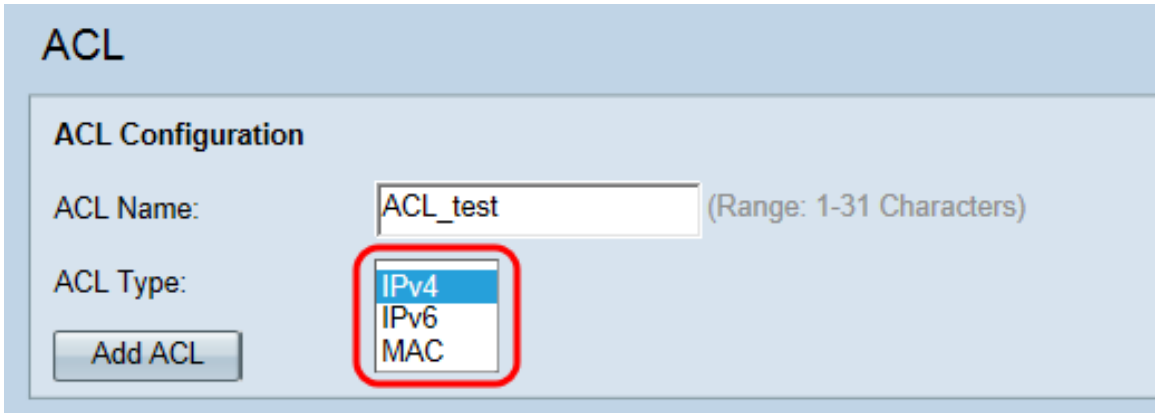


Stap 2. Voer de gewenste ACL-naam in het veld *ACL-naam* in. Het bereik bestaat uit 1-31 tekens.



Opmerking: De ACL-naam is een identificatiemiddel voor de specifieke ACL; het heeft geen invloed op de werking van het apparaat .

Stap 3. Selecteer het ACL-type in de vervolgkeuzelijst *ACL-type*.

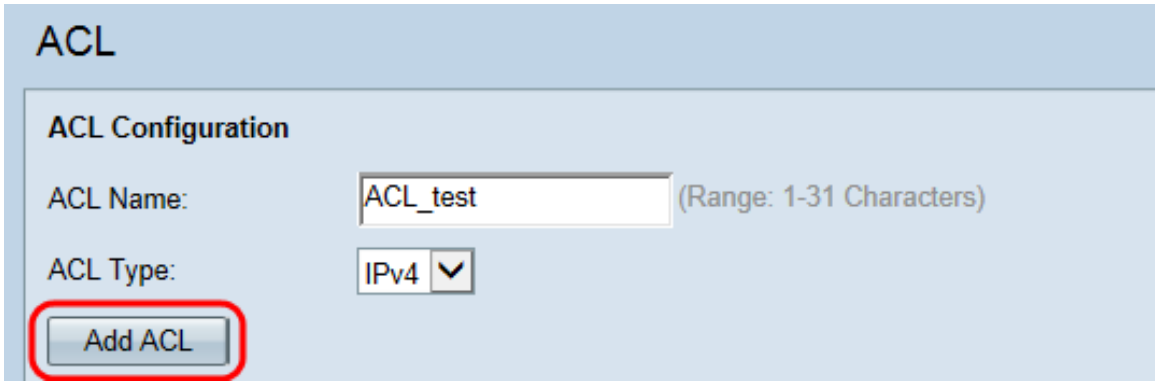


De opties zijn als volgt:

- IPv4 - A 32-bits (vier bytes) adres.
- IPv6 - Een opvolger van IPv4, bestaat uit een 128-bits (8 bytes) adres.
- MAC - Het MAC-adres is het unieke adres dat aan een netwerkinterface is toegewezen.

Opmerking: IPv4- en IPv6-ACL's controleren de toegang tot netwerkbronnen op basis van Layer 3 en Layer 4-criteria. MAC ACL's controleren toegang op basis van Layer 2-criteria.

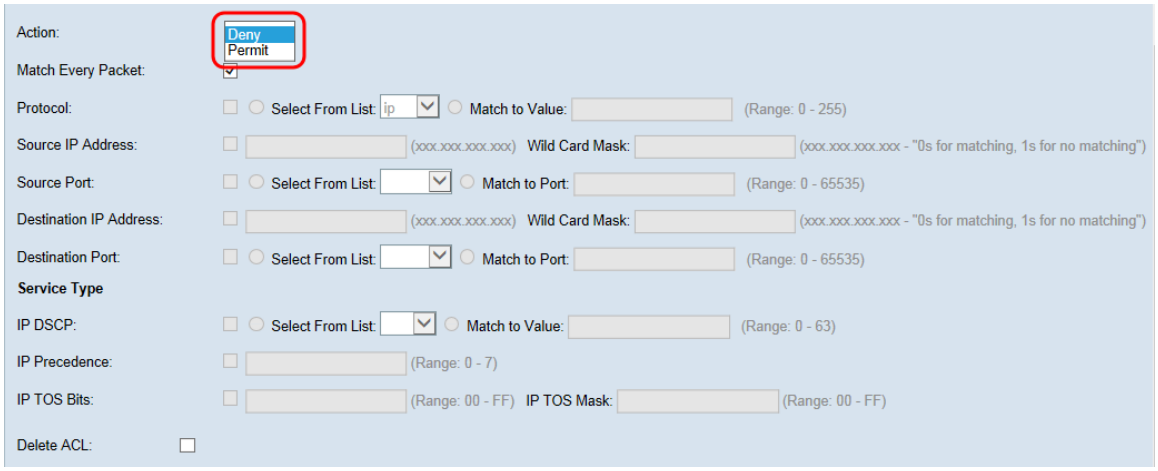
Stap 4. Klik op **Add ACL** om de nieuwe ACL's toe te voegen.



ACL-lijnconfiguratie voor IPv4 en IPv6

Opmerking: De volgende screenshots zijn voor IPv4 ACL-regels maar zijn uitwisselbaar met IPv6 ACL-regels.

Stap 1. Selecteer een actie voor de regel in de vervolgkeuzelijst *Action*.

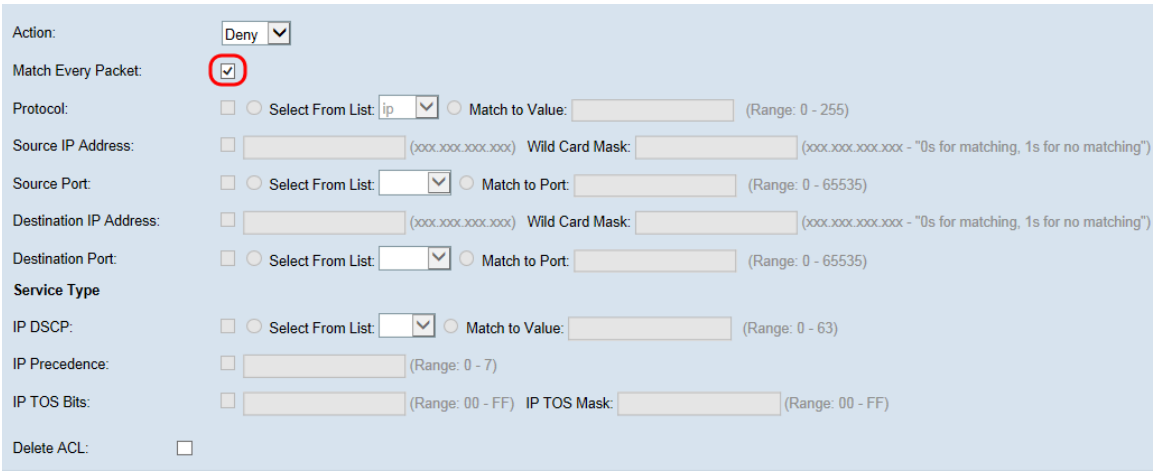


De opties worden als volgt beschreven:

- Vergunning - De regel staat al verkeer dat aan de lijncriteria voldoet toe om het WAP apparaat in te gaan of te verlaten. Verkeersverkeer dat niet aan de criteria voldoet, wordt geschrapt.

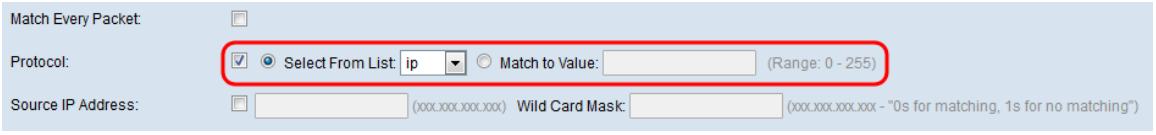
- Jeans: de regel blokkeert al het verkeer dat aan de standaardcriteria voldoet om het WAP-apparaat in te voeren of te verlaten. Verkeersverkeer dat niet aan de criteria voldoet wordt naar de volgende regel doorgestuurd. Als dit de laatste regel is, wordt het verkeer dat niet expliciet wordt toegestaan ingetrokken.

Stap 2. Controleer of koppel de selectieknop **bij elk pakket** los. Indien geselecteerd, past de regel, die of een vergunning of ontkent actie, het kader of het pakket ongeacht zijn inhoud aan.



Opmerking: Als u dit veld selecteert, kunt u geen extra matchcriteria instellen. De optie **Elke pakket aanpassen** is standaard voor een nieuwe regel geselecteerd. U moet de optie uitschakelen om andere overeenkomende velden te configureren.

Stap 3. Controleer het selectieteken **Protocol** om een L3 of L4 protocol-matchvoorwaarde te gebruiken die is gebaseerd op de waarde van het veld IP Protocol in IPv4-pakketten of het veld Volgende header in IPv6-pakketten. Selecteer een van de volgende knoppen als het vakje Protocol is ingeschakeld.



De opties worden als volgt beschreven:

- Selecteer vanuit lijst — Kies een protocol in de vervolgkeuzelijst *Lijst*. De opties zijn als volgt:

  - IP - Het Internet Protocol (IP) is het belangrijkste communicatieprotocol in het Internet Protocol Suite voor het doorgeven van gegevens via netwerken.

  - ICMP - Het Internet Control Message Protocol (ICMP) is een protocol in het Internet Protocol Suite dat door apparaten zoals routers wordt gebruikt om foutmeldingen te verzenden.

  - IGMP - Het Internet Group Management Protocol (IGMP) is een communicatieprotocol dat door host wordt gebruikt om multicast groeplidmaatschap op IPv4-netwerken op te zetten.

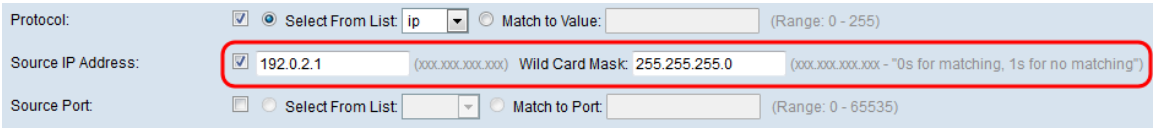
  - TCP - Het Transmission Control Protocol (TCP) stelt twee hosts in staat een verbinding te maken en gegevensstromen uit te wisselen.

  - UDP - Het User Datagram Protocol is een protocol in de Internet Protocol Suite dat gebruik maakt van een transmissiemodel zonder verbinding.

- Overeenkomend met waarde - Voer een standaard IANA-toegewezen protocol-ID in die van 0 tot 255 varieert voor alle niet-genoemde protocollen. Raadpleeg de *Toegewezen Internet Protocol Nummers* voor meer informatie over de door IANA toegewezen protocol-ID's.

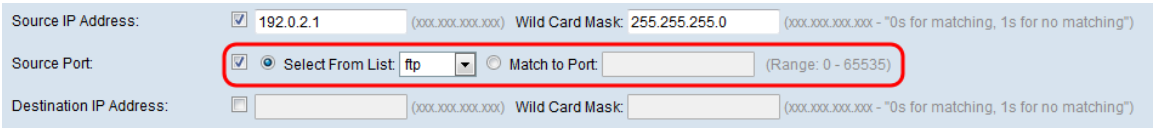
Stap 4. Controleer het selectieteken **IP-adres** van de **bron** om een IP-adres van de bron in

de matchomstandigheden op te nemen. Voer het IP-adres en het wild kaartmasker van de bron in hun respectievelijke velden in. Het wild kaartmasker bepaalt welke bits van het bronadres worden gebruikt en welke worden genegeerd. Het kan worden gezien als een omgekeerd SUBNET masker. Dit is nuttig om de grootte van een netwerk of van Subnet voor sommige routingprotocollen aan te geven of een bereik van IP adressen toe te staan of te ontkennen.



Opmerking: Het veld Veldkaartmasker is vereist als het selectieteken **IP-adres** van **bron** is ingeschakeld.

Stap 5. Controleer het selectieteken **van de Bron** om een bronpoort in de matchvoorwaarde te omvatten. Als het selectieknop **Source Port** is ingeschakeld, selecteert u een van de volgende radioknoppen.



De opties worden als volgt beschreven:

- Selecteer vanuit lijst — Kies een bronpoort in de vervolgkeuzelijst *Lijst*. De opties zijn als volgt:

  - FTP - Het File Transfer Protocol (FTP) is een standaardnetwerkprotocol dat wordt gebruikt om bestanden van de ene host naar de andere over een TCP-gebaseerd netwerk zoals het internet over te brengen.

  - FTP gegevens - Een gegevenskanaal dat door de server wordt geïnitieerd die op een client is aangesloten, doorgaans via poort 20.

  - HTTP - Het Hypertext Transfer Protocol (HTTP) is een toepassingsprotocol dat de basis vormt voor datacommunicatie voor het World Wide Web.

  - MTP - Het Simple Mail Transfer Protocol (MTP) is een Internet-standaard voor e-mailtransmissie.

  - SNMP - The Simple Network Management Protocol (SNMP) is een Internet-standaardprotocol voor het beheer van apparaten op IP-netwerken.

  - Telnet - Een protocol op de sessielaag dat op het internet of op lokale netwerken wordt gebruikt om bidirectionele interactieve tekstgeoriënteerde communicatie te bieden.

  - TFTP - Het Trivial File Transfer Protocol (TFTP) is een Internet software-hulpprogramma voor het overdragen van bestanden die eenvoudiger te gebruiken zijn dan FTP, maar minder geschikt.

  - WW - Het World Wide Web is een systeem van Internet servers die documenten ondersteunen die zijn geformatteerd op HTTP.

- Stem aan poort — Voer het poortnummer in dat varieert van 0 tot 65535 in het veld *Overeenkomend met Port* voor niet-beursgenoteerde bronpoorten. Het bereik omvat drie

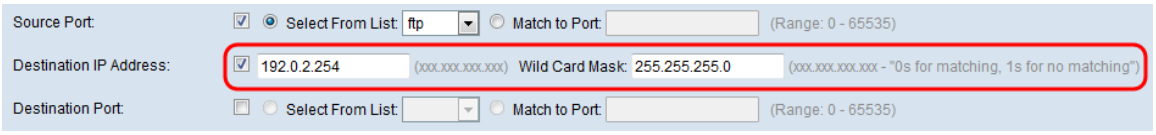
verschillende soorten havens. De marges worden als volgt beschreven:

- 0 tot 1023 — bekende havens.

- 1024 tot en met 49151 — Geregistreerde havens.

- 49152 tot en met 65535 — Dynamische en/of particuliere havens.

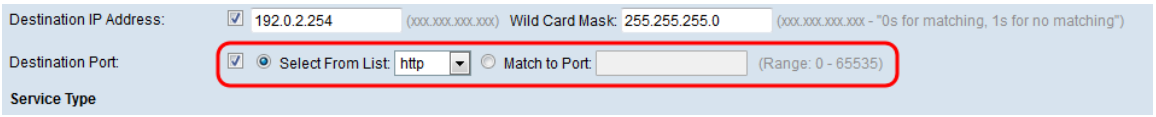
Stap 6. Controleer het selectieteken **IP-adres** van de **bestemming** om het IP-adres van de bestemming in de overeenkomstenvoorwaarde op te nemen. Voer het IP-adres en het wild kaartmasker van de bestemming in hun respectievelijke velden in. Het wild kaartmasker bepaalt welke bits van het bronadres worden gebruikt en welke worden genegeerd. Het kan worden gezien als een omgekeerd SUBNET masker. Dit is nuttig om de grootte van een netwerk of van Subnet voor sommige routingprotocollen aan te geven of een bereik van IP adressen toe te staan of te ontkennen.



Opmerking: Het veld *Kaartmasker* is vereist als het selectieteken **IP-adres** van **bestemming** is ingeschakeld.

Opmerking: Als u slechts één IP-adres wilt weergeven, gebruikt u het masker van 0,0.0.0 van de wild-kaart.

Stap 7. Controleer het selectieteken **van de** Doelpoort om een doelpoort in de matchconditie op te nemen. Als het vakje **Destination Port** is ingeschakeld, selecteert u een van de volgende radioknoppen.



De opties worden als volgt beschreven:

- Selecteer vanuit lijst — Kies een doelpoort in de vervolgkeuzelijst *Lijst*. De vervolgkeuzelijst bevat de volgende opties:

  - FTP - Het File Transfer Protocol (FTP) is een standaardnetwerkprotocol dat wordt gebruikt om bestanden van de ene host naar de andere over een TCP-gebaseerd netwerk zoals het internet over te brengen.

  - FTP gegevens - Een gegevenskanaal dat door de server wordt geïnitieerd die op een client is aangesloten, doorgaans via poort 20.

  - HTTP - Het Hypertext Transfer Protocol (HTTP) is een toepassingsprotocol dat de basis vormt voor datacommunicatie voor het World Wide Web.

  - MTP - Het Simple Mail Transfer Protocol (MTP) is een Internet-standaard voor e-mailtransmissie.

  - SNMP - The Simple Network Management Protocol (SNMP) is een Internet-standaardprotocol voor het beheer van apparaten op IP-netwerken.

- Telnet - Een protocol op de sessielaag dat op het internet of op lokale netwerken wordt gebruikt om bidirectionele interactieve tekstgeoriënteerde communicatie te bieden.

- TFTP - Het Trivial File Transfer Protocol (TFTP) is een Internet software-hulpprogramma voor het overdragen van bestanden die eenvoudiger te gebruiken zijn dan FTP, maar minder geschikt.

- WW - Het World Wide Web is een systeem van Internet servers die documenten ondersteunen die zijn geformatteerd op HTTP.

- Stem aan poort — Voer het poortnummer in dat varieert van 0 tot 65535 in het veld *Overeenkomend met Port* voor niet-genoemde doelpoorten. Het bereik omvat drie verschillende soorten havens. De marges worden als volgt beschreven:

- 0 tot 1023 — Goed bekende poorten.

- 1024 tot en met 49151 — geregistreerde poorten.

- 49152 tot en met 65535 — Dynamische en/of particuliere poorten.

Opmerking: Slechts één van de services kan worden geselecteerd in het gedeelte Service Type (servicetype) en kan worden toegevoegd voor de matchvoorwaarde.

Configuratie van ACL-servicetype voor IPv4

Stap 1. Controleer het **IP DSCP**-selectieteken om de pakketten aan te passen die op IP DSCP-waarden zijn gebaseerd. DSCP wordt gebruikt om de verkeersprioriteiten in de IP-header van het kader te specificeren. Dit categoriseert alle pakketten voor de geassocieerde verkeersstroom met de IP DSCP waarde die u uit de lijst selecteert. Als het IP DSCP-selectieknop is ingeschakeld, selecteert u een van de volgende radioknoppen.

De opties worden als volgt beschreven:

- Selecteer vanuit lijst — Kies een IP DSCP-waarde in de vervolgkeuzelijst *Selecteer vanuit Lijst*. De opties zijn als volgt:

- DSCP Assurance Forwarding (AS) - Hiermee kan de exploitant de levering garanderen zolang het verkeer niet een bepaald bedrag overschrijdt.

- Serviceklasse (CS) - hiermee kan de compatibiliteit worden verbeterd met netwerkapparaten die nog steeds het veld voorrang gebruiken.

- Snelated Forwarding (EF) - Gebruikt om een laag verlies, lage latentie, lage jitter, gegarandeerde bandbreedte, end-to-end service via DS (DiffServ)-domeinen te bouwen.

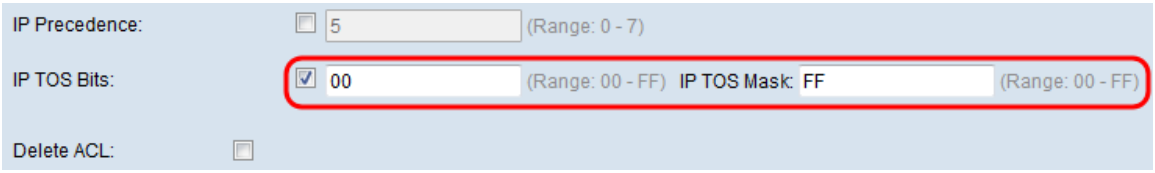
- Overeenkomend met waarde — Voer de DSCP-waarde in die van 0 tot 63 in het veld *Overeenkomend met Waarde* om DSCP-waarden aan te passen.

Opmerking: Raadpleeg *DSCP- en prioriteitswaarden* voor meer informatie over DSCP.

Stap 2. Controleer het selectieteken van het **IP-voorrang** om een IP-voorrang-waarde in de matchomstandigheden op te nemen. Dit is een mechanisme om een prioriteit aan elk IP pakket toe te wijzen waar 0 de laagste prioriteit is en 7 de hoogste prioriteit is. Als het selectieteken **IP** voorrang hebben ingeschakeld, voert u een IP-voorrang in die van 0 tot 7 varieert.

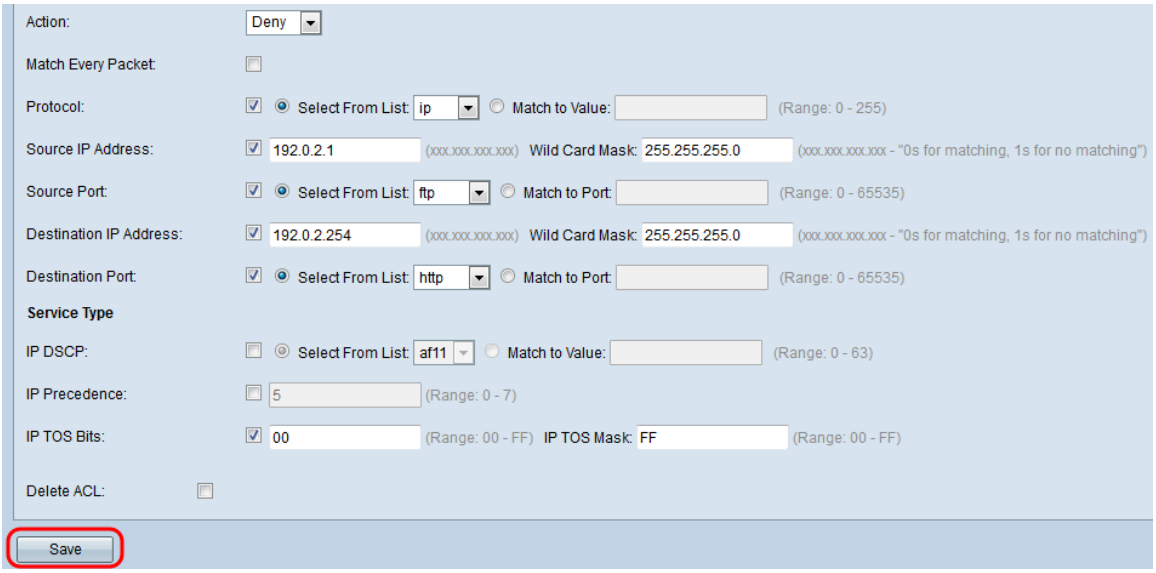
Opmerking: Raadpleeg *DSCP- en* prioriteitswaarden voor meer informatie over de IP-voorrang.

Stap 3. Controleer het selectieteken **IP TOS**-bits om de bits Type of Service (TOS) van het pakket in de IP-kop als overeenkomende criteria te gebruiken. Een TOS-veld wordt gebruikt om de prioriteit van een datagram op te geven en het dienovereenkomstig te routeren. Als het IP TOS-selectieteken is ingeschakeld, voert u de IP TOS-bits in die variëren van 00-FF- en IP TOS-masker, dat in hun respectievelijke velden varieert van 00-FF.



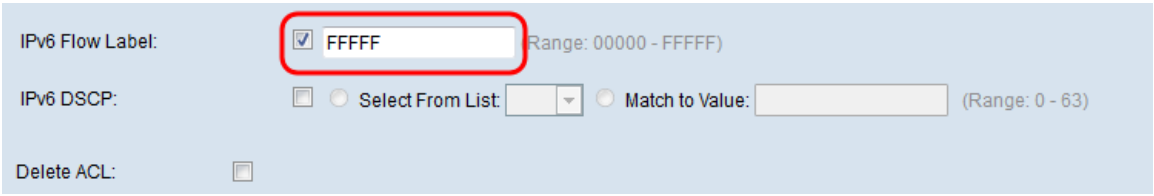
Stap 4. (Optioneel) Als u de ingesteld ACL wilt verwijderen, controleert u het selectieteken **ACL**-code **verwijderen**.

Stap 5. Klik op **Opslaan** om de instellingen op te slaan.

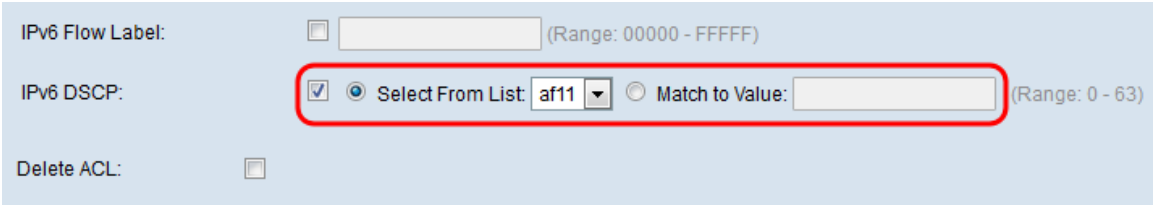


ACL-lijnconfiguratie voor IPv6

Stap 1. Controleer het **IPv6 Flow Label** selectieteken om een 20-bits getal in te stellen dat uniek is voor een IPv6-pakket. Het wordt gebruikt door eindstations om QoS-bewerking in routers (bereik 0 tot 1048575) te herkennen.



Stap 2. Controleer het **IPv6 DSCP-**selectieteken om de pakketten aan te passen die op IP DSCP-waarden zijn gebaseerd. DSCP wordt gebruikt om de verkeersprioriteiten in de IP-header van het kader te specificeren. Dit categoriseert alle pakketten voor de geassocieerde verkeersstroom met de IP DSCP waarde die u uit de lijst selecteert. Als het selectieknop **IPv6 DSCP** is ingeschakeld, selecteert u een van de volgende radioknoppen.



De opties worden als volgt beschreven:

- Selecteer vanuit lijst — Kies een IP DSCP-waarde in de vervolgkeuzelijst *Selecteer vanuit Lijst*. De opties zijn als volgt:

  - DSCP Assurance Forwarding (AS) - stelt de exploitant in staat een leveringszekerheid te bieden zolang het verkeer niet een bepaald geplaatste tarief overschrijdt.

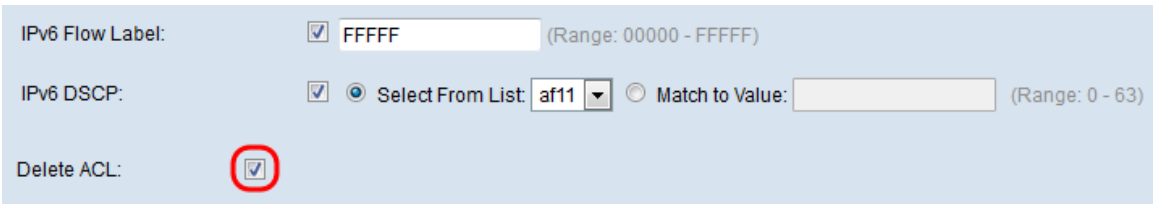
  - Serviceklasse (CS) - maakt achterwaartse compatibiliteit met netwerkapparaten mogelijk die nog steeds het veld voorrang gebruiken.

  - Snelated Forwarding (EF) - wordt gebruikt om een laag verlies-, lage latentie-, lage bandbreedte-, end-to-end service via DS (DiffServ)-domeinen te bouwen.

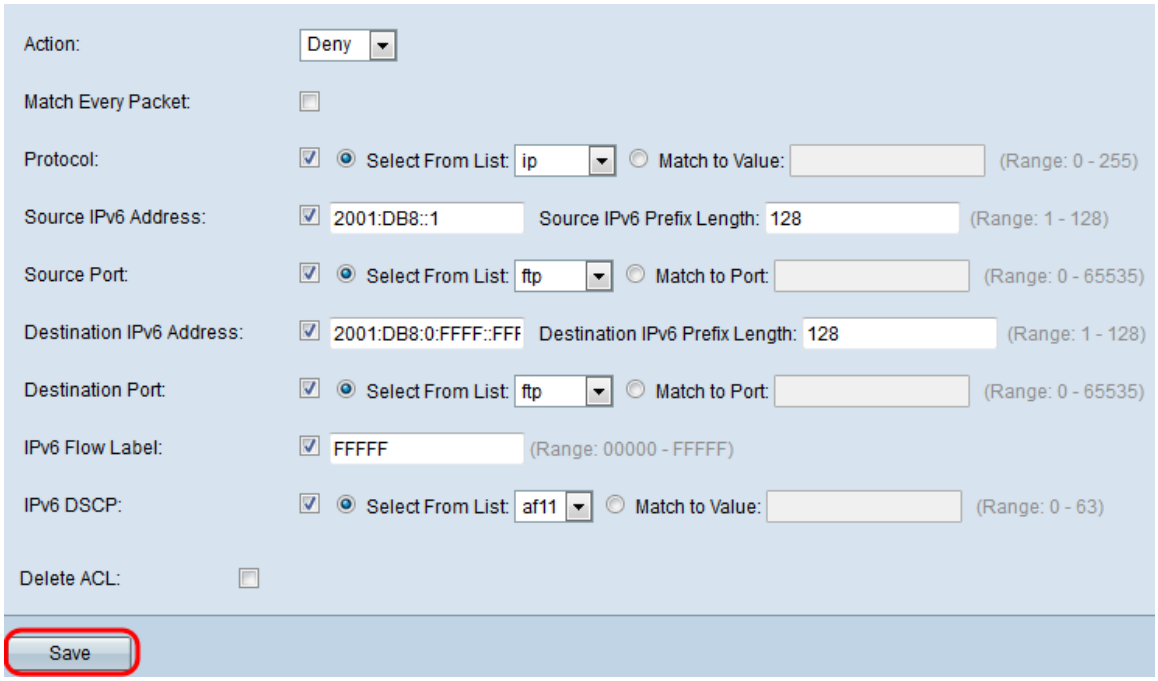
- Overeenkomend met waarde — Voer de DSCP-waarde in die van 0 tot 63 in het veld *Overeenkomend met Waarde* om DSCP-waarden aan te passen.

Opmerking: Raadpleeg *DSCP- en* prioriteitswaarden voor meer informatie over DSCP.

Stap 3. (Optioneel) Als u de ingesteld ACL wilt verwijderen, controleert u het selectieteken **ACL-**code **verwijderen**.

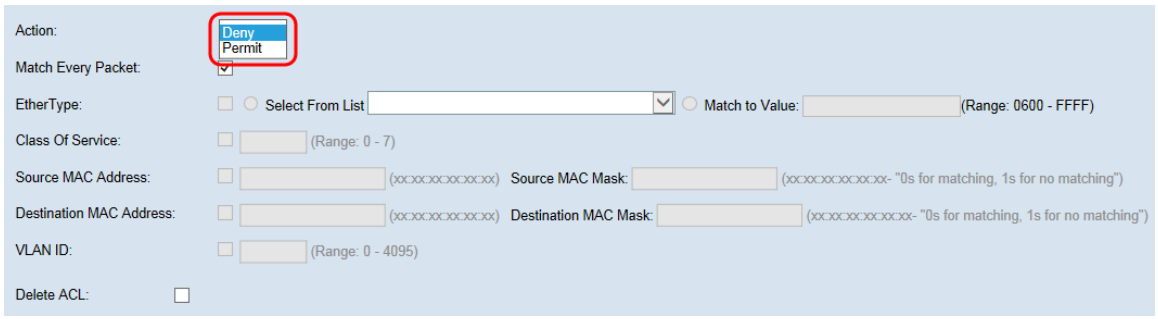


Stap 4. Klik op **Opslaan** om de instellingen op te slaan.



ACL-lijnconfiguratie voor MAC

Stap 1. Selecteer een actie voor de regel in de vervolgkeuzelijst *Action*.

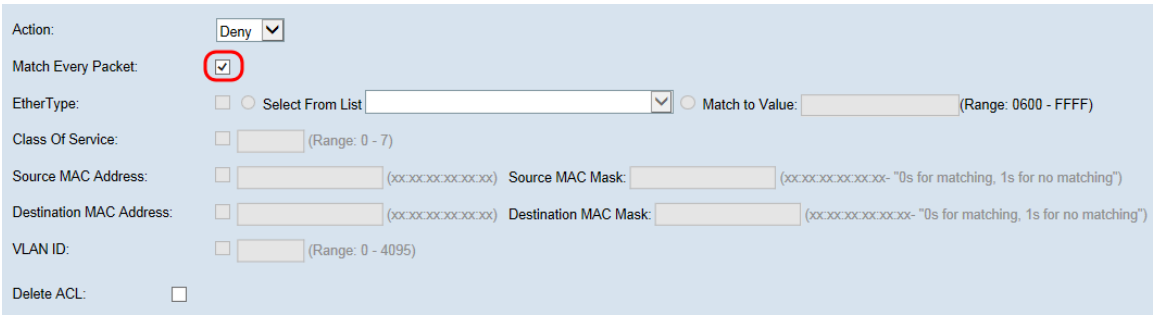


De opties worden als volgt beschreven:

- Vergunning - De regel staat al verkeer dat aan de lijncriteria voldoet toe om het WAP apparaat in te gaan of te verlaten. Verkeersverkeer dat niet aan de criteria voldoet, wordt geschrapt.

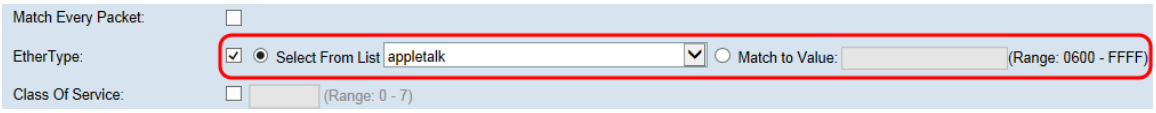
- Jeans: de regel blokkeert al het verkeer dat aan de standaardcriteria voldoet om het WAP-apparaat in te voeren of te verlaten. Verkeersverkeer dat niet aan de criteria voldoet wordt naar de volgende regel doorgestuurd. Als dit de laatste regel is, wordt het verkeer dat niet expliciet wordt toegestaan ingetrokken.

Stap 2. Controleer of koppel de selectieknop **bij elk pakket** los. Indien geselecteerd, past de regel, die of een vergunning of ontkent actie, het kader of het pakket ongeacht zijn inhoud aan.



Opmerking: Als u dit veld selecteert, kunt u geen extra matchcriteria instellen. De **optie Overeenkomsten met elk pakket** wordt standaard voor een nieuwe regel geselecteerd. U moet de optie uitschakelen om andere overeenkomende velden te configureren.

Stap 3. Controleer het selectieteken **Ether Type** om de overeenkomende criteria met de waarde in de kop van een Ethernet-frame te vergelijken. Als het vakje **Ether Type** is ingeschakeld, selecteert u een van de volgende radioknoppen.



De opties worden als volgt beschreven:

- Selecteer vanuit Lijst - Kies een protocol in de vervolgkeuzelijst *Lijst* selecteren. De opties zijn als volgt:

  - AppleTalk - AppleTalk is een eigen reeks van voorzien van een netwerk van protocollen die door Apple Inc. voor hun Macintosh-computers zijn ontwikkeld. AppleTalk omvatte een aantal functies die het mogelijk maakten dat lokale gebiedsnetwerken werden aangesloten zonder voorafgaande installatie of de behoefte aan een gecentraliseerde router of server van om het even welke soort.

  - ARP - Het Address Resolutie Protocol (ARP) is een telecommunicatieprotocol dat wordt gebruikt voor de oplossing van netwerklaagadressen in verbindingslaagadressen, een belangrijke functie in multi-access netwerken.

  - IPv4 - Internet Protocol versie 4 (IPv4) is de vierde versie van de ontwikkeling van het Internet Protocol (IP). Het is een van de kernprotocollen van op standaarden gebaseerde internetworking-methoden in het internet.

  - IPv6 - Internet Protocol versie 6 (IPv6) is de meest recente versie van het Internet Protocol (IP), het communicatieprotocol dat een identificatie- en locatiesysteem voor computers op netwerken en routeverkeer via het internet biedt.

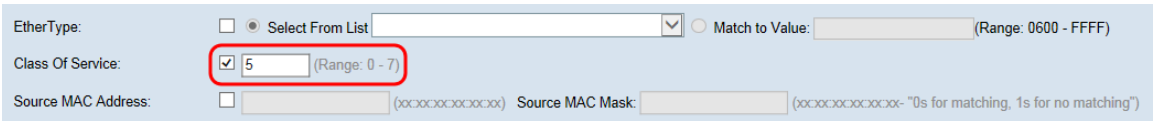
  - IPX - Internetwork Packet Exchange (IPX) is het protocol op de netwerklaag in de IPX/SPX-protocolreeks. IPX is afgeleid van de IDP van Xerox Network Systems. Het kan ook fungeren als een vervoerslaagprotocol.

  - Netoverheid - Netoverheid - Netoverheid is een acroniem voor Network Basic I/O System. Het biedt diensten met betrekking tot de sessielaag van het OSI-model, waardoor toepassingen op afzonderlijke computers kunnen communiceren via een lokaal netwerk. Netoverheid is, zoals strikt API, geen netwerkprotocol.

  - PPPOE - Het Point-to-Point Protocol over Ethernet (PPPoE) is een netwerkprotocol voor het insluiten van PPP-frames in Ethernet-frames.

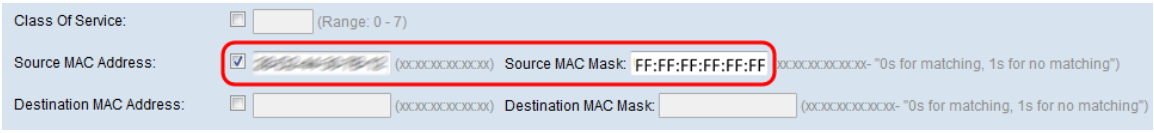
- Overeenkomend met waarde - Voer een douane protocol identificatie in waaraan pakketten zijn aangepast. De waarde is een viercijferige hexadecimale getal in het bereik van 0600 tot FFFF.

Stap 4. Controleer het selectieteken **van serviceklasse** om een 802.1p gebruikersprioriteit in te voeren om te vergelijken met een Ethernet-frame. Zoals IP-voorrang, is 0 de laagste prioriteit en 7 de hoogste. Het geldige bereik is van 0 tot 7.

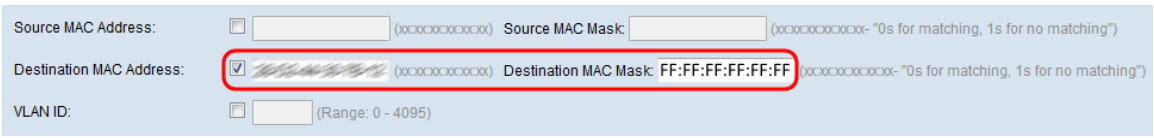


Stap 5. Controleer het selectieteken van het **Bron** van MAC om een bron MAC adres in te gaan om tegen een Ethernet kader te vergelijken. Als het selectieteken van het Bron-MAC wordt gecontroleerd, voer het bron-MAC-adres in het veld *Bron-MAC-adres in*. Voer vervolgens het bron MAC-adresmasker in het veld *Bron MAC-masker* in. Dit zal specificeren welke bits van het bron-MAC-adres zullen worden vergeleken met een Ethernet-frame.

Opmerking: Als u slechts één MAC-adres wilt weergeven, gebruikt u het wild card masker van 00:00:00:00:00:00:00.

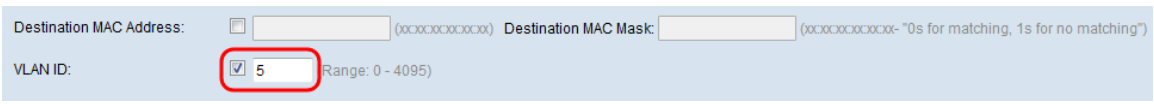


Stap 6. Controleer het selectieteken van het **MAC-adres van de Bestemming** om een MAC-adres in te voeren om dit te vergelijken met een Ethernet-kader. Als het selectieteken van het MAC-adres van de bestemming wordt gecontroleerd, voer dan het MAC-adres van de bestemming in het veld *MAC-adres van de* bestemming in. Voer vervolgens het MAC-adresmasker in het veld *MAC-masker* van *de doellocatie in*. Dit zal specificeren welke bits van het bestemming MAC-adres zullen worden vergeleken met een Ethernet-frame.

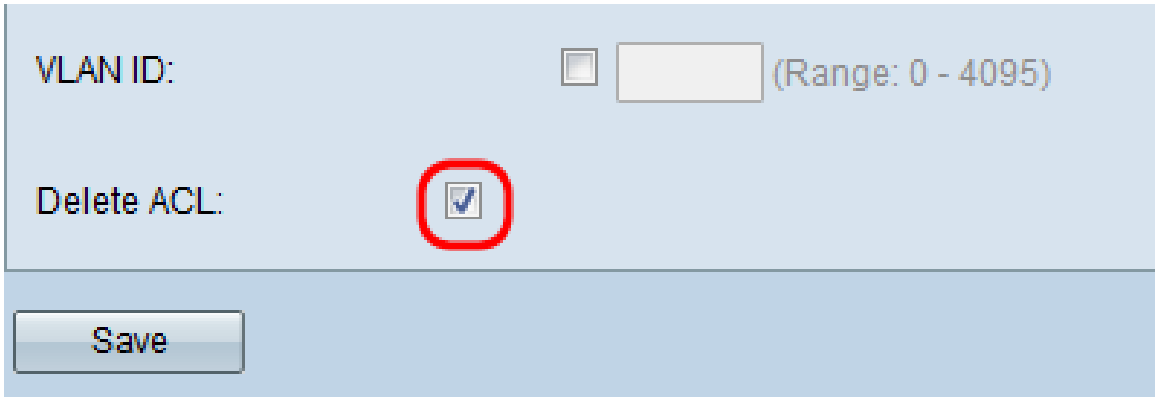


Opmerking: Als u slechts één MAC-adres wilt weergeven, gebruikt u het wild card masker van 00:00:00:00:00:00:00.

Stap 7. Controleer het selectieteken van **VLAN ID** om een VLAN-id in te voeren om tegen een Ethernet-kader te vergelijken. Als de selectieknop **VLAN ID** is ingeschakeld, voert u de VLAN-ID in het veld *VLAN-ID in*. Het VLAN ID bereik loopt van 0-4095.



Stap 4. (Optioneel) Als u de ingesteld ACL wilt verwijderen, controleert u het selectieteken **ACL-**code **verwijderen**.



Stap 9. Klik op **Opslaan** om de instellingen op te slaan.