

Configuratie van IPv4- en IPv6-gebaseerde toegangscontrolelijst (ACL's) op WAP551 en WAP561 access points

Doel

Toegangslijsten (ACL's) zijn verzamelingen van vergunningen en ontkennen voorwaarden, genaamd regels, die beveiliging bieden om onbevoegde gebruikers te blokkeren en geautoriseerde gebruikers toegang te geven tot specifieke bronnen. ACL's kunnen elke ongerechtvaardigde poging om netwerkbronnen te bereiken blokkeren. De QoS-functie bevat ondersteuning voor gedifferentieerde services (DiffServ) waardoor verkeer in streams kan worden geclassificeerd en bepaalde QoS-behandelingen kan worden gegeven in overeenstemming met gedefinieerd per-hop gedrag.

Dit artikel legt uit hoe u IPv4- en IPv6-gebaseerde ACL's (WAP551) en WAP561 access points (WAP) kunt maken en configureren.

Toepasselijke apparaten

- WAP551
- WAP561


Softwareversie

- v1.0.4.2

ACL-configuratie

IP ACL's classificeren verkeer voor Layer 3 in de IP-stapel. Elke ACL is een set van maximaal 10 regels van toepassing op verkeer dat vanuit een draadloze client wordt verstuurd of door een draadloze client wordt ontvangen. Elke regel bepaalt of de inhoud van een bepaald veld gebruikt moet worden om toegang tot het netwerk toe te staan of te weigeren. De regels kunnen op verschillende criteria worden gebaseerd en kunnen van toepassing zijn op een of meer velden in een pakket, zoals het bron- of doeladres, de bron- of doelpoort of het protocol dat in het pakket wordt meegeleverd.

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



The screenshot shows a web interface for configuring ACLs. The title is "ACL". Below it, there is a section titled "ACL Configuration". This section contains two input fields: "ACL Name:" with a text box and a note "(Range: 1-31 Characters)", and "ACL Type:" with a dropdown menu currently set to "IPv4". At the bottom of the configuration area is a button labeled "Add ACL".

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type:

Stap 2. Voer de naam van de ACL in het veld Naam van ACL in.

Stap 3. Kies het gewenste type ACL-type in de vervolgkeuzelijst ACL-type. Als IPv6 is geselecteerd, raadpleegt u het gedeelte [IPv6 ACL-configuratie](#). Als MAC-gebaseerde ACL uit de vervolgkeuzelijst ACL-type wordt geselecteerd, raadpleegt u [Artikel Configuration van MAC-gebaseerde Access Control List \(ACL\) op WAP551 en WAP561 access points](#).

Stap 4. Klik op **Add ACL** om een nieuwe ACL te maken.

IPv4 ACL-configuratie

Opmerking: Als IPv4 uit de vervolgkeuzelijst ACL-type is geselecteerd, volgt u de onderstaande stappen om de IPv4 ACL-regels te configureren.

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type:

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Delete ACL:

Stap 1. Kies de gemaakte ACL-naam-ACL-type in de vervolgkeuzelijst.

ACL Name - ACL Type: ▼

Rule: ▼

Action: ▼

Stap 2. Als een nieuwe regel moet worden geconfigureerd en als er minder dan 10 regels zijn voor de geselecteerde ACL, kiest u **Nieuwe regel** in de vervolgkeuzelijst Regel. Kies anders een van de huidige regels in de vervolgkeuzelijst Regels.

Opmerking: Er kunnen maximaal 10 regels worden gemaakt voor één ACL.

Stap 3. Kies de actie voor de ACL-regel in de vervolgkeuzelijst Actie.

- Ontken - blokkeert al het verkeer dat aan de standaardcriteria voldoet om het WAP-apparaat in te voeren of te verlaten.
- Toestaan van — Hiermee kan al het verkeer dat aan de criteria voldoet om het WAP-apparaat in te voeren of te verlaten.

Action: ▼

Match Every Packet:

Protocol: Select From List: ▼ Match to Value: (Range: 0 - 255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Source Port: Select From List: ▼ Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Destination Port: Select From List: ▼ Match to Port: (Range: 0 - 65535)

Opmerking: Alle volgende stappen zijn optioneel. Vakjes die zijn afgevinkt, worden ingeschakeld. Schakel het vakje uit als u geen specifieke regel wilt toepassen.

Stap 4. Controleer de optie **Overeenkomsten met elk pakket** aan om de regel voor elk frame of pakket **aan** te passen ongeacht de inhoud ervan. Schakel het vakje **Match Elk pakket** uit om **de** extra criteria van het pakket aan te passen.

Timesaver: Als overeenkomend met elk pakket is ingeschakeld, slaat u over op Stap 10.

Stap 5. Controleer het aankruisvakje **Protocol** om een L3- of L4-protocol-matchvoorwaarde te gebruiken die is gebaseerd op de waarde van het IP-protocolveld in IPv4-pakketten. Als het dialoogvenster Protocol is ingeschakeld, klikt u op een van deze knoppen:

- Selecteer vanuit Lijst - Protocol om uit de vervolgkeuzelijst Lijst te selecteren.
- Overeenkomend met waarde — Voor protocol niet in de lijst vermeld. Geef een standaard IANA-toegewezen protocol-ID op tussen 0 en 255.

Stap 6. Controleer het aankruisvakje **IP-adres** bron om het IP-adres van de bron in de matchomstandigheden op te nemen. Voer het IP-adres en het wild kaartmasker van de bron in de respectievelijke velden in.

Stap 7. Controleer het aanvinkvakje **Bron** om een bronpoort in de matchconditie op te nemen. Als het aankruisvakje Source Port is ingeschakeld, klikt u op een van deze radioknoppen:

- Selecteer vanuit Lijst - Bron poort om uit de vervolgkeuzelijst Lijst te kiezen.
- Overeenkomend met poort — Voor bronpoort die niet in de lijst staat. Voer het poortnummer in dat tussen 0 en 65535 ligt en drie verschillende typen poorten omvat.
 - 0 tot 1023 — bekende havens.
 - 1024 tot en met 49151 — Geregistreerde havens.
 - 49152 tot en met 65535 — Dynamische en/of particuliere havens.

Stap 8. Controleer het aankruisvakje **IP-adres** van de **bestemming** om het IP-adres van de bestemming in de matchomstandigheden op te nemen. Voer het IP-adres en het wild kaartmasker van de bestemming in de respectievelijke velden in.

Stap 9. Controleer het aanvinkvakje **Destination Port** om een bestemmingspoort in de matchconditie op te nemen. Als het aanvinkvakje Destination Port is ingeschakeld, klikt u op een van deze radioknoppen.

- Selecteer vanuit lijst — Doelpoort om uit de vervolgkeuzelijst Lijst te kiezen.
- Stem in op poort — Voor bestemmingspoorten die niet in de lijst staan. Voer het poortnummer in dat in het veld Overeenkomend met Port varieert van 0 tot 65535. Het bereik omvat drie verschillende soorten havens.
 - 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.

Stap 10. Controleer het **IP DSCP**-vakje om de pakketten aan te passen die op IP DSCP-waarden zijn gebaseerd. Als het vakje IP DSCP is ingeschakeld, klikt u op een van deze knoppen:

- Selecteer vanuit Lijst - Kies de gewenste IP DSCP-waarde in de vervolgkeuzelijst Selecteren.
- Overeenkomend met waarde — U kunt DSCP-waarden aanpassen. Voer de DSCP-waarde in die in het veld Overeenkomend met de waarde varieert van 0 tot 63.

Stap 1. Controleer het vakje **IP-voorrang** om een IP-voorrang-waarde in de matchomstandigheden te bevatten. Als het vakje IP-voorrang wordt gecontroleerd, voert u een IP-voorrang in die van 0 tot 7 varieert. De IP-prioriteitswaarden en de corresponderende waardebeschrijving kunnen als volgt worden uitgelegd:

- 0 — Routine of Best Forfort
- 1 — Prioriteit
- 2 — Onmiddellijk
- 3 — Flitser (hoofdzakelijk gebruikt voor spraaksignalering of voor video)
- 4 — Flitser Override
- 5 — Kritisch (hoofdzakelijk gebruikt voor spraak RTP)
- 6 — Internet
- 7 — Netwerk

Stap 12. Controleer het aankruisvakje **IP TOS**-bits om het type servicbits in de IP-kop als overeenkomende criteria te gebruiken. Als het vakje van de IP TOS Bits wordt gecontroleerd, voer de IP TOS bits in die van 00 tot FF en IP TOS masker variëren van 00 tot FF in de respectieve velden.

Stap 13. Om de geconfigureerde ACL te verwijderen, controleert u het vakje **ACL verwijderen** en vervolgens klikt u op **Opslaan**.

[IPv6-ACL-configuratie](#)

Opmerking: Als IPv6 uit de vervolgkeuzelijst ACL-type is geselecteerd, volgt u de onderstaande stappen om de IPv6 ACL-regels te configureren.

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type:

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IPv6 Address: Source IPv6 Prefix Length: (Range: 1 - 128)

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IPv6 Address: Destination IPv6 Prefix Length: (Range: 1 - 128)

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

IPv6 Flow Label: (Range: 00000 - FFFFF)

IPv6 DSCP: Select From List: Match to Value: (Range: 0 - 63)

Delete ACL:

Stap 1. Kies de gemaakte ACL-naam-ACL-type in de vervolgkeuzelijst.

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Stap 2. Als de nieuwe regel voor de geselecteerde ACL moet worden ingesteld, kiest u **Nieuwe regel** in de vervolgkeuzelijst Regel. Kies anders een van de huidige regels uit de vervolgkeuzelijst Regel.

Opmerking: U kunt maximaal 10 regels maken voor één ACL.

Stap 3. Kies de actie voor de ACL-regel in de vervolgkeuzelijst Actie.

- Ontken - blokkeert al het verkeer dat aan de standaardcriteria voldoet om het WAP-apparaat in te voeren of te verlaten.
- Toestaan van — Hiermee kan al het verkeer dat aan de criteria voldoet om het WAP-apparaat in te voeren of te verlaten.

Match Every Packet	<input type="checkbox"/>		
Protocol:	<input checked="" type="checkbox"/> <input type="radio"/> Select From List:	icmpv6	<input type="radio"/> Match to Value: <input type="text"/> (Range: 0 - 255)
Source IPv6 Address:	<input checked="" type="checkbox"/>	2001:db8:a442:3::	Source IPv6 Prefix Length: <input type="text"/> 64 (Range: 1 - 128)
Source Port:	<input checked="" type="checkbox"/> <input type="radio"/> Select From List:		<input type="radio"/> Match to Port: <input type="text"/> 56 (Range: 0 - 65535)
Destination IPv6 Address:	<input checked="" type="checkbox"/>	2001:db8:beef:3::	Destination IPv6 Prefix Length: <input type="text"/> 64 (Range: 1 - 128)
Destination Port:	<input checked="" type="checkbox"/> <input type="radio"/> Select From List:	snmp	<input type="radio"/> Match to Port: <input type="text"/> (Range: 0 - 65535)

Opmerking: Alle volgende stappen zijn optioneel. Vakjes die zijn afgevinkt, worden ingeschakeld. Schakel het vakje uit als u geen specifieke regel wilt toepassen.

Stap 4. Controleer de optie **Overeenkomsten met elk pakket** aan om de regel voor elk frame of pakket **aan** te passen ongeacht de inhoud ervan. Schakel het vakje **Match Elk pakket** uit om **de** extra criteria van het pakket aan te passen.

Timesaver: Als overeenkomend met elk pakket is ingeschakeld, slaat u over op Stap 12.

Stap 5. Controleer het aankruisvakje **Protocol** om een L3- of L4-protocol te gebruiken op basis van de waarde van het IP Protocol-veld in IPv6-pakketten. Als het dialoogvenster Protocol is ingeschakeld, klikt u op een van deze knoppen.

- Selecteer vanuit Lijst - Protocol om uit de vervolgkeuzelijst Lijst te selecteren.
- Overeenkomend met waarde — Voor protocol niet in de lijst vermeld. Geef een standaard IANA-toegewezen protocol-ID op tussen 0 en 255.

Stap 6. Controleer het aankruisvakje **IP-adres** 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 de respectievelijke velden in.

Stap 7. Controleer het aanvinkvakje **Bron** om een bronpoort in de matchconditie op te nemen. Als het aankruisvakje Source Port is ingeschakeld, klikt u op een van de volgende radioknoppen:

- Selecteer vanuit Lijst - Bron poort om uit de vervolgkeuzelijst Lijst te kiezen.
- Overeenkomsten met poorten — Voor bronpoorten die niet in de lijst staan. Voer het poortnummer in dat tussen 0 en 65535 ligt en drie verschillende typen poorten omvat.
 - 0 tot 1023 — bekende havens.
 - 1024 tot en met 49151 — Geregistreerde havens.
 - 49152 tot en met 65535 — Dynamische en/of particuliere havens.

Stap 8. Controleer het aankruisvakje **IP-adres** van de **bestemming** om het IP-adres van de bestemming in de matchomstandigheden op te nemen. Voer het IP-adres en het wild kaartmasker van de bestemming in de respectievelijke velden in.

Stap 9. Controleer het aanvinkvakje **Destination Port** om een bestemmingspoort in de matchconditie op te nemen. Als het aanvinkvakje Destination Port is ingeschakeld, klikt u op een van deze radioknoppen:

- Selecteer vanuit lijst — Doelpoort om uit de vervolgkeuzelijst Lijst te kiezen.
- Stem in op poort — Voor bestemmingspoorten die niet in de lijst staan. Voer het poortnummer in dat in het veld Overeenkomend met Port varieert van 0 tot 65535. Het bereik omvat drie verschillende soorten havens.
 - 0 tot 1023 — Goed bekende poorten.
 - 1024 tot en met 49151 — geregistreerde poorten.
 - 49152 tot en met 65535 — Dynamische en/of particuliere poorten.

IPv6 Flow Label: (Range: 00000 - FFFFF)

IPv6 DSCP: Select From List: Match to Value: (Range: 0 - 63)

Delete ACL:

Stap 10. Controleer het aankruisvakje voor **IPv6 Flow** om het IPv6-label in de softwarefunctie op te nemen. Het veld 20-bits stroomlabel in de IPv6-header kan door een bron worden gebruikt om een verzameling pakketten te labelen die tot dezelfde stroom behoren. Voer het nummer in dat varieert van 00000 tot FFF in het veld label voor IPv6-doorstroming.

Stap 1. Controleer het aankruisvakje **IPv6 DSCP** om de IP DSCP-waarden in de matchomstandigheden op te nemen. Als het vakje IP DSCP is ingeschakeld, klikt u op een van deze knoppen.

- Selecteer vanuit Lijst - IP DSCP-waarde om uit de vervolgkeuzelijst Lijst te selecteren.
- Overeenkomend met waarde - Om DSCP waarde aan te passen die van 0 tot 63 varieert.

Stap 12. (Optioneel) Controleer het vakje **ACL verwijderen** om de geconfigureerde ACL-code te verwijderen.

Stap 13. Klik op **Opslaan**.