

Creatie en configuratie van een regel voor IPv4-gebaseerde toegangscontrolelijst (ACL's) op WAP121 en WAP321 access points

Doel

Een toegangscontrolelijst (ACL) is een lijst van netwerkverkeersfilters en bijbehorende acties die worden gebruikt om de beveiliging te verbeteren. Een ACL bevat de hosts die toegang tot het netwerkapparaat is toegestaan of geweigerd. De optie QoS 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-hopgedrag.

Dit artikel legt uit hoe u IPv4-gebaseerde ACL's (WAP121 en WAP321 access points) kunt maken en configureren.

Toepasselijke apparaten

- WAP121
- WAP321

Softwareversie

- v1.0.3.4

IPv4-gebaseerde ACL-configuratie

IP ACL's classificeren verkeer voor Lagen 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.

Creatie van IPv4 ACL

Stap 1. Meld u aan bij het Access Point Configuration-hulpprogramma en kies **client-QoS > ACL**. De *ACL*-pagina wordt geopend:

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▼

Stap 2. Voer de naam van de ACL in het veld *ACL-naam in*.

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▼

Stap 3. Kies het **IPv4**-type voor ACL in de vervolgkeuzelijst *Type*.

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▼

Stap 4. Klik op **Add ACL** om een nieuwe IPv4 ACL te maken.

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▼

Configuratie van een regel voor IPv4 ACL

Stap 1. Kies de ACL van de vervolgkeuzelijst *ACL-type* waarvoor regels moeten worden ingesteld.

ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4

Rule: New Rule

Action: Deny

Match Every Packet:

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

ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4

Rule: New Rule

Action: Deny

Match Every Packet:

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

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

ACL

ACL Configuration

ACL Name: ExampleAllowSMTP (Range: 1-31 Characters)

ACL Type: IPv4

Add ACL

ACL Rule Configuration

ACL Name - ACL Type: User1 - IPv4

Rule: New Rule

Action: Deny

Match Every Packet:

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

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

De beschikbare opties worden als volgt beschreven:

- 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.

Stap 4. Controleer de selectieknop *Elke Packet* om de regel voor elk frame of pakket aan te passen, ongeacht de inhoud. Als u een bepaalde match criteria wilt configureren, schakelt u het selectieteken *Elke Packet* uit.

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range)

Service Type

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

IP Precedence: (Range: 0 - 7)

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

Delete ACL:

Timesaver: Als u *elke* selectieknop op *Overeenkomsten* controleert, slaat u de *knop* over naar [Stap 13](#).

Stap 5. (Optioneel) Controleer het selectieteken van het *Protocol* voor de L3- of L4-matchvoorwaarde op basis van de waarde van het IP Protocol-veld in IPv4-pakketten. Als het selectieknop *Protocol* is ingeschakeld, klikt u op een van deze radioknoppen.

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range:)

Source IP Address: (xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range:)

Destination IP Address: (xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:)

Service Type

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

De opties worden als volgt beschreven:

- Selecteer vanuit lijst — Kies een protocol in de vervolgkeuzelijst *Lijst*. De vervolgkeuzelijst bevat ip, icmp, igmp, tcp, udp protocollen.
- Overeenkomend met waarde — Voor protocol niet in de lijst vermeld. Geef een standaard IANA-toegewezen protocol-ID op die varieert van 0 tot 255.

Stap 6. (Optioneel) Controleer het selectieteken *IP-adres* bij *bron* om een IP-adres van de bron in de matchomstandigheden op te nemen. Voer het IP-adres en het *Wilde Kaartmasker* van de bron in de respectievelijke velden in. Met het wild card masker kunt u specificeren op welke host van het IP-adres deze toegangslijst wordt toegepast.

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 2)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx)

Source Port: Select From List: Match to Port: (Range: 0 - 6)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx)

Destination Port: Select From List: Match to Port: (Range: 0 - 6)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 6)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 0 - 255)

Delete ACL:

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

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 2)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx)

Source Port: Select From List: Match to Port: (Range: 0 - 6)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx)

Destination Port: Select From List: Match to Port: (Range: 0 - 6)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 6)

IP Precedence: (Range: 0 - 7)

- Selecteer vanuit lijst — Kies een bronpoort in de vervolgkeuzelijst *Selecteer deze optie*. De vervolgkeuzelijst heeft ftp, ftpdata, http, smtp, snmp, telnet, tftp, www poorten.

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:

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

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

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

- Overeenkomend met poort — Voor bronpoort die niet in de lijst staat. Voer het poortnummer in dat tussen 0 en 65535 ligt.

Stap 8. (Optioneel) Controleer het *IP-adres van de bestemming* om het IP-adres van de bestemming in de softwarefunctie op te nemen. Voer het IP-adres en het *Wilde Kaartmasker* van de bestemming in hun respectievelijke velden in. Met het wild card masker kunt u specificeren op welke host van het IP-adres van de bestemming deze toegangslijst wordt toegepast.

Action:

Match Every Packet:

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

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

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

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

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 9. (Optioneel) Controleer het aanvinkvakje **Destination Port** om een bestemmingspoorts in de matchconditie op te nemen. Als het vakje *Destination Port* is ingeschakeld, klikt u op een van deze radioknoppen.

Action: Deny

Match Every Packet:

Protocol: Select From List: ip Match to Value: (Range:)

Source IP Address: 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Source Port: Select From List: ftp Match to Port: (Range:)

Destination IP Address: 192.168.20.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Destination Port: Select From List: http Match to Port: (Range:)

Service Type

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

IP Precedence: (Range: 0 - 7)

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

Delete ACL:

Save

- Selecteer vanuit lijst — Kies een doelpoort in de vervolgkeuzelijst *Selecteer deze optie*. De vervolgkeuzelijst heeft ftp, ftpdata, http, smtp, snmp, telnet, tftp, www poorten.

Action: Deny

Match Every Packet:

Protocol: Select From List: ip Match to Value: (Range:)

Source IP Address: 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Source Port: Select From List: ftp Match to Port: (Range:)

Destination IP Address: 192.168.20.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Destination Port: Select From List: Match to Port: 80 (Range:)

Service Type

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

IP Precedence: (Range: 0 - 7)

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

Delete ACL:

Save

- 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.

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

Stap 10. (Optioneel) Controleer het *IP DSCP*-selectieteken om de pakketten aan te passen die op IP DSCP-waarden zijn gebaseerd. Als het selectieknop *IP DSCP* is ingeschakeld, klikt u op een van deze knoppen. 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. Raadpleeg [hier](#) voor meer informatie over DSCP.

The screenshot shows the 'ACL Rule Configuration' window. The 'Service Type' section is highlighted with a red box. It contains a dropdown menu with the following options: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs0, cs1, cs2, cs3, cs4, cs5, cs6. The 'IP DSCP' field is set to 'af11'. Other fields include 'Action: Deny', 'Source IP Address: 192.168.10.0', 'Destination IP Address: 192.168.20.0', and 'Match to Port: 80'. A 'Save' button is at the bottom.

- Selecteer vanuit lijst — Kies een IP DSCP-waarde in de vervolgkeuzelijst *Selecteer vanuit Lijst*. De vervolgkeuzelijst bevat waarden voor Gegarandeerd doorsturen (AS), Serviceklasse (CSC) of FEF-doorsturen.
- Overeenkomend met waarde — U kunt DSCP-waarden aanpassen. Voer de DSCP-waarde in die in het veld Overeenkomend met Waarde varieert van 0 tot 63.

Stap 1. (Optioneel) Controleer *het* selectieteken *IP-voorrang* om in de conditie van de match een IP-voorrang te geven. Als het vakje IP-voorrang wordt ingeschakeld, geeft u een IP-voorrang die varieert van 0 tot 7. Raadpleeg [hier](#) voor meer informatie over IP-voorrang.

The screenshot shows the 'Service Type' section of the ACL Rule Configuration window. The 'IP Precedence' field is highlighted with a red box and set to '5'. Other fields include 'IP DSCP: Match to Value: 24', 'IP TOS Bits: DF', and 'IP TOS Mask: DE'. A 'Save' button is at the bottom.

Stap 12. (Optioneel) Controleer het selectieteken *IP TOS Bits* om de Packet Type of Service bits in de IP-header als overeenkomende criteria te gebruiken. Als het vakje van de IP TOS Bits wordt gecontroleerd, voer de IP TOS bits in die van 00-FF en IP TOS masker variëren

van 00-FF in de respectieve velden.

Service Type

IP DSCP: Select From List: Match to Value: (R)

IP Precedence: (Range: 0 - 7)

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

Delete ACL:

Stap 13. (Optioneel) Als u de geconfigureerde ACL wilt verwijderen, controleert u het vakje *Verwijderen ACL*.

Service Type

IP DSCP: Select From List: Match to Value: (R)

IP Precedence: (Range: 0 - 7)

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

Delete ACL:

Stap 14. Klik op **Opslaan** om de instellingen op te slaan.