

Creatie en configuratie van een regel voor IPv6-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 toegangscontrolelijst bevat de hosts die toegang tot het netwerkapparaat is toegestaan of geweigerd. De QoS-functie bevat gedifferentieerde services (DiffServ) ondersteuning waarmee 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 IPv6 ACL's op WAP121 en WAP321 access points kunt maken en configureren.

Toepasselijke apparaten

- WAP121
- WAP321

Softwareversie

- v1.0.3.4

IPv6-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 verzonden van een draadloze client of ontvangen door een draadloze client. 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 IPv6 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 Alphanumeric Characters)

ACL Type:

Stap 3. Kies het **IPv6**-type voor ACL in de vervolgkeuzelijst *Type*.

Stap 4. Klik op **Add ACL** om een nieuwe IPv6-ACL te maken.

Configuratie van een regel voor IPv6 ACL

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value:

Source IPv6 Address: Source IPv6 Prefix Length:

Source Port: Select From List: Match to Port:

Destination IPv6 Address: Destination IPv6 Prefix Length:

Destination Port: Select From List: Match to Port:

IPv6 Flow Label: (Range: 00000 - FFFFF)

IPv6 DSCP: Select From List: Match to Value:

Delete ACL:

Stap 1. Kies de ACL van de vervolgkeuzelijst *ACL-naam-ACL (Naam-ACL)* waarvoor regel moet worden ingesteld.

Stap 2. Als een 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 *Action*.

- 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.

Voorzichtig: Je moet een vergunningsregel toevoegen die het verkeer toestaat omdat als een vergunning of ontkenning wordt gekozen altijd er een impliciet ontkennen is aan het eind van elke regel.

Stap 4. Controleer de selectieknop *Elke Packet* om de regel voor elk frame of pakket aan te passen, ongeacht de inhoud. Als u de configuratie van een van de extra wedstrijdcriteria wilt uitvoeren, schakelt u het selectieteken *Overeenkomsten met elk pakket* uit.

Timesaver: Als u *elke* selectieteken op *maat* controleert, slaat u de *optie* over naar [Stap 12](#).

Stap 5. Controleer het selectieteken *Protocol* om L3 of L4 (Network and Transport Layer of IP stapel) protocol *mogelijk* te maken op basis van de waarde van het *IP Protocol*-veld in IPv6-pakketten. Als het Protocol is ingeschakeld, klikt u op een van deze radioknoppen.

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

Stap 6. Controleer het selectieteken *Bron IPv6* om een IP-adres van de bron in de matchomstandigheden op te nemen. Voer het IPv6-adres in en de lengte van het IPv6-prefix van de bron in de relatieve velden.

Stap 7. Controleer het selectieteken *van de Bron* om een bronpoort in de matchvoorwaarde te omvatten. Als het aanvinkvakje Source Port is ingeschakeld, klikt u op een van deze radioknoppen.

- Selecteer vanuit lijst — Kies een bronpoort in de vervolgkeuzelijst Lijst. De vervolgkeuzelijst heeft ftp, ftpdata, http, smtp, snmp, telnet, tftp, www poorten.
- 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 — Goed bekende poorten. Poort die door het serverproces als contactpoort wordt gebruikt. De contacthaven wordt soms een bekende haven genoemd.
 - 1024 tot en met 49151 — geregistreerde poorten. Het is een netwerkpoort die wordt gebruikt voor bepaalde protocollen of voor een toepassing.
 - 49152 tot en met 65535 — Dynamische en/of particuliere poorten. Dynamische havens worden niet beheerd door een overheidsinstantie als IANA en hebben geen speciale

gebruiksbeperkingen.

Stap 8. Controleer het selectieteken van het *IPv6-adres op de bestemming* om het IP-adres van de bestemming in de matchomstandigheden op te nemen. Voer het IPv6-adres in en de lengte van het IPv6-prefix van de bestemming in de relatieve velden.

Stap 9. Controleer het selectieteken *van de poort op de bestemming* om een poort in de match te openen. Als het aanvinkvakje Destination Port is ingeschakeld, klikt u op een van deze radioknoppen.

- Selecteer vanuit lijst — Kies een doelpoort in de vervolgkeuzelijst Lijst. De vervolgkeuzelijst heeft ftp, ftpdata, http, smtp, snmp, telnet, tftp, www poorten.
- Stem in op poort — Voor bestemmingspoorten 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 — Goed bekende poorten.
 - 1024 tot en met 49151 — geregistreerde poorten.
 - 49152 tot en met 65535 — Dynamische en/of particuliere poorten.

Stap 10. Controleer het *label van IPv6 Flow* selectieteken om het IPv6 flow-label in de matchomstandigheden te bevatten. 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 *IP DSCP*-selectieteken om de IP DSCP-waarden in de matchconditie 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. De vervolgkeuzelijst bevat waarden voor Gegarandeerd doorsturen (AS), Serviceklasse (CSC) of FEF-doorsturen.
- Overeenkomend met waarde - Om DSCP waarde aan te passen die van 0 tot 63 varieert.

Stap 12. (Optioneel) Als u de geconfigureerde ACL wilt verwijderen, controleert u het selectieteken *ACL-code verwijderen*.

Stap 13. Klik op **Opslaan** om de instellingen op te slaan.