Configuratievoorbeeld voor access point ACL-filter

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Achtergrondinformatie](#)
[Configureren](#)
[Filters die standaard toegangslijsten gebruiken](#)
[Filters die uitgebreide toegangslijsten gebruiken](#)
[Filters die MAC-gebaseerde ACL's gebruiken](#)
[Filters die op tijd gebaseerde ACL's gebruiken](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Gerelateerde informatie](#)

Inleiding

Dit document legt uit hoe u op Cisco Aironet Access Point (AP) gebaseerde filters (ACL's) kunt configureren met gebruik van de opdrachtregel-interface (CLI).

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- De configuratie van een draadloze verbinding met het gebruik van een Aironet AP en een Aironet 802.11a/b/g clientadapter
- ACL's

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Aironet 1200 Series AP die Cisco IOS® softwarerelease 12.3(7)JA1 draait
- Aironet 802.11a/b/g clientadapter

- Aironet Desktop Utility (ADU) softwarerelease 2.5

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

U kunt filters op APs gebruiken om deze taken uit te voeren:

- Toegang tot het draadloze LAN (WLAN)-netwerk beperken
- Geef een extra laag draadloze beveiliging op

U kunt verschillende typen filters gebruiken om verkeer te filteren op basis van:

- Specifieke protocollen
- MAC-adres van het clientapparaat
- IP-adres van het clientapparaat

U kunt ook filters inschakelen om verkeer door gebruikers op het bekabelde LAN te beperken. IP-adres en MAC-adresfilters staan het verzenden van unicast en multicast pakketten die naar of van specifieke IP- of MAC-adressen worden verzonden toe of verbieden.

Protocol-gebaseerde filters bieden een meer granulaire manier om de toegang tot specifieke protocollen door de Ethernet en radio interfaces van het AP te beperken. U kunt een van deze methoden gebruiken om de filters op de AP's te configureren:

- Web GUI
- CLI

Dit document legt uit hoe u ACL's gebruikt om filters door de CLI te configureren. Zie Filters configureren voor informatie over het configureren van filters door de GUI.

U kunt de CLI gebruiken om deze types van op ACL gebaseerde filters op AP te configureren:

- Filters die standaard ACL's gebruiken
- Filters die uitgebreide ACL's gebruiken
- Filters die MAC-adres ACL's gebruiken

Opmerking: Het aantal toegestane items op een ACL is beperkt door de CPU van het AP. Als er een groot aantal items is om aan een ACL toe te voegen, bijvoorbeeld bij het filteren van een lijst met MAC-adressen voor de clients, gebruikt u een switch in het netwerk die de taak kan uitvoeren.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Alle configuraties in dit document gaan ervan uit dat er al een draadloze verbinding is gerealiseerd. Dit document concentreert zich alleen op het gebruiken van CLI om filters te configureren. Als u geen fundamentele draadloze verbinding hebt, raadpleegt u het Configuratievoorbeeld van Draadloze LAN-verbinding.

Filters die standaard toegangslijsten gebruiken

U kunt standaard ACL's gebruiken om de invoer van clientapparaten in het WLAN-netwerk toe te staan of af te schaffen op basis van het IP-adres van de client. Standaard ACL's vergelijken het bronadres van de IP-pakketten met de adressen die in ACL zijn geconfigureerd om het verkeer te controleren. Dit type ACL kan als bron-IP adres-gebaseerde ACL worden genoemd.

De opdrachtsyntaxis van een standaard ACL is **access-list access-list-number {permit | ontkennen} {host *ip-adres* | *bronip-bronvervanging* | eventueel**.

In Cisco IOS® softwarerelease 12.3(7)JA kan het ACL-nummer elk nummer van 1 tot 99 zijn. Standaard ACL's kunnen ook het uitgebreide bereik van 1300 tot 1999 gebruiken. Deze extra aantallen worden uitgebreid IP ACL's.

Wanneer een standaard ACL wordt ingesteld om toegang tot een client te ontkennen, associeert de client nog steeds met AP. Er is echter geen datacommunicatie tussen het AP en de cliënt.

Dit voorbeeld toont een standaard ACL die wordt gevormd om het IP-adres van de client 10.0.0.2 van de draadloze interface (radio0-interface) te filteren. Het IP-adres van het AP is 10.0.0.1.

Nadat dit is gedaan kan de client met IP-adres 10.0.0.2 geen gegevens verzenden of ontvangen via het WLAN-netwerk, ook al is de client gekoppeld aan de AP.

Voltooi deze stappen om een standaard ACL via de CLI te maken:

1. Meld u aan bij de AP via de CLI.Gebruik de console poort of gebruik telnet om ACL door de Ethernet interface of de draadloze interface te gebruiken.
2. Geef de configuratie van het besturingssysteem op:
   ```
   AP#configure terminal
   ```
3. Geef deze opdrachten uit om de standaard ACL te maken:
   ```
   AP<config>#access-list 25 deny host 10.0.0.2
   !--- Create a standard ACL 25 to deny access to the !--- client with IP address 10.0.0.2.
   AP<config>#access-list 25 permit any
   !--- Allow all other hosts to access the network.
   ```
4. Geef deze opdrachten uit om deze ACL op de radio-interface toe te passen:
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group 25 in
   !--- Apply the standard ACL to the radio interface 0.
   ```

U kunt ook een standaard met de naam ACL (NACL) maken. NACL gebruikt een naam in plaats van een aantal om ACL te definiëren.

```
AP#configure terminal
AP<config>#ip access-list standard name
```

```
AP<config>#permit | deny {host ip-address | source-ip [source-wildcard] | any} log
```

Geef deze opdrachten uit om de standaard NACL's te gebruiken om de host 10.0.2-toegang tot het WLAN-netwerk te weigeren:

```
AP#configure terminal
AP<config>#ip access-list standard TEST
!--- Create a standard NACL TEST.

AP<config-std-nacl>#deny host 10.0.0.2
!--- Disallow the client with IP address 10.0.0.2 !--- access to the network. AP<config-std-
nacl>#permit any
!--- Allow all other hosts to access the network. AP<config-std-nacl>#exit
!--- Exit to global configuration mode. AP<config>#interface Dot11Radio 0
!--- Enter dot11 radio0 interface mode. AP<config-if>#ip access-group TEST in
!--- Apply the standard NACL to the radio interface.
```

Filters die uitgebreide toegangslijsten gebruiken

Uitgebreide ACL's vergelijken de bron- en doeladressen van de IP-pakketten met de adressen die in ACL zijn geconfigureerd om het verkeer te controleren. Uitgebreide ACL's bieden ook een middel om verkeer te filteren op basis van specifieke protocollen. Dit biedt een meer granulaire controle voor de implementatie van filters op een WLAN-netwerk.

Uitgebreide ACL's staan een client toe toegang te hebben tot bepaalde bronnen op het netwerk terwijl de client geen toegang heeft tot de andere bronnen. U kunt bijvoorbeeld een filter implementeren die DHCP- en Telnet-verkeer naar de client toestaat terwijl het al ander verkeer beperkt.

Dit is de opdrachtsyntaxis van uitgebreide ACL's:

Opmerking: deze opdracht is vanwege ruimtelijke overwegingen op vier lijnen gewikkeld.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol
source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log |
log-input] [time-range time-range-name]
```

In Cisco IOS-softwarerelease 12.3(7)JA kunnen uitgebreide ACL's getallen gebruiken in het bereik van 100 tot 199. Uitgebreide ACL's kunnen ook getallen gebruiken in het bereik van 2000 tot 2699. Dit is het uitgebreide bereik voor uitgebreide ACL's.

Opmerking: het **logsleutelwoord** aan het eind van de individuele ACL-items toont:

- ACL-nummer en -naam
- Of de verpakking toegestaan of ontkend was
- Poortspecifieke informatie

Uitgebreide ACL's kunnen ook namen in plaats van getallen gebruiken. Dit is de syntaxis om uitgebreide NACL's te maken:

```
ip access-list extended name {deny | permit} protocol source source-wildcard destination
destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-
```

name]

Dit configuratievoorbeeld gebruikt uitgebreide NACL's. Het vereiste is dat de uitgebreide NACL de toegang van telers tot de cliënten moet toestaan. U moet alle andere protocollen op het WLAN-netwerk beperken. Ook gebruiken de clients DHCP om het IP-adres te bemachtigen. U moet een uitgebreide ACL maken:

- Hiermee kan DHCP- en Telnet-verkeer worden toegestaan
- Ontkent alle andere verkeerstypen

Zodra deze uitgebreide ACL op de radio interface wordt toegepast, associëren de klanten met AP en krijgen een IP adres van de server van DHCP. De klanten kunnen ook telnet gebruiken. Alle andere soorten verkeer worden ontkend.

Voltooi deze stappen om een uitgebreide ACL op AP te maken:

1. Meld u aan bij de AP via de CLI.Gebruik de console poort of telnet om ACL door de Ethernet interface of de draadloze interface te gebruiken.
2. Geef de configuratie van het besturingssysteem op:
   ```
   AP#configure terminal
   ```
3. Geef deze opdrachten uit om de uitgebreide ACL-opdracht te maken:
   ```
   AP<config>#ip access-list extended Allow_DHCP_Telnet
   !--- Create an extended ACL Allow_DHCP_Telnet.

   AP<config-extd-nacl>#permit tcp any any eq telnet
   !--- Allow Telnet traffic. AP<config-extd-nacl>#permit udp any any eq bootpc
   !--- Allow DHCP traffic. AP<config-extd-nacl>#permit udp any any eq bootps
   !--- Allow DHCP traffic. AP<config-extd-nacl>#deny ip any any
   !--- Deny all other traffic types. AP<config-extd-nacl>#exit
   !--- Return to global configuration mode.
   ```
4. Geef deze opdrachten af om ACL op de radio-interface toe te passen:
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group Allow_DHCP_Telnet in
   !--- Apply the extended ACL Allow_DHCP_Telnet !--- to the radio0 interface.
   ```

Filters die MAC-gebaseerde ACL's gebruiken

U kunt MAC-adresgebaseerde filters gebruiken om clientapparaten te filteren op basis van het harde gecodeerde MAC-adres. Wanneer een client geen toegang krijgt via een MAC-gebaseerd filter, kan de client niet associëren met AP. MAC-adresfilters staan het verzenden van unicast- en multicast-pakketten toe of verbieden deze worden verzonden van of gericht aan specifieke MAC-adressen.

Dit is de opdrachtsyntaxis om een MAC-adres-gebaseerde ACL op het AP te maken:

Opmerking: deze opdracht is vanwege ruimtelijke overwegingen op twee regels gewikkeld.

access-list *access-list-number* **{permit | deny}** *48-bit-hardware-address 48-bit-hardware-address-mask*

In Cisco IOS-softwarerelease 12.3(7)JA kunnen MAC-adres ACL's in het bereik van 700 tot 799 als het ACL-nummer gebruiken. Ze kunnen ook getallen gebruiken in het uitgebreide bereik van 1100 tot 1199.

Dit voorbeeld illustreert hoe u een MAC-gebaseerd filter via de CLI moet configureren om de client te filteren met een MAC-adres van **0040.96a5.b5d4**:

1. Meld u aan bij de AP via de CLI.Gebruik de console poort of telnet om ACL door de Ethernet interface of de draadloze interface te gebruiken.
2. Geef de configuratie van de configuratie op in het AP-CLI:
   AP#**configure terminal**

3. Maak een MAC-adres ACL 700.Met deze ACL kan client 0040.96a5.b5d4 niet worden geassocieerd met AP.

   ```
   access-list 700 deny 0040.96a5.b5d4 0000.0000.0000
   !--- This ACL denies all traffic to and from !--- the client with MAC address
   0040.96a5.b5d4.
   ```
4. Geef deze opdracht uit om deze MAC-gebaseerde ACL op de radio-interface toe te passen:

   ```
   dot11 association mac-list 700

   !--- Apply the MAC-based ACL.
   ```

Nadat u dit filter op AP hebt ingesteld, wordt de client met dit MAC-adres, dat eerder aan AP was gekoppeld, gescheiden. De AP console stuurt dit bericht:

```
AccessPoint# *Mar 1 01:42:36.743: %DOT11-6-DISASSOC: Interface
 Dot11Radio0, Deauthenticating Station 0040.96a5.b5d4
```

Filters die op tijd gebaseerde ACL's gebruiken

Tijdgebaseerde ACL's zijn ACL's die voor een specifieke periode kunnen worden ingeschakeld of uitgeschakeld. Deze capaciteit biedt robuustheid en de flexibiliteit om toegangscontrolemaatregelen te definiëren die bepaalde soorten verkeer toestaan of ontkennen.

Dit voorbeeld illustreert hoe te om een op tijd gebaseerde ACL door CLI te vormen, waar de verbinding van het telnet van binnenuit aan het buitennetwerk op weekdagen tijdens zakenuren wordt toegestaan:

Opmerking: Een tijdgebaseerde ACL kan op basis van uw vereisten worden gedefinieerd via de Fast Ethernet-poort of de Radio-poort van Aironet AP. Het wordt nooit toegepast op de Bridge Group Virtual Interface (BVI).

1. Meld u aan bij de AP via de CLI.Gebruik de console poort of telnet om ACL door de Ethernet interface of de draadloze interface te gebruiken.
2. Geef de configuratie van de configuratie op in het AP-CLI:
   AP#**configure terminal**

3. Maak een tijdbereik. Om dit te doen geeft u deze opdracht uit in de mondiale configuratiemodus:
   AP<config>#**time-range Test**
   !--- Create a time-range with name Test. AP(config-time-range)# **periodic weekdays 7:00 to 19:00**

```
!--- Allows access to users during weekdays from 7:00 to 19:00 hrs.
```

4. Maak een ACL 101:

```
AP<config># ip access-list extended 101
AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
Test
!--- This ACL permits Telnet traffic to and from !--- the network for the specified time-
range Test.
```

   Dit ACL maakt een Telnet-sessie naar AP in week toe.

5. Geef deze opdracht uit om deze op tijd gebaseerde ACL op de Ethernet-interface toe te passen:

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in

!--- Apply the time-based ACL.
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

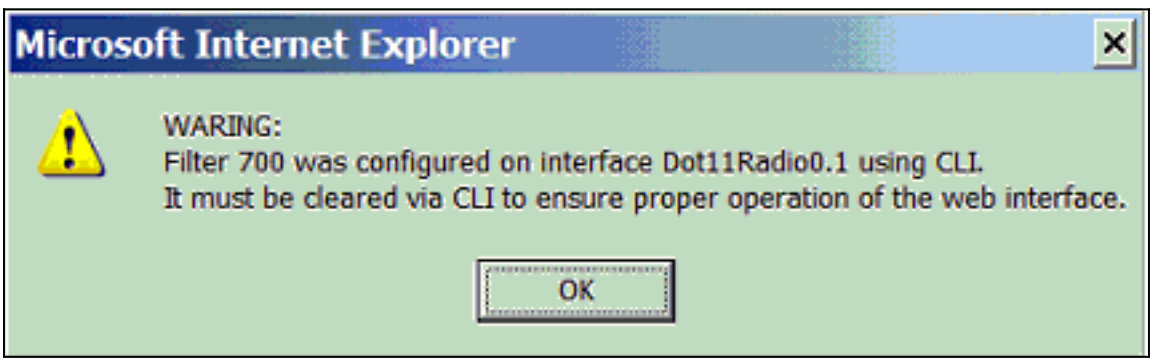
Voltooi deze stappen om een ACL uit een interface te verwijderen:

1. Ga naar de interfacemodi.
2. Voer **nr** voor de opdracht van de **ip access-group in**, zoals dit voorbeeld toont:

```
interface interface
no ip access-group {access-list-name | access-list-number} {in | out}
```

U kunt ook de *naam van* de **showaccess-list** gebruiken **|** ***number*** **opdracht** om problemen op te lossen met uw configuratie. Het bevel **om ip toegang-lijst te tonen** verstrekt een pakkettelling die toont welke ACL ingang wordt geraakt.

Vermijd het gebruik van zowel de CLI als de web-browser interfaces om het draadloze apparaat te configureren. Als u het draadloze apparaat met de CLI configureren kan de web-browser interface een onnauwkeurige interpretatie van de configuratie weergeven. De onnauwkeurigheid betekent echter niet noodzakelijkerwijs dat het draadloze apparaat verkeerd is geconfigureerd. Als u bijvoorbeeld ACL's met de CLI configureren kan de webbrowser-interface dit bericht weergeven:



Als u dit bericht ziet, gebruikt u de CLI om de ACL's te verwijderen en gebruikt u de web-browser interface om ze aan te passen.

Gerelateerde informatie

- Filters configureren
- Draadloze ondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems