Configuratievoorbeeld van ACL-filters op Aironet APâ€™s

Inhoud

Inleiding

Dit document beschrijft hoe u op ACL-filters (Access Control List) kunt configureren op basis van Cisco Aironet access points (APâ€™s) met gebruik van de GUI.

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis te hebben van deze onderwerpen:

- De configuratie van een draadloze verbinding met gebruik van een Aironet AP en een Aironet 802.11 a/b/g clientadapter
- ACLâ€™s

Gebruikte componenten

Dit document maakt gebruik van Aironet 1040 Series APâ€™s waarop Cisco IOS®-softwarerelease 15.2(2)JB wordt uitgevoerd.

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.

Achtergrondinformatie

U kunt filters op AP's gebruiken om deze taken uit te voeren:

- Toegang tot het draadloze LAN (WLAN)-netwerk beperken
- Een extra beveiligingslaag voor draadloos LAN bieden

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

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

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

Op protocollen gebaseerde filters bieden een korreliger manier om de toegang tot specifieke protocollen via de Ethernet- en radio-interfaces van het toegangspunt te beperken. U kunt deze methoden gebruiken om de filters op de toegangspunten te configureren:

- Web GUI
- CLI

Dit document legt uit hoe ACLâ€™s moeten worden gebruikt om filters via de GUI te configureren.

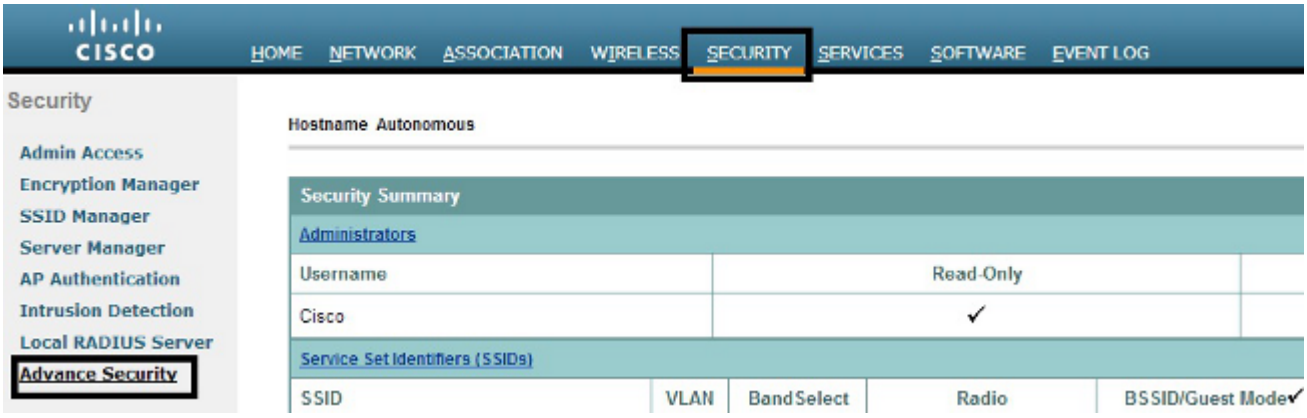
> **Opmerking**: Raadpleeg voor meer informatie over de configuratie door het gebruik van de CLI het Cisco-artikel Voorbeeld van configuratie van ACL-filter voor access point.

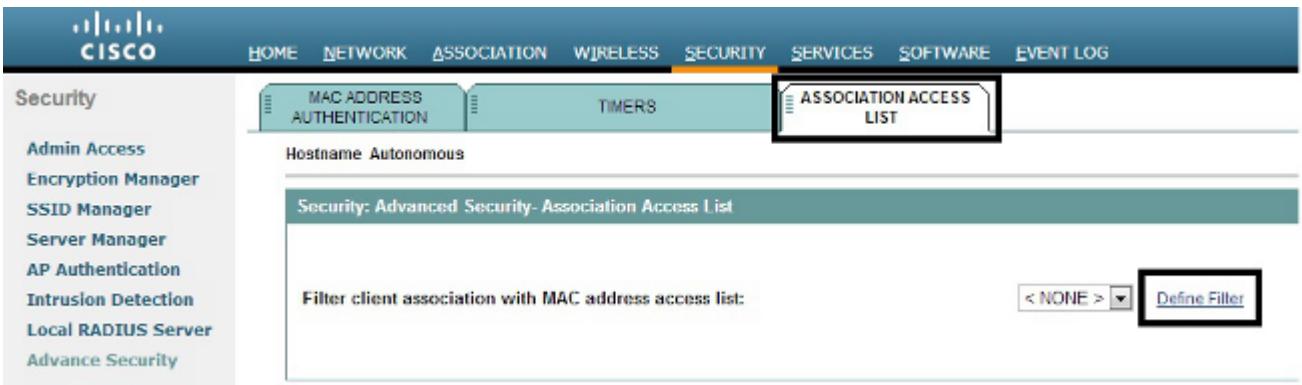
Configureren

In deze sectie wordt beschreven hoe u op ACL gebaseerde filters kunt configureren op Cisco Aironet APâ€™s met gebruik van de GUI.

Waar ACLâ€™s moeten worden gemaakt

Ga naar **Beveiliging** > **Geavanceerde beveiliging**. Kies het tabblad **Associatietoegangslijst** en klik op **Filter definiëren**:



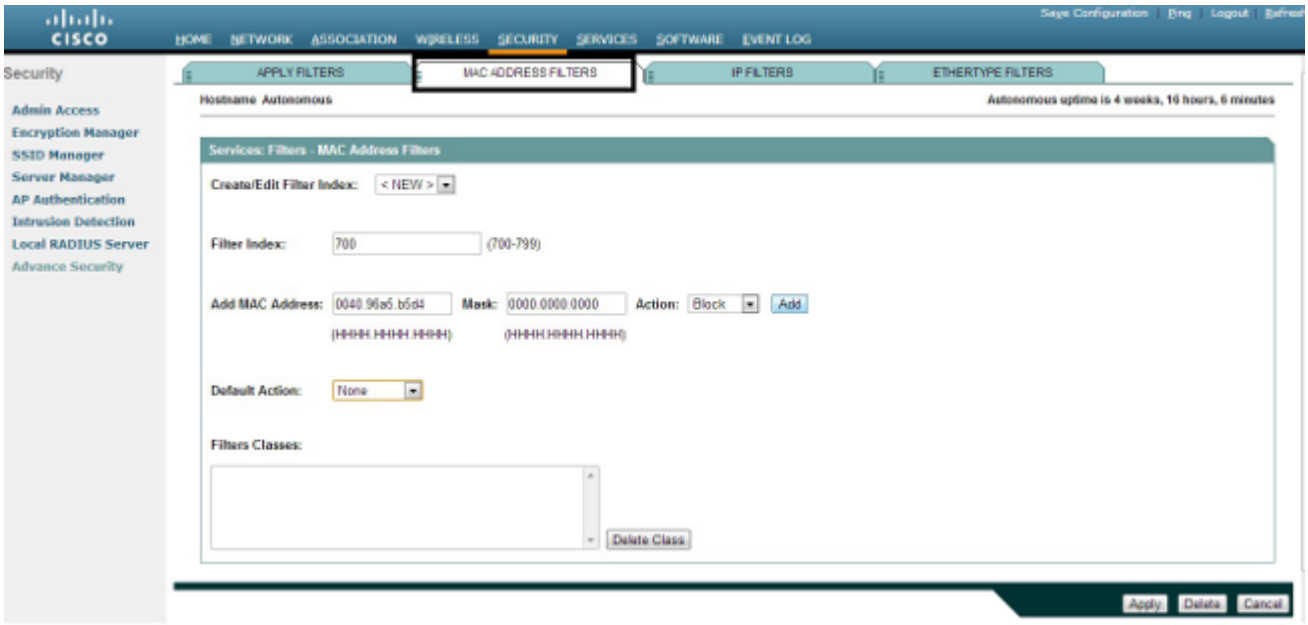


MAC-adresfilters

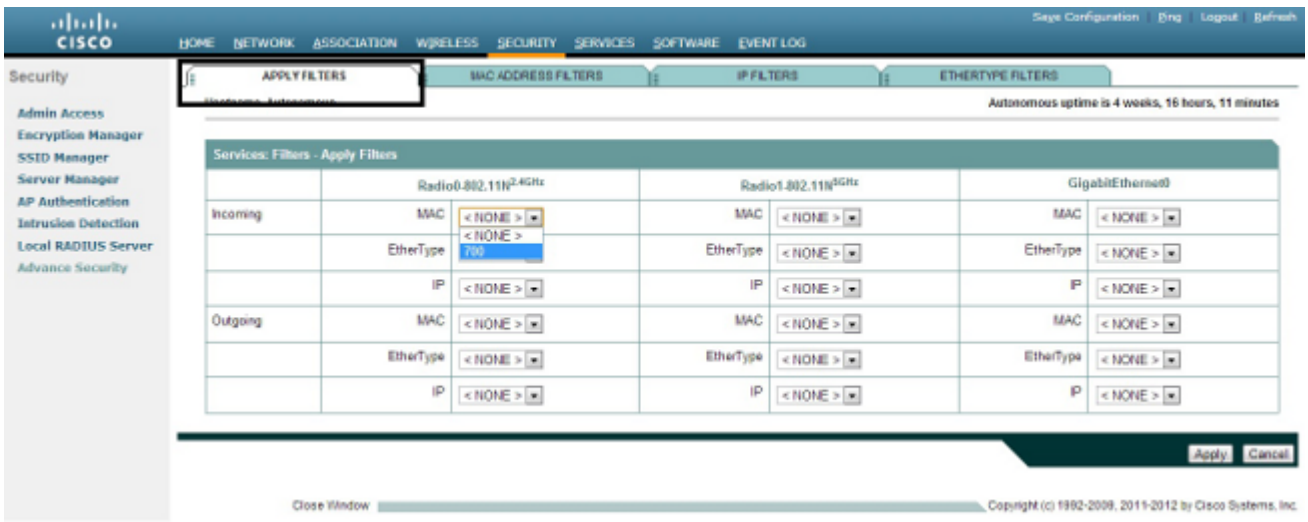
U kunt op MAC-adres gebaseerde filters gebruiken om clientapparaten te filteren op basis van het hardgecodeerde MAC-adres. Wanneer een client toegang wordt geweigerd via een op MAC gebaseerd filter, kan de client geen koppeling maken met het toegangspunt. Met MAC-adresfilters kan of kan het doorsturen van unicast- en multicast-pakketten die zijn verzonden van of zijn gericht aan specifieke MAC-adressen, worden verboden.

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

1. Maak het MAC-adres **ACL 700**. Met deze ACL kan de client **0040.96a5.b5d4** niet aan het AP worden gekoppeld.



2. Klik op **Add** om dit filter toe te voegen aan de Filterklassen. U kunt de standaardactie ook definiëren als **Alles doorsturen** of **Alles weigeren**.
3. Klik op Apply (Toepassen). **ACL 700** wordt nu gemaakt.
4. Als u **ACL 700** op een radio-interface wilt toepassen, navigeert u naar het gedeelte **Filters toepassen**. U kunt deze ACL nu toepassen op een inkomende of uitgaande radio of Gigabit Ethernet-interface.



IP-filters

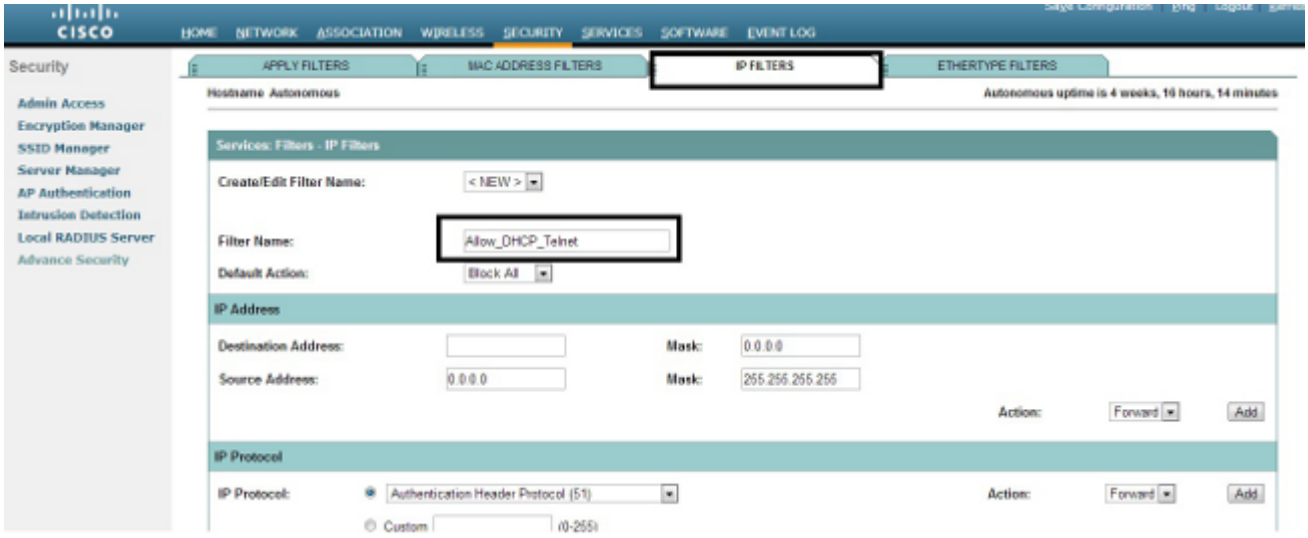
U kunt standaard of uitgebreide ACLâ€™s gebruiken om de toegang van clientapparaten tot het WLAN-netwerk toe te staan of te verbieden op basis van het IP-adres van de client.

Dit configuratievoorbeeld gebruikt uitgebreide ACLâ€™s. Uitgebreide ACL moet Telnet-toegang tot de clients toestaan. U moet alle andere protocollen op het WLAN-netwerk beperken. Ook gebruiken de clients DHCP om het IP-adres te verkrijgen. U moet een uitgebreide ACL maken die:

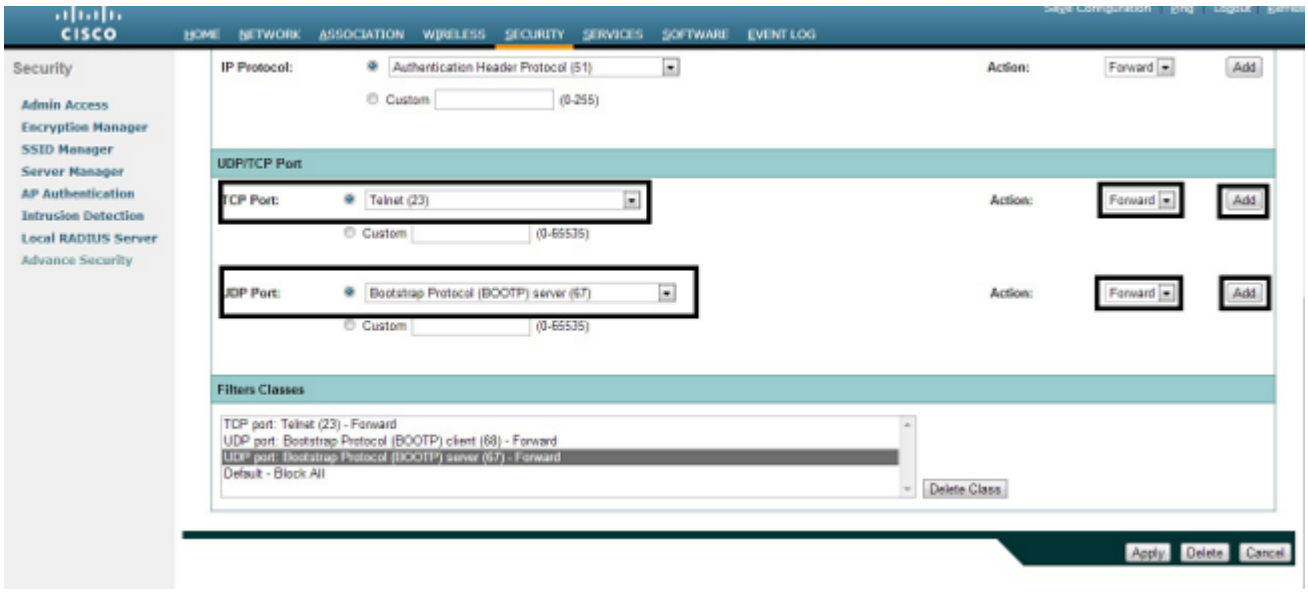
- Maakt DHCP- en Telnet-verkeer mogelijk
- Ontkent alle andere verkeerstypen

Voltooi de volgende stappen om een bestand te maken:

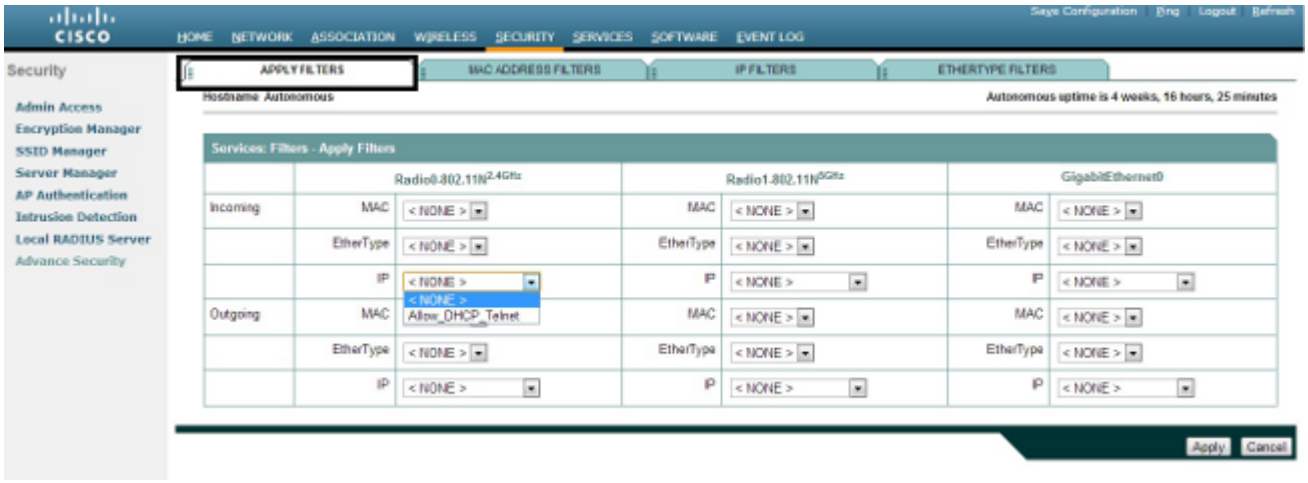
1. Geef het filter een naam en selecteer **Alles blokkeren** in de vervolgkeuzelijst **Standaardactie**, omdat het resterende verkeer moet worden geblokkeerd:



2. Selecteer Telnet in de vervolgkeuzelijst **TCP-poort** en **BOOTP-client**- en **BOOTP-server** in de **vervolgkeuzelijst UDP**-poort:



3. Klik op **Apply (Toepassen).** Het IP-filter **Allow_DHCP?_Telnet** is nu gemaakt en u kunt deze ACL toepassen op een inkomende of uitgaande radio of Gigabit Ethernet-interface.

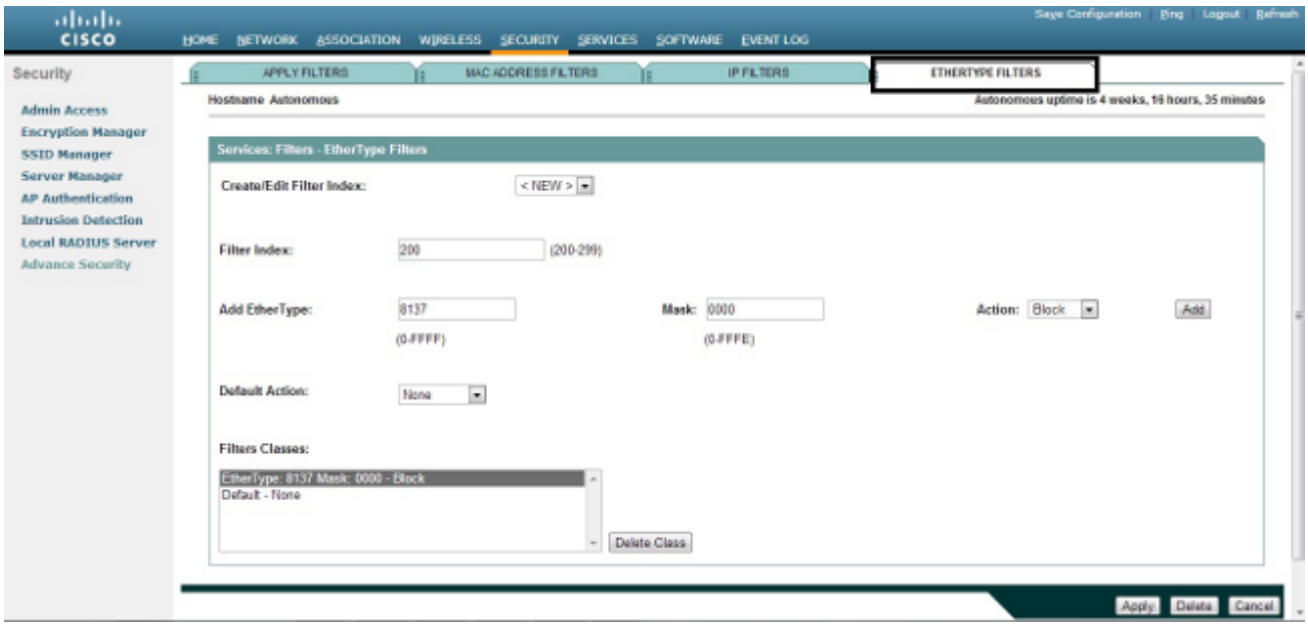


Ethertype-filters

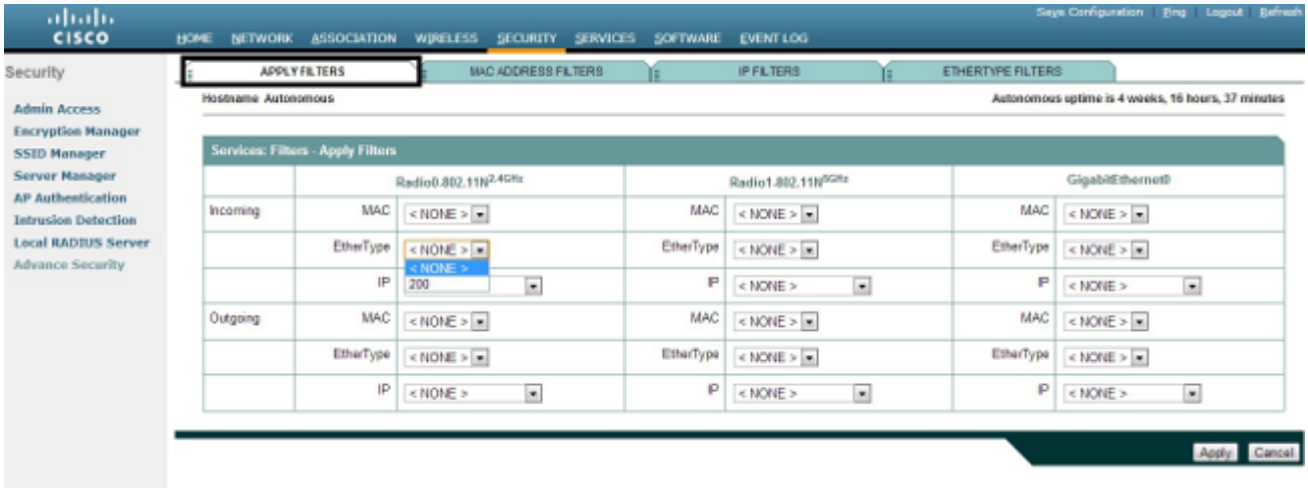
U kunt Ethertype-filters gebruiken om IPX-verkeer (Internetwork Packet Exchange) op Cisco Aironet AP te blokkeren. Een typische situatie waar dit nuttig is, is wanneer IPX-server uitzendt de draadloze verbinding verstikken, wat soms gebeurt op een groot ondernemingsnetwerk.

Voltooi deze stappen om een filter te configureren en toe te passen dat IPX-verkeer blokkeert:

1. Klik op het tabblad **Filters Ethernet**.
2. Noem het filter in het veld **Filter Index** met een nummer van 200 tot 299. Het nummer dat u toewijst, maakt een ACL voor het filter.
3. Typ **8137** in het veld **Add Ethertype**.
4. Laat het masker voor het Ethertype in het **veld Masker** staan op de standaardwaarde.
5. Selecteer **Blok** in het actiemenu en klik op **Toevoegen**.



6. Om Ethertype uit de lijst van de Klassen van Filters te verwijderen, selecteer het, en klik de **Klasse van de Schrapping**. Herhaal de vorige stappen en voeg de typen **8138**, **00ff** en **00e0** aan het filter toe. U kunt deze ACL nu toepassen op een inkomende of uitgaande radio of Gigabit Ethernet-interface.


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENT LOG
Security
Admin Access
Encryption Manager
SSID Manager
Server Manager
AP Authentication
Intrusion Detection
Local RADIUS Server
Advance Security
APPLY FILTERS
MAC ADDRESS FILTERS
IP FILTERS
ETHERTYPE FILTERS
Hostname Autonomous
Autonomous uptime is 4 weeks, 16 hours, 37 minutes
Services: Filters - Apply Filters
Radio0-802.11N2.4GHz
Radio1-802.11N5GHz
GigabitEthernet0
Incoming
Outgoing
MAC
EtherType
IP
< NONE >
200
Apply
Cancel

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.