Filtros ACL en el ejemplo de configuración del Aironet AP

Contenido

Introducción

Este documento describe cómo configurar la lista de control de acceso (ACL) - los filtros basados en el (APS) de los Puntos de acceso del Cisco Aironet con el uso del GUI.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- La configuración de una conexión de red inalámbrica con el uso de un Aironet AP y de un adaptador del cliente del a/b/g del 802.11 del Aironet
- ACL

Componentes Utilizados

Este documento utiliza las 1040 Series AP del Aironet que funcionan con el Software Release 15.2(2)JB del ® del Cisco IOS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Usted puede utilizar los filtros en los AP para realizar estas tareas:

- Restrinja el acceso a la red del Wireless LAN (red inalámbrica (WLAN))
- Proporcione una capa adicional de seguridad de red inalámbrica

Usted puede utilizar diversos tipos de filtrar tráfico de los filtros para basado encendido:

- Protocolos específicos
- La dirección MAC del dispositivo del cliente
- La dirección IP del dispositivo del cliente

Usted puede también permitir a los filtros para restringir el tráfico de los usuarios en el LAN cableado. Los filtros de la dirección IP y de la dirección MAC permiten o rechazan la expedición del unicast y de los paquetes de multidifusión que se envían a o desde el IP o las direcciones MAC específico.

Los filtros basados en protocolos proporcionan una manera más granular de restringir el acceso a los protocolos específicos a través de los Ethernetes y de las interfaces radio del AP. Usted puede utilizar cualquiera de estos métodos para configurar los filtros en los AP:

- Red GUI
- CLI

Este documento explica cómo utilizar los ACL para configurar los filtros con el GUI.

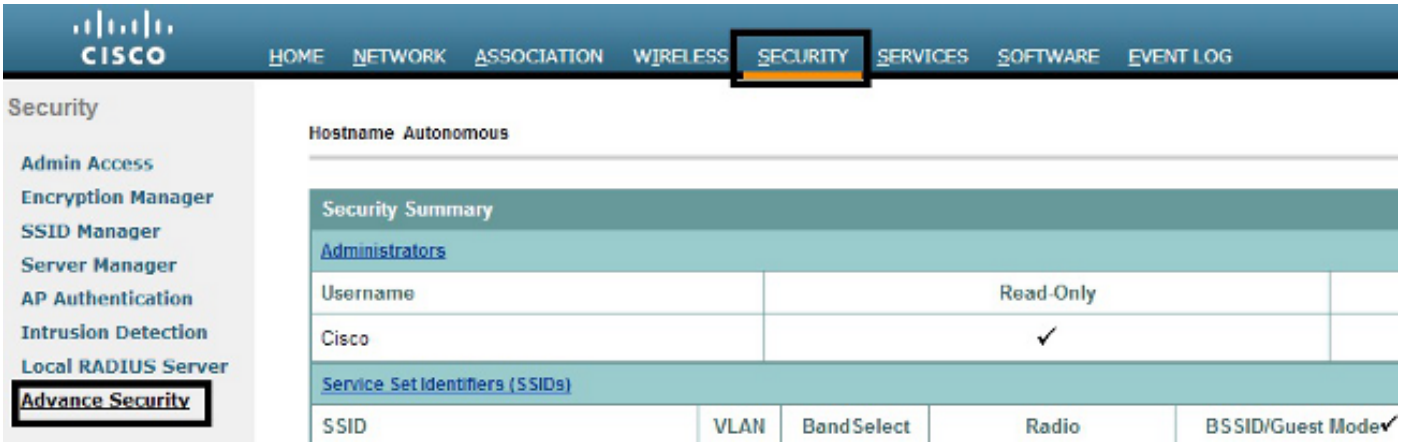
> **Note**: Para más información sobre la configuración con el uso del CLI, refiera al artículo de Cisco del ejemplo de la configuración de filtro del Punto de acceso ACL.

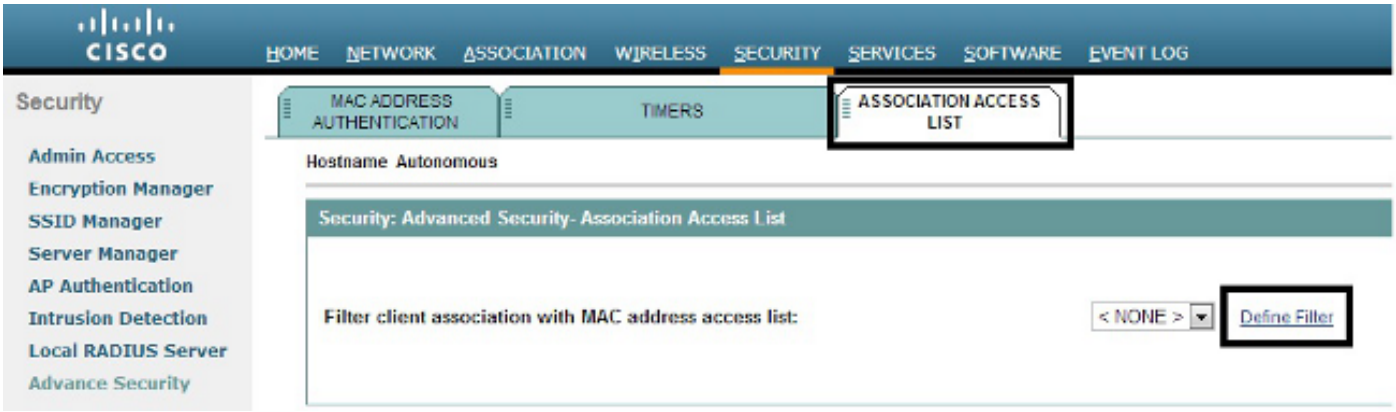
Configurar

Esta sección describe cómo configurar los filtros ACL-basados en el Cisco Aironet AP con el uso del GUI.

Donde crear los ACL

Navegue a la **Seguridad** > a la **Seguridad del avance**. Elija la lengueta de la **lista de acceso de la asociación**, y el tecleo **define el filtro**:



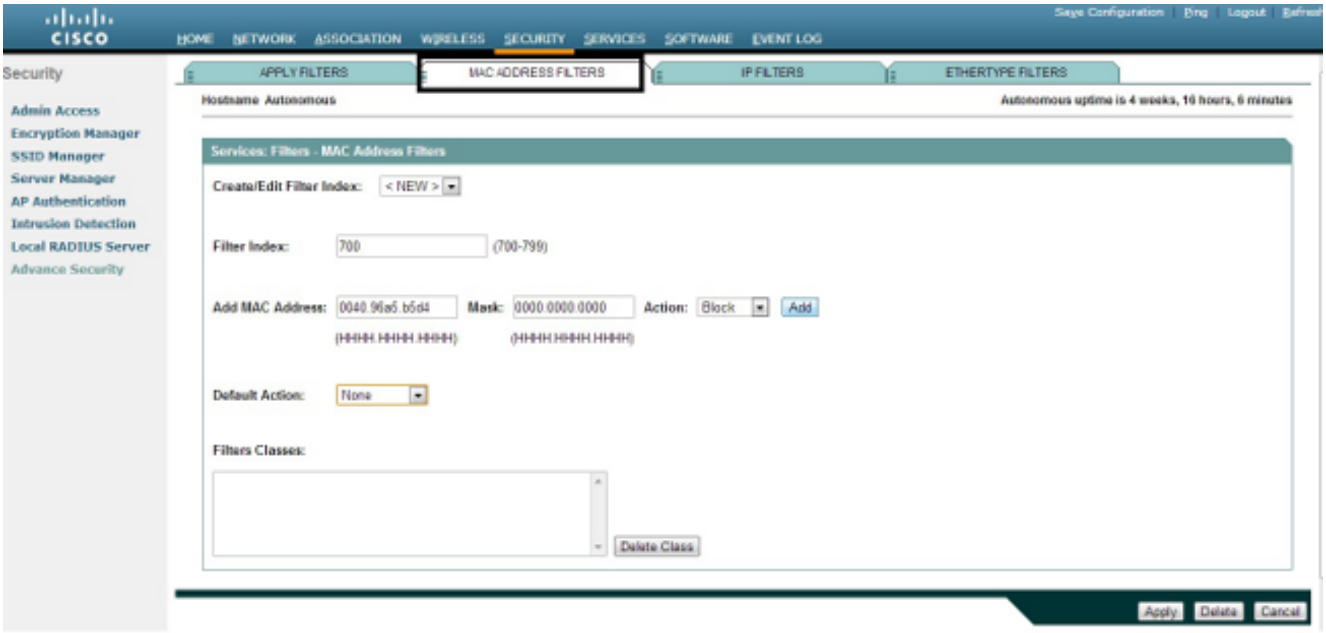


Filtros de la dirección MAC

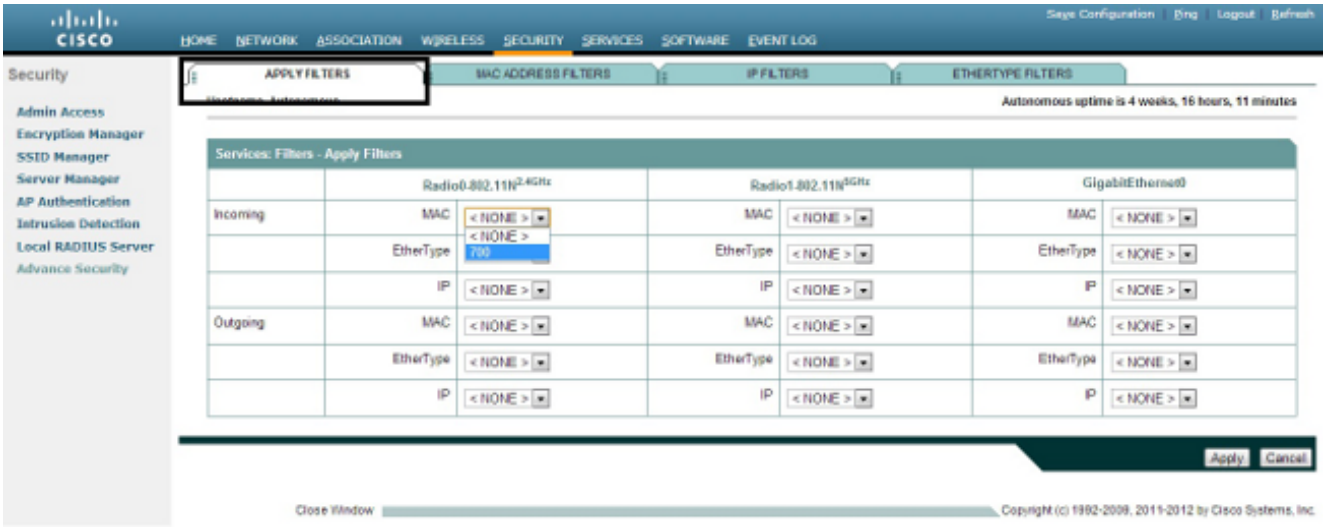
Usted puede utilizar los filtros del direccionamiento basado MAC para filtrar los dispositivos del cliente basados en la dirección MAC codificada por hardware. Cuando niegan un cliente el acceso a través de un filtro MAC basado, el cliente no puede asociarse al AP. Los filtros de la dirección MAC permiten o rechazan la expedición del unicast y de los paquetes de multidifusión enviados, o dirigidos, a las direcciones MAC específicas.

Este ejemplo ilustra cómo configurar un filtro MAC basado con el GUI para filtrar al cliente con una dirección MAC de **0040.96a5.b5d4**:

1. Cree la dirección MAC **ACL 700**. Este ACL no permite que el cliente **0040.96a5.b5d4** se asocie al AP.



2. El tecleo **agrega** para agregar este filtro a las clases de los filtros. Usted puede también definir la acción predeterminada como **delantero todo** o **negar todos**.
3. Haga clic en Apply (Aplicar). **El ACL 700** ahora se crea.
4. Para aplicar **ACL 700 a una** interfaz radio, navegue a la sección de los **filtros de la aplicación**. Usted puede ahora aplicar este ACL a una interfaz entrante o saliente de la radio o del gigabitethernet.



Filtros IP

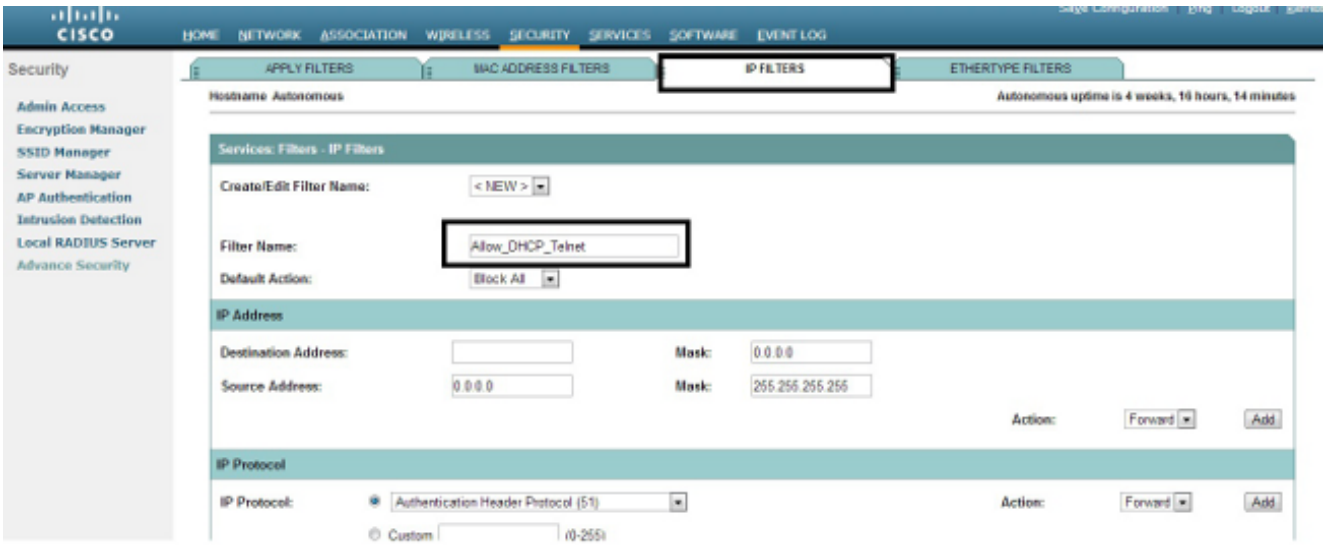
Usted puede utilizar el estándar o los ACL ampliados para permitir o rechazar la entrada de los dispositivos del cliente en la red WLAN basada en la dirección IP del cliente.

Este ejemplo de configuración utiliza los ACL ampliados. El ACL ampliado debe permitir el acceso de Telnet a los clientes. Usted debe restringir el resto de los protocolos en la red WLAN. También, los clientes utilizan el DHCP para obtener la dirección IP. Usted debe crear un ACL ampliado eso:

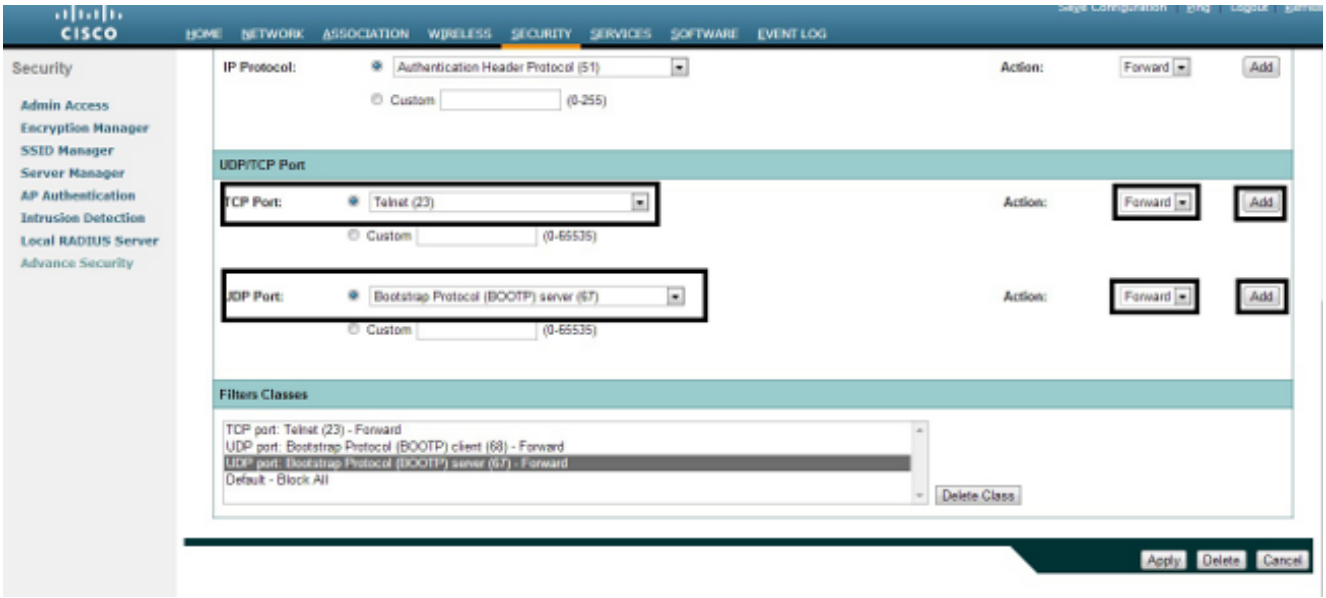
- Permite el DHCP y el tráfico de Telnet
- Niega el resto de los tipos de tráfico

Complete estos pasos para crearlo:

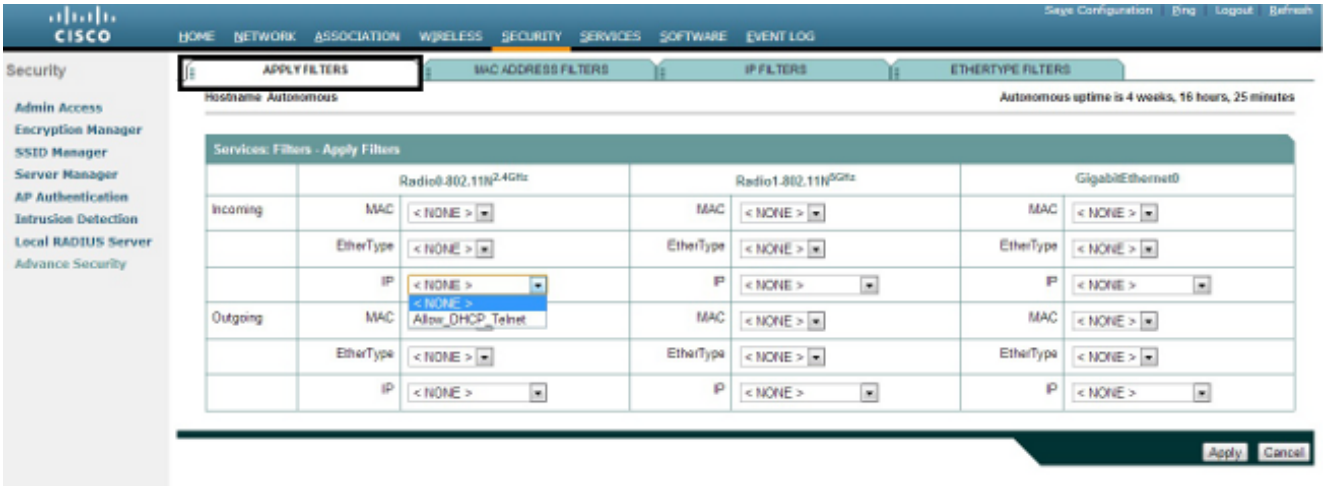
1. Nombre el filtro, y seleccione el **bloque todo de la** lista desplegable de la **acción predeterminada**, puesto que el tráfico restante debe ser bloqueado:



2. Seleccione **Telnet de la** lista desplegable del **puerto TCP**, y **cliente BOOTP** y del **servidor BOOTP de la** lista desplegable del **puerto UDP**:



3. Haga clic en Apply (Aplicar). **¿El filtro IP Allow_DHCP? el _Telnet** ahora se crea, y usted puede aplicar este ACL a una interfaz entrante o saliente de la radio o del gigabitethernet.

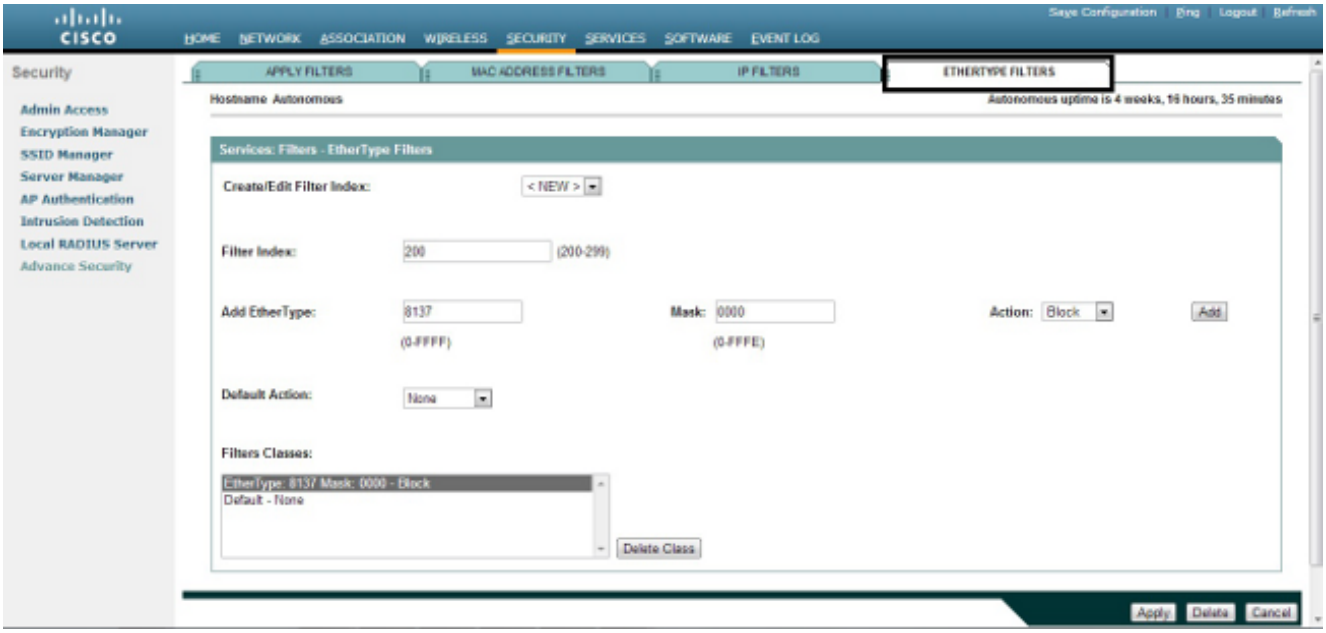


Filtros del Ethertype

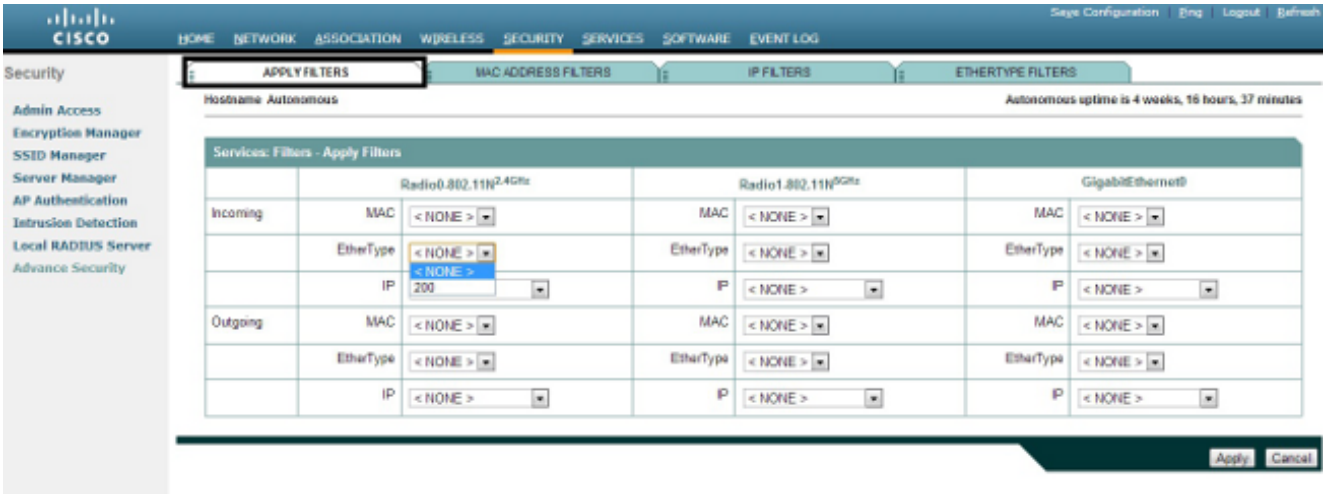
Usted puede utilizar los filtros del Ethertype para bloquear el tráfico del Intercambio de paquetes entre redes (IPX) en el Cisco Aironet AP. Una situación típica donde está útil esto está cuando los broadcasts del servidor IPX obstruyen el link de red inalámbrica, que sucede a veces en una red para empresas grande.

Complete estos pasos para configurar y aplicar un filtro que bloquee el tráfico IPX:

1. Haga clic la lengueta de los **filtros del Ethertype**.
2. En el **campo índice del filtro**, nombre el filtro con un número a partir del 200 a 299. El número que usted asigna crea un ACL para el filtro.
3. Ingrese **8137** en el campo del **Ethertype del agregar**.
4. Deje la máscara para el Ethertype en el **campo de la máscara** en el valor predeterminado.
5. Seleccione el **bloque del** Menú Action (Acción), y el haga click en Add



6. Para quitar el Ethertype de la lista de clases de los filtros, seleccionarlo, y hacer clic la **clase de la cancelación**. Relance los pasos anteriores, y agregue los tipos **8138**, **00ff**, y **00e0 al** filtro. Usted puede ahora aplicar este ACL a una interfaz entrante o saliente de la radio o del gigabitethernet.


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