Ejemplo de Configuración de Filtros ACL en AP Aironet

Contenido

Introducción

Este documento describe cómo configurar filtros basados en listas de control de acceso (ACL) en puntos de acceso (AP) Cisco Aironet con el uso de la GUI.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- La configuración de una conexión inalámbrica con el uso de un Aironet AP y un Aironet 802.11 a/b/g Client Adapter
- Listas de control de acceso (ACL)

Componentes Utilizados

Este documento utiliza los AP Aironet 1040 Series que ejecutan Cisco IOS® software Release 15.2(2)JB.

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). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Puede utilizar filtros en los AP para realizar estas tareas:

- Restringir el acceso a la red LAN inalámbrica (WLAN)
- Proporcionar una capa adicional de seguridad inalámbrica

Puede utilizar diferentes tipos de filtros para filtrar el tráfico basado en:

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

También puede activar filtros para restringir el tráfico de los usuarios en la LAN por cable. Los filtros de direcciones IP y MAC permiten o no el reenvío de paquetes de unidifusión y multidifusión enviados a o desde direcciones IP o MAC específicas.

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

- GUI web
- CLI

Este documento explica cómo utilizar las ACL para configurar filtros a través de la GUI.

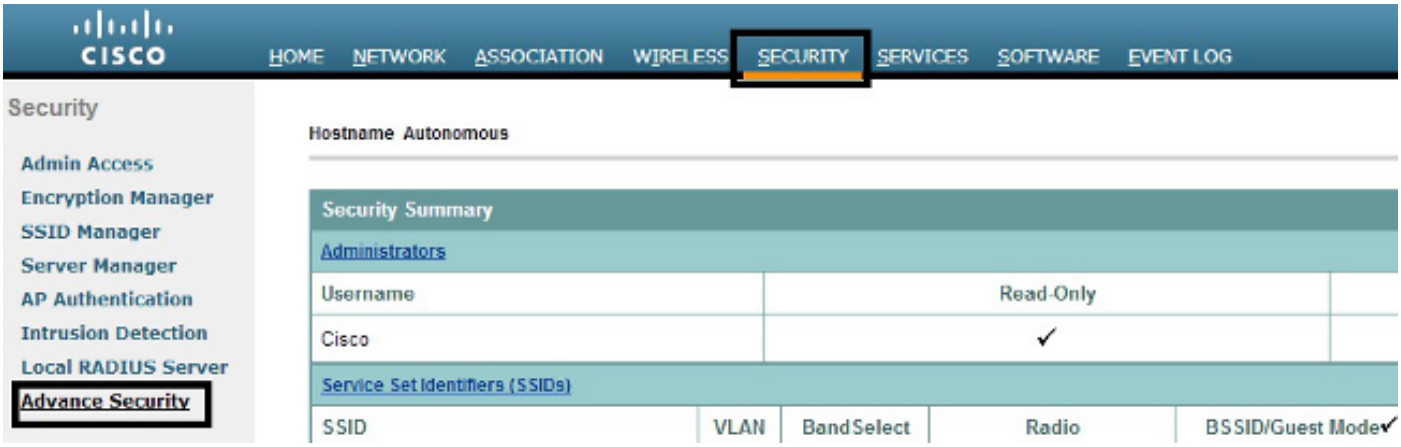
> Nota: Para obtener más información sobre la configuración mediante el uso de la CLI, consulte el artículo Ejemplo de configuración del filtro ACL del punto de acceso Cisco.

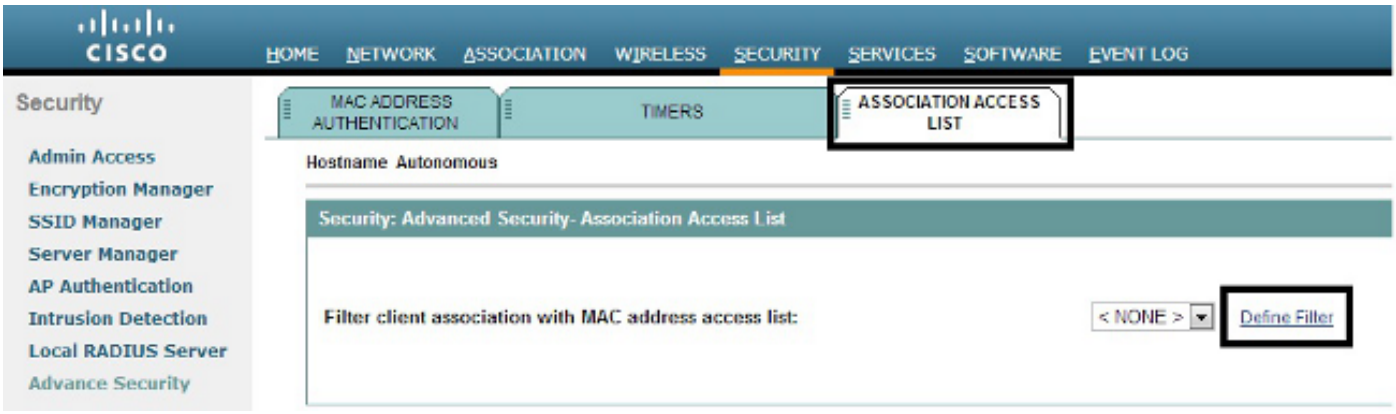
Configurar

Esta sección describe cómo configurar filtros basados en ACL en Cisco Aironet AP con el uso de la GUI.

Dónde crear ACL

Vaya a Seguridad > Seguridad avanzada. Elija la pestaña Association Access List y haga clic en Define Filter:



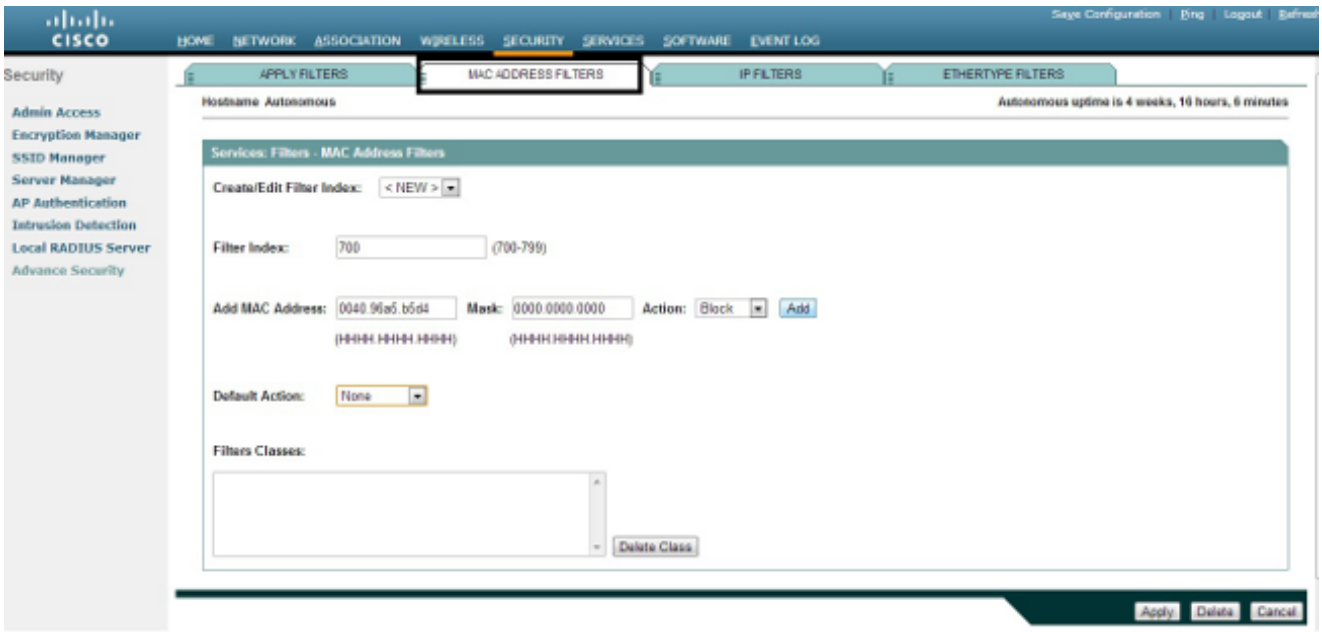


Filtros de dirección MAC

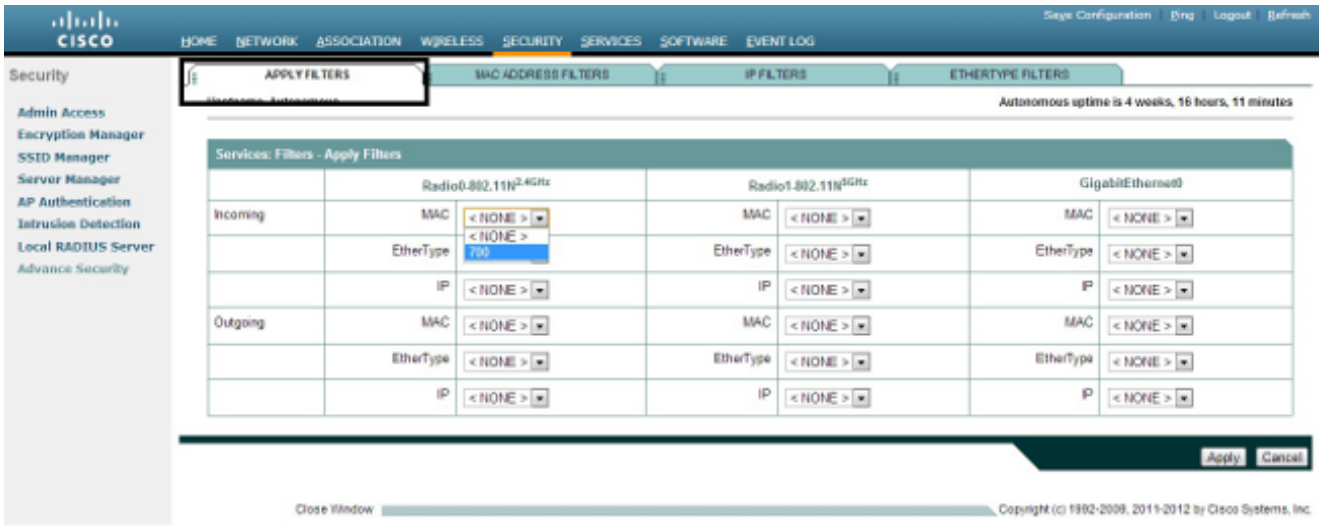
Puede utilizar filtros basados en direcciones MAC para filtrar los dispositivos cliente basados en la dirección MAC codificada de forma rígida. Cuando a un cliente se le niega el acceso a través de un filtro basado en MAC, el cliente no puede asociarse con el AP. Los filtros de direcciones MAC permiten o no el reenvío de paquetes de unidifusión y multidifusión enviados desde direcciones MAC específicas o dirigidos a ellas.

Este ejemplo ilustra cómo configurar un filtro basado en MAC a través de la GUI para filtrar el cliente con una dirección MAC de 0040.96a5.b5d4:

1. Cree la dirección MAC ACL 700. Esta ACL no permite que el cliente 0040.96a5.b5d4 se asocie con el AP.



2. Haga clic en Agregar para agregar este filtro a las Clases de Filtros. También puede definir la acción predeterminada como Reenviar todas o Denegar todas.
3. Haga clic en Apply (Aplicar). ACL 700 se ha creado.
4. Para aplicar ACL 700 a una interfaz de radio, navegue hasta la sección Aplicación de Filtros. Ahora puede aplicar esta ACL a una Radio entrante o saliente o a una interfaz GigabitEthernet.



Filtros IP

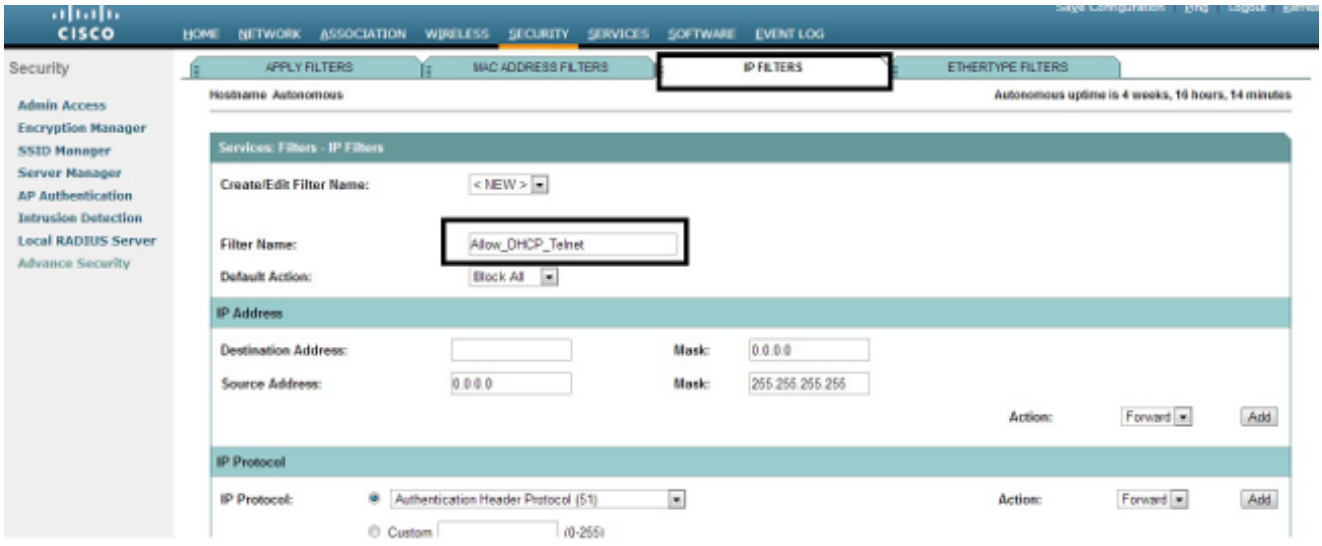
Puede utilizar ACL estándar o extendidas para permitir o no la entrada de dispositivos cliente en la red WLAN basada en la dirección IP del cliente.

Este ejemplo de configuración utiliza ACL extendidas. La ACL extendida debe permitir el acceso Telnet a los clientes. Debe restringir todos los demás protocolos de la red WLAN. Además, los clientes utilizan DHCP para obtener la dirección IP. Debe crear una lista de control de acceso ampliada que:

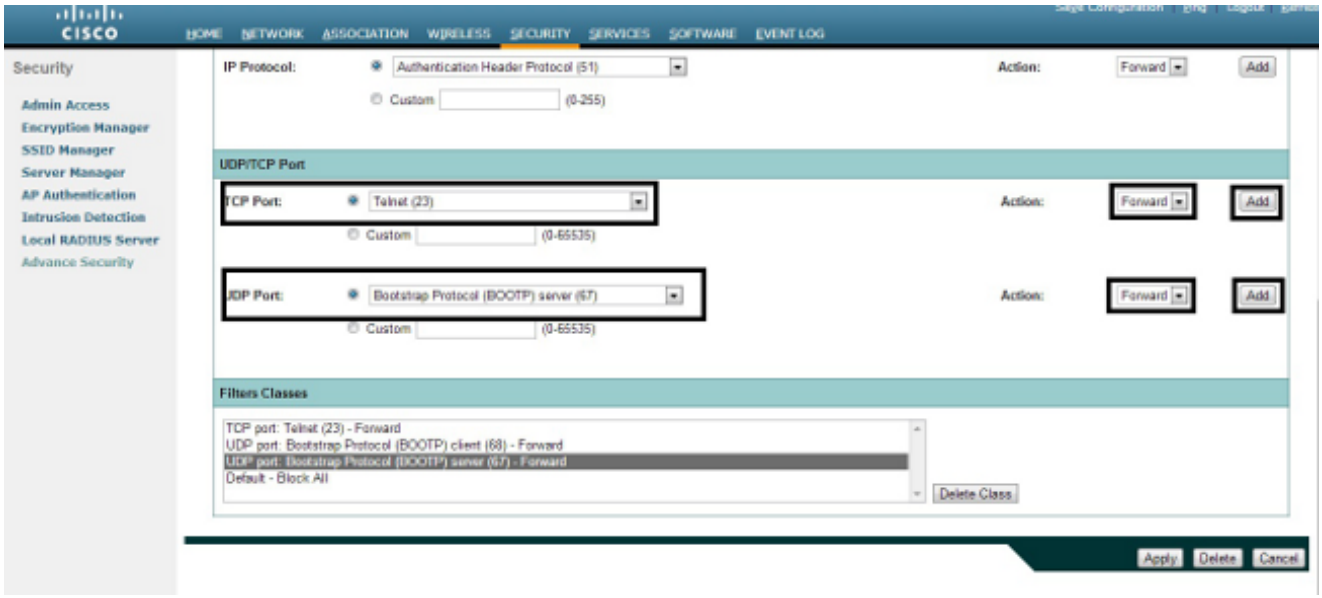
- Permite el tráfico DHCP y Telnet
- Niega todos los demás tipos de tráfico

Complete estos pasos para crearlo:

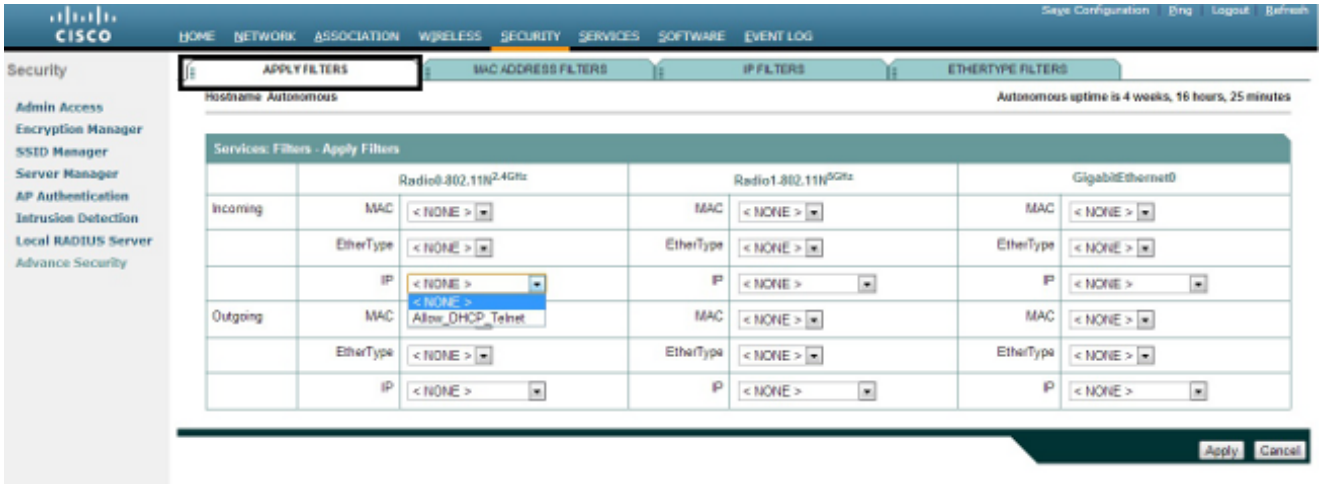
1. Asigne un nombre al filtro y seleccione Block All en la lista desplegable Default Action, ya que el tráfico restante debe bloquearse:



2. Seleccione Telnet en la lista desplegable TCP Port y BOOTP client & BOOTP server en la lista desplegable UDP Port:



3. Haga clic en Apply (Aplicar). Ahora se crea el filtro IP Allow_DHCP?_Telnet, y puede aplicar esta ACL a una Radio entrante o saliente o a una interfaz GigabitEthernet.



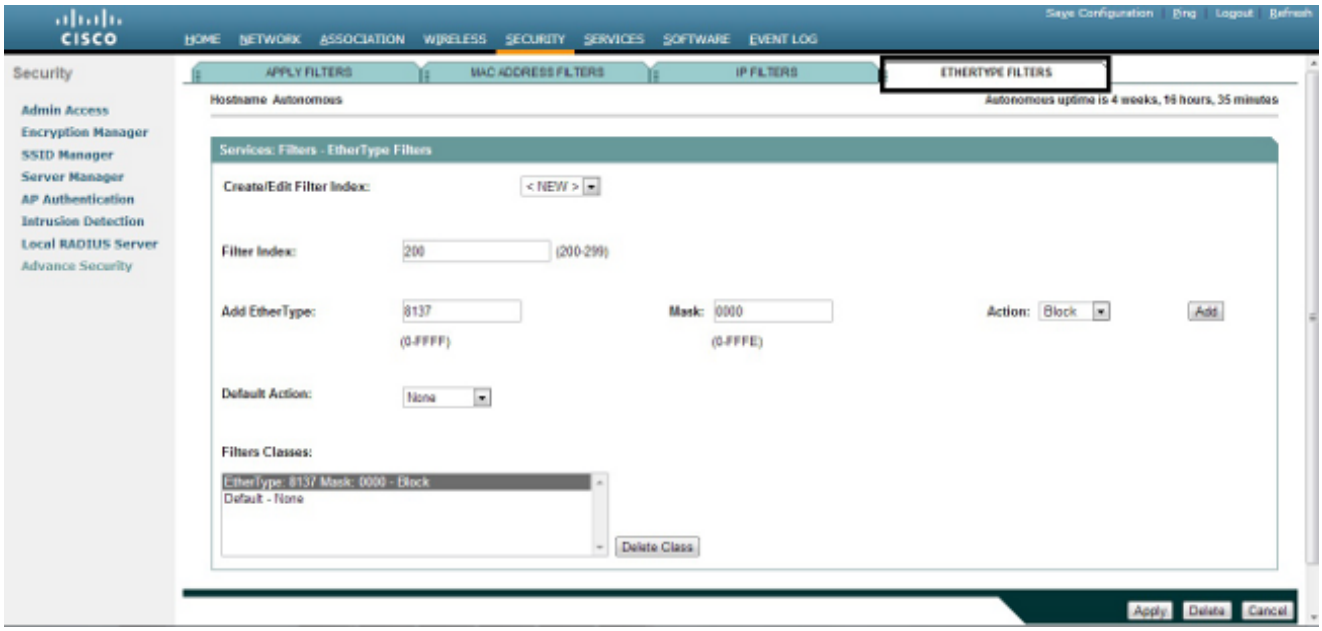
Filtros Ethertype

Puede utilizar los filtros Ethertype para bloquear el tráfico Internetwork Packet Exchange (IPX) en el Cisco Aironet AP. Una situación típica en la que esto es útil es cuando las transmisiones del servidor IPX bloquean el link inalámbrico, lo que a veces sucede en una red empresarial grande.

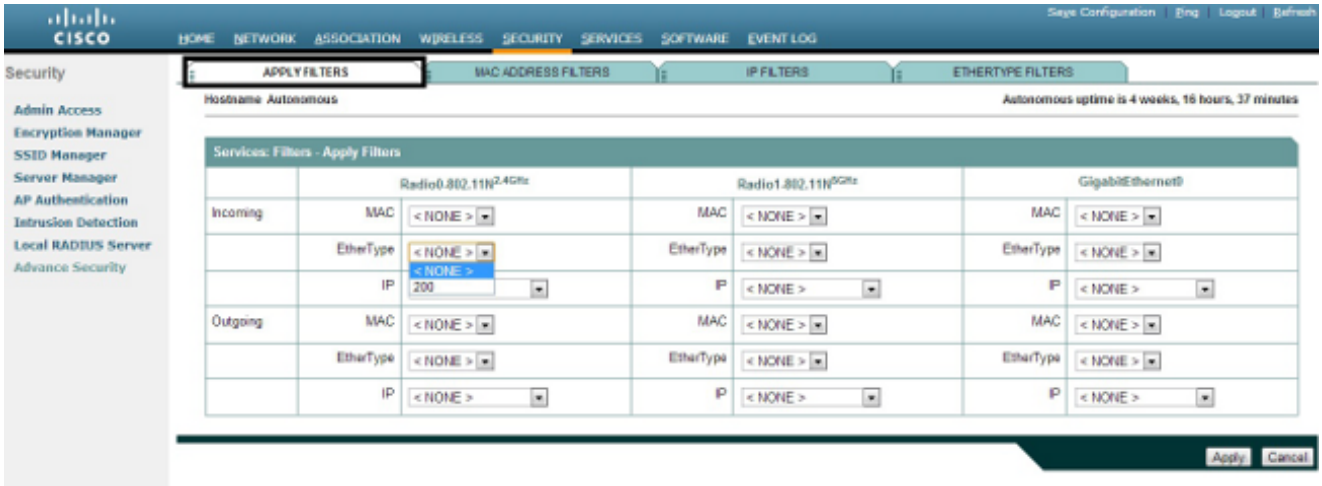
Complete estos pasos para configurar y aplicar un filtro que bloquee el tráfico IPX:

1. Haga clic en la pestaña Ethertype Filters.
2. En el campo Filter Index, asigne al filtro un nombre con un número entre 200 y 299. El número que asigne creará una ACL para el filtro.
3. Ingrese 8137 en el campo Add Ethertype.
4. Deje la máscara para el Ethertype en el campo Mask en el valor predeterminado.

5. Seleccione Block en el menú action y haga clic en Add.



6. Para quitar el Ethertype de la lista de las clases de los filtros, selecciónelo, y haga clic en Borrar clase. Repita los pasos anteriores y agregue los tipos 8138, 00ff y 00e0 al filtro. Ahora puede aplicar esta ACL a una Radio entrante o saliente o a una interfaz GigabitEthernet.



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).