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 Cisco Aironet (AP) con el uso de la GUI.

prerrequisitos

Requisitos

Cisco recomienda que tenga 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 Aironet 1040 Series AP 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).Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Puede utilizar filtros en los AP para realizar estas tareas:

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

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

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

También puede habilitar los filtros para restringir el tráfico de los usuarios en la LAN por cable. Los filtros de dirección IP y dirección MAC permiten o no permitir el reenvío de paquetes unidifusión y multidifusión que se envían 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.

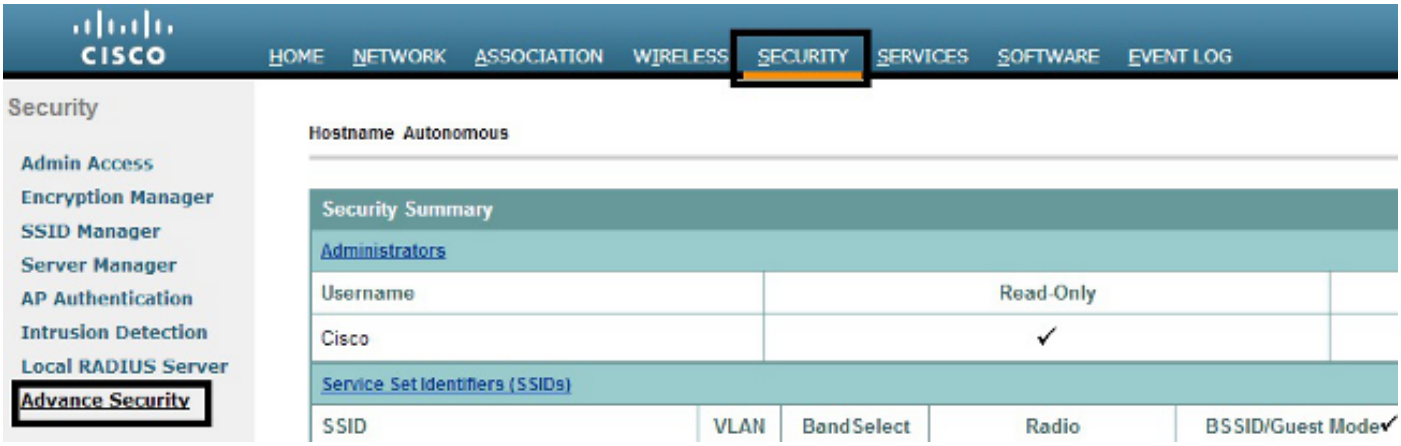
> Nota: Para obtener más información sobre la configuración mediante el uso de la CLI, refiérase al artículo de Cisco Ejemplo de Configuración del Filtro ACL del Punto de Acceso.

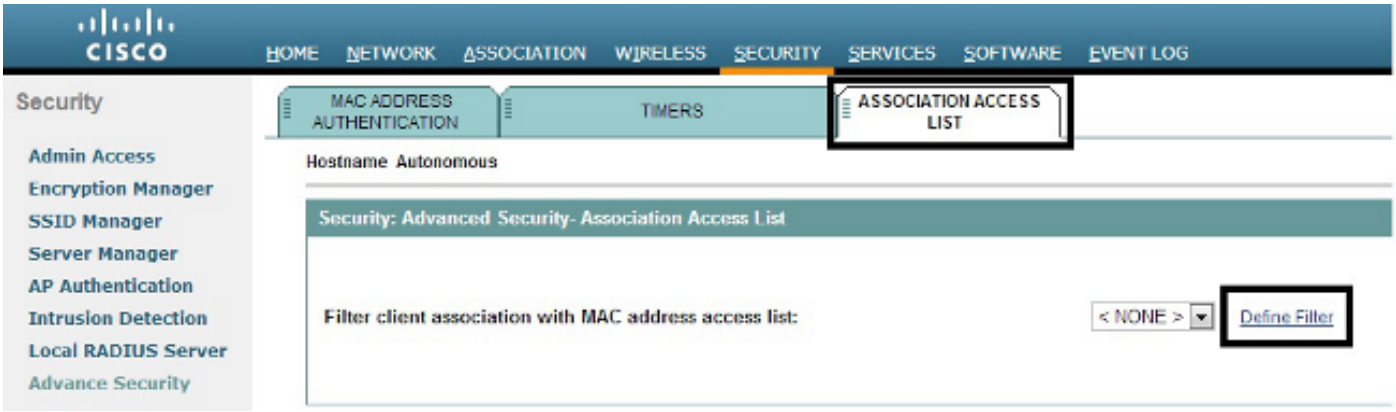
Configurar

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

Dónde crear ACL

Vaya a **Seguridad > Seguridad avanzada**. Elija la pestaña **Lista de Acceso de Asociación** y haga clic en **Definir Filtro**:



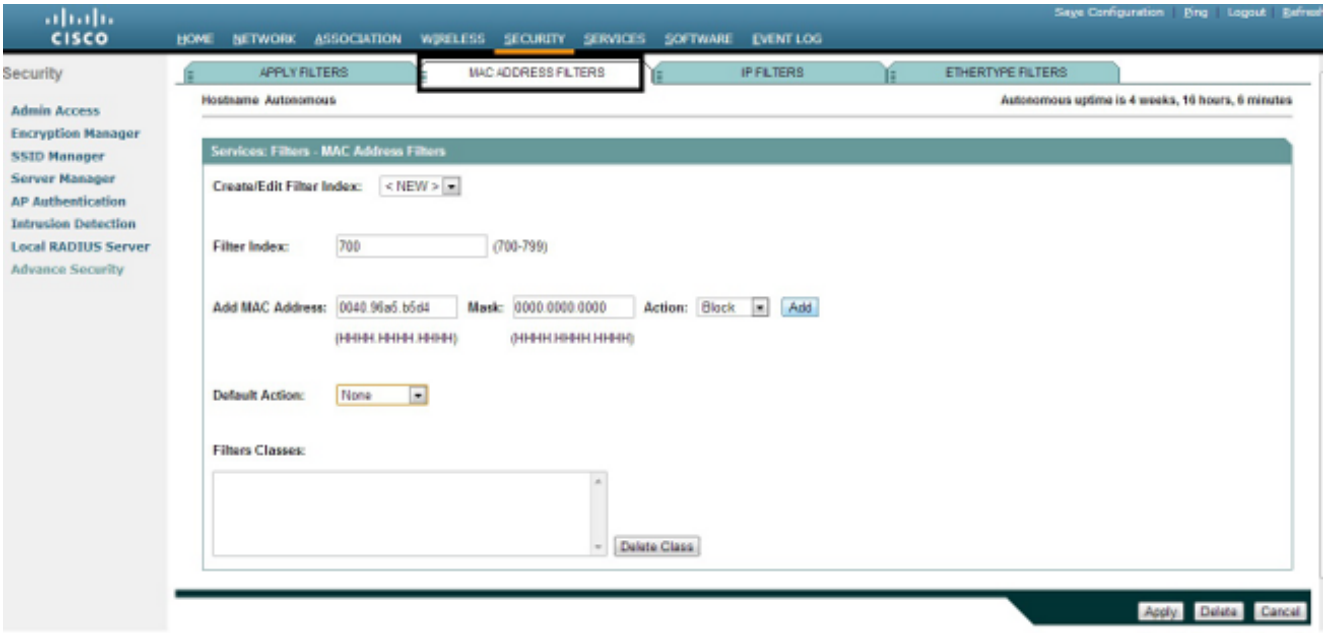


Filtros de direcciones MAC

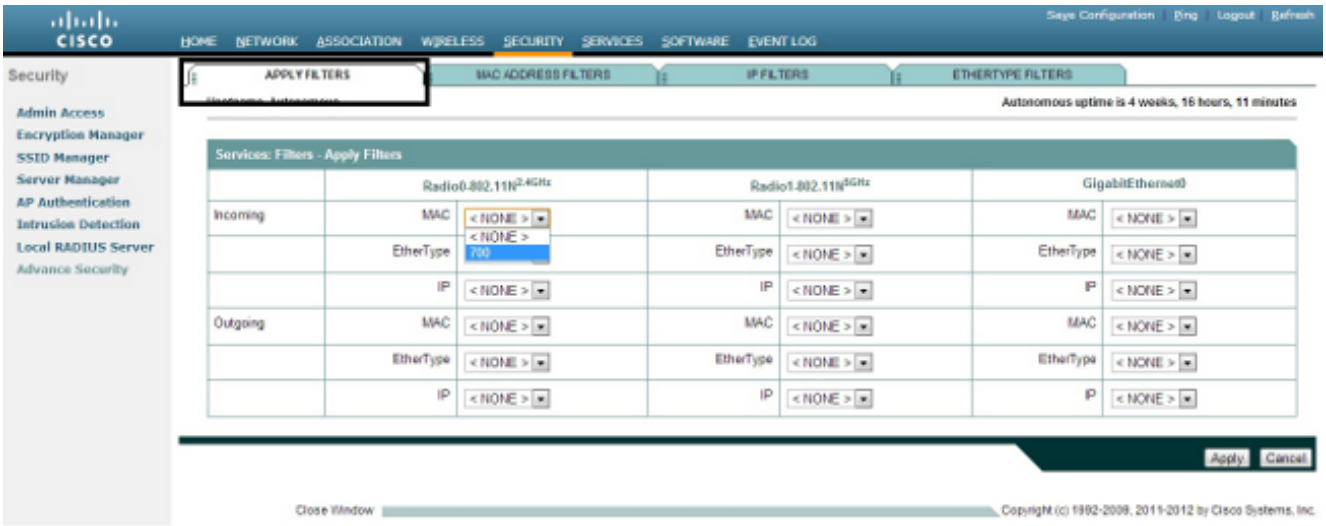
Puede utilizar filtros basados en direcciones MAC para filtrar los dispositivos cliente según la dirección MAC codificada. Cuando a un cliente se le niega el acceso a través de un filtro basado en MAC, el cliente no puede asociarse con el AP. Los filtros de direcciones MAC permiten o no permitir el reenvío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

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 **Forward All** o **Deny All**.
3. Haga clic en Apply (Aplicar). Ahora se crea **la ACL 700**.
4. Para aplicar **ACL 700** a una interfaz de radio, navegue a la sección **Aplicar filtros**. Ahora puede aplicar esta ACL a una interfaz de radio o GigabitEthernet entrante o saliente.



Filtros IP

Puede utilizar ACL estándar o extendidas para permitir o denegar la entrada de dispositivos cliente en la red WLAN basada en la dirección IP del cliente.

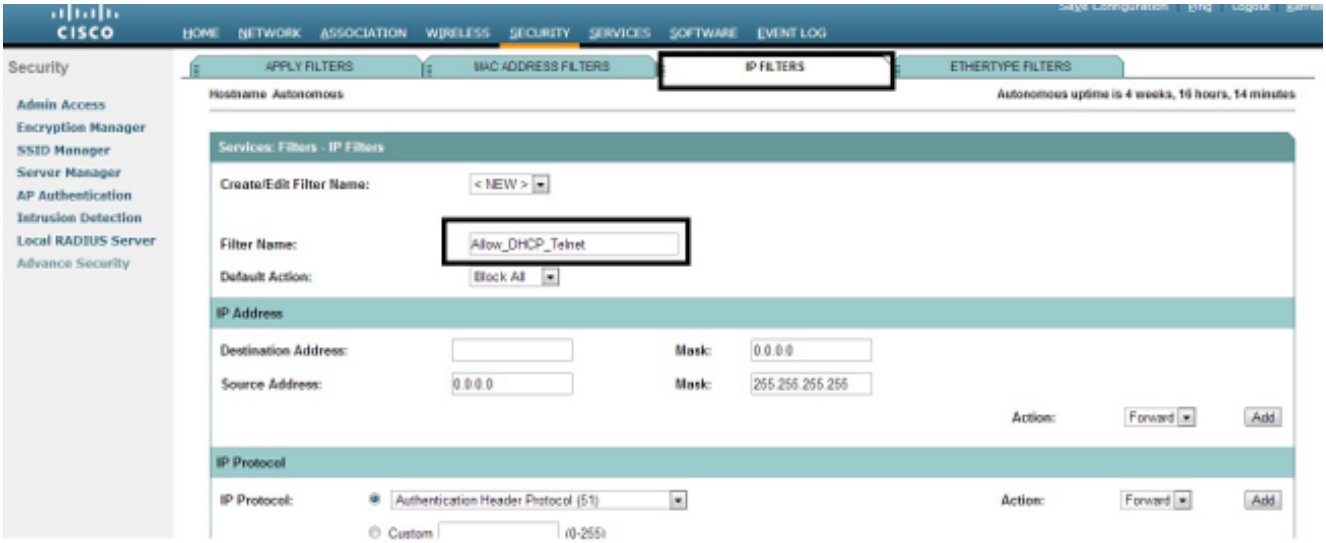
Este ejemplo de configuración utiliza ACL extendidas. La ACL extendida debe permitir el acceso Telnet a los clientes. Debe restringir todos los demás protocolos en la red WLAN. Además, los clientes utilizan DHCP para obtener la dirección IP. Debe crear una ACL extendida que:

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

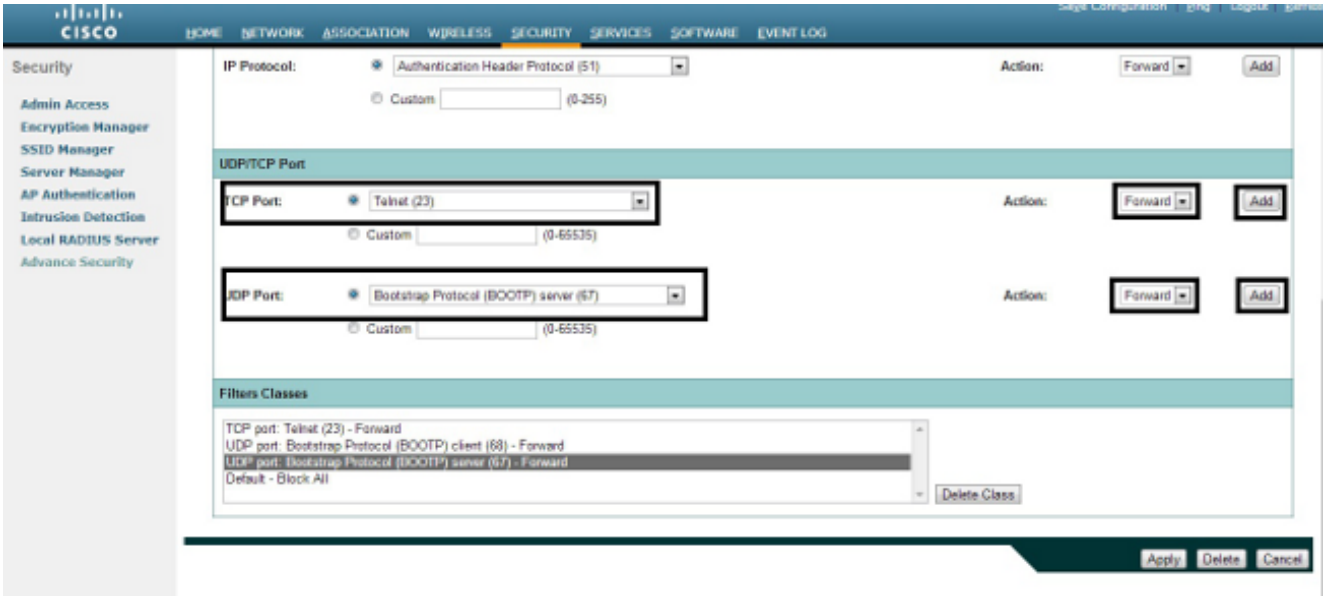
Complete estos pasos para crearlo:

1. Asigne un nombre al filtro y seleccione **Bloquear todo** en la lista desplegable **Acción**

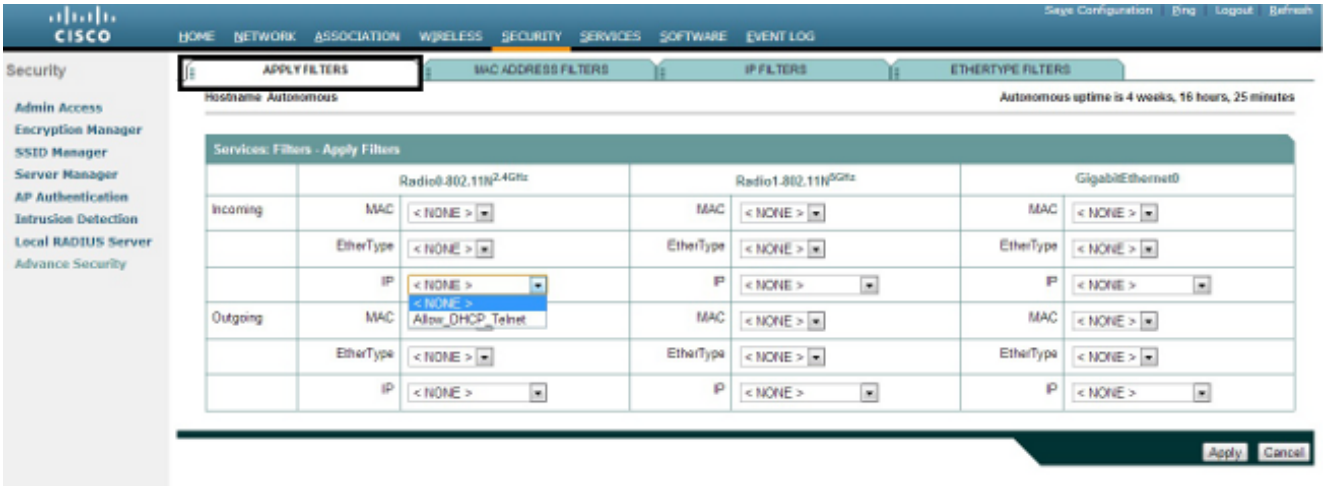
predeterminada, ya que el tráfico restante debe estar bloqueado:



2. Seleccione **Telnet** en la lista desplegable **Puerto TCP**, y **Cliente BOOTP** y **Servidor BOOTP** en la lista desplegable **Puerto UDP:**



3. Haga clic en Apply (Aplicar). El filtro IP **Allow_DHCP?_Telnet** se crea ahora y puede aplicar esta ACL a una interfaz de radio entrante o saliente o GigabitEthernet.

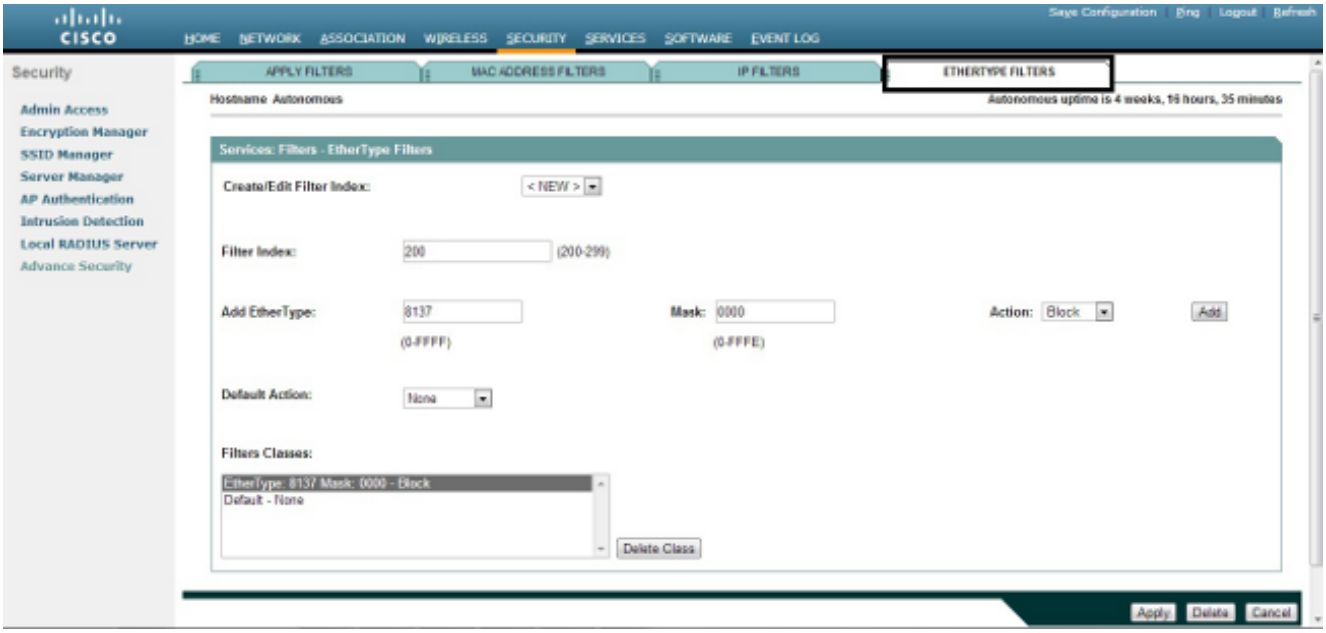


Filtros Ethertype

Puede utilizar filtros Ethertype para bloquear el tráfico de Intercambio de Paquetes entre Redes (IPX) en el AP Cisco Aironet. Una situación típica en la que esto es útil es cuando los servidores IPX emiten el link inalámbrico, lo que a veces ocurre en una red de grandes empresas.

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

1. Haga clic en la pestaña **Filtros Ethertype**.
2. En el campo **Filter Index**, asigne un nombre al filtro con un número entre 200 y 299. El número que asigna crea una ACL para el filtro.
3. Ingrese **8137** en el campo **Add Ethertype**.
4. Deje la máscara para el tipo Ethertype en el **campo Mask** con el valor predeterminado.
5. Seleccione **Block** en el menú de acción y haga clic en **Add**.



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