Exemplo de configuração de filtros ACL em APs Aironet

Contents

Introduction

Este documento descreve como configurar filtros baseados em Access Control List (ACL) em Access Points (APs) Cisco Aironet com o uso da GUI.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- A configuração de uma conexão sem fio com o uso de um AP Aironet e um Adaptador Cliente Aironet 802.11 a/b/g
- â€ªACLs

Componentes Utilizados

Este documento usa os APs Aironet 1040 Series que executam o software Cisco IOS® versão 15.2(2)JB.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Você pode usar filtros em APs para executar estas tarefas:

- Restringir o acesso à rede LAN sem fio (WLAN)
- Fornecer uma camada adicional de segurança sem fio

Você pode usar diferentes tipos de filtros para filtrar o tráfego com base em:

- Protocolos específicos

- O endereço MAC do dispositivo cliente
- O endereço IP do dispositivo cliente

Você também pode habilitar filtros para restringir o tráfego de usuários na LAN com fio. Os filtros de endereço IP e endereço MAC permitem ou não o encaminhamento de pacotes unicast e multicast que são enviados para ou de endereços IP ou MAC específicos.

Os filtros baseados em protocolo fornecem uma maneira mais granular de restringir o acesso a protocolos específicos através das interfaces de rádio e Ethernet do AP. Você pode usar qualquer um destes métodos para configurar os filtros nos APs:

- GUI da Web
- CLI

Este documento explica como usar ACLs para configurar filtros através da GUI.

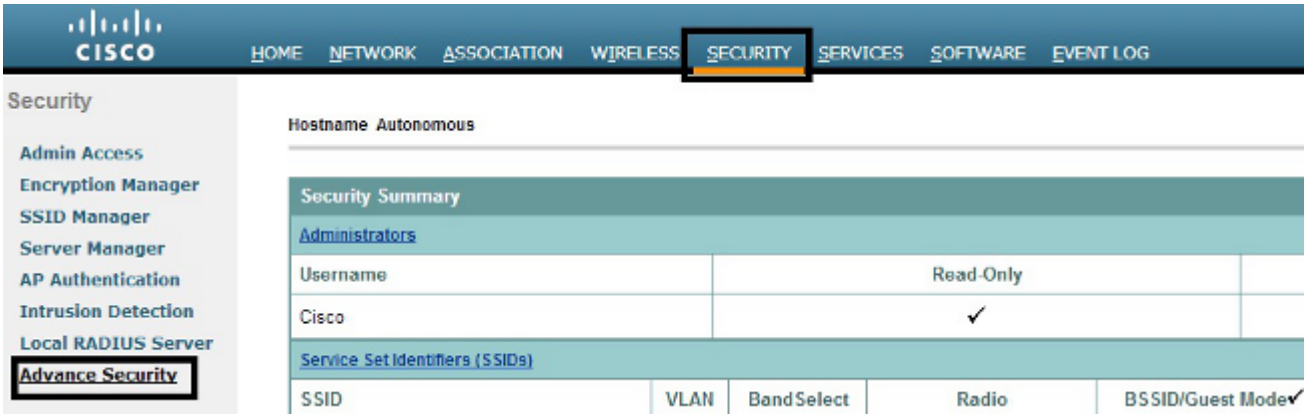
> **Observação**: para obter mais informações sobre a configuração por meio do uso do CLI, consulte o artigo Access Point ACL Filter Configuration Example Cisco.

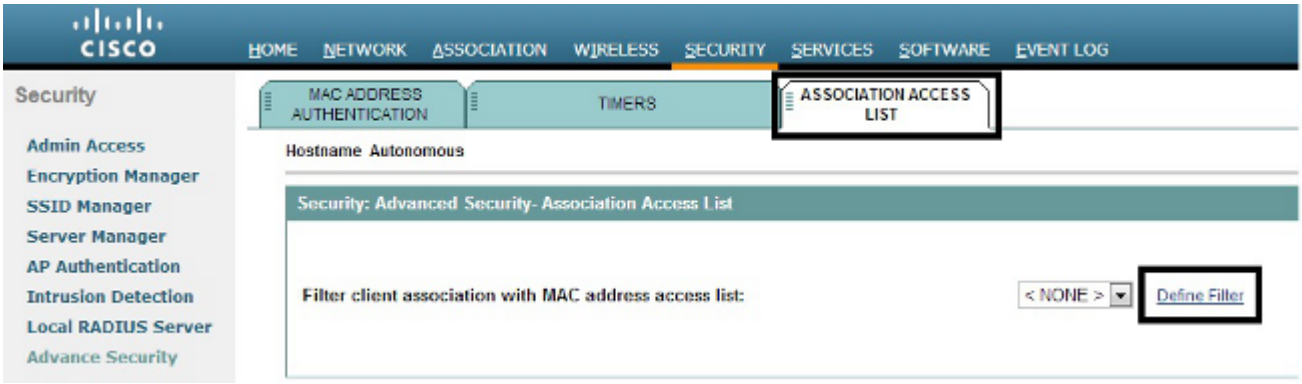
Configurar

Esta seção descreve como configurar filtros baseados em ACL em APs Cisco Aironet com o uso da GUI.

Onde criar ACLs

Navegue até **Segurança** > **Segurança avançada**. Escolha a guia **Lista de Acesso de Associação** e clique em **Definir Filtro**:



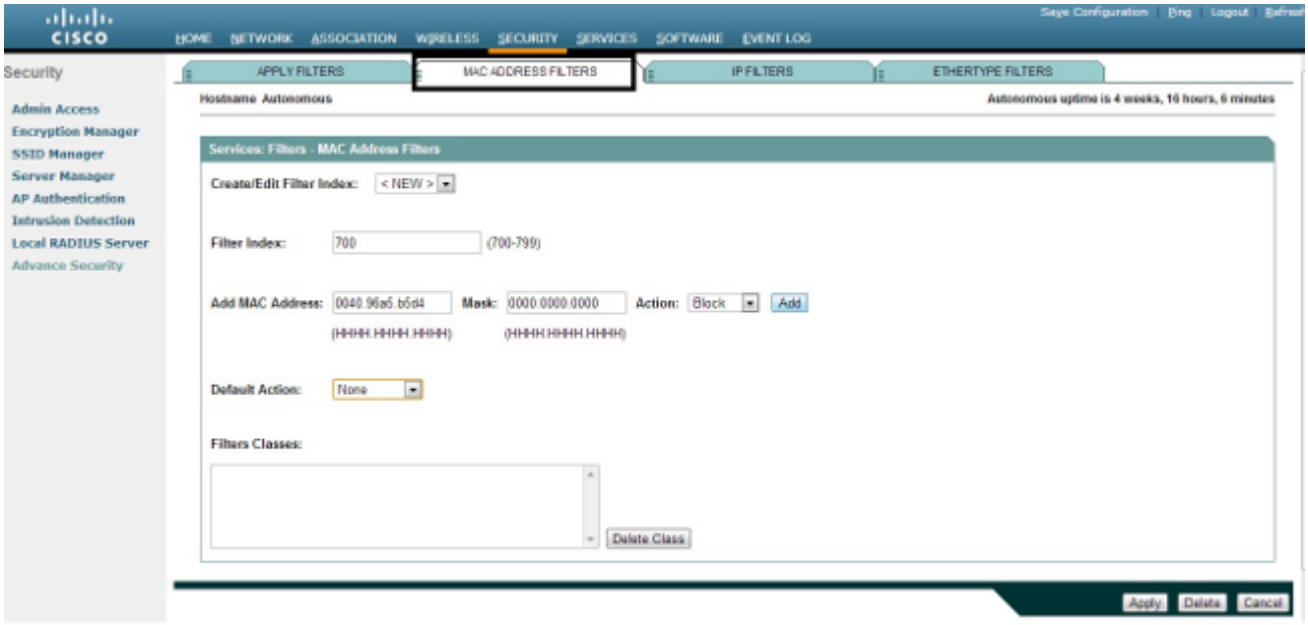


Filtros de endereço MAC

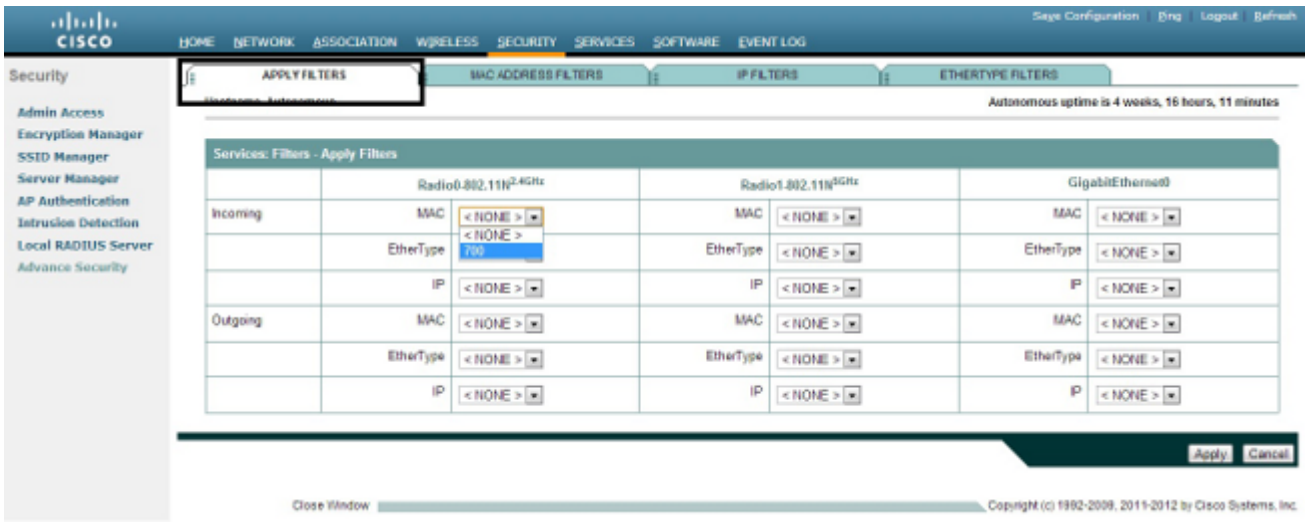
Você pode usar filtros baseados em endereço MAC para filtrar dispositivos clientes com base no endereço MAC codificado. Quando um cliente tem o acesso negado através de um filtro baseado em MAC, o cliente não pode se associar ao AP. Os filtros de endereço MAC permitem ou não o encaminhamento de pacotes unicast e multicast enviados de, ou endereçados a, endereços MAC específicos.

Este exemplo ilustra como configurar um filtro baseado em MAC através da GUI para filtrar o cliente com um endereço MAC de **0040.96a5.b5d4**:

1. Crie o endereço MAC **ACL 700**. Essa ACL não permite que o cliente **0040.96a5.b5d4** se associe ao AP.



2. Clique em **Add** para adicionar esse filtro às Classes de filtros. Você também pode definir a ação padrão como **Encaminhar tudo** ou **Negar tudo**.
3. Clique em Apply. **A ACL 700** foi criada.
4. Para aplicar a **ACL 700** a uma interface de rádio, navegue para a seção **Aplicar filtros**. Agora você pode aplicar essa ACL a uma interface de entrada ou saída de rádio ou GigabitEthernet.



Filtros IP

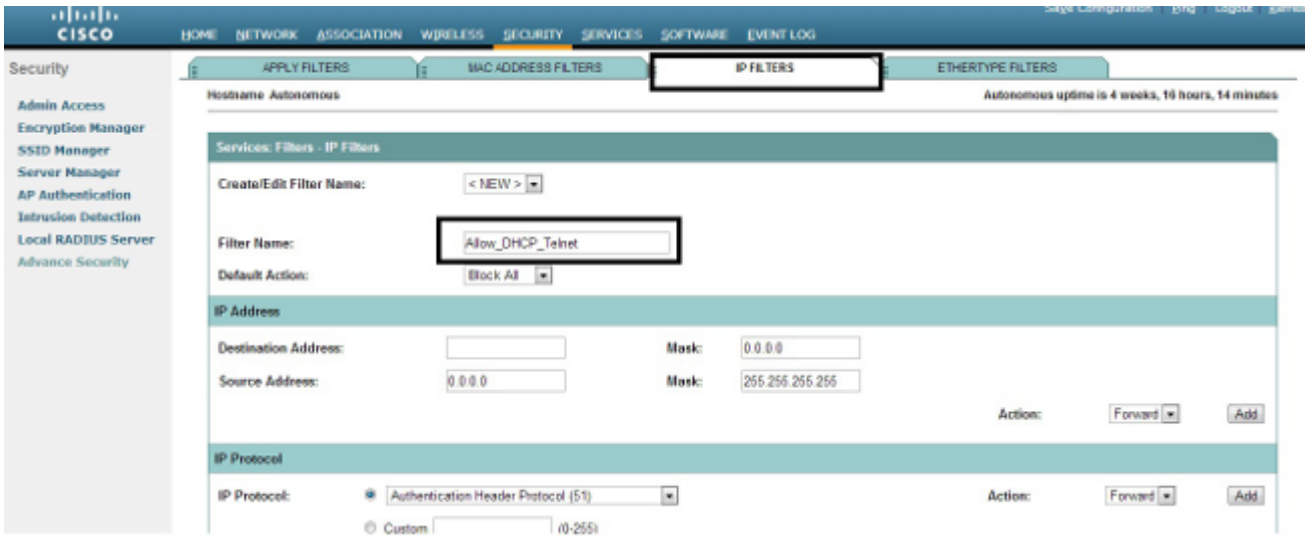
Você pode usar ACLs padrão ou estendidas para permitir ou não a entrada de dispositivos cliente na rede WLAN com base no endereço IP do cliente.

Este exemplo de configuração usa ACLs estendidas. A ACL estendida deve permitir acesso Telnet aos clientes. Você deve restringir todos os outros protocolos na rede WLAN. Além disso, os clientes usam DHCP para obter o endereço IP. Você deve criar uma ACL estendida que:

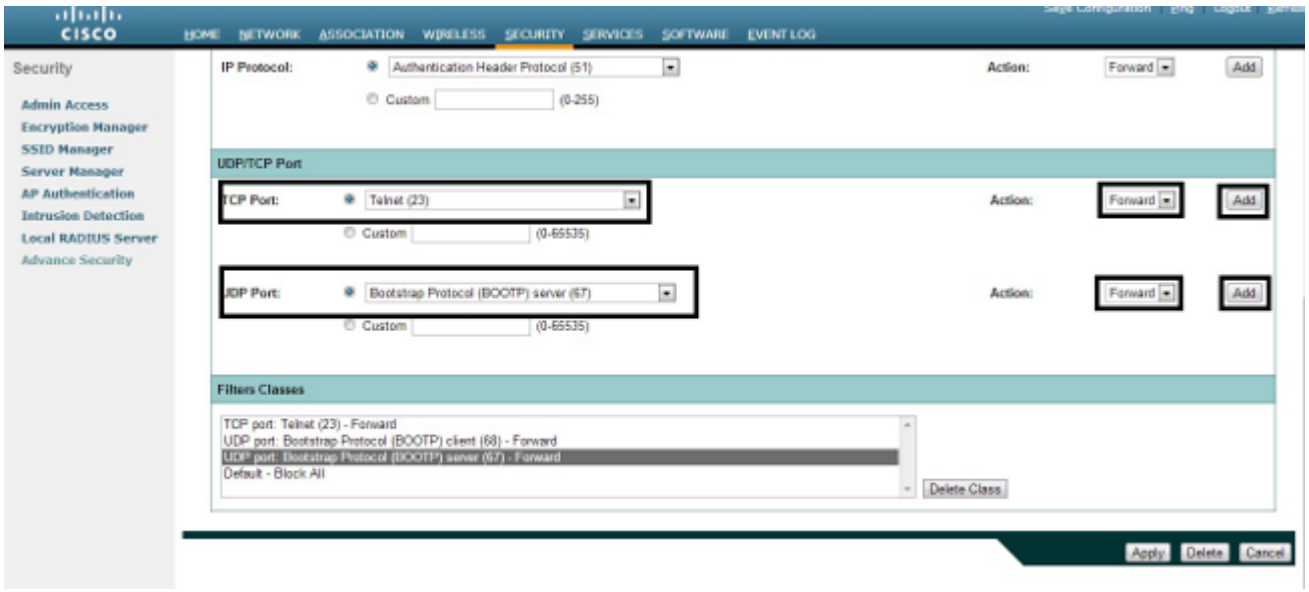
- Permite tráfego DHCP e Telnet
- Nega todos os outros tipos de tráfego

Conclua estas etapas para criá-lo:

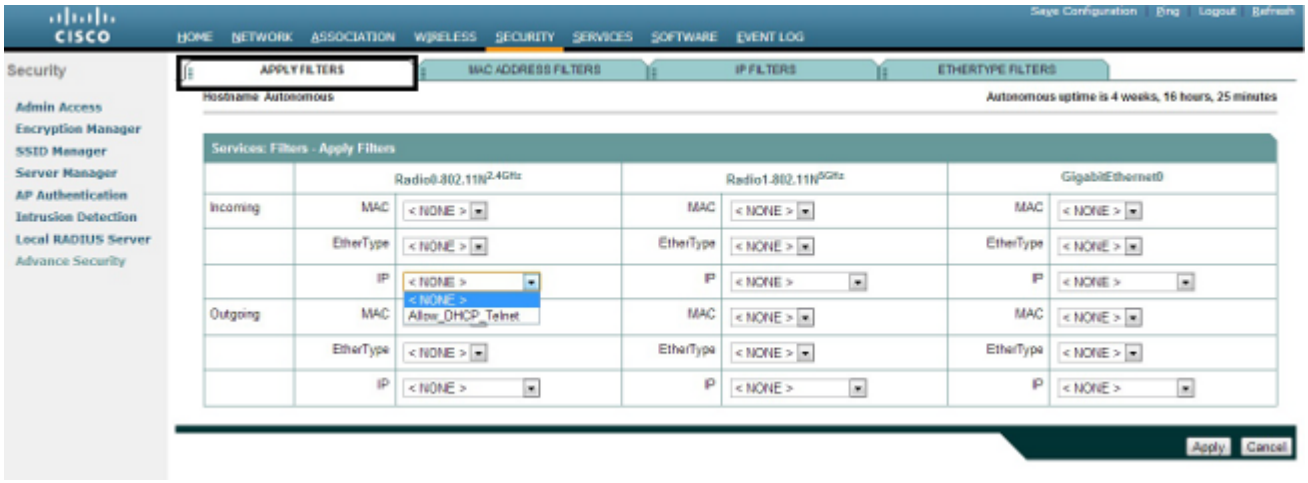
1. Nomeie o filtro e selecione **Block All** na lista suspensa **Default Action**, já que o tráfego restante deve ser bloqueado:



2. Selecione Telnet na lista suspensa **Porta TCP** e **cliente BOOTP** e servidor BOOTP na lista suspensa Porta UDP:



3. Clique em Apply. O filtro IP **Allow_DHCP?_Telnet** foi criado e você pode aplicar essa ACL a uma interface de entrada ou saída de rádio ou GigabitEthernet.

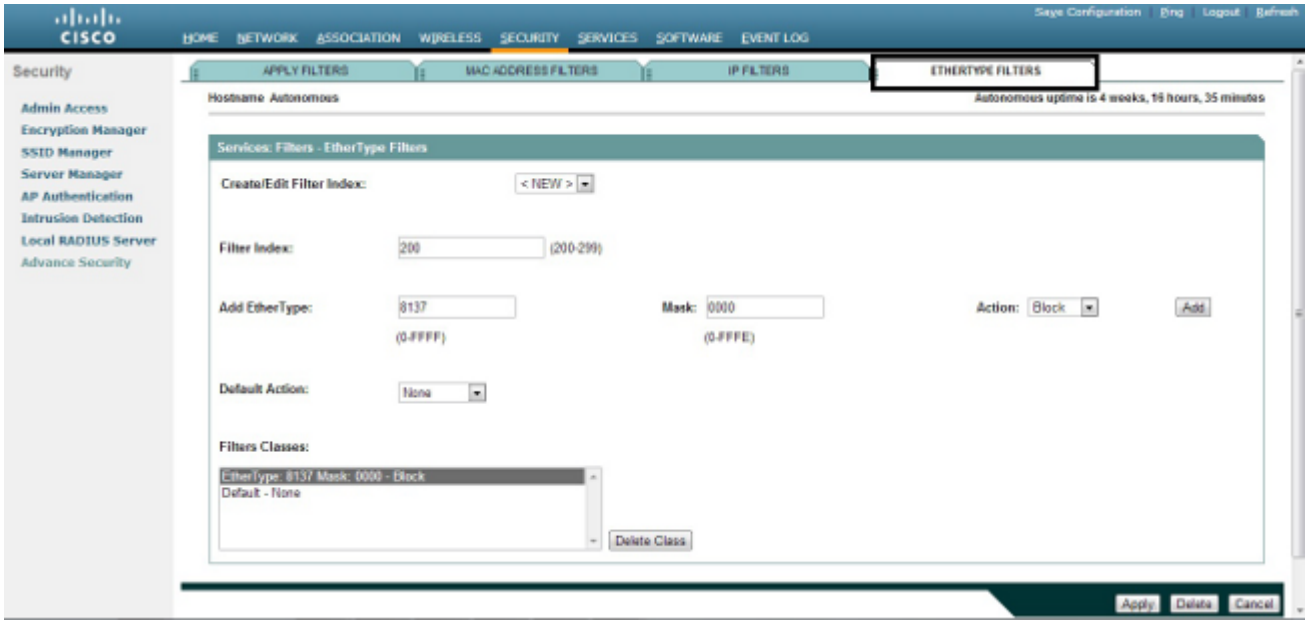


Filtros Ethertype

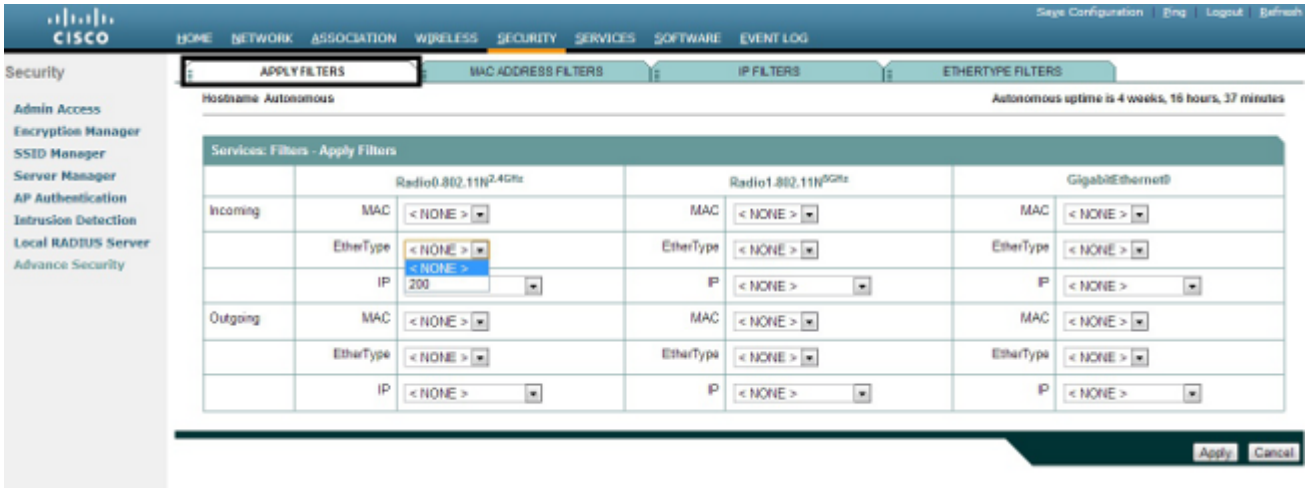
Você pode usar filtros Ethertype para bloquear o tráfego do Internetwork Packet Exchange (IPX) no AP Cisco Aironet. Uma situação típica em que isso é útil é quando os broadcasts do servidor IPX sufocam o link sem fio, o que às vezes acontece em uma rede corporativa de grande porte.

Conclua estas etapas para configurar e aplicar um filtro que bloqueie o tráfego IPX:

1. Clique na guia **Ethertype Filters**.
2. No campo **Índice do filtro**, nomeie o filtro com um número de 200 a 299. O número atribuído cria uma ACL para o filtro.
3. Digite **8137** no campo **Add Ethertype**.
4. Deixe a máscara para o Ethertype no **campo Mask** com o valor padrão.
5. Selecione **Bloquear** no menu de ação e clique em **Adicionar**.



6. Para remover o Ethertype da lista Filters Classes, selecione-o e clique em **Delete Class**. Repita as etapas anteriores e adicione os tipos **8138**, **00ff** e **00e0** ao filtro. Agora você pode aplicar essa ACL a uma interface de entrada ou saída de rádio ou 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.