ACL Filters on Aironet APs Configuration Example

Document ID: 116583

Contributed by Varun Ajmani, Cisco TAC Engineer.
Oct 15, 2013

Contents

Introduction
Prerequisites
- Requirements
- Components Used

Background Information
Configure
- Where to Create ACLs
- MAC Address Filters
- IP Filters
- Ethertype Filters

Introduction

This document describes how to configure Access Control List (ACL)−based filters on Cisco Aironet Access Points (APs) with use of the GUI.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- The configuration of a wireless connection with use of an Aironet AP and an Aironet 802.11 a/b/g Client Adapter
- ACLs

Components Used

This document uses Aironet 1040 Series APs that run Cisco IOS® software Release 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.

Background Information

You can use filters on APs in order to perform these tasks:

- Restrict access to the wireless LAN (WLAN) network
- Provide an additional layer of wireless security

You can use different types of filters in order to filter traffic based on:

- Specific protocols
- The MAC address of the client device
- The IP address of the client device

You can also enable filters in order to restrict traffic from users on the wired LAN. IP address and MAC address filters allow or disallow the forwarding of unicast and multicast packets that are sent to or from specific IP or MAC addresses.

Protocol−based filters provide a more granular way to restrict access to specific protocols through the Ethernet and radio interfaces of the AP. You can use either of these methods in order to configure the filters on the APs:

- Web GUI
- CLI

This document explains how to use ACLs in order to configure filters through the GUI.

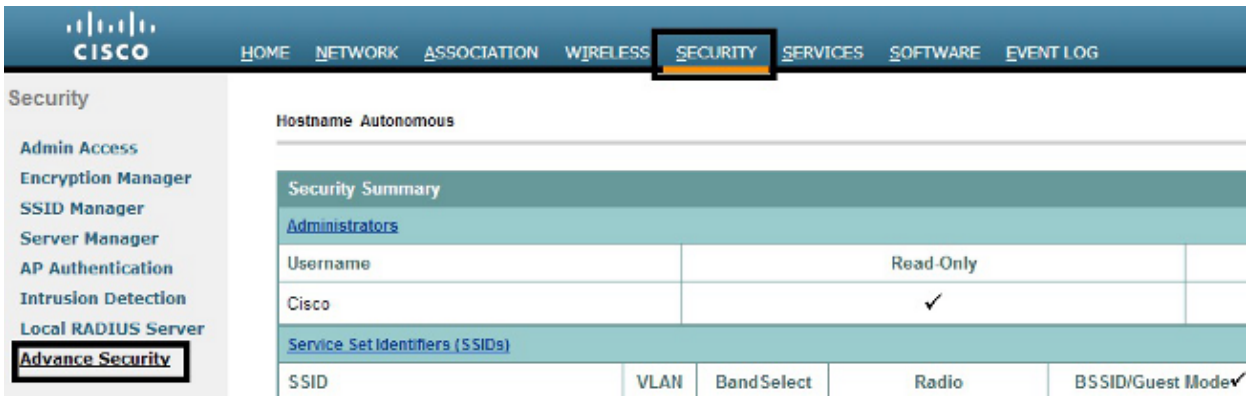
Note: For more information about configuration through use of the CLI, refer to the Access Point ACL Filter Configuration Example Cisco article.

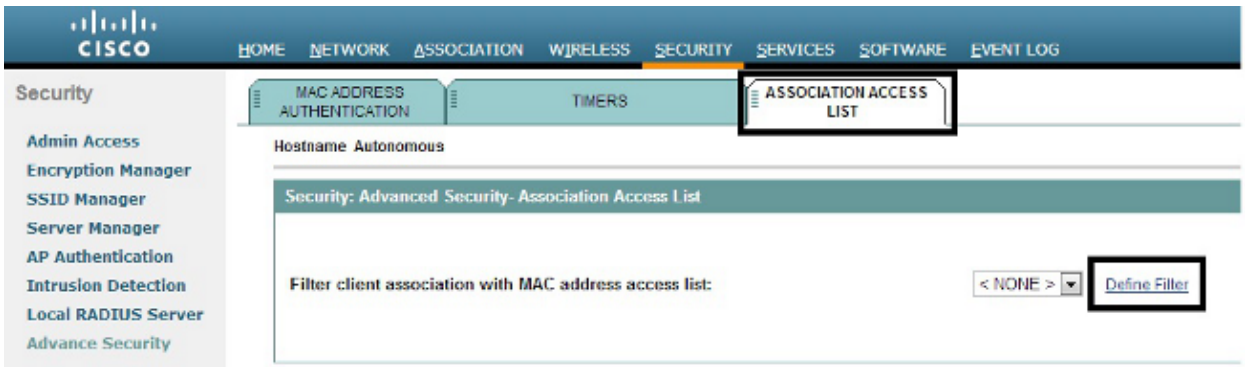
Configure

This section describes how to configure ACL−based filters on Cisco Aironet APs with use of the GUI.

Where to Create ACLs

Navigate to ***Security*** > ***Advance Security***. Choose the ***Association Access List*** tab, and click ***Define Filter***:



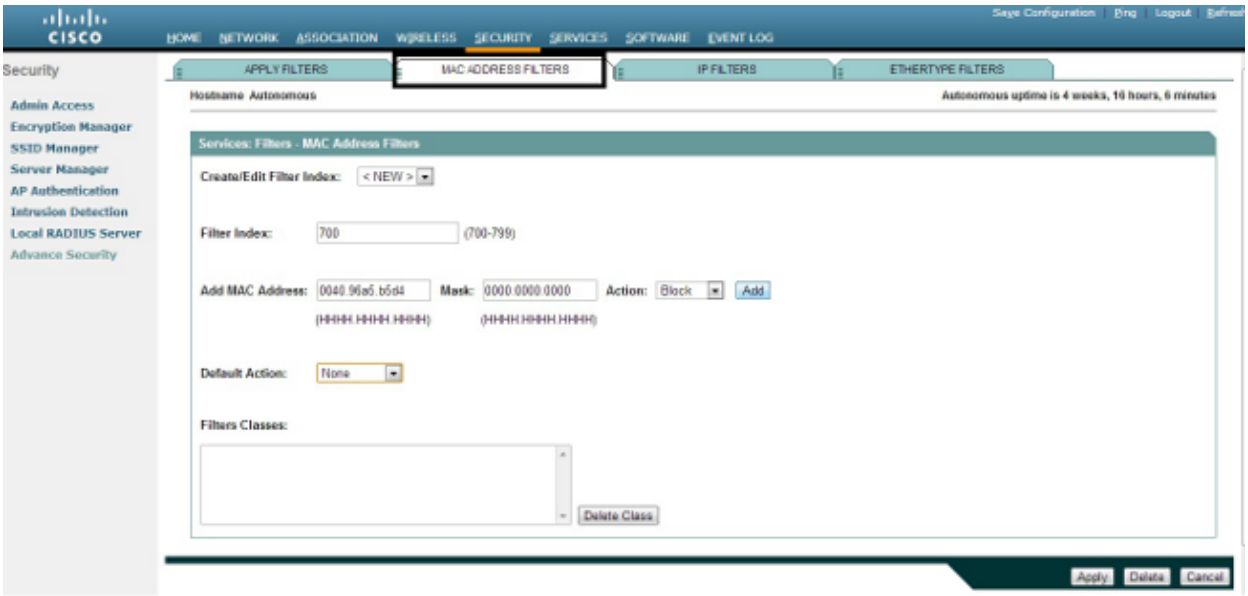


MAC Address Filters

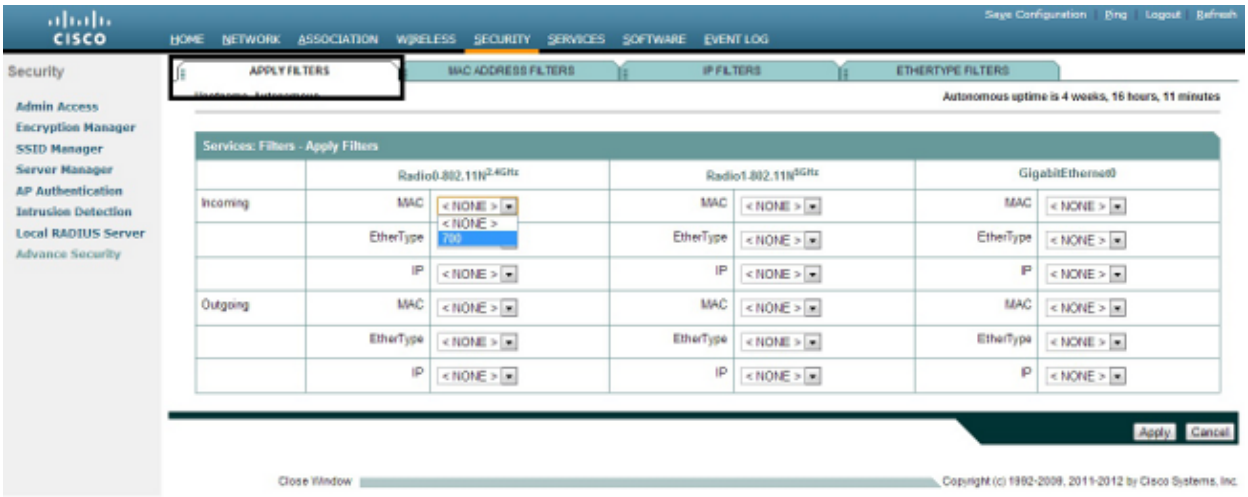
You can use MAC address−based filters in order to filter client devices based on the hard−coded MAC address. When a client is denied access through a MAC−based filter, the client cannot associate with the AP. MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from, or addressed to, specific MAC addresses.

This example illustrates how to configure a MAC−based filter through the GUI in order to filter the client with a MAC address of ***0040.96a5.b5d4***:

1. Create the MAC address ***ACL 700***. This ACL does not allow the client ***0040.96a5.b5d4*** to associate with the AP.



2. Click ***Add*** in order to add this filter to the Filters Classes. You can also define the default action as ***Forward All*** or ***Deny All***.
3. Click ***Apply***. ***ACL 700*** is now created.
4. In order to apply ***ACL 700*** to a radio interface, navigate to the ***Apply Filters*** section. You can now apply this ACL to an incoming or outgoing Radio or GigabitEthernet interface.



IP Filters

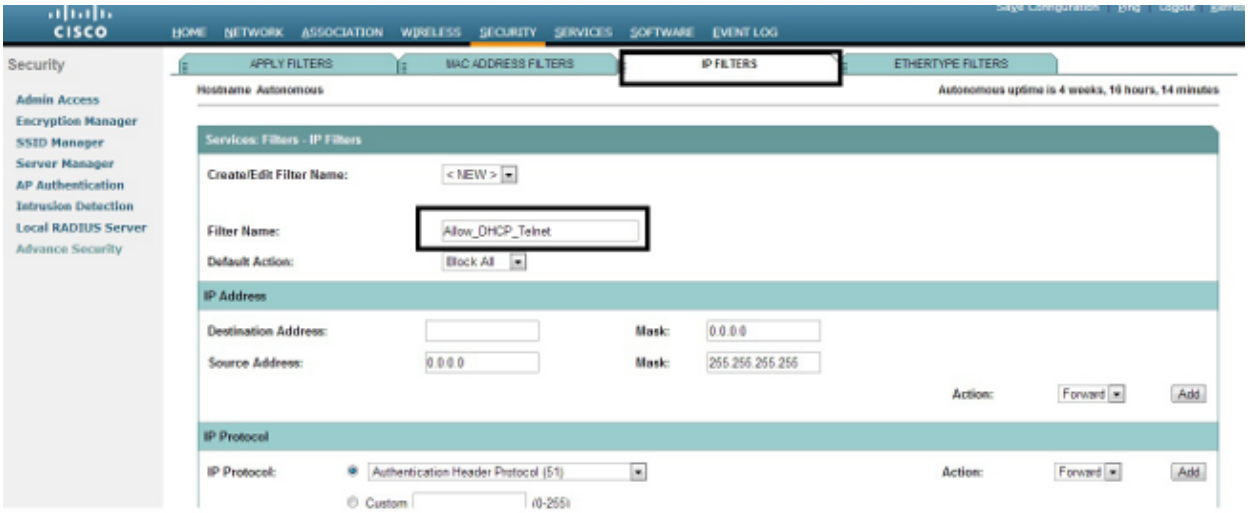
You can use standard or extended ACLs in order to allow or disallow the entry of client devices into the WLAN network based on the IP address of the client.

This configuration example uses extended ACLs. The extended ACL must allow Telnet access to the clients. You must restrict all other protocols on the WLAN network. Also, the clients use DHCP in order to obtain the IP address. You must create an extended ACL that:

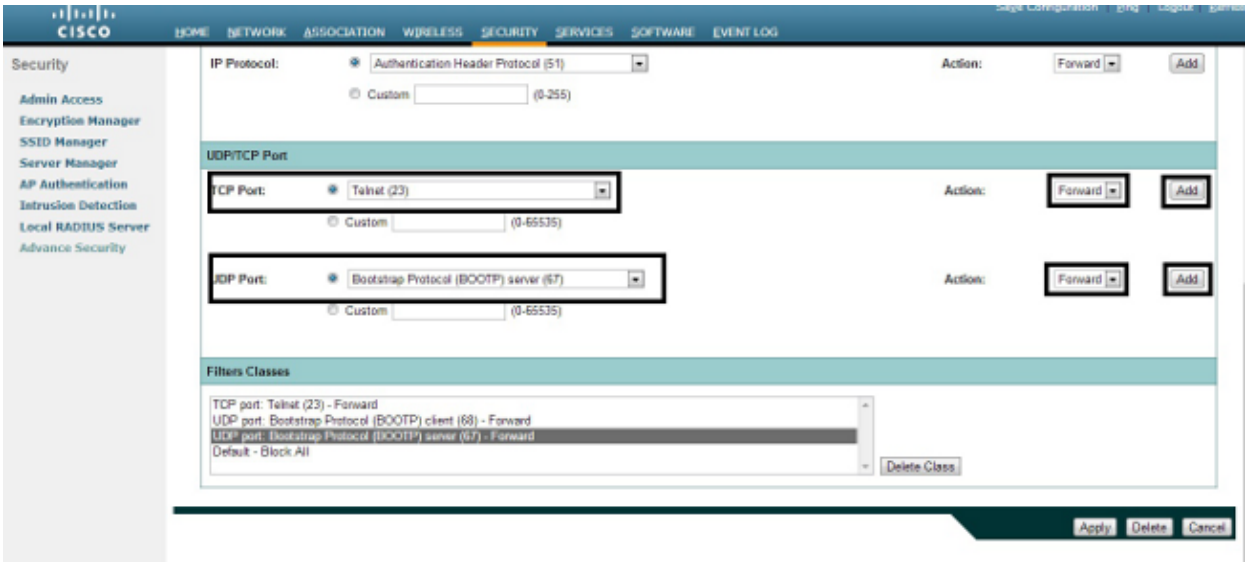
- Allows DHCP and Telnet traffic
- Denies all other traffic types

Complete these steps in order to create it:

1. Name the filter, and select ***Block All*** from the ***Default Action*** drop−down list, since the remaining traffic must be blocked:

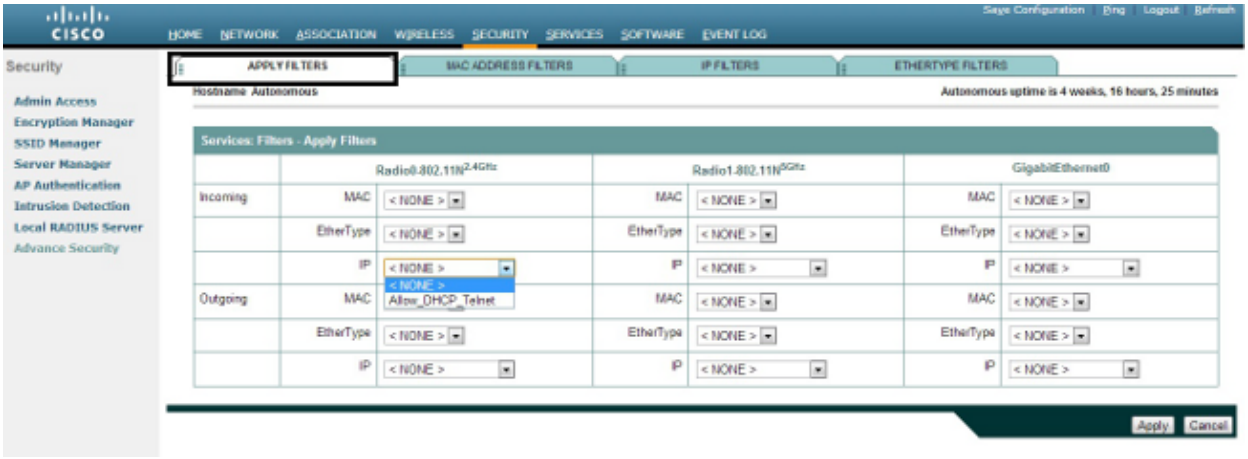


2. Select ***Telnet*** from the ***TCP Port*** drop−down list, and ***BOOTP client*** & ***BOOTP server*** from the ***UDP Port*** drop−down list:



3. Click ***Apply***. The IP filter ***Allow_DHCP-_Telnet*** is now created, and you can apply this ACL to an

incoming or outgoing Radio or GigabitEthernet interface.

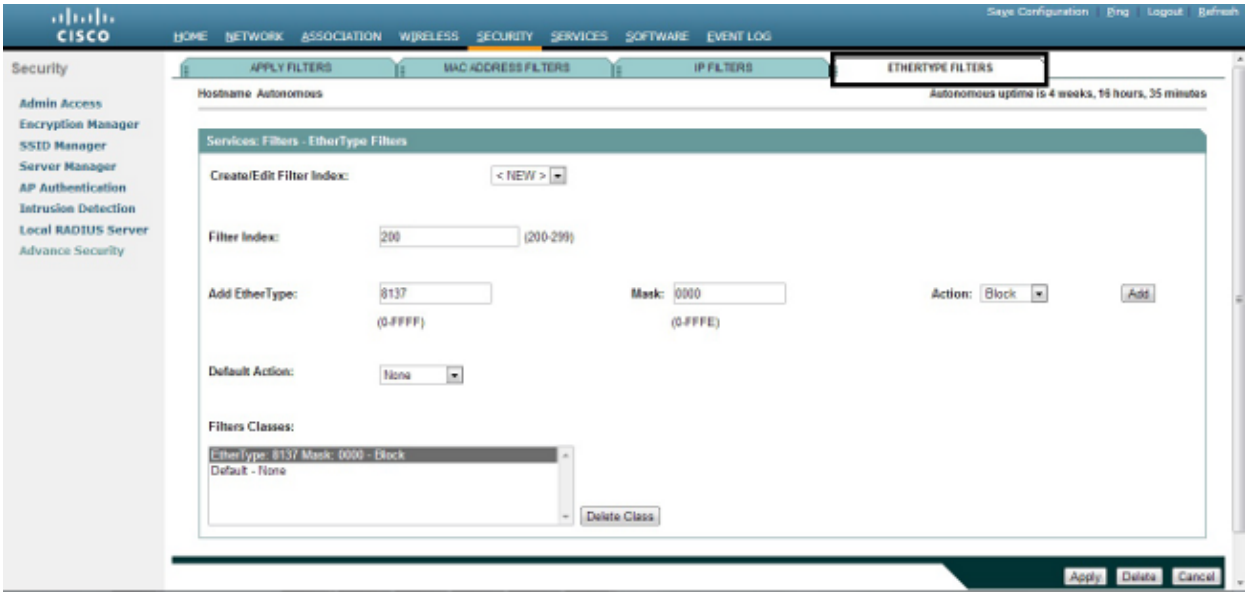


Ethertype Filters

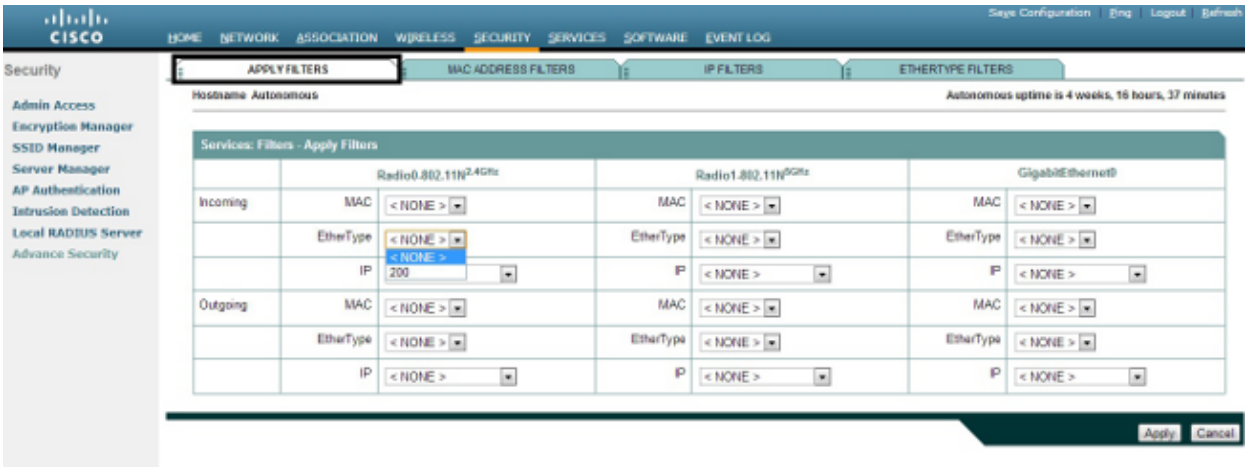
You can use Ethertype filters in order to block Internetwork Packet Exchange (IPX) traffic on the Cisco Aironet AP. A typical situation where this is useful is when IPX server broadcasts choke the wireless link, which sometimes happens on a large enterprise network.

Complete these steps in order to configure and apply a filter that blocks IPX traffic:

1. Click the ***Ethertype Filters*** tab.
2. In the ***Filter Index*** field, name the filter with a number from 200 to 299. The number you assign creates an ACL for the filter.
3. Enter ***8137*** in the ***Add Ethertype*** field.
4. Leave the mask for the Ethertype in the ***Mask field*** at the default value.
5. Select ***Block*** from the action menu, and click ***Add***.



6. In order to remove the Ethertype from the Filters Classes list, select it, and click ***Delete Class***. Repeat the previous steps, and add types ***8138***, ***00ff***, and ***00e0*** to the filter. You can now apply this ACL to an incoming or outgoing Radio or GigabitEthernet interface.



Updated: Oct 15, 2013 Document ID: 116583