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*:

ululu cisco	HOME	<u>N</u> ETWORK	ASSOCIATION	WIREL	ess <u>s</u> i	CURITY	<u>s</u> ervice	s <u>s</u> oftwa	re <u>e</u> vent	LOG	
Security Admin Access Encryption Manager SSID Manager Server Manager	Ho: Si	stname Autono scurity Sumn Iministrators	omous nary								
AP Authentication Intrusion Detection	Ci	sername isco						Read-Or	nly		
Advance Security	S	ervice SetIden SID	tifiers (SSIDs)		VLAN	BandS	elect	Radio	0	BSSID/Gues	t Mode√
ىرايىرانى cısco	НОМЕ	NETWORK	ASSOCIATION	WIRELES	s <u>s</u> eci	JRITY <u>s</u>	ERVICES	SOFTWARE	EVENT LOG		
Security Admin Access Encryption Manager SSID Manager	Hos	AC ADDRESS THENTICATION tname Autonor	mous	TIMER:	8 Access Lie	at a state	ASSOCIATIO LIS	T			_
Server Manager AP Authentication Intrusion Detection Local RADIUS Server Advance Security	F	ilter client as	ociation with MA	C address	access I	ist:			< NONE >	Define Fill	<u>er</u>

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.

	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENTLOS	Saye Configuration Bing Logout Bafred
CISCO Security Admin Access Encryption Manager SSID Monoper SSID Monoper SSID Monoper SSID Monoper SSID Monoper Server Manager AP Authentication Intrusion Detection Local RADIUS Server Advance Security	HOME NETWORK ASSOCIATION WIPELESS SECURITY SERVICES SOTWARE EVENT LOG # APPLY FLITERS MAC ADDRESS FLITERS IP FLITERS IP FLITERS IP FLITERS Hostisame Autosomous Services: Filters MAC Address Filters Filter Index: (700-799) Add MAC Address: (000.0000.0000.0000 Action: Block Add Add Helleki Helleki Helleki Helleki Helleki Helleki (Helleki Helleki Hel	ETHERTYPE FILTERS Autonomous uptime is 4 weeks, 10 hours, 6 minutes
	- [Delete Class]	

- 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.

Admin Access Excryption Manager SSID Menager	s 4 weeks, 16 hours, 11 min
scryption Manager StD Menager Services: Filters - Apply Filters	
rvor Manager Radio0.002.11N ^{2.4GHz} Radio1.002.11N ^{5GHz} Gigabi	itEthernet0
Authentication Incoming MAC KIONE> MAC KIONE> MAC KIONE>	NONE >
cal RADIUS Server EtherType <ndie> EtherType <ndie></ndie></ndie>	NONE >
IP CNDE>. IP CNDE>.	NONE >
Outgoing MAC <none> MAC <none> MAC MAC</none></none>	NONE >
EtherType <nome> EtherType <nome> EtherType <</nome></nome>	NONE >
IP <note>* IP <note>* IP</note></note>	NONE > .

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:

0100		ON WIRD DEC DECIDITY STRUCTS	CORTANNE DURITI OG	Sage Low	idmustion Rud rodons Paul
Security	APPLY FILTERS	1 INC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS Autonomous uptime in	s 4 weeks, 16 hours, 14 minutes
Admin Access Encryption Manager SSID Manager	Services: Filters - IP Filters				
Server Manager AP Authentication Intrusion Detection	Create/Edit Filter Name:	< NEW > •	_		
Local RADIUS Server Advance Security	Filter Name: Default Action:	Allow_DHCP_Telnet			
	IP Address				
	Destination Address: Source Address:	0.0.0.0	Mask: 0.0.0.0 Mask: 255.255.255		
				Action:	Forward • Add
	IP Protocol				
	IP Protocol:	Authentication Header Protocol (51) Custom (0-255)		Action:	Forward • Add

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

cisco	HOM	E BETWORK	ASSOCIATION W	RELESS SECURITY	SERVICES	SOFTWARE	EVENTLOG		Sage Co	ungunation [Bing	rogent Ferre
Security		IP Protocol:	Authenti	ication Header Protocol	(51)	-		Acti	on:	Forward .	Add
Admin Access Encryption Manager			Custom	(0	1-255)						
SSID Manager Server Manager		UDP/TCP Port									
AP Authentication Intrusion Detection		TCP Port:	Teinet (23)					Acti	ion:	Forward	Add
Local RADIUS Server Advance Security			© Custom	(0-655	535)	_					
		JDP Port:	Bootstrap Pr	rotocol (BOOTP) server	(67)			Acti	ion:	Forward .	Add
			Custom	(0-655	535)						
		Filters Classes									
		TCP part: Telms UDP part: Bost UDP part: Bost Default - Block	t (23) - Ferward strap Protocol (BOOTP strap Extend (BOOTP All) client (68) - Forward) sonver (67) - Forward				- Delete Class			
	_									Acris De	nte Concel
											00100

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.

ahaha						Se	ve Configuration Ping	Logout Befreeh
CISCO	HOME NETWORK	ASSOCIATION	WIRELESS SECURITY	SERVICES SOFTWARE	EVENTLOG			
Security	E APPL	Y FILTERS	BAC ADDRESS	FLTERS 1	IP FILTERS	ETHERTYPE BLTER	\$	
Admin Access	Hostname Auto	nomous				Autonomou	is uptime is 4 weeks, 16 h	ours, 25 minutes
Encryption Manager								
SSID Manager	Services: Filt	ers - Apply Filters						
Server Manager			ladio0-802.11N ^{2.4GHz}		Radio1-802.11N ^{SGHz}		GigabitEthernet0	
Intrusion Detection	Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE > m	
Local RADIUS Server Advance Security		EtherType	< NONE > .	EtherType	< NONE > x	EtherType	< NONE > x	
		IP	< NONE >	P	< NONE >	P	< NONE >	-
	Outgoing	MAC	Allow_DHCP_Telnet	MAC	< NONE > ×	MAC	< NONE > *	
		EtherType	< NONE > 📼	EtherType	< NONE > •	EtherType	< NONE > •	
		IP	< NONE >	P	< NONE >	P P	< NONE >	-
								Apply Cencel

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*.

cisco	HOME NETWORK ASSOCIAT	ION WIRELESS SECURITY SEA	WICES SOFTWARE EVENTLOG	Saye Configuratio	n Eing Logout Befrich
Security	APPLY FILTERS	H MAC ADDRESS FILTERS	I IP FILTERS	ETHERTYPE FILTERS	
Admin Access	Hostname Autonomous			Autonomous uptime is 4 week	ks, 16 hours, 35 minutes
Encryption Manager SSID Manager	Services: Filters - EtherTyp	e Filters			
Server Manager	Create/Edit Filter Index:	< NEW > .			
Intrusion Detection Local RADIUS Server Advance Security	Filter Index:	200 (200-299	9		
	Add EtherType:	8137 (0-FFFF)	Mask: 0000 (0-FFFE)	Action: Block 💌	Add
	Default Action:	None			
	Filters Classes:				
	EtherType: 8137 Mask: 000 Default - None	- Block A			
			Delate Class		
					nt Dates Canad

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.

ity	APPL	Y FILTERS	WAC ADDRESS FILTERS	8 ¥	IP FILTERS	ETHERTYPE FILTER	s
n Access	Hostname Autor	nomous				Autonomou	s uptime is 4 weeks, 16 hours, 3
ption Manager Manager	Services: Filb	ers - Apply Filters	8				
er Manager			Radio0-802.11N ^{2.4GHz}		Radio1-802.11NSGHz		GigabitEthernetD
sion Detection	Incoming	MAC	< NONE > •	MAC	< NONE > .	MAC	< NONE > •
RADIUS Server		EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
ice security		IP	200 ·	P	< NONE >	P	< NONE >
	Outgoing	MAC	< NONE > .	MAC	< NONE > .	MAC	< NONE >
		EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
		IP	<none></none>	P	< NONE >	P	< NONE >

Updated: Oct 15, 2013

Document ID: 116583