# Aironet AP上的ACL过滤器配置示例

## 目录

简介 先决条件 要求 使用的组件 背景信息 配置 创建ACL的位置 MAC 地址过滤器 IP 过滤器 Ethertype过滤器

# 简介

本文档介绍如何使用GUI在Cisco Aironet接入点(AP)上配置基于访问控制列表(ACL)的过滤器。

# 先决条件

### 要求

Cisco 建议您具有以下主题的基础知识:

- 使用 Aironet AP 和 Aironet 802.11 a/b/g 客户端适配器配置无线连接
- ACL

使用的组件

本文档使用运行Cisco IOS®软件版本15·2(2)JB的Aironet 1040系列AP。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

## 背景信息

可以在AP上使用过滤器执行以下任务:

- 限制对无线 LAN (WLAN) 网络的访问
- 提供附加的无线安全层

您可以使用不同类型的过滤器来根据以下内容过滤流量:

- 特定协议
- 客户端设备的MAC地址
- 客户端设备的IP地址

您还可以启用过滤器以限制来自有线LAN上用户的流量。IP 地址和 MAC 地址过滤器可允许或禁止 转发特定 IP 或 MAC 地址接收或发送的单播和组播数据包。

基于协议的过滤器提供一种更精细的方式来限制通过 AP 的以太网和无线电接口对特定协议的访问 。您可以使用以下方法之一在AP上配置过滤器:

- Web GUI
- CLI

本文档说明如何使用ACL通过GUI配置过滤器。

注意:有关使用CLI进行配置的详细信息,请参阅<u>Access Point ACL Filter Configuration</u> <u>Example Cisco</u>文章。

## 配置

本节介绍如何使用GUI在Cisco Aironet AP上配置基于ACL的过滤器。

创建ACL的位置

导航到安全 > 高级安全。选择Association Access List选项卡,然后单击Define Filter:

ululu cisco	HOME	NETWORK	ASSOCIATION	WIRELESS	SEC	CURITY <u>s</u>	ERVICES	<u>S</u> OFTWARE	EVENT LO	G	
Security Admin Access	Hos	tname Autono	mous								
Encryption Manager	Se	acurity Summ	iary								
SSID Manager Server Manager	Ad	Iministrators									
AP Authentication	Us	ername						Read-Only			
Intrusion Detection	Ci	sco						1			
Local RADIUS Server	Se	ervice Set Iden	tifiers (SSIDs)								
Advance Secondy	S	SID		VI	AN	BandSele	ect	Radio	В	SSID/Guest	Mode√



#### MAC 地址过滤器

您可以使用基于MAC地址的过滤器来根据硬编码MAC地址过滤客户端设备。当通过基于 MAC 的过滤器拒绝客户端访问时,该客户端不能与 AP 产生关联。MAC地址过滤器允许或不允许转发从特定 MAC地址发送或发往特定MAC地址的单播和组播数据包。

本示例说明如何通过GUI配置基于MAC的过滤器,以便使用MAC地址0040.96a5.b5d4过滤客户端:

1. 创建MAC地址ACL 700。此 ACL 不允许客户端 0040.96a5.b5d4 与 AP 关联。

	HOME BETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENTLOG	Saya Configuration (Bing Logaut) Bafrie
Security	APPLY FILTERS MAC ADDRESS FILTERS	ETHERTYPE FILTERS
Admin Access	Hostname Autonomous	Autonomous uptime is 4 weeks, 10 hours, 6 minutes
Encryption Manager SSID Manager	Services: Filters - MAC Address Filters	
Server Manager AP Authentication	Create/Edit Filter Index: < NEW > .	
Intrusion Detection Local RADIUS Server Advance Security	Filter Index: 700 (700-799)	
	Add MAC Address:         0040.9695.55d4         Mask:         0000.0000.0000         Action:         Block         Add           (HHHH HHHH)         (HHHH HHHH)         (HHHH HHHH)         (HHHH HHHH)         (HHHH HHHH)	
	Default Action: None -	
	Filters Classes:	
	~ Delete Class.	
		Apply Delate Cancel

- 2. 单击Add以将此过滤器添加到Filters Classes中。还可以将默认操作定义为Forward All或Deny All。
- 3. 单击 Apply。ACL 700现已创建。
- 4. 要将ACL 700应用到无线电接口,请导航到应用过滤器部分。现在可以将此ACL应用于传入或 传出Radio或GigabitEthernet接口。

ecurity	í.	APPLY	FILTERS	MAC ADDRESS FLITERS	II IPFL	TERS (1	ETHERTYPE RLTERS	
Idmin Access	Ľ.,	ofacera Julian					Autonomous uptin	e is 4 weeks, 16 hours, 11 minute
incryption Manager ISID Manager		Services: Filter	s - Apply Filters					
ierver Manager	- F		Radio	0-802.11N <sup>2.4GHz</sup>	Radi	io1-802.11N <sup>8GHz</sup>	Gig	abitEthernet0
IP Authentication	1	ncoming	MAC	< NONE >	MAC	< NONE >	MAG	< NONE >
ocal RADIUS Server			EtherType	< NONE >	EtherType	<none> *</none>	EtherType	< NONE > .
dvance security			IP	< NONE > •	IP	< NONE > •	P	< NONE > .
	9	Outgoing	MAC	< NONE > .	MAC	<none> *</none>	MAC	< NONE >
			EtherType	< NONE > .	EtherType	< NONE >	EtherType	< NONE > .
			IP	< NONE > .	IP	< NONE > *	P	< NONE > .
	_							
								Apply Can

您可以使用标准ACL或扩展ACL来根据客户端的IP地址允许或禁止客户端设备进入WLAN网络。

此配置示例使用扩展ACL。扩展ACL必须允许对客户端进行Telnet访问。您必须限制 WLAN 网络上的所有其他协议。此外,客户端使用DHCP来获取IP地址。您必须创建以下这种扩展 ACL:

- 允许 DHCP 和 Telnet 流量
- 拒绝所有其他数据流类型

完成以下步骤以创建它:

1. 为过滤器命名,并从Default Action下拉列表中选择Block All,因为必须阻止剩余流量:

cisco	HOME NETWORK ASS	OCIATION WIRELESS SECURITY SERV	VICES SOFTWARE EVENTLOG	Selfe roa	udinasion Fuld redork Fie
Security	APPLY FILTER	S I NAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS	
Admin Access	Hostname Autonomous			Autonomous uptime i	s 4 weeks, 16 hours, 14 minutes
Encryption Manager SSID Manager	Services: Filters - IP	Filters			
Server Manager AP Authentication Intrusion Detection	Create/Edit Filter Na	< NEW > •			
Local RADIUS Server	Filter Name:	Allow_DHCP_Telnet			
Advance Security	Default Action:	Block All			
	IP Address				
	Destination Address		Mask: 0.0.0.0	]	
	Source Address:	0.0.0.0	Mask: 255.255.255.255	1	
				Action:	Forward  Add
	IP Protocol				
	IP Protocel:	Authentication Header Protocol (51)	×	Action:	Forward  Add
		© Custom (0-255)			

2. 从TCP Port下拉列表中选择Telnet,从UDP Port下拉列表中选择BOOTP client & BOOTP server:

		Selfs combination Find	rodore Reuen
CISCO	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENTLOG		
Security	IP Protocol:      Authentication Header Protocol (51)	Action: Forward	Add
Admin Access Encryption Manager	© Custom (0-255)		
Server Manager	UDP/TCP Port		
AP Authentication Intrusion Detection	TCP Port:   Tahat (23)  TCP Port:	Action: Forward	Add
Local RADIUS Server	© Gustom (0-65535)		
Advance Security	JDP Port:	Action: Forward •	Add
	(u-dubba)		
	Filters Classes		
	TCP port: Telinat (23) - Forward UDP port: Bottstrap Protocol (BOOTP) client (68) - Forward BDM port: Bottstrap Protocol (BOOTP) server (67) - Forward Default - Block All	- Delete Class	
		Apply, Del	ete Cancel

3. 单击 Apply。IP过滤器Allow\_DHCP?\_Telnet现已创建,您可以将此ACL应用于传入或传出

#### Radio或GigabitEthernet接口。

սիսիս						Say	e Configuration Eing Logout Befreah
CISCO	HOME NETWORK	ASSOCIATION	WIRELESS SECURITY S	ERVICES SOFTWARE	EVENTLOG		
Security	APPL	FILTERS	MAC ADDRESS FILTE	IRS	IP FLITERS	ETHERTYPE RUTER:	1
Admin Access	Hostname Autor	omous				Autonomour	s uptime is 4 weeks, 16 hours, 25 minutes
Encryption Manager							
SSID Manager	Services: Filb	irs - Apply Filters					
Server Manager		6	tadio0-802.11N <sup>2.4GHz</sup>		Radio1-802.11NSGHz		GigabitEthernet0
Intrusion Detection	Incoming	MAC	< NONE >	MAC	< NONE > .	MAC	< NONE > .
Local RADIUS Server		EtherType	< NONE > .	EtherType	< NONE > m	EtherType	< NONE > m
Paranta secondy		IP	< NONE >	P	< NONE >	P	< NONE >
	Outgoing	MAC	Allow_OHCP_Telnet	MAC	< NONE > .	MAC	< NONE > *
		EtherType	< NONE > .	EtherType	< NONE > •	EtherType	< NONE > •
		IP	< NONE >	P	< NONE >	P	< NONE >
	_						
							Apply. Gencel

## Ethertype过滤器

您可以使用Ethertype过滤器阻止Cisco Aironet AP上的网间数据包交换(IPX)流量。当IPX服务器广播阻塞无线链路时(有时在大型企业网络中发生),这是非常有用的情况。

要配置和应用阻止IPX流量的过滤器,请完成以下步骤:

- 1. 单击Ethertype Filters选项卡。
- 2. 在Filter Index字段中,使用介于200和299之间的数字命名过滤器。您指定的数字会为过滤器 创建ACL。
- 3. 在Add Ethertype字段中输入8137。
- 4. 将Mask字段中的Ethertype掩码保留为默认值。
- 5. 从操作菜单中选择Block,然后单击Add。

cisco	HOME DETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENTLO	Saya Configuration (Ding) Logost (Bafnach G
Security	APPLY FILTERS	ETHERTYPE FILTERS Autonomous uptime is 4 weeks, 16 hours, 35 minutes
Encryption Manager SSID Manager	Services: Filters - EtherType Filters	
Server Manager AP Authentication	Create/Edit Filter Index: < NEW >	
Local RADIUS Server Advance Security	Filter Index: 200 (200-299)	
	Add EtherType: 8137 Mask: 0000 (0.FFFE) (0.FFFE)	Action: Block x Add
	Default Action: None .	
	Filters Classes:	
	Etherlype: 8137 Mask: 0000 - Block A Default - None	
	- Delute Class	
		Apply Delate Cancel

6. 要从Filters Classes列表中删除Ethertype,请选择它,然后单击Delete Class。重复上述步骤 ,将类型8138、00ff和00e0添加到过滤器。现在可以将此ACL应用于传入或传出Radio或

## GigabitEthernet接口。

/	APPLY	YFILTERS	MAC ADDRESS FILTERS	¥.	IP FILTERS	ETHERTYPE FILTER	S
Access	Hostname Autor	nomous				Autonomou	s uptime is 4 weeks, 16 hours, 3
ion Manager onøger	Services: Filte	ers - Apply Filters					
Manager			Radio0.802.11N <sup>2.4GHz</sup>		Radio1-802.11N <sup>5GHz</sup>		GigabitEthernet®
a Detection	Incoming	MAC	< NONE > •	MAC	< NONE > •	MAC	< NONE > •
DIUS Server		EtherType	<none> x</none>	EtherType	< NONE > m	EtherType	< NONE >
		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 >

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。