# **Exemplo de configuração de filtros ACL em APs Aironet**

### Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configurar Onde criar ACLs Filtros de endereço MAC Filtros IP Filtros Ethertype

## 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 <u>Access Point ACL Filter Configuration Example</u> 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**:

.վովո cisco	HOME	NETWORK	ASSOCIATION	WIREL	ess <u>s</u> i	ECURITY	<u>s</u> ervice	:S <u>s</u> oftwa	re <u>e</u> vent	LOG	
Security Admin Access Encryption Manager SSID Manager	Hos	stname Autono ecurity Sumn Iministrators	omous nary		-						
AP Authentication Intrusion Detection	Username Cisco					Read-Only					
Advance Security	S	ervice SetIden SID	tifiers (SSIDs)		VLAN	BandS	elect	Radio	•	BSSID/Guest	t Mode√
uluulu cisco	Номе	NETWORK	ASSOCIATION	WIRELES	s <u>s</u> eci	JRITY <u>s</u> i	ERVICES	SOFTWARE	EVENT LOG	5	
Security Admin Access Encryption Manager	AU	IAC ADDRESS THENTICATION tname Autonor	nous	TIMER	3	ĺ.	ASSOCIATIO	T			_
SSID Manager Server Manager AP Authentication Intrusion Detection Local RADIUS Server Advance Security	F	acurity: Advan	ced Security-As	sociation A	access I	at ist:			< NONE >	Define Fill	er

### 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.

Security	APPLY FILTERS	MAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE RUTERS								
Admin Access	Hostname Autonomous			Autonomous uptima	is 4 weeks, 16 hours, 6 minutes							
Encryption Manager SSID Manager	Services: Filters - MAC Address Filters											
Server Manager AP Authentication	Creana/Edit Filter Index: < NEW >											
Intrusion Detection Local RADIUS Server Advance Security	Filter Index: 700	(700-799)										
	Add MAC Address: 0040.962 (HHHH.H	6.5564 Mesil: 0000.0000.0000 Actio	m: Block 💌 Add									
	Default Action: None											
	Filters Classes:											
		- Delete Ci	ass.									

- 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.

urity	APPLY	IL TERS	MAC ADDRESS FILTERS	E IPFL	TERS I	ETHERTYPE RLTERS					
min Access	linetanes lutera					Autonomous uptim	e is 4 weeks, 16 hours, 11 minu				
Encryption Manager SSID Manager	Services: Filters - Apply Filters										
rver Hanager		Radio	0-802.11N <sup>2.4GHz</sup>	Radi	o1-802.11NSGHz	GigabitEthernet0					
rusion Detection	Incoming	MAC	< NONE >	MAC	< NONE >	MAG	< NONE > .				
Local RADIUS Server		EtherType	< NONE >	EtherType	<none> x</none>	EtherType	< NONE >				
vance securey		IP	< NONE > •	IP	< NONE > •	P	< NONE > •				
	Outgoing	MAC	< NONE >	MAC	< NONE > x	MAC	< NONE > m				
		EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >				
		IP	< NONE >	IP	< NONE >	P	< NONE >				
							Apply C				

### **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:

cisco	HOME NETWORK ASSO	CIATION WIRELESS SECURITY SERVICE	ES SOFTWARE EVENTLOG	Sage Lonn	idmanica Rud rodons Rea
Security	E APPLY FILTERS	NAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS	1
Admin Access	Hostname Autonomous			Autonomous uptime is	4 weeks, 16 hours, 14 minutes
Encryption Manager SSID Manager	Services: Filters - IP F	itters			
Server Manager AP Authentication	Create/Edit Filter Nat	< NEW > •			
Intrusion Detection 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 Protocel:	Authentication Header Protocol (51)	*	Action:	Forward  Add

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

cisco	1400	E NETWORK	ASSOCIATION	WIRELESS	SECURITY	SERVICES	SOFTWARE	EVENTLOG		Sile	Computition Find	rogent   Beue
Security Admin Access Encryption Manager SSID Manager Server Manager AP Authentication Intrusion Detection Local RADIUS Server	Ber	IP Protocol:	<ul> <li>Aut</li> <li>Cust</li> </ul>	hentication Hea	ader Protocol	(51) -255)		Even con		Action:	Forward •	Add
		UDP/TCP Port	<ul> <li>Telnet (</li> <li>Custom</li> </ul>	23)	(0-655	35)				Action:	Forward	Add
Advance Security		JOP Port:	<ul> <li>Bootsto</li> <li>Custom</li> </ul>	ap Protocol (BC	00TP) server (	(67) 35)				Action:	Forward •	Add
		Filters Classes										
		TCP port: Telma UDP port: Bost Networker(1995) Default - Block	t (23) - Forward strap Protocol (BO strap Protocol (II) All	OTP) client (6) OTP) server (6	l) - Forward 7) - Forward				, and the second	Jelete Class		
											Apply De	lete Cancel

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.

	HOME	NETWORK	ASSOCIATION	WRELESS	SECURITY	SERVICES	SOFTWARE	EVENTLOG		Saj	e Configuration Bing Lagout Befm	enh.	
Security	Ĵ.	APPLY	FILTERS	1 MA	C ADDRESS FI	LTERS	)i	IP FILTERS	- I	ETHERTYPE PLTER	\$	_	
Admin Access	Hos	Hosthame Autonomous aptime is 4 weeks, 16 hours, 25 minutes Sorvices: Filters - Apply Filters											
SSID Manager	s												
Server Manager			1	Radio0-802.11N <sup>2.4GHz</sup>			Radio1-802.11N <sup>5GHz</sup>		Gfz	GigabitEthernet0			
Intrusion Detection	in	coming	MAC	< NONE > 💌	1		MAC	< NONE >		MAC	< NONE >		
Local RADIUS Server			EtherType	< NONE > .	1		EtherType	< NONE > .		EtherType	< NONE > #		
Automa Security			IP	< NONE >			P	< NONE >		P	< NONE >		
	0	utgoing	MAC	Allow_DHCP	Telnet		MAC	< NONE > 💌		MAC	< NONE > *		
			EtherType	< NONE >	1		EtherType	< NONE > •		EtherType	< NONE > •		
			IP	< NONE >			Ρ	< NONE >		P	< NONE >		
	-										Apply Cano		

#### **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.

cisco	HOME NETWORK ASSOCIAT	ION WIRELESS SECURITY SE	RVICES SOFTWARE EVENTLOG	Saya Configu	nation <u>B</u> ing Logout Befreeh
Security Admin Access Encryption Manager SSTD Manager Server Manager AP Authentication Intrusion Detection Local RADIUS Server Advance Security	APPLY FILTERS Hostname Autonomous	TE MAC ADDRESS FILTER	S IS IP FATERS	ETHERTYPE FILTERS Autonomous uptime is 4	meeks, 16 hours, 35 minutes
	Create/Edit Filter Index:	< NEW >	1		
	Filter Index:	200 (200-25	9) Mask: 0000	Action: Block	Add
	Default Action:	(G.FFFF)	(0.##PE)		
	Filters Classes:				
	Default - None	9 - DADCK	- [Delate Class]		
					Apply Delete Cancel

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.

cisco	HOME NETWORK	ASSOCIATION	WIRELESS SECURITY	SERVICES SOFTWARE	EVENT LOG	Say	e Configuration   Eng	Logout Befreah					
Security	APPL	Y FILTERS	MAC ADDRESS	FILTERS	IP FILTERS	ETHERTYPE PLTER	B						
Admin Access	Hostname Auto	nomous	_			Autonomou	s uptime is 4 weeks, 16	hours, 37 minutes					
Encryption Manager SSID Manager	Services: Filt	Services: Filters - Apply Filters											
Server Manager			Radio0.802.11N <sup>2.4GHz</sup>		Radio1-802.11NSGRs		GigabitEthernetD	EthernetD					
Intrusion Detection	Incoming	MAC	< NONE > •	MAC	< NONE > •	MAC	< NONE > •						
Local RADIUS Server		EtherType	< NONE > IN	EtherType	< NONE > x	EtherType	< NONE > .						
		IP	200 •	P	< NONE >	P	< NONE >	•					
	Outgoing	MAC	< NONE > .	MAC	< NONE > x	MAC	< NONE > *						
		EtherType	< NONE > •	EtherType	< NONE > .	EtherType	< NONE > x						
		IP	< NONE >	P	< NONE >	P	< NONE >						
								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.