Ejemplo de Configuración de Filtros ACL en AP Aironet

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Configurar Dónde crear ACL Filtros de dirección MAC Filtros IP Filtros Ethertype

Introducción

Este documento describe cómo configurar filtros basados en listas de control de acceso (ACL) en puntos de acceso (AP) Cisco Aironet con el uso de la GUI.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- La configuración de una conexión inalámbrica con el uso de un Aironet AP y un Aironet 802.11 a/b/g Client Adapter
- Listas de control de acceso (ACL)

Componentes Utilizados

Este documento utiliza los AP Aironet 1040 Series que ejecutan Cisco IOS[®] software Release 15.2(2)JB.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Puede utilizar filtros en los AP para realizar estas tareas:

- Restringir el acceso a la red LAN inalámbrica (WLAN)
- Proporcionar una capa adicional de seguridad inalámbrica

Puede utilizar diferentes tipos de filtros para filtrar el tráfico basado en:

- Protocolos específicos
- · La dirección MAC del dispositivo cliente
- · La dirección IP del dispositivo cliente

También puede activar filtros para restringir el tráfico de los usuarios en la LAN por cable. Los filtros de direcciones IP y MAC permiten o no el reenvío de paquetes de unidifusión y multidifusión enviados a o desde direcciones IP o MAC específicas.

Los filtros basados en protocolo proporcionan una manera más granular de restringir el acceso a protocolos específicos a través de las interfaces Ethernet y de radio del AP. Puede utilizar cualquiera de estos métodos para configurar los filtros en los AP:

- GUI web
- CLI

Este documento explica cómo utilizar las ACL para configurar filtros a través de la GUI.

Nota: Para obtener más información sobre la configuración mediante el uso de la CLI, consulte el artículo <u>Ejemplo de configuración del filtro ACL del punto de acceso</u> Cisco.

Configurar

Esta sección describe cómo configurar filtros basados en ACL en Cisco Aironet AP con el uso de la GUI.

Dónde crear ACL

Vaya a Seguridad > Seguridad avanzada. Elija la pestaña Association Access List y haga clic en Define Filter:

uluilu cisco	HOME	<u>N</u> ETWORK	ASSOCIATION	WIRELESS	SEC	CURITY <u>s</u> e	RVICES	SOFTWARE	EVENTLO)G	
Security Admin Access	Hos	stname Autono	omous								
Encryption Manager SSID Manager Server Manager	S.	ecurity Summ dministrators	nary								
AP Authentication	U	sername						Read-Only			
Intrusion Detection	Cisco					✓					
Local RADIUS Server	50	ervice Set Iden	tifiers (SSIDs)		1						
	S	SID		VL	AN	BandSelec	t	Radio	E	3SSID/Guest	Mode√



Filtros de dirección MAC

Puede utilizar filtros basados en direcciones MAC para filtrar los dispositivos cliente basados en la dirección MAC codificada de forma rígida. Cuando a un cliente se le niega el acceso a través de un filtro basado en MAC, el cliente no puede asociarse con el AP. Los filtros de direcciones MAC permiten o no el reenvío de paquetes de unidifusión y multidifusión enviados desde direcciones MAC específicas o dirigidos a ellas.

Este ejemplo ilustra cómo configurar un filtro basado en MAC a través de la GUI para filtrar el cliente con una dirección MAC de 0040.96a5.b5d4:

1. Cree la dirección MAC ACL 700. Esta ACL no permite que el cliente 0040.96a5.b5d4 se asocie con el AP.

	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENTLOG	Saye Configuration Bing Logout Bafree
CISCO Security Admin Access Encryption Manager SSID Monager Server Manager AP Authentication Intrusion Detection	HOME BETWORK ASSOCIATION WEELESS SECURITY SERVICES SOFTWARE LVENT LOS APPLY FILTERS HOSTBARE Autonomous Services: Filters - MAC Address Filters Creata/Edit Filter Index: <new></new>	ETHERTYPE RLTERS Autonomous uptime is 4 weeks, 16 hours, 6 minutes
Local RADIUS Server Advance Security	Filter Index: 700 (700-799) Add MAC Address: 0040 96x5.b5d4 Mastic 0000 0000 0000 Action: Block Add (HHHH HHHH HHHH HHHH) Default Action: None	
	Filters Classes:	
		Apply: Delete Cancel

- 2. Haga clic en Agregar para agregar este filtro a las Clases de Filtros. También puede definir la acción predeterminada como Reenviar todas o Denegar todas.
- 3. Haga clic en Apply (Aplicar). ACL 700 se ha creado.
- Para aplicar ACL 700 a una interfaz de radio, navegue hasta la sección Aplicación de Filtros. Ahora puede aplicar esta ACL a una Radio entrante o saliente o a una interfaz GigabitEthernet.

 cisco	HOME NETWOR	K ASSOCIATION WIRE	LESS SECURITY S	ERVICES SOFTWARE	EVENT	106	Saya Corr	igunation <u>Bing</u> Logout Befree
Security Admin Access		YFRITERS	WAC ADDRESS FILTE	RS	IPFLT	IRS	ETHERTYPE RLTERS Autonomous uptin	e is 4 weeks, 16 hours, 11 minutes
Encryption Manager SSID Manager Server Manager	Services: Fill	ters - Apply Filters						- 1964
AP Authentication	Incoming	Radio	< NONE >		Radio/	< NONE > •	GIG	< NONE > .
Local RADIUS Server Advance Security		EtherType	< NONE >	Ethe	Type	< NONE > •	EtherType	< NONE > x
	Outoning	IP	< NONE > •		IP	< NONE > •	P	< NONE > .
	ouguig	EtherType	<none> .</none>	Ethe	Туре	<none> •</none>	EtherType	< NONE >
		IP	< NONE >		IP	< NONE > .	P	< NONE > .
					_			Apply. Cancel
		Close Window			_		Copyright (c) 1992-	2009, 2011-2012 by Cisco Systems, ir

Filtros IP

Puede utilizar ACL estándar o extendidas para permitir o no la entrada de dispositivos cliente en la red WLAN basada en la dirección IP del cliente.

Este ejemplo de configuración utiliza ACL extendidas. La ACL extendida debe permitir el acceso Telnet a los clientes. Debe restringir todos los demás protocolos de la red WLAN. Además, los clientes utilizan DHCP para obtener la dirección IP. Debe crear una lista de control de acceso ampliada que:

- Permite el tráfico DHCP y Telnet
- · Niega todos los demás tipos de tráfico

Complete estos pasos para crearlo:

1. Asigne un nombre al filtro y seleccione Block All en la lista desplegable Default Action, ya que el tráfico restante debe bloquearse:

cisco	HOME NETWORK ASSO	CIATION WIRELESS SECURITY SERVIC	ES SOFTWARE EVENTLOG	Saya La	udnumou Fud redont Paul
Security	APPLY FILTERS	HE WAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS Autonomous uptime	is 4 weeks, 16 hours, 14 minutes
Encryption Manager SSID Monoper Server Manager	Services: Filters - IP F	iten			
AP Authentication Intrusion Detection Local RADIUS Server Advance Security	Filter Name: Default Action:	Allow_DHCP_Teinet			
	IP Address				
	Destination Address: Source Address:	0.00.0	Mask: 0.0.0.0 Mask: 255.255.255.255	Artise	Fround w Add
	IP Protocol			ACOUR.	
	IP Protocol:	Authentication Header Photocol (51) Custom (0-255)	×	Action:	Forward

2. Seleccione Telnet en la lista desplegable TCP Port y BOOTP client & BOOTP server en la lista desplegable UDP Port:

cisco	HOM	E NETWORK	ASSOCIATION	WIRELESS	SECURITY	SERVICES	SOFTWARE	EVENTLOG			Sege Computition But	d rodony Rewee
Security		IP Protocol:	Aut	hentication Hea	der Protocol (5	1)	•			Action:	Forward .	Add
Admin Access Encryption Manager			© Cust	om	(0-2	55)						
SSID Manager Server Manager		UDP/TCP Port										
AP Authentication Intrusion Detection		TCP Port:	Teinet (23)						Action:	Forward .	Add
Local RADIUS Server Advance Security			© Custom		(0-66535	5)	_					
		JDP Port:	Bootstra	ap Protocol (BC	OTP) server (6	ŋ				Action:	Forward •	Add
			© Custom		(0-66535	5)						
		Filters Classes										
		TCP part: Telhe UDP part: Boot	it (23) - Forward strap Protocol (BO	OTP) client (68) - Forward				1			
		Default - Block	All	orrej same (a) - Porward					Delete Class		
	_									_	_	
											Apply	Delete Cancel

3. Haga clic en Apply (Aplicar). Ahora se crea el filtro IP Allow_DHCP?_Telnet, y puede aplicar esta ACL a una Radio entrante o saliente o a una interfaz GigabitEthernet.

cisco	HOME NETWORK	ASSOCIATION	WIRELESS SECURITY SER	VICES SOFTWARE	EVENTLOG		fe countration bud rothers Per
surity	APPLY	FILTERS	MAC ADDRESS FILTERS	i ji	IP FLITERS	ETHERTYPE RUTER	8
min Access	Hostname Autor	omous				Autonomou	s uptime is 4 weeks, 16 hours, 25 minutes
cryption Manager 3D Manager	Services: Filte	ers - Apply Filters					
rver Manager			Radio0-802.11N ^{2.4GHz}		Radio1-802.11N ^{5GHz}		GigabitEthernet0
Authentication trusion Detection	Incoming	MAC	< NONE > .	MAC	< NONE > .	MAC	< NONE > •
cal RADIUS Server		EtherType	< NONE >	EtherType	< NONE > m	EtherType	< NONE >
vulle secarey		IP	< NONE >	P	< NONE >	P	< NORE >
	Outgoing	MAC	Allow_DHCP_Telnet	MAC	< NONE > .	MAC	< NONE > *
		EtherType	< NONE > .	EtherType	< NONE > •	EtherType	< NONE > •
		IP	<none></none>	ρ	< NONE >	P	< NONE >

Filtros Ethertype

Puede utilizar los filtros Ethertype para bloquear el tráfico Internetwork Packet Exchange (IPX) en el Cisco Aironet AP. Una situación típica en la que esto es útil es cuando las transmisiones del servidor IPX bloquean el link inalámbrico, lo que a veces sucede en una red empresarial grande.

Complete estos pasos para configurar y aplicar un filtro que bloquee el tráfico IPX:

- 1. Haga clic en la pestaña Ethertype Filters.
- 2. En el campo Filter Index, asigne al filtro un nombre con un número entre 200 y 299. El número que asigne creará una ACL para el filtro.
- 3. Ingrese 8137 en el campo Add Ethertype.
- 4. Deje la máscara para el Ethertype en el campo Mask en el valor predeterminado.

5. Seleccione Block en el menú action y haga clic en Add.

rity	E APPLY FILTERS	H WAC ADDRESS FILTERS	IF IP FILTERS	ETHERTYPE FILTERS	
in Access	Hostname Autonomous			Autonomous uptime is 4 wee	ks, 16 hours, 35 minute
yption Manager) Manager	Services: Filters - EtherType	a Filters			
er Manager uthentication	Create/Edit Filter Index:	< NEW > -			
asion Detection al RADIUS Server ance Security	Filter Index:	200 (200-299)			
	Add EtherType:	8137	Mask: 0000	Action: Block 💌	Add
		(0.4444)	(0-FFFE)		
	Default Action:	None			
	Filters Classes:				
	EtterType: 8137 Mask: 0000 Default - None	- Block A			
		-	Delute Class		

6. Para quitar el Ethertype de la lista de las clases de los filtros, selecciónelo, y haga clic en Borrar clase. Repita los pasos anteriores y agregue los tipos 8138, 00ff y 00e0 al filtro. Ahora puede aplicar esta ACL a una Radio entrante o saliente o a una interfaz GigabitEthernet.

ity	APPL	YFILTERS	WAC ADDRESS	FILTERS	IP FILTERS	ETHERTYPE FILTERS	8
Access	Hostname Auto	namous				Autonomous	uptime is 4 weeks, 16 hours, 37 n
Manager Manager	Services: Filt	ers - Apply Filters	6				
r Manager			Radio0-802.11N ^{2.4GHz}		Radio1-882.11NSGRs		GigabitEthernet®
ion Detection	Incoming	MAC	< NONE > •	MAC	< NONE > •	MAC	< NONE > •
RADIUS Server		EtherType	<none></none>	EtherType	< NONE > m	EtherType	< NONE >
Chi Jacan ny		IP	200 ·	P	< NONE >	P	< NONE >
	Outgoing	MAC	< NONE >	MAC	< NONE > m	MAC	< NONE > 💌
		EtherType	< NONE > •	EtherType	< NONE > .	EtherType	< NONE > .
		IP	<none></none>	P	< NONE >	P	< NONE >

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).