Ejemplo de Configuración de ACL en el Controlador de LAN Inalámbrica

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones ACL en WLC Consideraciones Cuando los ACL se Configuran en los WLCs Configuración de ACL en WLC Configurar reglas que permiten servicios de usuario invitado Configuración de ACL de CPU Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe cómo configurar las listas de control de acceso (ACL) en los controladores de LAN inalámbrica (WLAN) para filtrar el tráfico a través de la WLAN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo configurar el WLC y el Lightweight Access Point (LAP) para el funcionamiento básico
- Conocimientos básicos sobre el protocolo de punto de acceso ligero (LWAPP) y los métodos de seguridad inalámbrica

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de la serie 2000 de Cisco que ejecuta firmware 4.0
- LAP de la serie 1000 de Cisco
- Adaptador de cliente inalámbrico Cisco 802.11a/b/g que ejecuta firmware 2.6
- Cisco Aironet Desktop Utility (ADU) versión 2.6

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). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

ACL en WLC

Las ACL en el WLC están destinadas a restringir o permitir a los clientes inalámbricos a los servicios en su WLAN.

Antes de la versión 4.0 del firmware del WLC, las ACL se omiten en la interfaz de administración, por lo que no puede afectar el tráfico destinado al WLC; sólo puede impedir que los clientes inalámbricos administren el controlador con la opción **Administración vía inalámbrica**. Por lo tanto, las ACL sólo se pueden aplicar a interfaces dinámicas. En la versión 4.0 del firmware del WLC, hay ACL de la CPU que pueden filtrar el tráfico destinado para la interfaz de administración. Consulte la sección <u>Configuración de ACL de CPU</u> para obtener más información.

Puede definir hasta 64 ACL, cada una con hasta 64 reglas (o filtros). Cada regla tiene parámetros que afectan a su acción. Cuando un paquete coincide con todos los parámetros de una regla, la acción establecida para esa regla se aplica al paquete. Puede configurar las ACL mediante la GUI o la CLI.

Estas son algunas de las reglas que necesita entender antes de configurar una ACL en el WLC:

- Si el origen y el destino son **cualquiera**, la dirección en la que se aplica esta ACL puede ser **cualquiera**.
- Si source ordestination **no** es **any**, se debe especificar la dirección del filtro y se debe crear una instrucción inversa en la dirección opuesta.
- La noción de WLC de entrante versus saliente no es intuitiva. Es desde la perspectiva del WLC que mira hacia el cliente inalámbrico, más que desde la perspectiva del cliente. Por lo tanto, la dirección entrante significa un paquete que entra en el WLC del cliente inalámbrico y la dirección saliente significa un paquete que sale del WLC hacia el cliente inalámbrico.
- Hay una negación implícita al final de la ACL.

Consideraciones Cuando los ACL se Configuran en los WLCs

Los ALCs en los WLCs funcionan de manera diferente que en los routers. Éstas son algunas cosas a recordar cuando usted configura los ACL en los WLCs:

- El error más común es seleccionar IP cuando pretende denegar o permitir paquetes IP. Dado que selecciona lo que está dentro del paquete IP, deniega o permite los paquetes IP en IP.
- Las ACL del controlador no pueden bloquear la dirección IP virtual del WLC y, por lo tanto, los paquetes DHCP para los clientes inalámbricos.
- Las ACL de controlador no pueden bloquear el tráfico de multidifusión recibido de las redes con cable destinadas a los clientes inalámbricos. Las ACL de controlador se procesan para el

tráfico multicast iniciado desde clientes inalámbricos, destinados a redes cableadas u otros clientes inalámbricos en el mismo controlador.

- A diferencia de un router, la ACL controla el tráfico en ambas direcciones cuando se aplica a una interfaz, pero no realiza un stateful firewall. Si olvida abrir un agujero en la ACL para el tráfico de retorno, esto causa un problema.
- Las ACL de controlador solo bloquean los paquetes IP. No puede bloquear las ACL de Capa 2 o los paquetes de Capa 3 que no son IP.
- Las ACL de controlador no utilizan máscaras inversas como los routers. Aquí, 255 significa que coincide exactamente con ese octeto de la dirección IP.
- Las ACL en el controlador se realizan en el software y afectan el rendimiento de reenvío.

Nota: Si aplica una ACL a una interfaz o a una WLAN, el rendimiento inalámbrico se degrada y puede conducir a la pérdida potencial de paquetes. Para mejorar el rendimiento, elimine la ACL de la interfaz o WLAN y mueva la ACL a un dispositivo con cables vecino.

Configuración de ACL en WLC

Esta sección describe cómo configurar una ACL en el WLC. El objetivo es configurar una ACL que permita a los clientes invitados acceder a estos servicios:

- Protocolo de configuración dinámica de host (DHCP) entre clientes inalámbricos y servidor DHCP
- Protocolo de mensajes de control de Internet (ICMP) entre todos los dispositivos de la red
- Sistema de nombres de dominio (DNS) entre los clientes inalámbricos y el servidor DNS
- Telnet a una subred específica

Todos los demás servicios deben estar bloqueados para los clientes inalámbricos. Complete estos pasos para crear la ACL con la GUI del WLC:

 Vaya a la GUI del WLC y elija Security > Access Control Lists. Aparecerá la página Listas de Control de Acceso. Esta página enumera las ACL que se configuran en el WLC. También le permite editar o eliminar cualquiera de las ACL. Para crear una nueva ACL, haga clic en New

G · O · 🛃 🙆 :	🐔 🔎 👷 🧐 🧔 - 🍓 " Address 🕘 https://172.16.1.40/screens/fire 🚽 🛃 Go 🛛 Linis " Norton Additions 🧐 - 🧉 🖉 - 🖉 - 🖉
Casco Sestens	Save Configuration Ping Logout Refresh
A. A.	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	Access Control Lists New
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Name
Access Control Lists	
Web Auth Certificate	
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Suspature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	
Web Login Page CIDS Sensors Shunned Clients	
8)	🥥 Internet

Listas de control de acceso

2. Introduzca el nombre de la ACL y haga clic en **Apply**.Puede ingresar hasta 32 caracteres alfanuméricos. En este ejemplo, el nombre de la ACL es **Guest-ACL**. Una vez creada la ACL, haga clic en **Editar** para crear reglas para la ACL.



Introduzca el nombre de la ACL

 Cuando aparezca la página Listas de control de acceso > Editar, haga clic en Agregar nueva regla. Aparecerá la página Listas de Control de Acceso > Reglas > Nuevo.

Security	MONITOR W	ol Lists > Edit	R WIRELESS	SECURITY			Si	we Configura	tion Ping Logout Refresh
Security	MONITOR W	ILANS CONTROLLE	R WIRELESS	SECURITY	Construction of the local sectors of the local sect				
Security	Access Contr	ol Lists > Edit			MANAGE	MENT	COMMAN	VDS HELP	
occomy							1	< Back	Add New Rule
AAA General	General								
RADIUS Authentication RADIUS Accounting Local Net Users	Access List Nam	Guest-ACL	Destination	Protocol	Source	Dest	DSCP	Direction	
Disabled Clients User Login Policies AP Policies			IP/Mask		Port	Port			
Access Control Lists									
Web Auth Certificate									
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection									
Web Login Page CIDS Sensors Shunned Clients									
Done									🕘 Internet

Agregar nuevas reglas ACL

4. Configure reglas que permitan a un usuario invitado estos servicios:DHCP entre los clientes inalámbricos y el servidor DHCPICMP entre todos los dispositivos de la redDNS entre los clientes inalámbricos y el servidor DNSTelnet a una subred específica

Configurar reglas que permiten servicios de usuario invitado

Esta sección muestra un ejemplo de cómo configurar las reglas para estos servicios:

- DHCP entre los clientes inalámbricos y el servidor DHCP
- ICMP entre todos los dispositivos de la red
- DNS entre los clientes inalámbricos y el servidor DNS
- Telnet a una subred específica
- Para definir la regla para el servicio DHCP, seleccione los rangos de IP de origen y de destino.En este ejemplo se utiliza any para el origen, lo que significa que se permite el acceso de cualquier cliente inalámbrico al servidor DHCP. En este ejemplo, el servidor 172.16.1.1 actúa como servidor DHCP y DNS. Por lo tanto, la dirección IP de destino es 172.16.1.1/255.255.255.255 (con una máscara de host).Debido a que DHCP es un protocolo basado en UDP, seleccione UDP en el campo desplegable Protocol . Si ha seleccionado TCP o UDP en el paso anterior, aparecerán dos parámetros adicionales: Puerto de origen y Puerto de destino. Especifique los detalles del puerto de origen y de destino. Para esta regla, el puerto de origen es DHCP Client y el puerto de destino es DHCP Server .Elija la dirección en la que se aplicará la ACL. Dado que esta regla va del cliente al servidor, en este ejemplo se utiliza Inbound. En el cuadro desplegable Action (Acción), elija Permit para que

esta ACL permita paquetes DHCP del cliente inalámbrico al servidor DHCP. El valor predeterminado es Deny. Haga clic en Apply

(Aplicar).

0 · 0 · 1	6 P + 8 6	Address 💩 http	s://172.16.1.40/screens/fre 💙 🖁	Go Links Norton A	int/linus 🧕 •	🦓 – 8 ×
Casco Stattan				Save Confi	iguration Ping	Logout Refresh
A. A.	MONITOR WLANS	CONTROLLER WIRELES	S SECURITY MANAGEM	ENT COMMANDS H	ELP	
Security	Access Control Lists	s > Rules > New			< Back	Apply
ARA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Sequence Source Destination Protocol	1 Any V IP Address V	IP Address 172.16.1.1	Netmask 255.255.255.255		
Access Control Lists	Source Port	DHCP Client				
Web Auth Certificate Wireless Protection Policies	Destination Port	DHCP Server				
Trusted AP Policies	DSCP	Any 💙				
Standard Signatures Custom Signatures	Direction	Inbound 👻				
Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	Action	Permit 💌				
Web Login Page						
CIDS Sensors Shunned Clients						
53	1					
				en manifesti anni fan ben b	🥥 Interr	WC.

Elija Permit para que ACL permita paquetes DHCP Si el origen o el destino no son **cualquiera**, se debe crear una sentencia inversa en la dirección opuesta. Aquí está un ejemplo.

G · 🕑 · 🛃 🛃	🚯 🔎 🛪 🥹 🖗	Address 🔬 🕺 Https:	//172.16.1.40/screens,fire 🎽 🄁 G	io Liniks Norton Ar	kilvirus 🚱 •	
Ance Station		COMPOUND WIDE COL		Save Config	juration Ping	Logout Refres
	MONITOR WEARS	CONTROLLER WIRELESS	SECORITY MEANAGEMENT	COMMANDS H		
Security	Access Control Lists	s > Rules > New			< Back	Apply
AAA General	Sequence	2	IP Address	Netmask		
RADIUS Authentication RADIUS Accounting	Source	IP Address 😪	172.16.1.1	255.255.255.255		
Local Net Users MAC Filtering	Destination	Any 🐱				
Disabled Clients User Login Policies	Protocol	UDP 💌				
Access Control Lists	Source Port	DHCP Server 💌				
Web Auth Certificate	Destination Port	DHCP Client				
Wireless Protection Policies Trusted AP Policies	DSCP	Any 🛩				
Rogue Policies Standard Signatures	Direction	Outbound 💌				
Custom Signatures Signature Events Summary	Action	Permit 💌				
Client Exclusion Policies AP Authentication / MFP Management Frame Protection						
Web Login Page						
CIDS Sensors Shunned Clients						
9					 Inte 	rmet

Origen o destino establecidos en Cualquiera

2. Para definir una regla que permita paquetes ICMP entre todos los dispositivos, seleccione any en los campos Source (Origen) y Destination (Destino). Este es el valor predeterminado.Elija ICMP en el campo desplegable Protocol . Dado que en este ejemplo se utiliza any para los campos Source y Destination, no es necesario especificar la dirección. Se puede dejar con el valor predeterminado de any. Además, no se requiere la instrucción inversa en la dirección opuesta.En el menú desplegable Action, elija Permit para que esta ACL permita paquetes DHCP del servidor DHCP al cliente inalámbrico. Haga clic en Apply (Aplicar).

G · O · E	6 P * 0	Address 🔬 http	s://172.16.1.40/so	eens,lfre 🖌 🄁 Go	Links No	ton AnkiWrus 🧕 -	🥂 – ē ×
Cinca Statian					Save	Configuration Ping	Logout Refresh
the standard and a	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Access Control List	s > Rules > New				< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies	Sequence Source Destination Protocol	3 Any X Any X ICMP					
AP Policies Access Control Lists	DSCP	Any 👻					
Web Auth Certificate	Direction	Any 👻					
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custem Signatures	Action	Fermit					
Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection							
Web Login Page							
CDS Sensors Shunned Clients							
🛃 Done			100000000000000000000000000000000000000			🔵 Ind	ernet

Permitir que ACL haga que permitan paquetes DHCP del servidor DHCP al cliente inalámbrico

 De manera similar, cree reglas que permitan el acceso del servidor DNS a todos los clientes inalámbricos y el acceso del servidor Telnet para el cliente inalámbrico a una subred específica. Estos son los ejemplos.

G · O · 🗷 🖻	6 P 🛠 🛛	😞 • 👌 🕺 Address 🔬 https:	//172.16.1.40/screens/fre 🎽 🔂 Go	Links No	rton AnkliVirus 😣 🔹	
alle alle	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS	HELP	Logout Keire:
Security	Access Control List	s > Rules > New			< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering	Sequence Source Destination	3 Any X Any X				
Disabled Clients User Login Policies AP Policies	Protocol	ICMP 💌				
Access Control Lists	DSCP	Any 💌				
Web Auth Certificate	Direction	Any 💌				
Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Summary Client Exclusion Policies AP Authentication / MFP Management Frame	Action	Permit				
Protection Web Login Dage						
CIDS Sensors Shunned Clients						
Done				100 P 1	int.	ernet
Crear reglas que pei	rmitan el acceso o	el servidor DNS a todo.	s los clientes inalámbri	cos		
	AAA	A 1 H		39		<u>a</u> - 8

Cinca Station				Save Confi	guration Ping	Logout Refresh
de de	MONITOR WLANS	CONTROLLER WIRELES	S SECURITY MANAGEMEN	IT COMMANDS H	ELP	en staar, en lie daarsteer, e
Security	Access Control Lis	ts > Rules > New			< Back	Apply
ARA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Sequence Source Destination Protocol	4 Any V IP Address V UDP V	IP Address 172.16.1.1	Netmask 255.255.255.255		
Access Control Lists	Source Port	Any 👻				
Web Auth Certificate Wireless Protection Policies Trusted AP Policies Standard Signatures Custom Signatures Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection Web Login Page CIDS Sensors Shunned Clients	Destination Port DSCP Direction Action	DNS V Any V Inbound V Permit V				
67.7752.6777.7777.7777 61					a Inte	errvet

Crear reglas que permitan el acceso del servidor Telnet para el cliente inalámbrico a una subred Defina esta regla

para permitir el acceso del cliente inalámbrico al servicio

Telnet.



Permitir el acceso del cliente inalámbrico al servicio Telnet

🕝 · 🕑 · 🖹 📓	6 × × 8	🍰 • 🍓 🎽 Address 🕘 Ht	tps://172.16.1.40/screens,fre 💌	🔁 Go Links ** Norton A	intilleus 😵 • 🛛 🦓 – 8 ×
Cinca Stattan	ana	and the second	Mensionarching	Save Conf	iguration Ping Logout Refresh
A. A. Brandstein	MONITOR WLANS	CONTROLLER WIRELE	SS SECURITY MANAGE	MENT COMMANDS H	εD
Security	Access Control List	s > Rules > New			< Back Apply
AAA General RADIUS Authentication RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Access Control Lists Web Auth Certificate	Sequence Source Destination Protocol Source Port Destination Port	6 Any V IP Address V TCP V Any V	IP Address 172.18.0.0	Netmask 255.255.0.0	
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame	DSCP Direction Action	Any V Inbound V Permit V			
Web Login Page					
CIDS Sensors Shunned Clients					
https://172.16.1.40/screens/b	anner.html#				🔮 Internet

Otro ejemplo de acceso de cliente inalámbrico al servicio Telnet La página ACL > Edit muestra todas las reglas que se definen para la

ACL.

curity	Acce	ss Contro	ol Lists > Edit						< Back		Add New	Rule
AAA General RADIUS Authentication RADIUS Accounting Local Net Users	Gene	ral										
	Access List Name Guest-ACL				_							
MAC Filtering	Seq	Action	Source IP/Mas	ik	IP/Mask		Protocol	Port	Port	DSCP	Direction	
User Login Policies AP Policies	1	Permit	0.0.0.0	/	172.16.1.1 255.255.255.255	<i>'</i>	UDP	DHCP Client	DHCP Server	Any	Inbound	Edit Remove
Access Control Lists Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events	2	Permit	172.16.1.1 255.255.255.255	1	0.0.0	1	UDP	DHCP Server	DHCP Client	Any	Outbound	Edit Remove
	э	Permit	0.0.0.0	/	0.0.0	1	ICMP	Any	Any	Any	Any	Edit Remove
	4	Permit	0.0.0.0	/	172.16.1.1 255.255.255.255	1	UDP	Any	DNS	Any	Inbound	Edit Remove
	5	Permit	172.16.1.1 255.255.255.255	/	0.0.0.0	/	UDP	DNS	Any	Any	Outbound	Edit Remove
Client Exclusion Policies IP Authentication / MFP	6	Permit	0.0.0.0	/	172.18.0.0 255.255.0.0	/	TCP	Any	Teinet	Any	Inbound	Edit Remove
tanagement Frame Protection	7	Permit	172.18.0.0 255.255.0.0	1	0.0.0.0	1	TCP	Teinet	Any	Any	Outbound	Edit Remove
DS ensors hunned Clients												

Página Editar Muestra todas las Reglas Definidas para la ACL

- 4. Una vez creada la ACL, debe aplicarse a una interfaz dinámica. Para aplicar la ACL, elija **Controller > Interfaces** y edite la interfaz a la que desea aplicar la ACL.
- 5. En la página Interfaces > Edit para la interfaz dinámica, elija la ACL apropiada del menú desplegable Access Control Lists . Aquí está un ejemplo.

3 · 0 · 2	🕼 🔎 🛧 🚱 🙆 🎍	Address 1/172.16.1.40/so	reens,lfre 🛩 🛃 Go	Links Norb	on AntiVirus 😡 🔹	🦓 – 8 ×
Cases Statems				Save C	onfiguration Ping	Logout Refresh
A. A.	MONITOR WLANS CONTR	OLLER WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	
Controller	Interfaces > Edit				< Back	Apply
General Inventory	General Information					
Interfaces	Interface Name G	uest				
Internal DHCP Server Mobility Management	Interface Address					
Mobility Groups Mobility Statistics	VLAN Identifier	1				
Ports	IP Address	172.19.1.10				
Master Controller Mode	Netmask	255.255.0.0				
Network Time Protocol	Gateway	172.19.1.50				
etwork Time Protocol oS Profiles	Physical Information					
	Port Number	1				
	Configuration					
	Quarantine					
aster Controller Mode etwork Time Protocol oS Profiles	DHCP Information					
	Primary DHCP Server	172.16.1.1				
	Secondary DHCP Server					
	Access Control List					
	ACL Name	Guest-ACL V				
	Note: Changing the Interface pa temporarily disabled and thus m some clients.	rameters causes the WLANs to be ay result in loss of connectivity for				
0				00000101	🎱 Int	ernet

Elija la ACL adecuada del menú Lista de control de acceso

Una vez hecho esto, la ACL permite y deniega el tráfico (según las reglas configuradas) en la WLAN que utiliza esta interfaz dinámica. Interface-ACL sólo se puede aplicar a AP de H-Reap en el modo conectado pero no en el modo autónomo.

Nota: Este documento asume que las WLANs y las interfaces dinámicas están configuradas. Consulte <u>Configuración de VLAN en Controladores de LAN Inalámbricos</u> o información sobre cómo crear interfaces dinámicas en WLC.

Configuración de ACL de CPU

Anteriormente, las ACL en los WLC no tenían una opción para filtrar el tráfico de datos LWAPP/CAPWAP, el tráfico de control LWAPP/CAPWAP y el tráfico de movilidad destinados a las interfaces de administración y administrador de AP. Para abordar este problema y filtrar el LWAPP y el tráfico de la movilidad, las ACL de la CPU fueron introducidas con la versión 4.0 del firmware del WLC.

La configuración de las ACL de CPU implica dos pasos:

- 1. Configure reglas para la ACL de CPU.
- 2. Aplique la ACL de la CPU en el WLC.

Las reglas para la ACL de CPU deben configurarse de manera similar a las otras ACL.

Verificación

Cisco recomienda que pruebe las configuraciones ACL con un cliente inalámbrico para asegurarse de que las ha configurado correctamente. Si no funcionan correctamente, verifique las ACL en la página web de ACL y verifique que los cambios de ACL se aplicaron a la interfaz del controlador.

También puede utilizar estos comandos show para verificar su configuración:

• **show acl summary**: para mostrar las ACL configuradas en el controlador, utilice el comando **show acl summary**. Aquí tiene un ejemplo:

(Cisco Controller) >show acl summary

ACL	Name	Applied
Gues	st-ACL	Yes

 show acl detailedACL_Name: muestra información detallada sobre las ACL configuradas.Aquí tiene un ejemplo:

(Cisco Controller) >show acl detailed Guest-ACL

	Source	Destination	Source Port		
Dest Por	t				
I Dir	IP Address/Netmask	IP Address/Netmask	Prot	Range	
Range	DSCP Action				
1 In	0.0.0/0.0.0.0	172.16.1.1/255.255.255.255	17	68-68	
67-67	Any Permit				
2 Out	172.16.1.1/255.255.255.255	0.0.0/0.0.0.0	17	67-67	
68-68	Any Permit				
3 Any	0.0.0/0.0.0.0	0.0.0/0.0.0.0	1	0-65535	
0-65535	Any Permit				
4 In	0.0.0/0.0.0.0	172.16.1.1/255.255.255.255	17	0-65535	
53-53	Any Permit				
5 Out	172.16.1.1/255.255.255.255	0.0.0/0.0.0.0	17	53-53	
0-65535	Any Permit				
6 In	0.0.0/0.0.0.0	172.18.0.0/255.255.0.0		60-65535	
23-23	Any Permit				
7 Out	172.18.0.0/255.255.0.0	0.0.0/0.0.0.0	6	23-23	
0-65535	Anv Permit				

• **show acl cpu**: para visualizar las ACL configuradas en la CPU, utilice el comando **show acl cpu**. Aquí tiene un ejemplo:

(Cisco Controller) >show acl cpu

CPU Acl Name..... CPU-ACL Wireless Traffic..... Enabled Wired Traffic..... Enabled

Troubleshoot

La versión 4.2.x o posterior del software del controlador le permite configurar los contadores de ACL. Los contadores de ACL pueden ayudar a determinar qué ACL se aplicaron a los paquetes transmitidos a través del controlador. Esta función es útil para solucionar problemas del sistema.

Los contadores de ACL están disponibles en estos controladores:

• Serie 4400

- WiSM de Cisco
- Switch de controlador de LAN inalámbrica integrado Catalyst 3750G

Para habilitar esta función, complete estos pasos:

- 1. Elija Security > Access Control Lists > Access Control Lists para abrir la página Access Control Lists.Esta página enumera todas las ACL que se han configurado para este controlador.
- 2. Para ver si los paquetes alcanzan alguna de las ACL configuradas en su controlador, marque la casilla de verificación **Enable Counters** y haga clic en **Apply**. De lo contrario, deje la casilla de verificación sin marcar. Este es el valor predeterminado.
- 3. Si desea borrar los contadores para una ACL, pase el cursor sobre la flecha desplegable azul para esa ACL y elija **Clear Counters** .

Información Relacionada

- Guía de configuración de controlador de LAN inalámbrica de Cisco, versión 6.0
- <u>Configuración de VLAN en controladores de LAN inalámbrica</u>
- Solucione problemas de un AP ligero que no puede unirse a un WLC
- Asistencia técnica y descargas de Cisco

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).