

# ACL en el ejemplo de la configuración de controlador del Wireless LAN

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[ACL en el WLCs](#)

[Consideraciones al configurar los ACL en el WLCs](#)

[Configuración ACL en el WLCs](#)

[Reglas de la configuración que permiten los servicios del Usuario invitado](#)

[Configuración CPU ACL](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

## Introducción

Este documento explica cómo configurar el Listas de control de acceso (ACL) en el filtrar tráfico de los reguladores del Wireless LAN (WLCs) para que ingresa y sale de un WLAN.

## prerrequisitos

### Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el WLC y el Lightweight Access Point (REVESTIMIENTO) para la operación básica
- Conocimiento básico de los métodos del protocolo (LWAPP) y de la seguridad de red inalámbrica del Lightweight Access Point

### Componentes Utilizados

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

- WLC de las Cisco 2000 Series que funciona con el firmware 4.0

- REVESTIMIENTO de las Cisco 1000 Series
- Adaptador de red inalámbrica de cliente de Cisco 802.11a/b/g que funciona con el firmware 2.6
- Versión 2.6 de la utilidad de escritorio del Cisco Aironet (ADU)

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

## ACL en el WLCs

Los ACL en el WLC se significan para restringir o para permitir a los clientes de red inalámbrica a los servicios en su red inalámbrica (WLAN).

Antes de la versión de firmware 4.0 del WLC, los ACL se desvían en la interfaz de administración, así que usted no puede afectar al tráfico destinado al WLC con excepción de evitar que los clientes de red inalámbrica manejen el regulador con la **Administración vía la opción inalámbrica**. Por lo tanto, los ACL se pueden aplicar solamente a las interfaces dinámicas. En la versión de firmware 4.0 del WLC, hay el CPU ACL que puede filtrar tráfico destinado para la interfaz de administración. Un ejemplo de cómo [configurar CPU ACL](#) se proporciona más adelante en este documento.

Usted puede definir hasta 64 ACL, cada uno con hasta 64 reglas (o los filtros). Cada regla tiene parámetros que afectan a su acción. Cuando un paquete hace juego todos los parámetros para una regla, la acción fijada para esa regla se aplica al paquete. Usted puede configurar los ACL con el GUI o el CLI.

Éstos son algunas de las reglas que usted necesita entender antes de que usted configure un ACL en el WLC:

- Si la fuente y el destino son **ninguna**, la dirección en la cual este ACL es aplicado puede ser **ninguna**.
- Si la fuente o el destino no es **ninguna**, después la dirección del filtro debe ser especificada, y una declaración inversa en la dirección opuesta debe ser creada.
- La noción WLC de entrante contra saliente es nonintuitive. Está desde la perspectiva del WLC que hace frente hacia el cliente de red inalámbrica, bastante que desde la perspectiva del cliente. Así pues, la dirección entrante significa que un paquete que entra en el WLC del cliente de red inalámbrica y de la dirección saliente significa un paquete ese las salidas del WLC hacia el cliente de red inalámbrica.
- Hay un implícito niega en el final del ACL.

## Consideraciones al configurar los ACL en el WLCs

Los ALC en el WLCs trabajan diferentemente que en el Routers. Éstas son algunas cosas a

recordar cuando usted configura los ACL en el WLCs:

- La mayoría del error común es seleccionar el IP cuando usted se propone negar o permitir los paquetes del IP. Porque usted selecciona cuál está dentro del paquete del IP, usted termina para arriba la negación o permitir de los paquetes del IP en IP.
- El regulador ACL no puede bloquear 1.1.1.1 (dirección IP virtual), y por lo tanto los paquetes DHCP para los clientes de red inalámbrica.
- El regulador ACL no puede bloquear el tráfico Multicast recibido de las redes alámbricas que se destina a los clientes de red inalámbrica. El regulador ACL se procesa para el tráfico Multicast iniciado de los clientes de red inalámbrica, destinados a las redes alámbricas o a otros clientes de red inalámbrica en el mismo regulador.
- A diferencia de un router, el ACL controla el tráfico en las ambas direcciones cuando está aplicado a una interfaz, pero no realiza el firewalling stateful. Si usted olvida abrir un agujero en el ACL para el tráfico de vuelta, éste causa un problema.
- El regulador ACL bloquea solamente los paquetes del IP. Usted no puede bloquear la capa 2 ACL o acodar 3 paquetes que no sean IP.
- El regulador ACL no utiliza las máscaras inversas como el Routers. Aquí, 255 significa la coincidencia ese octeto de la dirección IP exactamente.
- Los ACL en el regulador se hacen en el rendimiento de reenvío del software y del impacto.

**Nota:** Si usted aplica un ACL a una interfaz o a una red inalámbrica (WLAN), la producción inalámbrica se degrada y puede llevar a la pérdida potencial de paquetes. Para mejorar la producción, quitar el ACL de la interfaz o de la red inalámbrica (WLAN) y mover el ACL a un dispositivo atado con alambre vecino.

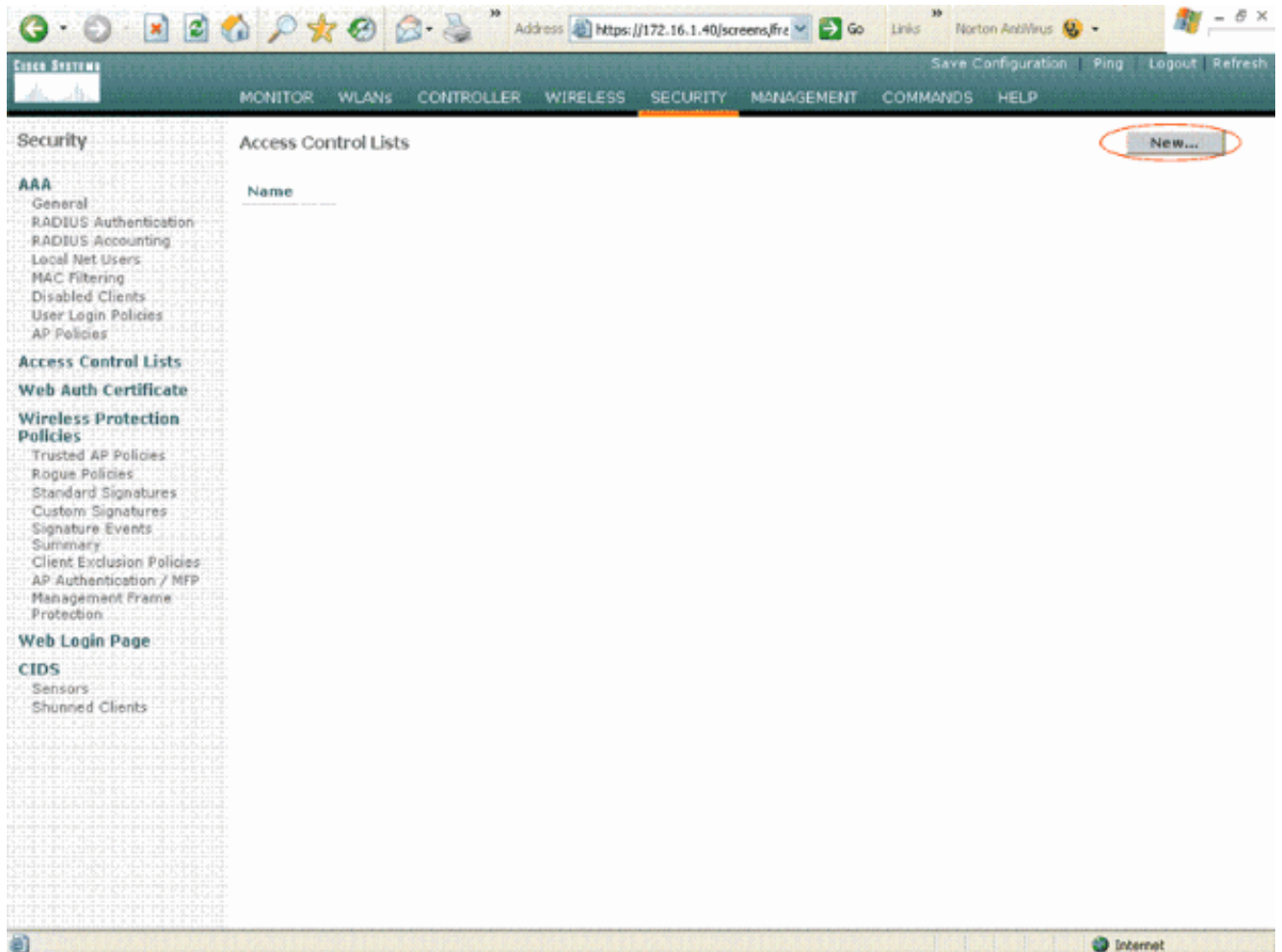
## Configuración ACL en el WLCs

Esta sección describe cómo configurar un ACL en el WLC. El objetivo es configurar un ACL que permita que los clientes del invitado accedan estos servicios:

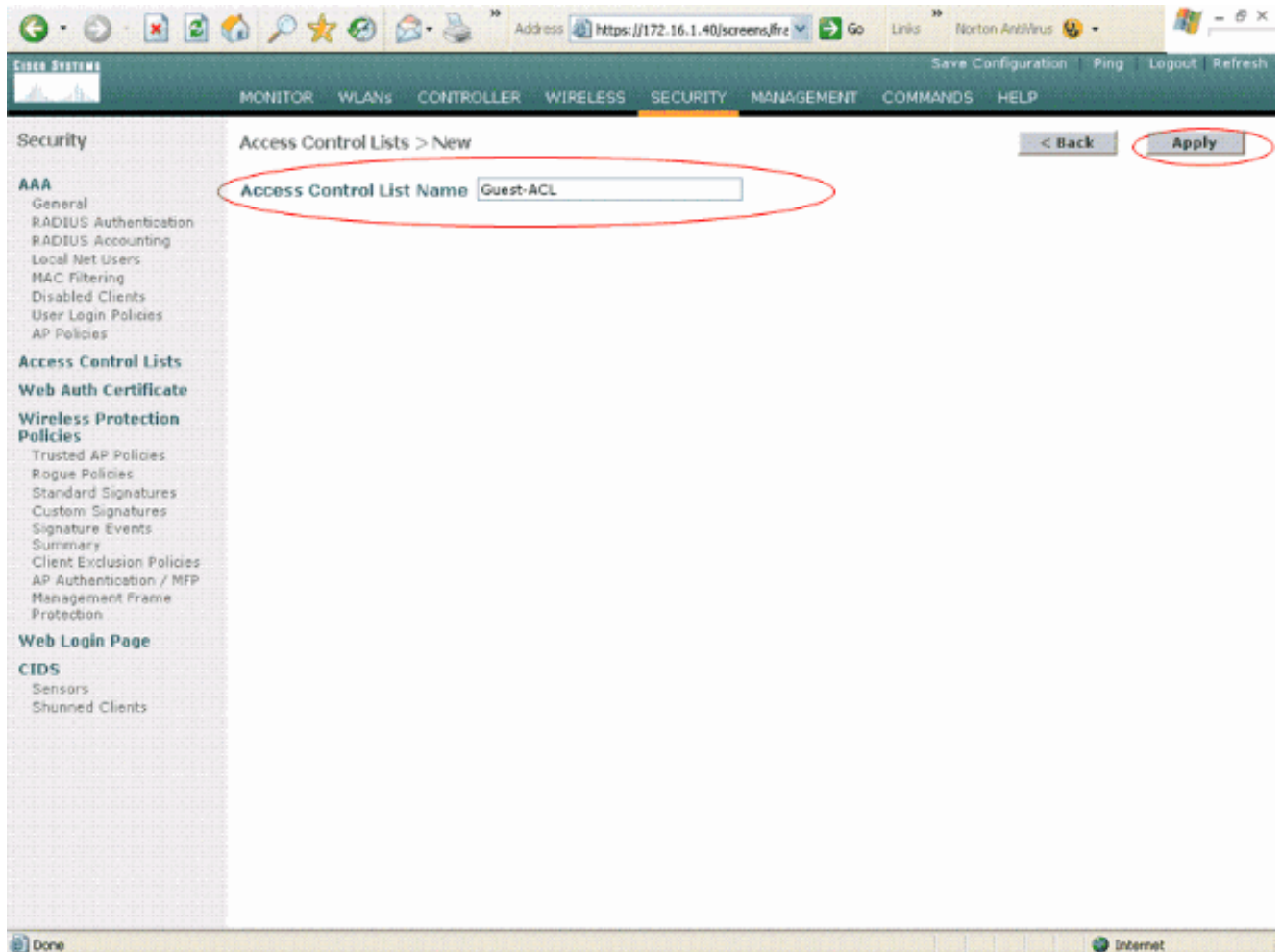
- Protocolo de configuración dinámica de host (DHCP) entre los clientes de red inalámbrica y el servidor DHCP
- Internet Control Message Protocol (ICMP) entre todos los dispositivos en la red
- Domain Name System (DNS) entre los clientes de red inalámbrica y el servidor DNS
- Telnet a una subred específica

Todos los otros servicios deben ser bloqueados para los clientes de red inalámbrica. Complete estos pasos para crear el ACL usando el WLC GUI:

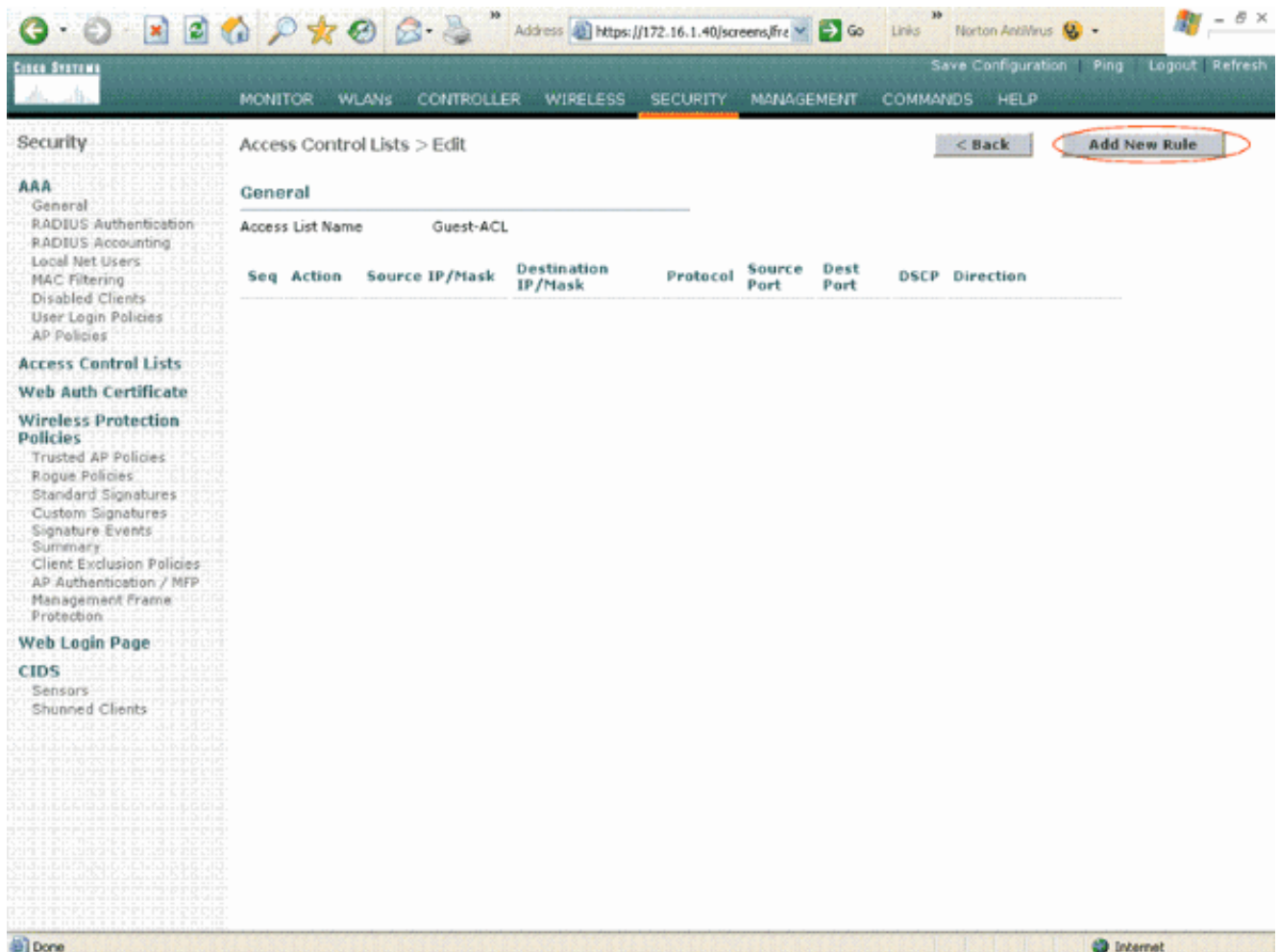
1. Vaya al WLC GUI y elija la **Seguridad > las listas de control de acceso**. La página de las listas de control de acceso aparece. Esta página enumera los ACL que se configuran en el WLC. También le permite para editar o para quitar los ACL uces de los. Para crear un nuevo ACL, haga clic **nuevo**.



2. Ingrese el nombre del ACL y del tecleo **se aplican**. Usted puede ingresar hasta 32 caracteres alfanuméricos. En este ejemplo, el nombre del ACL es Invitado-ACL. Una vez que se crea el ACL, el tecleo **edita** para crear las reglas para el ACL.



3. Cuando las listas de control de acceso > editan la página aparece, tecleo **agrega la nueva regla**. Las listas de control de acceso > gobiernan > nueva página aparecen.



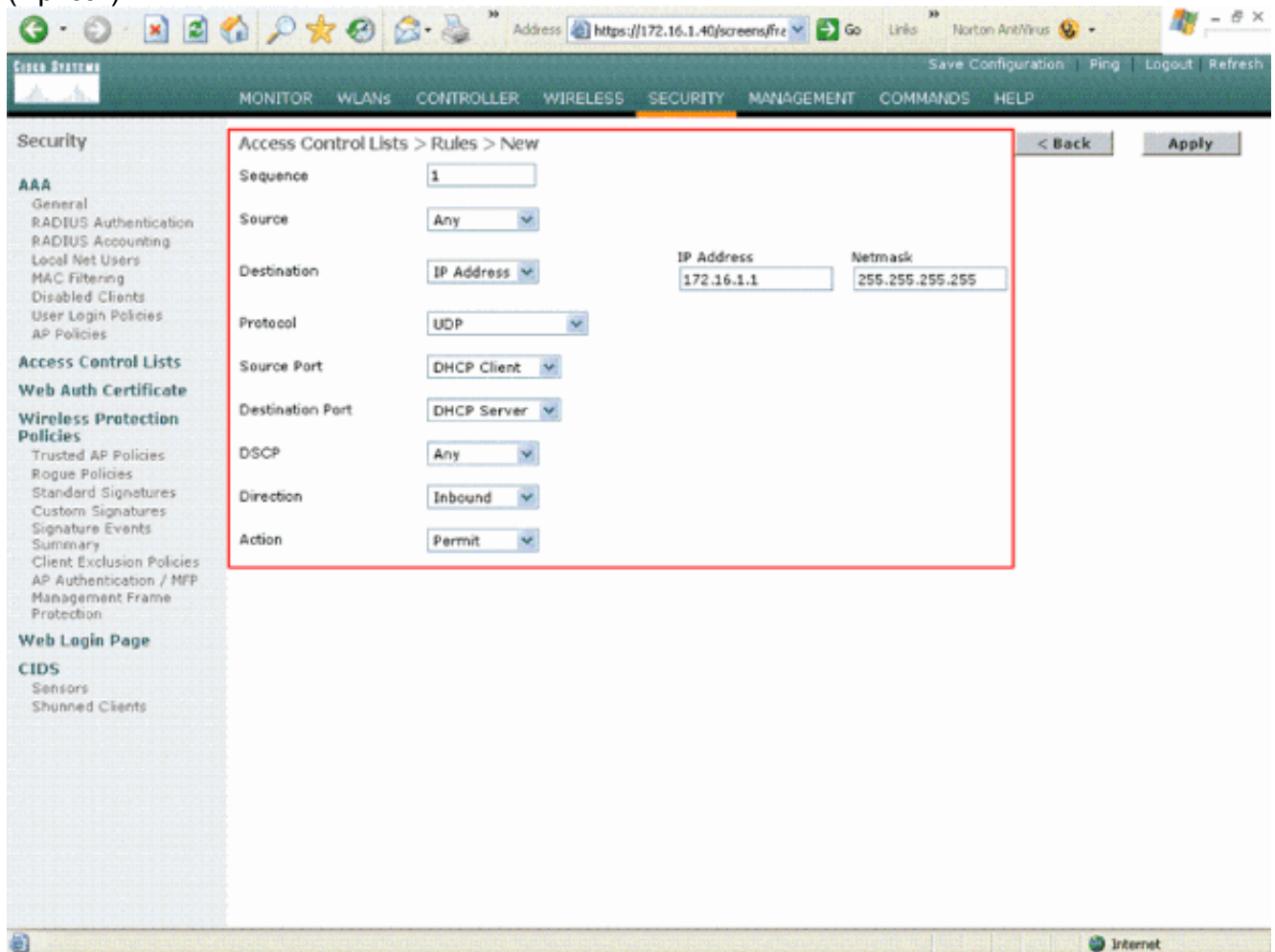
4. Configure las reglas que no prohíben a Usuario invitado estos servicios:DHCP entre los clientes de red inalámbrica y el servidor DHCPICMP entre todos los dispositivos en la redDNS entre los clientes de red inalámbrica y el servidor DNSTelnet a una subred específica

## [Reglas de la configuración que permiten los servicios del Usuario invitado](#)

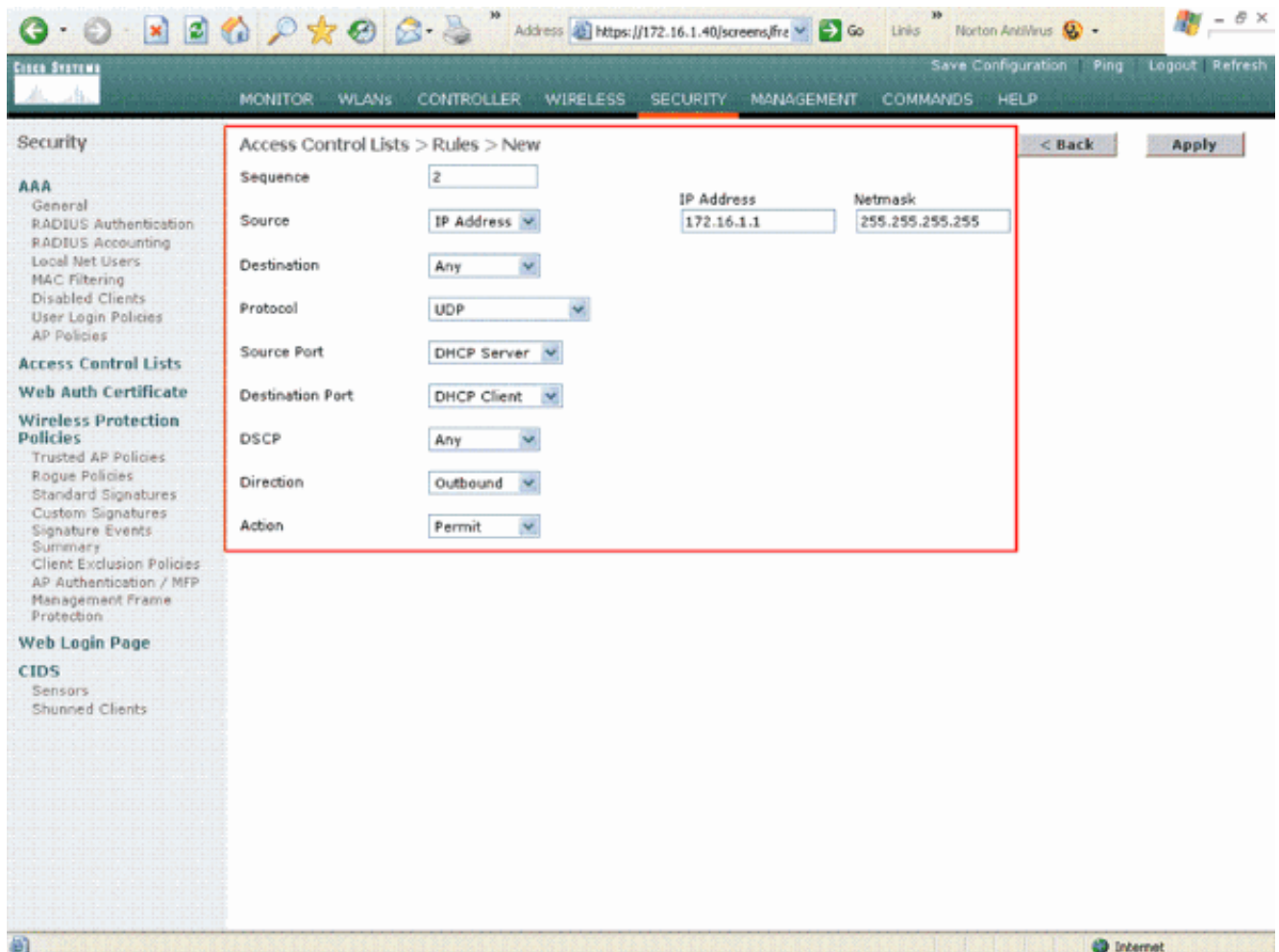
Esta sección muestra un ejemplo para que cómo configure las reglas para estos servicios:

- DHCP entre los clientes de red inalámbrica y el servidor DHCP
  - ICMP entre todos los dispositivos en la red
  - DNS entre los clientes de red inalámbrica y el servidor DNS
  - Telnet a una subred específica
1. Para definir la regla para el servicio del DHCP, seleccione la fuente y los rangos del IP de destino. Este ejemplo utiliza **ningunos** para la fuente que significa que no prohíben cualquier cliente de red inalámbrica el acceso al servidor DHCP. En este ejemplo, el servidor 172.16.1.1 actúa como el DHCP y el servidor DNS. Así pues, el IP Address de destino es 172.16.1.1/255.255.255.255 (con una máscara del host). Porque el DHCP es un protocolo basado en UDP, seleccione el **UDP** del campo del descenso-abajo del protocolo. Si usted eligió el TCP o el UDP en el paso anterior, dos parámetros adicionales aparecen: Puerto de origen y puerto destino. Especifique los detalles del puerto de origen y de destino. Para esta regla, el puerto de origen es **Cliente de DHCP** y el puerto destino es **servidor DHCP**. Elija la dirección en la cual el ACL debe ser aplicado. Porque esta regla es del cliente al servidor, las aplicaciones de este ejemplo **entrantes**. De la casilla desplegable de la acción, elija el

permiso de hacer este ACL permitir los paquetes DHCP del cliente de red inalámbrica al servidor DHCP. El valor predeterminado es niega. Haga clic en Apply (Aplicar).

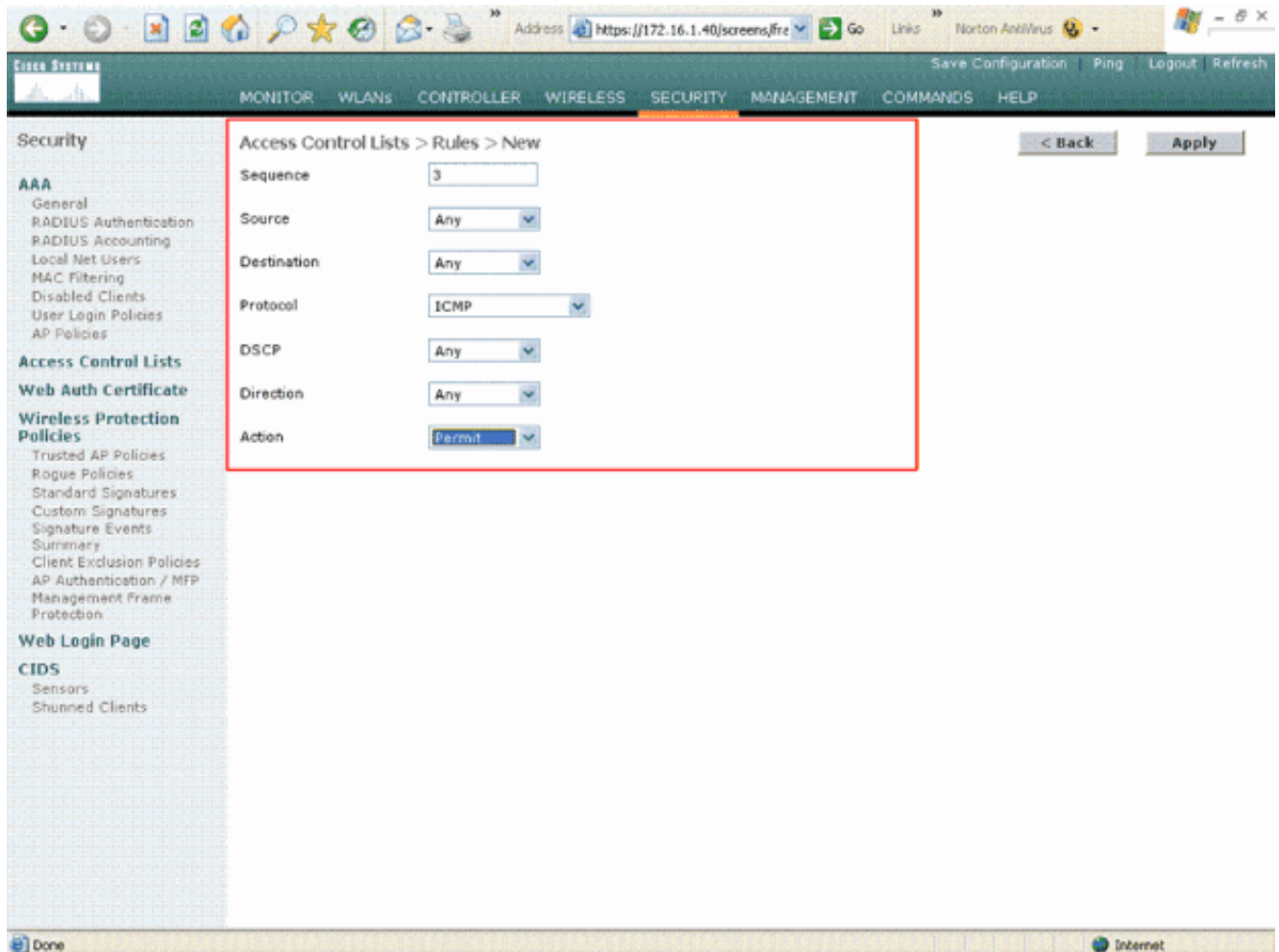


Si la fuente o el destino no es **ninguna**, después una declaración inversa en la dirección opuesta debe ser creada. Aquí está un ejemplo.



2. Para definir una regla que permita los paquetes icmp entre todos los dispositivos, seleccione **ningunos** para la fuente y los Campos Destination. Éste es el valor predeterminado. Elija el **ICMP del** campo del descenso-abajo del protocolo. Porque este ejemplo utiliza **ningunos** para la fuente y los Campos Destination, usted no tiene que especificar la dirección. Puede ser dejado en su valor predeterminado de **ningunos**. También, la declaración inversa en la dirección opuesta no se requiere. Del menú desplegable de la acción, elija el **permiso** para hacer este ACL permitir los paquetes DHCP del servidor DHCP al cliente de red inalámbrica. Haga clic en Apply (Aplicar).





3. Semejantemente, cree las reglas que permiten el acceso del servidor DNS a todos los clientes de red inalámbrica y el acceso del servidor Telnet para el cliente de red inalámbrica a una subred específica. Aquí están los ejemplos.

The screenshot shows the Cisco Systems configuration interface for a network device. The browser address bar displays <https://172.16.1.40/screens/fre>. The navigation menu includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar lists various configuration categories: Security, AAA, Access Control Lists, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area is titled "Access Control Lists > Rules > New" and contains the following configuration fields:

- Sequence: 4
- Source: Any
- Destination: IP Address (172.16.1.1) with Netmask (255.255.255.255)
- Protocol: UDP
- Source Port: Any
- Destination Port: DNS
- DSCP: Any
- Direction: Inbound
- Action: Permit

Buttons for "< Back" and "Apply" are visible at the top right of the configuration area.

The screenshot shows the Cisco Systems configuration interface for a network device. The browser address bar displays <https://172.16.1.40/screens/fre>. The navigation menu includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar lists various configuration categories: Security, AAA, Access Control Lists, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area is titled "Access Control Lists > Rules > New" and contains the following configuration fields:

- Sequence: 5
- Source: IP Address (172.16.1.1) with Netmask (255.255.255.255)
- Destination: Any
- Protocol: UDP
- Source Port: DNS
- Destination Port: Any
- DSCP: Any
- Direction: Outbound
- Action: Permit

Buttons for "< Back" and "Apply" are visible at the top right of the configuration area. The browser address bar at the bottom of the page shows <https://172.16.1.40/screens/banner.html#>.

Defina esta regla para permitir el acceso para el cliente de red inalámbrica al servicio de

# Telnet.

Access Control Lists > Rules > New

Sequence: 6

Source: Any

Destination: IP Address, IP Address: 172.18.0.0, Netmask: 255.255.0.0

Protocol: TCP

Source Port: Any

Destination Port: Telnet

DSCP: Any

Direction: Inbound

Action: Permit

< Back Apply

Access Control Lists > Rules > New

Sequence: 7

Source: IP Address, IP Address: 172.18.0.0, Netmask: 255.255.0.0

Destination: Any

Protocol: TCP

Source Port: Telnet

Destination Port: Any

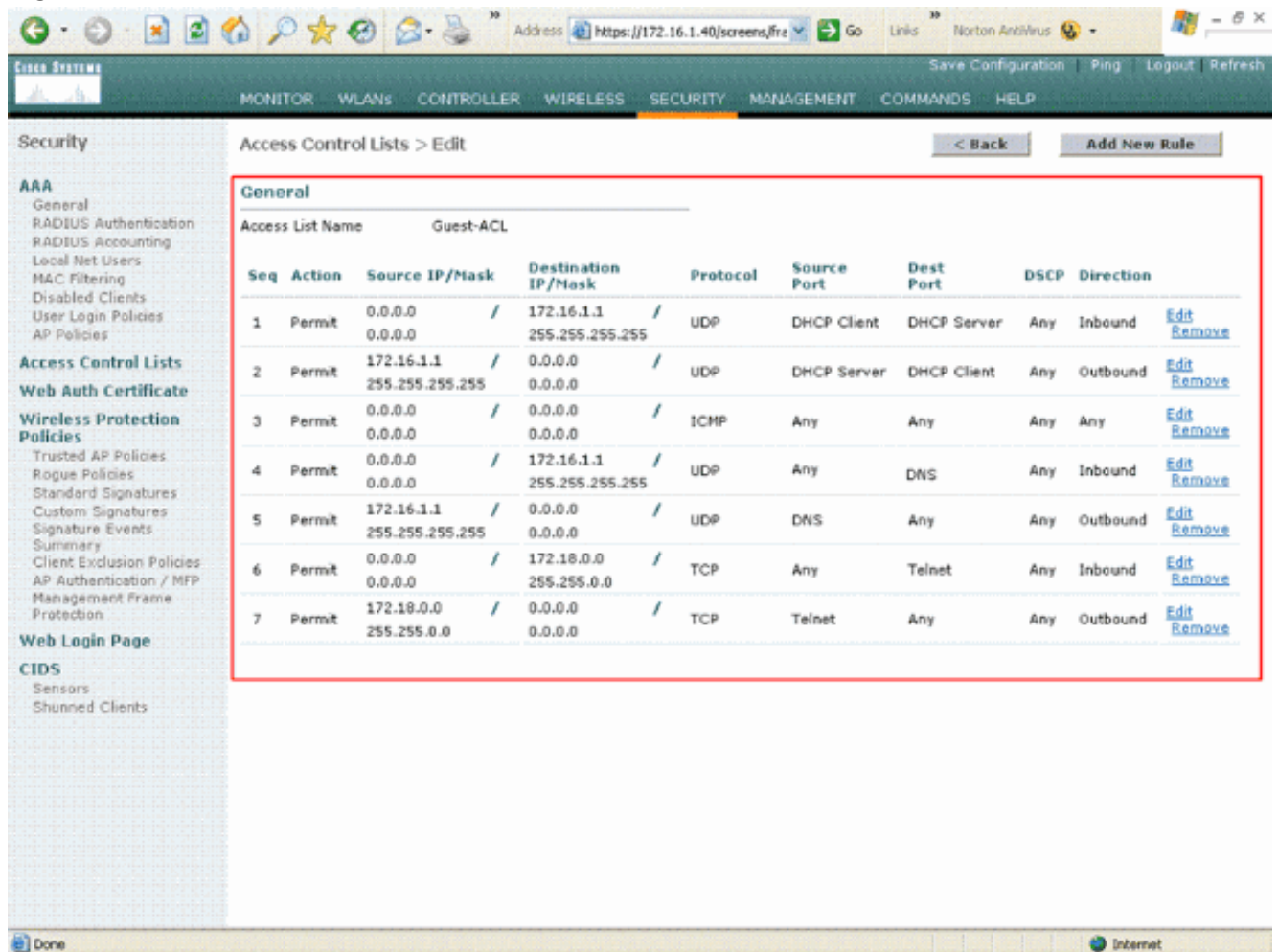
DSCP: Any

Direction: Outbound

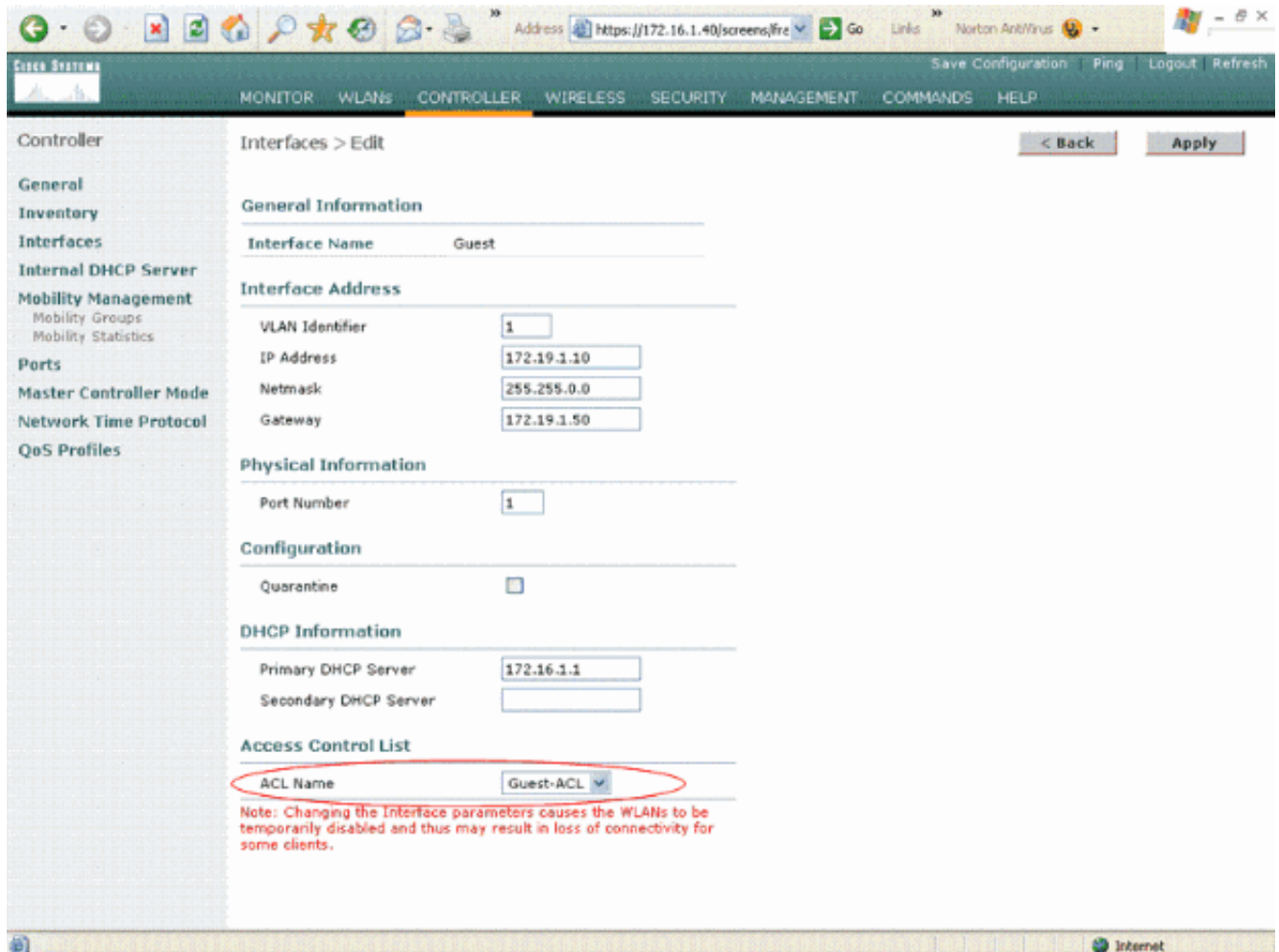
Action: Permit

< Back Apply

El ACL > edita la página enumera todas las reglas que se definen para el ACL.



- Una vez que se crea el ACL, necesita ser aplicado a una interfaz dinámica. Para aplicar el ACL, elegir el **regulador > las interfaces** y editar la interfaz a la cual usted quiere aplicar el ACL.
- En las **interfaces > edite la página** para la interfaz dinámica, eligen el ACL apropiado del menú desplegable de las listas de control de acceso. Aquí está un ejemplo.



Una vez que se hace esto, el ACL permite y niega el tráfico (basado en las reglas configuradas) en la red inalámbrica (WLAN) que utiliza esta interfaz dinámica. El Interfaz-ACL se puede aplicar solamente H-para cosechar los AP en el modo conectado pero no en el modo autónomo.

**Nota:** Refiérase [usando el CLI para configurar las listas de control de acceso](#) para la información sobre cómo crear un ACL con el CLI en el WLC.

**Nota:** Este documento asume que los WLAN y las interfaces dinámicas están configurados. Refiera a los [VLAN en el ejemplo de configuración de los reguladores del Wireless LAN](#) para la información sobre cómo crear las interfaces dinámicas en el WLCs.

## [Configure CPU ACL](#)

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

La configuración de CPU ACL implica dos pasos:

1. Reglas de la configuración para el CPU ACL.
2. Aplique el CPU ACL en el WLC.

Las reglas para el CPU ACL se deben configurar de una manera similar a los otros ACL. Refiera a la sección [CPU ACL de asegurar los reguladores del Wireless LAN \(WLCs\)](#) para más información sobre CPU ACL.

## Verificación

Cisco recomienda que usted prueba sus configuraciones ACL con un cliente de red inalámbrica para asegurarse de que usted las ha configurado correctamente. Si no pueden actuar correctamente, verifique los ACL en la página web ACL y verifíquelos que sus cambios ACL fueran aplicados a la interfaz del regulador.

Usted puede también utilizar estos **comandos show** para verificar su configuración:

- **muestre el resumen acl** — Para visualizar los ACL que se configuran en el regulador, utilice el **comando summary acl de la demostración**. Aquí tiene un ejemplo: (Cisco Controller) >show acl summary

```
ACL Name                               Applied
-----                               -
Guest-ACL                              Yes
```

- **muestre el acl\_name detallado acl** — Visualiza la información detallada en los ACL configurados. Aquí tiene un ejemplo: (Cisco Controller) >show acl detailed **Guest-ACL** Source Destination Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action -- -- ----- 1 In 0.0.0.0/0.0.0.0 172.16.1.1/255.255.255.255 17 68-68 67-67 Any Permit 2 Out 172.16.1.1/255.255.255.255 0.0.0.0/0.0.0.0 17 67-67 68-68 Any Permit 3 Any 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 1 0-65535 0-65535 Any Permit 4 In 0.0.0.0/0.0.0.0 172.16.1.1/255.255.255.255 17 0-65535 53-53 Any Permit 5 Out 172.16.1.1/255.255.255.255 0.0.0.0/0.0.0.0 17 53-53 0-65535 Any Permit 6 In 0.0.0.0/0.0.0.0 172.18.0.0/255.255.0.0 60-65535 23-23 Any Permit 7 Out 172.18.0.0/255.255.0.0 0.0.0.0/0.0.0.0 6 23-23 0-65535 Any Permit

- **muestre la CPU acl** — Para visualizar los ACL configurados en el CPU, utilice el **comando cpu acl de la demostración**. Aquí tiene un ejemplo: (Cisco Controller) >show acl cpu

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

## Troubleshooting

El Software Release 4.2.61.0 o Posterior del regulador le permite para configurar los contadores ACL. Los contadores ACL pueden ayudar a determinar qué ACL fueron aplicados a los paquetes transmitidos a través del regulador. Esta característica es útil cuando usted resuelve problemas su sistema.

Los contadores ACL están disponibles en estos reguladores:

- 4400 Series
- Cisco WiSM
- Switch integrado 3750G del regulador del Wireless LAN del Catalyst

Para habilitar esta característica, complete estos pasos:

1. Elija la **Seguridad > las listas de control de acceso > las listas de control de acceso** para abrir la página de las listas de control de acceso. Esta página enumera todos los ACL que se han configurado para este regulador.
2. Para ver si los paquetes están golpeando los ACL uces de los configurados en su regulador,

marque la casilla de verificación de los **contadores del permiso** y el tecleo **se aplica**. Si no, deje la casilla de verificación desmarcada. Éste es el valor predeterminado.

3. Si usted quiere borrar los contadores para un ACL, asoma su cursor sobre la flecha desplegable azul para ese ACL y elige los **contadores claros**.

## [Información Relacionada](#)

- [Configurando y aplicando las listas de control de acceso](#)
- [Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica](#)
- [Registro de AP Ligero \(LAP\) a un Controlador de LAN Inalámbrica \(WLC\)](#)
- [Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0](#)
- [Soporte de tecnología del Tecnología inalámbrica/Movilidad](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)