ACL en el ejemplo inalámbrico de la configuración del regulador LAN

Contenido

Introducción

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

Prerequisites

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el WLC y el Punto de acceso ligero (REVESTIMIENTO) para la operación básica
- Conocimiento básico de los métodos ligeros del protocolo (LWAPP) y de la seguridad de red inalámbrica del Punto de acceso

Componentes usados

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

- Cisco 2000 Series WLC que funciona con los firmwares 4.0

- REVESTIMIENTO de las Cisco 1000 Series
- Adaptador de red inalámbrica de cliente de Cisco 802.11a/b/g que funciona con los firmwares 2.6
- Versión 2.6 de Cisco utilidad Aironet Desktop (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 TécnicosCisco para obtener más información sobre las convenciones del documento.

ACL en 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 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 los interfaces dinámicos. En la versión de firmware 4.0 WLC, hay la 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 afecten 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 WLCs

ALCs en el trabajo de WLCs diferentemente que en el Routers. Éstas son algunas cosas a recordar cuando usted configura los ACL en WLCs:

- La mayoría del error común es seleccionar el IP cuando usted se prepone negar o permitir los paquetes IP. Porque usted selecciona cuál está dentro del paquete 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 del 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 ambas direcciones cuando está aplicado a un interfaz, pero no realiza 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 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.

Note: Si usted aplica un ACL a un 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 del interfaz o de la red inalámbrica (WLAN) y mover el ACL a un dispositivo atado con alambre vecino.

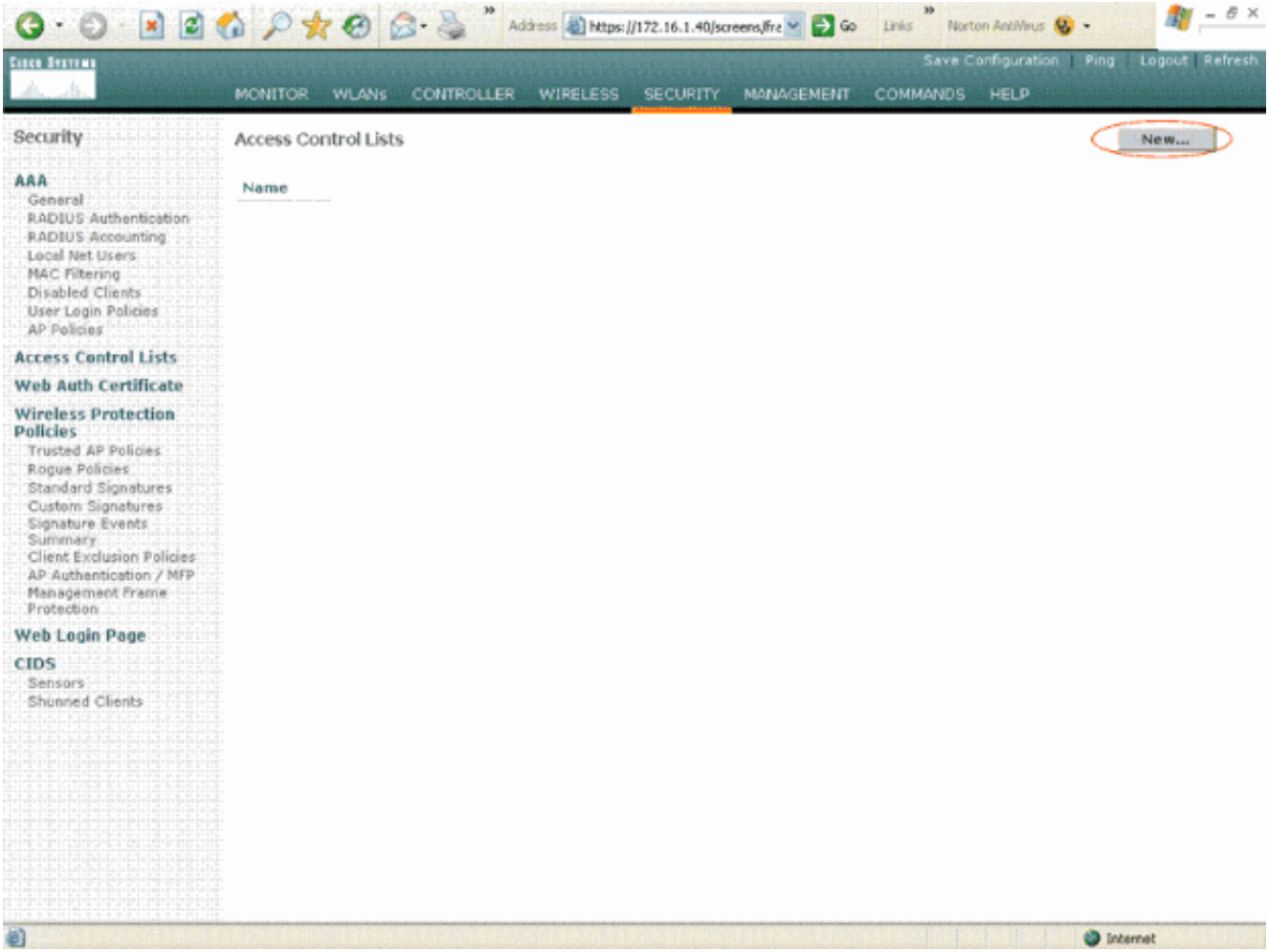
Configure el ACL en WLCs

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

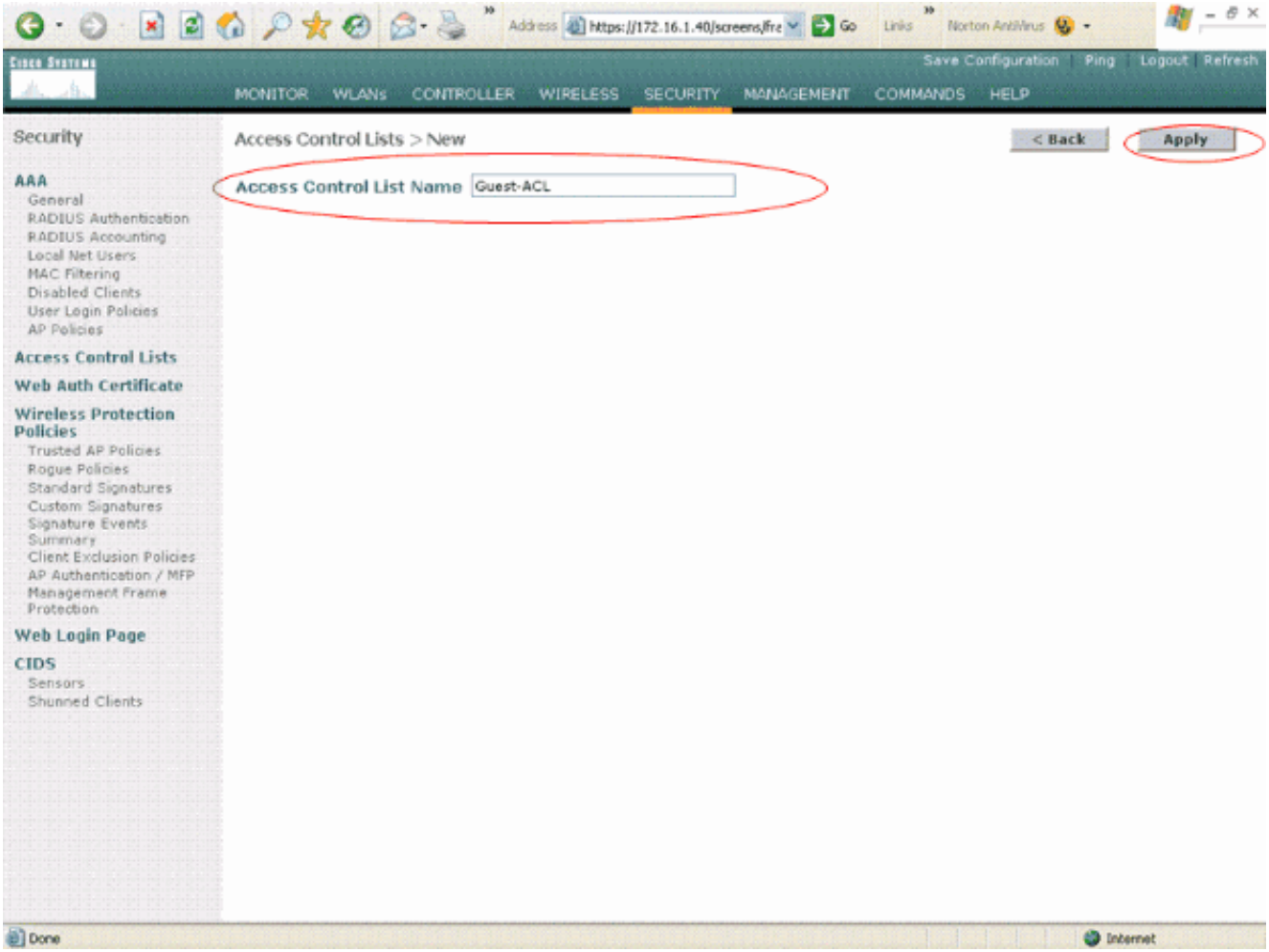
- Protocolo de configuración dinámica de host (DHCP) entre los clientes de red inalámbrica y el servidor del DHCP
- Internet Control Message Protocol (ICMP) entre todos los dispositivos en la red
- Domain Name System (DNS) entre los clientes de red inalámbrica y el servidor DNS
- Telnet a una subred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

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

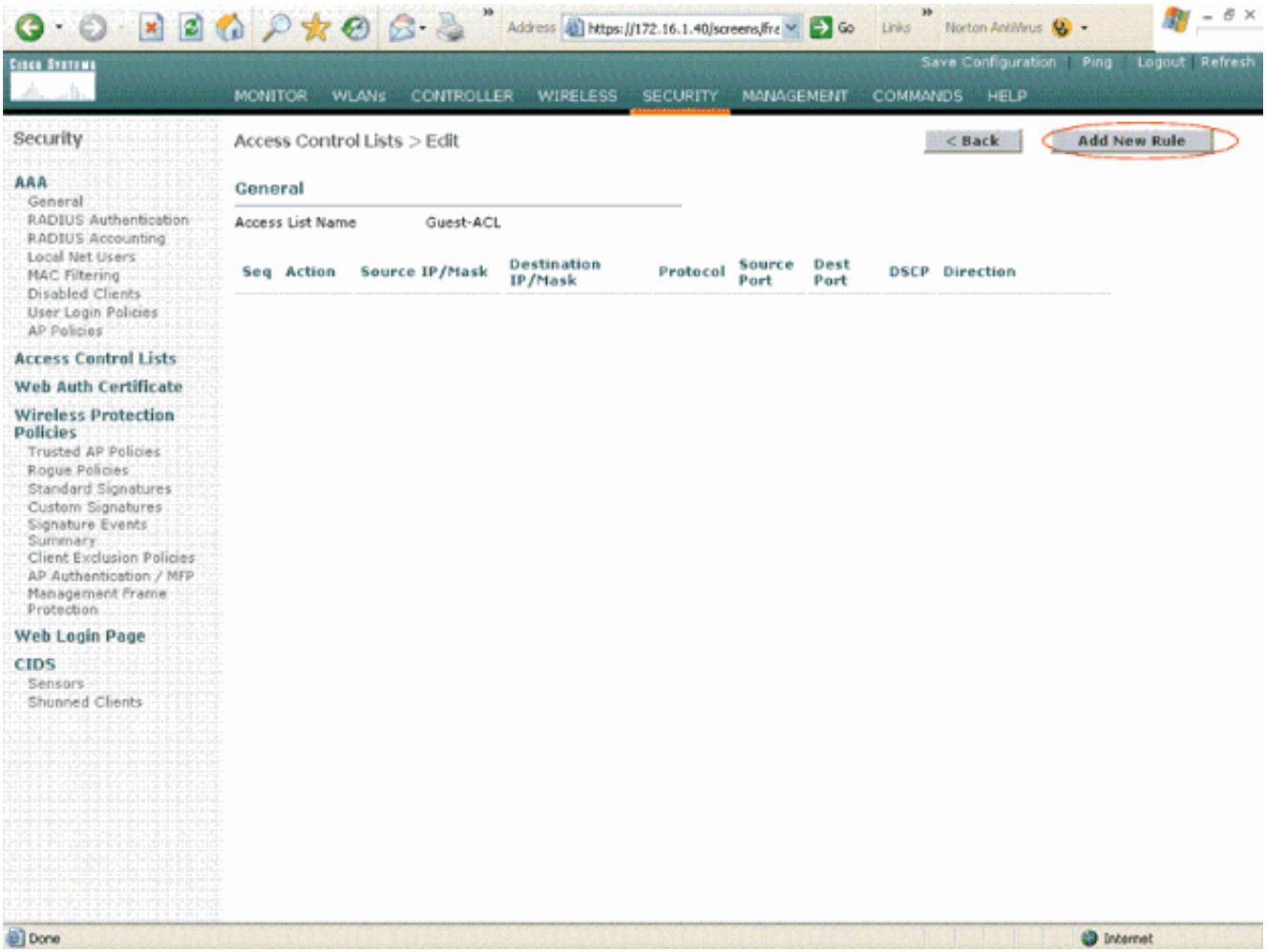
1. Vaya al GUI WLC y elija la **Seguridad > las listas de control de acceso**.La página de las listas de control de acceso aparece. Esta página enumera los ACL que se configuran en el WLC. También le permite corregir o quitar los ACL uces de los. Para crear un nuevo ACL, haga clic
   nuevo.



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 **corrige** para crear las reglas para el
ACL.



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



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

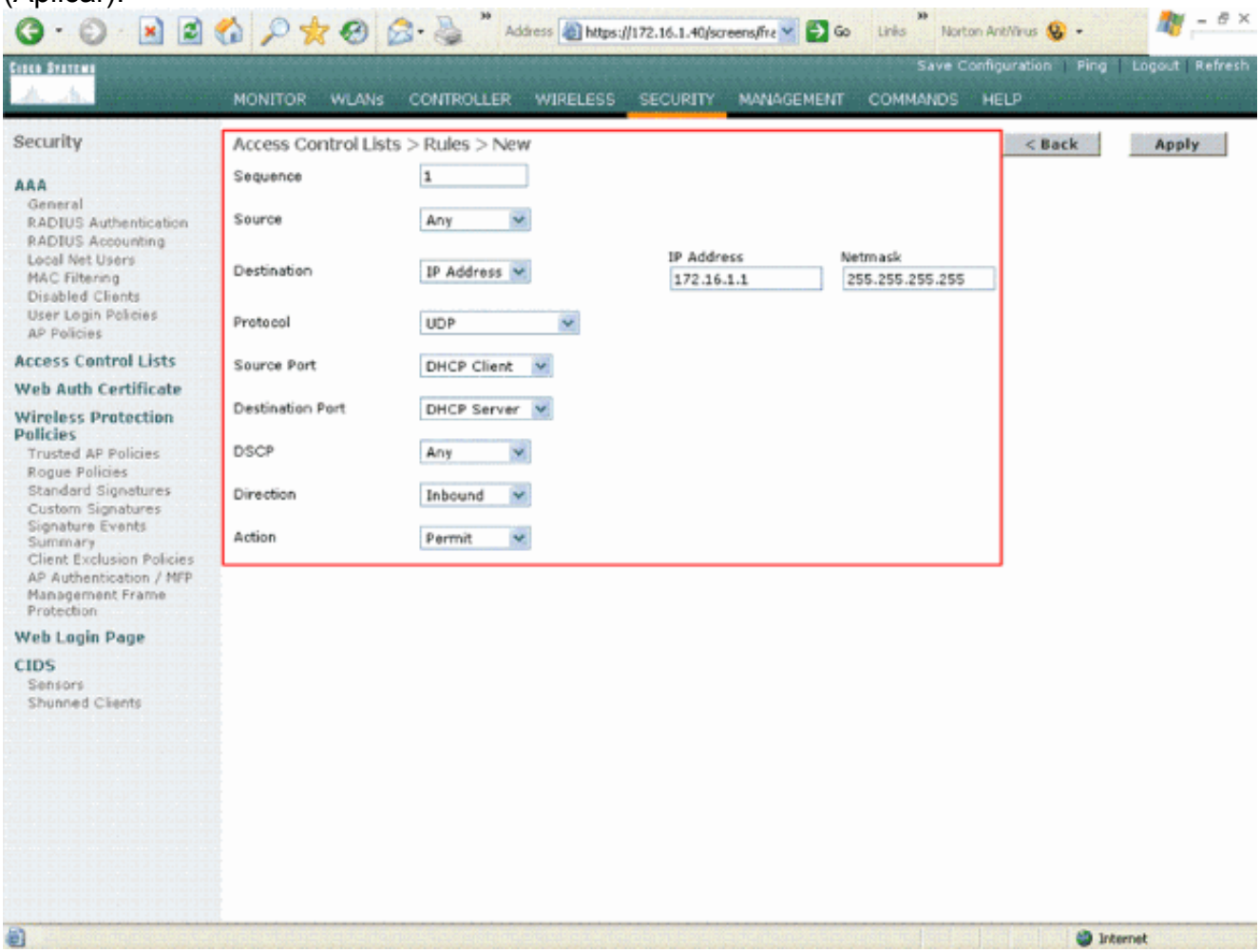
Configure las reglas que permiten los servicios del Usuario invitado

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

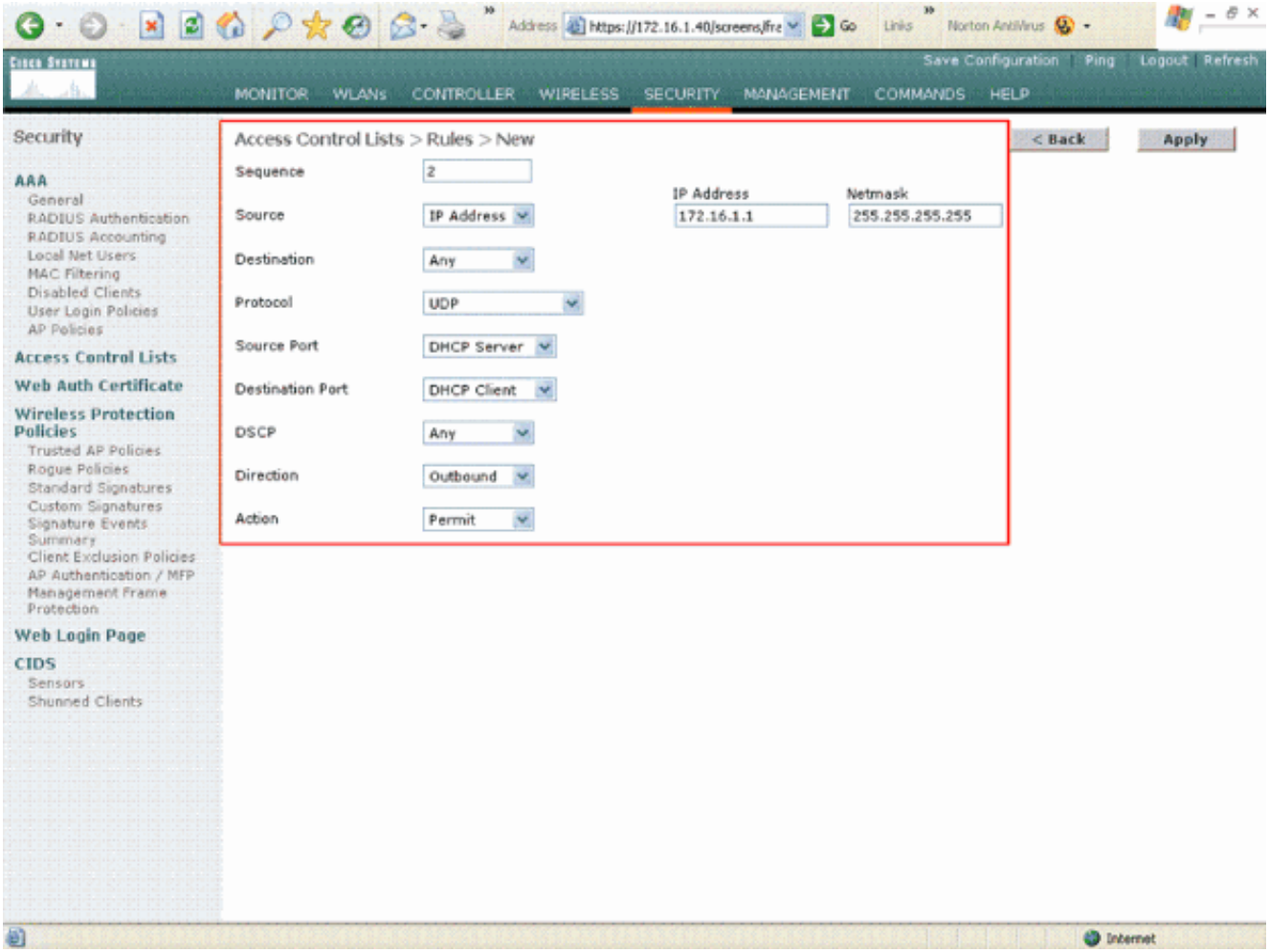
- DHCP entre los clientes de red inalámbrica y el servidor del DHCP
- ICMP entre todos los dispositivos en la red
- DNS entre los clientes de red inalámbrica y el servidor DNS
- Telnet a una subred específica

1. Para definir la regla para el servicio del DHCP, seleccione la fuente y los intervalos de direcciones IP del destino.Este ejemplo utiliza **ningunos** para la fuente que significa que no prohiben cualquier cliente de red inalámbrica el acceso al servidor del DHCP. En este ejemplo, el servidor 172.16.1.1 actúa como el servidor del DHCP y DNS. Así pues, la dirección IP del 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 del puerto de origen y de 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 de destino es **servidor del 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

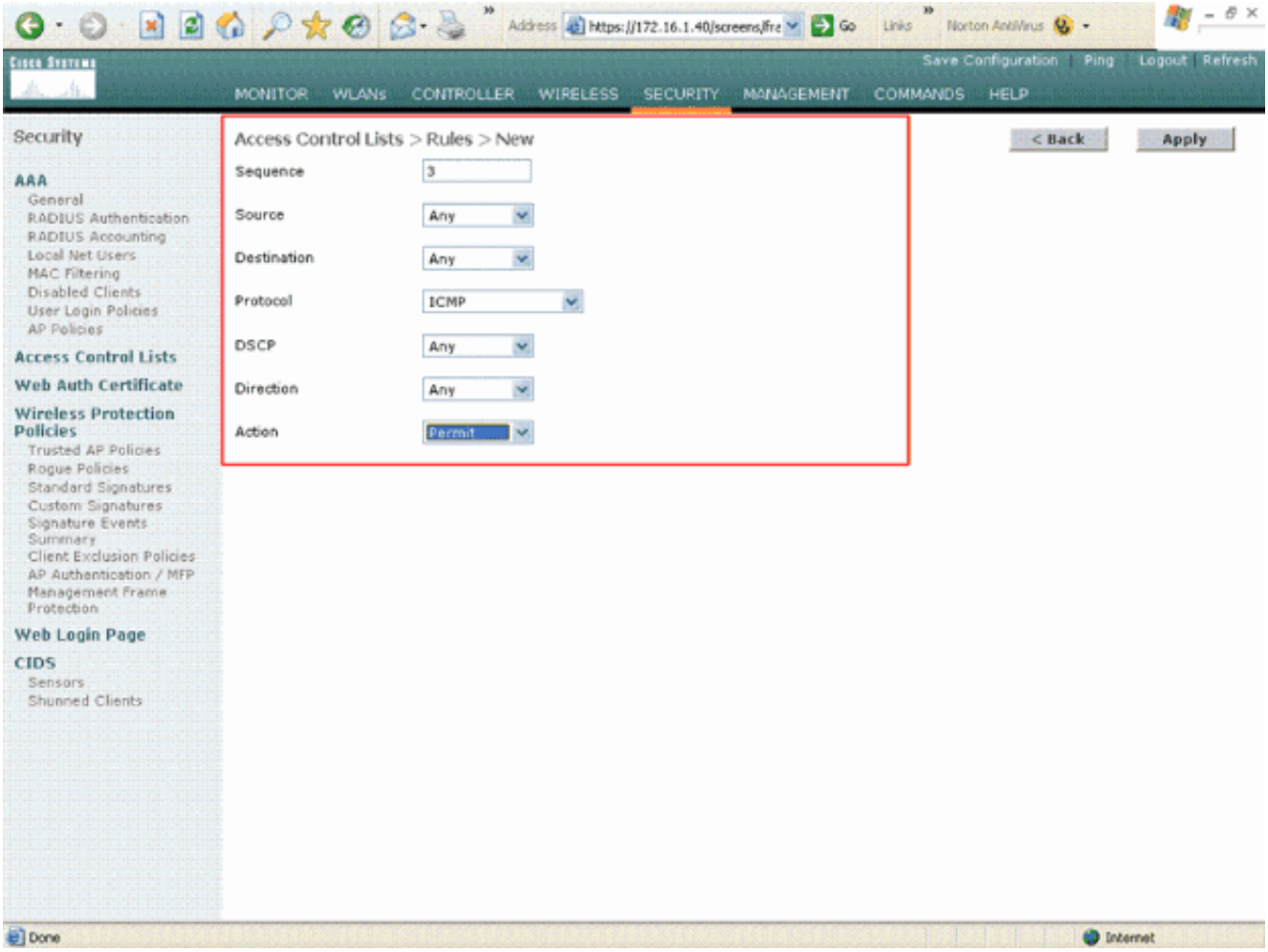
entrantes. De la casilla desplegable de la acción, elija el **permiso** de hacer este ACL permitir los paquetes del DHCP del cliente de red inalámbrica al servidor del DHCP. El valor predeterminado es niega. Haga clic en Apply
(Aplicar).



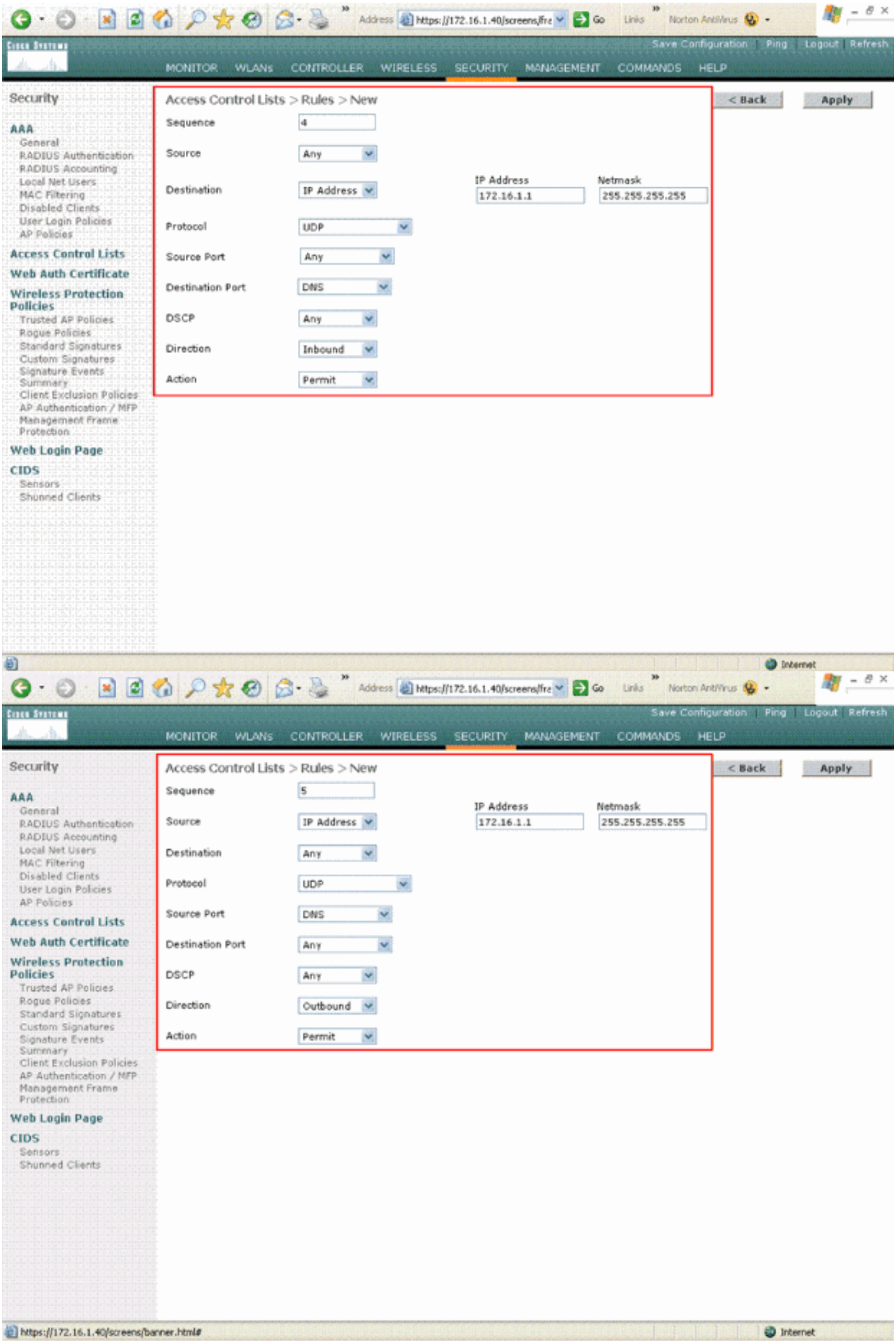
Si la fuente o el destino no es **ninguna**, después una declaración inversa en la dirección opuesta debe ser creada. Aquí está un
ejemplo.



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 del DHCP del servidor del DHCP al cliente de red inalámbrica. Haga clic en Apply (Aplicar).

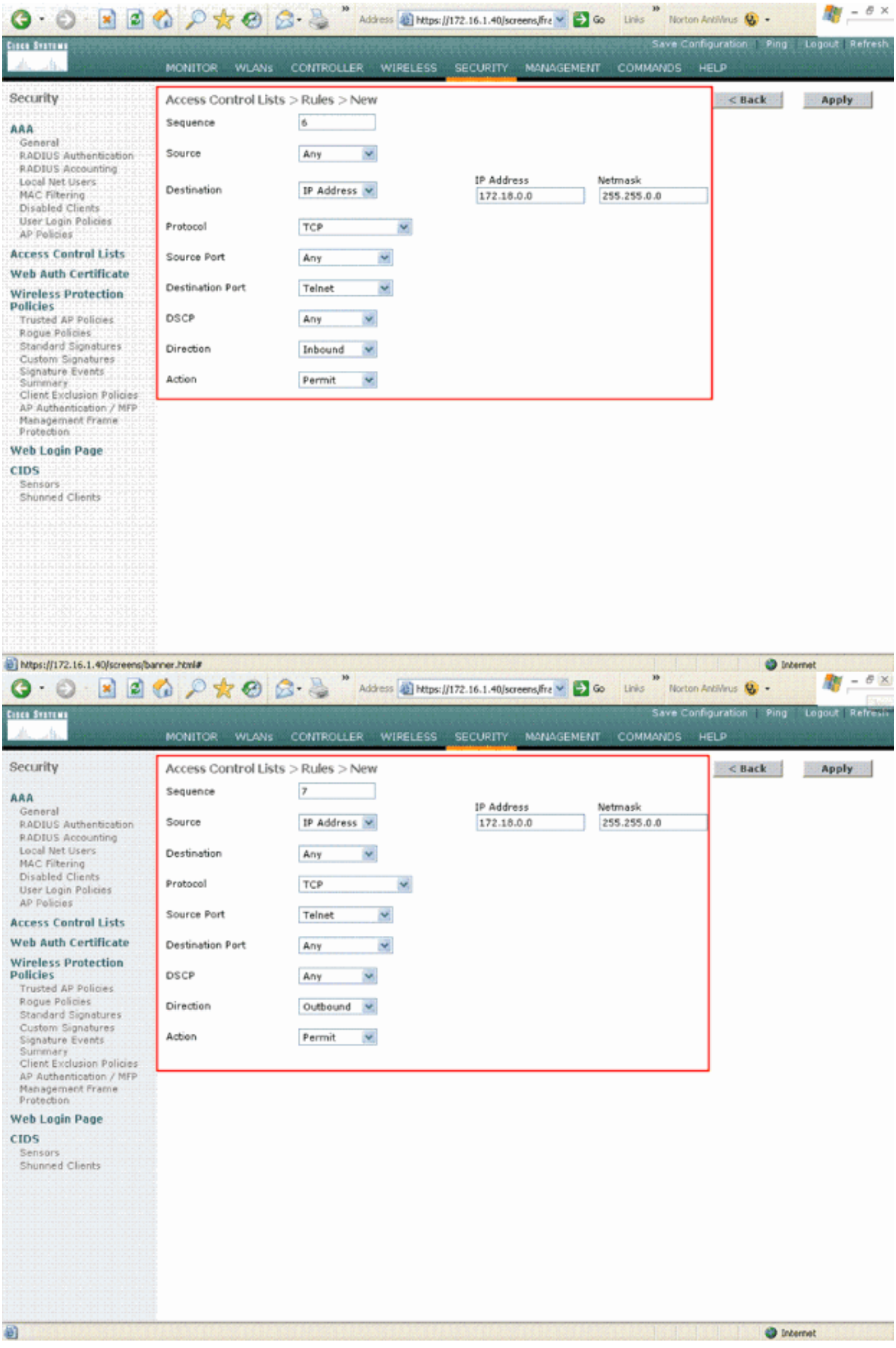


3. Semejantemente, cree las reglas que permiten el acceso al servidor DNS a todos los clientes de red inalámbrica y el acceso del servidor Telnet para el cliente de red inalámbrica a una subred específica. Aquí están los ejemplos.

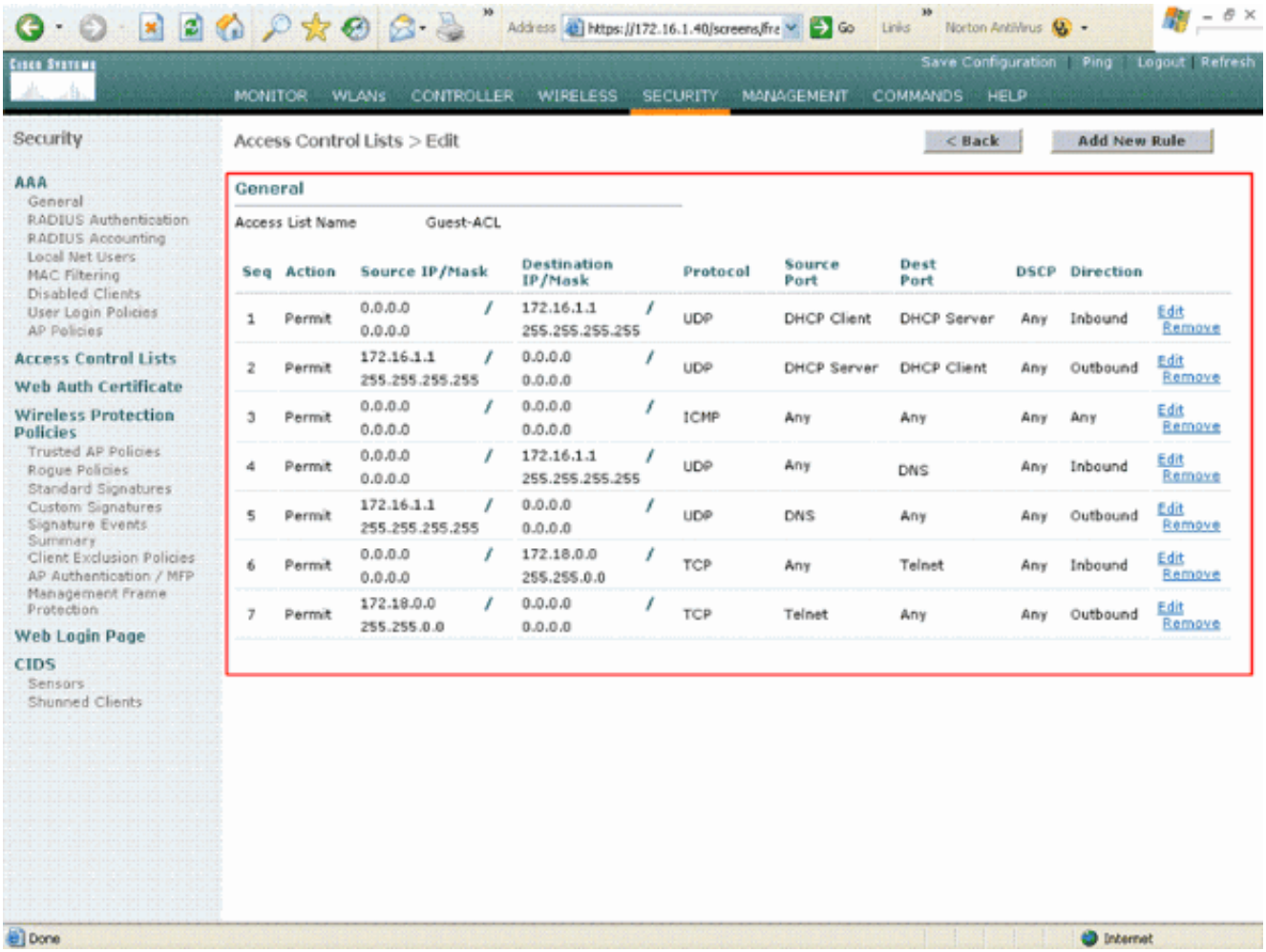


Defina esta regla para permitir el acceso para el cliente de red inalámbrica al servicio de

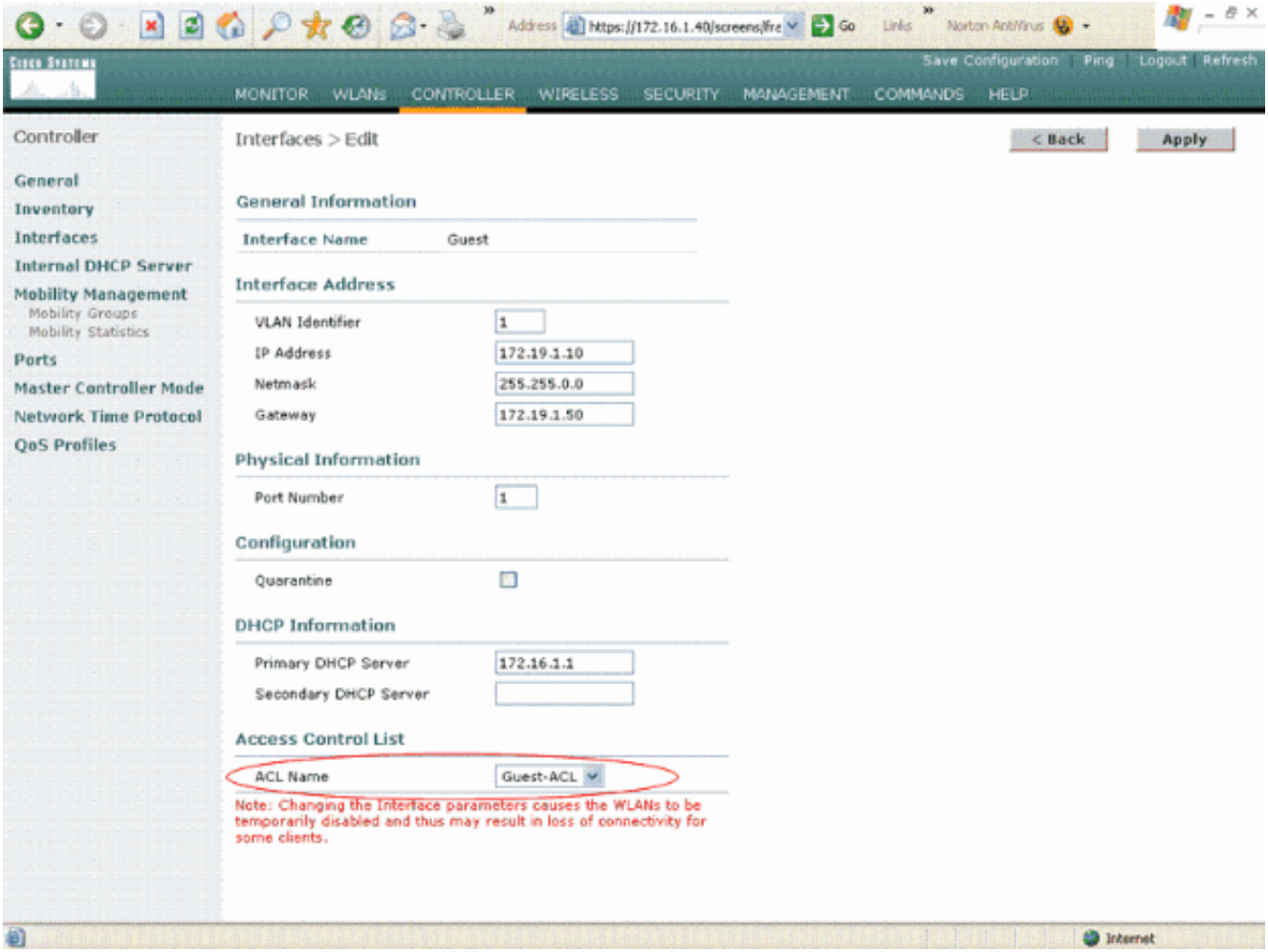
Telnet.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events Summary
Client Exclusion Policies
AP Authentication / MFP
Management Frame Protection
Web Login Page
CIDS
Sensors
Shunned Clients
Access Control Lists > Rules > New
< Back
Apply
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
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events Summary
Client Exclusion Policies
AP Authentication / MFP
Management Frame Protection
Web Login Page
CIDS
Sensors
Shunned Clients
Access Control Lists > Rules > New
< Back
Apply
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

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



4. Una vez que se crea el ACL, necesita ser aplicado a un interfaz dinámico. Para aplicar el ACL, elija el **regulador > los interfaces** y corrija el interfaz al cual usted quiere aplicar el ACL.
5. En los **interfaces > corrija la** página para el interfaz dinámico, 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 este interfaz dinámico. El Interfaz-ACL se puede aplicar solamente H-para cosechar los APs en el modo conectado pero no en el modo autónomo.

Note: 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.

Note: Este documento asume que las redes inalámbricas (WLAN) y los interfaces dinámicos están configurados. Refiera a los VLA N en el ejemplo inalámbrico de la configuración de los reguladores LAN para la información sobre cómo crear los interfaces dinámicos en WLCs.

Configure CPU ACL

Previamente, los ACL en 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 los interfaces de la Administración y del encargado AP. Para abordar este problema y filtro LWAPP y movilidad trafique, CPU ACL fueron introducidos con la versión 4.0 de los firmwares WLC.

La configuración de CPU ACL implica dos pasos:

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

Las reglas para la CPU ACL se deben configurar de una manera similar a los otros ACL. Refiera a la sección CPU ACL de asegurar los reguladores inalámbricos LAN (WLCs) para más información sobre CPU ACL.

Verifique

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 verifique que sus cambios ACL fueran aplicados al 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 está un ejemplo:

```
(Cisco Controller) >show acl summary

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

- **muestre *ACL_Name* detallado acl** — Visualiza la información detallada sobre los ACL configurados.Aquí está 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 la CPU, utilice el **comando cpu acl de la demostración**.Aquí está 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
```

Troubleshooting

El Software Release 4.2.61.0 o Posterior del regulador le permite 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
- Conmutador integrado del regulador LAN de la Tecnología inalámbrica del catalizador 3750G

Para activar 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, controle la casilla de verificación de los **contadores del permiso** y el tecleo **se aplica**. Si no, deje la casilla de verificación desenfrenada. 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