Ejemplo de Configuración de ACL en el Controlador de LAN Inalámbrica

Contenido

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 Configuración de ACL de CPU 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.

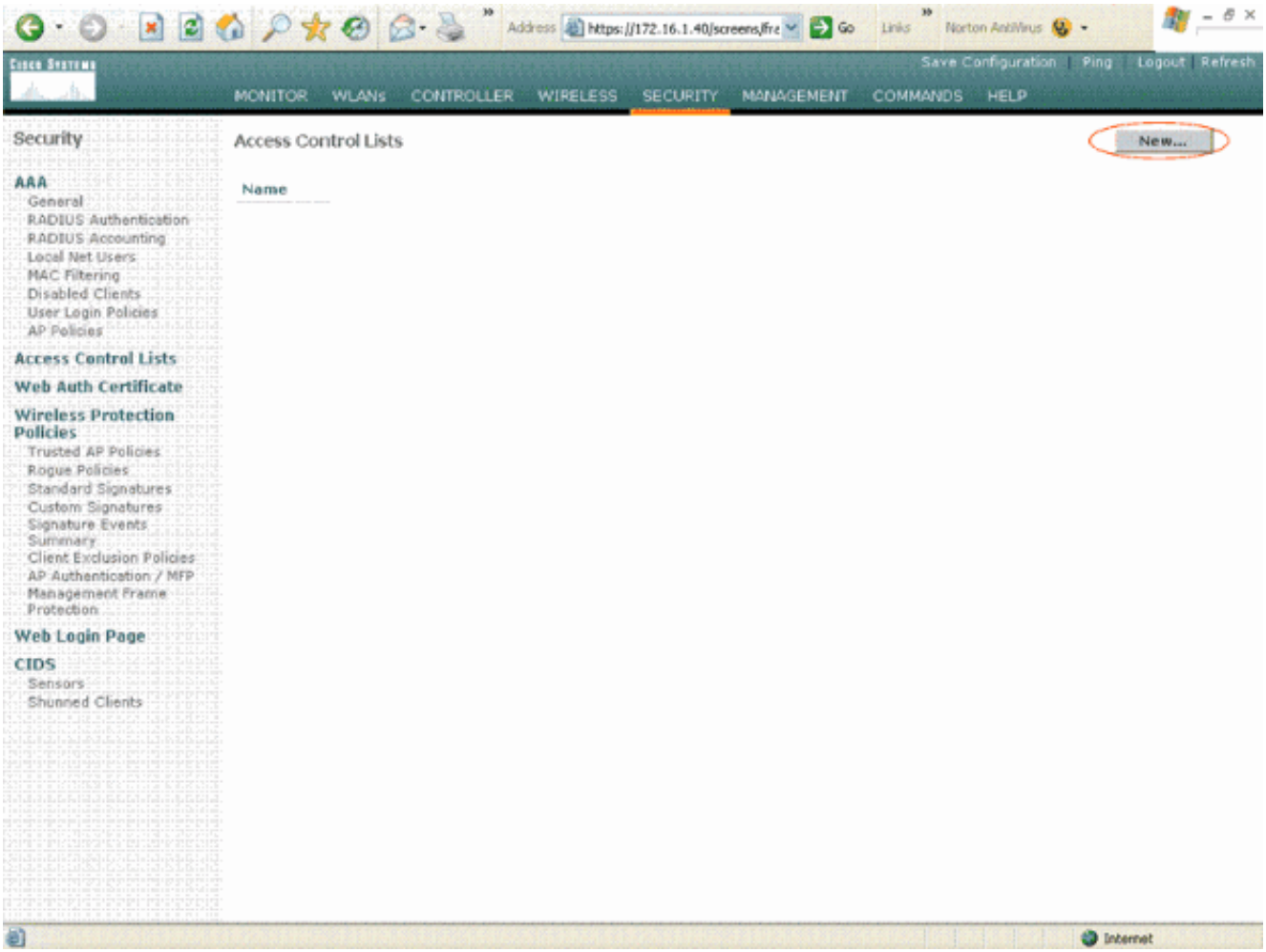
Configuración de ACL en WLC

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

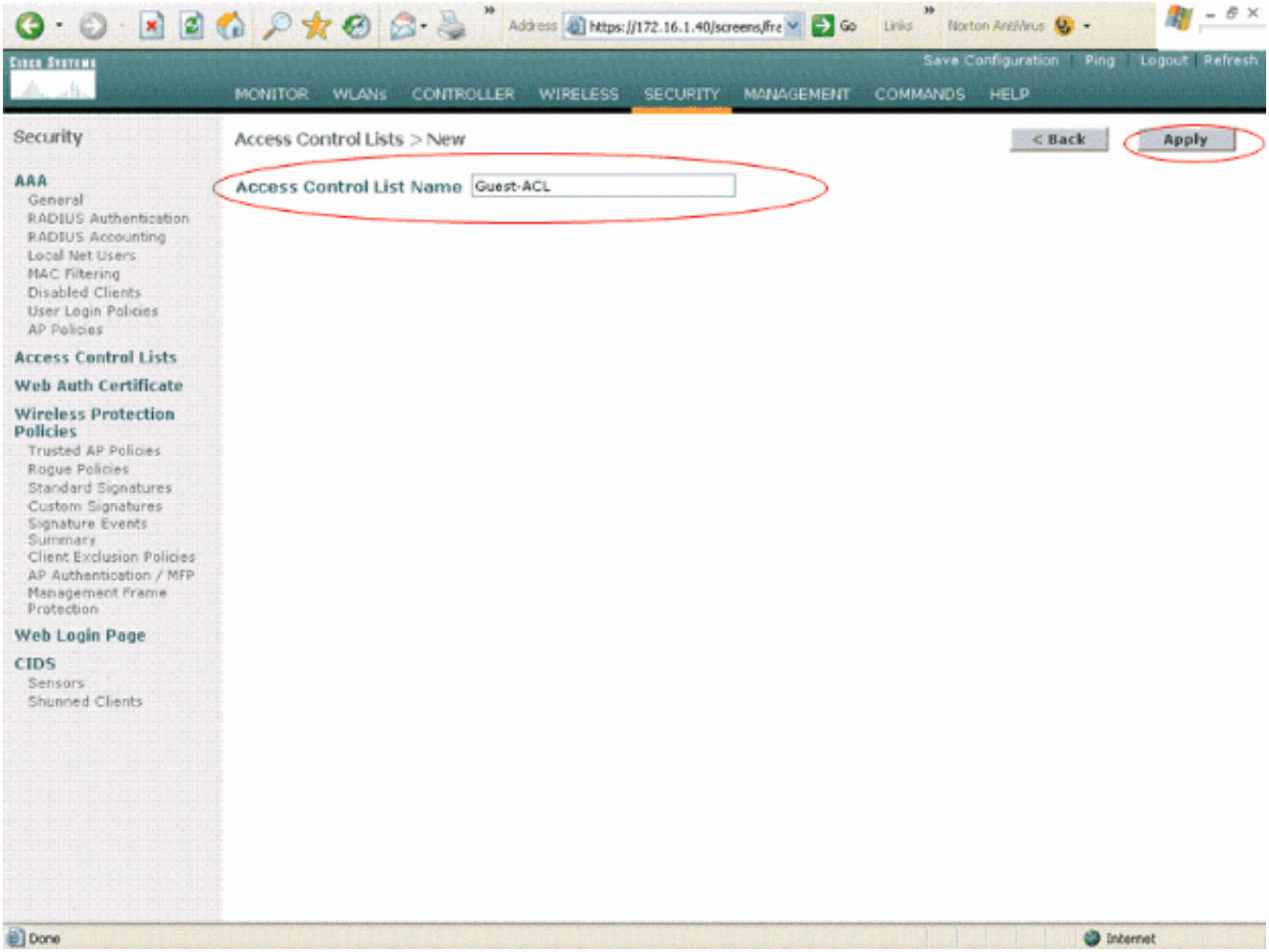
Todos los demás servicios deben estar bloqueados para los clientes inalámbricos. Complete estos pasos para crear la ACL con la GUI del WLC:

1. 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**
.



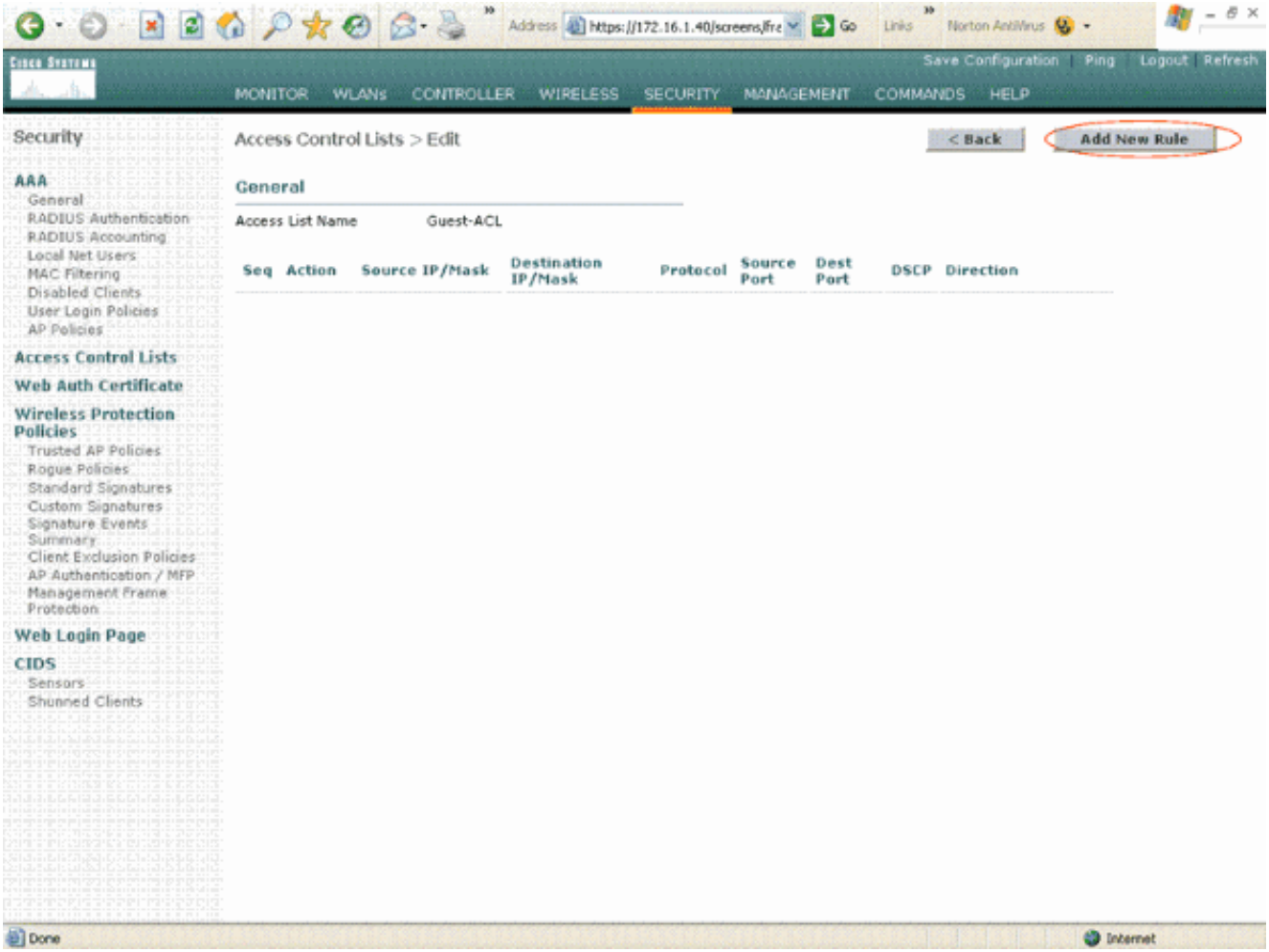
Listas de control de acceso

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

3. 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.



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

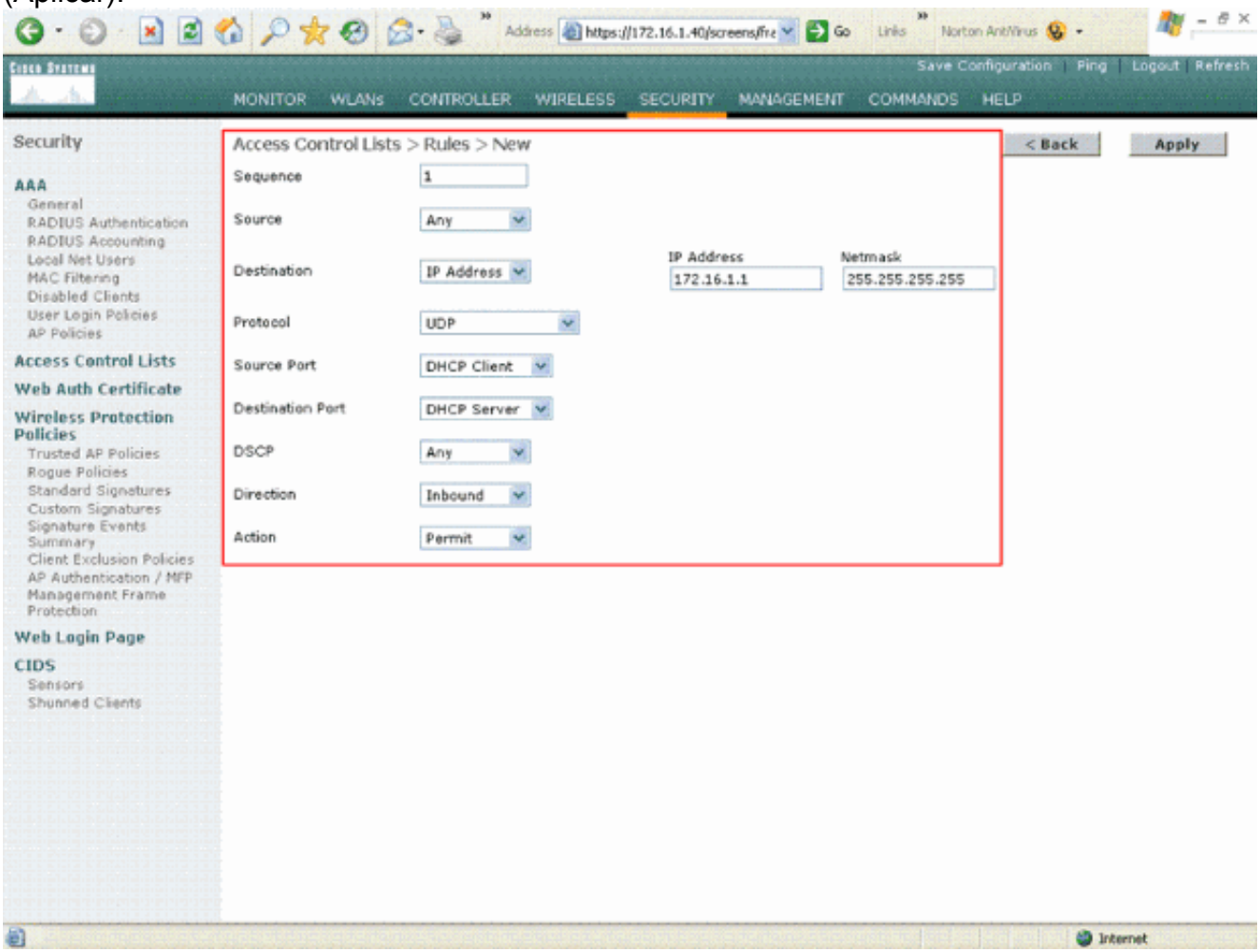
Configurar reglas que permiten servicios de usuario invitado

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

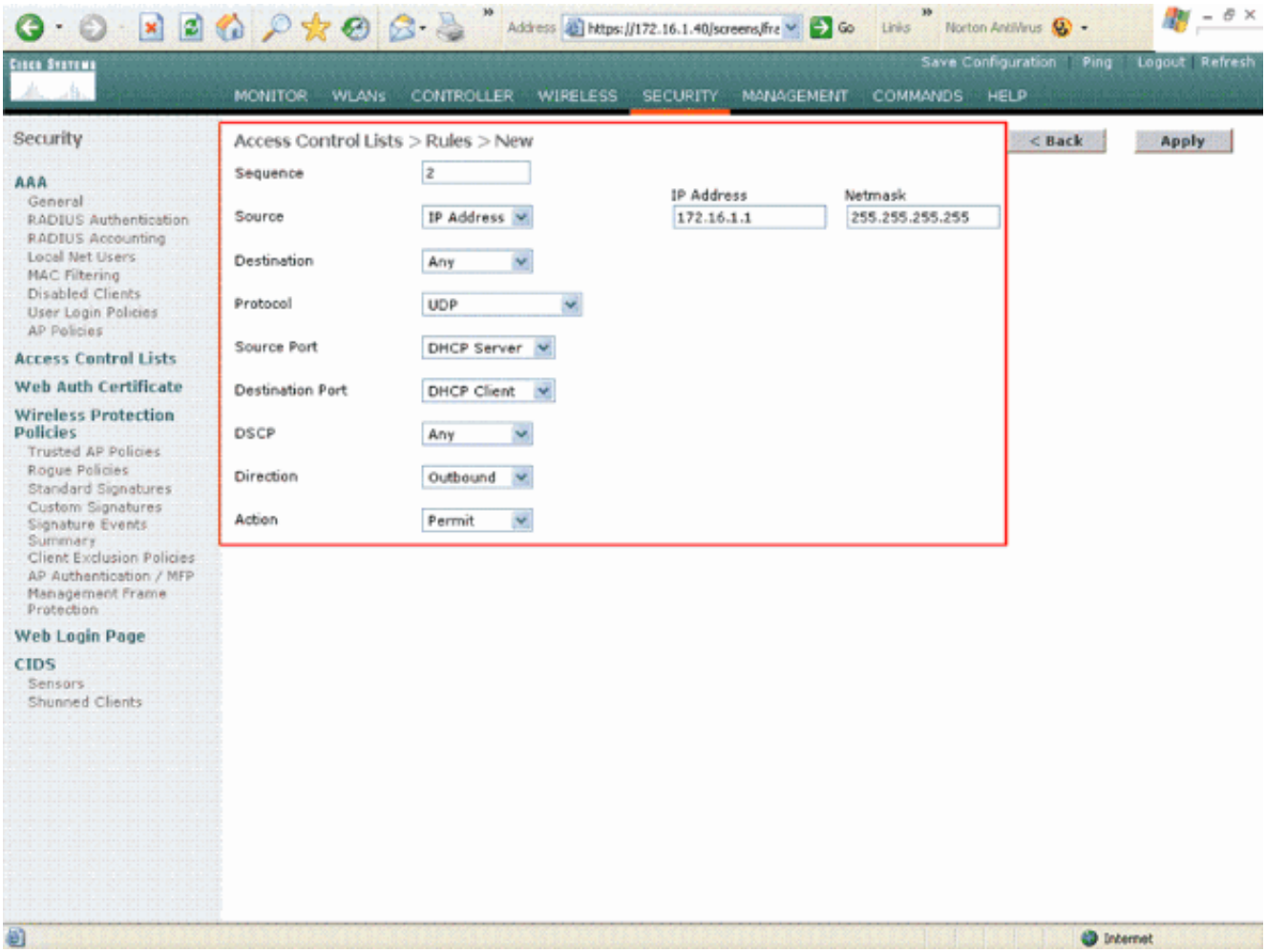
- DHCP entre los clientes inalámbricos y el servidor DHCP
- ICMP entre todos los dispositivos de la red
- DNS entre los clientes inalámbricos y el servidor DNS
- Telnet a una subred específica

1. 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).

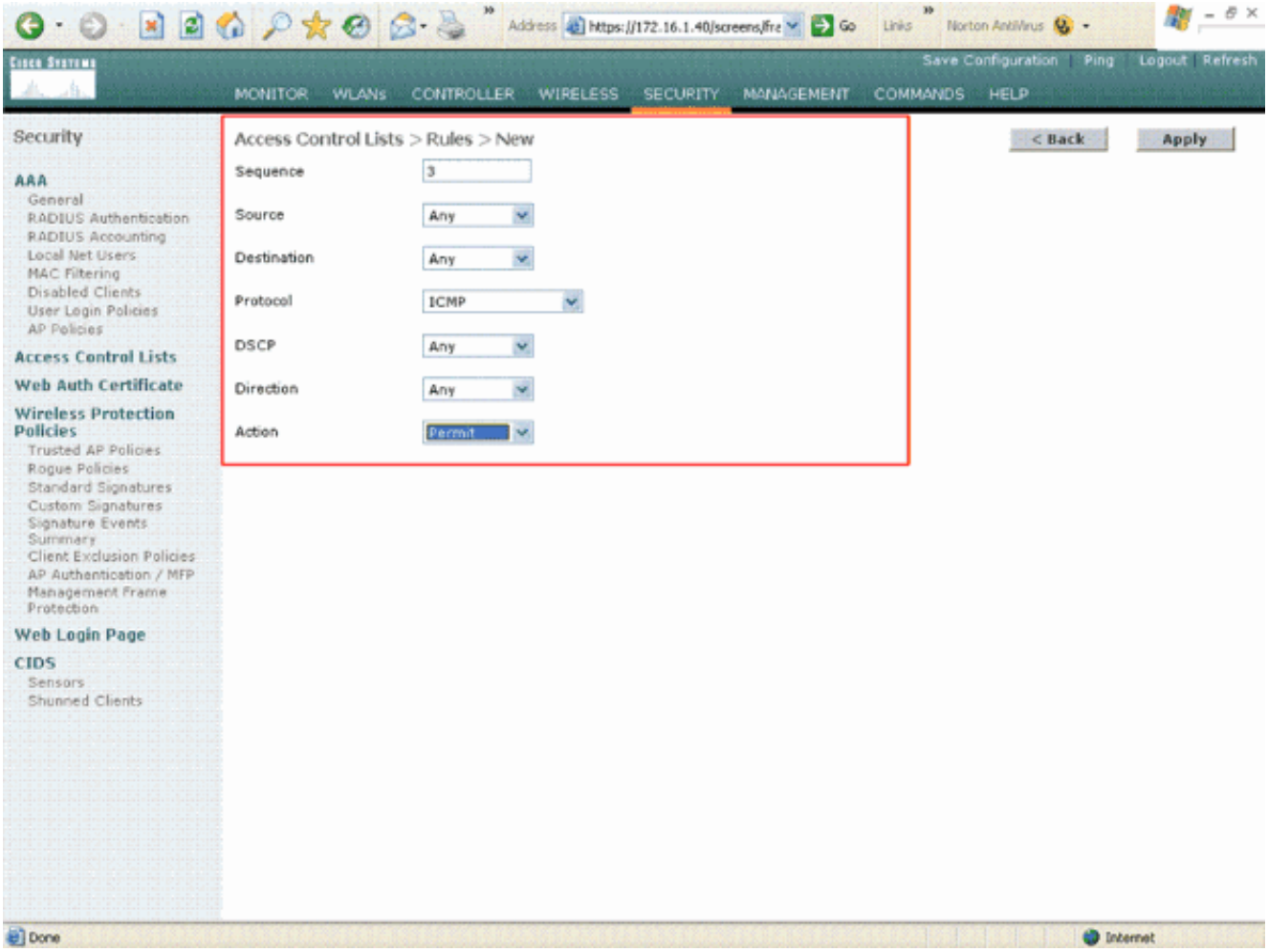


Elija Permit para que ACL permita paquetes DHCP Si el origen o el destino no son **cualquiera** , se debe crear una sentencia inversa en la dirección opuesta. Aquí está un
ejemplo.



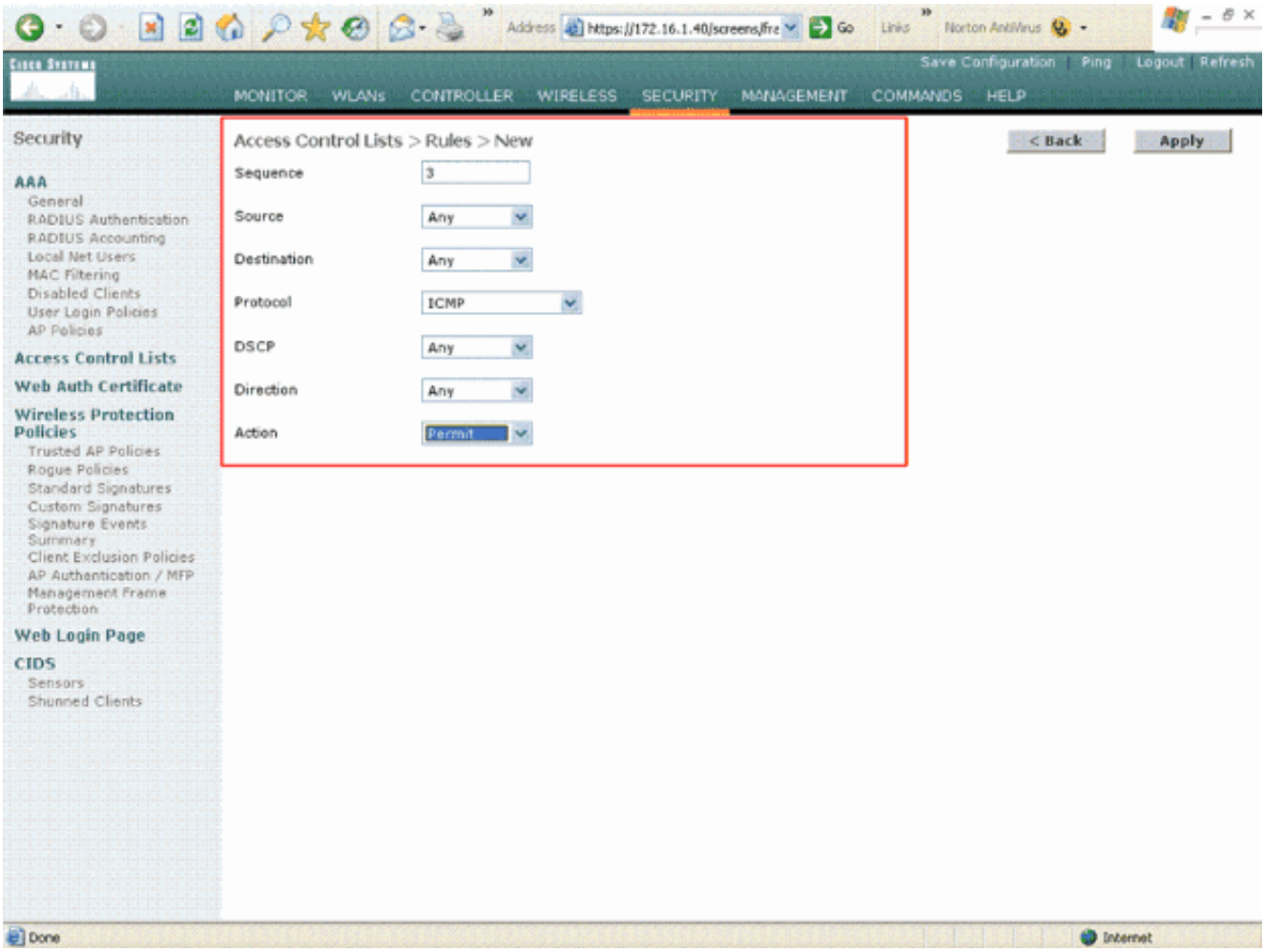
Origen o destino establecidos en Cualquiera

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).

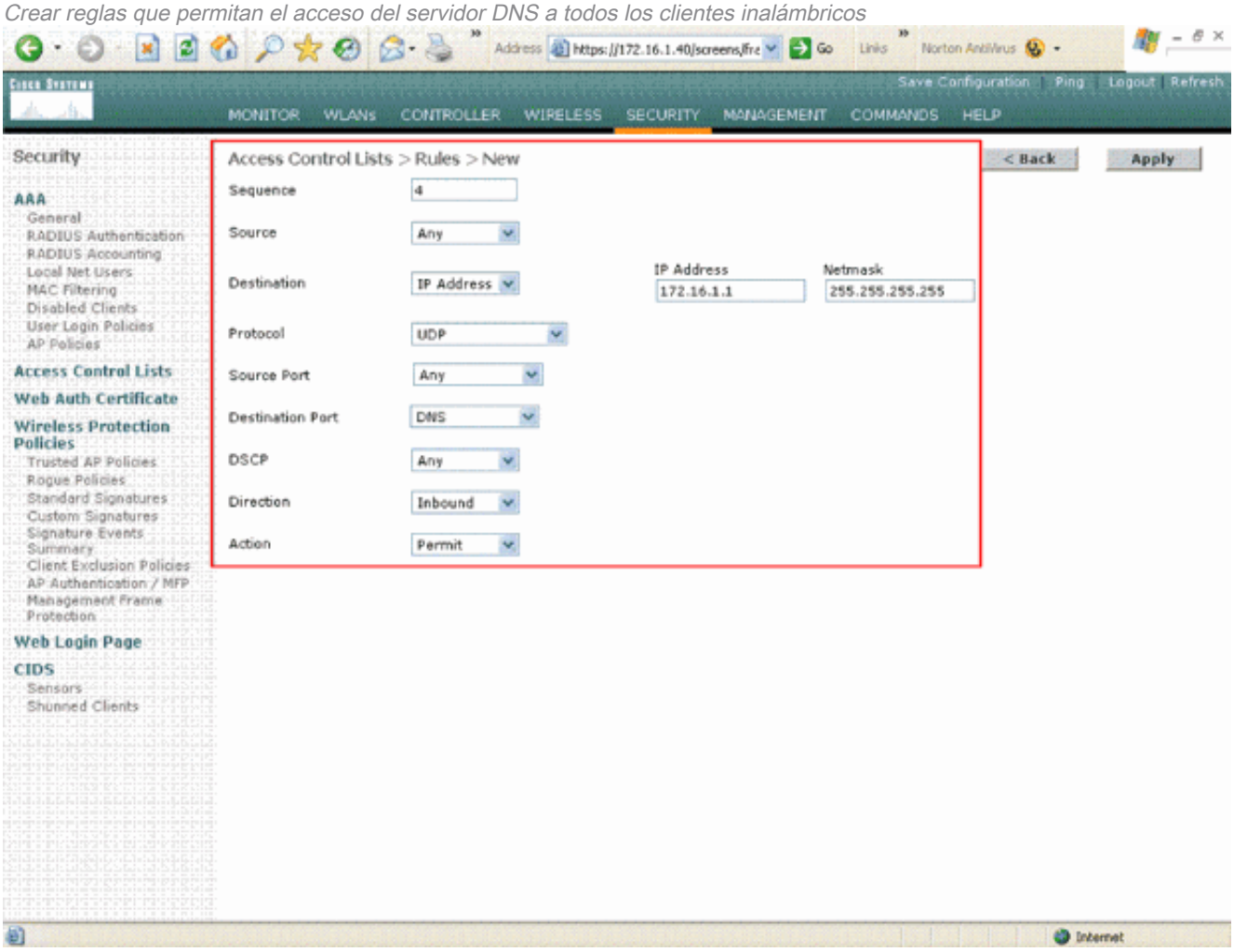


Permitir que ACL haga que permitan paquetes DHCP del servidor DHCP al cliente inalámbrico

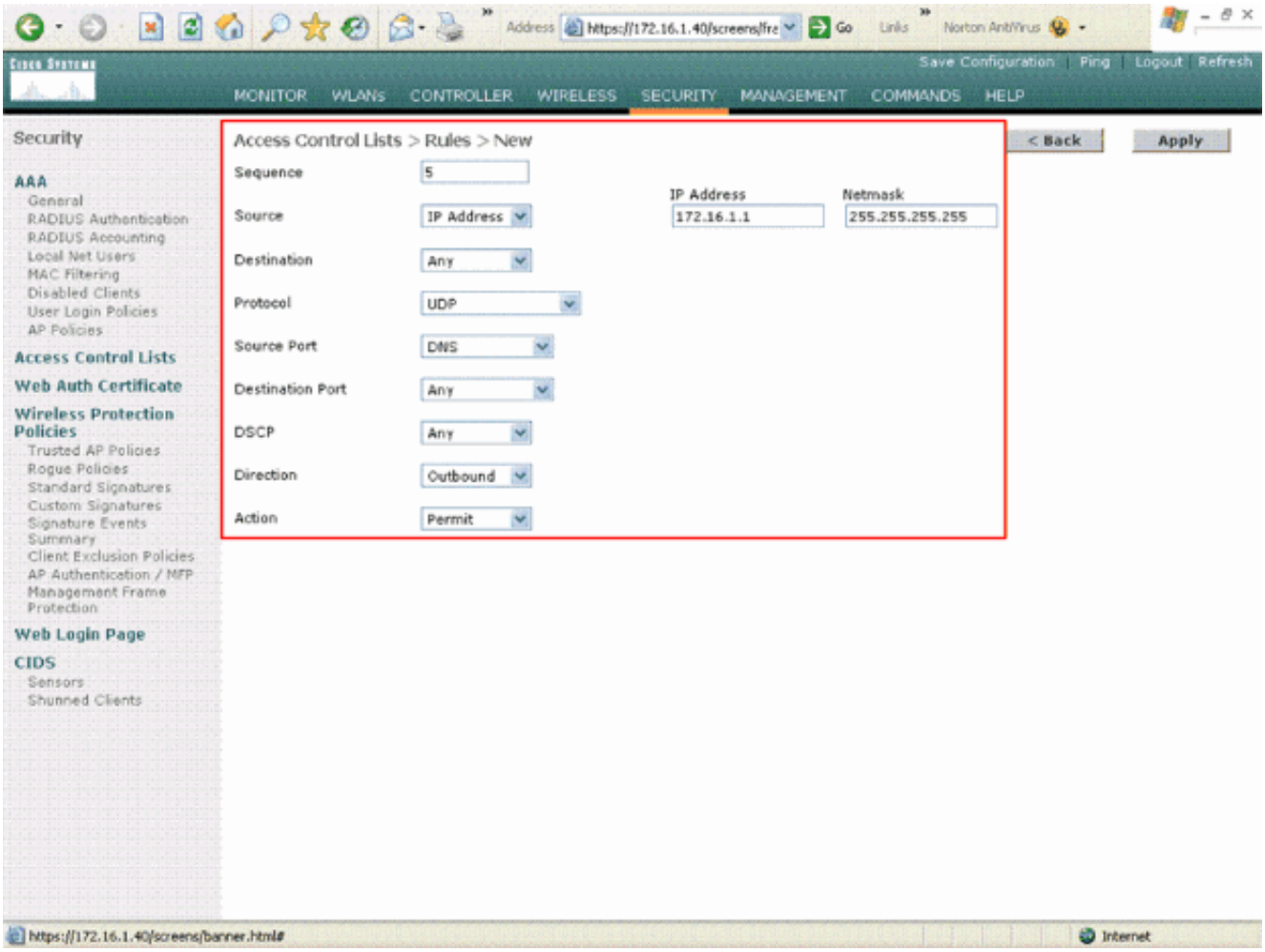
3. De manera similar, cree reglas que permitan el acceso del servidor DNS a todos los clientes inalámbricos y el acceso del servidor Telnet para el cliente inalámbrico a una subred específica. Estos son los
ejemplos.



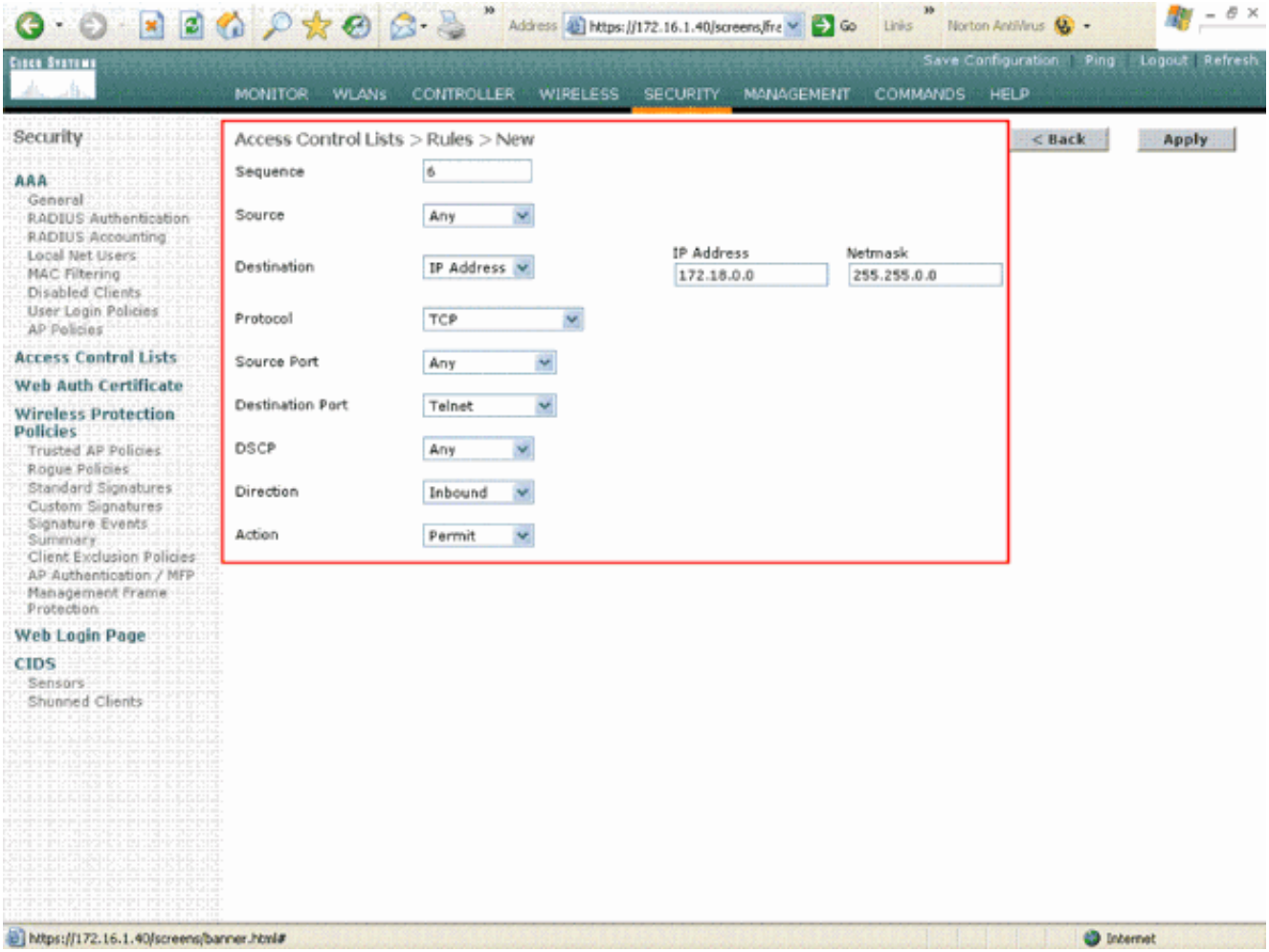
Crear reglas que permitan el acceso del servidor DNS a todos los clientes inalámbricos



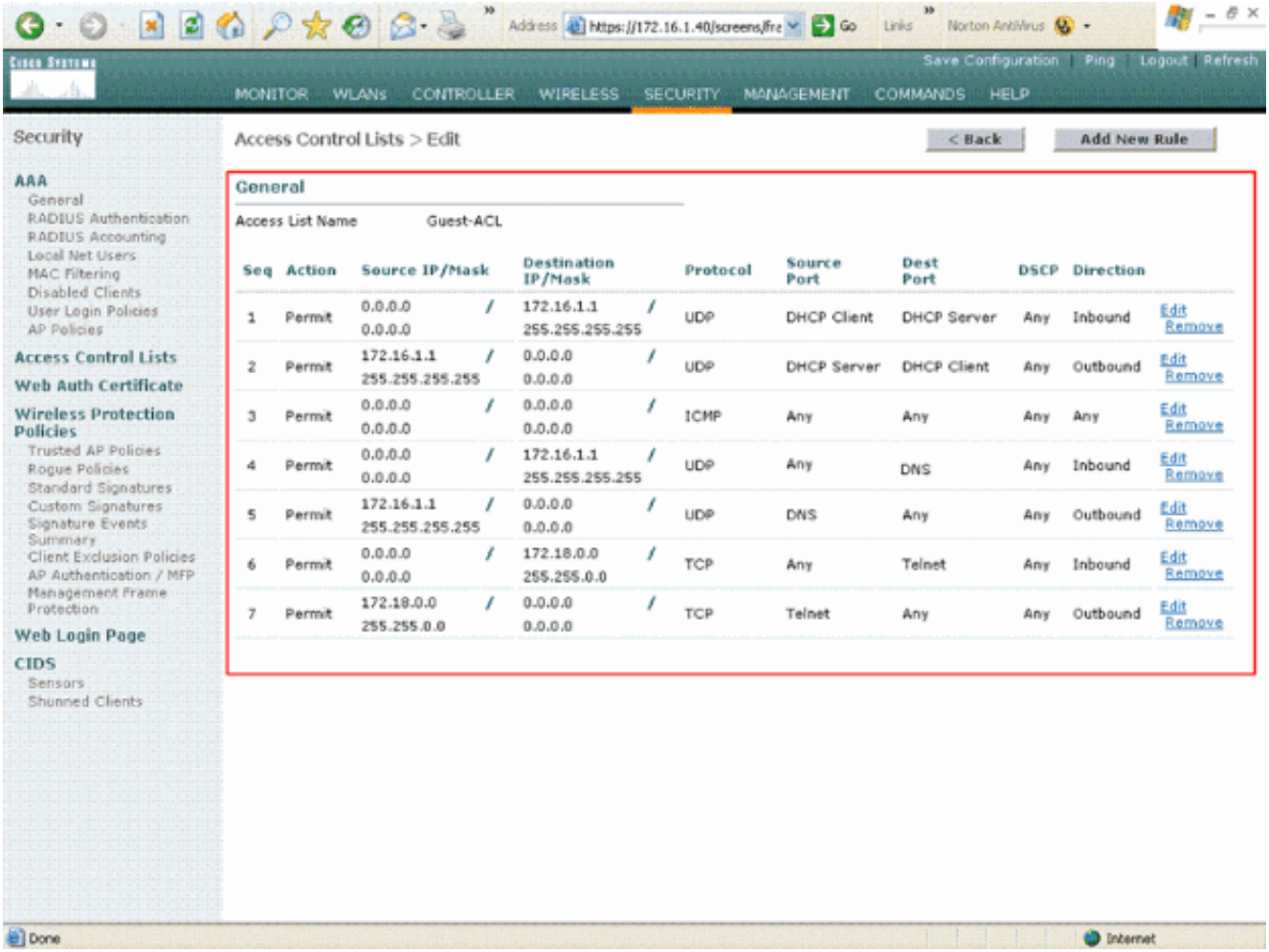
Crear reglas que permitan el acceso del servidor Telnet para el cliente inalámbrico a una subred Defina esta regla para permitir el acceso del cliente inalámbrico al servicio Telnet.



Permitir el acceso del cliente inalámbrico al servicio Telnet

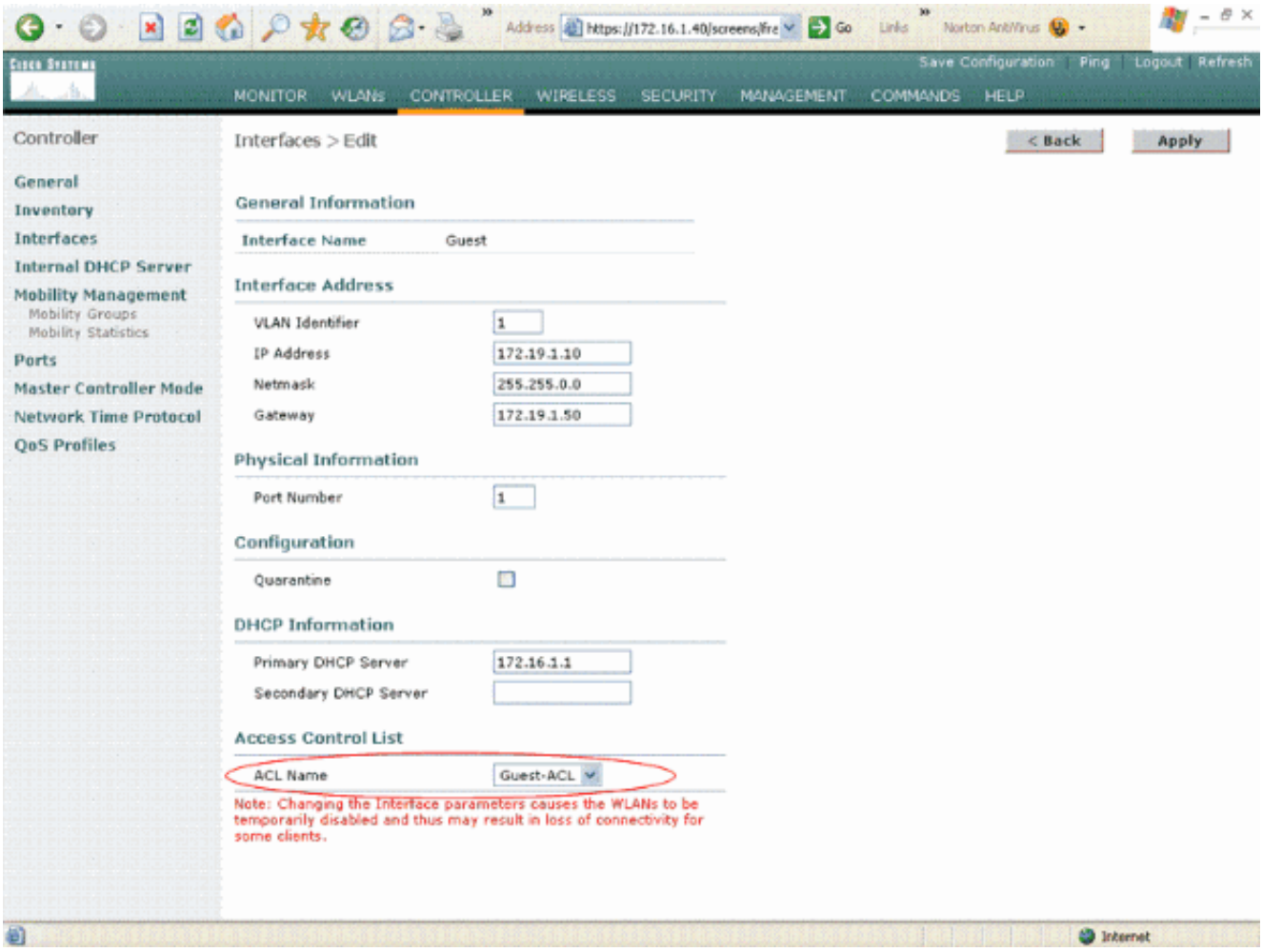


Otro ejemplo de acceso de cliente inalámbrico al servicio Telnet La página **ACL > Edit** muestra todas las reglas que se definen para la ACL.



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.



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 Configuración de VLAN en Controladores de LAN Inalámbricos 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
-------------------------------- -------
Guest-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 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
```

- **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
- Configuración de VLAN en controladores de LAN inalámbrica
- 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).