Asegurando los reguladores del Wireless LAN (WLCs)

Contenido

Introducción

Este documento ofrece una descripción de varios aspectos importantes necesarios para manejar la interacción de la Seguridad entre los reguladores del Wireless LAN (WLCs) y la red donde están conectadas. Este documento se centra sobre todo en el control de tráfico, y no dirige las políticas de seguridad WLAN, AAA o WPS.

Los temas que afectan al tráfico con el destino “al regulador” se cubren en este documento, y no se relacionan para traficar que se relacione con el “usuario a la red”.

Nota: Valide los cambios antes de aplicarlos a su red, como algunos de los ejemplos en este documento pueden bloquear el acceso administrativo a sus reguladores si están aplicada incorrectamente.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar el WLC y el Lightweight Access Point (REVESTIMIENTO) para la operación básica
- Conocimiento básico del modelo de OSI
- Entendiendo cómo la lista de control de acceso (ACL) trabaja

Componentes Utilizados

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

- WLC del Cisco 2000/2100/4400 Series que funciona con el firmware 4.2.130.0, 5.2.157.0 o más adelante

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.

Gestión de tráfico en el WLCs

Un componente crítico en la seguridad de la red es control de tráfico. En cualquier despliegue, es muy importante para los tipos de bloque de tráfico que llegan los dispositivos para prevenir los problemas de seguridad potencial (DOS, pérdida de información, escalada del privilegio, etc).

En el WLC, el control de tráfico es afectado por un hecho importante: hay dos componentes que manejan el tráfico en el dispositivo:

- CPU — Procesador principal que toma el cuidado de toda la actividad de la Administración, control RRM, del LWAPP, autenticación, DHCP, etc.
- NPU — Procesador de red que toma el cuidado del reenvío de tráfico rápido para los clientes autenticados (atados con alambre a la Tecnología inalámbrica y vice versa).

Esta arquitectura permite un reenvío de tráfico rápido, y reduce la carga en la CPU principal, que pueden entonces dedicar todos sus recursos para las tareas de alto nivel.

Esta arquitectura se encuentra en los 4400, WiSM y 3750 reguladores integrados. Para 2106 y NM-WLC y los reguladores relacionados, la expedición es hecha en el software, también por la CPU principal. Por lo tanto, toma un impuesto más alto sobre el CPU. Por eso estas Plataformas ofrecen un soporte más bajo del usuario y de la cuenta AP.

Tráfico que controla

Siempre usted quiere al filtrar tráfico en relación con un WLC, es importante saber si esto es usuario al tráfico de la red o está hacia la CPU principal.

- Para cualquier tráfico al CPU, por ejemplo, los protocolos de la Administración tales como SNMP, HTTPS, SSH, Telnet, o protocolos de los servicios de red tales como radio o DHCP, utilizan un “CPU ACL”.
- Para cualquier tráfico a y desde un cliente de red inalámbrica, incluyendo el tráfico que pasa a través de un túnel de EoIP (acceso de invitado), se utiliza una interfaz ACL, una red inalámbrica (WLAN) ACL, o a por el usuario ACL.

El tráfico se define “al CPU”, como tráfico que esté ingresando el regulador, con el destino al IP Address de administración, a las interfaces dinámicas unas de los o a la dirección de puerto del servicio. El AP manager no maneja ningún otro tráfico excepto LWAPP/CAPWAP.

Acceso de administración que controla

El WLCs tiene un control de acceso llano de la “sesión” para los protocolos de la Administración. Es importante entender cómo trabajan para prevenir la evaluación incorrecta sobre lo que es permitido o no permitido por el regulador.

Los comandos de restringir se permiten qué protocolos de la Administración son (en un ámbito global):

- **permiso del ssh de la red de los config|neutralización** — Esto habilita o inhabilita el servicio de SSH en el regulador. Esto se activa como opción predeterminada. Una vez discapacitado, el puerto (TCP 22) no será accesible.
- **permiso telnet de la red de los config|neutralización** — Esto habilita o inhabilita el servicio de Telnet en el regulador. Esto se inhabilita por abandono. Una vez discapacitado, el puerto (TCP 23) no será accesible.
- **permiso HTTP de la red de los config|neutralización** — Esto habilita o inhabilita el servicio HTTP en el regulador. El puerto (TCP 80) no es un accesible más largo. Esto se inhabilita por abandono.
- **permiso del https de la red de los config|neutralización** — Esto habilita o inhabilita el servicio del https en el regulador. Esto se activa como opción predeterminada. Una vez discapacitado, el puerto (TCP 443) no será accesible.
- **permiso de la versión v1|v2|v3 SNMP de los config|neutralización** — Esto habilita o inhabilita las versiones específicas del servicio SNMP en el regulador. Usted necesita inhabilitar todos para prevenir el acceso SNMP al regulador, a menos que use un ACL.
- **permiso de la mgmt-vía-Tecnología inalámbrica de la red de los config|neutralización** — Esto previene que los clientes asociados a este regulador puedan los protocolos de la Administración de acceso a él (ssh, https, etc). Esto no previene ni cierra los puertos correspondientes TCP desde el punto de vista del dispositivo de red inalámbrica. Esto significa que un dispositivo de red inalámbrica, cuando éste se fija para inhabilitar, puede abrir una conexión SSH, si se habilita el protocolo. El usuario pudo ver un prompt de nombre de usuario generado por el daemon ssh, no obstante la sesión se cierra tan pronto como usted intente teclear un nombre de usuario.
- **permiso de la mgmt-vía-dinámico-interfaz de la red de los config|neutralización** — Esto previene que los dispositivos en el mismo VLA N que el regulador puedan los protocolos de la Administración de acceso a él (ssh, https, etc) al direccionamiento correspondiente de la

interfaz dinámica en ese VLA N. Esto no previene ni cierra los puertos correspondientes TCP desde el punto de vista del dispositivo. Esto significa que un dispositivo, cuando éste se fija para inhabilitar, puede abrir una conexión SSH, si se habilita el protocolo. El usuario pudo ver un prompt de nombre de usuario generado por el daemon ssh, no obstante la sesión se cierra tan pronto como usted intente teclear un nombre de usuario. Además, la dirección de administración seguirá siendo siempre accesible de un VLA N de la interfaz dinámica, a menos que un CPU ACL esté en el lugar.

Por ejemplo, ésta es la configuración usando la información antedicha:

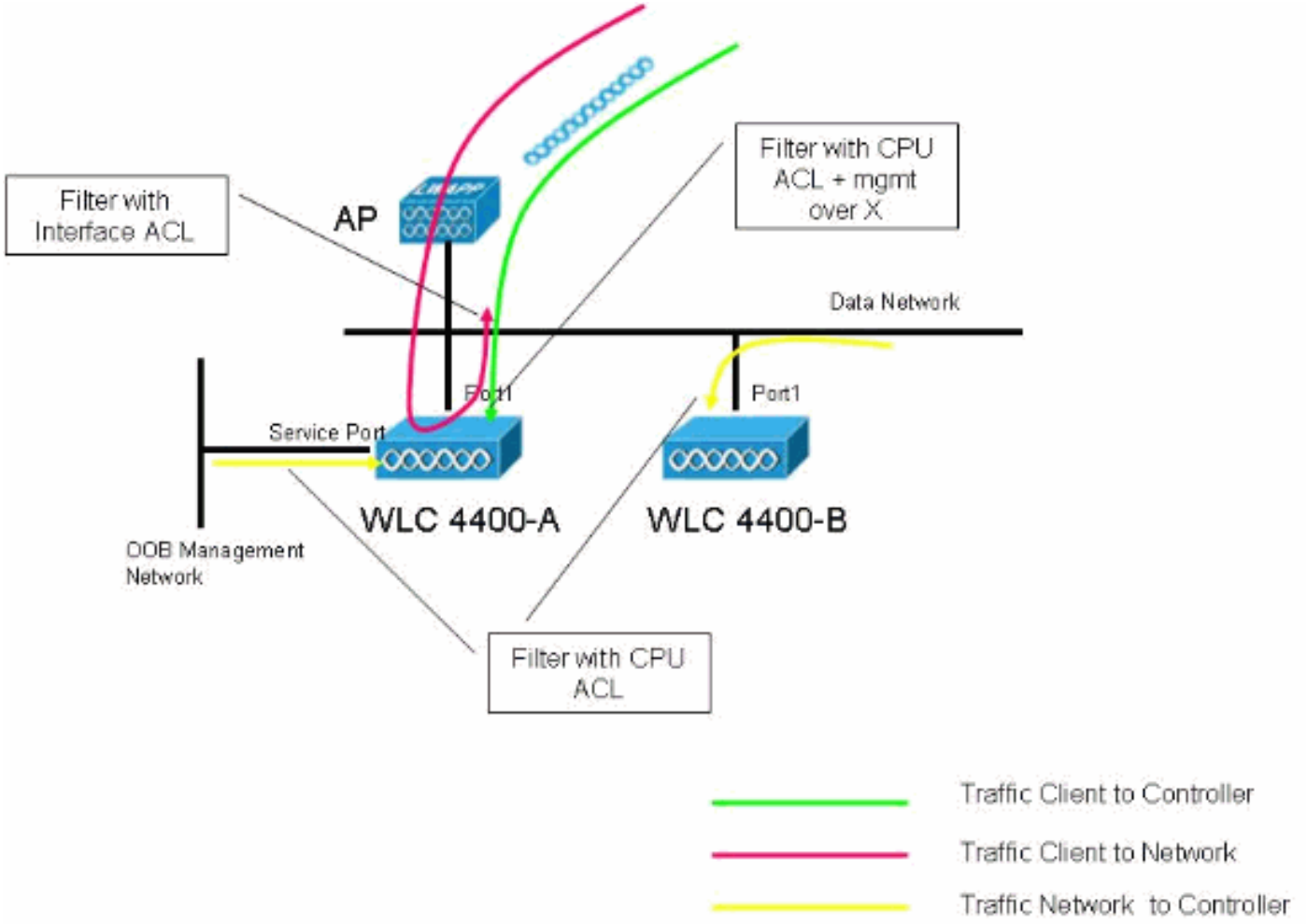
```
(Cisco Controller) >show network summary


RF-Network Name............................. 4400
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Disable
Ethernet Multicast Mode..................... Enable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
AP Multicast Mode........................... Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority............................ Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Mesh Full Sector DFS........................ Enable
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
AP Fallback ................................ Enable
Web Auth Redirect Ports .................... 80
Fast SSID Change ........................... Disabled
802.3 Bridging ............................. Disable
IP/MAC Addr Binding Check .................. Enabled


(Cisco Controller) >show acl cpu

CPU Acl Name................................ NOT CONFIGURED
Wireless Traffic............................ Disabled
Wired Traffic............................... Disabled
```

Usted puede concluir eso:

- Telnet y el HTTP no estarán disponibles, así que todo el tráfico de administración interactivo al regulador será hecho con HTTPS/SSH (cifrado).
- Un usuario de red inalámbrica asociado a este regulador no podrá conseguir el acceso administrativo.
- Si un usuario de red inalámbrica, asociado a este regulador, hace una exploración del puerto, mostrará SSH y el HTTP como abierto, aunque no se permite ningún acceso administrativo.
- Si un usuario atado con alambre (el mismo VLA N que una interfaz dinámica) hace una exploración del puerto, mostrará SSH y el HTTP como abierto, aunque no se permite ningún

acceso administrativo.

Es importante observar que en los entornos con más de un regulador en el mismo grupo de la movilidad, la relación de cuál es un cliente de red inalámbrica está solamente al regulador actualmente asociado. Por lo tanto, si asocian a un cliente al regulador A, después para un regulador B en el mismo grupo de la movilidad, este cliente es un dispositivo que viene de una interfaz VLAN/dynamic. Esto es importante tener en cuenta en la Administración sobre la configuración inalámbrica. Vea este diagrama para un ejemplo de donde poner una restricción del tráfico, y qué comandos pueden afectar a cada punto de ingreso:



CPU ACL

Siempre que usted quiera controlar que los dispositivos pueden hablar con la CPU principal, se utiliza un CPU ACL. Es importante mencionar varias características para éstos:

- Filtrar tráfico CPU ACL solamente hacia el CPU, y no ningún tráfico que sale o generado por el CPU.**Nota:** Para las 5500 Series del WLC en las versiones 6.0 y posterior, el CPU ACL es aplicable para el tráfico originado del WLC también. Para las otras Plataformas del WLC, este comportamiento se implementa en las versiones 7.0 y posterior. También, al crear los campos de dirección CPU ACL no tenga ningún impacto.
- El soporte completo para CPU ACL para toda la administración IP y direcciones dinámicas del regulador está solamente presente en 4.2.130.0 y posterior.
- El CPU ACL que bloquea el tráfico del puerto del servicio está solamente presente en 5.0 y posterior.
- Cuando se diseña un CPU ACL, es importante permitir el tráfico de control entre los

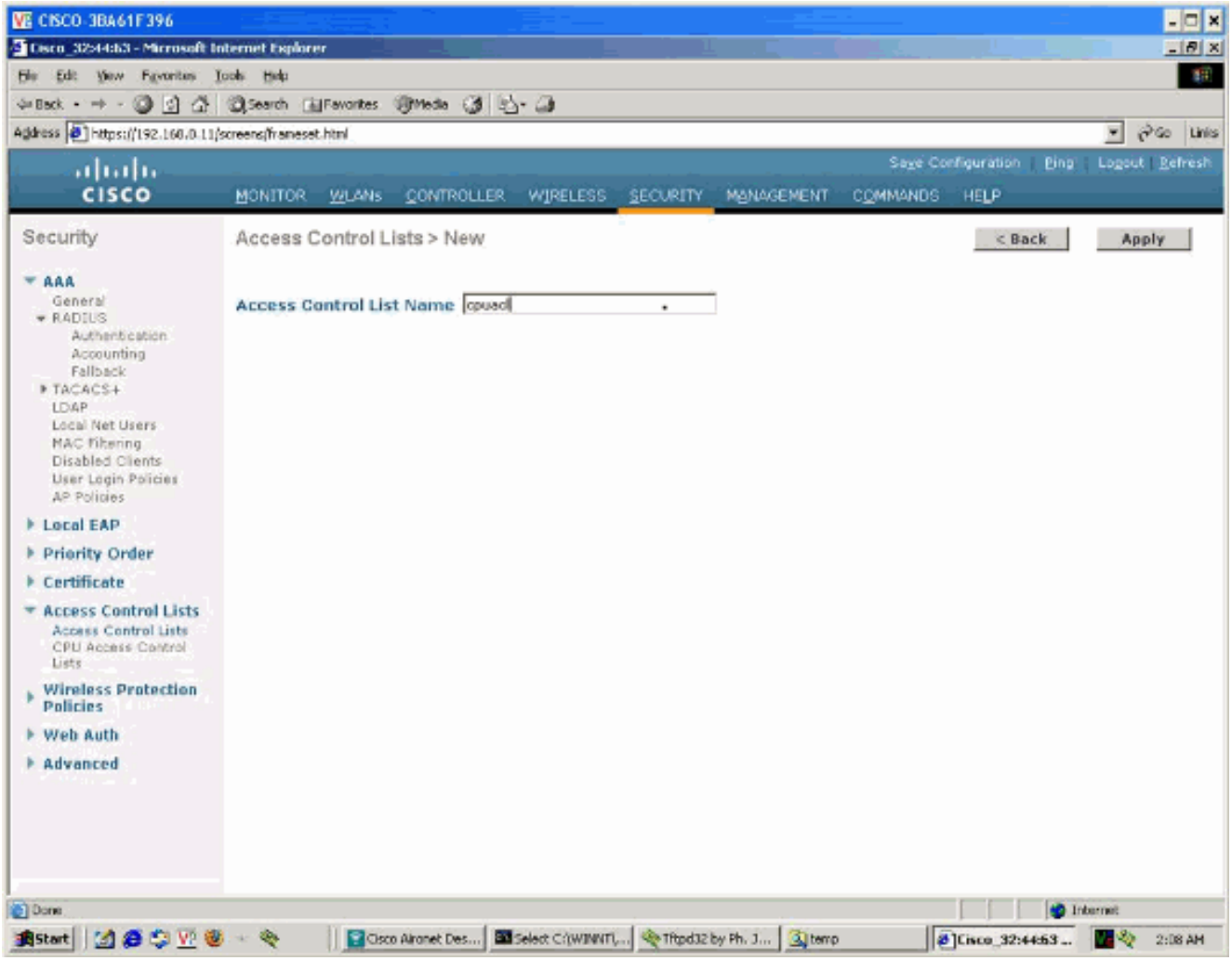
reguladores. El comando **sh de las reglas** puede ofrecer una vista rápida del tráfico permitida a CPU ACL en las condiciones normales.

- El regulador tiene un conjunto de las reglas para filtros para los procesos internos, que se pueden marcar con el comando **sh de las reglas**. Los ACL no afectan a estas reglas, ni se pueden estas reglas modificar simultáneamente. El CPU ACL toma la precedencia sobre ellas.
- El tráfico de datos del LWAPP o CAPWAP no es afectado por las reglas CPU ACL en 4400 reguladores basados, tráfico de control es afectado (si hace un ACL estricto, usted necesita permitirlo explícitamente).**Nota:** El tráfico de control CAPWAP no es afectado por CPU ACL.

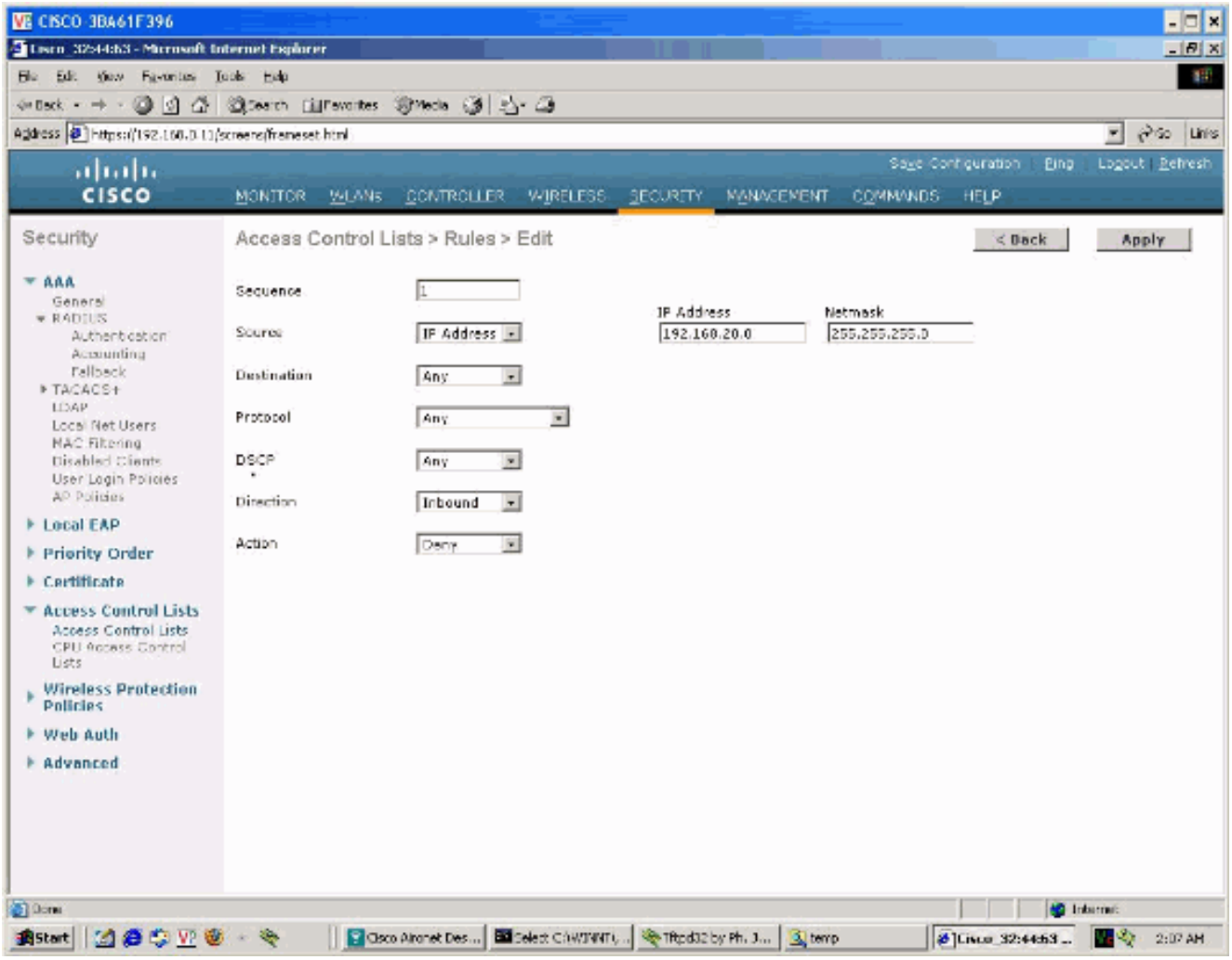
Ejemplo:

Por ejemplo, usted puede ser que quiera bloquear todo el tráfico que venía del interface/VLAN dinámico (192.168.20.0/24) donde están asociados los usuarios, hacia el CPU, pero se permite cualquier otro tráfico. Esto no debe prevenir a los clientes de red inalámbrica para conseguir a una dirección negociada del DHCP.

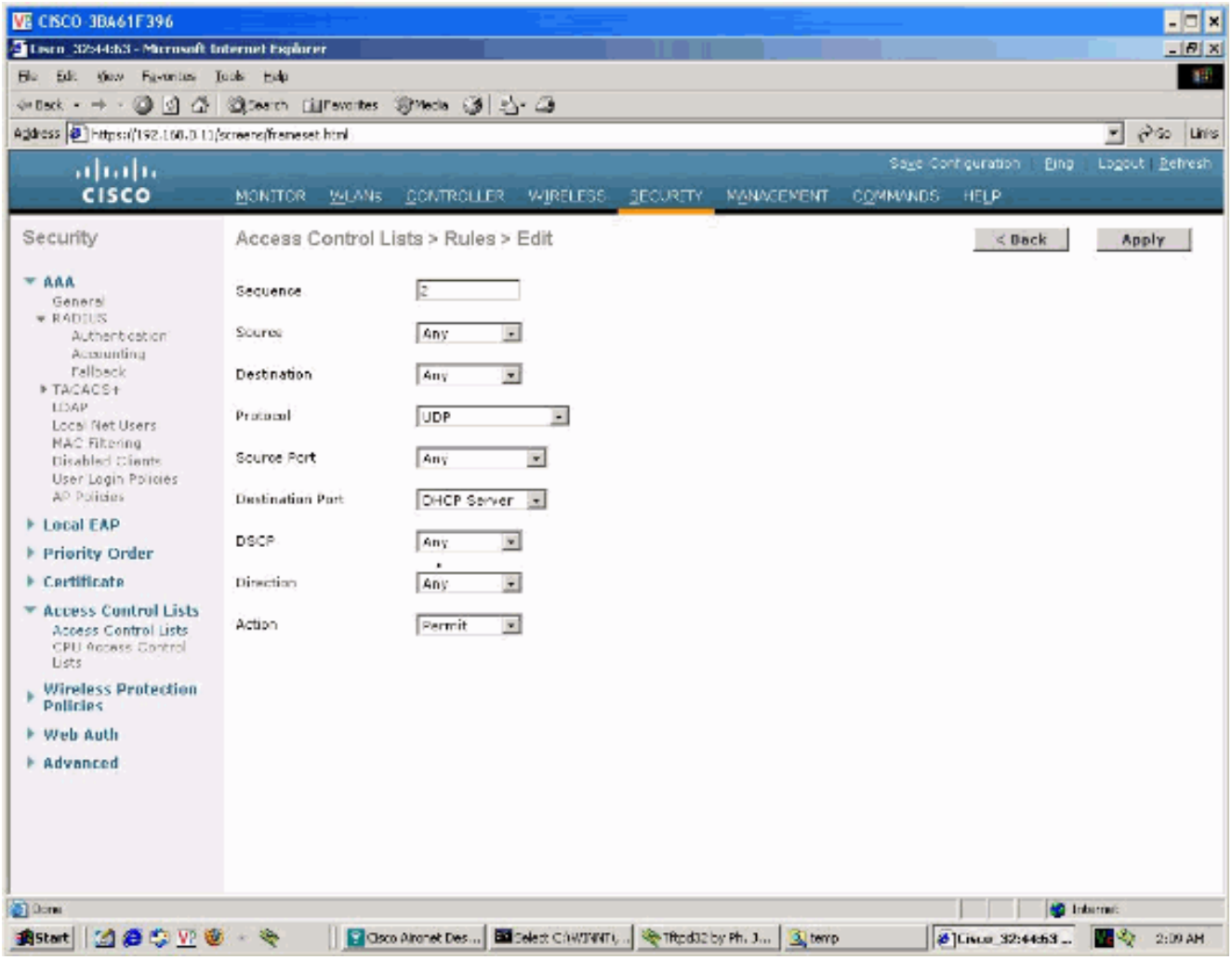
1. Como primer paso, se crea una lista de acceso:



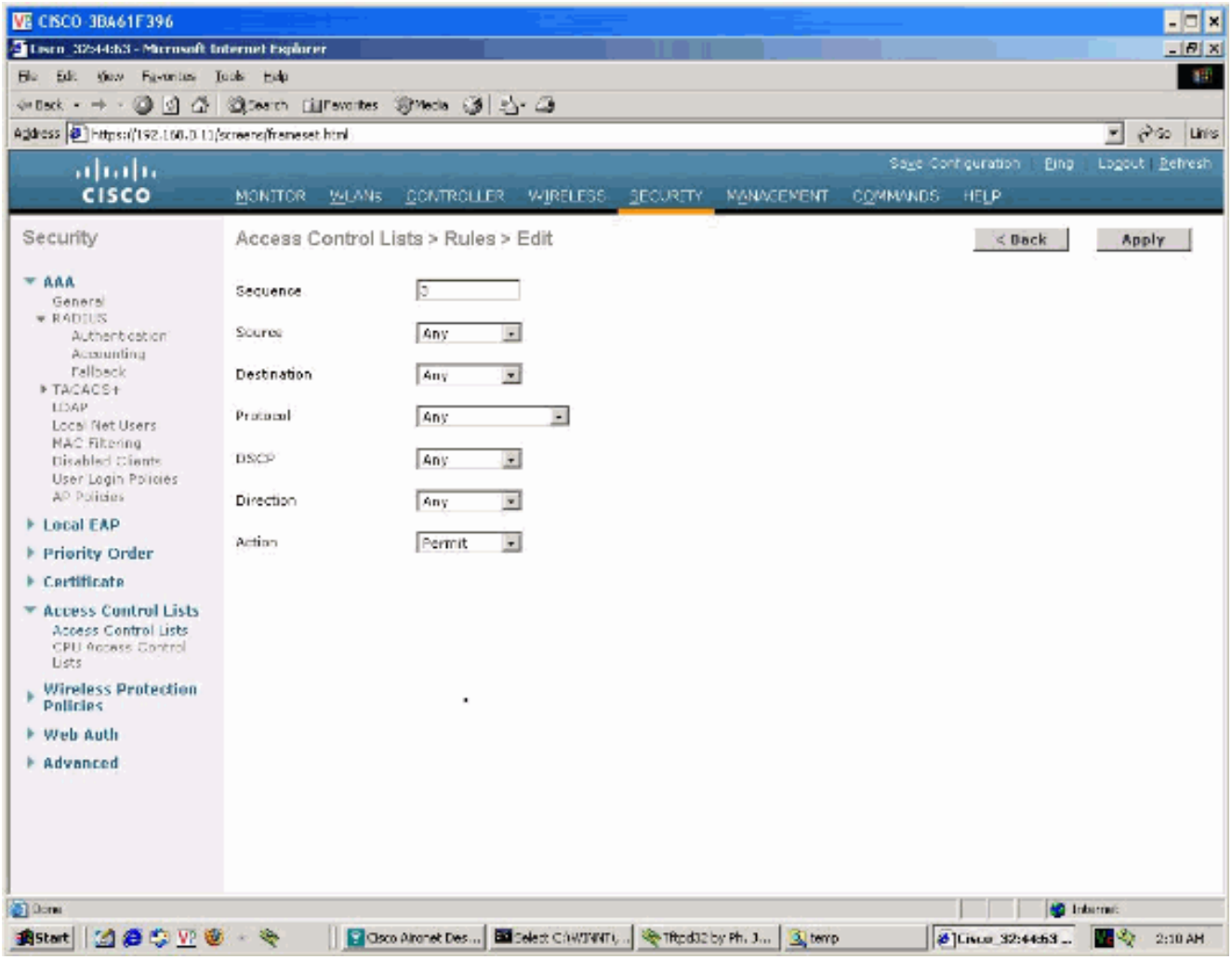
2. Haga clic **agregan la nueva regla**, y la fijan para bloquear todo el tráfico de origen que viene a partir del 192.168.20.0/24 a cualquier destino.



3. Agregue una segunda regla, para el tráfico del DHCP, con el puerto de servidor de destino, pero con la acción del
permiso:

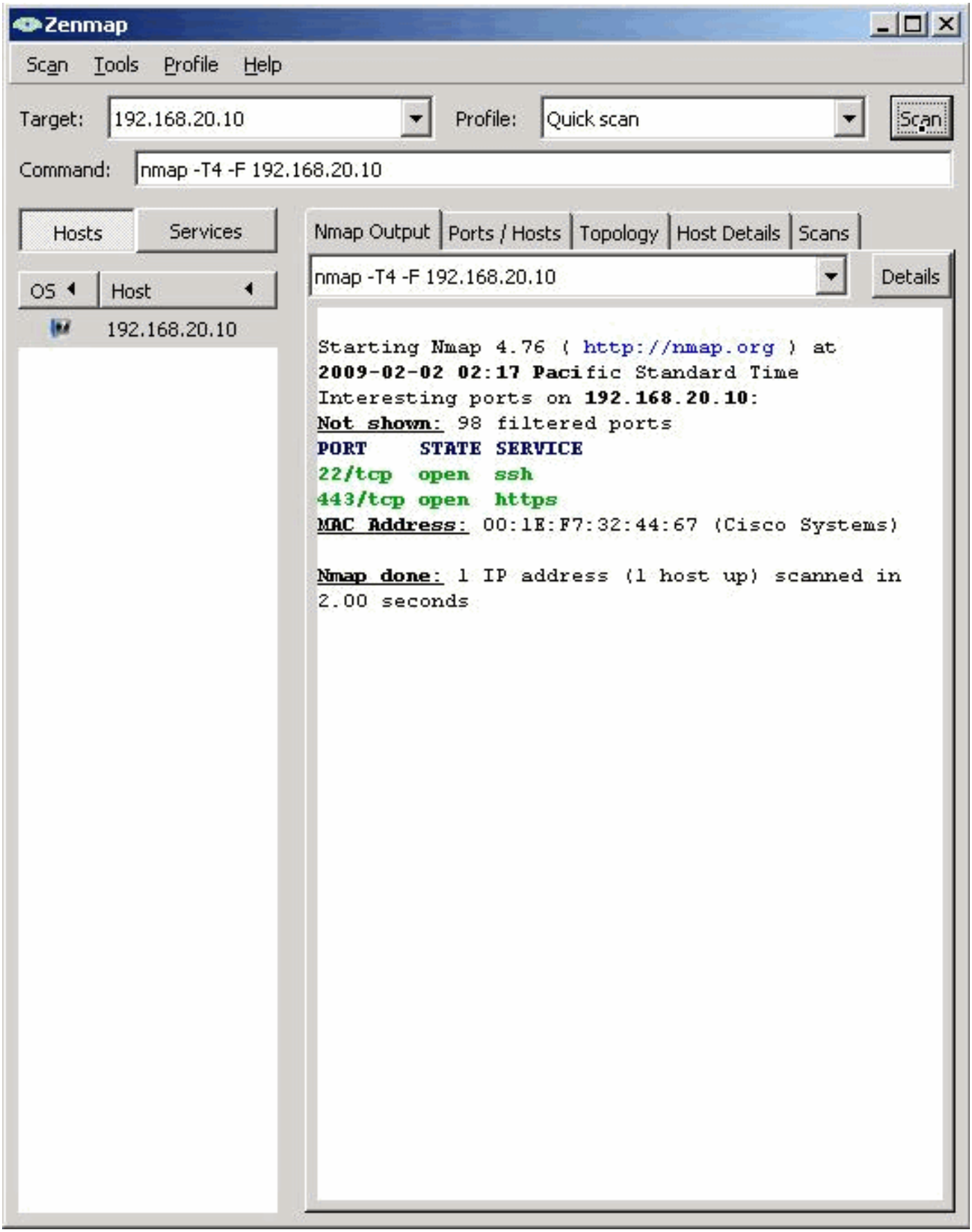


Entonces, por las políticas de seguridad de la compañía, se permite el resto del tráfico:



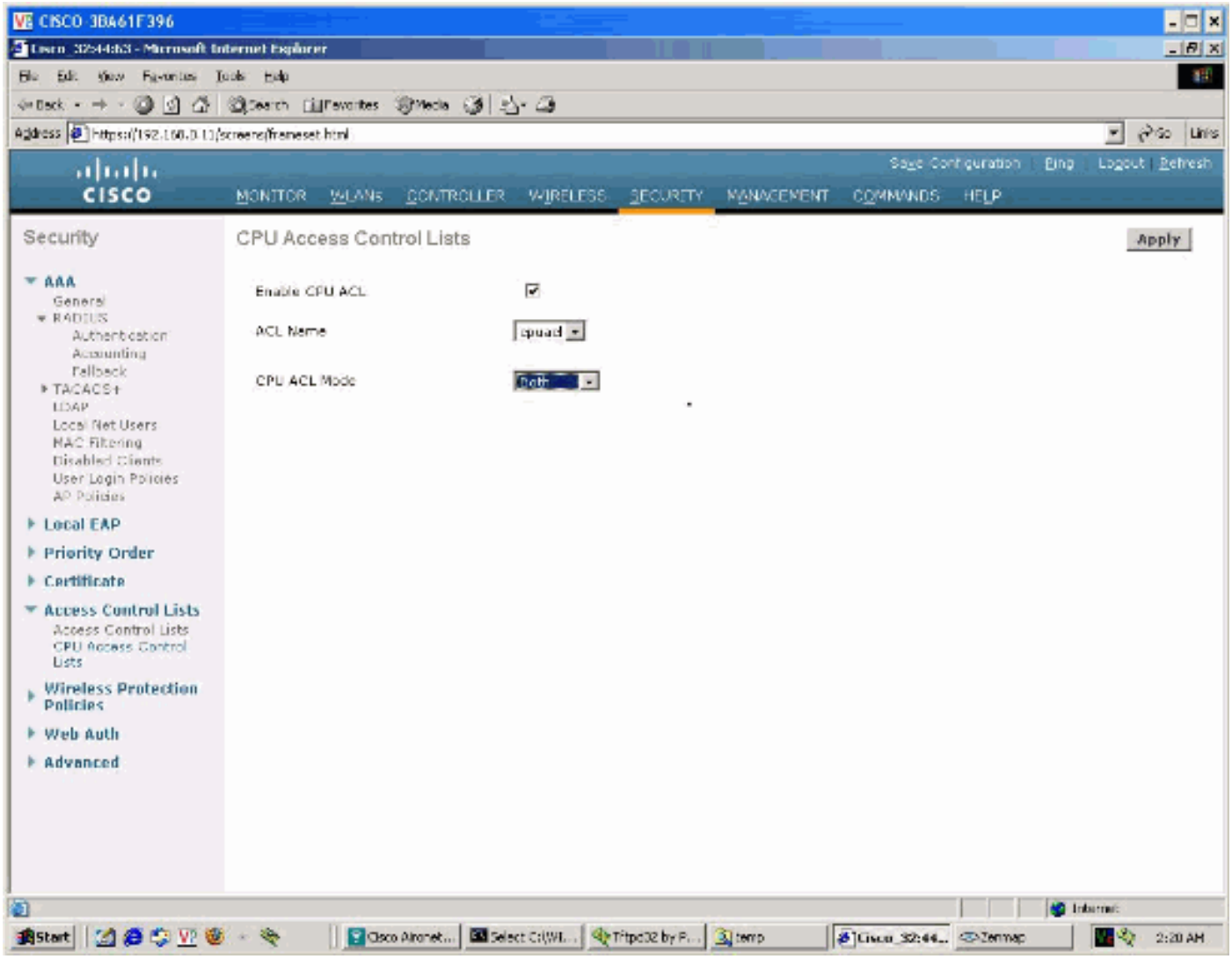
Prueba antes de CPU ACL

Para validar el efecto del CPU ACL, usted puede realizar un análisis rápido de un cliente de red inalámbrica asociado en el estatus EJECUTADO para ver los puertos abiertos actuales, sobre la base de la configuración, antes de aplicar el CPU ACL:



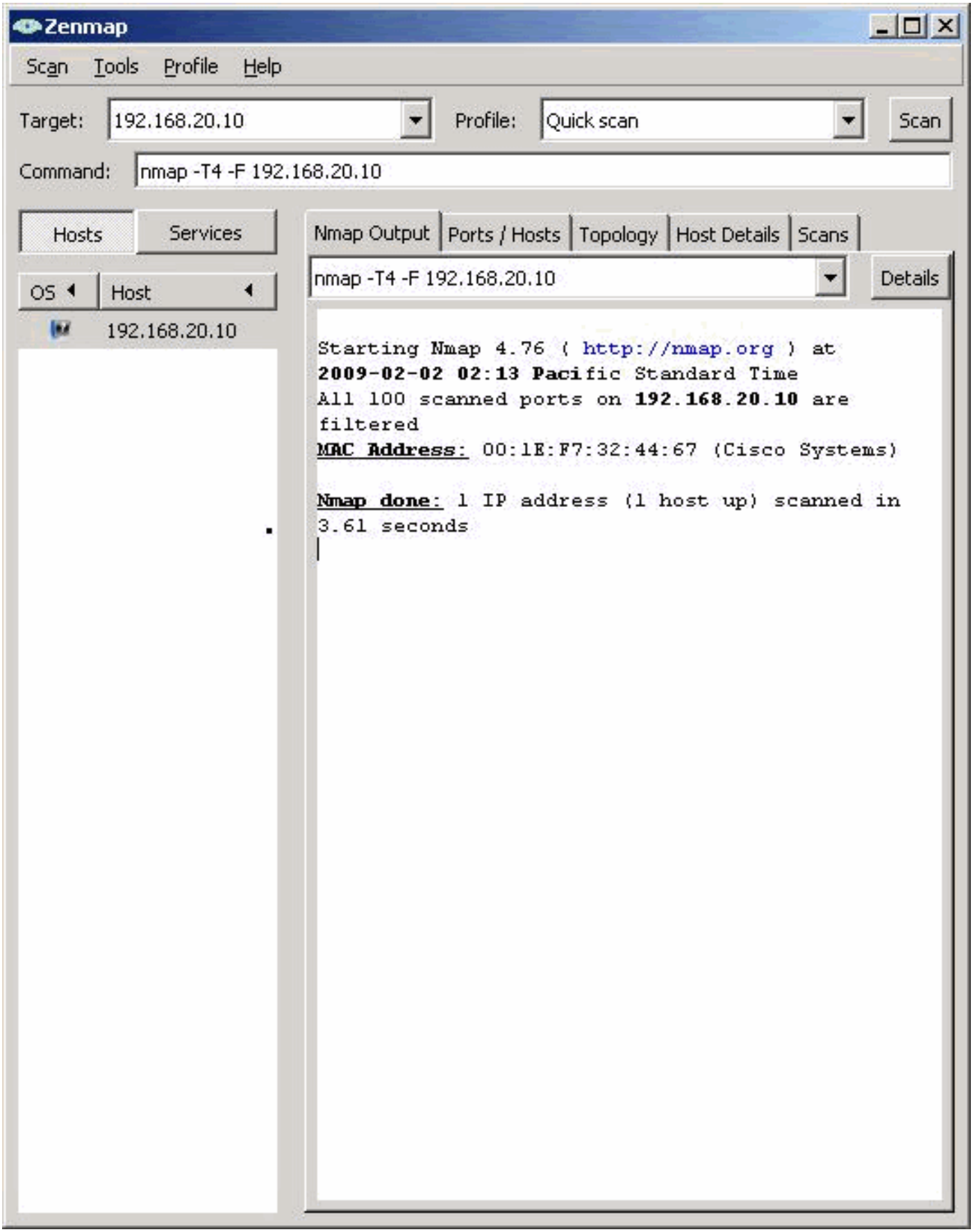
Prueba después del CPU ACL

Vaya a la **Seguridad > a la Administración > a la lista de control de acceso CPU**. Haga clic el **permiso CPU ACL**, y seleccione el ACL que fue creado previamente. Entonces, elija **ambos** como la dirección para asegurar esto se aplica para traficar de los clientes de red inalámbrica, y de los otros dispositivos en los VLA N de la interfaz dinámica:



Nota: No hay dirección para el tráfico CPU acl a partir del 7.0 hacia adelante para todas las Plataformas del WLC y solamente para WLC5500 en 6.0.

Ahora, si la misma exploración usada antes se relanza, todos los puertos del regulador se muestran según lo cerrado:



CPU estricto ACL

Si la demanda de las políticas de seguridad “niega ningunos” pues más reciente línea para una directiva, es importante entender que hay varios tipos de tráfico enviados entre el regulador en el mismo grupo de la movilidad para RRM, movilidad y otras tareas, y que usted puede ser que haga el tráfico proxied por el regulador a sí mismo para algunas operaciones, particularmente DHCP,

donde el regulador en el modo de representación del DHCP (el valor por defecto) puede generar el tráfico a sí mismo con el destino UDP 1067 para procesar.

Para una lista completa de puertos permitió por las reglas predeterminadas internas de la expedición, marcan la salida del comando **sh de las reglas**. El análisis de la lista completa está fuera del alcance de este documento.

Usted puede marcar qué reglas ACL están siendo golpeadas por el tráfico con el **comando start del contador acl de los config**. Los contadores se pueden visualizar con el comando **sh del detalle ACLNAME acl**.

Políticas del plano de control

Un aspecto de proteger un dispositivo de red, es aseegurarse que no está abrumado con más tráfico de administración que pueda procesar. En todos los reguladores, después del código 4.1, hay una limitación plana del control habilitada por abandono, que golpeará con el pie adentro si el tráfico para el CPU excede el 2 mbps.

En las redes ocupadas, es posible observar la limitación en efecto (por ejemplo, el monitor caído hace ping al CPU). La característica se puede controlar con el **comando rate avanzado los config**. Usted puede habilitar o inhabilitar solamente las, pero las tarifas no fijadas o contra qué tráfico actuará primero.

En los funcionamientos normales, se recomienda esto se va habilitado.

Encripción fuerte para el tráfico HTTP

Por abandono, el regulador ofrece ambas cifras altas y bajas de la fuerza para asegurar la compatibilidad con más viejos navegadores durante la configuración HTTPS. El regulador tiene disponible desde 40 bits RC4, 56 bits DES, hasta los bits AES 256. La selección de la cifra más fuerte es hecha por el navegador.

Para aseegurarse que solamente las cifras fuertes están utilizadas, usted puede habilitarlos con **comando enable de la cifra-opción del secureweb de la red de los config el alto**, tan los solamente 168 3DES o el 128 AES y longitudes más altas de la cifra son ofrecidas por el regulador en el acceso de la administración de HTTPS.

Control de sesión

Configuraciones del telnet/SSH

Por abandono, el regulador permite un máximo de 5 usuarios concurrentes, con un descanso de 5 minutos. Es crítico que estos valores están configurados adecuadamente en su entorno, pues la determinación de ellos a ilimitado (cero) puede abrir la puerta en la negación de servicio potencial contra los reguladores, si los usuarios intentaran un ataque de fuerza bruta contra ellos. Éste es un ejemplo de las configuraciones predeterminadas:

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)..... 5
```

```
Maximum Number of CLI Sessions..... 5
```
Recuerde eso por el diseño, incluso si inhabilitan a la Administración sobre la Tecnología inalámbrica o la interfaz dinámica, un dispositivo puede todavía hacer una conexión SSH al regulador. Esto es un CPU que grava la tarea, y el WLC limita el número de sesiones simultáneas, y durante cuánto tiempo usando estos parámetros.

Los valores se pueden ajustar con el **comando sessions de los config**.

Puerto de consola

El puerto serial tiene un valor de agotamiento del tiempo separado, que se fija a 5 minutos por abandono, pero se cambia comúnmente a 0 (ilimitado) durante las sesiones de Troubleshooting.

```
Cisco Controller) >show serial

Serial Port Login Timeout (minutes)..... 5
Baud Rate.............................. 9600
Character Size......................... 8
Flow Control:.......................... Disable
Stop Bits.............................. 1
Parity Type:........................... none
```
Es recomendable utilizar el valor por defecto de 5 minutos. Esto previene cualquier persona que tiene acceso físico al regulador para tener el acceso administrativo, en caso de que un usuario autenticado en el puerto de la consola deje la sesión abierta. Los valores se pueden ajustar con el **comando serial de los config**.

Juntando todos

Después de marcar el diverso aspecto de asegurar un WLC, esto puede ser resumida:

- Es importante prevenir los dispositivos con excepción de las estaciones de administración melladas para acceder el WLC, no sólo inhabilitando los protocolos NON-usados, pero también limitando el acceso en la capa 4/layer 3 con CPU ACL.
- La limitación de la tarifa debe ser habilitada (está por abandono).
- El acceso que controla a través de la **Administración sobre los comandos x** no es bastante para las instalaciones seguras, pues los usuarios todavía pueden los protocolos de la Administración de acceso que hablan directamente con el IP Address de administración, usando el CPU y los recursos de memoria.

Prácticas de la Seguridad

Aquí están algunas de las prácticas de la Seguridad:

- Cree el acceso de caída CPU ACL de todos los VLA N o redes secundarios de la interfaz dinámica. Sin embargo, permita el tráfico del DHCP al puerto de servidor (67) así que los clientes pueden obtener a la dirección negociada del DHCP si se habilita el proxy del DHCP (está por abandono). Si la interfaz dinámica tiene un IP Address público, se recomienda para tener regla ACL que niega todo el tráfico de las fuentes desconocidas al direccionamiento de la interfaz dinámica.
- Fije todas las reglas ACL como entrante o con la dirección, y marqúelas tan aplicadas como

ambos (opción atada con alambre y inalámbrica).Cómo validar:`(Cisco Controller) >show acl cpu`

```
CPU Acl Name.............................. acl1
Wireless Traffic.......................... Enabled
Wired Traffic............................. Enabled
```

- Limitación plana del control del permiso (se habilita por abandono).Cómo validar:`(Cisco Controller) >show advanced rate`

```
Control Path Rate Limiting.....................  Enabled
```

- Utilice siempre los protocolos cifrados de la Administración (HTTPS, SSH). Ésta es la configuración predeterminada para la Administración interactiva. Para el SNMP usted puede ser que necesite permitir al v3 para permitir el tráfico cifrado/autenticado SNMP. Recuerde recargar el regulador si usted realiza los cambios a la configuración SNMP.Éste es cómo validar:`(Cisco Controller) >show network summary`

```
RF-Network Name........................... 4400
Web Mode.................................. Disable
Secure Web Mode........................... Enable
Secure Web Mode Cipher-Option High........ Enable
Secure Web Mode Cipher-Option SSLv2....... Enable
Secure Shell (ssh)........................ Enable
Telnet.................................... Disable
...
```

- Encripción alta del permiso para el HTTPS (esto se inhabilita por abandono).
- Es una buena idea configurar un certificado de servidor validado para el acceso HTTPS a su regulador (firmado por su CA de confianza), substituyendo el certificado firmado del uno mismo instalado por abandono.
- Fije el descanso de la sesión y de la consola a 5 minutos.`(Cisco Controller) >show serial`

```
Serial Port Login Timeout (minutes)..... 5
Baud Rate................................ 9600
Character Size........................... 8
Flow Control:............................ Disable
Stop Bits................................ 1
Parity Type:............................. none
```

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)............ 5
Maximum Number of CLI Sessions......... 5
```

Información Relacionada

- Lightweight Access Point FAQ
- Preguntas Frecuentes sobre el Troubleshooting de los Controladores de WAN Inalámbricos (WLC)
- Preguntas y Respuestas del Módulo Cisco Wireless LAN Controller
- Administración de Recursos de Radio en Redes Inalámbricas Unificadas
- Soporte Técnico y Documentación - Cisco Systems