Guía de integración de IPS y controlador de LAN inalámbrica

Contenido

Introducción

El sistema Cisco Unified Intrusion Detection System (IDS)/Intrusion Prevention (IPS) forma parte de Cisco Self-Defending Network y es la primera solución de seguridad alámbrica e inalámbrica cableada de la industria. Cisco Unified IDS/IPS adopta un enfoque integral de la seguridad, en el perímetro inalámbrico, en el perímetro de la red por cable, en el perímetro de la WAN y a través del Data Center. Cuando un cliente asociado envía tráfico malintencionado a través de Cisco Unified Wireless Network, un dispositivo IDS con cables de Cisco detecta el ataque y envía solicitudes de rechazo a Cisco Wireless LAN Controllers (WLC), que luego desasocia el dispositivo cliente.

Cisco IPS es una solución en línea basada en la red, diseñada para identificar, clasificar y detener

con precisión el tráfico malintencionado, incluidos gusanos, spyware/adware, virus de red y abuso de aplicaciones, antes de que afecte a la continuidad empresarial.

Con la utilización de la versión 5 del software Cisco IPS Sensor, la solución Cisco IPS combina servicios de prevención en línea con tecnologías innovadoras para mejorar la precisión. El resultado es una confianza total en la protección proporcionada de su solución IPS, sin el temor de que se interrumpa el tráfico legítimo. La solución Cisco IPS también ofrece una protección completa de su red gracias a su capacidad exclusiva de colaborar con otros recursos de seguridad de la red y proporciona un enfoque proactivo para la protección de su red.

La solución Cisco IPS ayuda a los usuarios a detener más amenazas con mayor confianza mediante el uso de estas funciones:

- **Tecnologías de prevención en línea precisas**: proporciona una confianza incomparable para tomar medidas preventivas frente a una gama más amplia de amenazas sin el riesgo de descartar el tráfico legítimo. Estas tecnologías únicas ofrecen un análisis contextual inteligente, automatizado y automatizado de sus datos y ayudan a garantizar que se saca el máximo partido de su solución de prevención de intrusiones.
- **Identificación de amenazas multivectoriales**: protege su red de violaciones de políticas, vulnerabilidades y actividades anómalas mediante una inspección detallada del tráfico en las capas 2 a 7.
- **Colaboración de red única**: mejora la escalabilidad y la resistencia mediante la colaboración de red, incluidas técnicas de captura de tráfico eficientes, capacidades de equilibrio de carga y visibilidad del tráfico cifrado.
- **Soluciones de implementación integrales**: proporciona soluciones para todos los entornos, desde pequeñas y medianas empresas (PYMES) y ubicaciones de sucursales hasta instalaciones de grandes empresas y proveedores de servicios.
- **Potente administración, correlación de eventos y servicios de soporte**: permite una solución completa, que incluye configuración, gestión, correlación de datos y servicios de soporte avanzados. En concreto, el sistema de supervisión, análisis y respuesta de seguridad (MARS) de Cisco identifica, aísla y recomienda la eliminación precisa de los elementos infractores para una solución de prevención de intrusiones en toda la red. Además, Cisco Incident Control System evita nuevos brotes de virus y gusanos al permitir que la red se adapte rápidamente y proporcione una respuesta distribuida.

Cuando se combinan, estos elementos proporcionan una solución de prevención en línea completa y le proporcionan la confianza necesaria para detectar y detener la gama más amplia de tráfico malintencionado antes de que afecte a la continuidad empresarial. La iniciativa Cisco Self-Defending Network exige una seguridad integrada e integrada para las soluciones de red. Los sistemas WLAN basados en el protocolo de punto de acceso ligero (LWAPP) actuales sólo admiten funciones IDS básicas debido al hecho de que es esencialmente un sistema de capa 2 y tiene una potencia de procesamiento de línea limitada. Cisco publica el nuevo código de forma oportuna para incluir nuevas funciones mejoradas en los nuevos códigos. La versión 4.0 tiene las últimas funciones que incluyen la integración de un sistema WLAN basado en LWAPP con la línea de productos Cisco IDS/IPS. En esta versión, el objetivo es permitir que el sistema IDS/IPS de Cisco ordene a los WLC que bloqueen el acceso de ciertos clientes a las redes inalámbricas cuando se detecta un ataque desde la Capa 3 hasta la Capa 7 que involucra al cliente en consideración.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos mínimos:

- Versión 4.x y posterior del firmware del WLC
- Es deseable saber cómo configurar Cisco IPS y Cisco WLC.

Componentes Utilizados

WLC de Cisco

Estos controladores se incluyen con la versión de software 4.0 para las modificaciones de IDS:

- WLC de las Cisco 2000 Series
- WLC de las Cisco 2100 Series
- WLC de las Cisco 4400 Series
- Módulo de servicios inalámbricos de Cisco (WiSM)
- Switch de acceso unificado Cisco Catalyst serie 3750G
- Módulo de controlador de LAN inalámbrica de Cisco (WLCM)

Puntos de acceso

- Puntos de acceso ligeros Cisco Aironet serie 1100 AG
- Puntos de acceso ligeros Cisco Aironet serie 1200 AG
- Puntos de acceso ligeros Cisco Aironet serie 1300
- Puntos de acceso ligeros Cisco Aironet serie 1000

Administración

- Cisco Wireless Control System (WCS)
- Sensor de la serie Cisco 4200
- Gestión de Cisco IDS - Cisco IDS Device Manager (IDM)

Plataformas Cisco Unified IDS/IPS

- Sensores Cisco IPS serie 4200 con Cisco IPS Sensor Software 5.x o posterior.
- SSM10 y SSM20 para los dispositivos de seguridad adaptable Cisco ASA serie 5500 con Cisco IPS Sensor Software 5.x
- Dispositivos de seguridad adaptable Cisco ASA serie 5500 con el software Cisco IPS Sensor 5.x
- Cisco IDS Network Module (NM-CIDS) con Cisco IPS Sensor Software 5.x
- Módulo 2 del sistema de detección de intrusiones Cisco Catalyst serie 6500 (IDSM-2) con el software de sensor Cisco IPS 5.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

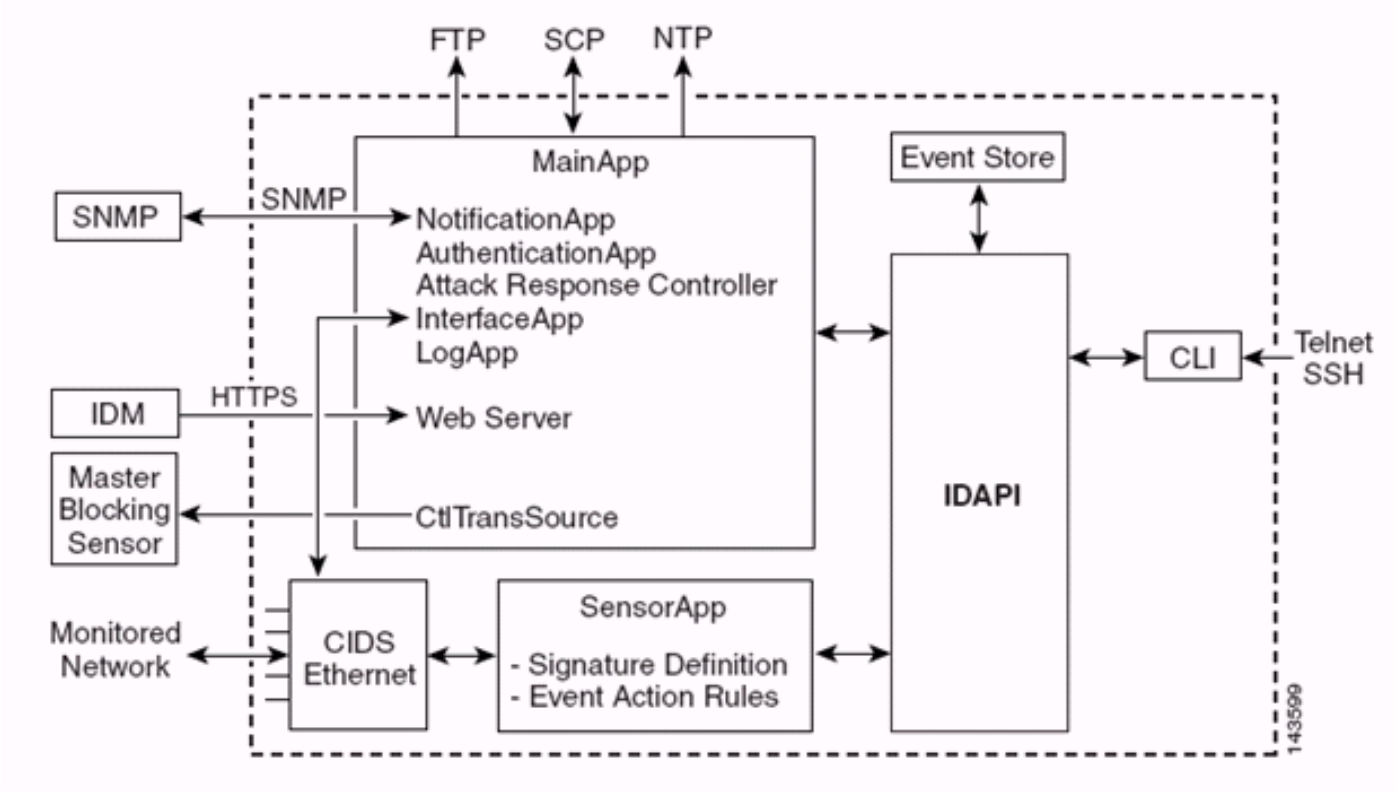
Convenciones

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

Descripción general de Cisco IDS

Los principales componentes de Cisco IDS (versión 5.0) son:

- **Aplicación Sensor**: realiza la captura y el análisis de paquetes.
- **Event Storage Management and Actions Module**: proporciona almacenamiento de violaciones de políticas.
- **Imaging, Install and Startup Module**: carga, inicializa e inicia todo el software del sistema.
- **Interfaces de usuario y Módulo de soporte de interfaz de usuario**: proporciona una CLI integrada y la IDM.
- **Sensor OS**: sistema operativo host (basado en Linux).



La aplicación Sensor (software IPS) consta de:

- **Aplicación principal**: Inicializa el sistema, inicia y detiene otras aplicaciones, configura el sistema operativo y es responsable de las actualizaciones. Contiene estos componentes:**Control Transaction Server**: permite a los sensores enviar transacciones de control que se utilizan para habilitar la función Sensor de bloqueo maestro del controlador de respuesta de ataques (anteriormente conocido como controlador de acceso a la red).**Event Store**: almacén indexado que se utiliza para almacenar eventos IPS (errores, estado y mensajes del sistema de alerta) al que se puede acceder a través de CLI, IDM, Adaptive Security Device Manager (ASDM) o Remote Data Exchange Protocol (RDEP).
- **Aplicación de interfaz**: gestiona la omisión y la configuración física y define las interfaces emparejadas. La configuración física consta de los estados de velocidad, dúplex y administrativo.
- **Aplicación de registro**: escribe los mensajes de registro de la aplicación en el archivo de registro y los mensajes de error en el almacén de eventos.
- **Atack Response Controller (ARC) (anteriormente conocido como Network Access Controller)**: gestiona dispositivos de red remotos (firewalls, routers y switches) para proporcionar

funciones de bloqueo cuando se produce un evento de alerta. ARC crea y aplica listas de control de acceso (ACL) en el dispositivo de red controlado o utiliza el comando **shun** (firewalls).
- **Aplicación de notificación**: envía trampas SNMP cuando se activan por una alerta, estado y eventos de error. La Aplicación de notificación utiliza un agente SNMP de dominio público para esto. Los GET SNMP proporcionan información sobre el estado de un Sensor.**Servidor Web (servidor HTTP RDEP2)**: proporciona una interfaz de usuario Web. También proporciona un medio para comunicarse con otros dispositivos IPS a través de RDEP2 usando varios servlets para proporcionar servicios IPS.**Aplicación de autenticación**: verifica que los usuarios estén autorizados para realizar acciones CLI, IDM, ASDM o RDEP.
- **Aplicación Sensor (Analysis Engine)**: realiza la captura y el análisis de paquetes.
- **CLI**: la interfaz que se ejecuta cuando los usuarios inician sesión con éxito en el sensor a través de Telnet o SSH. Todas las cuentas creadas a través de la CLI utilizan la CLI como su shell (excepto la cuenta de servicio: sólo se permite una cuenta de servicio). Los comandos CLI permitidos dependen del privilegio del usuario.

Todas las aplicaciones IPS se comunican entre sí a través de una interfaz de programa de aplicaciones (API) común denominada IDAPI. Las aplicaciones remotas (otros sensores, aplicaciones de gestión y software de terceros) se comunican con los sensores mediante los protocolos RDEP2 y Security Device Event Exchange (SDEE).

Debe tenerse en cuenta que el Sensor tiene estas particiones de disco:

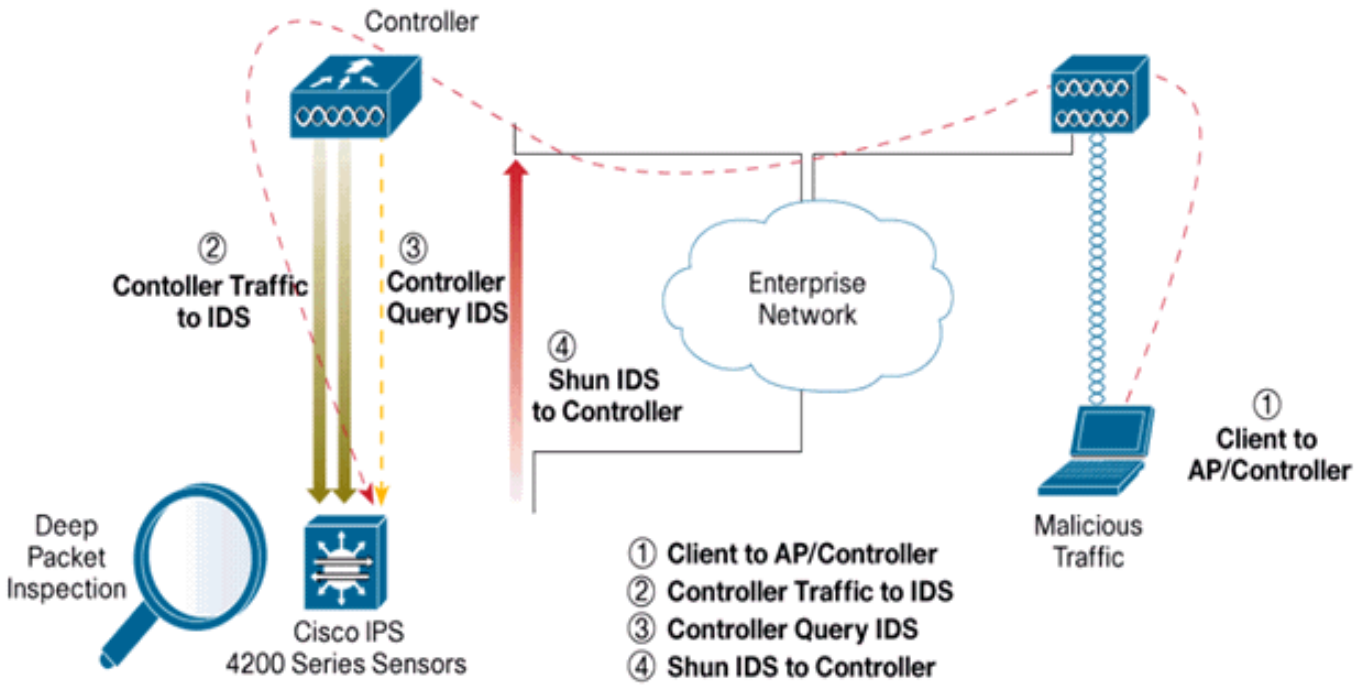
- **Partición de aplicación**: contiene la imagen completa del sistema IPS.
- **Partición de mantenimiento**: imagen IPS de propósito especial utilizada para recrear la imagen de la partición de aplicación del IDSM-2. Una nueva imagen de la partición de mantenimiento produce una pérdida de configuración.
- **Partición de recuperación**: imagen de propósito especial utilizada para la recuperación del sensor. El inicio en la partición de recuperación permite a los usuarios recrear completamente la partición de la aplicación. Los parámetros de red se conservan, pero se pierden todas las demás configuraciones.

Cisco IDS y WLC - Descripción general de la integración

La versión 5.0 de Cisco IDS introduce la capacidad de configurar acciones de denegación cuando se detectan violaciones de políticas (firmas). Según la configuración del usuario en el sistema IDS/IPS, se puede enviar una solicitud de rechazo a un firewall, router o WLC para bloquear los paquetes de una dirección IP determinada.

Con Cisco Unified Wireless Network Software Release 4.0 para Cisco Wireless Controllers, se debe enviar una solicitud de rechazo a un WLC para activar el comportamiento de exclusión o lista negra del cliente disponible en un controlador. La interfaz que utiliza el controlador para obtener la solicitud shun es la interfaz de comando y control en el Cisco IDS.

- El controlador permite configurar hasta cinco sensores IDS en un controlador determinado.
- Cada sensor IDS configurado se identifica por su dirección IP o por el nombre de red calificado y las credenciales de autorización.
- Cada sensor IDS se puede configurar en un controlador con una velocidad de consulta única en segundos.



Reducción de IDS

El controlador consulta al Sensor a la velocidad de consulta configurada para recuperar todos los eventos shun. Una solicitud de rechazo dada se distribuye en todo el grupo de movilidad del controlador que recupera la solicitud del sensor IDS. Cada solicitud de rechazo para una dirección IP del cliente está en vigor para el valor de segundos de tiempo de espera especificado. Si el valor de tiempo de espera indica un tiempo infinito, el evento shun finaliza sólo si la entrada shun se elimina en el IDS. El estado del cliente evitado se mantiene en cada controlador del grupo de movilidad incluso si se reinicia alguno o todos los controladores.

Nota: La decisión de rechazar un cliente siempre la toma el sensor IDS. El controlador no detecta ataques de Capa 3. Se trata de un proceso mucho más complicado para determinar que el cliente está iniciando un ataque malicioso en la capa 3. El cliente se autentica en la Capa 2, lo cual es suficientemente bueno para que el controlador conceda acceso de Capa 2.

Nota: Por ejemplo, si a un cliente se le asigna una dirección IP ofensiva anterior (rechazada), el tiempo de espera del sensor depende de que se desbloquee el acceso de Capa 2 para este nuevo cliente. Incluso si el controlador da acceso en la Capa 2, el tráfico del cliente podría ser bloqueado en los routers en la Capa 3 de todos modos, porque el Sensor también informa a los routers del evento shun.

Suponga que un cliente tiene la dirección IP A. Ahora, cuando el controlador sondea el IDS para los eventos shun, el IDS envía la solicitud shun al controlador con la dirección IP A como la dirección IP de destino. Ahora, el controlador negro enumera este cliente A. En el controlador, los clientes se desactivan en función de una dirección MAC.

Ahora, supongamos que el cliente cambia su dirección IP de A a B. Durante la siguiente encuesta, el controlador obtiene una lista de clientes rechazados basada en la dirección IP. De nuevo, la dirección IP A sigue en la lista rechazada. Pero como el cliente ha cambiado su dirección IP de A a B (que no está en la lista rechazada de direcciones IP), este cliente con una nueva dirección IP de B se libera una vez que se alcanza el tiempo de espera de los clientes de lista negra en el controlador. Ahora, el controlador comienza a permitir a este cliente con la nueva

dirección IP de B (pero la dirección MAC del cliente sigue siendo la misma).

Por lo tanto, aunque un cliente permanece inhabilitado durante el tiempo de exclusión del controlador y se vuelve a excluir si vuelve a adquirir su dirección DHCP anterior, ese cliente ya no se inhabilita si cambia la dirección IP del cliente que se rechaza. Por ejemplo, si el cliente se conecta a la misma red y el tiempo de espera de concesión DHCP no caduca.

Los controladores sólo soportan la conexión con el IDS para las solicitudes de rechazo del cliente que utilizan el puerto de administración en el controlador. El controlador se conecta al IDS para la inspección de paquetes a través de las interfaces VLAN aplicables que transportan tráfico de cliente inalámbrico.

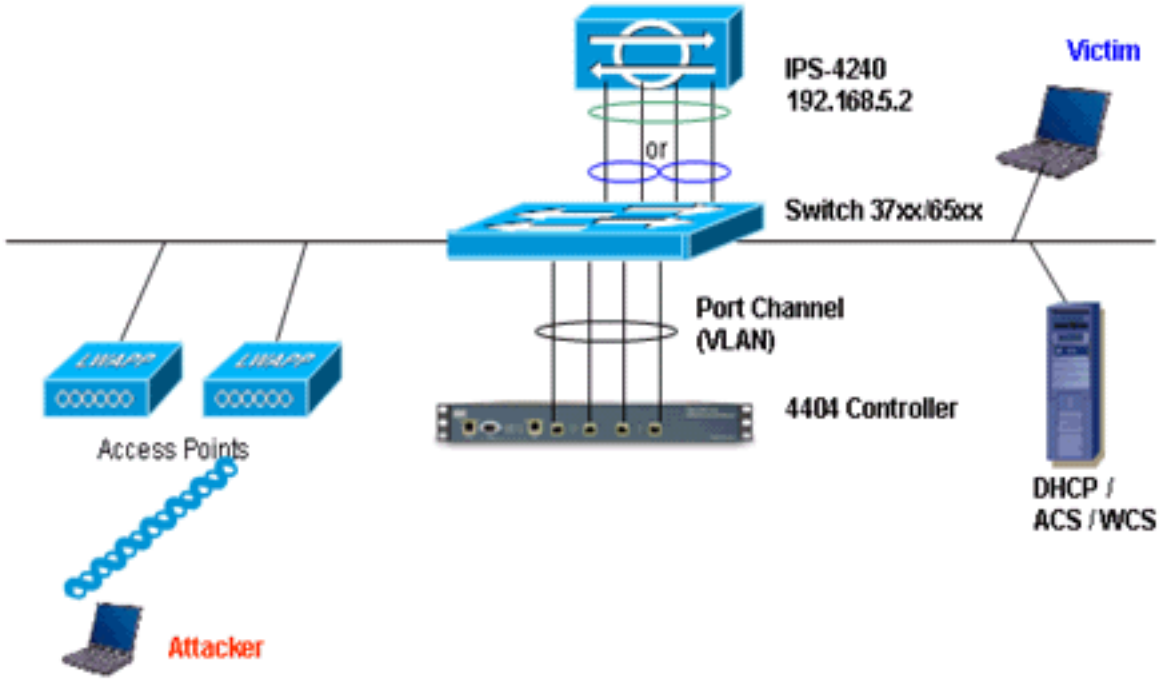
En el controlador, la página Deshabilitar clientes muestra cada cliente que se ha inhabilitado a través de una solicitud de sensor IDS. El comando **show** CLI también muestra una lista de clientes en la lista negra.

En WCS, los clientes excluidos se muestran en la subficha Seguridad.

Estos son los pasos a seguir para completar la integración de Cisco IPS Sensors y Cisco WLC.

1. Instale y conecte el dispositivo IDS en el mismo switch donde reside el controlador inalámbrico.
2. Refleje (SPAN) los puertos WLC que llevan el tráfico del cliente inalámbrico al dispositivo IDS.
3. El dispositivo IDS recibe una copia de cada paquete e inspecciona el tráfico de la capa 3 a la 7.
4. El dispositivo IDS ofrece un archivo de firma descargable, que también se puede personalizar.
5. El dispositivo IDS genera la alarma con una acción de evento de rechazo cuando se detecta una firma de ataque.
6. El WLC sondea el IDS para las alarmas.
7. Cuando se detecta una alarma con la dirección IP de un cliente inalámbrico, que está asociado al WLC, coloca al cliente en la lista de exclusión.
8. El WLC genera una trampa y se notifica al WCS.
9. El usuario se elimina de la lista de exclusión después del período de tiempo especificado.

Diseño de arquitectura de red



El WLC de Cisco está conectado a las interfaces gigabit en el Catalyst 6500. Cree un canal de puerto para las interfaces gigabit y habilite la agregación de enlaces (LAG) en el WLC.

```
(Cisco Controller) >show interface summary

Interface Name                    Port  Vlan Id   IP Address       Type     Ap Mgr
--------------------------------  ----  --------  ---------------  -------  ------
ap-manager                        LAG   untagged  10.10.99.3       Static   Yes
management                        LAG   untagged  10.10.99.2       Static   No
service-port                      N/A   N/A       192.168.1.1      Static   No
virtual                           N/A   N/A       1.1.1.1          Static   No
vlan101                           LAG   101       10.10.101.5      Dynamic  No
```

El controlador está conectado a la interfaz gigabit 5/1 y gigabit 5/2 en el Catalyst 6500.

```
cat6506#show run interface gigabit 5/1
Building configuration...

Current configuration : 183 bytes
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
 channel-group 99 mode on
end

cat6506#show run interface gigabit 5/2
Building configuration...

Current configuration : 183 bytes
!
interface GigabitEthernet5/2
 switchport
```

```
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
 channel-group 99 mode on
end

cat6506#show run interface port-channel 99
Building configuration...

Current configuration : 153 bytes
!
interface Port-channel99
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
end
```

Las interfaces de detección del sensor IPS pueden funcionar individualmente en el **modo Promiscuo** o puede emparejarlas para crear interfaces en línea para el **modo de detección en línea**.

En el modo Promiscuous, los paquetes no fluyen a través del Sensor. El sensor analiza una copia del tráfico monitoreado en lugar del paquete reenviado real. La ventaja de funcionar en modo Promiscuous es que el Sensor no afecta el flujo de paquetes con el tráfico reenviado.

Nota: El diagrama de arquitectura es sólo un ejemplo de configuración de la arquitectura integrada WLC e IPS. El ejemplo de configuración que se muestra aquí explica la interfaz de detección de IDS que actúa en modo Promiscuo. El diagrama de arquitectura muestra las interfaces de detección que se emparejan para actuar en el modo Par en línea. Consulte Modo en línea para obtener más información sobre el modo de interfaz en línea.

En esta configuración, se asume que la interfaz de detección actúa en el modo Promiscuous. La interfaz de supervisión del sensor IDS de Cisco está conectada a la interfaz gigabit 5/3 en el Catalyst 6500. Cree una sesión de monitor en el Catalyst 6500 donde la interfaz de canal de puerto es el origen de los paquetes y el destino es la interfaz gigabit donde se conecta la interfaz de monitoreo del sensor Cisco IPS. Esto replica todo el tráfico de ingreso y egreso desde las interfaces cableadas del controlador al IDS para la inspección de Capa 3 a Capa 7.

```
cat6506#show run | inc monitor
monitor session 5 source interface Po99
monitor session 5 destination interface Gi5/3

cat6506#show monitor session 5
Session 5
---------
Type                   : Local Session
Source Ports           :
    Both               : Po99
Destination Ports      : Gi5/3
cat6506#
```

Configuración del sensor IDS de Cisco

La configuración inicial del sensor IDS de Cisco se realiza desde el puerto de la consola o conectando un monitor y un teclado al sensor.

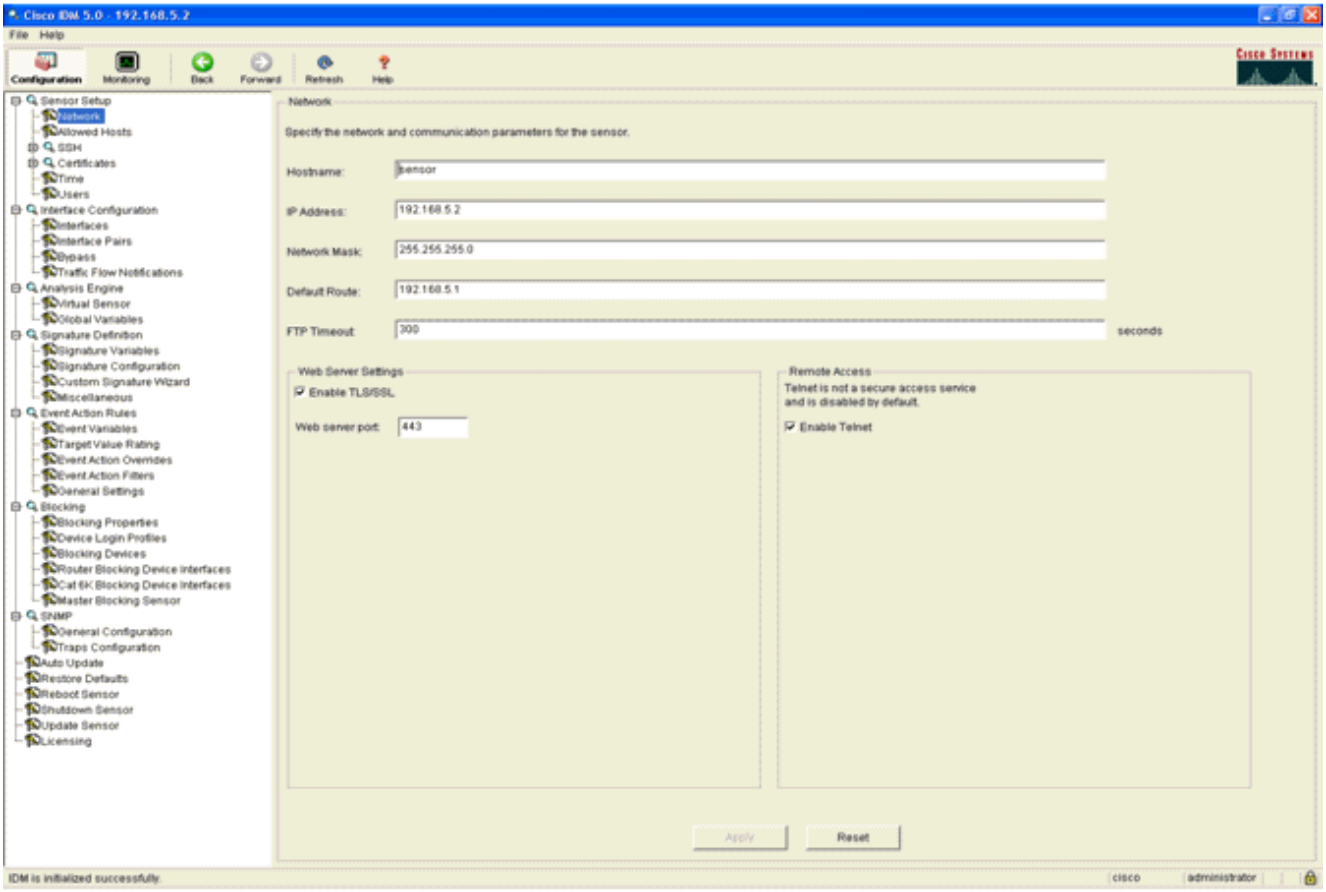
1. Inicie sesión en el dispositivo:Conecte un puerto de consola al sensor.Conecte un monitor y un teclado al sensor.
2. Escriba su nombre de usuario y contraseña en el mensaje de inicio de sesión.**Nota:** Tanto el nombre de usuario como la contraseña predeterminados son cisco. Se le solicitará que los cambie la primera vez que inicie sesión en el dispositivo. Primero debe introducir la contraseña de UNIX, que es cisco. A continuación, debe introducir la nueva contraseña dos veces.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute or
use encryption. importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws.
By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may
be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending
email to export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet (registered
customers only) to obtain a new license or install a license.
```

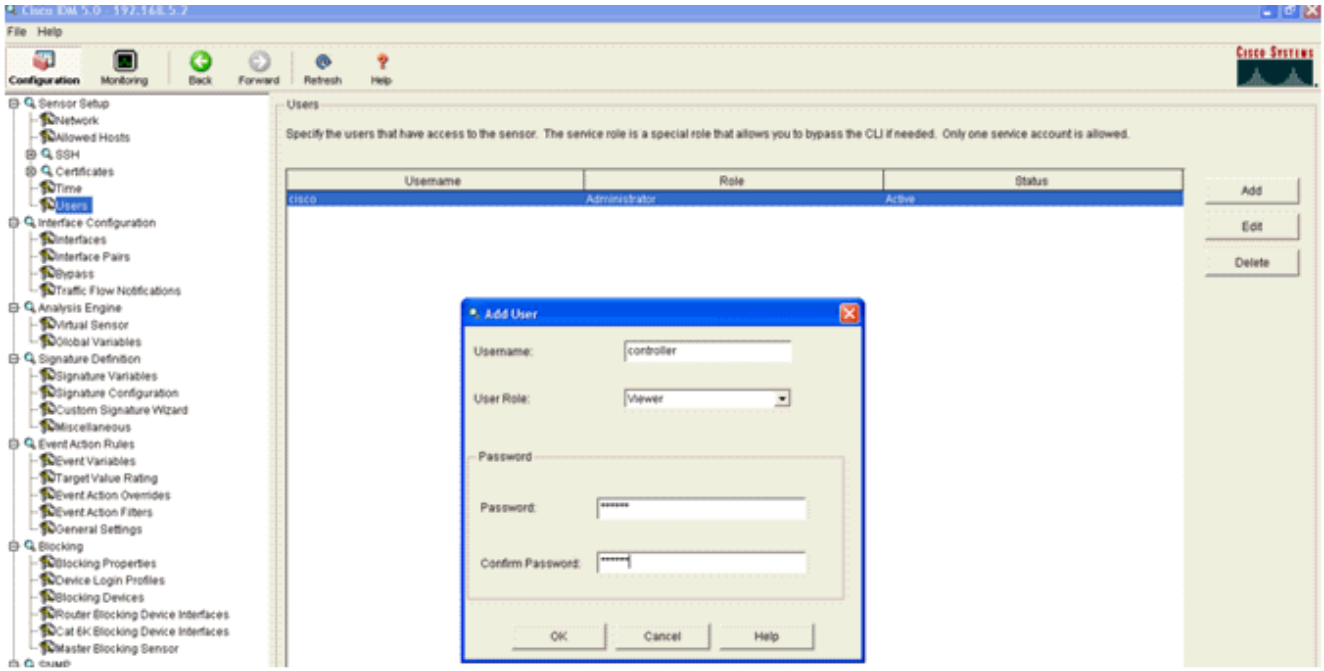
3. Configure la dirección IP, la máscara de subred y la lista de acceso en el sensor.**Nota:** Ésta es la interfaz de comando y control en el IDS utilizada para comunicarse con el controlador. Esta dirección debe ser enrutable a la interfaz de administración del controlador. Las interfaces de detección no requieren direccionamiento. La lista de acceso debe incluir la dirección de la interfaz de administración del controlador, así como las direcciones permitidas para la administración del IDS.

```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit
sensor(config-hos)#exit
Apply Changes:?[yes]: yes
sensor(config)#exit
sensor#
sensor#ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=1 ttl=255 time=0.9 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=255 time=1.0 ms
--- 192.168.5.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.6/1.0 ms
sensor#
```

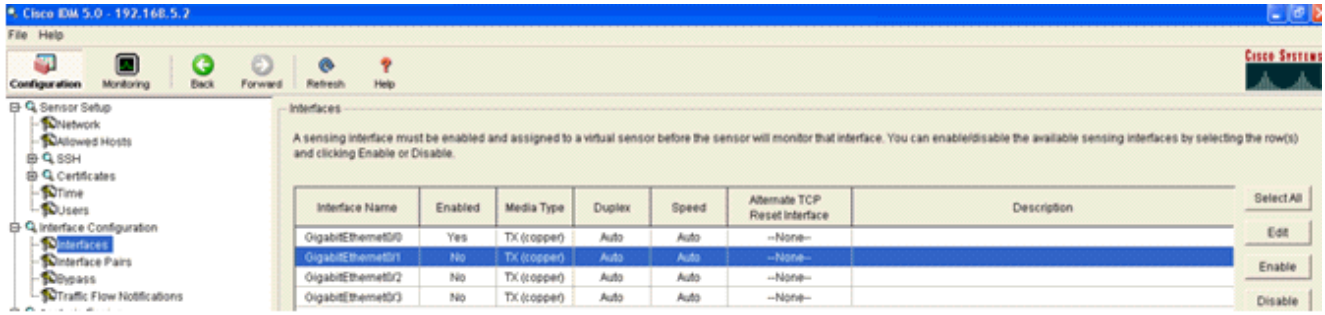
4. Ahora puede configurar el sensor IPS desde la GUI. Señale el explorador a la dirección IP de administración del sensor. Esta imagen muestra un ejemplo donde el Sensor está configurado con 192.168.5.2.



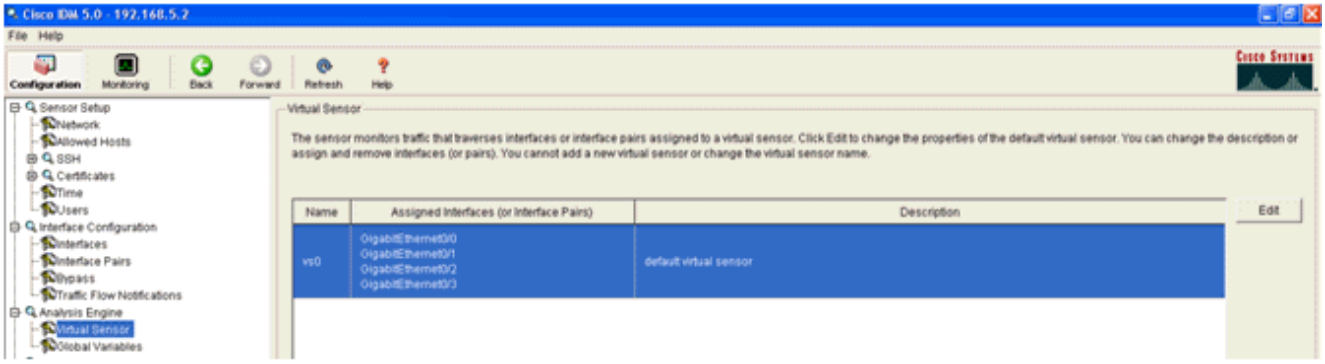
5. Agregue un usuario que el WLC utilice para acceder a los eventos del sensor IPS.



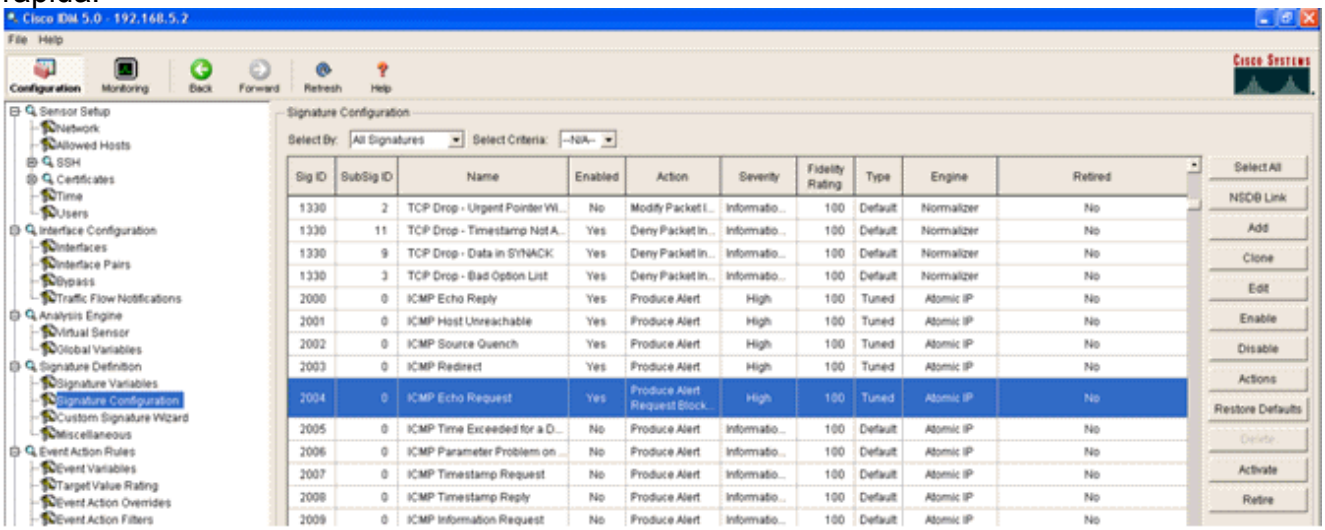
6. Habilite las interfaces de supervisión.



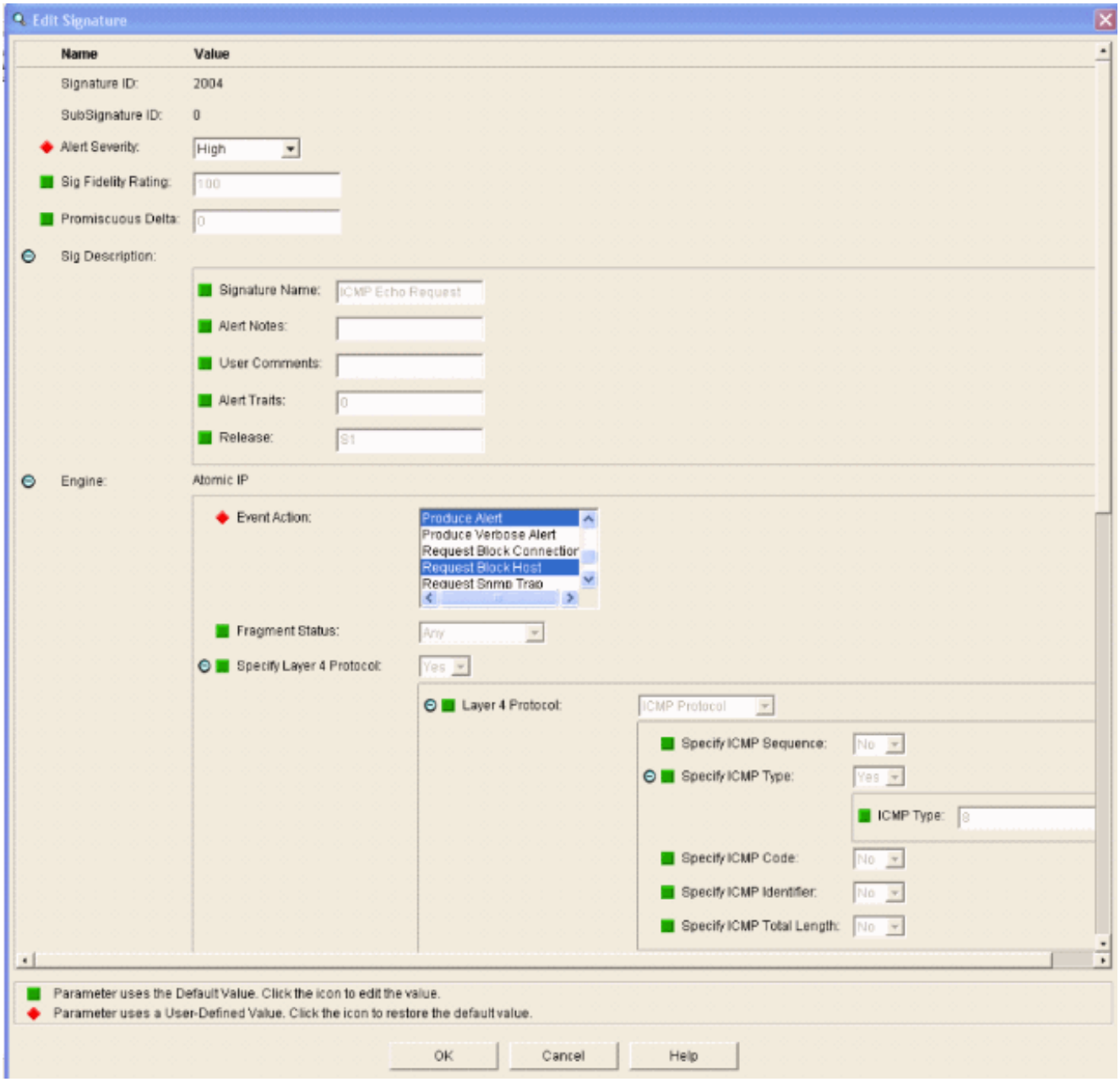
Las interfaces de supervisión se deben agregar al motor de análisis, como muestra esta ventana:



7. Seleccione la firma 2004 (Solicitud de eco ICMP) para realizar una verificación de configuración
rápida.



La firma debe estar habilitada, la gravedad de la alerta se establece en **Alto** y la acción del evento se establece en **Producir alerta** y **Solicitar bloque host** para que este paso de verificación se
complete.

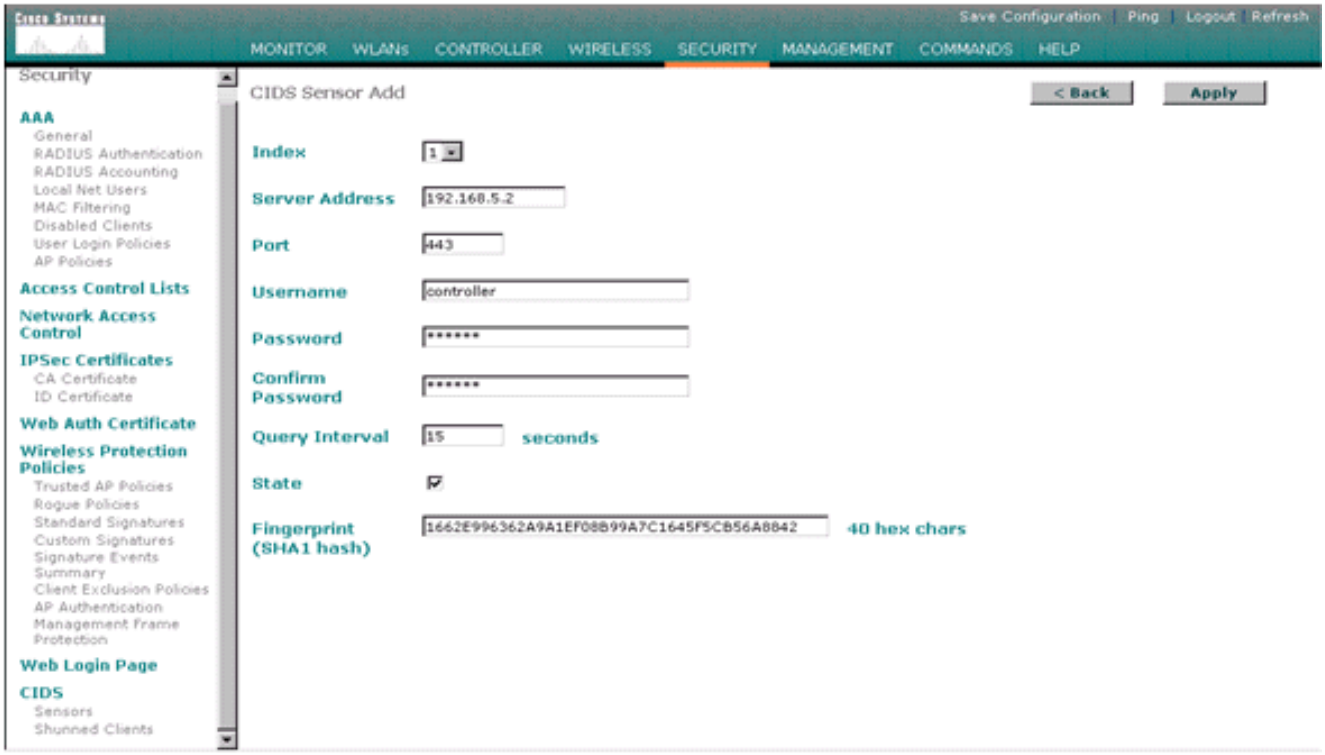


Configurar la WLC

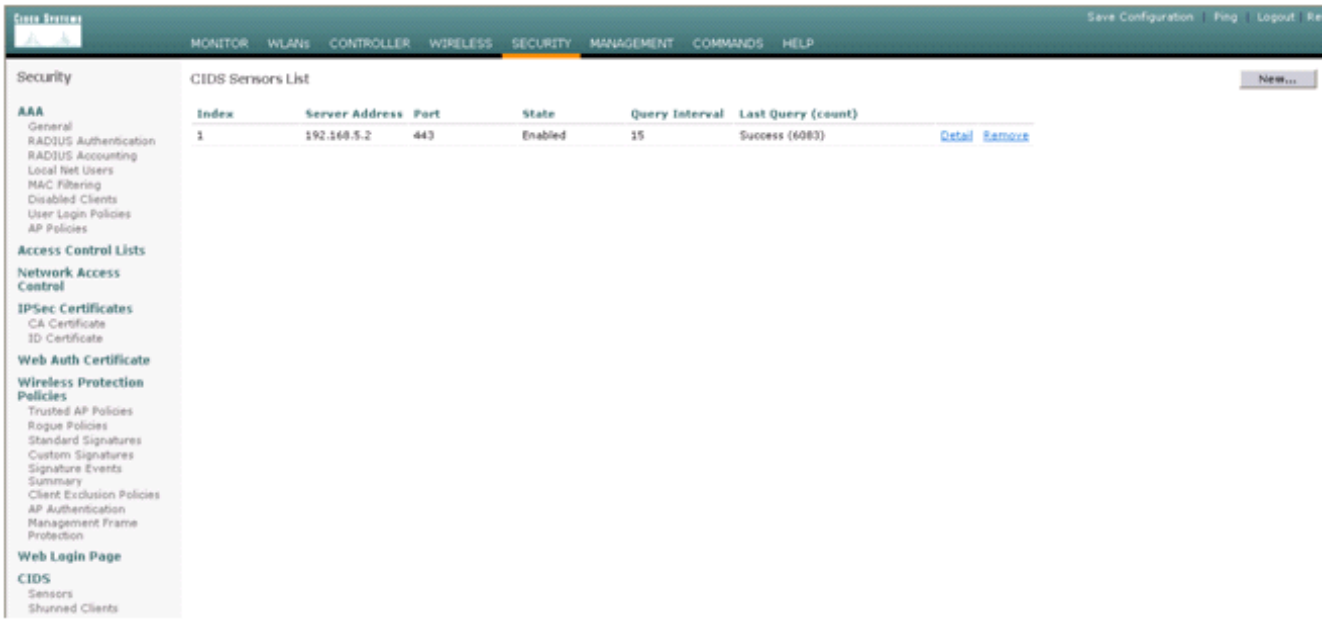
Complete estos pasos para configurar el WLC:

1. Una vez que el dispositivo IPS esté configurado y listo para ser agregado en el controlador, elija **Security > CIDS > Sensors > New**.
2. Agregue la dirección IP, el número de puerto TCP, el nombre de usuario y la contraseña que creó anteriormente.Para obtener la huella dactilar del sensor IPS, ejecute este comando en el sensor IPS y agregue la huella digital SHA1 en el WLC (sin los dos puntos). Esto se utiliza para asegurar la comunicación de sondeo de controlador a IDS.

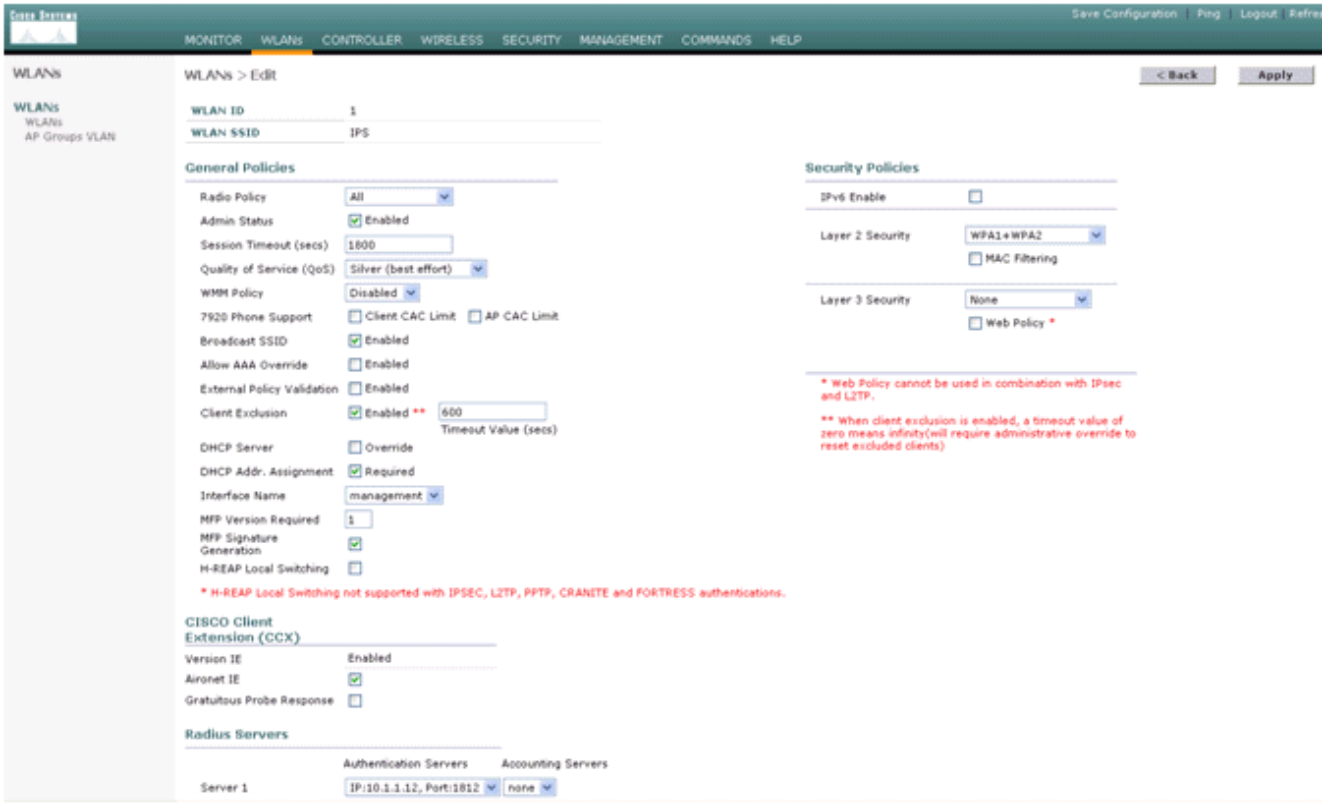
```
sensor#show tls fingerprint
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



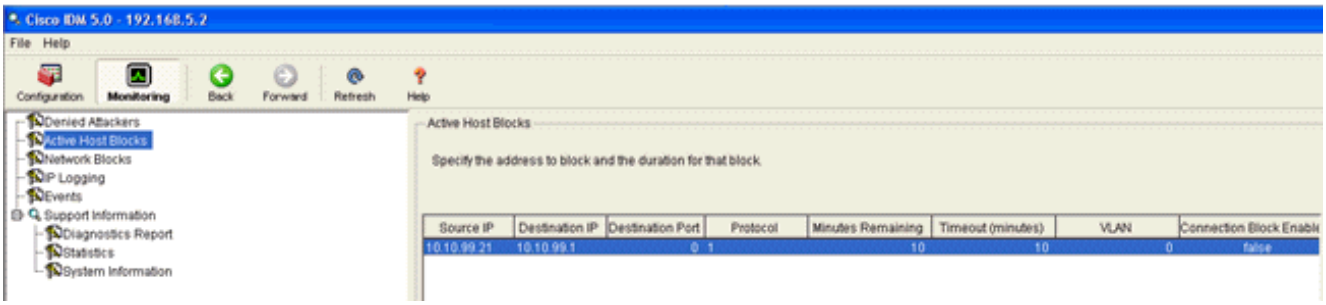
3. Verifique el estado de la conexión entre el sensor IPS y el WLC.



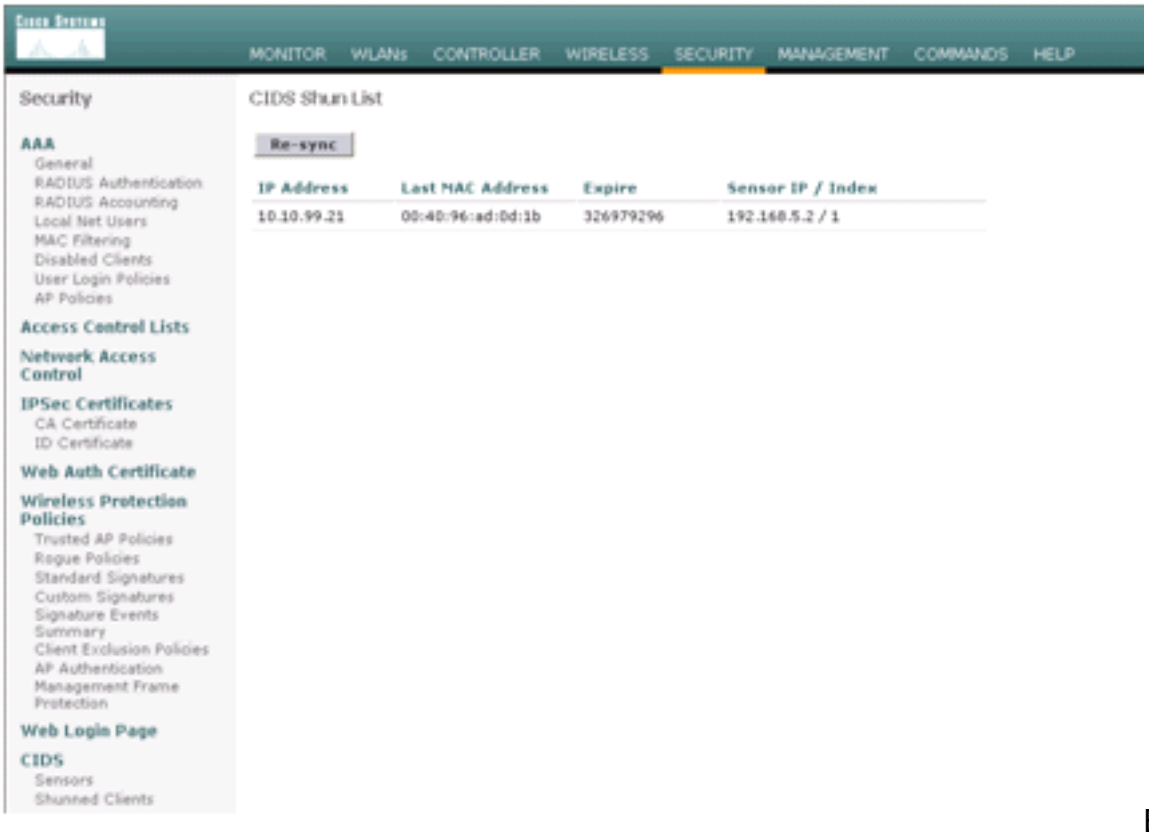
4. Una vez que establezca la conectividad con el sensor de Cisco IPS, asegúrese de que la configuración de WLAN sea correcta y de que habilite **la exclusión de cliente**.El valor predeterminado del tiempo de espera de exclusión del cliente es de 60 segundos. Tenga en cuenta también que independientemente del temporizador de exclusión del cliente, la exclusión del cliente persiste mientras el bloque del cliente invocado por el IDS permanezca activo. El tiempo de bloqueo predeterminado en el IDS es de 30 minutos.



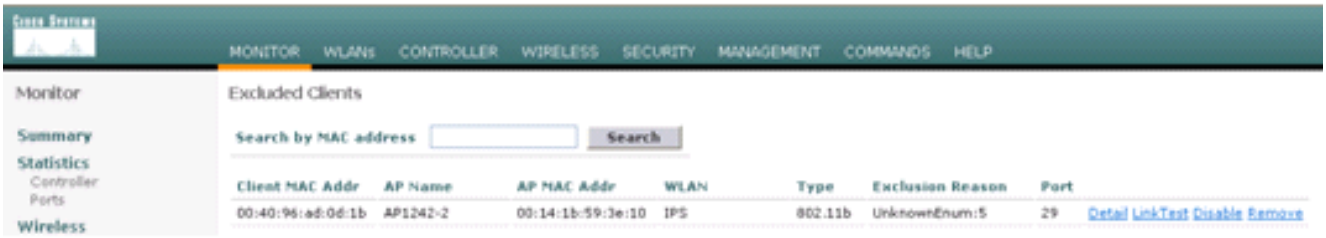
5. Puede activar un evento en el sistema Cisco IPS cuando realiza un análisis NMAP en determinados dispositivos de la red o cuando hace un ping a algunos hosts supervisados por el sensor Cisco IPS. Una vez que se activa una alarma en Cisco IPS, vaya a **Monitoreo y Bloques de Host Activo** para verificar los detalles del host.



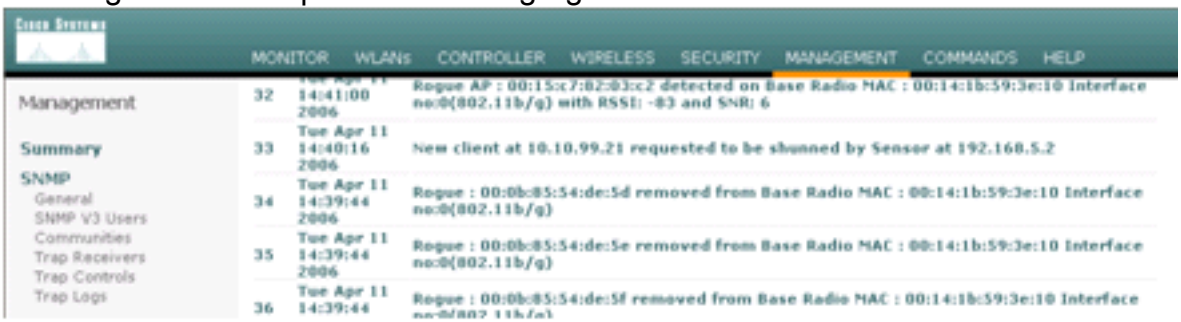
La lista de clientes rechazados en el controlador ahora se completa con la dirección IP y MAC del



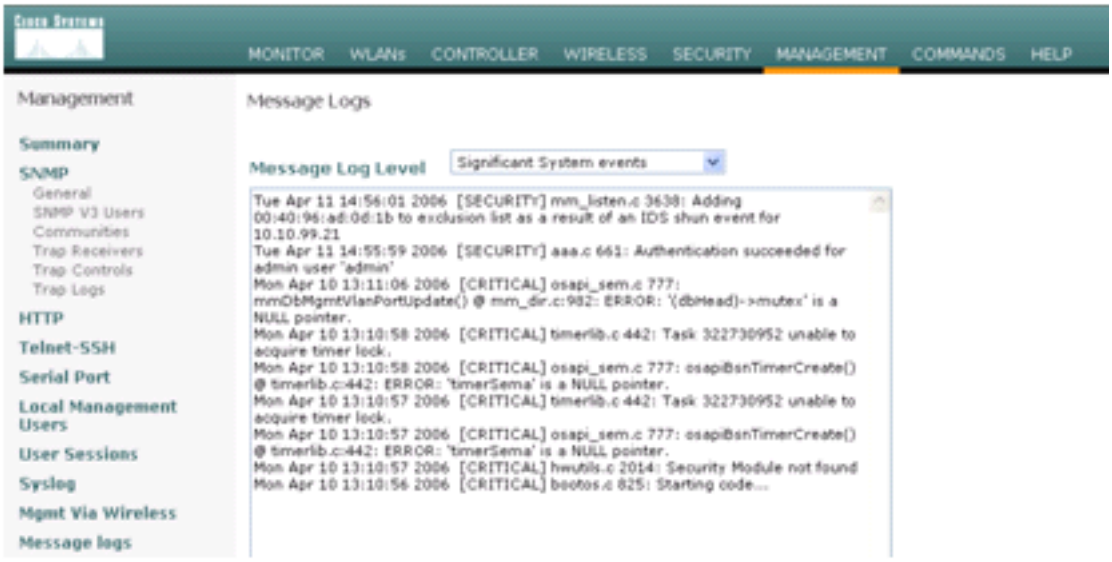
host. El usuario se agrega a la lista de exclusión de cliente.



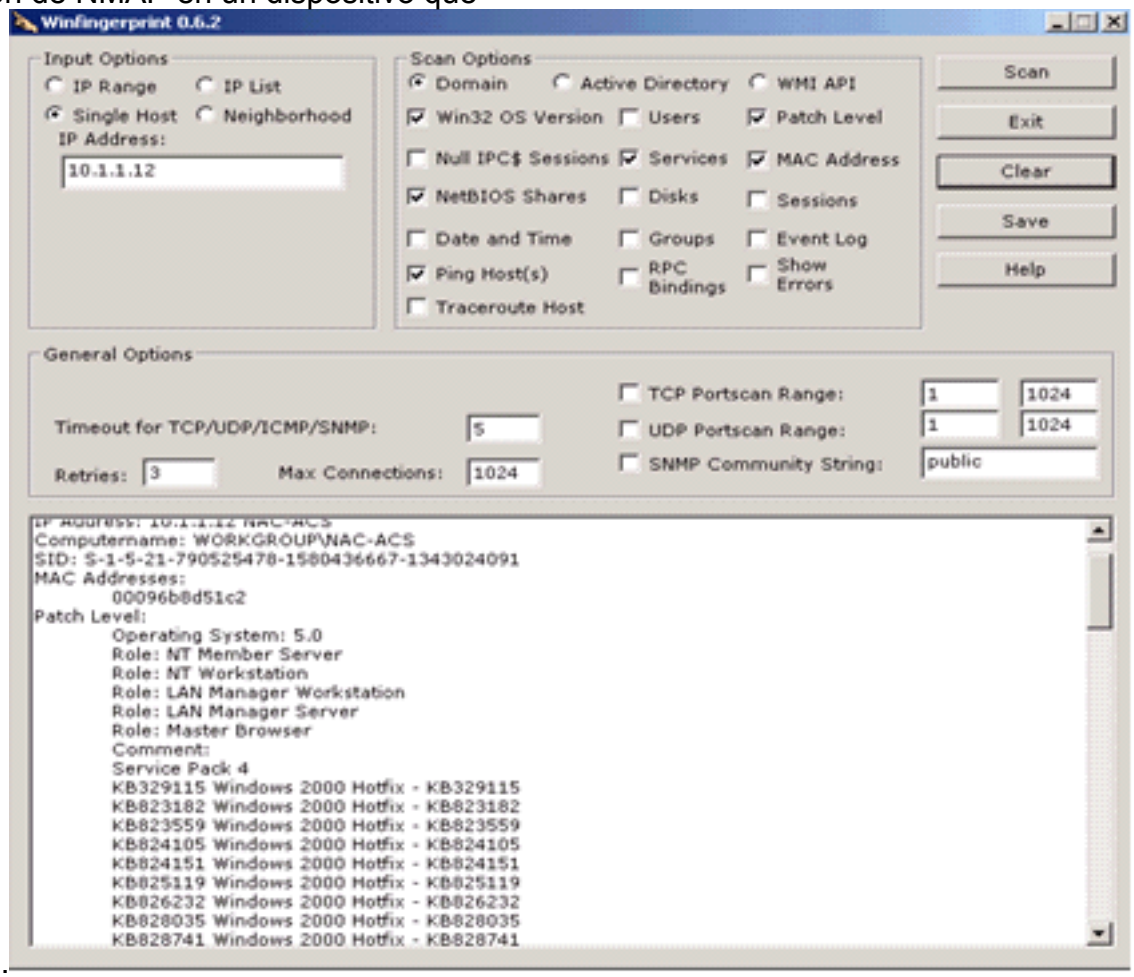
Se genera un registro de trampa cuando se agrega un cliente a la lista de rechazo.



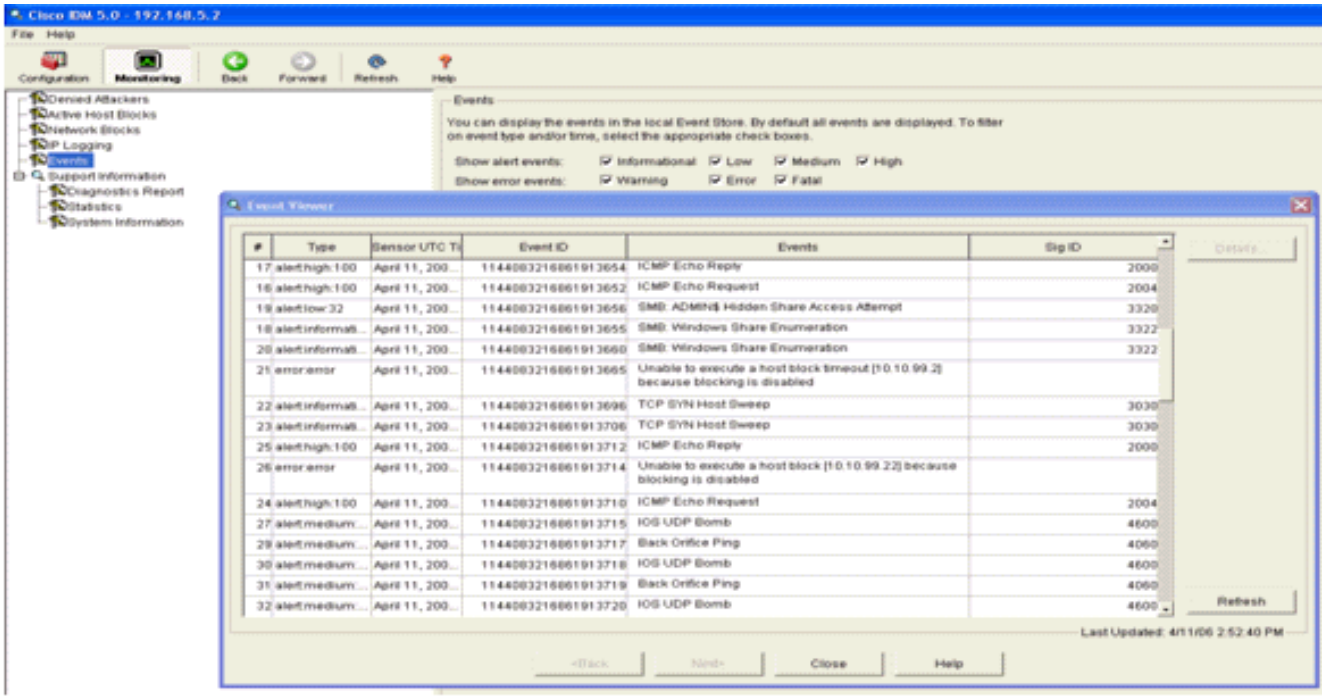
También se genera un registro de mensajes para el



evento. Alguno
s eventos adicionales se generan en el sensor de Cisco IPS cuando se realiza una exploración de NMAP en un dispositivo que



monitorea. Es
ta ventana muestra los eventos generados en el sensor de Cisco IPS.



Ejemplo de configuración del sensor IDS de Cisco

Este es el resultado del script de configuración de la instalación:

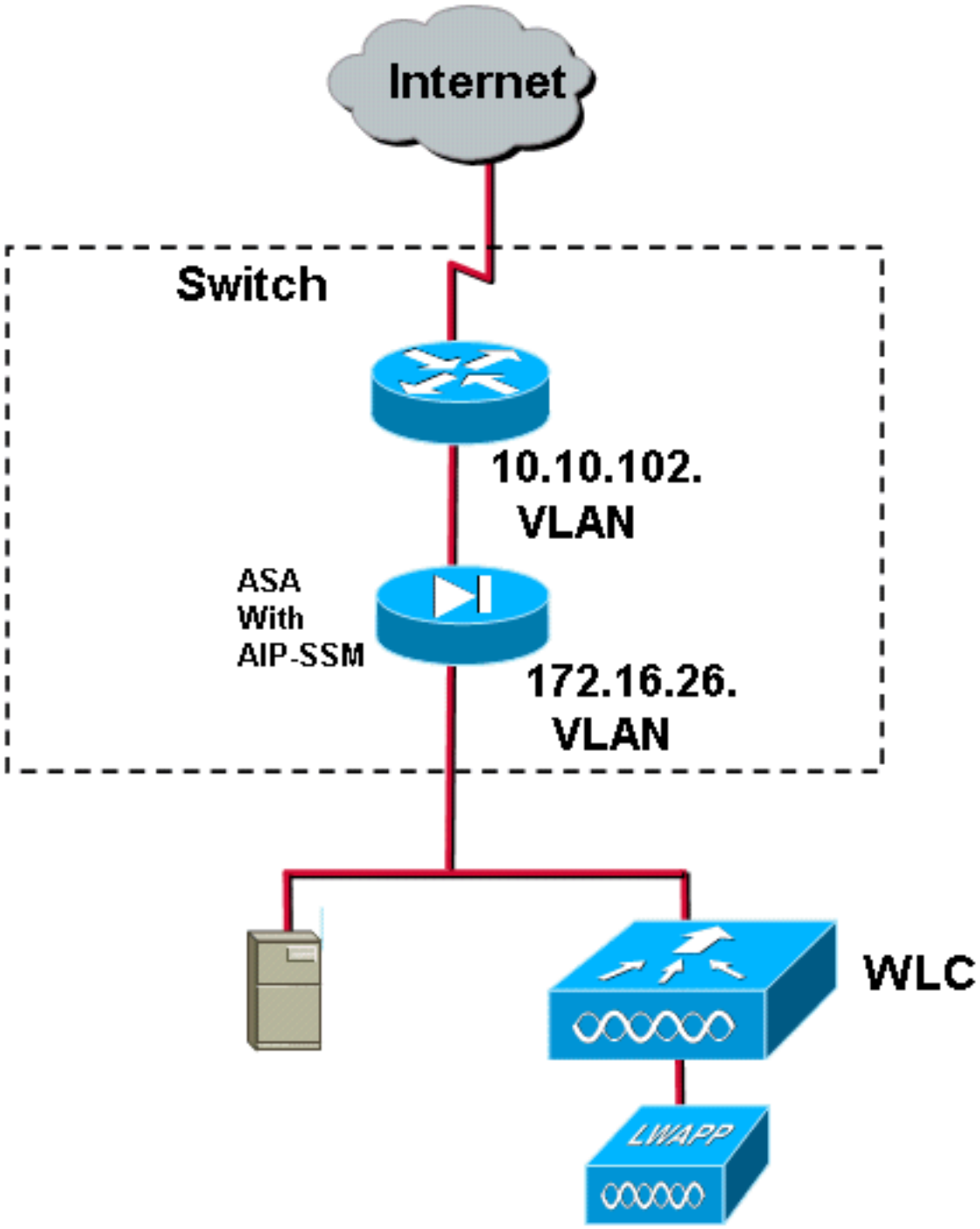
```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------------------------------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
exit
signatures 2001 0
alert-severity high
status
enabled true
exit
```

```
exit
signatures 2002 0
alert-severity high
status
enabled true
exit
exit
signatures 2003 0
alert-severity high
status
enabled true
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service authentication
exit
! ------------------------------
service web-server
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/0
exit
exit
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
exit
! ------------------------------
service trusted-certificates
exit
sensor#
```

Configure un ASA para IDS

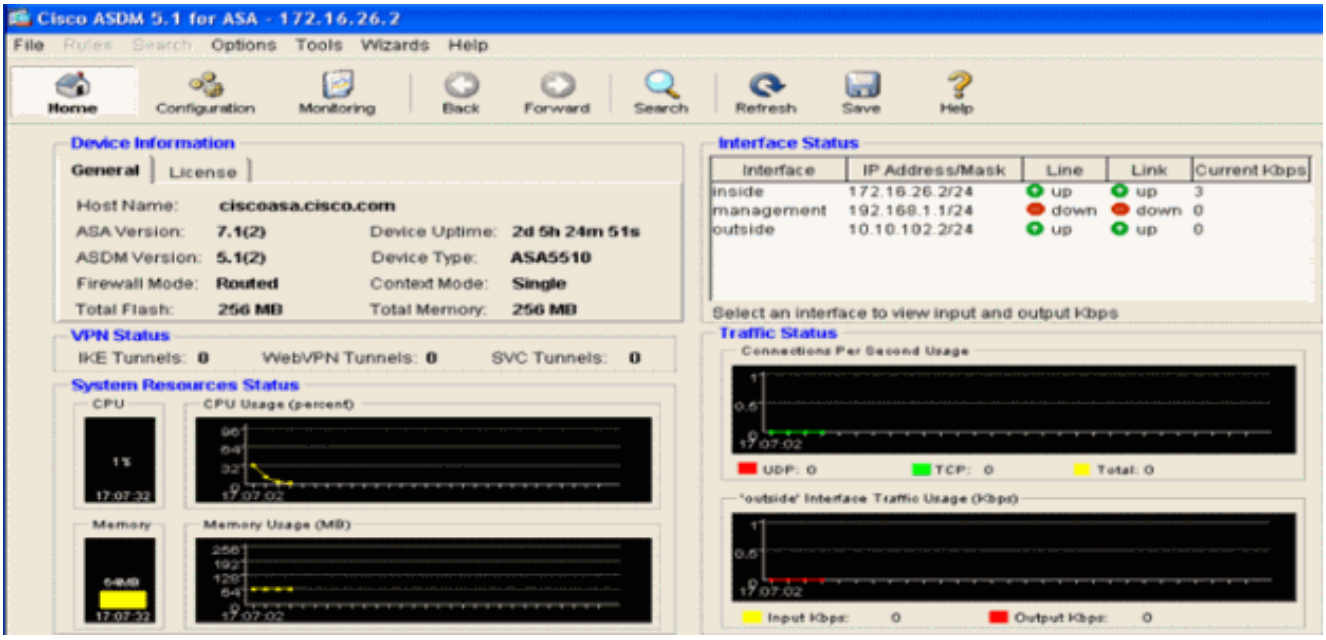
A diferencia de un sensor de detección de intrusiones tradicional, un ASA siempre debe estar en la ruta de datos. En otras palabras, en lugar de extender el tráfico desde un puerto del switch a un

puerto de rastreo pasivo en el Sensor, el ASA debe recibir los datos en una interfaz, procesarlos internamente y luego reenviarlos a otro puerto. Para el IDS, utilice el marco de políticas modular (MPF) para copiar el tráfico que el ASA recibe en el módulo de servicios de seguridad de prevención e inspección avanzada (AIP-SSM) interno para su inspección.

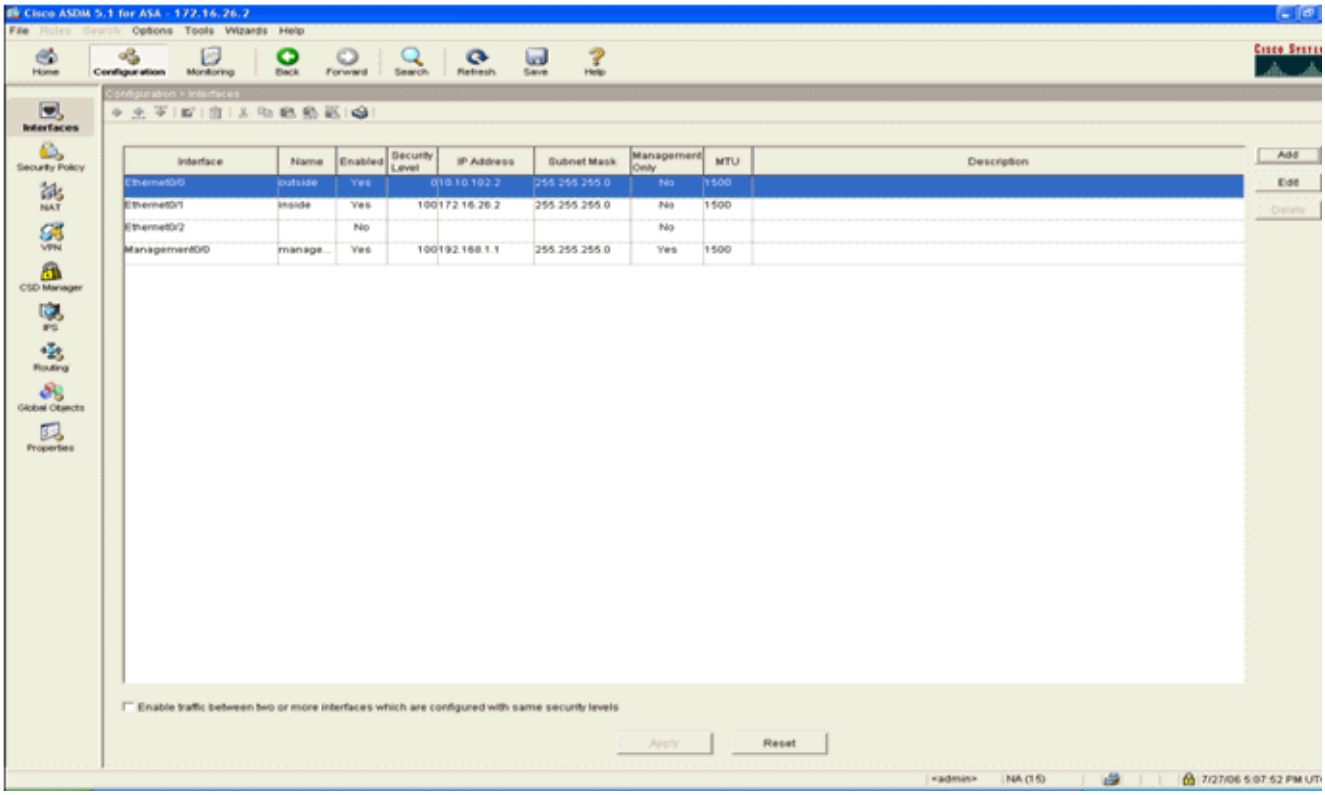


En este ejemplo, el ASA utilizado ya está configurado y pasa tráfico. Estos pasos demuestran cómo crear una política que envía datos al AIP-SSM.

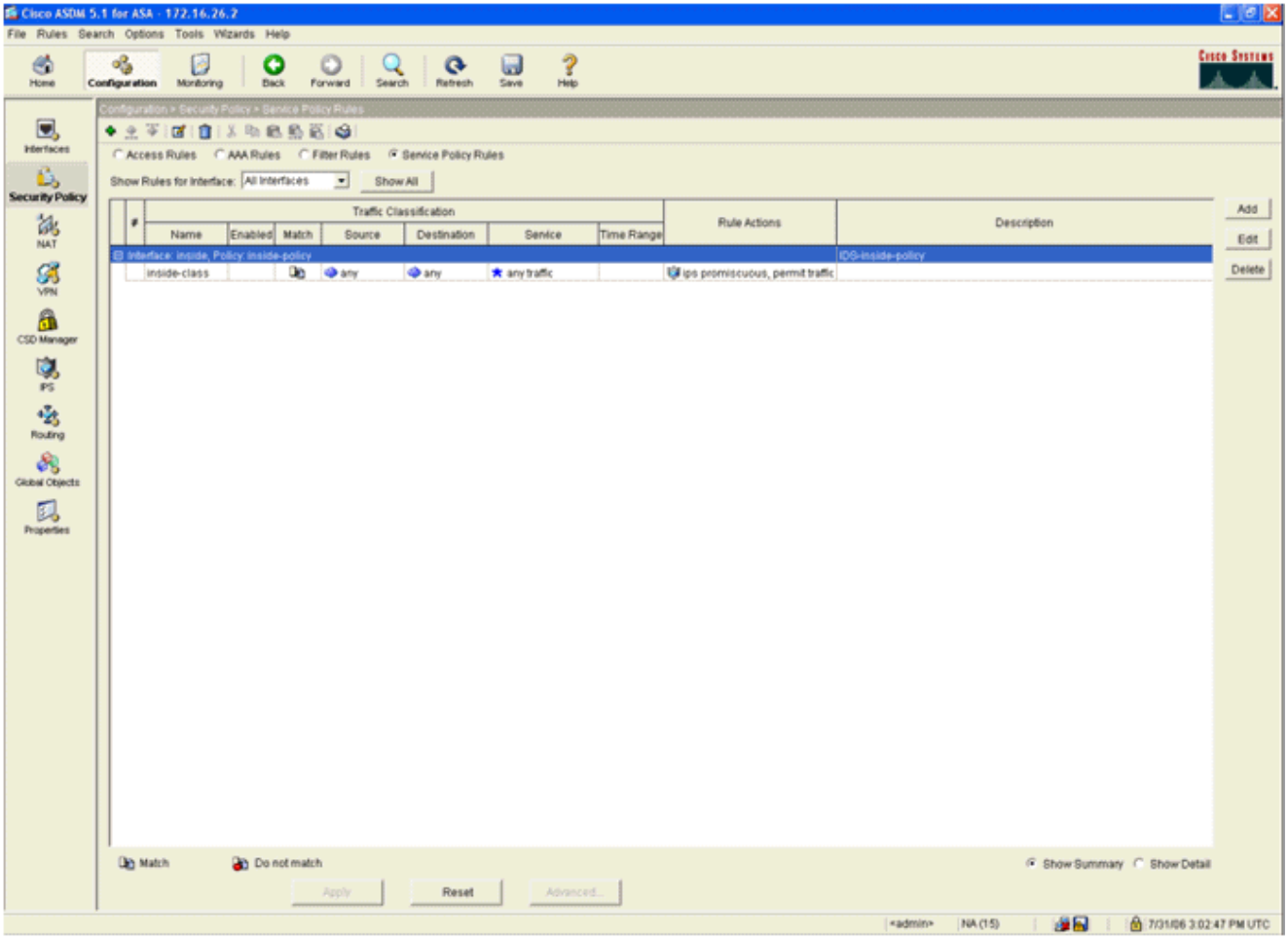
1. Inicie sesión en ASA con ASDM. Al iniciar sesión correctamente, aparece la ventana ASA Main System (Sistema principal de
   ASA).



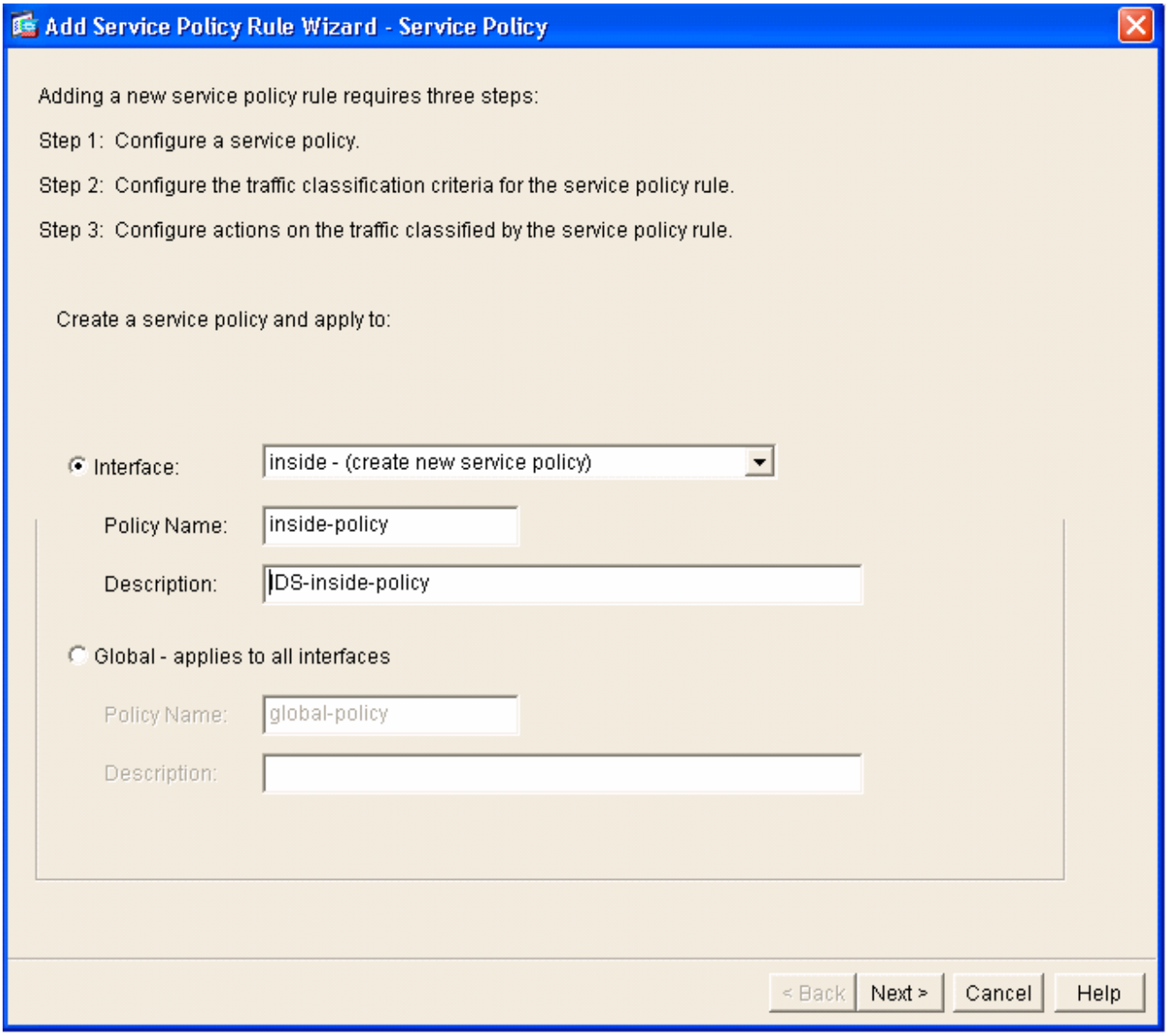
2. Haga clic en **Configuración** en la parte superior de la página. La ventana cambia a una vista de las interfaces
ASA.



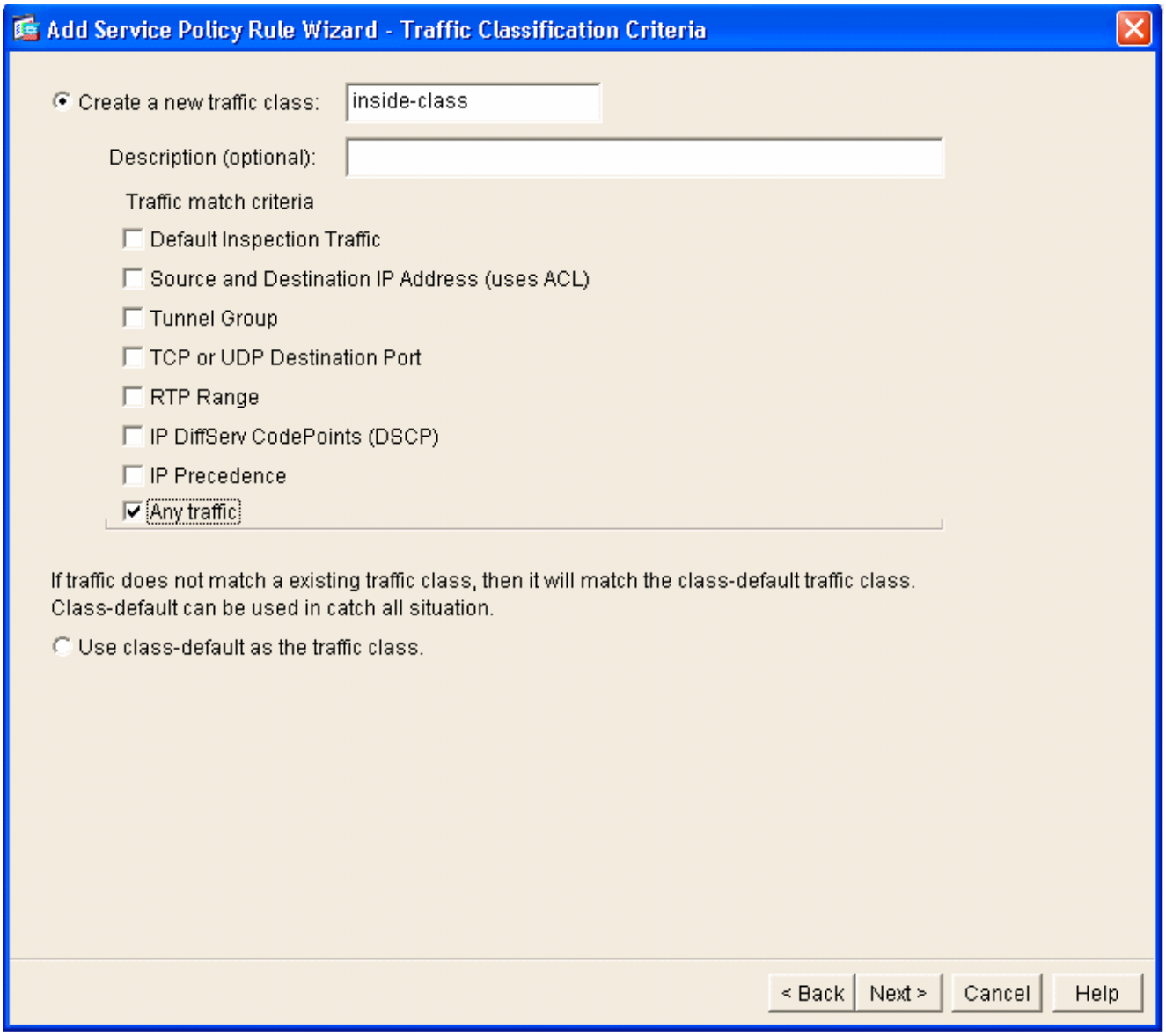
3. Haga clic en **Política de seguridad** en el lado izquierdo de la ventana. En la ventana resultante, elija la pestaña **Reglas de política de servicio**.



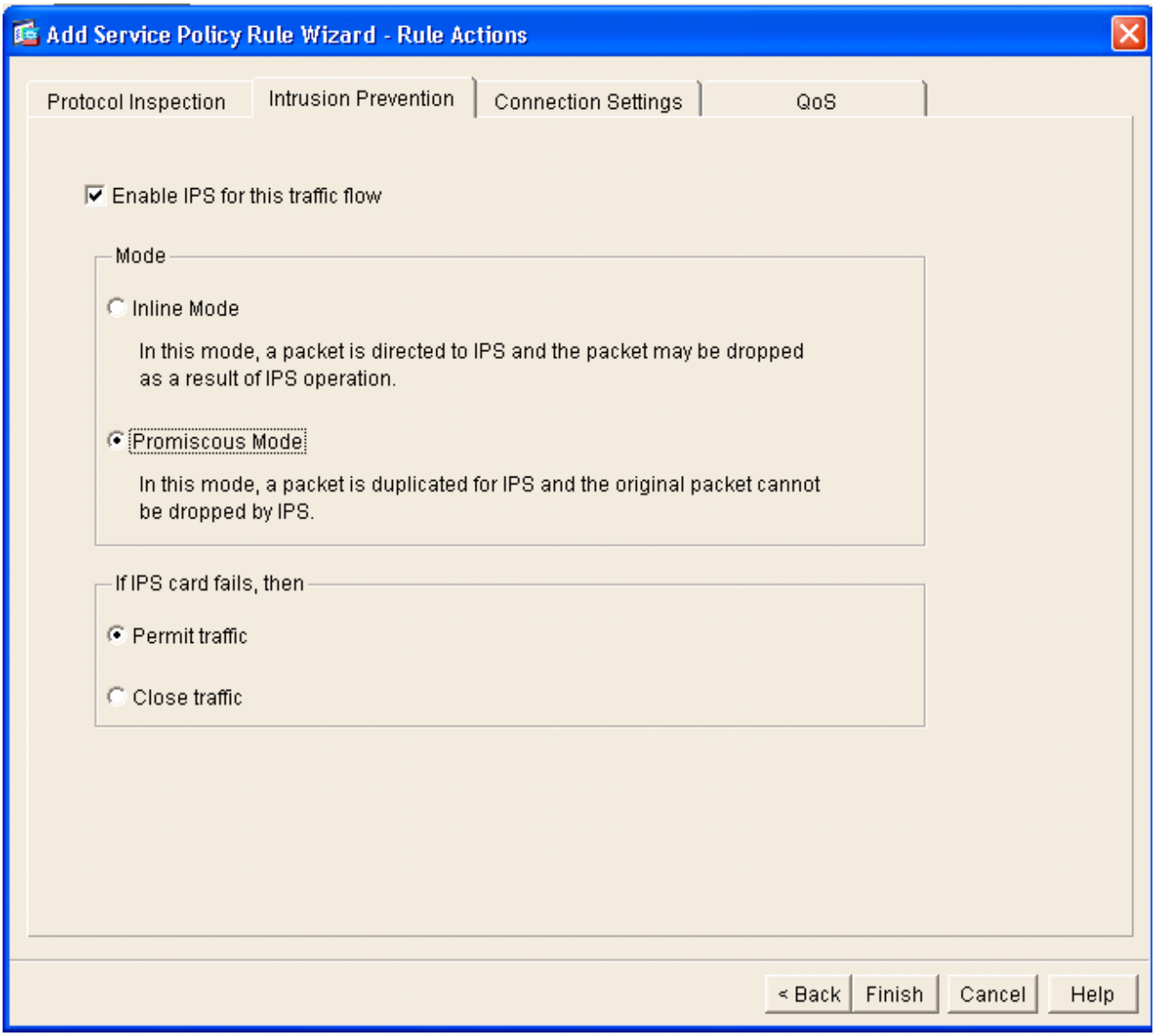
4. Haga clic en **Agregar** para crear una nueva política. El Asistente para agregar reglas de directivas de servicio se inicia en una nueva ventana.Haga clic en **Interface** y luego elija la interfaz correcta de la lista desplegable para crear una nueva política que se enlaza a una de las interfaces que pasa tráfico.Asigne a la directiva un nombre y una descripción de lo que hace la política utilizando los dos cuadros de texto.Haga clic en **Next** para pasar al siguiente paso.



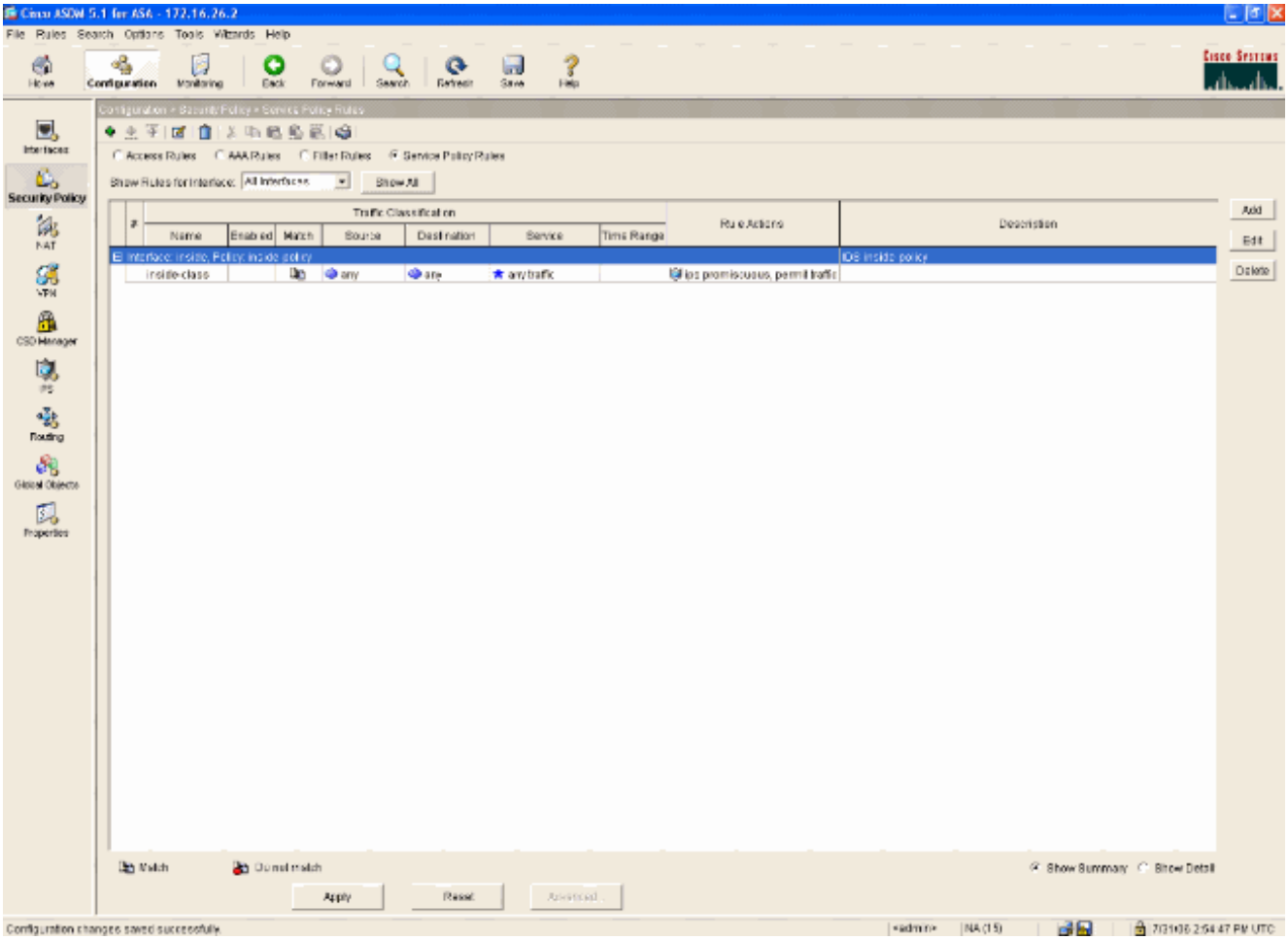
5. Cree una nueva clase de tráfico para aplicarla a la política.Es razonable generar clases específicas para inspeccionar tipos de datos específicos, pero en este ejemplo, se selecciona Cualquier tráfico por simplicidad. Haga clic en **Next** para continuar.



6. Complete estos pasos paraindique al ASA que dirija el tráfico a su AIP-SSM.Verifique **Enable IPS para este flujo de tráfico** para habilitar la detección de intrusiones.Establezca el modo en **Promiscuous** para que se envíe una copia del tráfico al módulo fuera de banda en lugar de colocar el módulo en línea con el flujo de datos.Haga clic en **Permit traffic** para asegurarse de que ASA conmute a un estado de fallo-apertura en caso de que el AIP-SSM falle.Haga clic en **Finalizar** para confirmar el cambio.



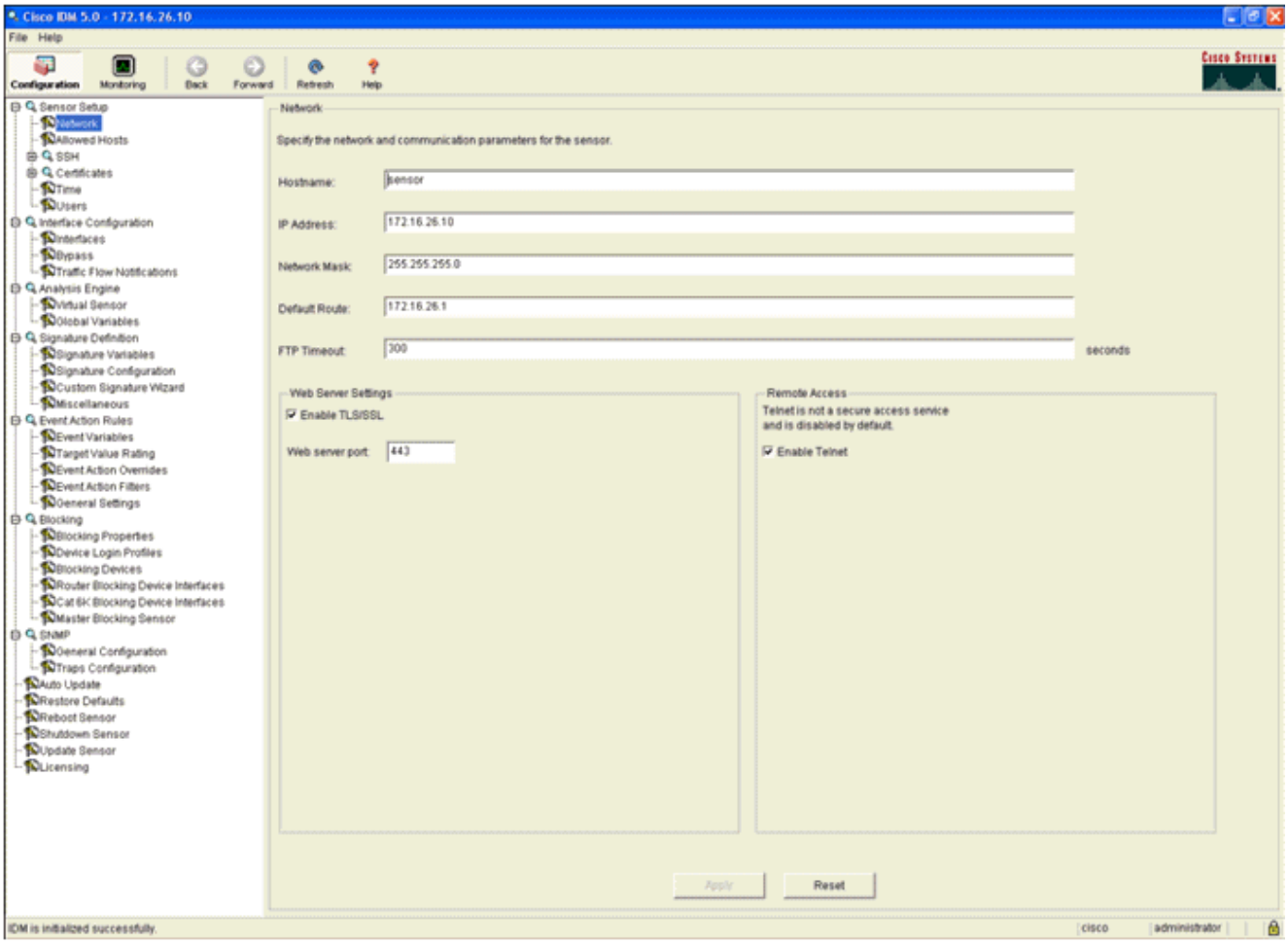
7. El ASA ahora está configurado para enviar tráfico al módulo IPS. Haga clic en **Guardar** en la fila superior para escribir los cambios en el ASA.



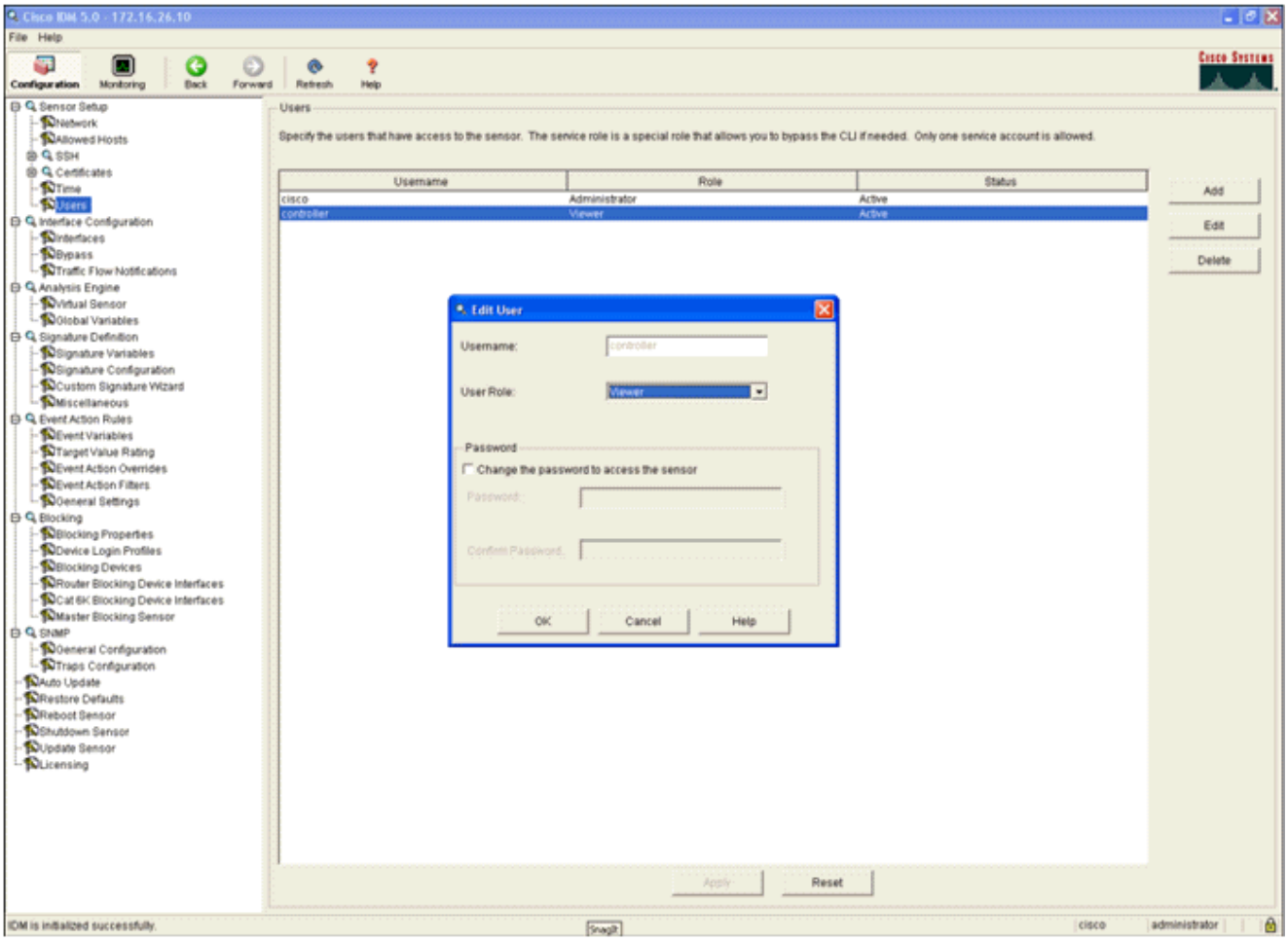
Configuración de AIP-SSM para la Inspección del Tráfico

Mientras el ASA envía datos al módulo IPS, asocie la interfaz AIP-SSM a su motor de sensor virtual.

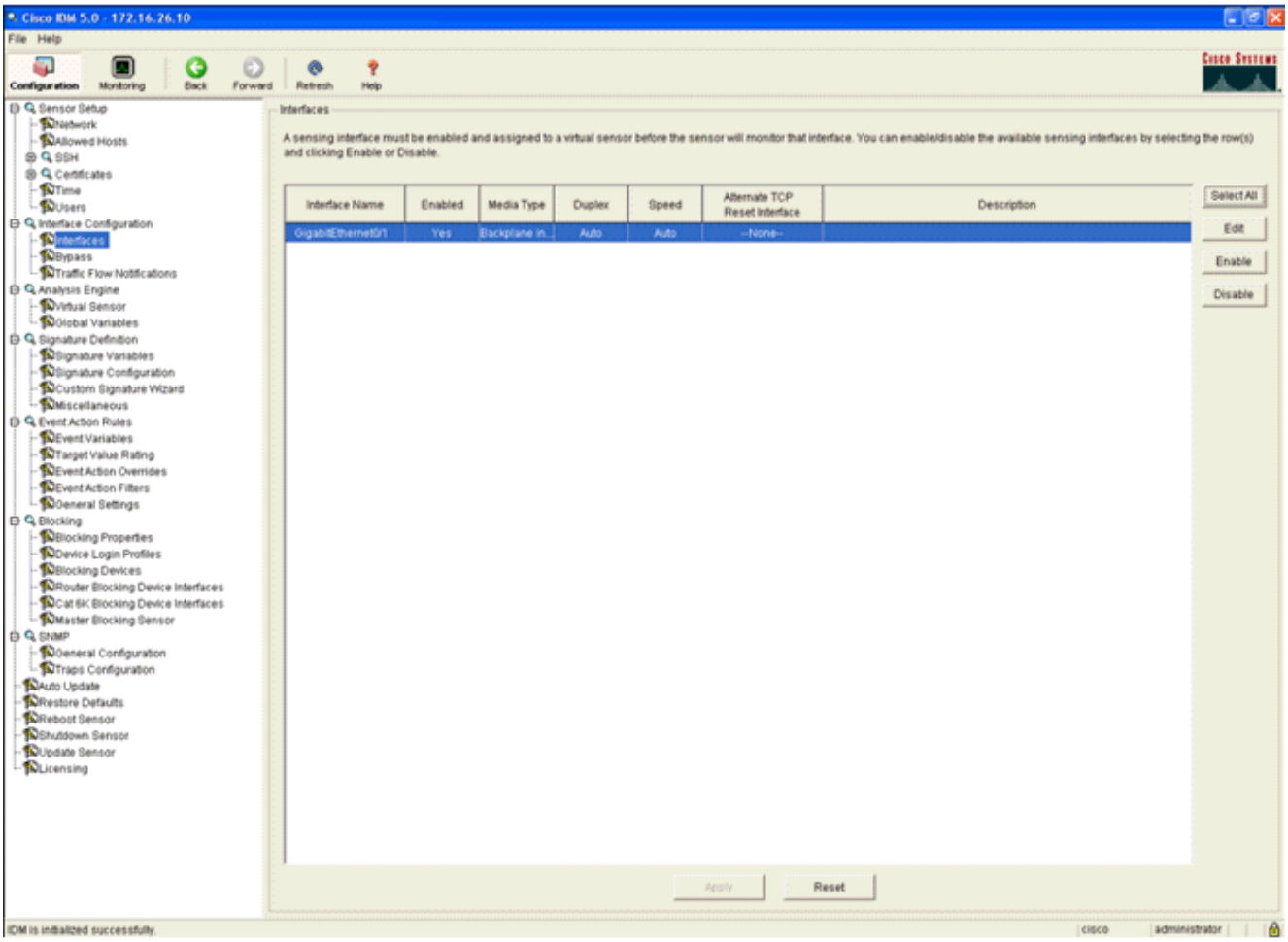
1. Inicie sesión en AIP-SSM con
   IDM.



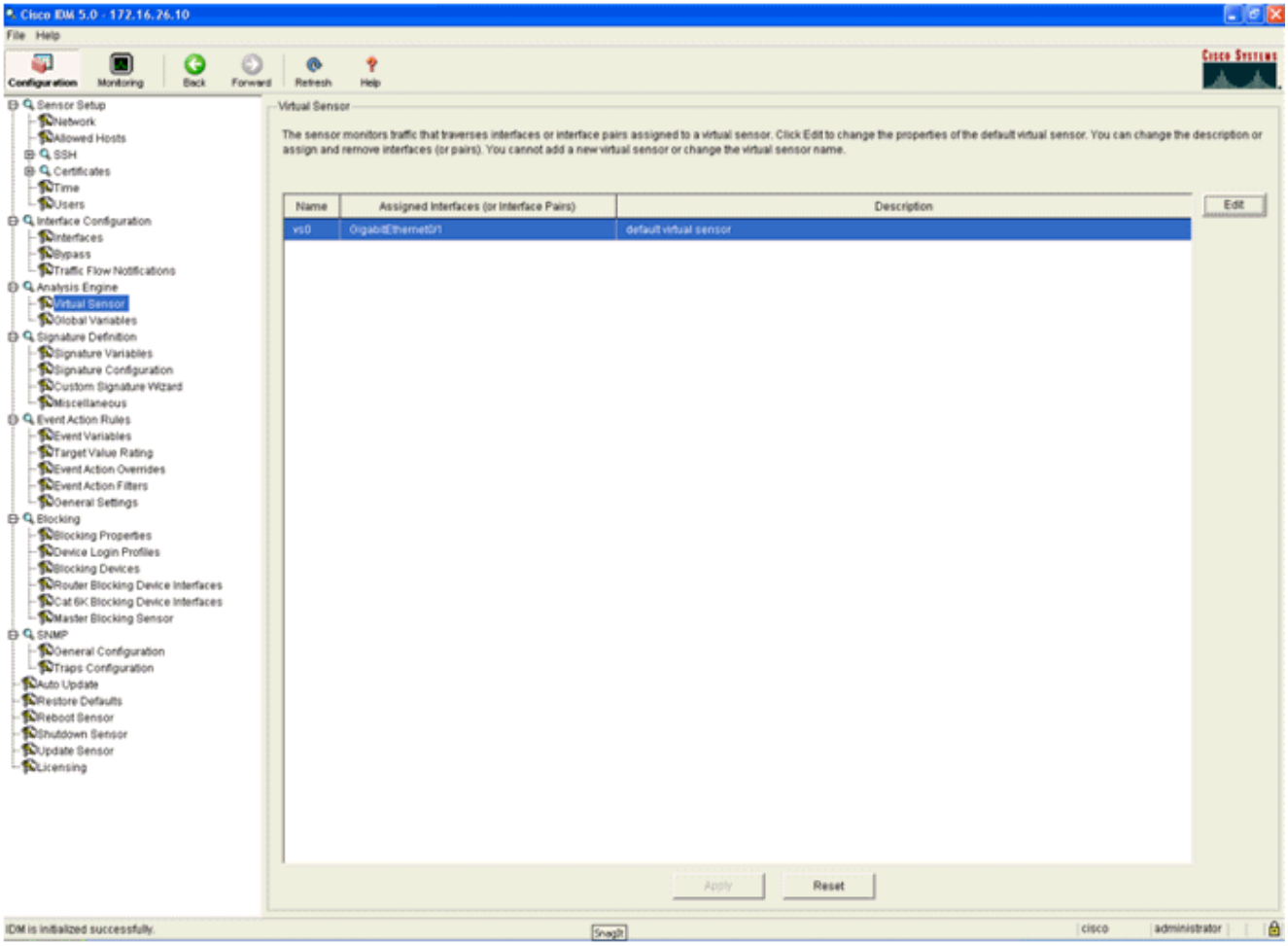
2. Agregue un usuario con al menos privilegios de visor.



3. Habilite la interfaz.



4. Verifique la configuración del sensor virtual.

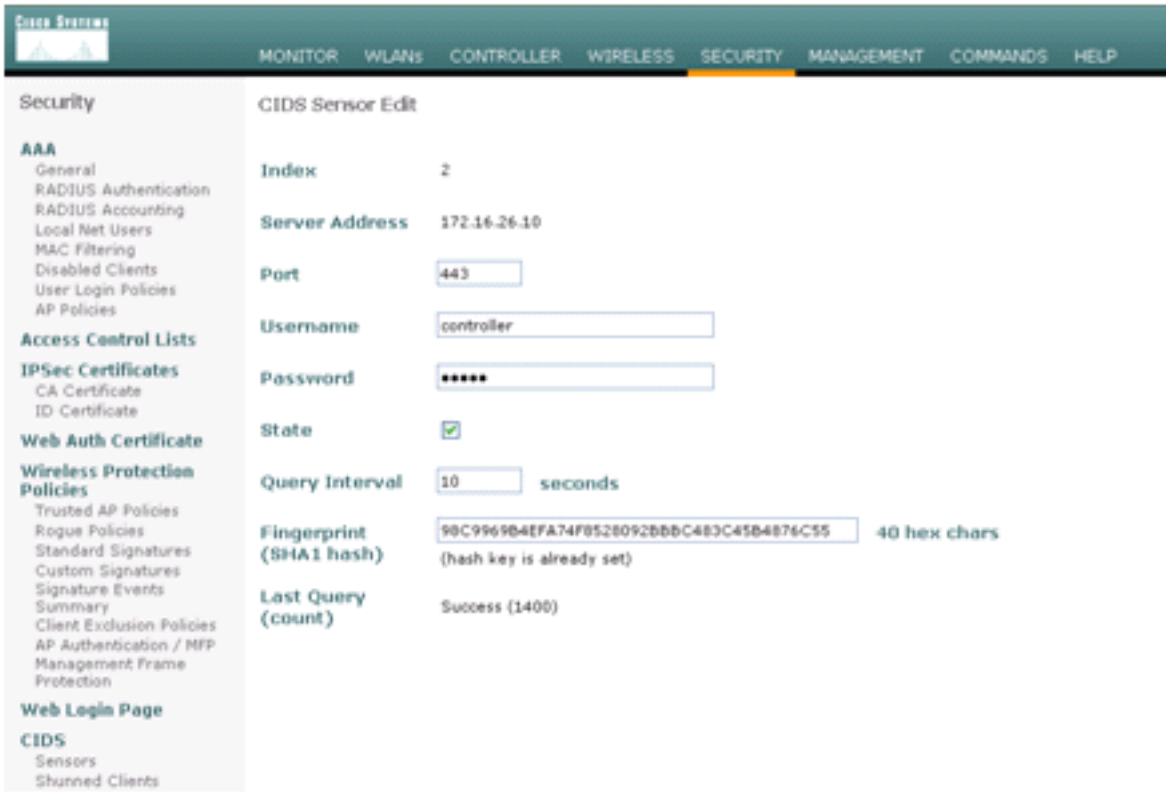


Configure un WLC para sondear el AIP-SSM para los bloques de clientes

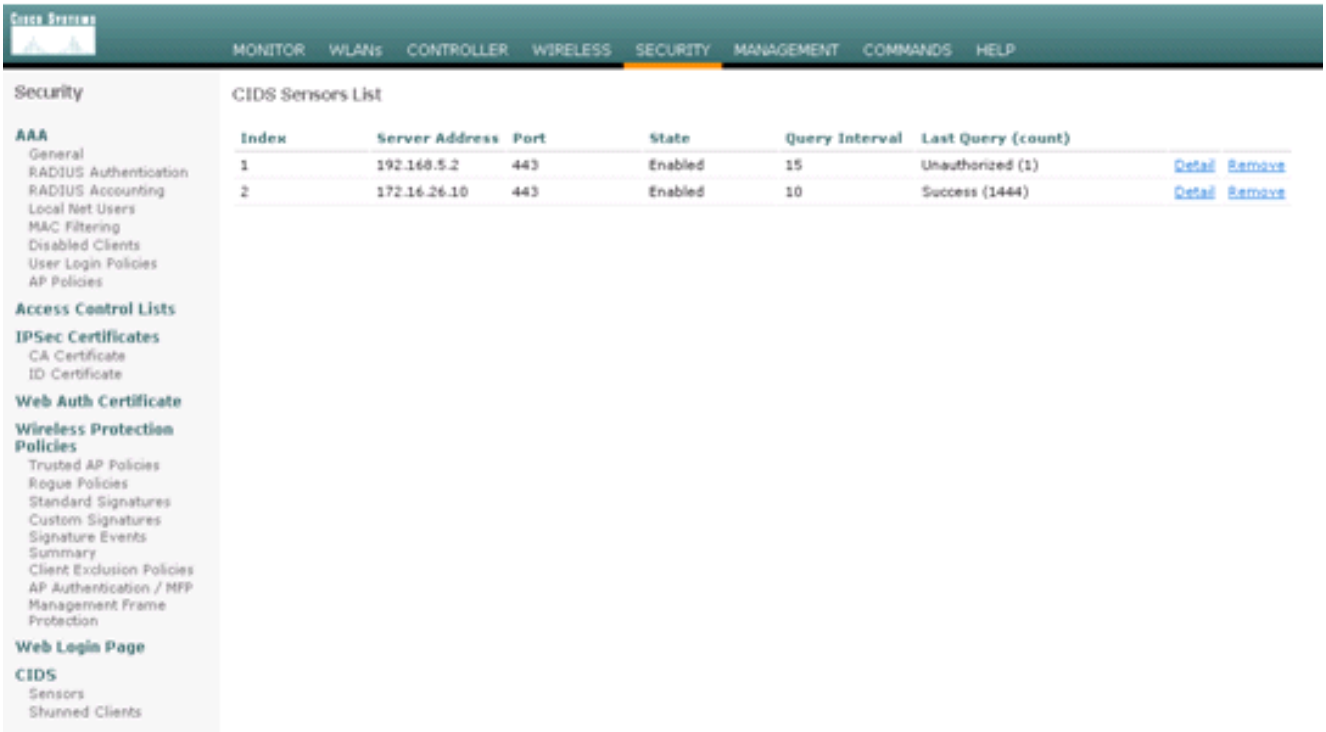
Complete estos pasos una vez que el Sensor esté configurado y listo para ser agregado en el controlador:

1. Elija **Security > CIDS > Sensors > New** en el WLC.
2. Agregue la dirección IP, el número de puerto TCP, el nombre de usuario y la contraseña que creó en la sección anterior.
3. Para obtener la huella dactilar del Sensor, ejecute este comando en el Sensor y agregue la huella digital SHA1 en el WLC (sin los dos puntos). Esto se utiliza para asegurar la comunicación de sondeo de controlador a IDS.

```
sensor#show tls fingerprint
MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E
SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55
```



4. Verifique el estado de la conexión entre el AIP-SSM y el WLC.

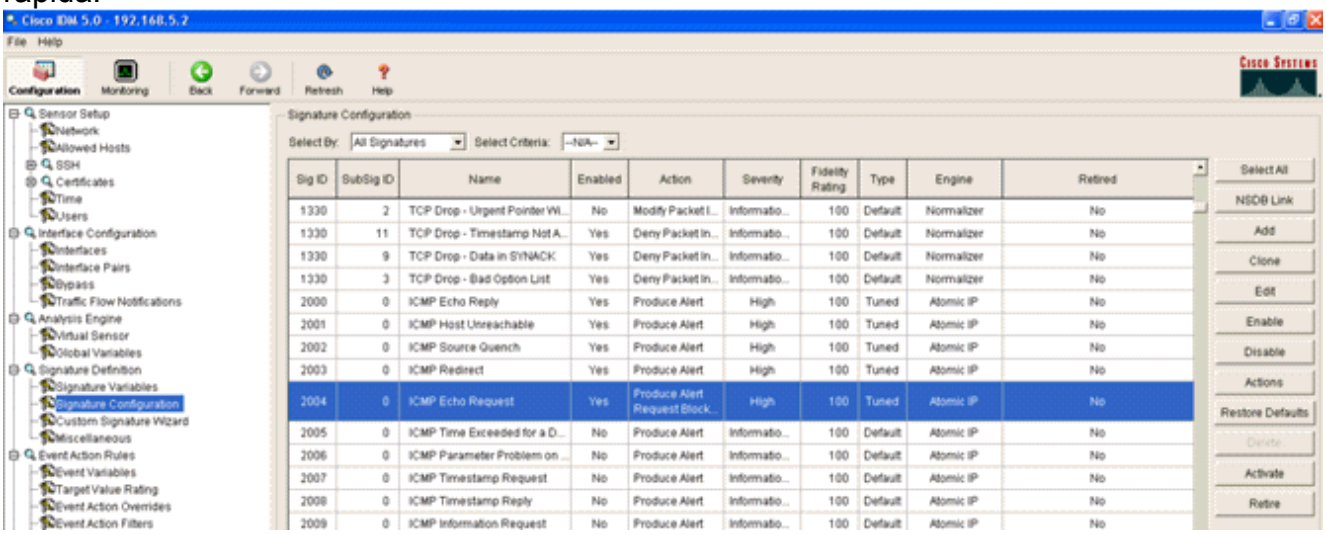


Agregar una firma de bloqueo al AIP-SSM

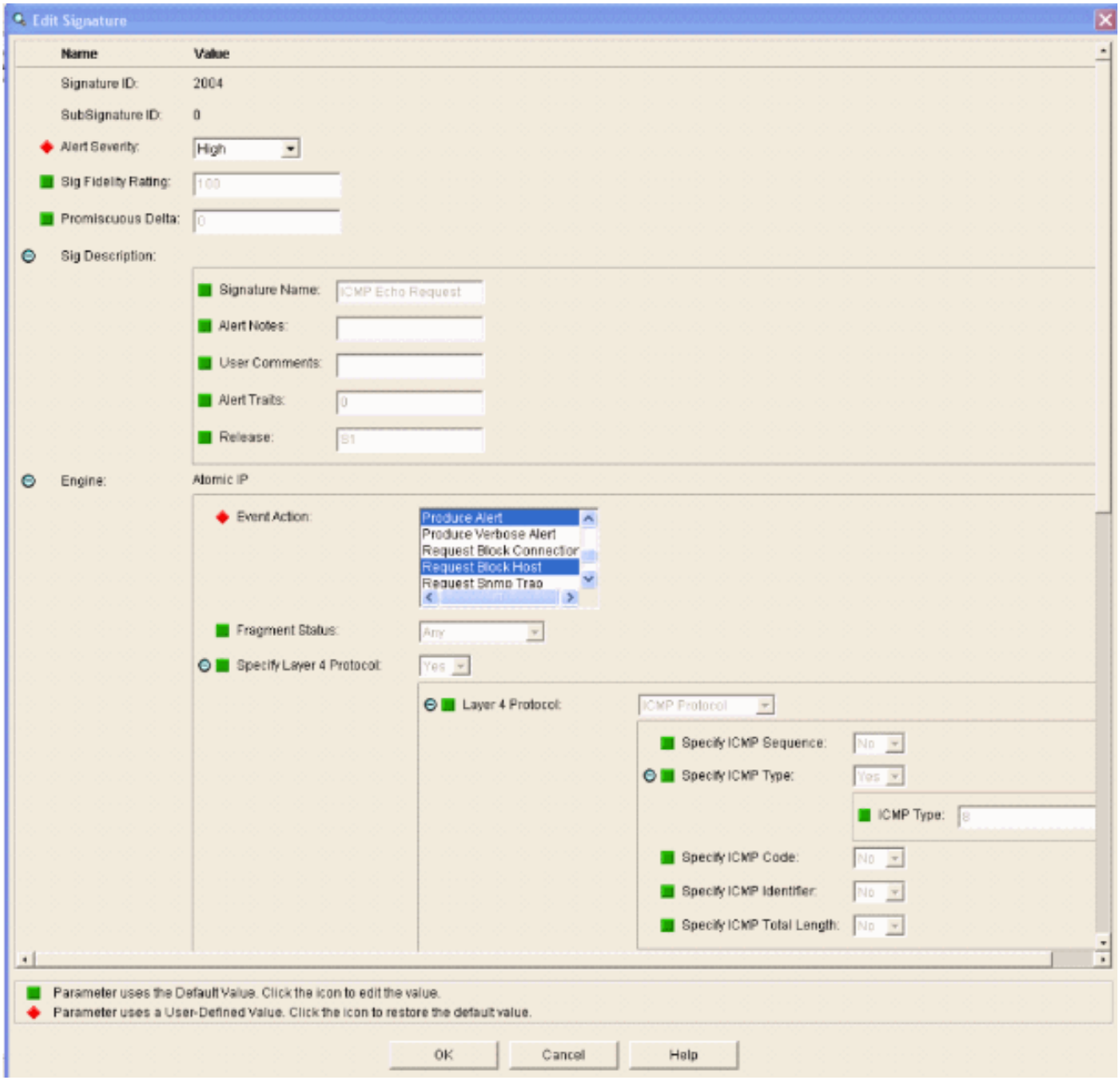
Agregue una firma de inspección para bloquear el tráfico. Aunque hay muchas firmas que pueden realizar el trabajo basándose en las herramientas disponibles, este ejemplo crea una firma que bloquea los paquetes ping.

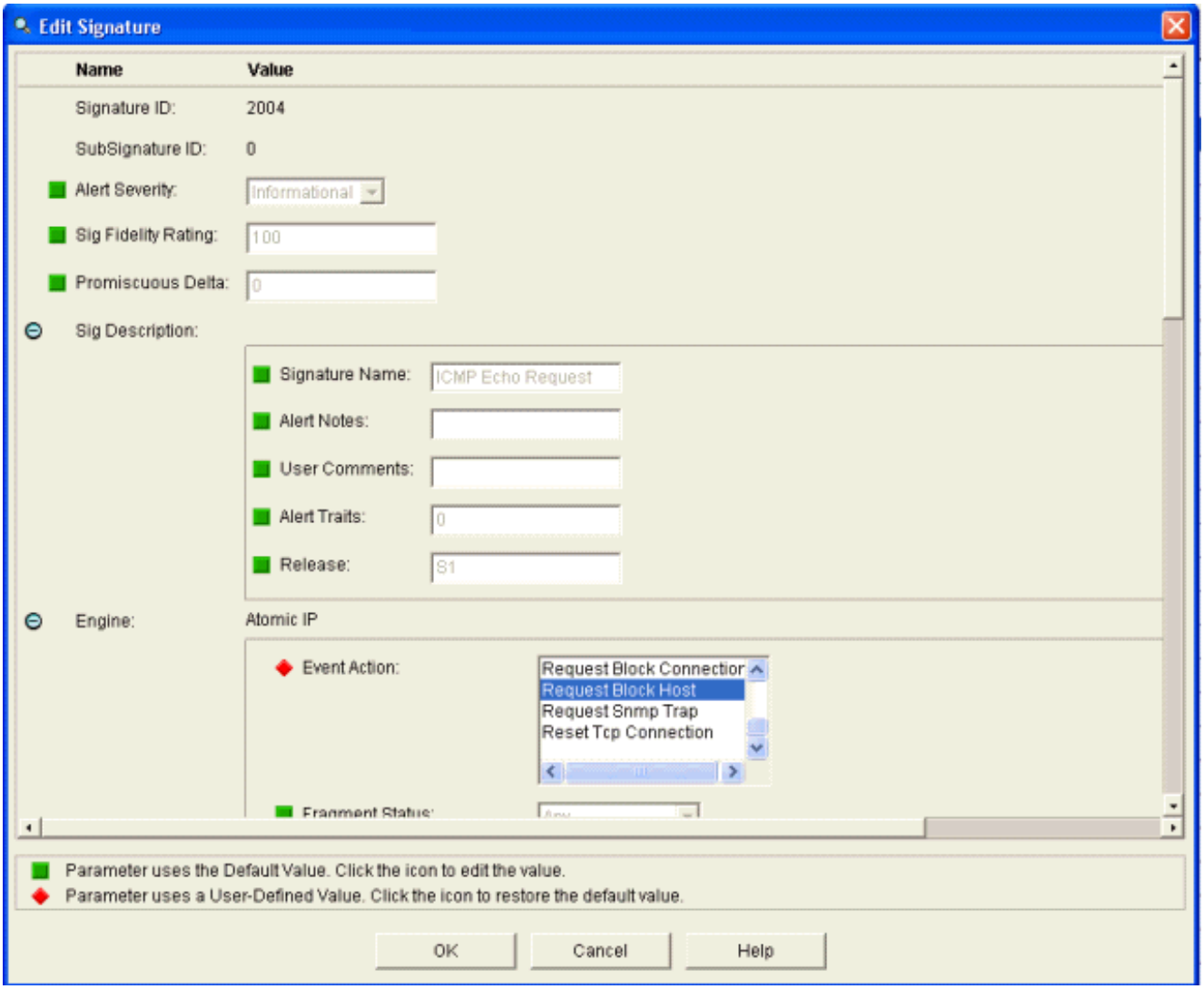
1. Seleccione la **firma 2004 (Solicitud de eco ICMP)** para realizar una verificación de configuración

rápida.



2. Habilite la firma, establezca la gravedad de la alerta en **alto** y establezca la acción del evento en **Producir alerta** y **Solicitar bloqueo de host** para completar este paso de verificación. Tenga en cuenta que la acción Host de Bloqueo de Solicitud es la clave para señalizar el WLC para crear excepciones de
cliente.


Edit Signature
Name
Value
Signature ID:
2004
SubSignature ID:
0
Alert Severity:
High
Sig Fidelity Rating:
100
Promiscuous Delta:
0
Sig Description:
Signature Name:
ICMP Echo Request
Alert Notes:
User Comments:
Alert Traits:
0
Release:
S1
Engine:
Atomic IP
Event Action:
Produce Alert
Produce Verbose Alert
Request Block Connection
Request Block Host
Request Snmp Trap
Fragment Status:
Any
Specify Layer 4 Protocol:
Yes
Layer 4 Protocol:
ICMP Protocol
Specify ICMP Sequence:
No
Specify ICMP Type:
Yes
ICMP Type:
8
Specify ICMP Code:
No
Specify ICMP Identifier:
No
Specify ICMP Total Length:
No
Parameter uses the Default Value. Click the icon to edit the value.
Parameter uses a User-Defined Value. Click the icon to restore the default value.
OK
Cancel
Help

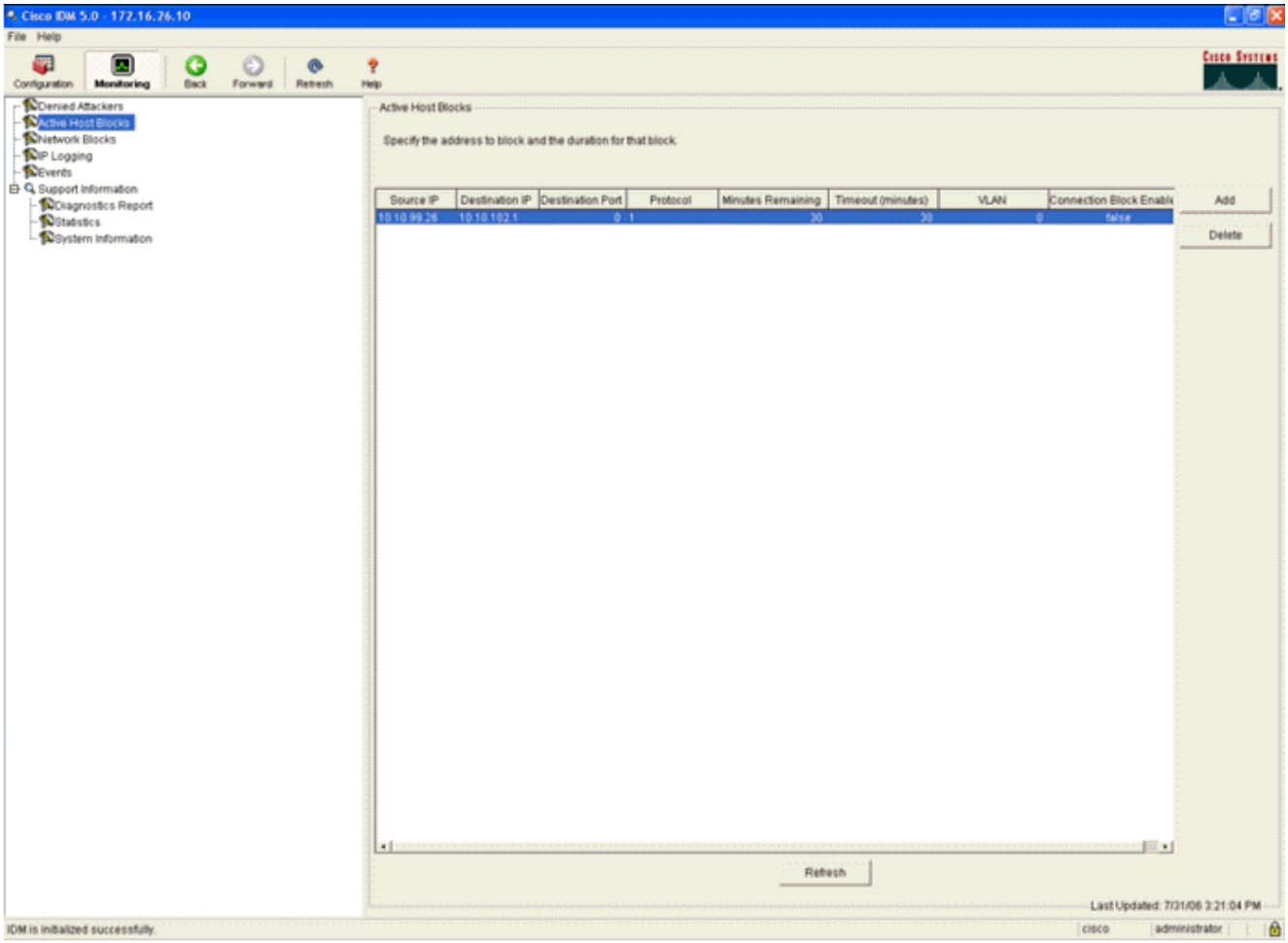


3. Haga clic en **Aceptar** para guardar la firma.
4. Verifique que la firma esté activa y que esté configurada para realizar una acción de bloqueo.
5. Haga clic en **Aplicar** para enviar la firma al módulo.

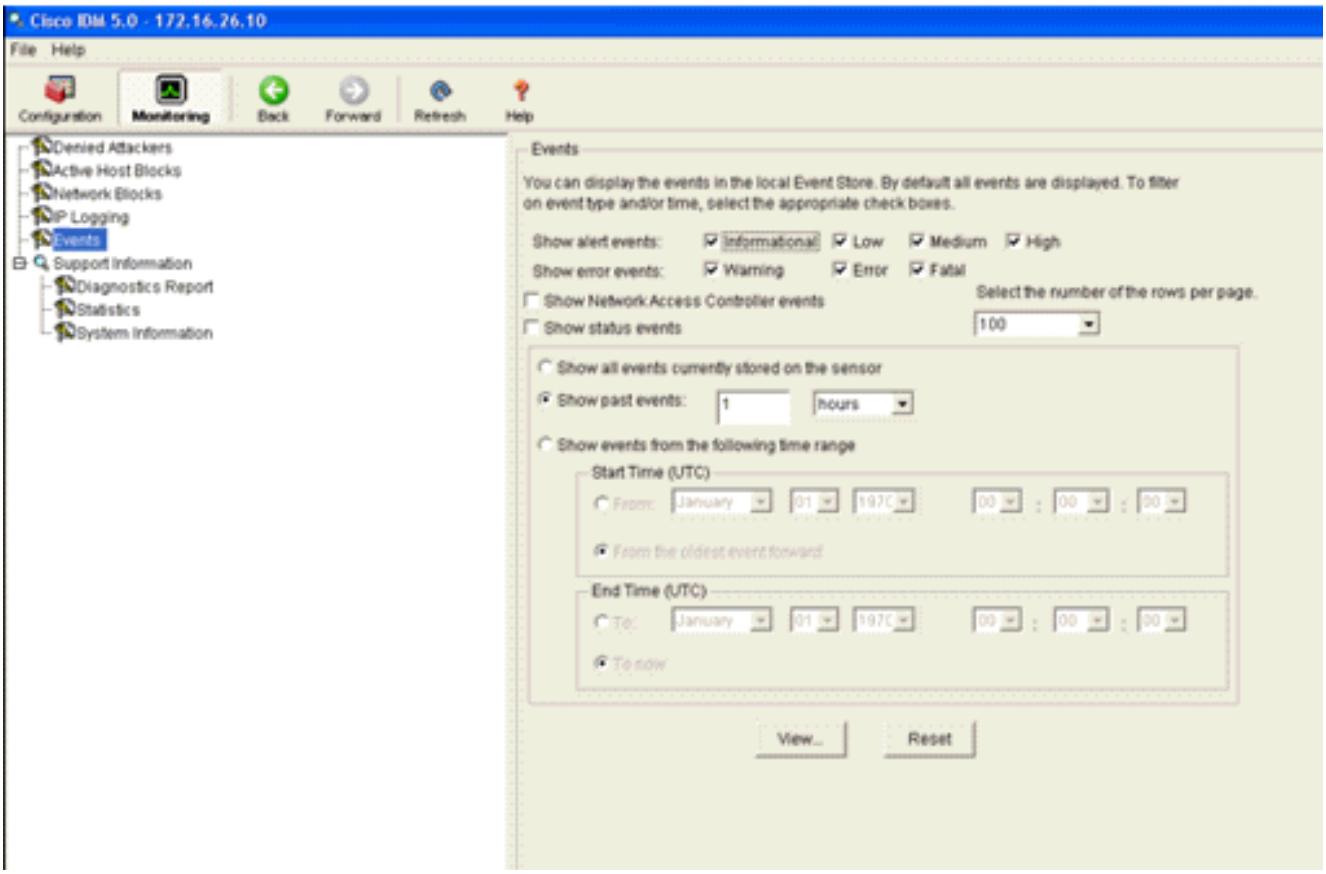
Supervisión de eventos y bloqueos con IDM

Complete estos pasos:

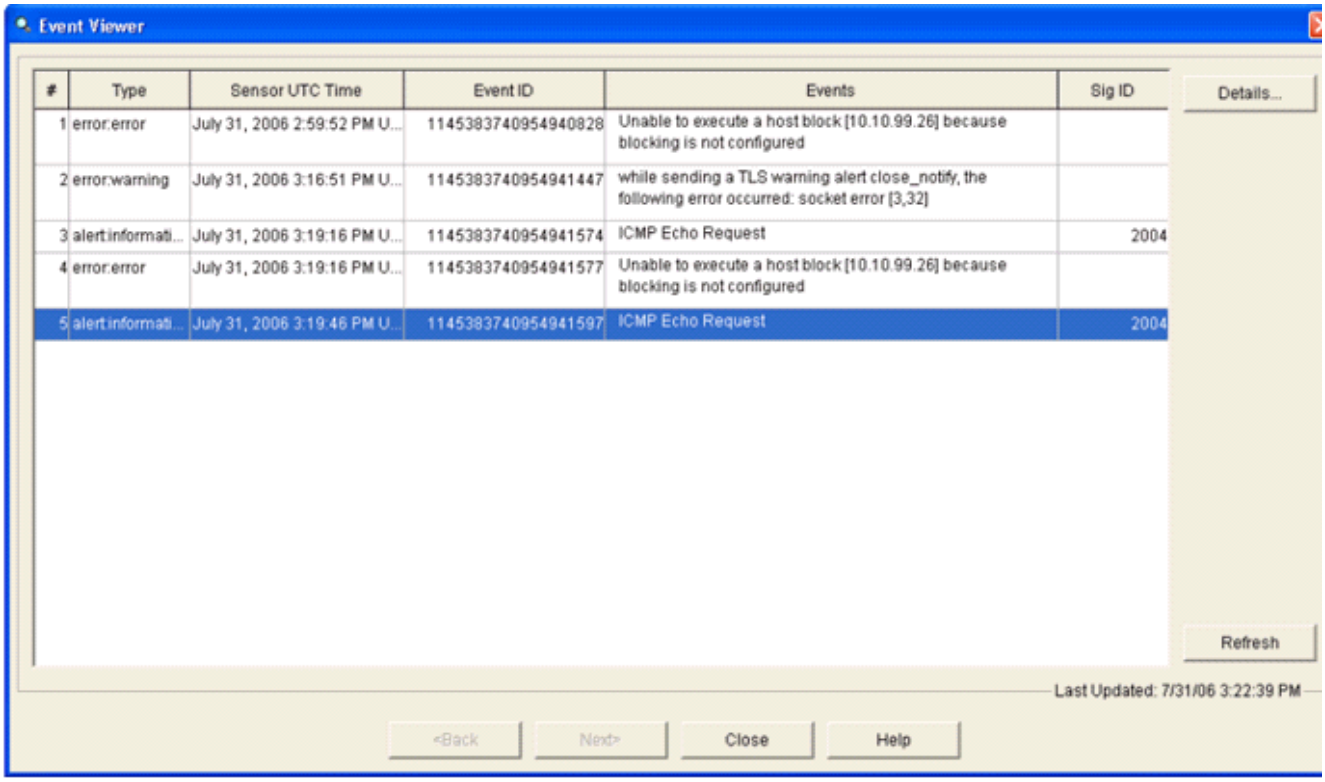
1. Cuando la firma se activa correctamente, hay dos lugares dentro de IDM para notar esto.El primer método muestra los bloques activos que el AIP-SSM ha instalado. Haga clic en **Supervisión** en la fila superior de acciones. Dentro de la lista de elementos que aparece en el lado izquierdo, seleccione **Bloques de host activos**. Siempre que se activa la firma ping, la ventana Bloques de host activos muestra la dirección IP del infractor, la dirección del dispositivo que se está atacando y el tiempo que queda para el cual el bloque está en vigor. El tiempo de bloqueo predeterminado es de 30 minutos y se puede ajustar. Sin embargo, en este documento no se explica cómo cambiar este valor. Consulte la documentación de configuración de ASA según sea necesario para obtener información sobre cómo cambiar este parámetro. Quite el bloque inmediatamente, selecciónelo de la lista y haga clic en **Eliminar**.



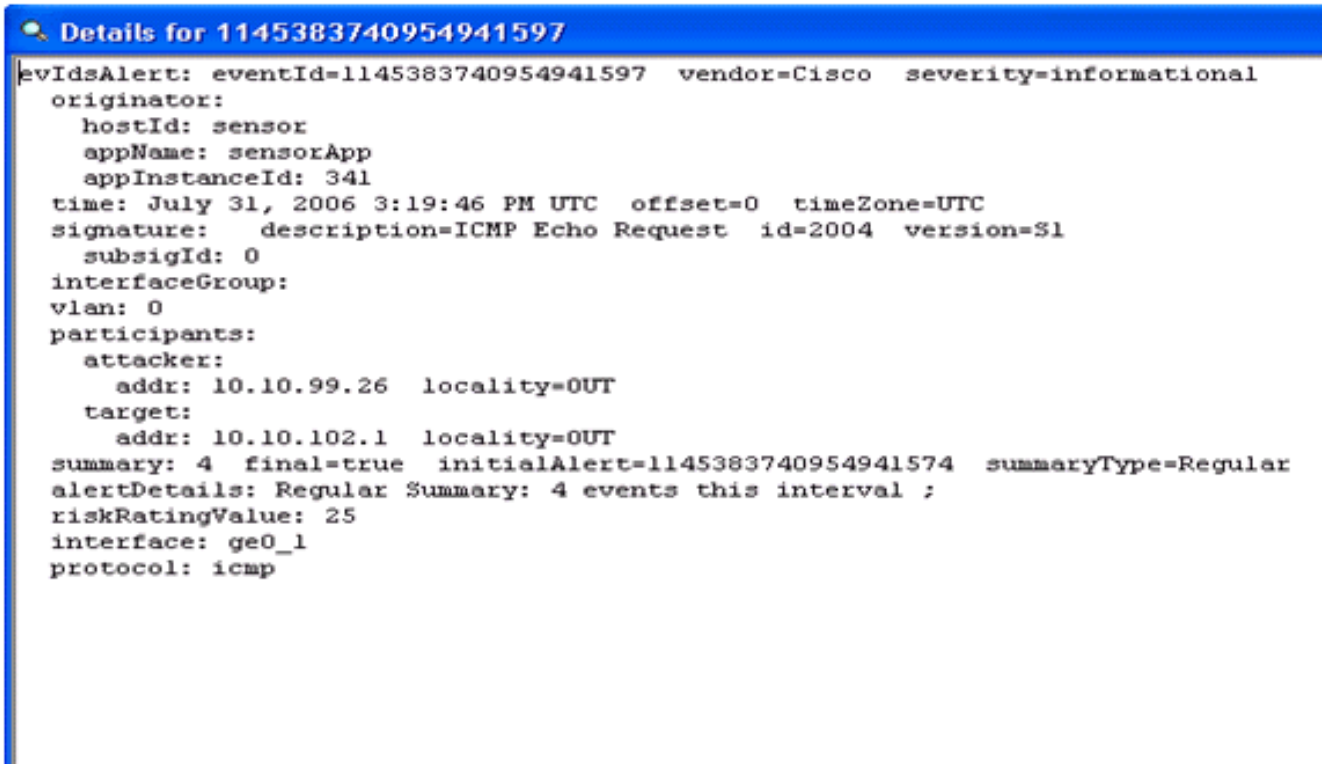
El segundo método para ver las firmas activadas utiliza el búfer de eventos AIP-SSM. En la página Supervisión de IDM, seleccione **Eventos** en la lista de elementos del lado izquierdo. Aparecerá la utilidad de búsqueda Eventos. Establezca los criterios de búsqueda adecuados y haga clic en
Ver....



2. A continuación, aparece el Visor de eventos con una lista de eventos que coinciden con los criterios dados. Desplácese por la lista y busque la firma de Solicitud de eco ICMP modificada en los pasos de configuración anteriores.Busque en la columna Eventos el nombre de la firma o busque el número de identificación de la firma en la columna ID de firma.

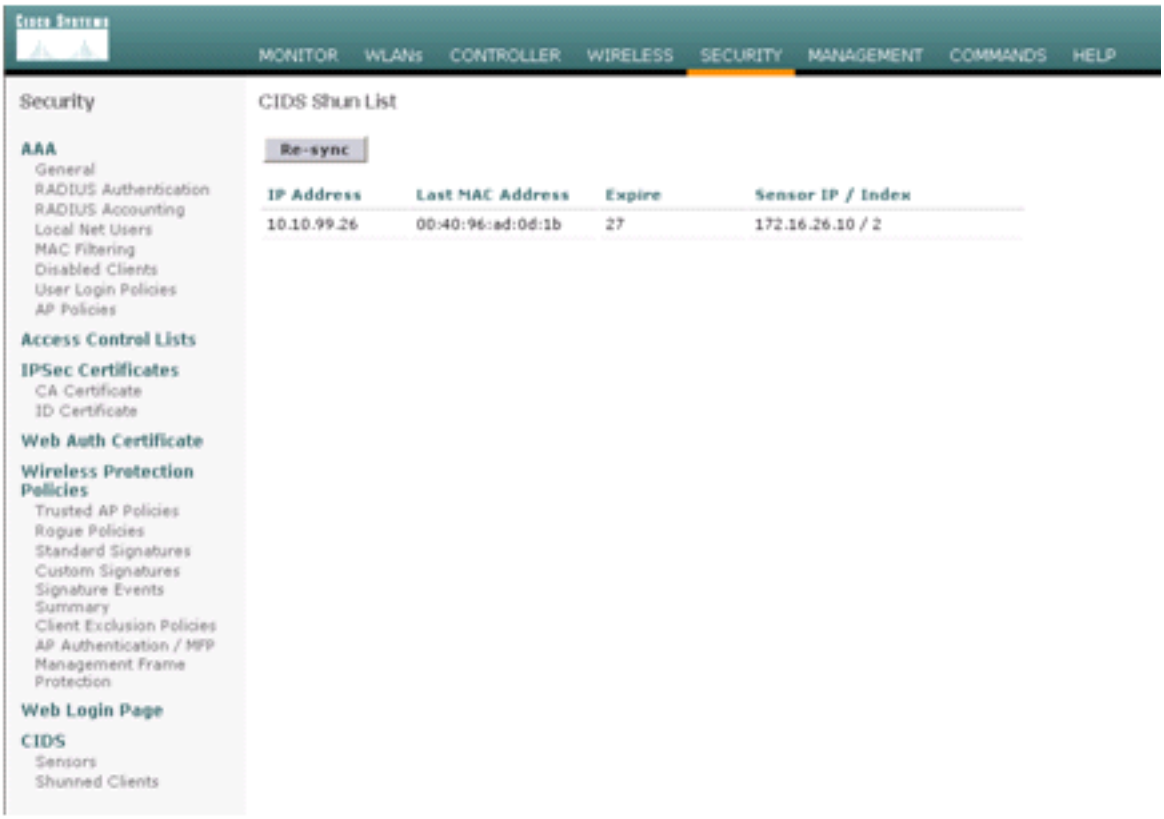


3. Después de localizar la firma, haga doble clic en la entrada para abrir una nueva ventana. La nueva ventana contiene información detallada sobre el evento que desencadenó la firma.

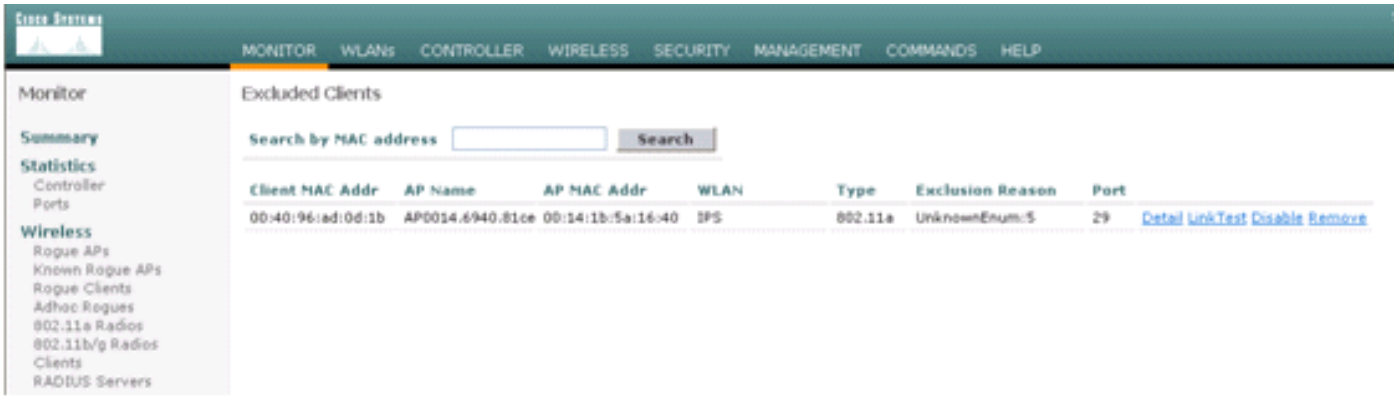


Supervisión de la exclusión de clientes en un controlador inalámbrico

La lista de clientes rechazados en el controlador se rellena en este momento con la dirección IP y MAC del host.



El usuario se agrega a la lista de exclusión de cliente.

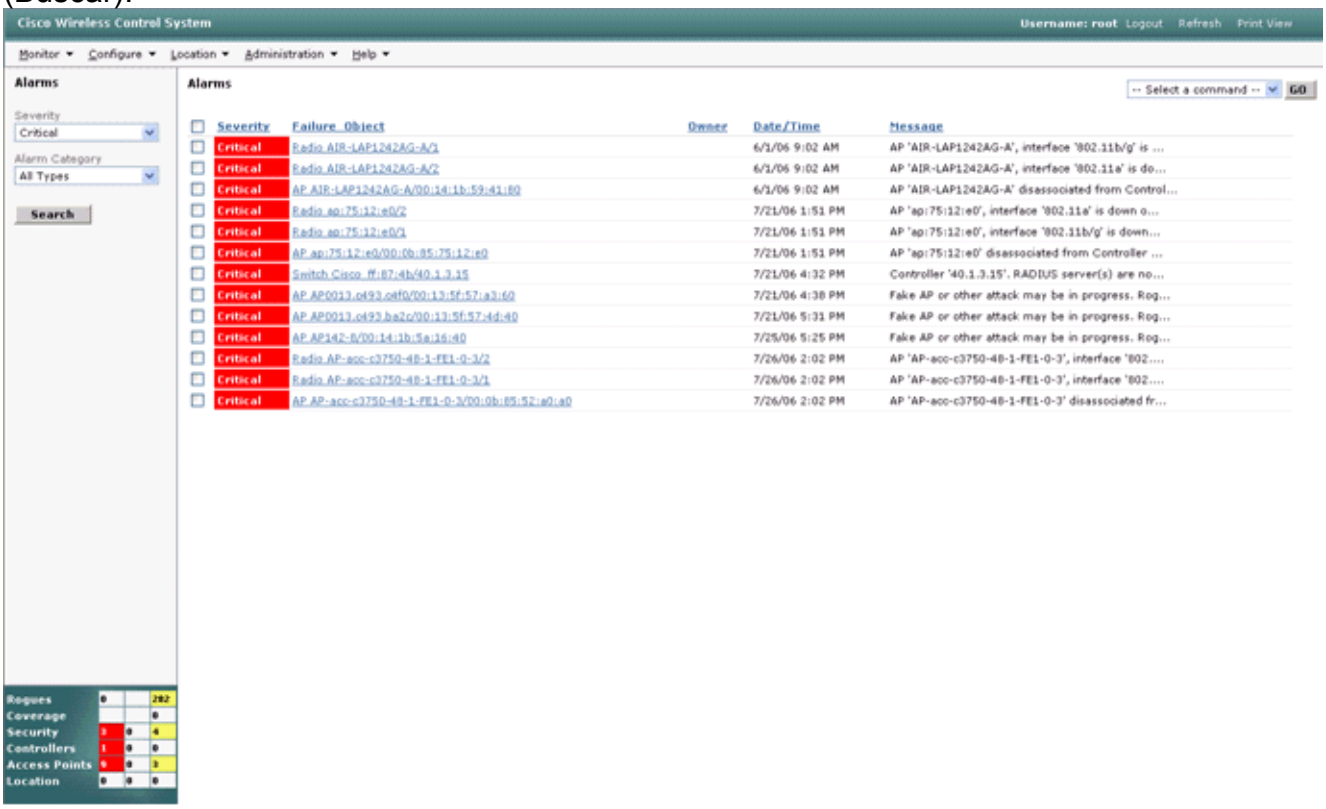


Supervisar eventos en WCS

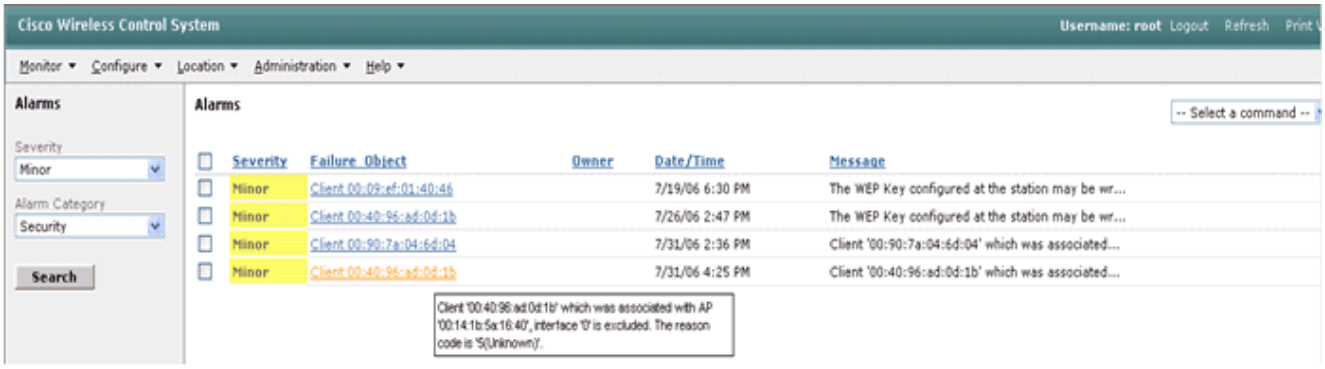
Los eventos de seguridad que activan un bloque dentro del AIP-SSM hacen que el controlador agregue la dirección del infractor a la lista de exclusión del cliente. También se genera un evento en WCS.

1. Utilice la utilidad **Monitor > Alarmas** del menú principal de WCS para ver el evento de exclusión. En un principio, WCS muestra todas las alarmas no despejadas y también presenta una función de búsqueda en el lado izquierdo de la ventana.
2. Modifique los criterios de búsqueda para encontrar el bloque de cliente. En Gravedad, elija **Menor**, y también establezca la Categoría de alarma en **Seguridad**.
3. Haga clic en Search

(Buscar).



4. A continuación, la ventana Alarma sólo muestra alarmas de seguridad con una gravedad mínima. Apunte el ratón al evento que activó el bloque dentro del AIP-SSM.En particular, WCS muestra la dirección MAC de la estación cliente que causó la alarma. Al señalar la dirección adecuada, WCS muestra una pequeña ventana con los detalles del evento. Haga clic en el enlace para ver estos mismos detalles en otra ventana.



Ejemplo de configuración de Cisco ASA

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(2)
!
hostname ciscoasa
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 nameif outside
```

```
 security-level 0
 ip address 10.10.102.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.26.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
pager lines 24
logging asdm informational
mtu inside 1500
mtu management 1500
mtu outside 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
nat-control
global (outside) 102 interface
nat (inside) 102 172.16.26.0 255.255.255.0
nat (inside) 102 0.0.0.0 0.0.0.0
route inside 0.0.0.0 0.0.0.0 172.16.26.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.12 255.255.255.255 inside
http 0.0.0.0 0.0.0.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 50
dhcpd enable management
!
class-map inside-class
 match any
!
!
policy-map inside-policy
 description IDS-inside-policy
```

```
 class inside-class
  ips promiscuous fail-open
!
service-policy inside-policy interface inside
Cryptochecksum:699d110f988e006f6c5c907473939b29
: end
ciscoasa#
```

Configuración de ejemplo del sensor del sistema de prevención de intrusiones de Cisco

```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Tue Jul 25 12:15:19 2006
! ------------------------------
service host
network-settings
host-ip 172.16.26.10/24,172.16.26.1
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2004 0
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service authentication
exit
! ------------------------------
service web-server
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/1
exit
```

```
exit
! ----------------------------
service interface
exit
! ----------------------------
service trusted-certificates
exit
sensor#
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Instalación y uso de Cisco Intrusion Prevention System Device Manager 5.1
- Dispositivos de seguridad adaptable Cisco ASA serie 5500 - Guías de configuración
- Configuración del Sensor del Sistema de Prevención de Intrusiones de Cisco Usando la Interfaz de Línea de Comandos 5.0 - Configuración de Interfaces
- Guía de configuración de WLC 4.0
- Soporte técnico inalámbrico
- Preguntas frecuentes sobre Wireless LAN Controller (WLC)
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Configuración de soluciones de seguridad
- Soporte Técnico y Documentación - Cisco Systems