Regulador del Wireless LAN y guía de integración IPS

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. El IDS/IPS unificado Cisco toma un enfoque amplio a la Seguridad — en el borde inalámbrico, borde atado con alambre, borde PÁLIDO, y a través del centro de datos. Cuando un cliente asociado envía el tráfico malévolo a través de la red del Cisco Unified Wireless, un dispositivo IDS atado con alambre Cisco detecta el ataque y lo envía evita las peticiones a los controladores LAN de la tecnología inalámbrica de Cisco (WLCs), que entonces desasocian el dispositivo del cliente.

El IPS de Cisco es una solución en línea, Basada en red, diseñada para identificar, para clasificar,

y para parar exactamente el tráfico malévolo, incluyendo los gusanos, el spyware/el adware, los virus de la red, y el abuso de la aplicación, antes de que afecten a la continuidad del negocio.

Con la utilización de la versión 5 del software sensor del IPS de Cisco, la solución del IPS de Cisco combina los servicios en línea de la prevención con las Tecnologías innovadoras para mejorar la exactitud. El resultado es confianza total en la protección proporcionada de su solución IPS, sin el miedo del tráfico legítimo que es caído. La solución del IPS de Cisco también ofrece la protección completa de su red con su capacidad única de colaborar con otros recursos de la seguridad de la red y proporciona un enfoque proactivo a la protección de su red.

Los usuarios de las ayudas de la solución del IPS de Cisco paran más amenazas con la mayor confianza con el uso de estas características:

- **Tecnologías en línea exactas de la prevención** — Proporciona la confianza incomparable para tomar medidas preventivas contra una gama más amplia de amenazas sin el riesgo de caer el tráfico legítimo. Estas Tecnologías únicas ofrecen el análisis inteligente, automatizado, del contexto de sus datos y ayudan a asegurarse de que usted recibe la mayoría fuera de su solución de la prevención de intrusiones.
- **identificación de la amenaza del Multi-vector** — Protege su red contra las infracciones de la directiva, las explotaciones de la vulnerabilidad, y la actividad anómala con el examen detallado del tráfico en las capas 2 a 7.
- **Colaboración de la red única** — Aumenta el scalability y la elasticidad con la Colaboración de la red, incluyendo las técnicas de la captura del tráfico, las capacidades del balanceo de carga, y la visibilidad eficientes en el tráfico encriptado.
- **Soluciones completas del despliegue** — Proporciona las soluciones para todos los entornos, de las pequeñas y medianas empresas (SMB) y de las ubicaciones de la sucursal a las instalaciones grandes de la empresa y del proveedor de servicio.
- **Administración, correlación de eventos, y los servicios del soporte potentes** — habilita una solución completa, incluyendo la configuración, la Administración, la correlación de los datos, y los servicios del soporte avanzados. Particularmente el monitorear, el análisis, y el sistema de respuesta del Cisco Security (MARTE) identifica, los aislantes, y recomienda el retiro de la precisión de los elementos que ofenden, para una solución ancha de la prevención de intrusiones de la red. Y el Cisco Incident Control System previene el nuevo gusano y los brotes de virus habilitando la red para adaptar y para proporcionar rápidamente una respuesta distribuida.

Cuando están combinados, estos elementos proporcionan una solución en línea completa de la prevención y le dan la confianza para detectar y para parar el rango más amplio del tráfico malévolo antes de que afecte a la continuidad del negocio. La iniciativa de la red Auto-Defensiva de Cisco pide la Seguridad integrada y incorporada para las soluciones de red. El protocolo actual del Lightweight Access Point (LWAPP) - los sistemas WLAN basados soporta solamente las características básicas IDS debido al hecho de que es esencialmente un sistema de la capa 2 y ha limitado el línea-proceso del poder. Nuevo código de las Versiones de Cisco a tiempo para incluir las nuevas características mejoradas en los nuevos códigos. La versión 4.0 tiene las últimas características que incluyen la integración de un sistema WLAN Lwapp-basado con la línea de producto de Cisco IDS/IPS. En esta versión, la meta es permitir que el sistema de Cisco IDS/IPS dé instrucciones el WLCs para bloquear a ciertos clientes del acceso a las redes inalámbricas cuando un ataque es dondequiera la capa detectada 3 a la capa 7 que implica al cliente en la consideración.

prerrequisitos

Requisitos

Asegúrese de que usted cumpla estos requerimientos mínimos:

- Versión de firmware 4.x del WLC y posterior
- El conocimiento en cómo configurar el IPS de Cisco y el WLC de Cisco es deseable.

Componentes Utilizados

WLC de Cisco

Estos reguladores se incluyen con el Software Release 4.0 para las modificaciones IDS:

- WLC de las Cisco 2000 Series
- WLC de las Cisco 2100 Series
- WLC de las Cisco 4400 Series
- Módulo de servicios de la tecnología inalámbrica de Cisco (WiSM)
- Las Cisco Catalyst 3750G Series unificaron el switch de acceso
- Módulo controlador de LAN de la tecnología inalámbrica de Cisco (WLCM)

Puntos de acceso

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

Administración

- Cisco Wireless Control System (WCS)
- Sensor de las Cisco 4200 Series
- Administración del Cisco IDS - Administrador de dispositivo del Cisco IDS (IDM)

Cisco unificó las Plataformas IDS/IPS

- Sensores Cisco IPS de la serie 4200 con software sensor 5.x del IPS de Cisco o más adelante.
- SSM10 y SSM20 para el Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 con el software sensor 5.x del IPS de Cisco
- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 con el software sensor 5.x del IPS de Cisco
- Módulo de red del Cisco IDS (NM-CIDS) con el software sensor 5.x del IPS de Cisco
- Módulo intrusion detection system 2 (IDSM-2) de las Cisco Catalyst 6500 Series con el software sensor 5.x del IPS de Cisco

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.

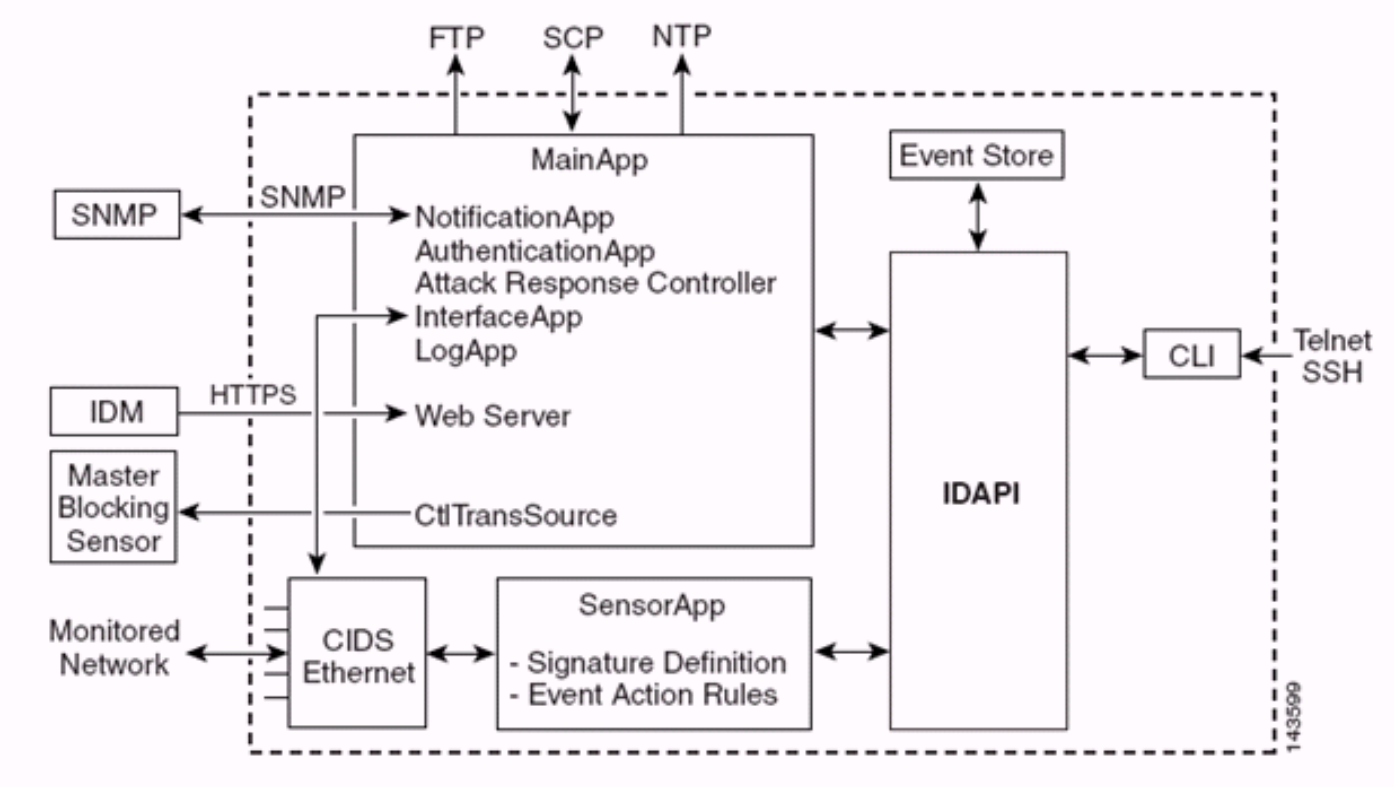
Convenciones

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

Descripción del Cisco IDS

Los componentes importantes del Cisco IDS (versión 5.0) son:

- **App del sensor** — Realiza la captura de paquetes y el análisis.
- **Gestión de la memoria externa del evento y módulo de las acciones** — Proporciona el almacenamiento de las infracciones de la directiva.
- **La proyección de imagen, instala y módulo de lanzamiento** — Las cargas, inicializan, y comienzan todo el software del sistema.
- **Las interfaces de usuario y el UI soportan el módulo** — Proporciona un CLI integrado y el IDM.
- **Sensor OS** — Sistema operativo del host (basado en Linux).



La aplicación del sensor (software IPS) consiste en:

- **App principal** — Inicializa el sistema, comienza y para otras aplicaciones, configura el OS y es responsable de las actualizaciones. Contiene estos componentes:**Servidor de transacción del control** — Permite que los sensores envíen las transacciones del control que se utilizan para habilitar al master del regulador de la respuesta a ataques (conocido antes como regulador del acceso a la red) que bloquea la capacidad del sensor.**Almacén del evento** — Un almacén puesto en un índice usado para salvar los eventos IPS (errores, estatus y mensajes del sistema de la alerta) que es accesible con el CLI, el IDM, el Administrador de dispositivos de seguridad adaptante (ASDM), o el protocolo de intercambio de datos remoto (RDEP).
- **App de la interfaz** — Las manijas desvían y las configuraciones físicas y definen las interfaces emparejadas. Las configuraciones físicas consisten en la velocidad, el duplex, y los estados administrativos.

- **App del registro** — Escribe los mensajes del registro de la aplicación al archivo del registro y a los mensajes de error al almacén del evento.
- **Regulador de la respuesta a ataques (ARCO) (conocido antes como regulador del acceso a la red)** — maneja los dispositivos de red remota (Firewall, Routers, y Switches) para proporcionar el bloqueo de las capacidades cuando ha ocurrido un evento alerta. El ARCO crea y aplica el Listas de control de acceso (ACL) en el dispositivo de red controlado o utiliza el **comando shun** (Firewall).
- **App de la notificación** — Envía el SNMP traps cuando es accionado por una alerta, un estatus, y los eventos de error. El App de la notificación utiliza un agente SNMP del public domain para esto. El SNMP GET proporciona la información sobre la salud de un sensor.**Servidor Web (servidor HTTP RDEP2)** — Proporciona una interfaz del Web User. También proporciona los medios de comunicar con otros dispositivos IPS con RDEP2 usando varios servlets para proporcionar los servicios IPS.**App de la autenticación** — Verifica que autoricen a los usuarios a realizar las acciones CLI, IDM, del ASDM, o RDEP.
- **App del sensor (motor del análisis)** — Realiza la captura de paquetes y el análisis.
- **CLI** — La interfaz se funciona con que cuando los usuarios inician sesión con éxito al sensor con Telnet o SSH. Todas las cuentas creadas con el CLI utilizan el CLI como su shell (a menos que la Cuenta de servicio - se permite solamente una Cuenta de servicio). Los comandos CLI permitidos dependen del privilegio del usuario.

Todas las aplicaciones IPS comunican con uno a través de una interfaz de programación de aplicaciones (API) común llamada IDAPI. Las aplicaciones remotas (los otros sensores, aplicaciones de administración, y software de tercero) comunican con los sensores con RDEP2 y los protocolos del intercambio del evento del dispositivo de seguridad (SDEE).

Debe ser observado que el sensor tiene estas particiones de disco:

- **Partición de aplicación** — Contiene la imagen del sistema completa IPS.
- **División del mantenimiento** — Una imagen IPS del propósito especial usada para rehacer la imagen la partición de aplicación del IDSM-2. Una re-imagen de la división del mantenimiento da lugar a los ajustes de la configuración perdidos.
- **División de la recuperación** — Una imagen del propósito especial usada para la recuperación del sensor. Iniciando en los permisos de la división de la recuperación a los usuarios para rehacer la imagen totalmente la partición de aplicación. Se preservan las configuraciones de red, pero se pierden el resto de las configuraciones.

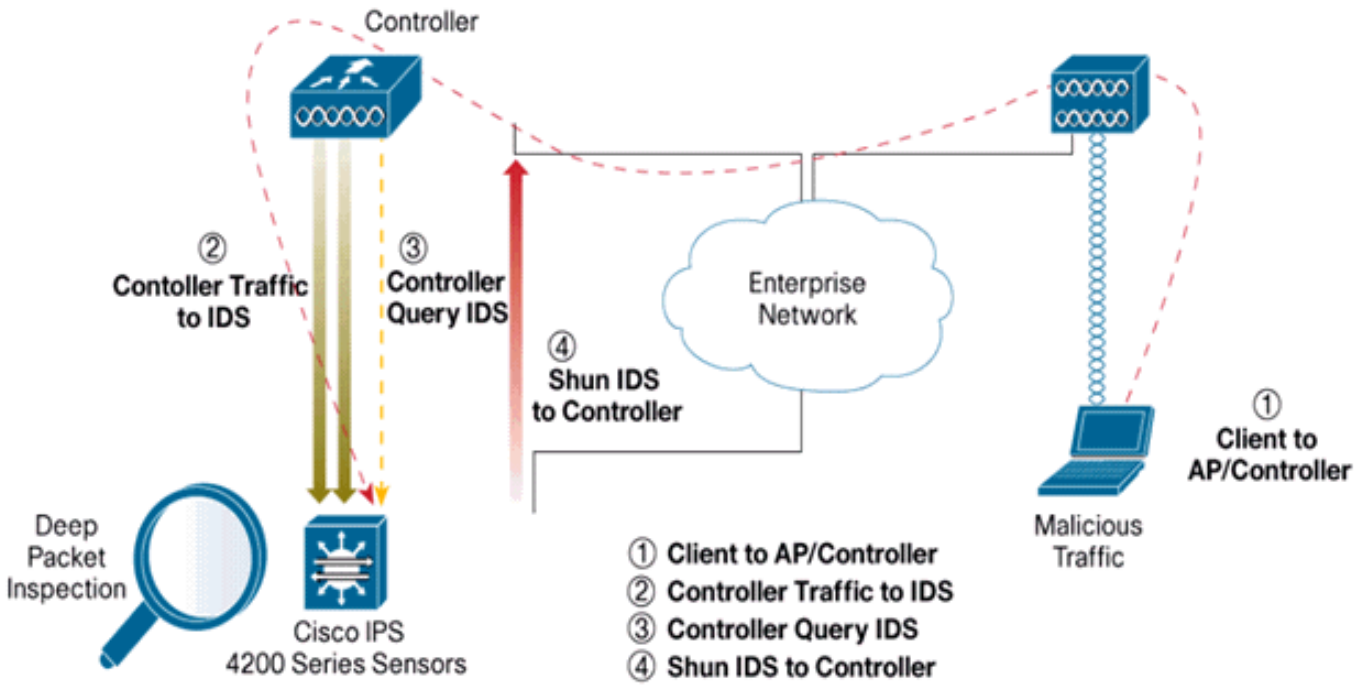
Cisco IDS y WLC – Descripción de la integración

La versión 5.0 del Cisco IDS introduce la capacidad de configurar niega las acciones cuando se detectan las infracciones de la directiva (firmas). De acuerdo con la configuración de usuario en el sistema IDS/IPS, una petición del evitar se puede enviar a un Firewall, a un router, o a un WLC para bloquear los paquetes de un IP Address particular.

Con la versión de software de red del Cisco Unified Wireless 4.0 para los reguladores de la tecnología inalámbrica de Cisco, una petición del evitar necesita ser enviada a un WLC para accionar el cliente que pone o el comportamiento de la exclusión disponible en un regulador. La interfaz que el regulador utiliza para conseguir la petición del evitar es el comando y la interfaz de control en el Cisco IDS.

- El regulador permite que hasta cinco sensores IDS sean configurados en un regulador dado.

- Cada sensor IDS configurado es identificado por su dirección IP o credenciales calificadas del nombre de red y de la autorización.
- Cada sensor IDS se puede configurar en un regulador con una tarifa única de la interrogación en los segundos.



El evitar IDS

El regulador pregunta el sensor a la tarifa configurada de la interrogación para extraer todos los eventos del evitar. Dado evita la petición se distribuye en el grupo entero de la movilidad del regulador que extrae la petición del sensor IDS. Cada uno evita el pedido un dirección IP del cliente está en efecto para el valor especificado de los segundos del descanso. Si el valor de agotamiento del tiempo indica un rato infinito, después el evento del evitar termina solamente si la entrada del evitar se quita en el IDS. El estatus evitado del cliente se mantiene en cada regulador en el grupo de la movilidad incluso si cualquiera o todo el de los reguladores se reajustan.

Nota: La decisión para evitar a un cliente es tomada siempre por el sensor IDS. El regulador no detecta los ataques de la capa 3. Es un proceso lejos más complicado a determinar que el cliente está iniciando un ataque malicioso en la capa 3. Autentican al cliente en la capa 2 que es bastante buena para que el regulador conceda el acceso de la capa 2.

Nota: Por ejemplo, si un cliente consigue una dirección IP (evitada) que ofende anterior asignada, está hasta el descanso del sensor para desbloquear el acceso de la capa 2 para este nuevo cliente. Incluso si el regulador da el acceso en la capa 2, el tráfico del cliente se pudo bloquear en el Routers en la capa 3 de todos modos, porque el sensor también informa al Routers el evento del evitar.

Asuma que un cliente tiene dirección IP A. Ahora, cuando el regulador sondea el IDS para evite los eventos, el IDS envía la petición del evitar al regulador con la dirección IP A como el IP Address de destino. Ahora, el negro del regulador enumera a este cliente A. En el regulador, los clientes son minusválidos basados en una dirección MAC.

Ahora, asuma que el cliente cambia su dirección IP de A al B. Durante la encuesta siguiente, el

regulador consigue una lista de clientes evitados basados en la dirección IP. Otra vez, la dirección IP A todavía está en la lista evitada. Pero puesto que el cliente ha cambiado su dirección IP de A a B (que no está en la lista evitada de IP Addresses), liberan a este cliente con una nueva dirección IP de B una vez que el descanso de los clientes mencionados negros se alcanza en el regulador. Ahora, el regulador comienza a no prohibir a este cliente con nuevo la dirección IP de B (solamente del MAC Address del cliente permanece lo mismo).

Por lo tanto, aunque un cliente siga siendo discapacitado para la duración del tiempo de la exclusión del regulador y re-se excluya si las readquieras su DHCP Address anterior, ese cliente se inhabilita no más si la dirección IP del cliente que es cambios evitados. Por ejemplo, si el cliente conecta con la misma red y el descanso del arriendo del DHCP no se expira.

Conexión del soporte de los reguladores solamente al IDS para el cliente que evita las peticiones que utilizan el puerto de administración en el regulador. El regulador conecta con el IDS para la inspección de paquetes vía las interfaces VLAN aplicables que llevan el tráfico del cliente de red inalámbrica.

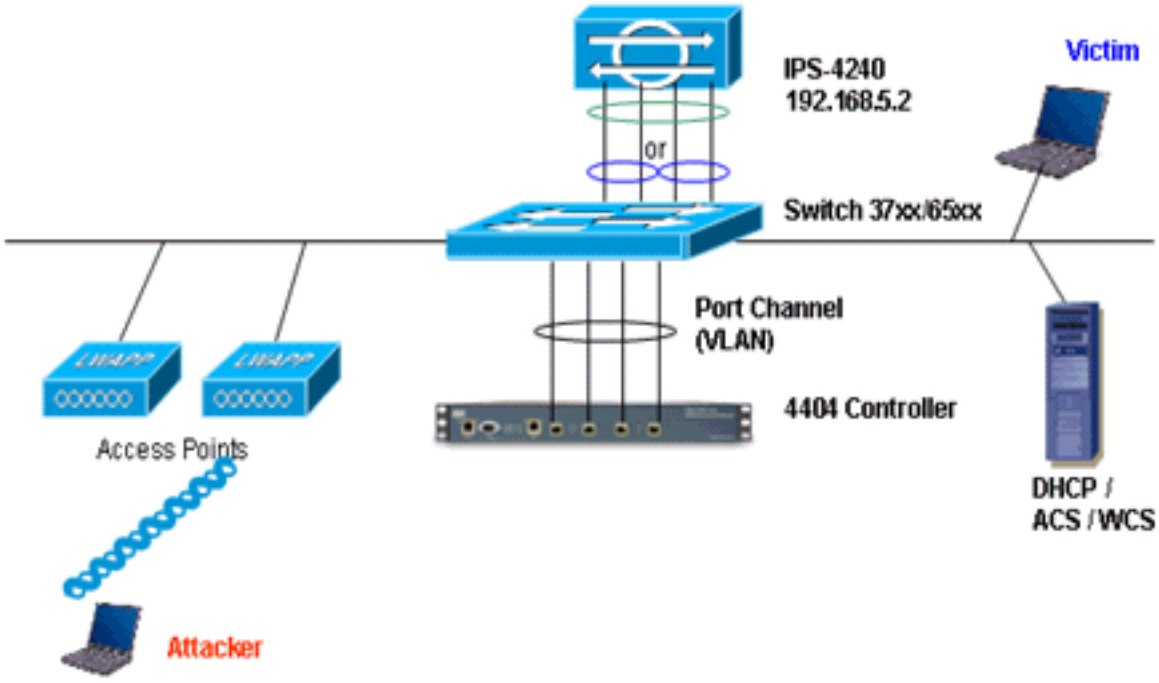
En el regulador, la página de los clientes de la neutralización muestra a cada cliente que se ha inhabilitado vía una petición del sensor IDS. El comando cli show también visualiza una lista de clientes puestos.

En el WCS, visualizan a los clientes excluidos bajo lengueta del submarino de la Seguridad.

Aquí están los pasos a seguir para completar la integración de los sensores del IPS de Cisco y del WLCs de Cisco.

1. Instale y conecte el ids appliance en el mismo Switch donde reside el regulador inalámbrico.
2. Duplique el (SPAN) los puertos del WLC que llevan el tráfico del cliente de red inalámbrica al ids appliance.
3. El ids appliance recibe una copia de cada paquete y examina el tráfico en la capa 3 a 7.
4. El ids appliance ofrece un archivo de firma transferible, que puede también ser personalizado.
5. El ids appliance genera la alarma con una acción del evento de evita cuando se detecta una firma del ataque.
6. El WLC sondea el IDS para las alarmas.
7. Cuando una alarma con la dirección IP de un cliente de red inalámbrica, que se asocia al WLC, se detecta, pone al cliente en la lista de la exclusión.
8. Un desvío es generado por el WLC y se notifica el WCS.
9. Quitan al usuario de la lista de la exclusión después del periodo de tiempo especificado.

Diseño de la arquitectura de red



El WLC de Cisco está conectado con las interfaces Gigabit en el Catalyst 6500. Cree un canal del puerto para las interfaces Gigabit y habilite la agregación del link (RETRASO) 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 regulador está conectado para interconectar el gigabit 5/1 y el 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 actuar individualmente en el **modo promiscuo** o usted puede emparejarlas para crear las interfaces en línea para el **modo de detección en línea**.

En el modo promiscuo, los paquetes no atraviesan el sensor. El sensor analiza una copia del tráfico monitoreado bastante que el paquete remitido real. La ventaja del funcionamiento en el modo promiscuo es que el sensor no afecta al flujo de paquetes con el tráfico remitido.

Nota: El diagrama de la arquitectura es apenas una configuración del ejemplo del WLC y del IPS de arquitectura integrada. El ejemplo de configuración mostrado aquí explica el IDS que detecta la interfaz que actúa en el modo promiscuo. El diagrama de la arquitectura muestra las interfaces de detección que son emparejadas junto para actuar en el modo en línea de los pares. Refiera al modo en línea para más información sobre el modo en línea de la interfaz.

En esta configuración, se asume que la interfaz de detección actúa en el modo promiscuo. La interfaz de la supervisión del sensor del Cisco IDS está conectada con la interfaz Gigabit 5/3 en el Catalyst 6500. Cree a una sesión de monitoreo en el Catalyst 6500 donde está la fuente la

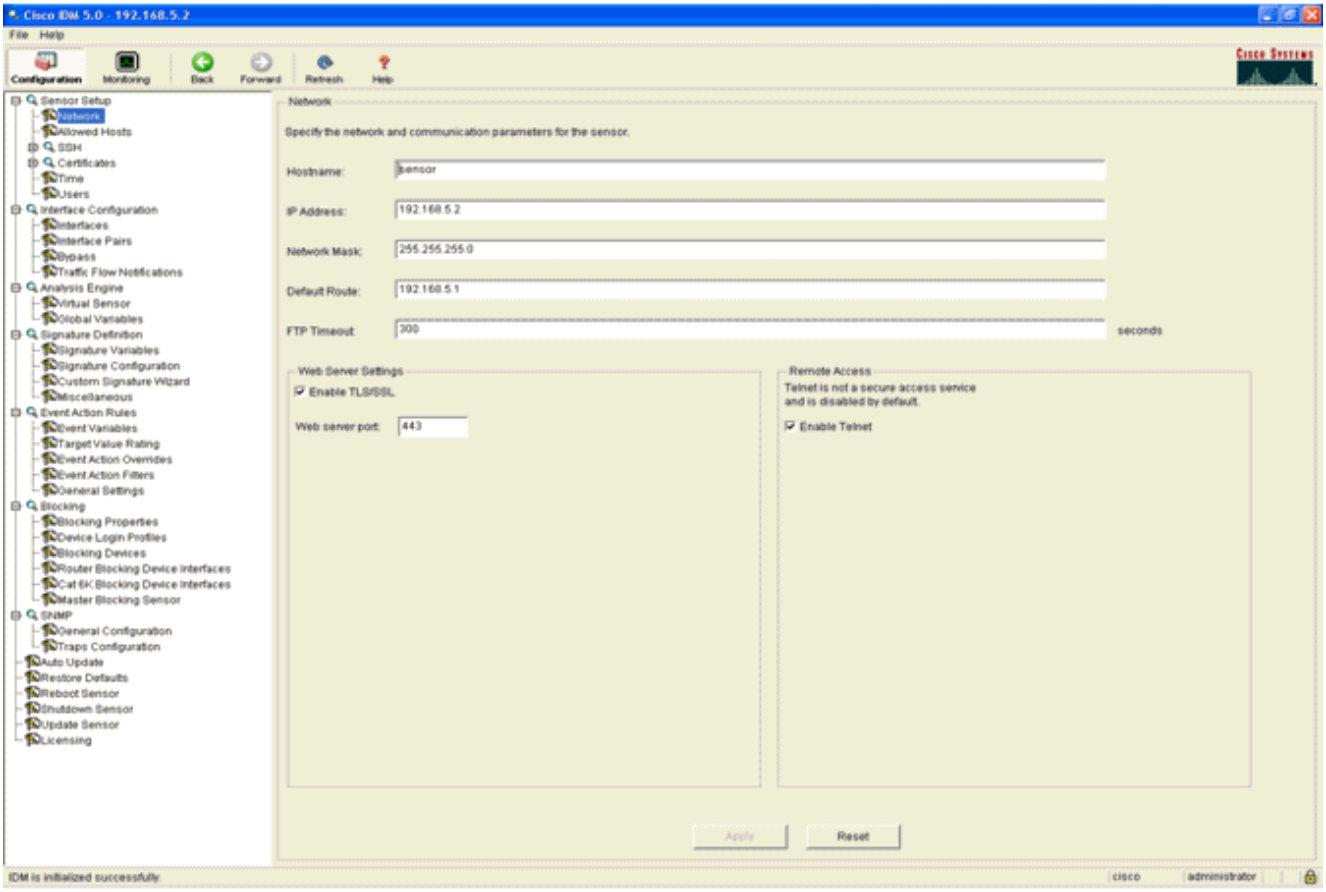
interfaz de canal de puerto de los paquetes y el destino es la interfaz Gigabit donde la interfaz de la supervisión del sensor del IPS de Cisco está conectada. Esto replica todo el ingreso y tráfico de salida de las interfaces atadas con alambre regulador al IDS para el examen de la capa 3 a de la capa 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#
```

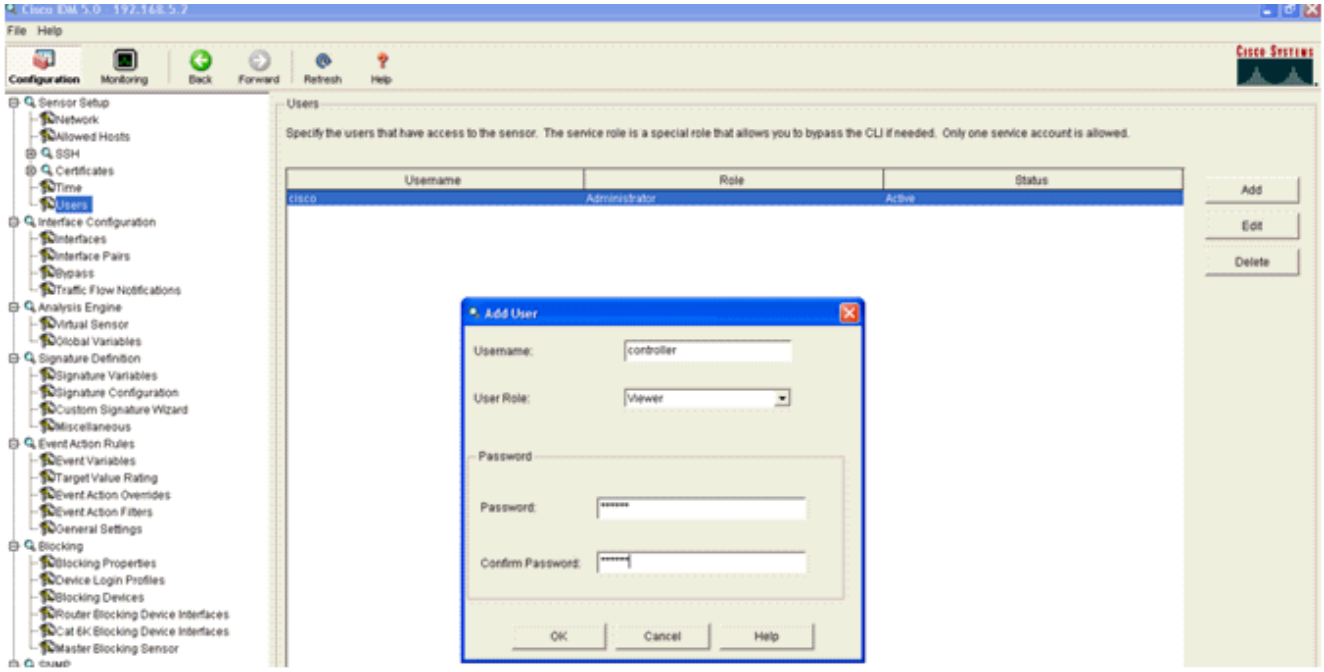
Configure el sensor del Cisco IDS

La configuración inicial del sensor del Cisco IDS es hecha del puerto de la consola o conectando un monitor y un teclado con el sensor.

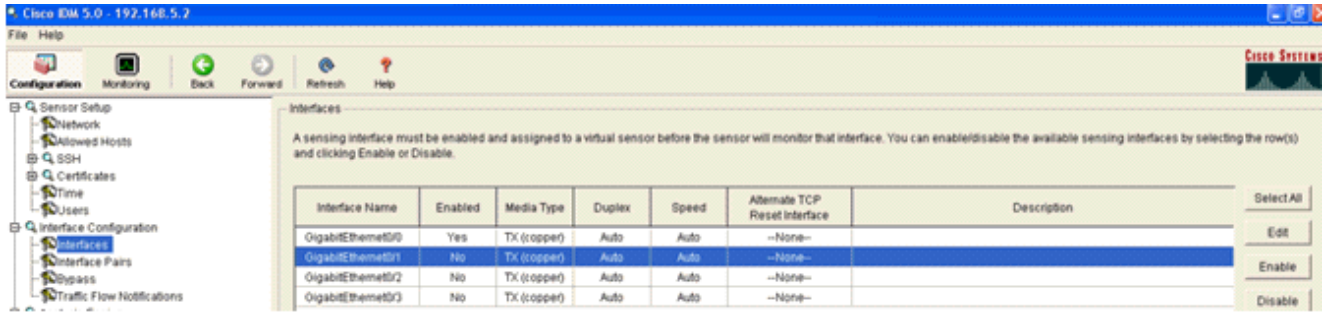
1. Login al dispositivo:Conecte un puerto de la consola con el sensor.Conecte un monitor y un teclado con el sensor.
2. Teclee su nombre de usuario y contraseña en el prompt de inicio de sesión.**Nota:** El nombre de usuario predeterminado y la contraseña son ambo Cisco. A le indican que los cambie la primera vez que usted inicia sesión al dispositivo. Usted debe primero ingresar la contraseña UNIX, que es Cisco. Entonces usted debe ingresar 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 el comando y la interfaz de control en el IDS usado para comunicar con el regulador. Este direccionamiento debe ser routable a la interfaz de administración del regulador. Las interfaces de detección no requieren la dirección. La lista de acceso debe incluir el direccionamiento de la interfaz de administración de los reguladores, así como los direccionamientos permisibles 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. Usted puede ahora configurar el sensor IPS del GUI. Señale al navegador al IP Address de administración del sensor. Este visualizaciones de imágenes una muestra donde el sensor se configura con
192.168.5.2.



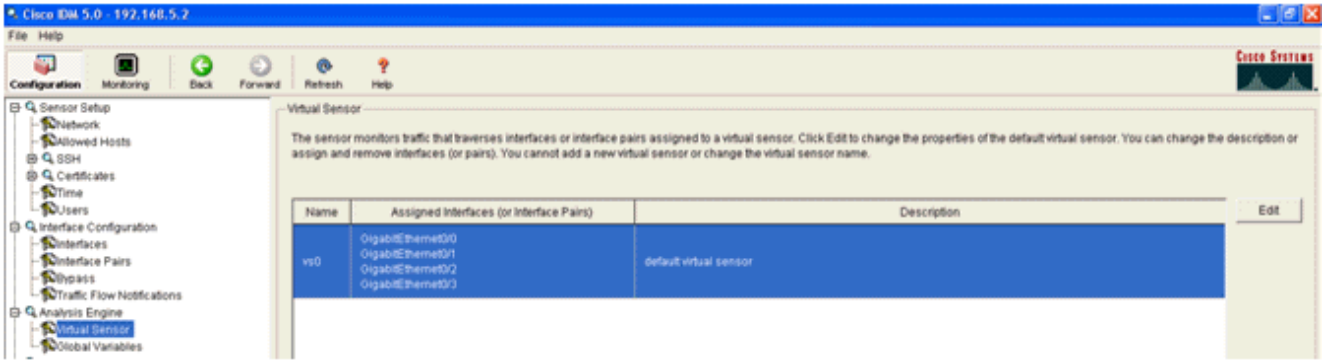
5. Agregue a un usuario que el WLC utilice para acceder los eventos del sensor IPS.



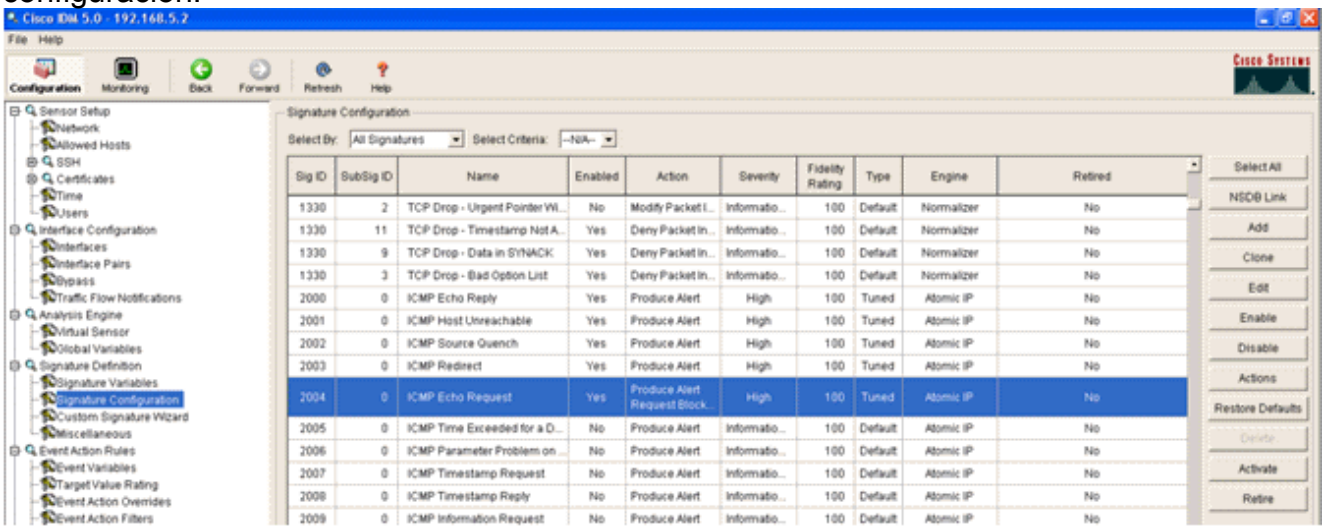
6. Habilite las interfaces de la supervisión.



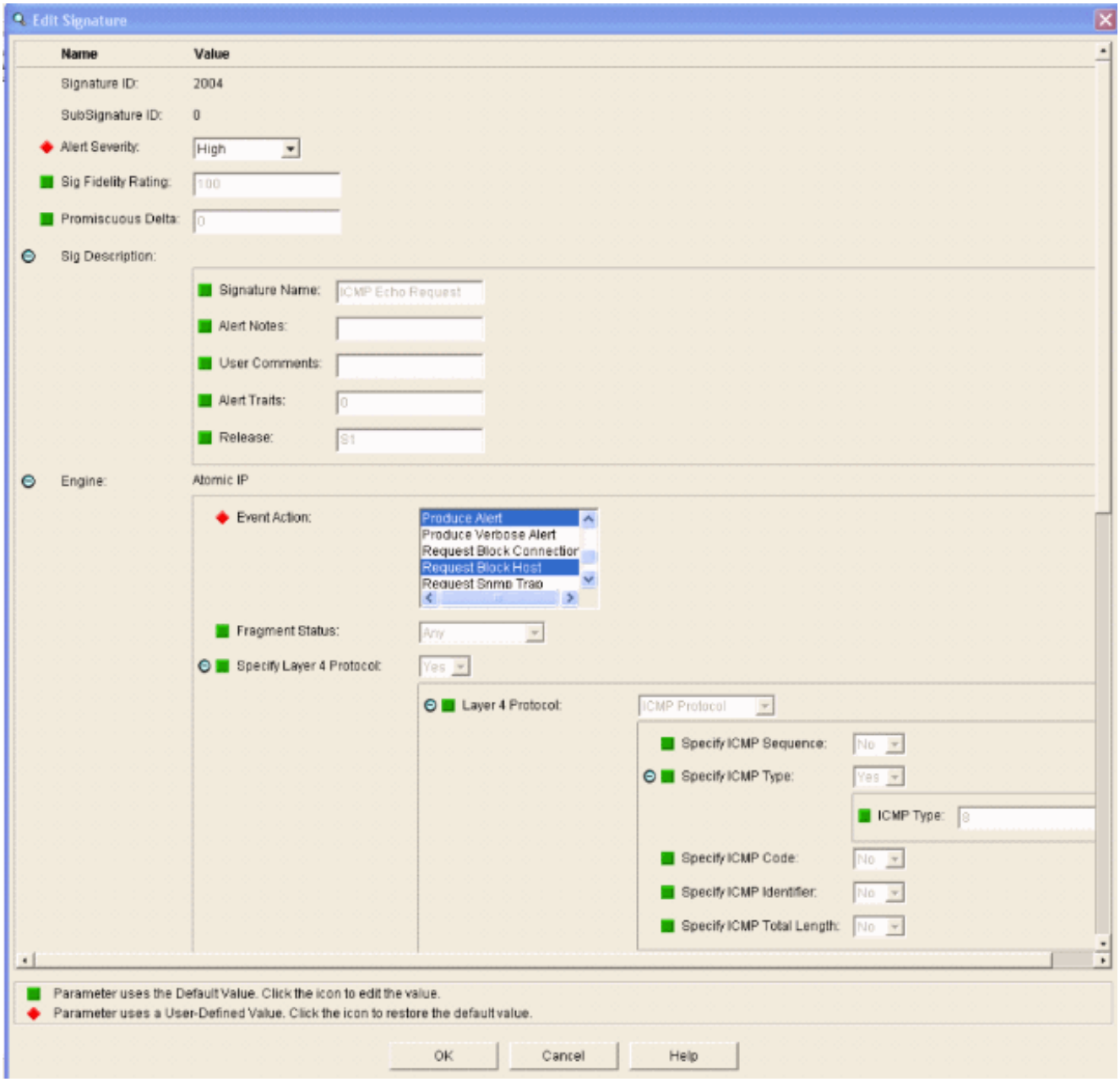
Las interfaces de la supervisión se deben agregar al motor del análisis, pues esta ventana muestra:



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



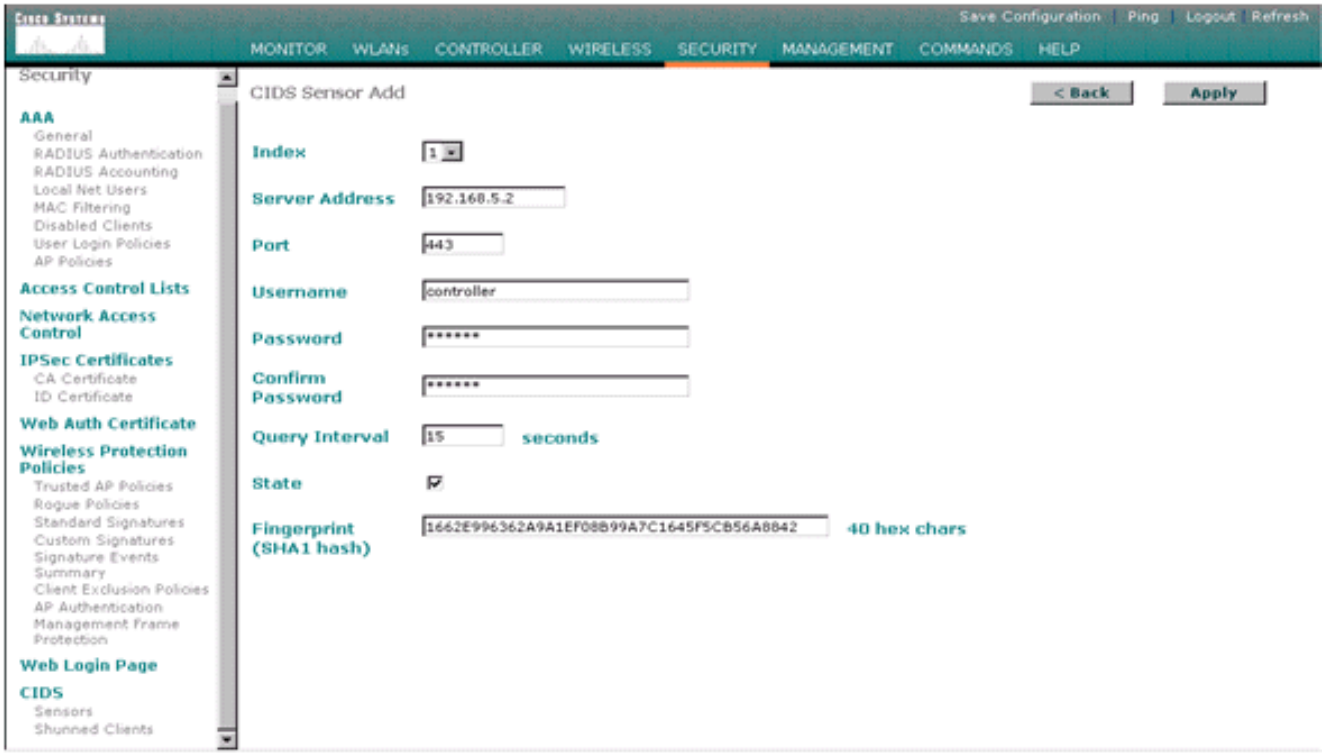
La firma se debe habilitar, conjunto alerta de la gravedad al **alto** y conjunto de la acción del evento **para producir la alerta** y el **host del bloque de petición** para que este paso de verificación sea
completado.



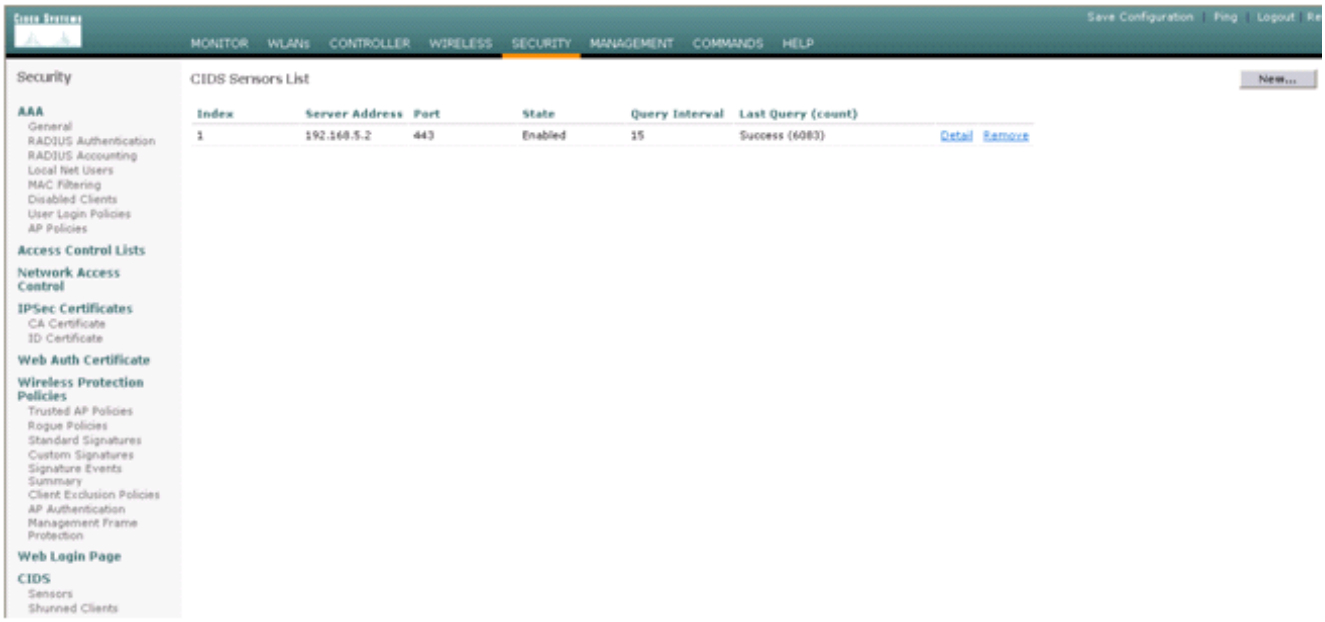
Configure el WLC

Complete estos pasos para configurar el WLC:

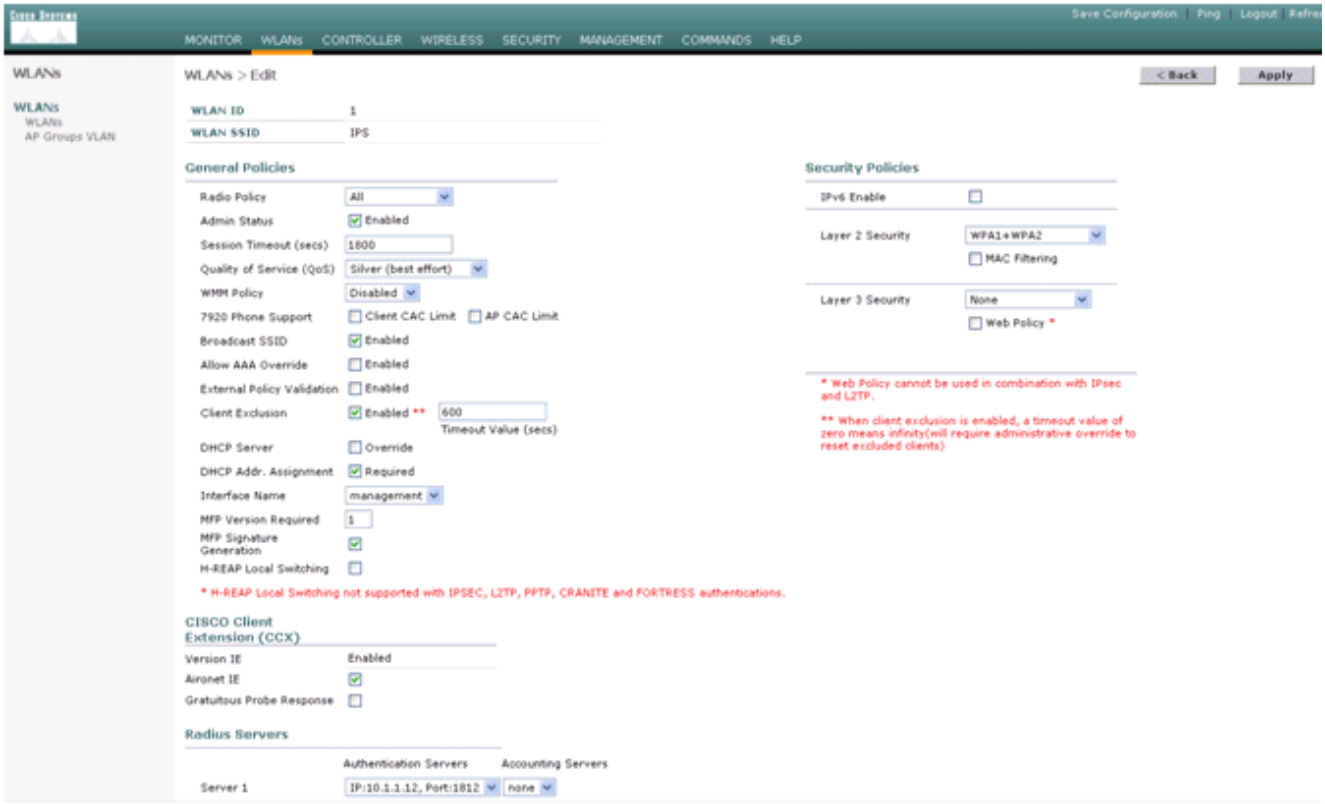
1. Una vez que el dispositivo IPS se configura y alista para ser agregado en el regulador, elija la **Seguridad > los CID > los sensores > nuevo**.
2. Agregue la dirección IP, número del puerto TCP, nombre de usuario y contraseña que usted creó previamente.Para obtener la huella dactilar del sensor IPS, ejecute este comando en el sensor IPS y agregue la huella dactilar SHA1 en el WLC (sin los dos puntos). Esto se utiliza para asegurar la comunicación de la interrogación regulador-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`



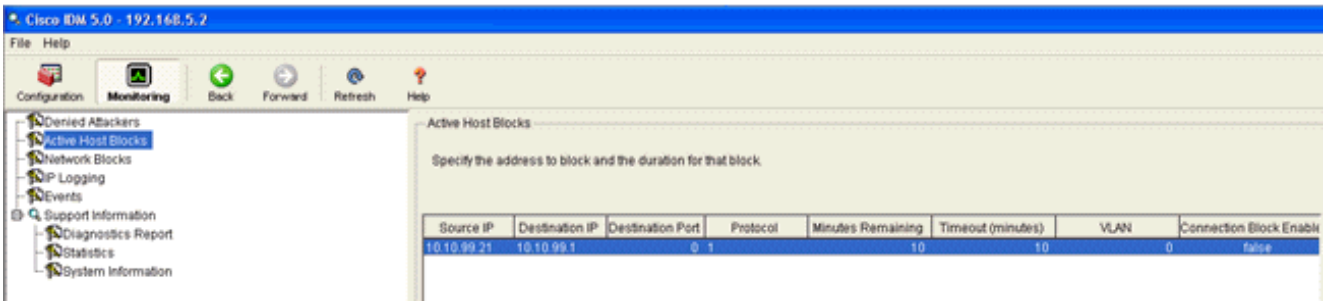
3. Marque el estatus de la conexión entre el sensor IPS y el WLC.



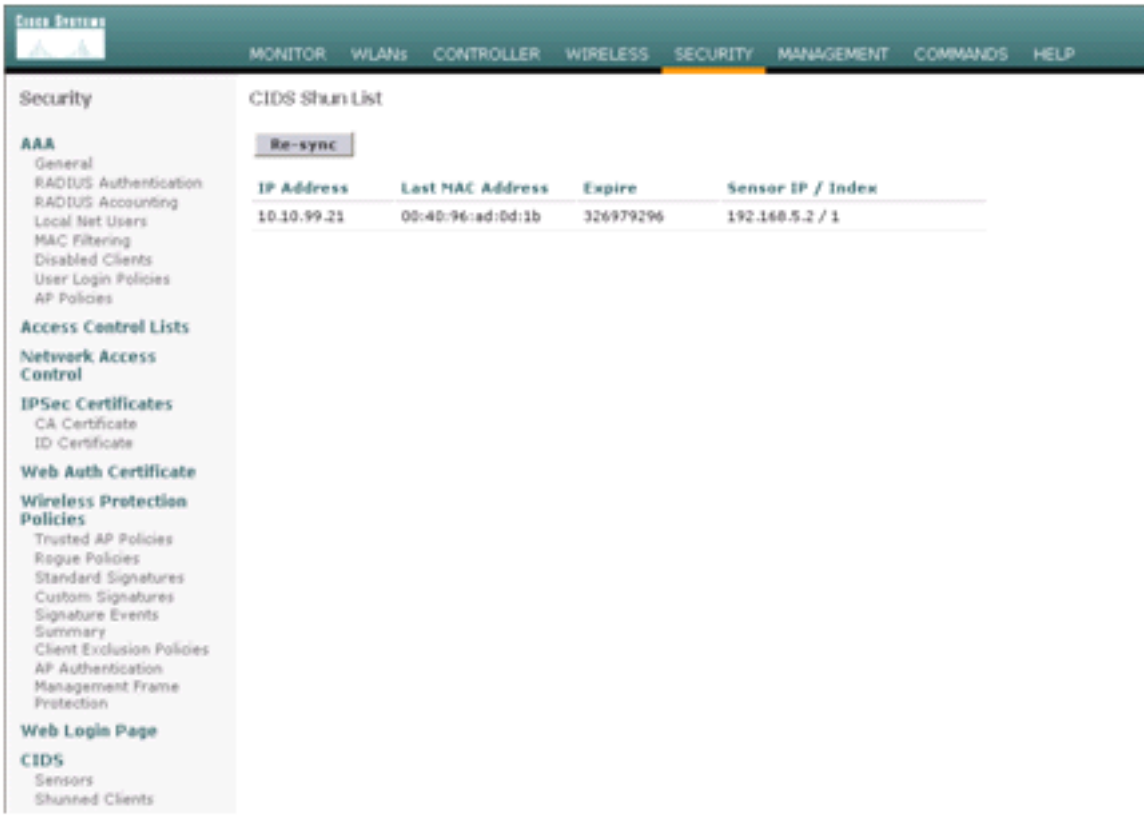
4. Una vez que usted establece la Conectividad con el sensor del IPS de Cisco, aseegurese la configuración de la red inalámbrica (WLAN) está correcto y eso usted habilita la **exclusión del cliente**.El valor de agotamiento del tiempo predeterminado de la exclusión del cliente es 60 segundos. También observe que sin importar el temporizador de la exclusión del cliente, persiste la exclusión del cliente mientras el bloque del cliente invocado por el IDS siga siendo activo. El tiempo predeterminado del bloque en el IDS es 30 minutos.



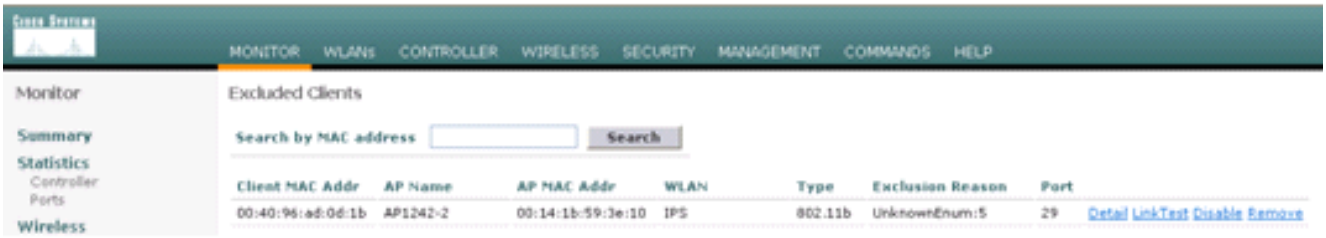
5. Usted puede accionar un evento en el sistema del IPS de Cisco cualquiera cuando usted hace una exploración NMAP a ciertos dispositivos en la red o cuando usted hace un ping a algunos host monitoreados por el sensor del IPS de Cisco. Una vez que una alarma se acciona en el IPS de Cisco, vaya a los **bloques el monitorear y del host activo** para marcar los detalles sobre el
host.



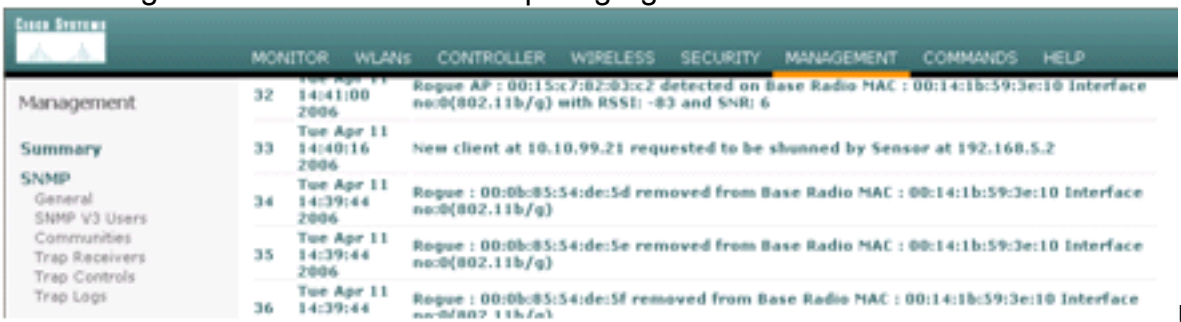
Los clientes evitados enumeran en el regulador ahora se pueblan con el IP y la dirección MAC del

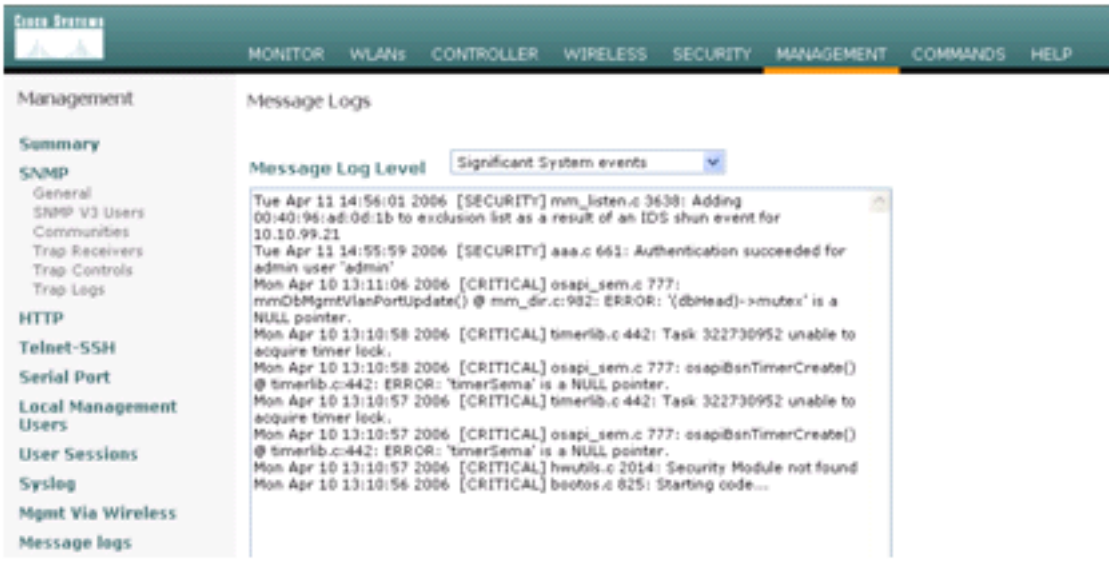


host. Agrega n al usuario a la lista de la exclusión del cliente.

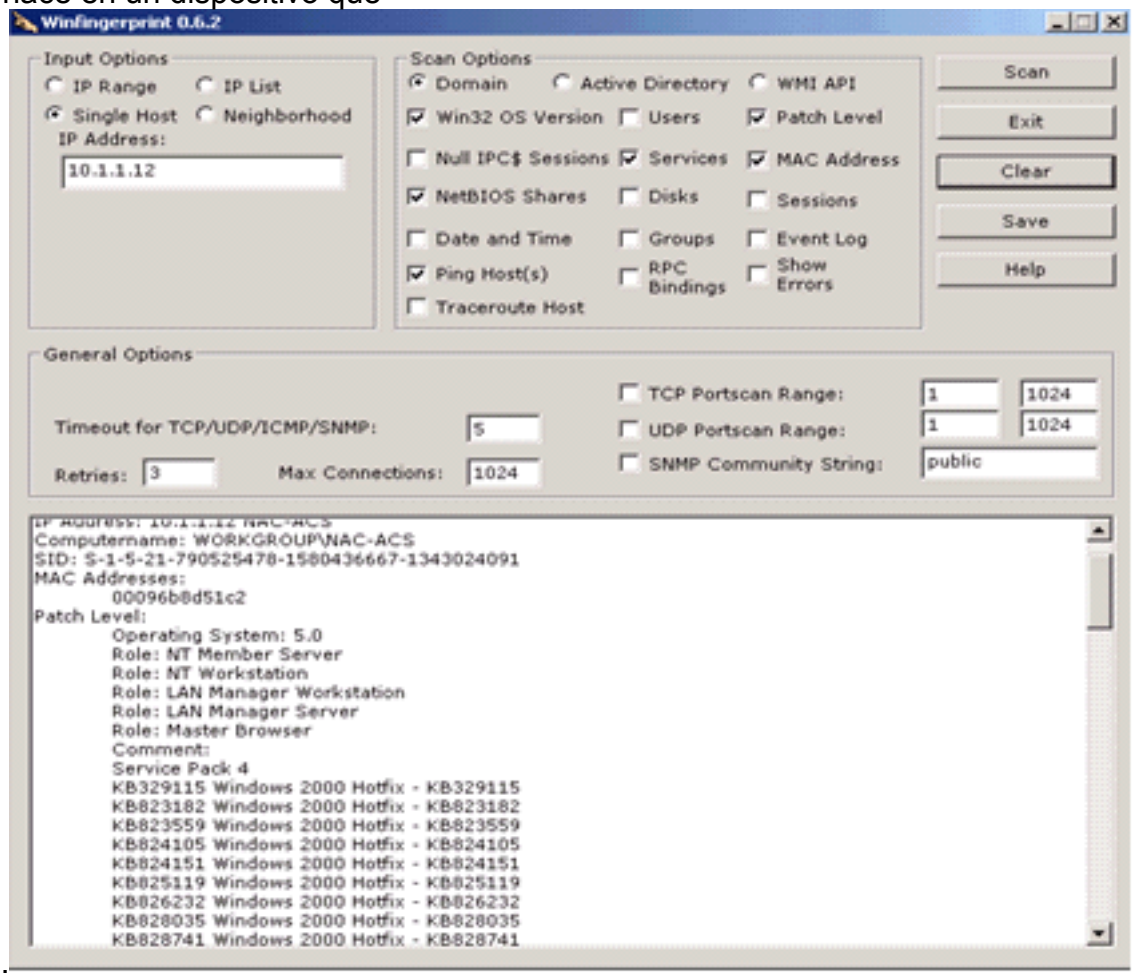


Se genera un registro del desvío mientras que agregan a un cliente a la lista del evitar. Un registro de mensajes también se genera para el

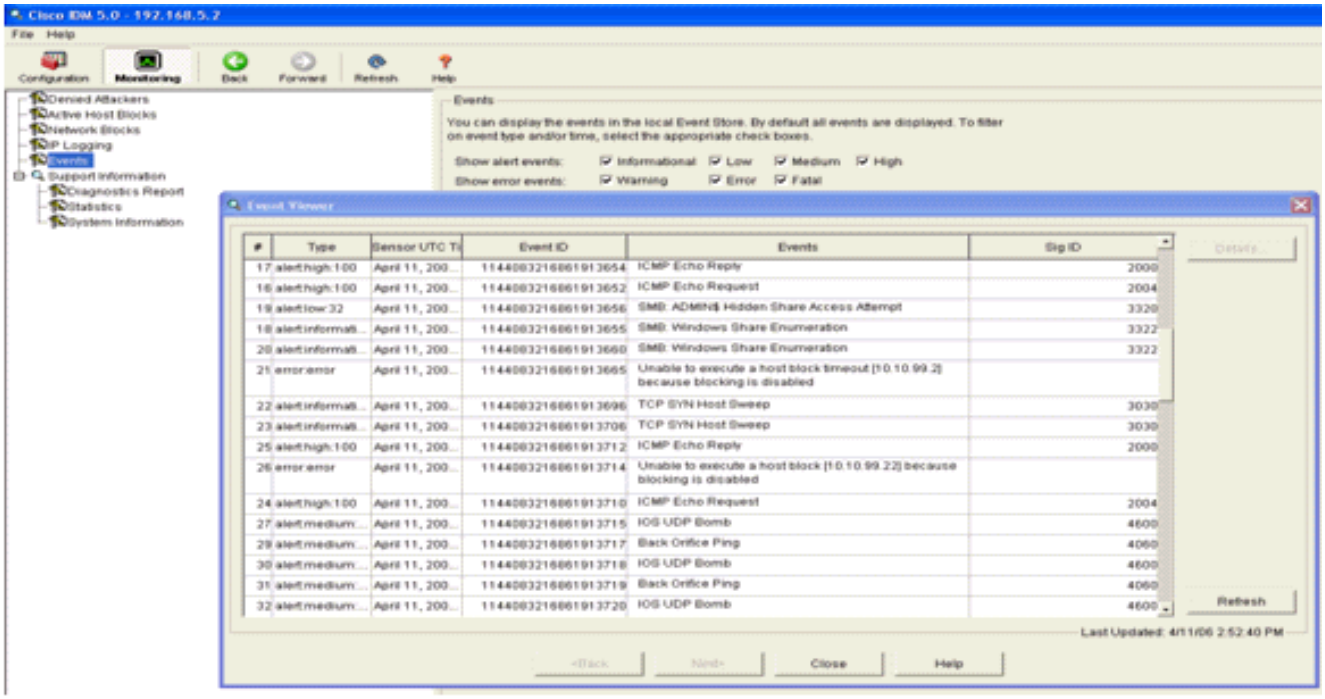




evento. Alguno
s eventos adicionales se generan en el sensor del IPS de Cisco cuando una exploración NMAP se hace en un dispositivo que



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



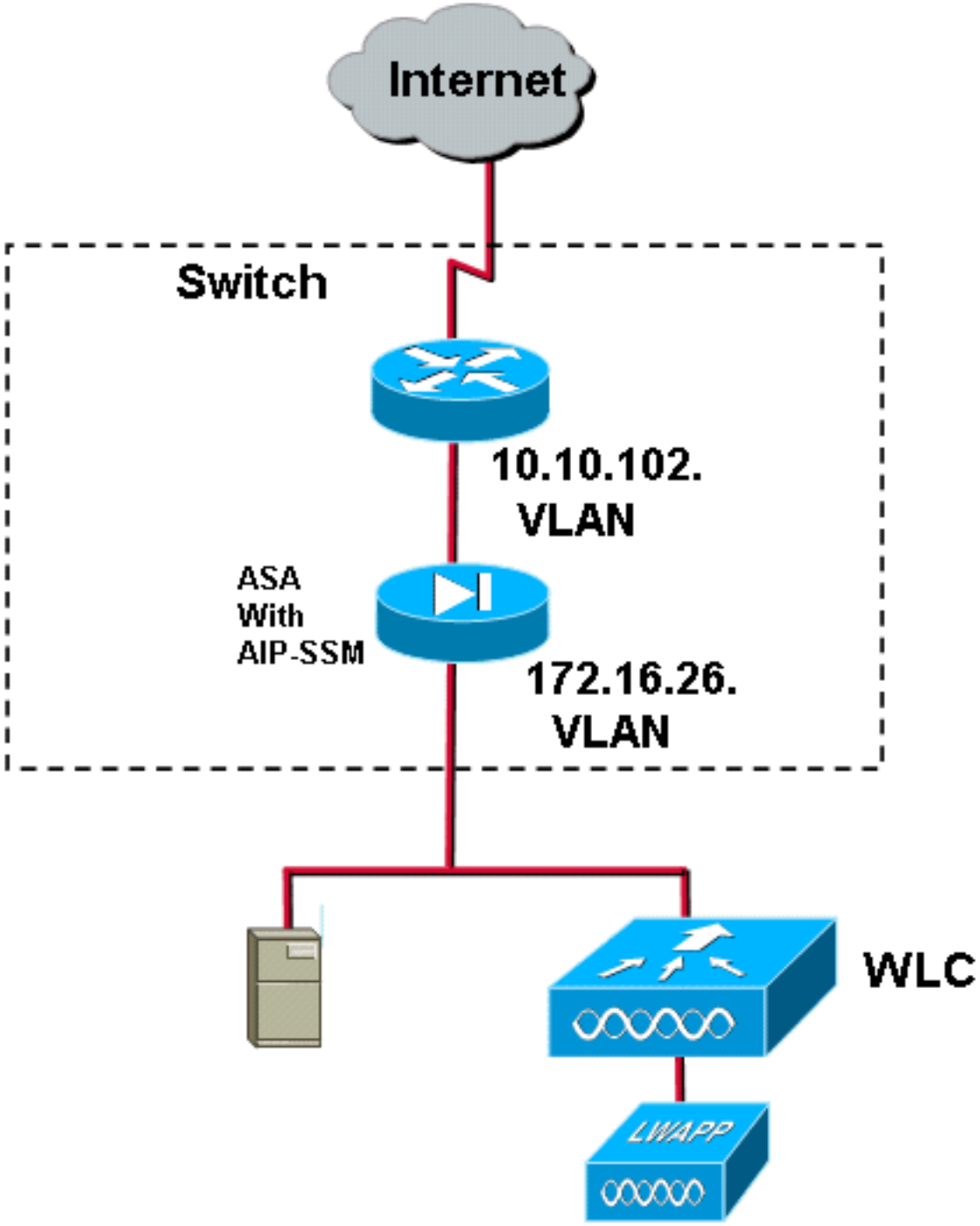
Configuración de muestra del sensor del Cisco IDS

Ésta es la salida de la secuencia de comandos 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#
```

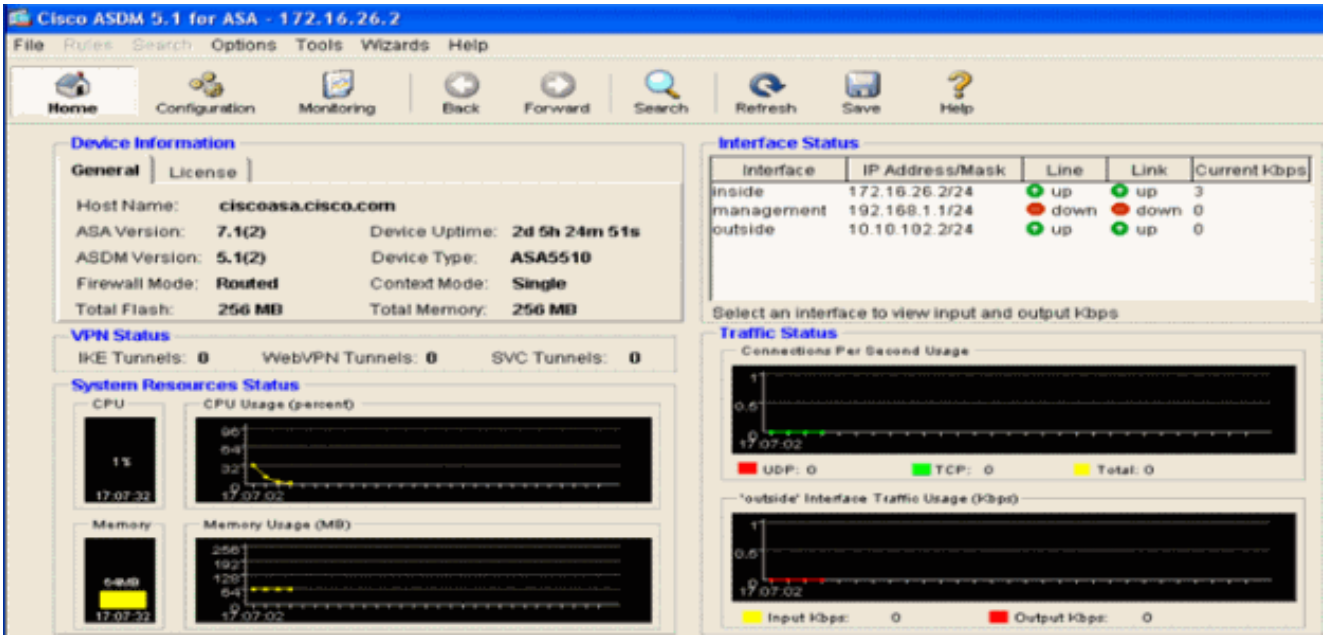
Configure un ASA para el IDS

A diferencia de un sensor tradicional de la detección de intrusos, un ASA debe siempre estar en el trayecto de datos. Es decir en vez de atravesar el tráfico de un puerto del switch encima a un puerto pasivo el oler en el sensor, el ASA debe recibir los datos sobre una interfaz, la procesa internamente, y después le remite hacia fuera otro puerto. Para el IDS, utilice el Marco de políticas modular (MPF) para copiar el tráfico que el ASA recibe encima al módulo de Servicios de seguridad avanzado interno del examen y de la prevención (AIP-SSM) para el examen.

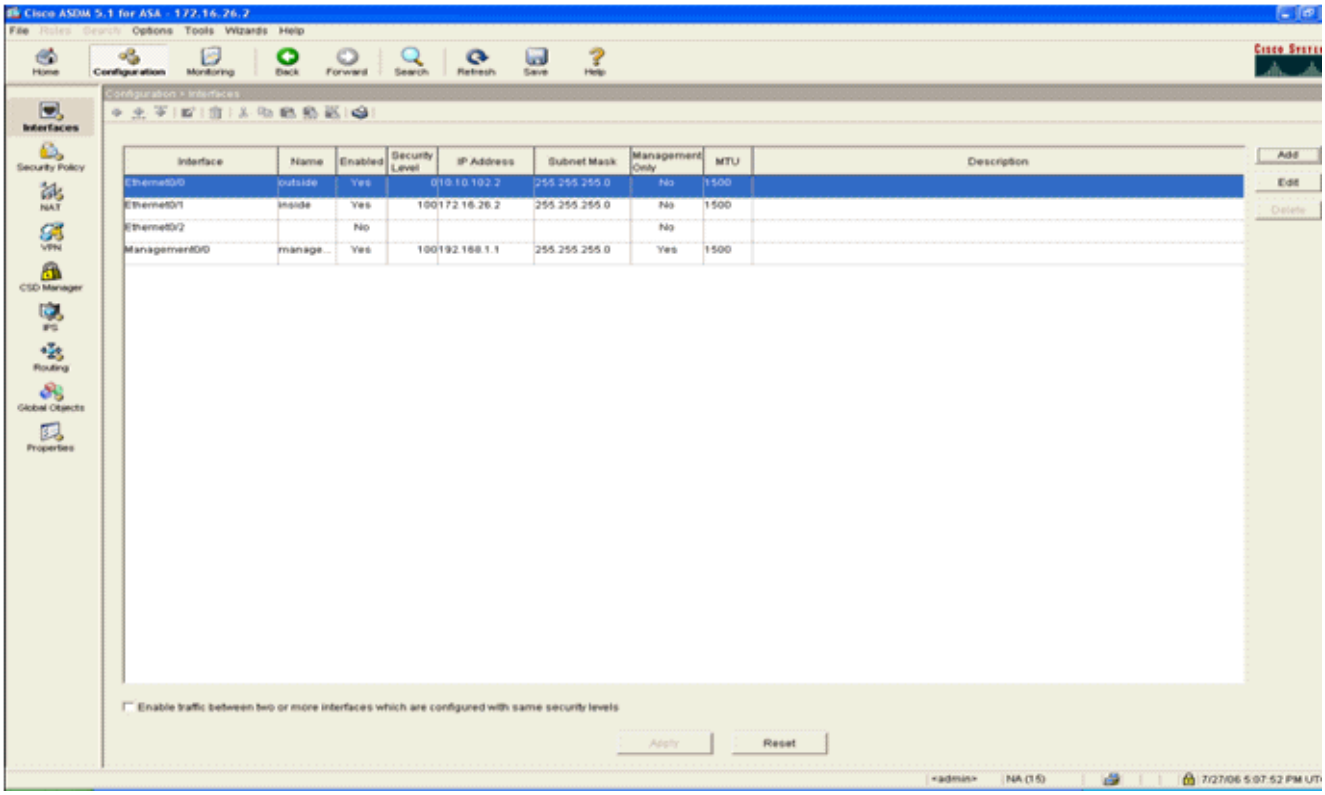


En este ejemplo, el ASA usado se pone y pasa ya el tráfico. Estos pasos demuestran cómo crear una directiva que envíe los datos al AIP-SSM.

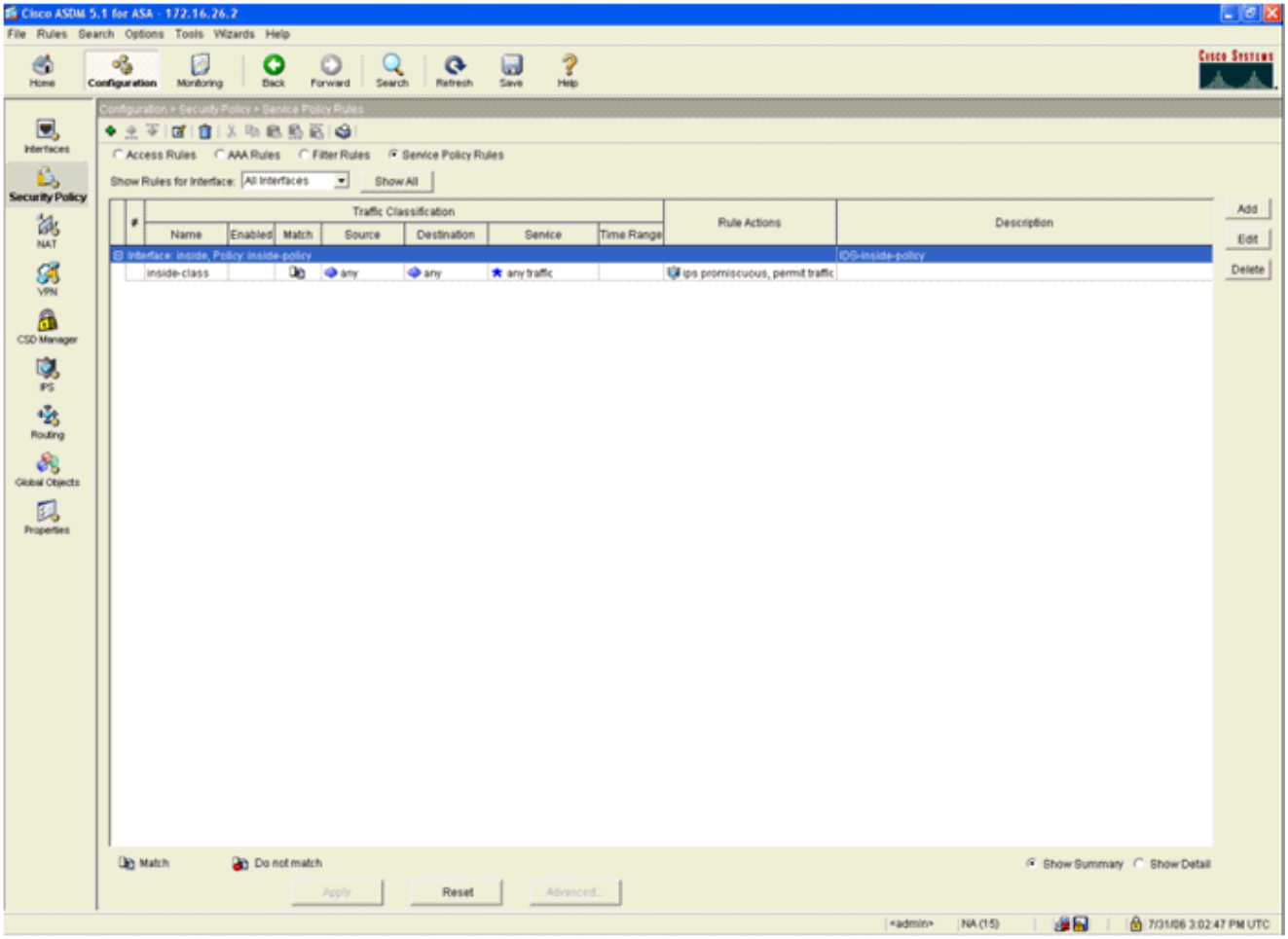
1. Registro en el ASA usando el ASDM. Sobre la registración satisfactoria, la ventana del sistema principal ASA
   aparece.



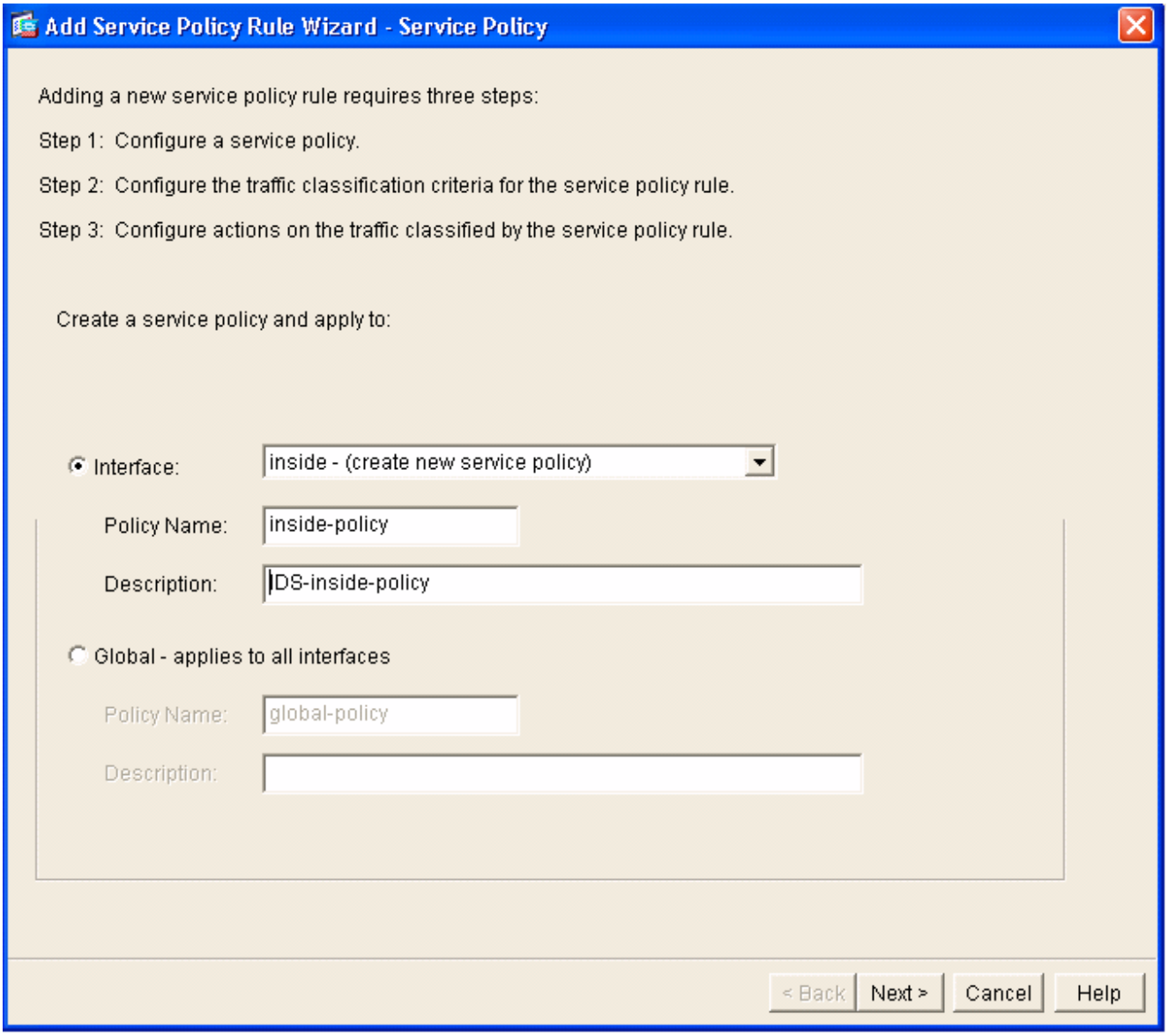
2. **Configuración del** tecleo en la cima de la página. El Switches de la ventana a una vista del ASA
interconecta.



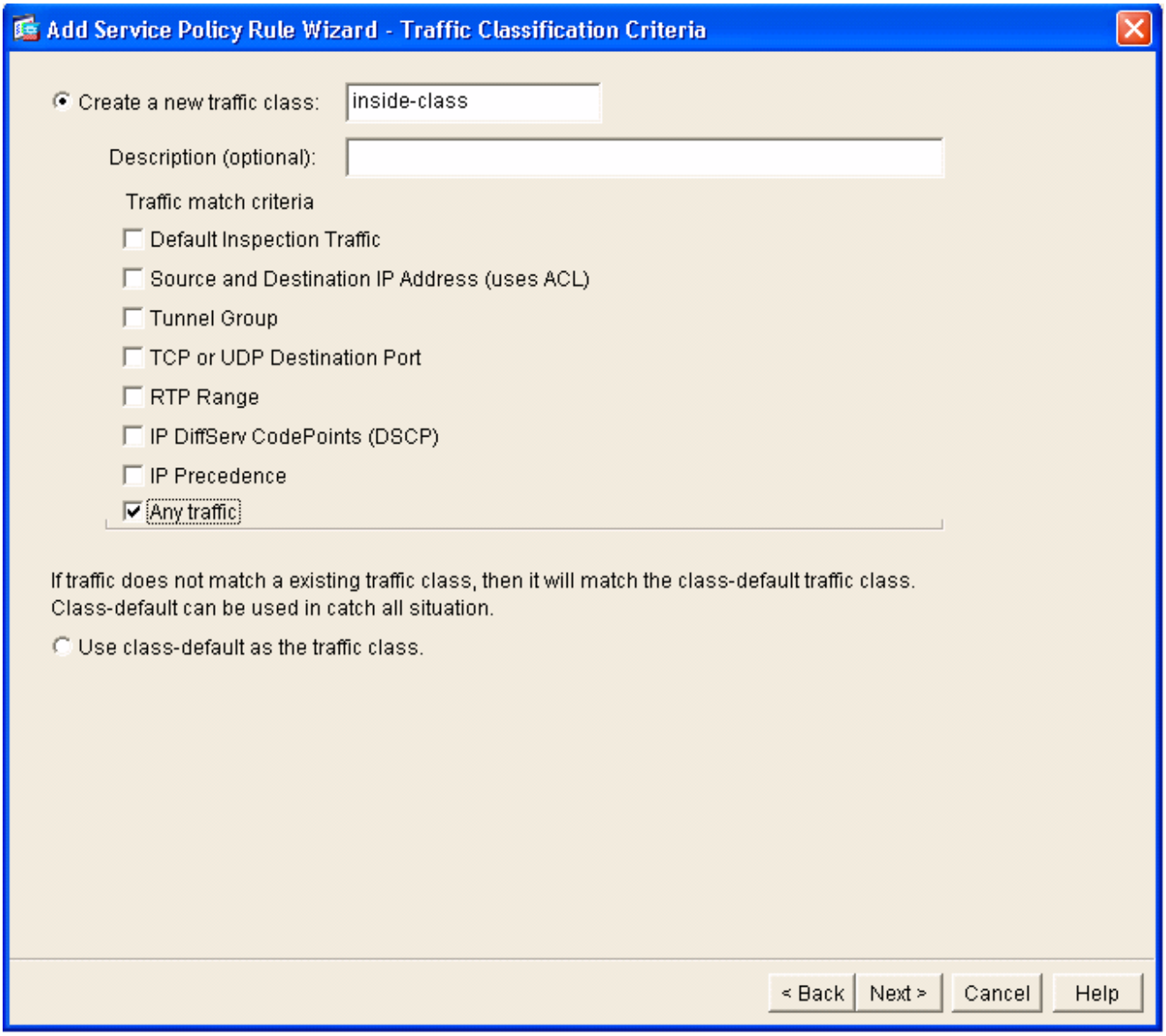
3. Haga clic la **política de seguridad** en el lado izquierdo de la ventana. En la ventana resultante, elija la lengueta de las **reglas de la política de servicio**.



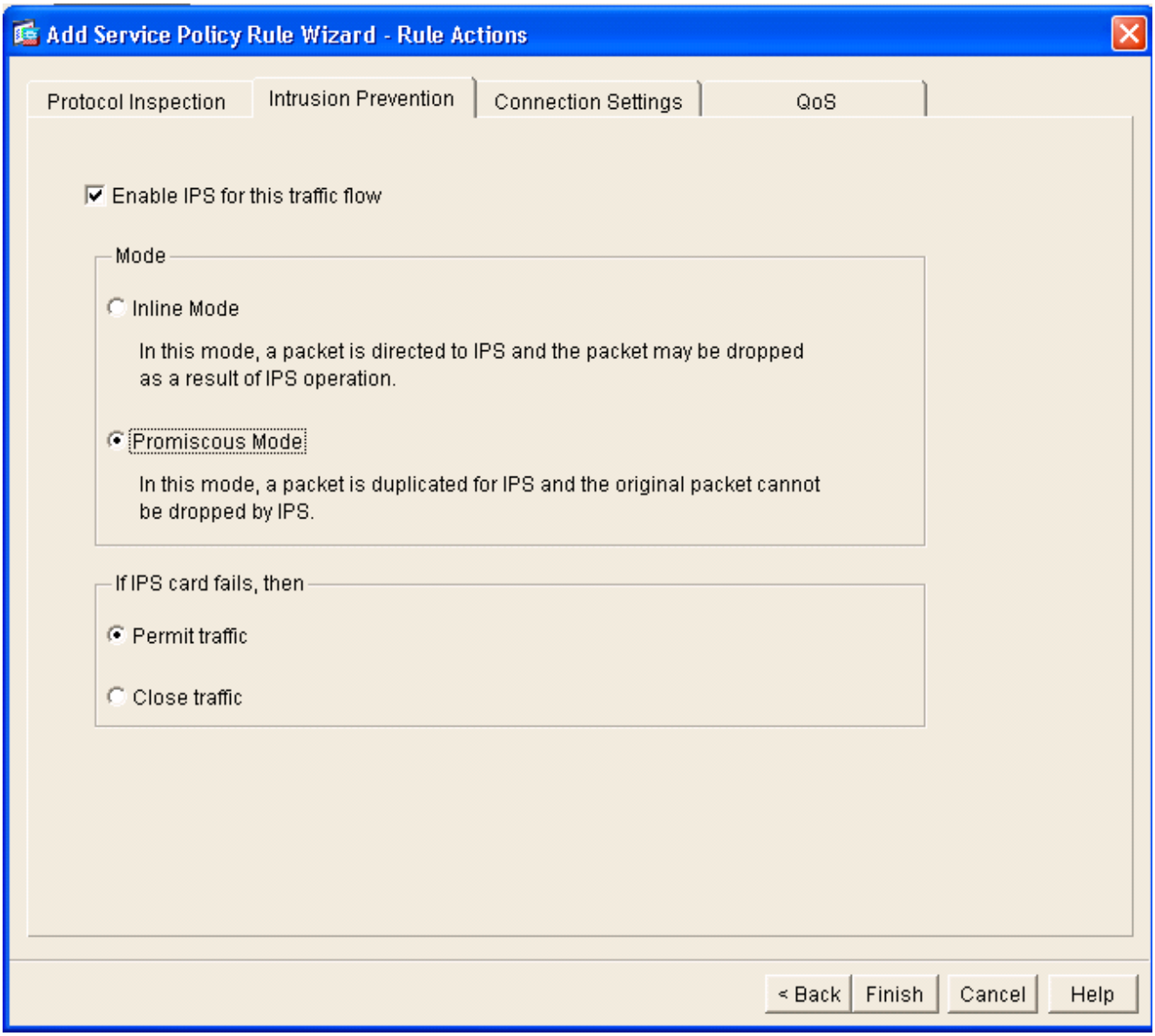
4. El tecleo **agrega** para crear una nueva directiva. Los lanzamientos del Asisitente de la regla de la política de servicio del agregar en una nueva ventana.Haga clic la **interfaz** y después elija la interfaz correcta de la lista desplegable para crear una nueva directiva que esté limitada a una de las interfaces que pase el tráfico.Dé a directiva un nombre y una descripción de lo que hace la directiva usando los dos cuadros de texto.Haga clic **después** para moverse al siguiente
paso.



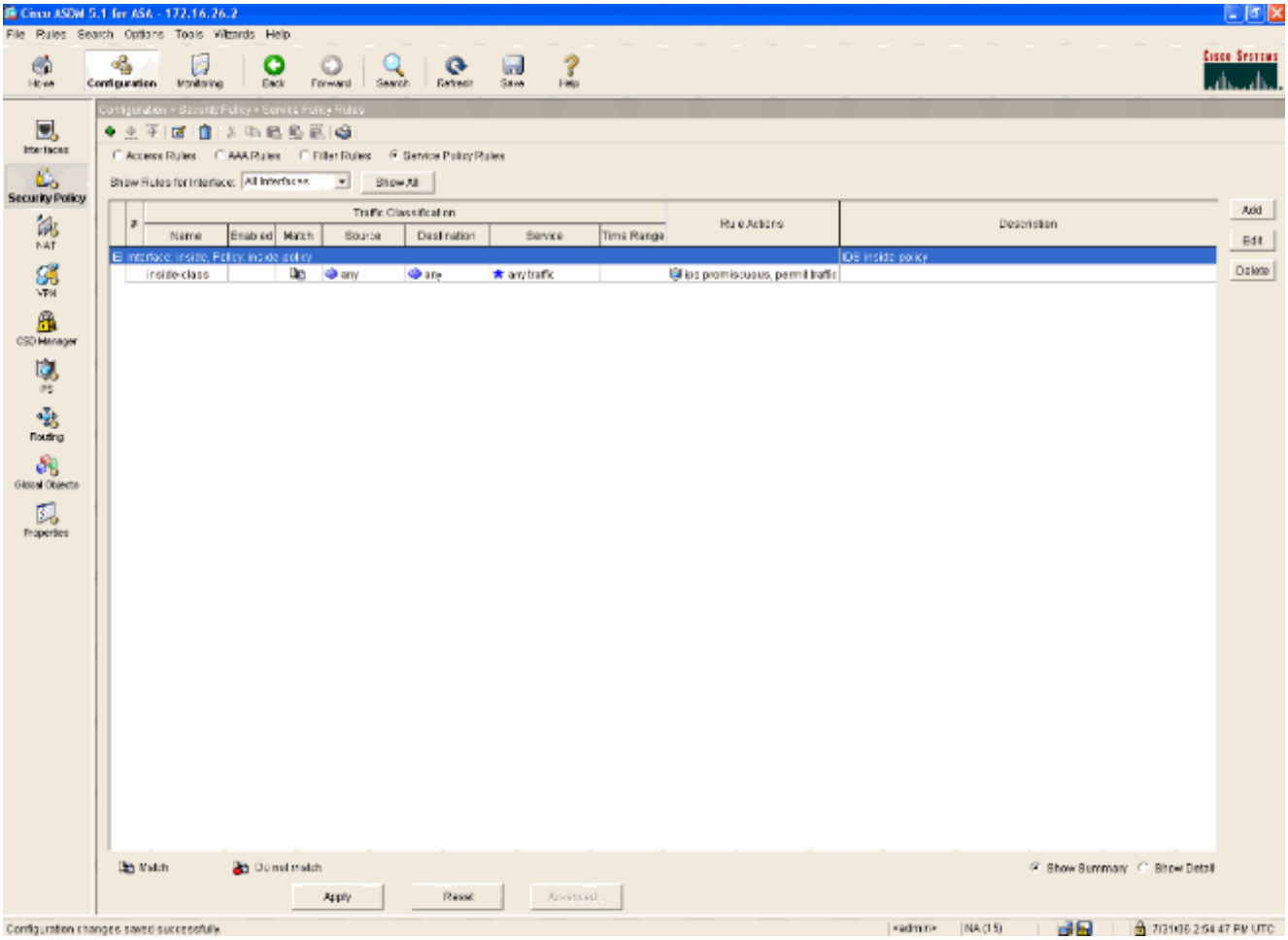
5. Construya una nueva clase de tráfico para aplicarse a la directiva.Es razonable construir las clases específicas para examinar los tipos de datos específicos, pero en este ejemplo, cualquier tráfico se selecciona para la simplicidad. Tecleo **después** para proceder.



6. Complete estos pasos paradé instrucciones el ASA para dirigir el tráfico encima a su AIP-SSM.Marque el **permiso IPS para este flujo de tráfico** para habilitar la detección de intrusos.Fije el modo a **promiscuo** para enviar una copia del tráfico al módulo fuera de banda en vez de colocar el módulo en línea con el flujo de datos.Haga clic el **tráfico del permiso** para asegurarse de que el Switches ASA a un estado fracaso-abierto en caso que el AIP-SSM falle.Clic en Finalizar para confiar el
cambio.



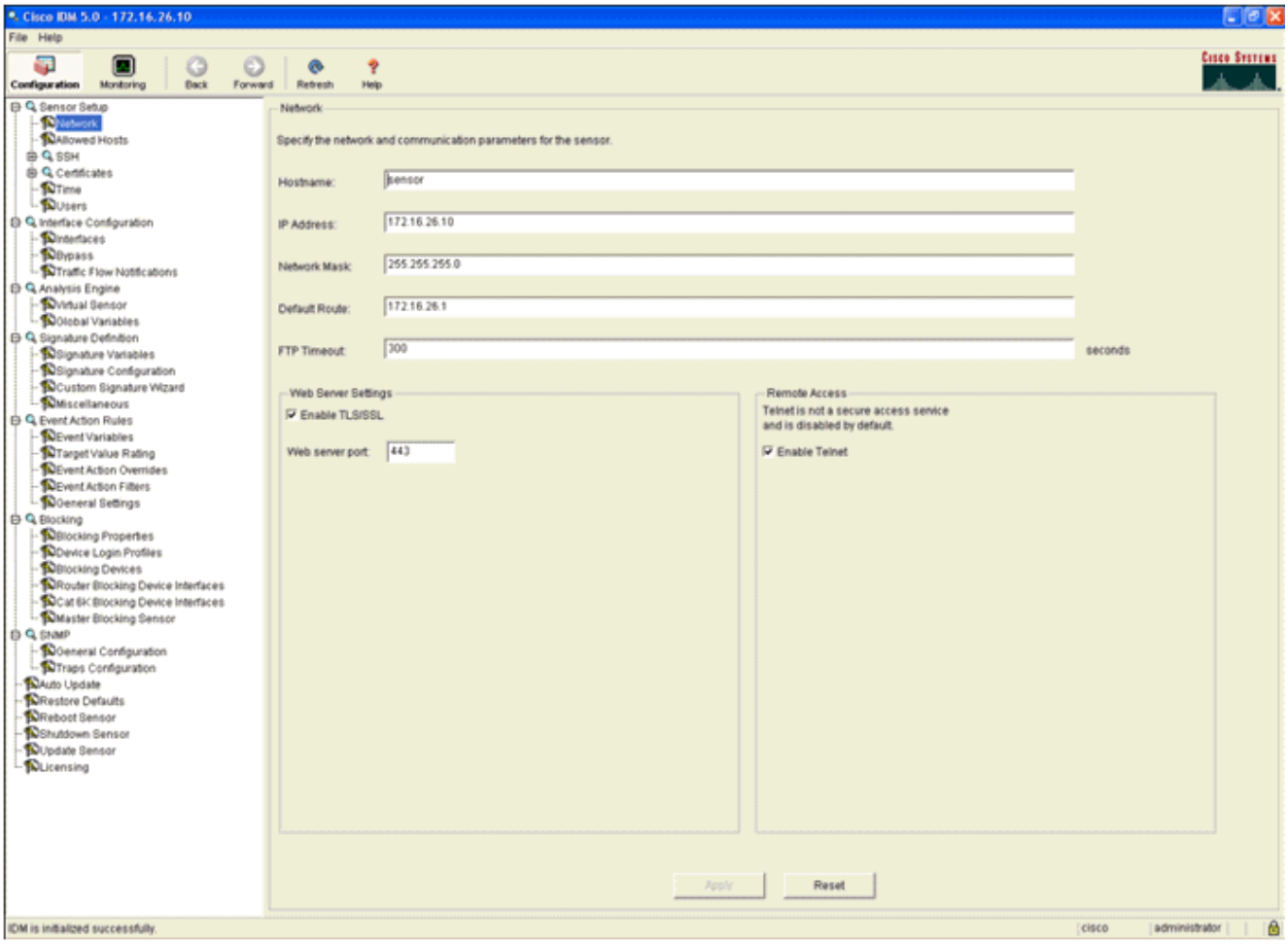
7. El ASA ahora se configura para enviar el tráfico al módulo ips. **Salvaguardia del** tecleo en la fila superior para escribir los cambios al
ASA.



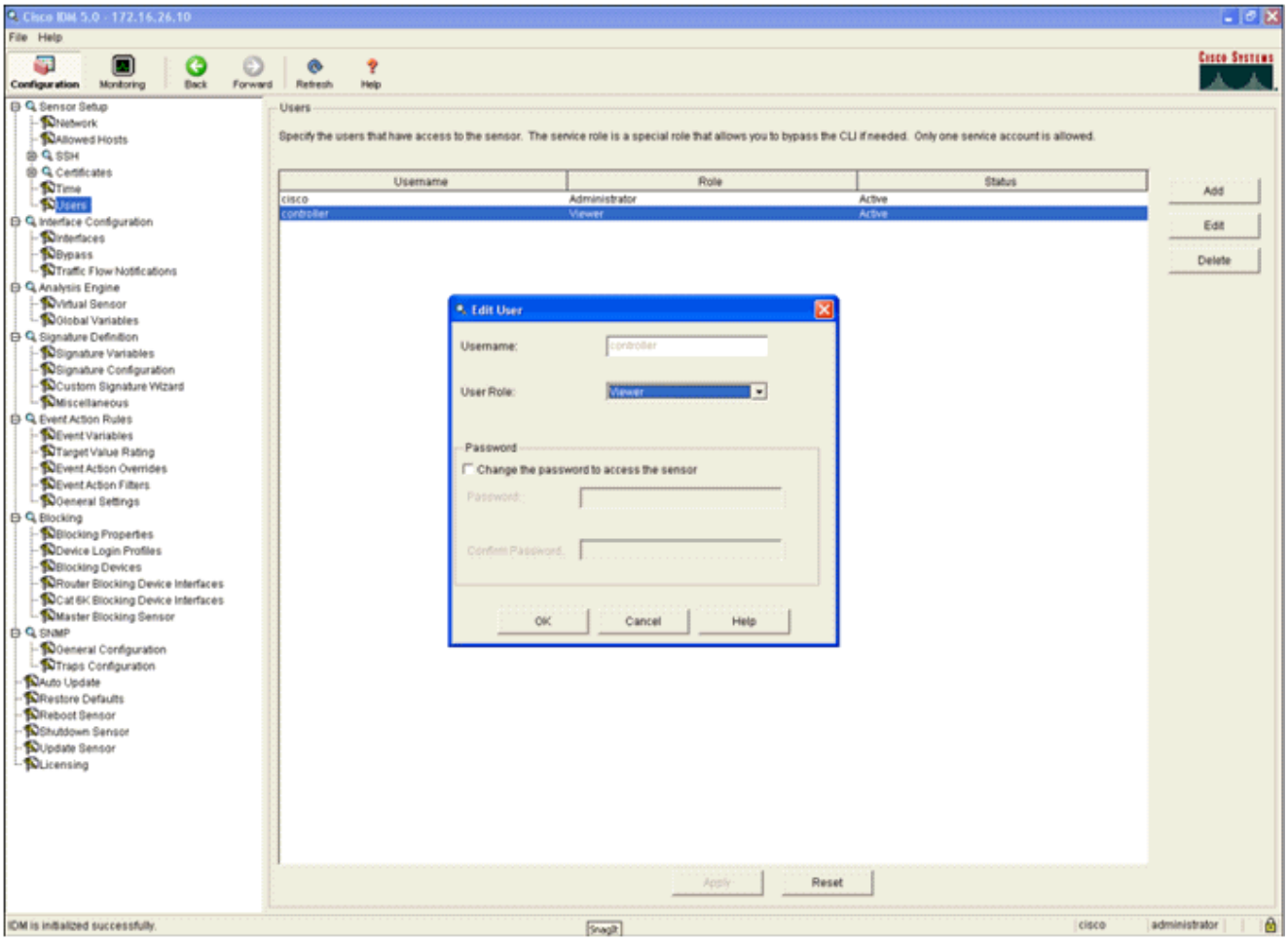
Configure el AIP-SSM para el examen del tráfico

Mientras que el ASA envía los datos al módulo ips, asocie la interfaz AIP-SSM a su motor virtual del sensor.

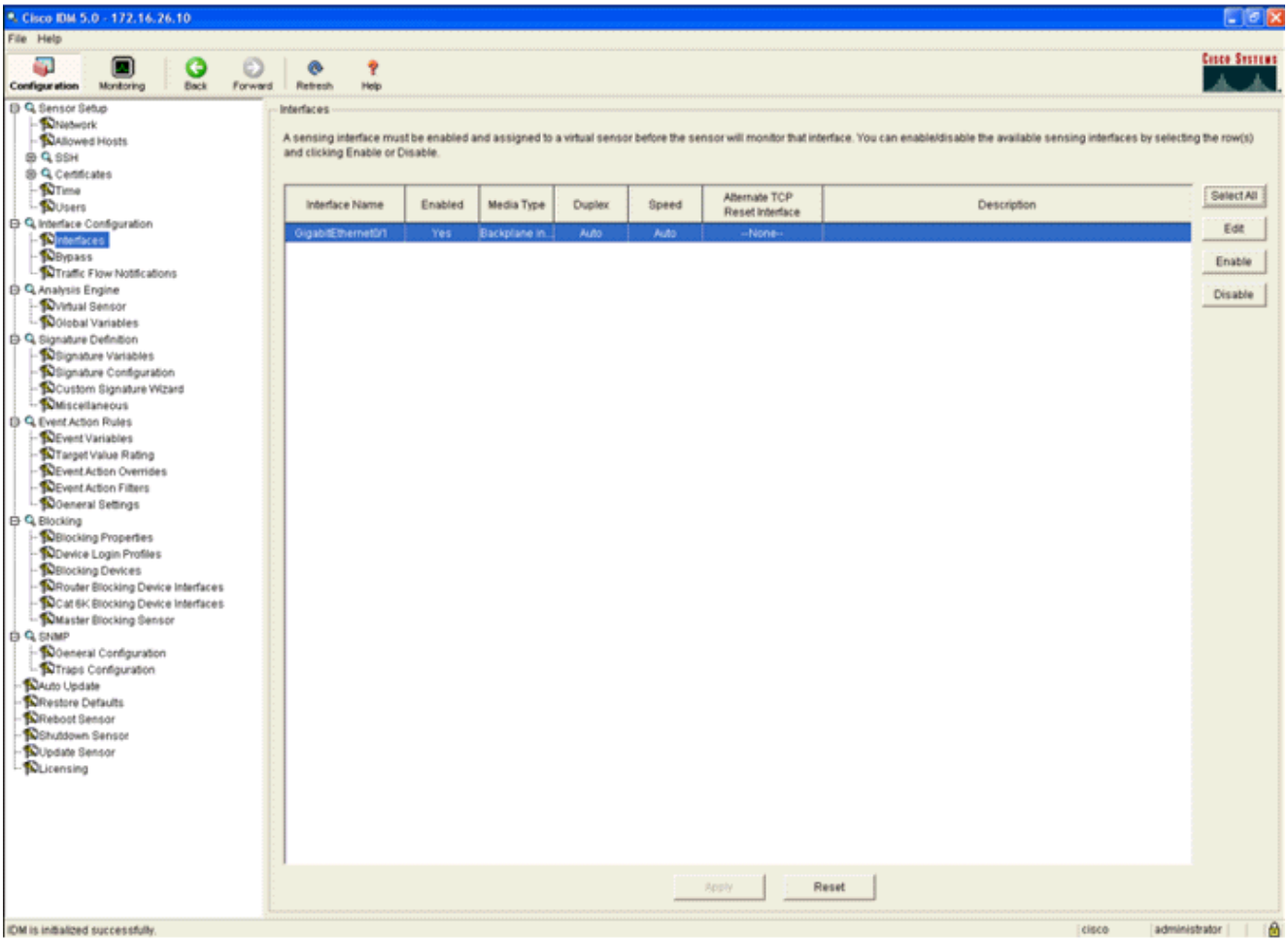
1. Inicie sesión al AIP-SSM usando el IDM.



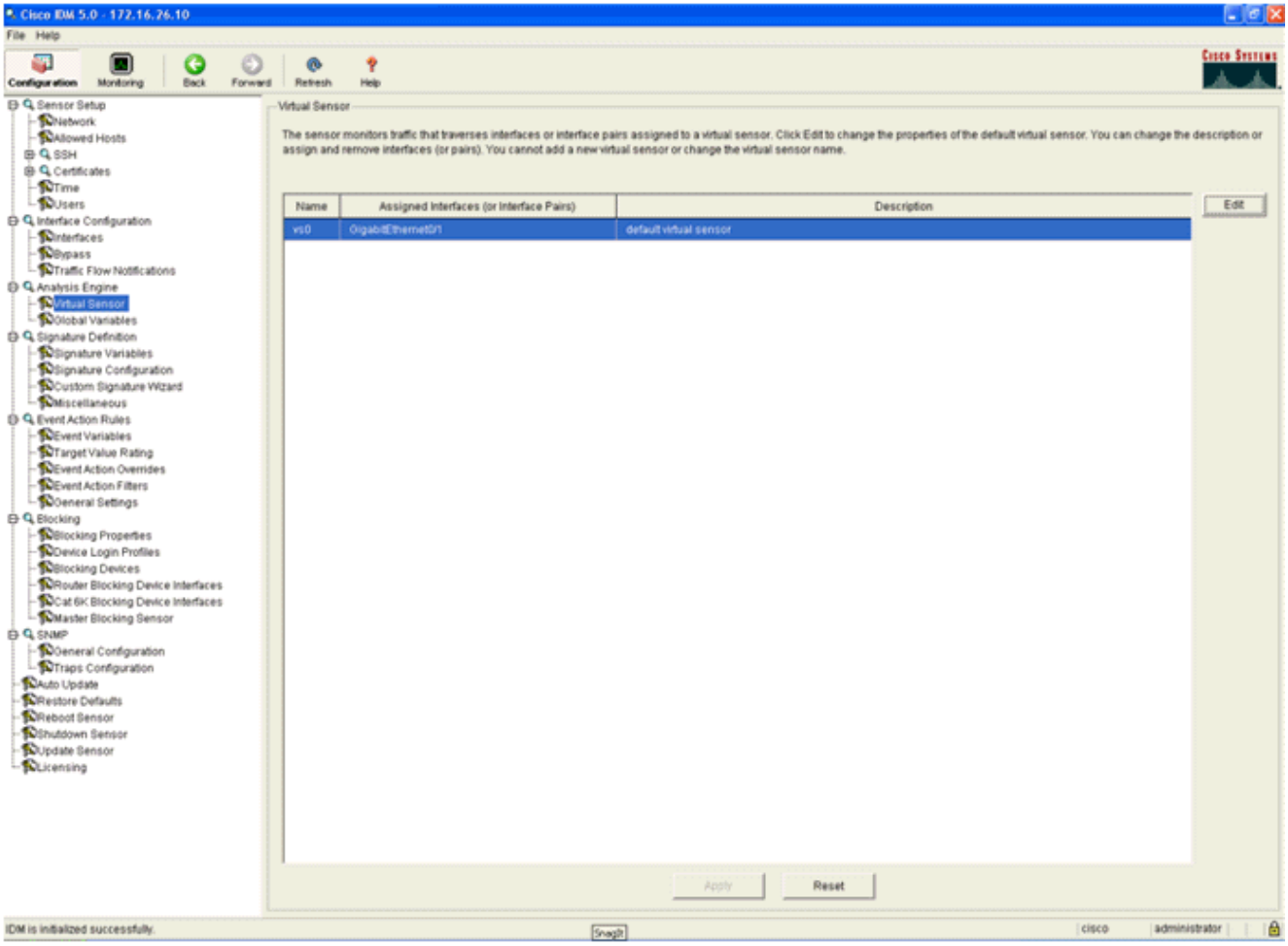
2. Agregue a un usuario con por lo menos los privilegios del Visualizador.



3. Habilite la interfaz.



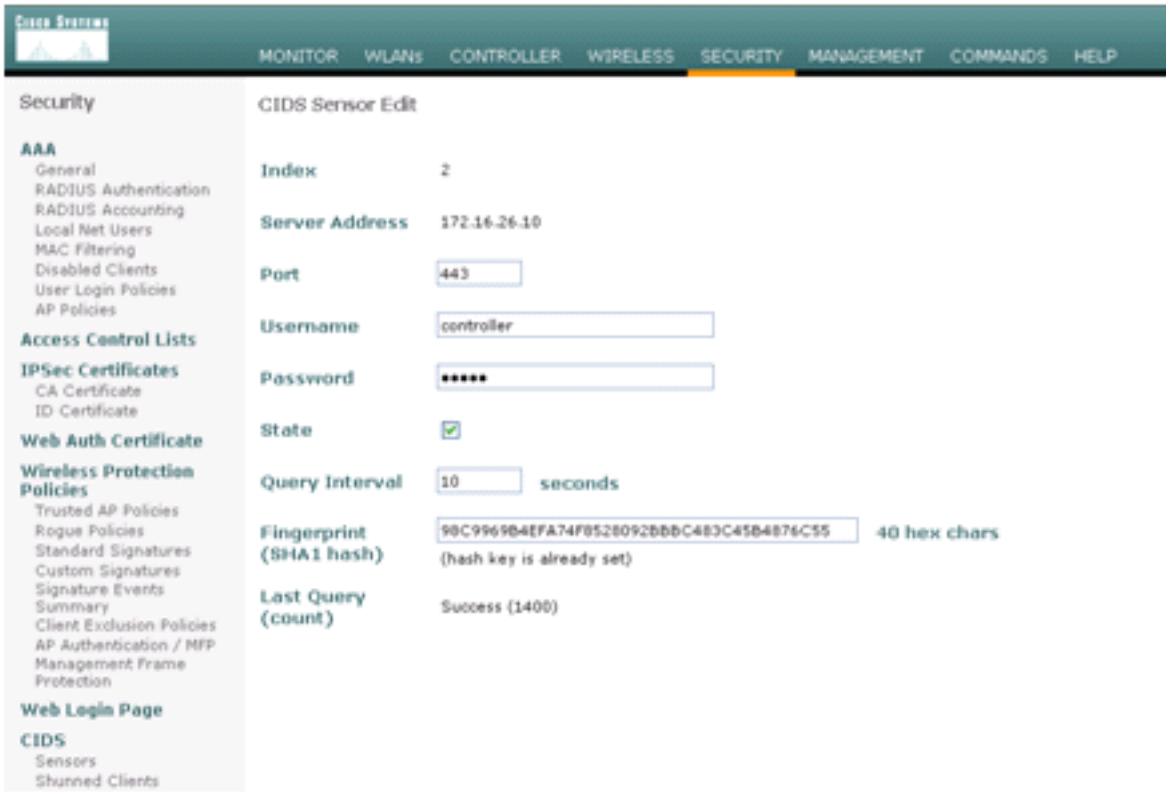
4. Marque Virtual Sensor Configuration (Configuración de sensor virtual).



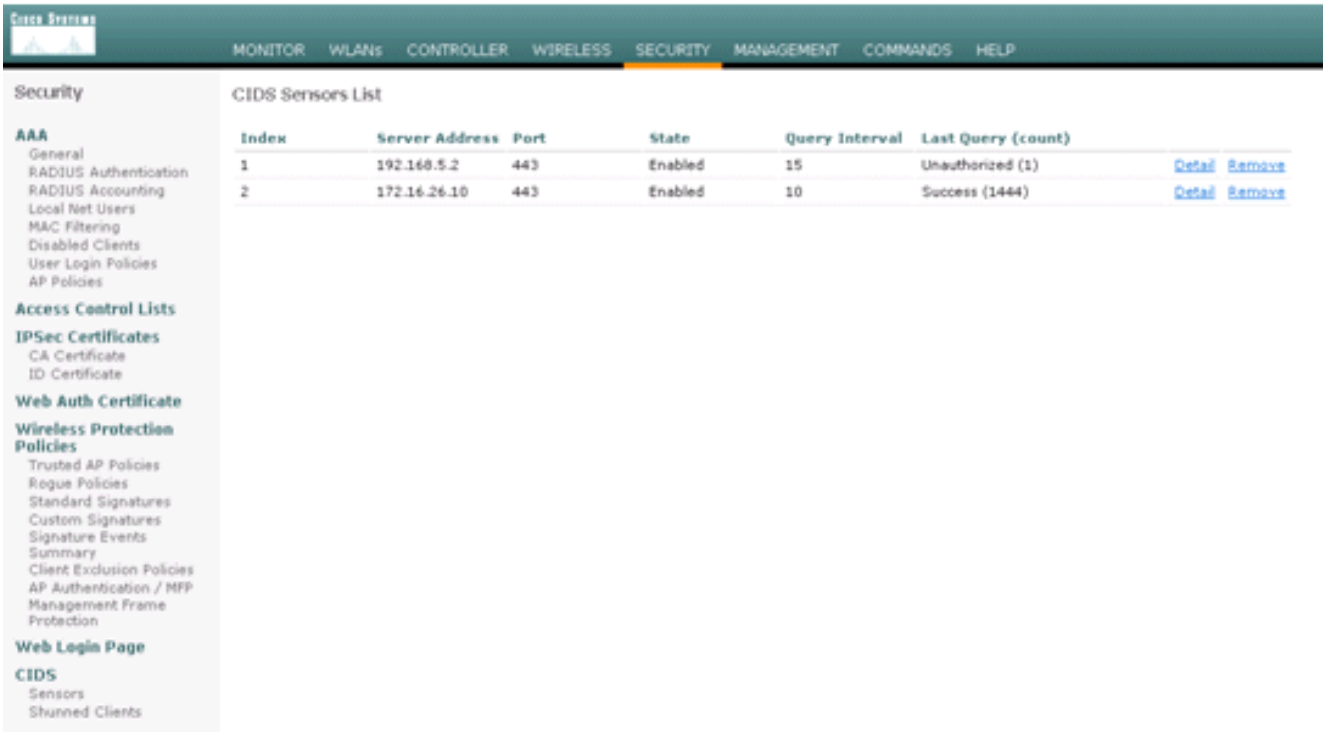
Configure un WLC para sondear el AIP-SSM para los bloques del cliente

Complete estos pasos una vez que se configura el sensor y alístelos para ser agregados en el regulador:

1. Elija la **Seguridad > los CID > los sensores > nuevo** en el WLC.
2. Agregue la dirección IP, número del puerto TCP, nombre de usuario y contraseña que usted creó en la sección anterior.
3. Para obtener la huella dactilar del sensor, ejecute este comando en el sensor y agregue la huella dactilar SHA1 en el WLC (sin los dos puntos). Esto se utiliza para asegurar la comunicación de la interrogación regulador-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`



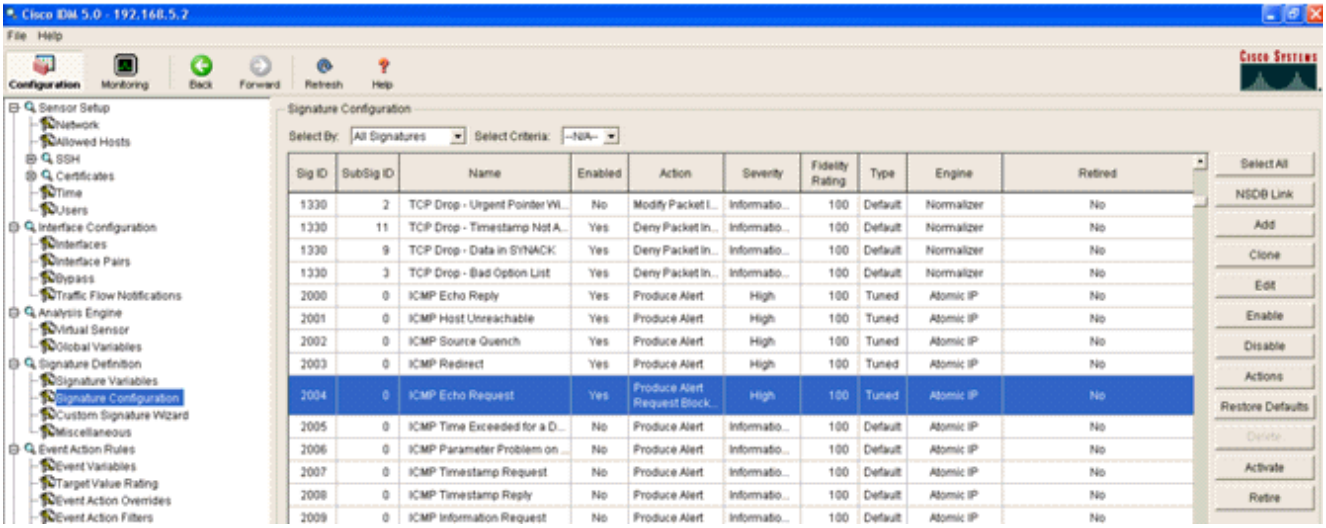
4. Marque el estatus de la conexión entre el AIP-SSM y el WLC.



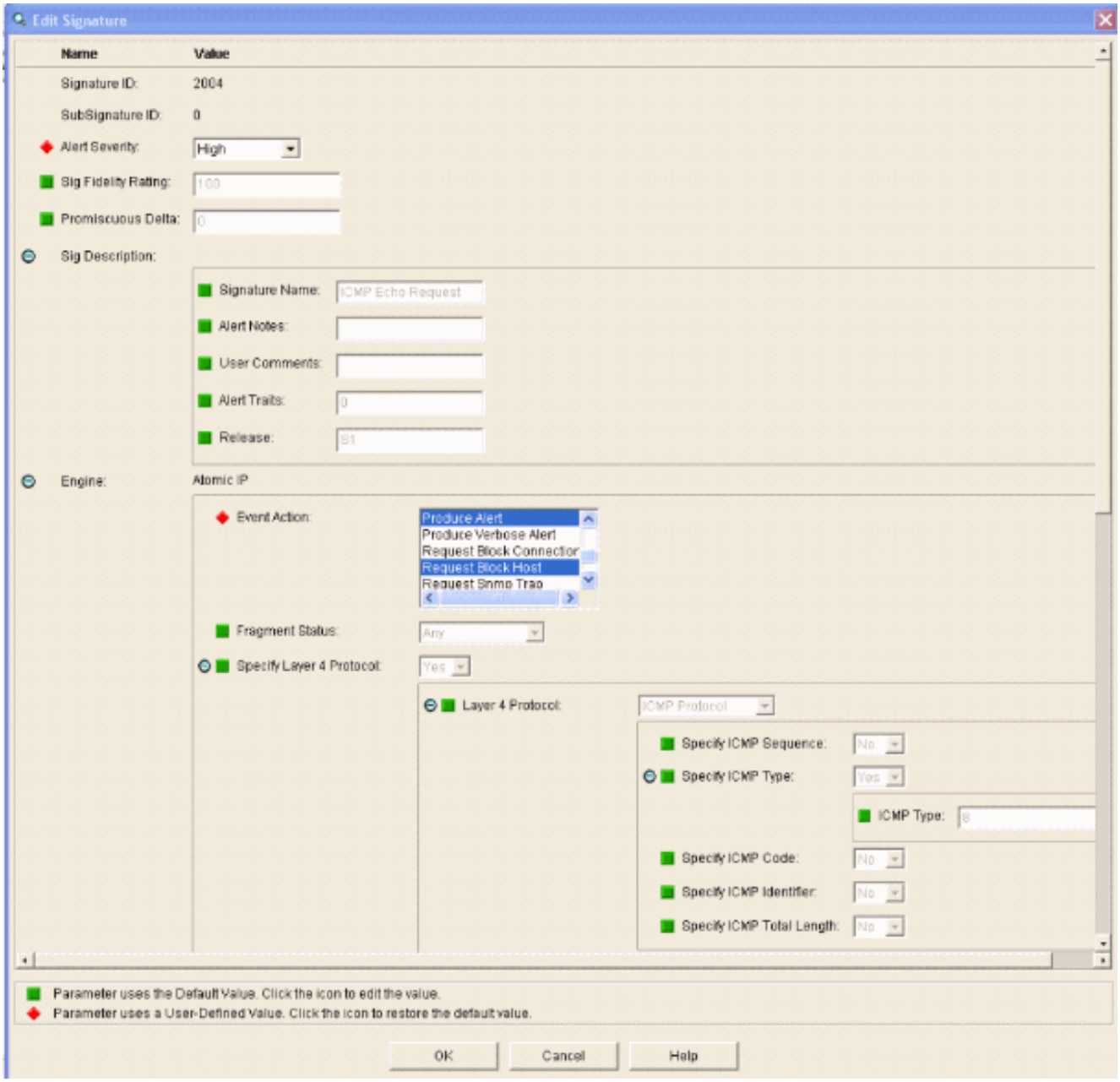
Agregue una firma de bloqueo al AIP-SSM

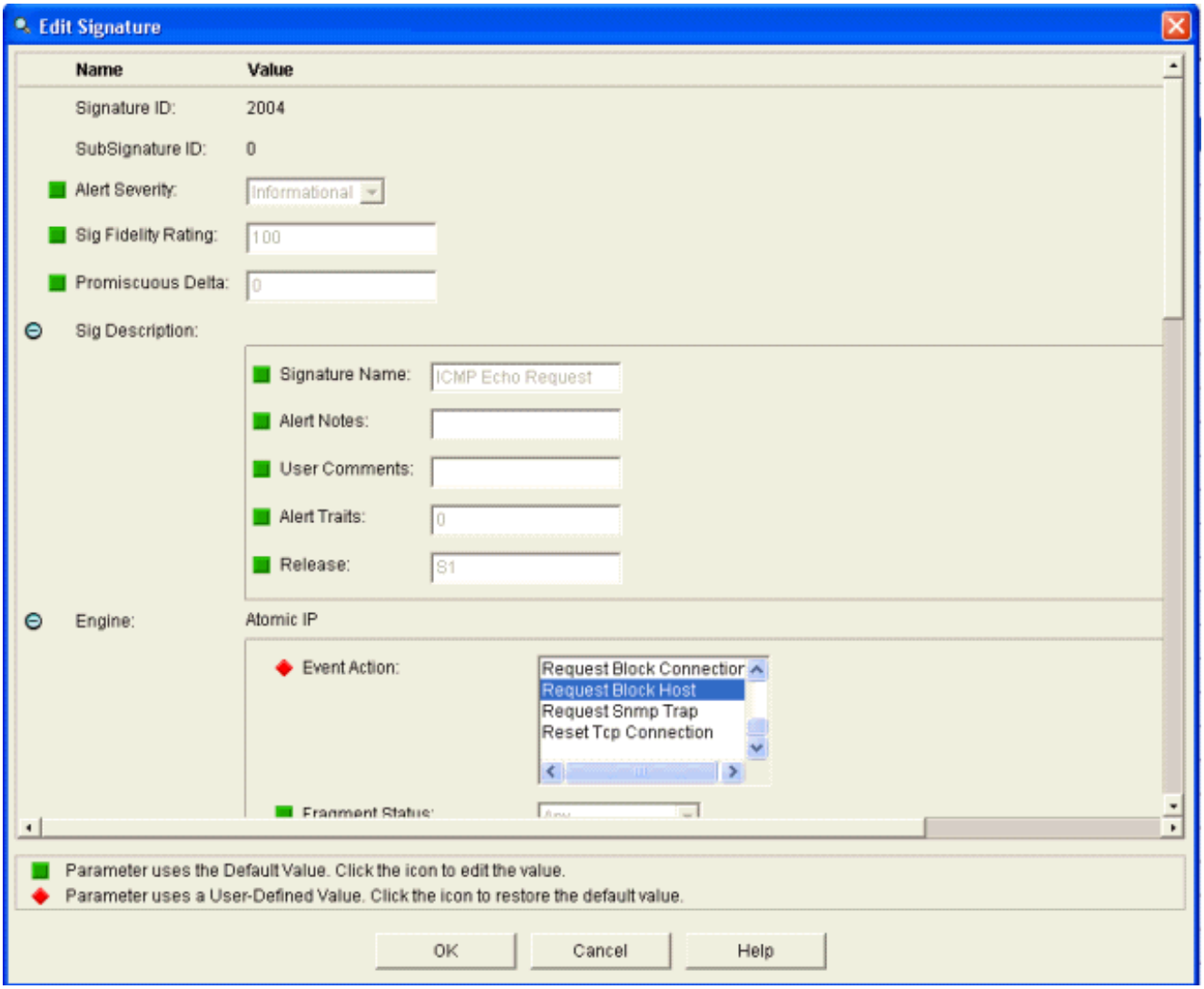
Agregue una firma del examen para bloquear el tráfico. Aunque haya muchas firmas que pueden hacer el trabajo basado en las herramientas disponibles, este ejemplo crea una firma que bloquee los paquetes ping.

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



2. Habilite la firma, fije la gravedad alerta al **alto** y fije la acción del evento **para producir la alerta** y el **host del bloque de petición** para completar este paso de verificación. Observe que la acción del host del bloque de petición es la clave a señalar el WLC para crear las excepciones del
cliente.



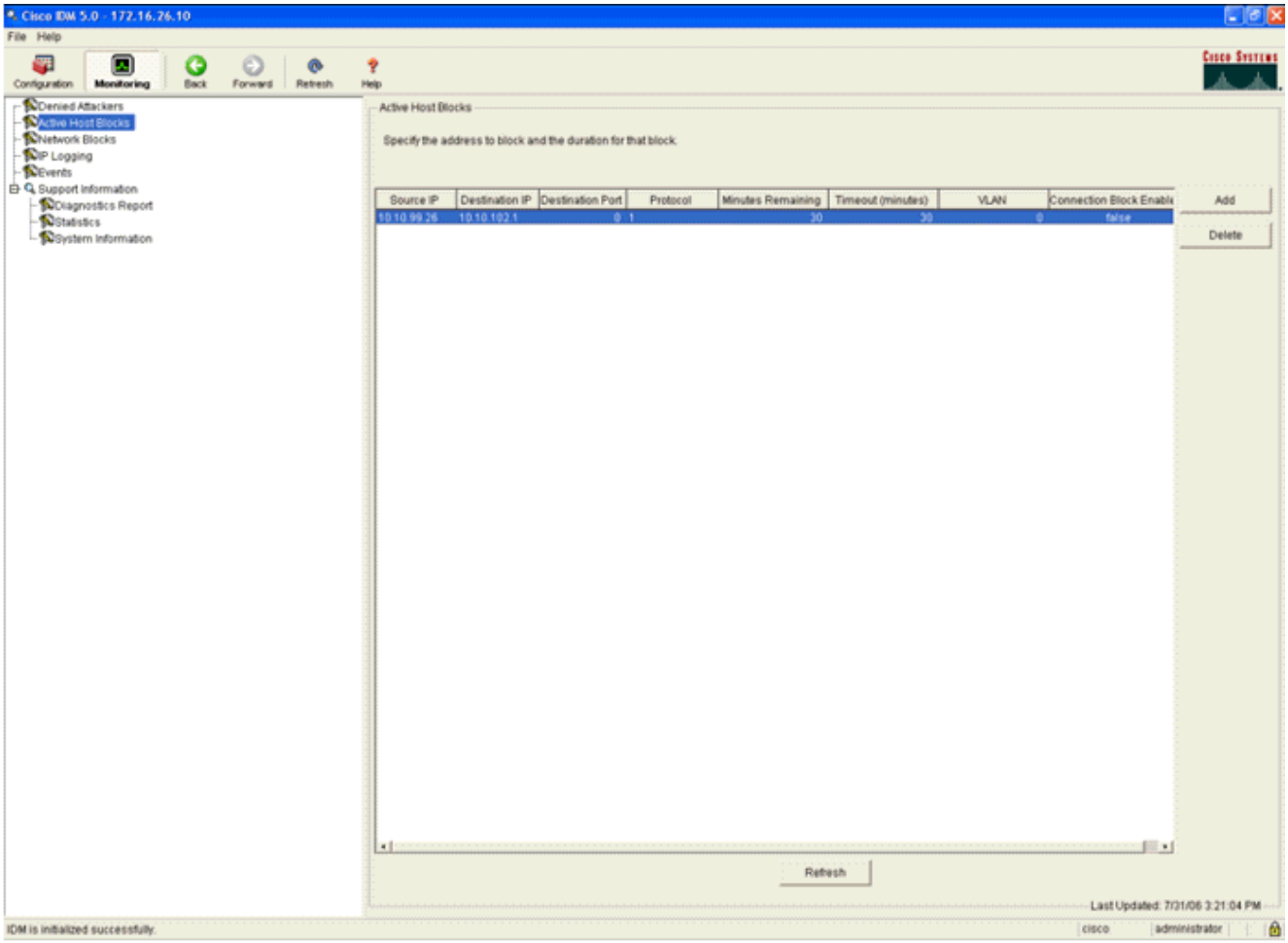


3. Haga Click en OK para salvar la firma.
4. Verifique que la firma sea activa y que está fijada para realizar una acción de bloqueo.
5. El tecleo **se aplica** para confiar la firma al módulo.

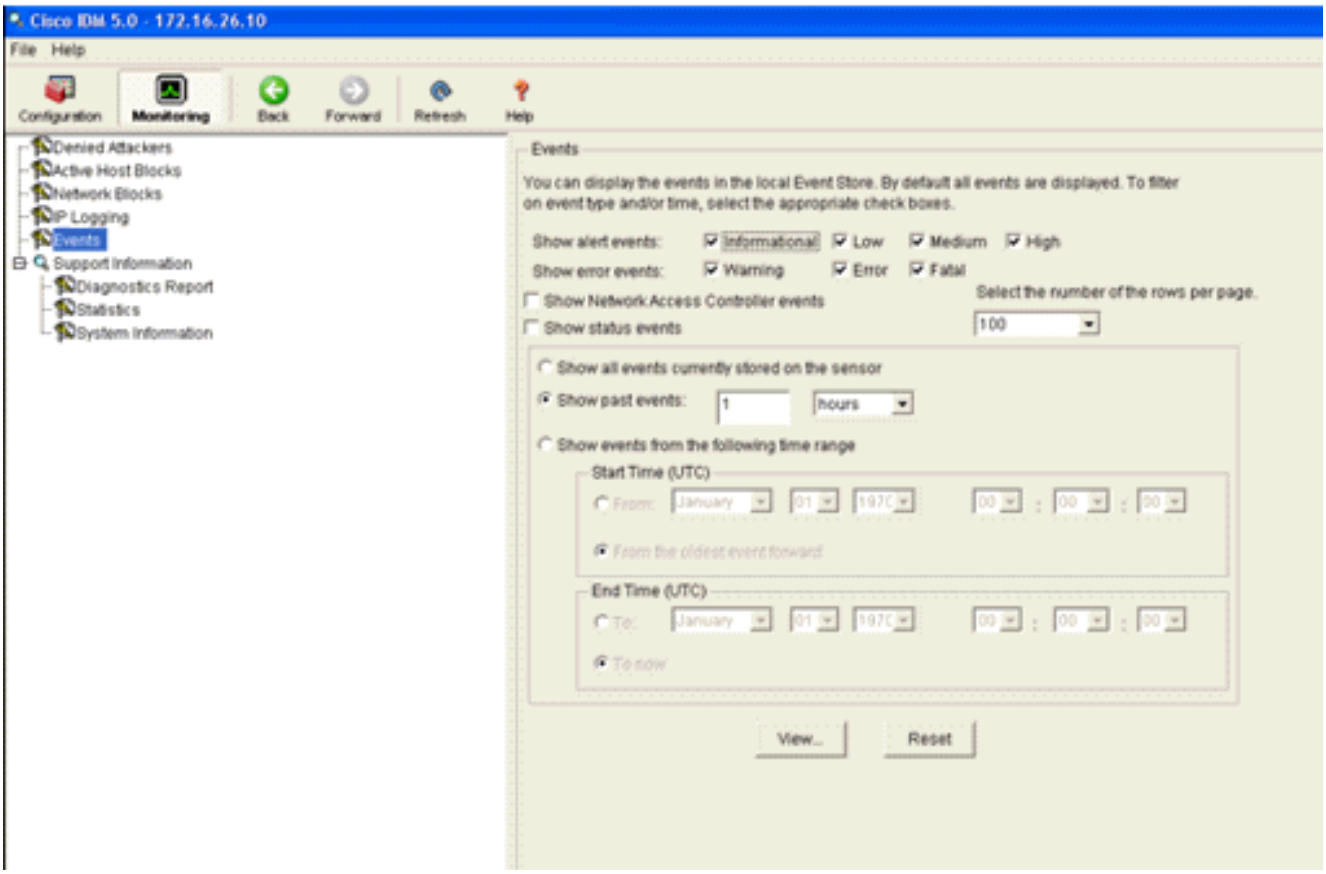
Bloqueo y eventos del monitor con el IDM

Complete estos pasos:

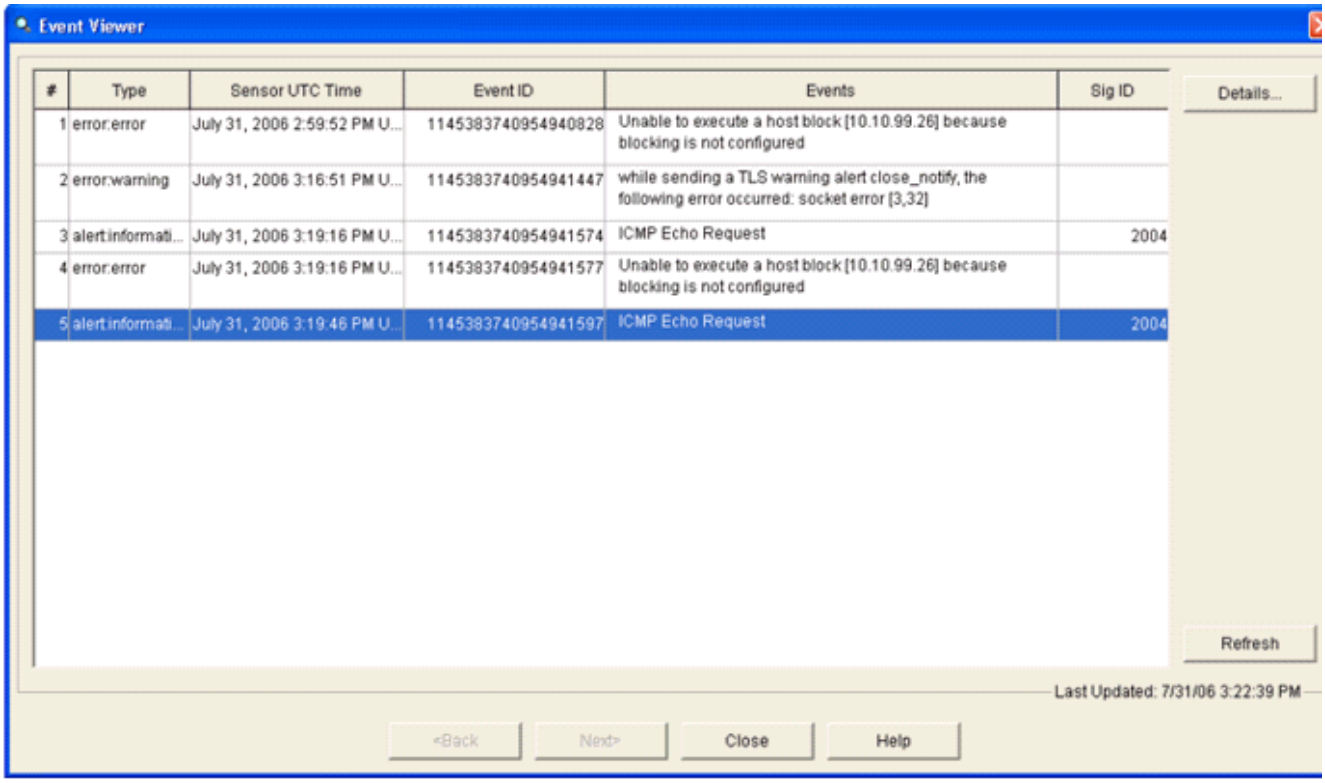
1. Cuando los fuegos de la firma con éxito, allí son dos lugares dentro del IDM para observar esto.El primer método muestra a bloques activos que el AIP-SSM ha instalado. Haga clic la **supervisión** a lo largo de la fila superior de las acciones. Dentro de la lista de elementos que aparece en el lado izquierdo, el **host activo** selecto **bloquea**. Siempre que los activadores de la firma del ping, el host activo bloqueen la ventana muestra la dirección IP del delincuente, el direccionamiento del dispositivo bajo ataque, y el tiempo que sigue habiendo para cuál es el bloque en efecto. El tiempo de bloqueo predeterminado es 30 minutos y es armonioso. Sin embargo, cambiando este valor no se discute en este documento. Consulte la documentación de la configuración ASA cuanto sea necesario para la información sobre cómo cambiar este parámetro. Quite el bloque inmediatamente, selecciónelo de la lista y después haga clic la
cancelación.



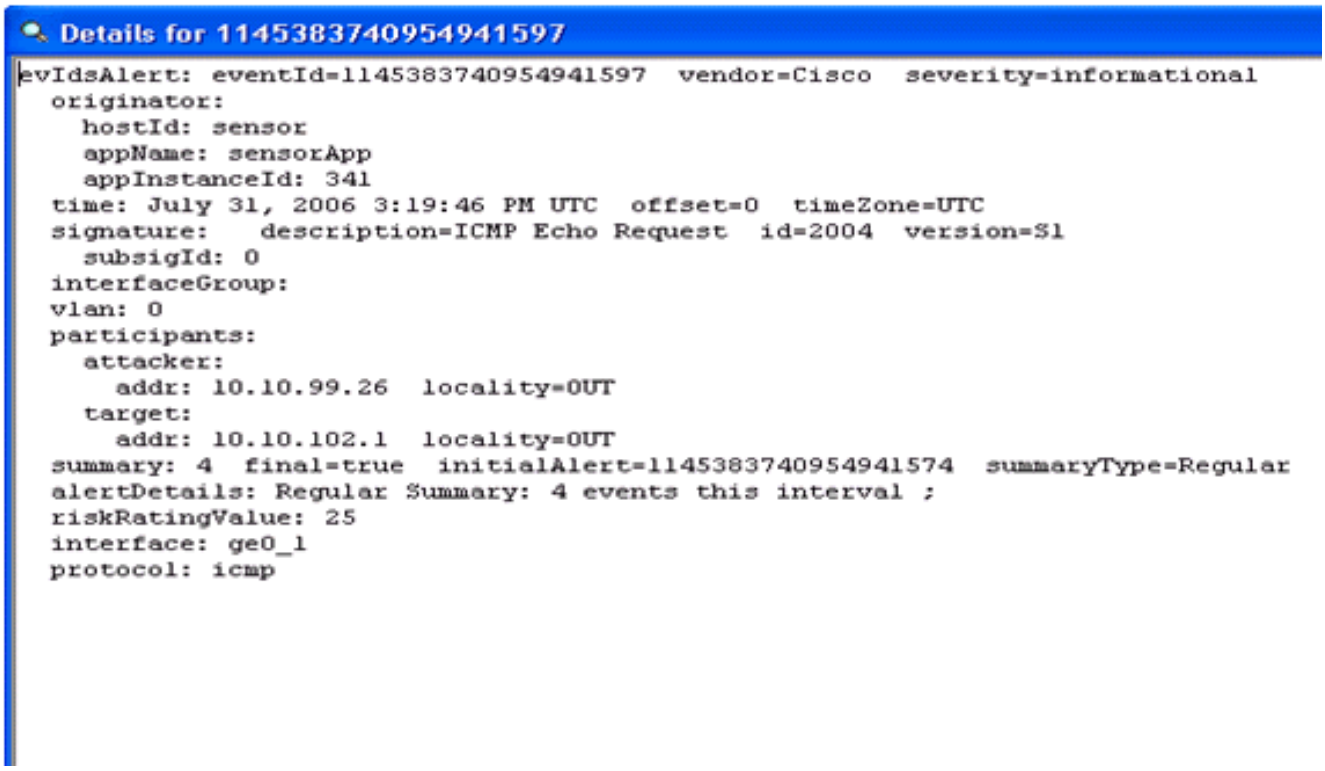
El segundo método para ver las firmas accionadas utiliza el buffer del evento AIP-SSM. De la página de la supervisión IDM, seleccione los **eventos** en la lista de los elementos en el lado izquierdo. La utilidad de la búsqueda de los eventos aparece. Fije los criterios de búsqueda y la **opinión** apropiados del tecleo....



2. El visor de eventos entonces aparece con una lista de eventos que hagan juego los criterios dados. Navegue a través de la lista y encuentre la firma del pedido de eco ICMP modificada en los pasos de la configuración previa.Mire en la columna de los eventos para el nombre de la firma, o bien busque para el número de identificación de la firma bajo la columna de los Sig
ID.

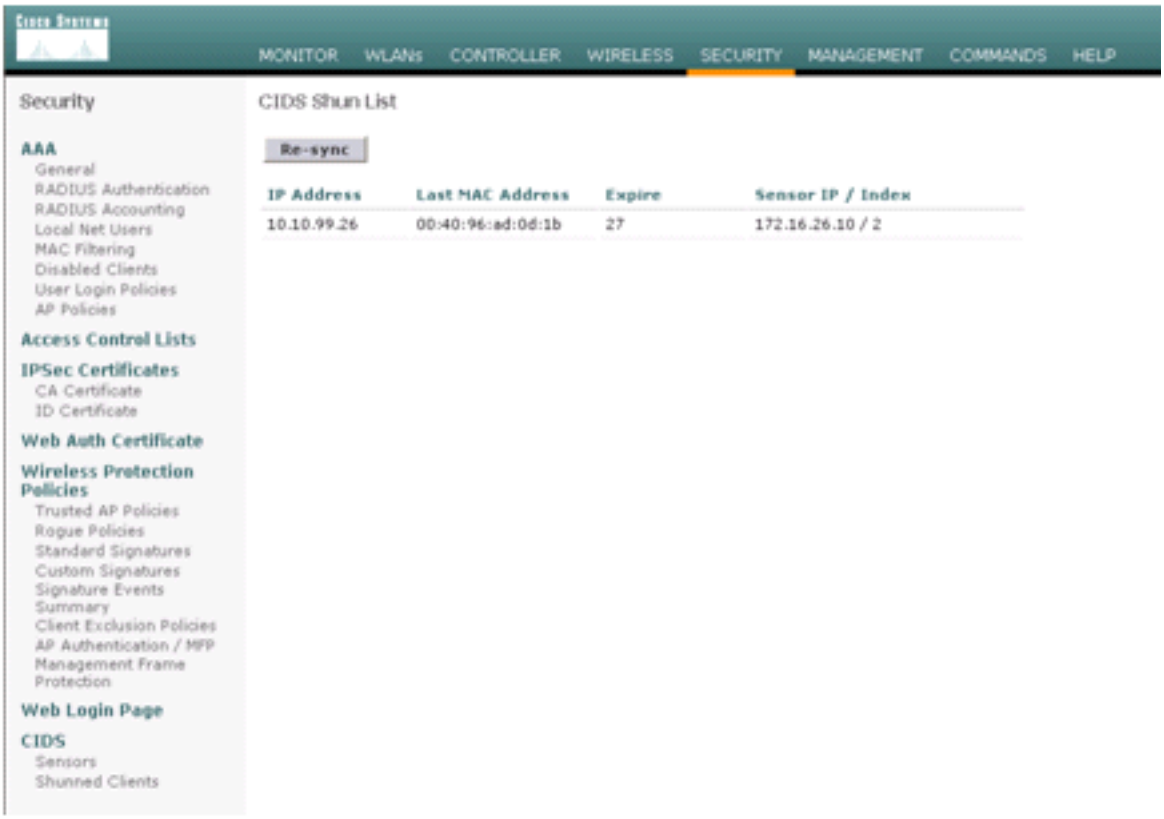


3. Después de que usted localice la firma, haga doble clic la entrada para abrir una nueva ventana. La nueva ventana contiene la información detallada en el evento que accionó la firma.

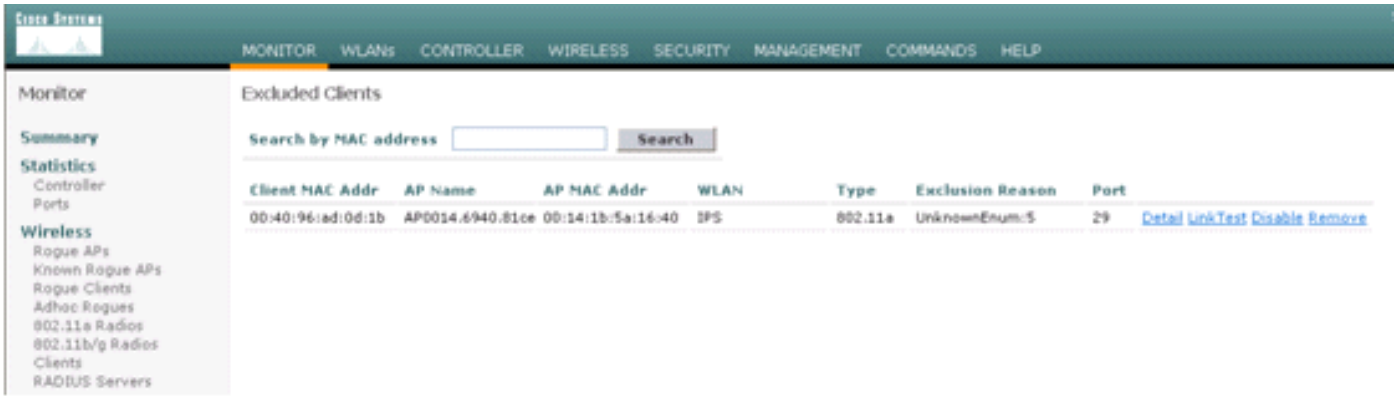


Exclusión del cliente del monitor en un regulador inalámbrico

Los clientes evitados enumeran en el regulador se pueblan en este momento del tiempo con el IP y la dirección MAC del host.



Agregan al usuario a la lista de la exclusión del cliente.

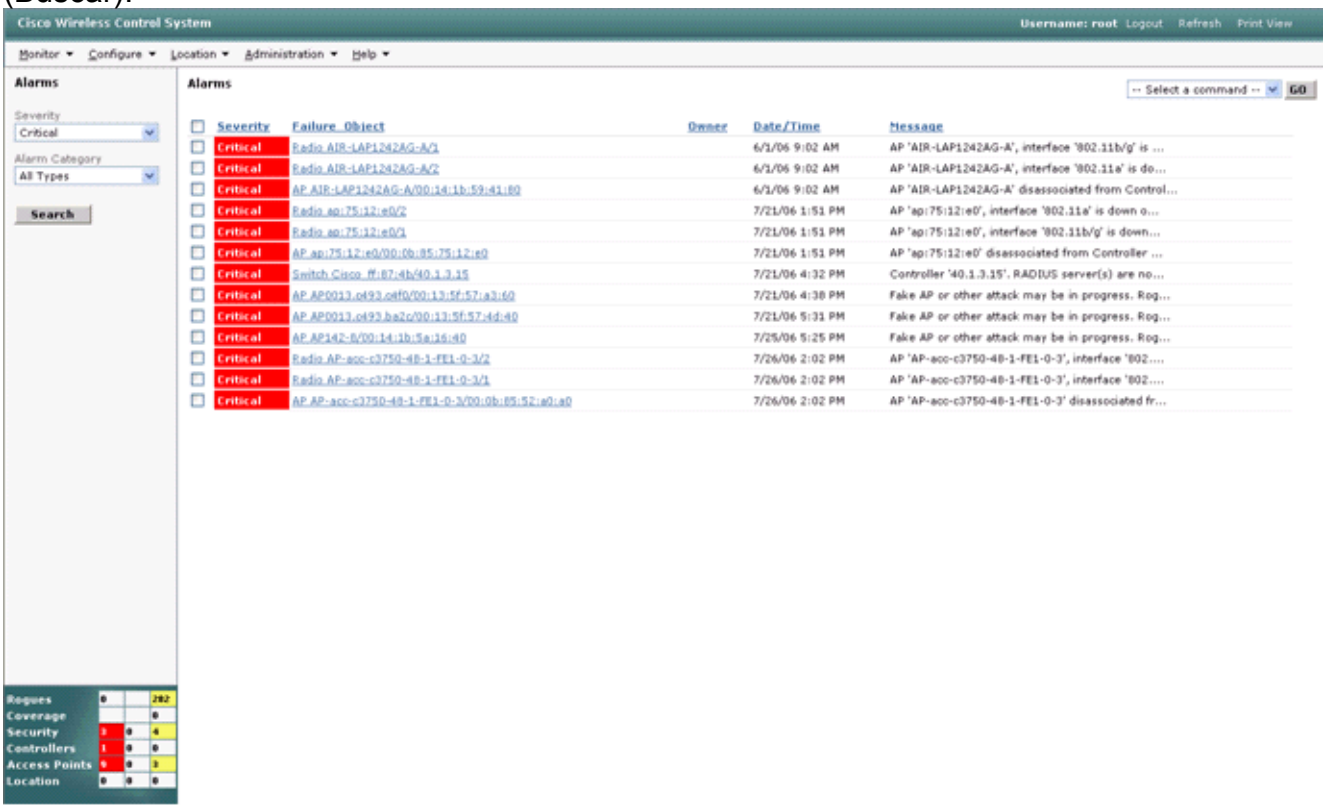


Eventos del monitor en el WCS

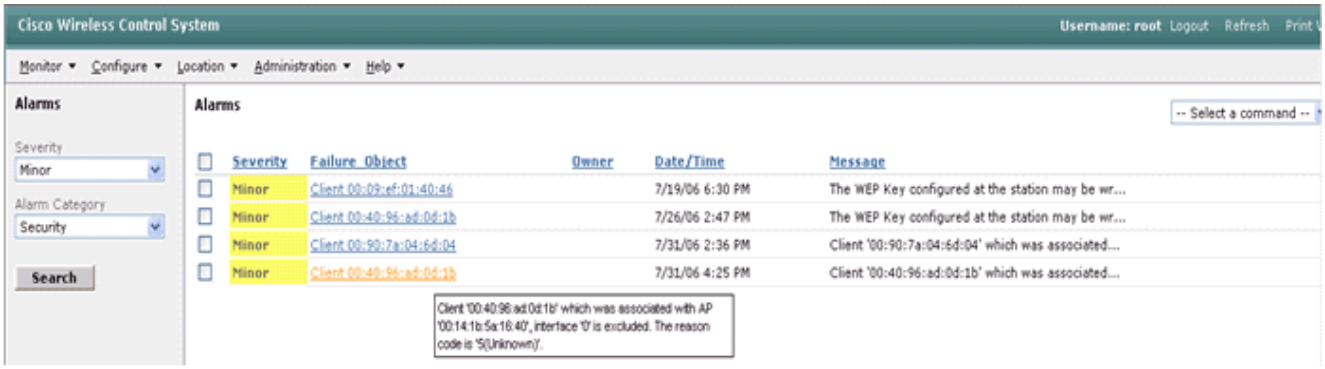
Eventos de seguridad que accionan un bloque dentro de la causa AIP-SSM el regulador para agregar el direccionamiento del delincuente a la lista de la exclusión del cliente. Un evento también se genera dentro del WCS.

1. Utilice el **monitor > las alarmas** utilitarios del menú principal WCS para ver el evento de la exclusión. El WCS visualiza inicialmente todas las alarmas sin declarar y también presenta una función de búsqueda en el lado izquierdo de la ventana.
2. Modifique los criterios de búsqueda para encontrar el bloque del cliente. Bajo gravedad, elija al **menor**, y también fije la categoría de la alarma a la **Seguridad**.
3. Haga clic en Search

(Buscar).



4. La ventana de alarma entonces enumera solamente las alarmas de la Seguridad con la gravedad de menor importancia. Señale el ratón en el evento que accionó el bloque dentro del AIP-SSM.Particularmente, el WCS muestra la dirección MAC de la estación del cliente que causó la alarma. Señalando en la dirección apropiada, estallidos-para arriba WCS que una pequeña ventana con el evento detalla. Haga clic el link para ver estos mismos detalles en otra
ventana.



Configuración de muestra 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 muestra del sensor de Cisco Intrusion Prevention System

```
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.

Troubleshooting

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

Información Relacionada

- Instalando y con al administrador de dispositivo 5.1 del Cisco Intrusion Prevention System
- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 - Guías de configuración
- Configurando el sensor de Cisco Intrusion Prevention System usando la interfaz de línea de comando 5.0 - configurar las interfaces
- Guía de configuración 4.0 del WLC
- Soporte técnico inalámbrico
- Regulador del Wireless LAN (WLC) FAQ
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Soluciones de Configurar directivo de seguridad
- Soporte Técnico y Documentación - Cisco Systems