

Regulador inalámbrico LAN y guía de integración IPS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requisitos](#)

[Componentes usados](#)

[Convenciones](#)

[Descripción identificación de Cisco](#)

[Identificación y WLC de Cisco – Descripción de la integración](#)

[El evitar identificación](#)

[Diseño de la arquitectura de red](#)

[Configure el sensor IDS de Cisco](#)

[Configure el WLC](#)

[Configuración de muestra del sensor IDS de Cisco](#)

[Configure un ASA para la identificación](#)

[Configure el AIP-SSM para el examen del tráfico](#)

[Configure un WLC para sondear el AIP-SSM para los bloques del cliente](#)

[Agregue una firma de bloqueo al AIP-SSM](#)

[Vigile el bloqueo y los eventos con el IDM](#)

[Vigile la exclusión del cliente en un regulador inalámbrico](#)

[Vigile los eventos en el WCS](#)

[Configuración de muestra de Cisco ASA](#)

[Configuración de muestra del sensor de Cisco Intrusion Prevention System](#)

[Verifique](#)

[Troubleshooting](#)

[Información Relacionada](#)

[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 inalámbrica unificada Cisco, un dispositivo IDS atado con alambre Cisco detecta el ataque y lo envía evita las peticiones a los reguladores inalámbricos LAN de Cisco (WLCs), que entonces desasocian el dispositivo 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 a 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 a 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 la intrusión.
- **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 la capacidad de conversión a escala y la elasticidad con la Colaboración de la red, incluyendo las técnicas de la captura del tráfico, las capacidades del Equilibrio de carga, y la visibilidad eficientes en el tráfico encriptado.
- **Soluciones completas del despliegue** — Proporciona a 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 del evento, y los servicios del soporte potentes** — activa una solución completa, incluyendo la configuración, la Administración, la correlación de los datos, y los servicios del soporte avanzados. Particularmente el vigilar del Cisco Security, el análisis, y el sistema de la respuesta (MARTE) identifica, los aislantes, y recomienda el retiro de la precisión de los elementos que ofenden, para una solución ancha de la prevención de la intrusión de la red. Y el Cisco Incident Control System previene el nuevo gusano y los brotes de virus permitiendo a la red adaptar y proporcionar rápidamente a una respuesta distribuida.

Cuando están combinados, estos elementos proporcionan a 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 ligero actual del Punto de acceso (LWAPP) - los sistemas basados de la red inalámbrica (WLAN) utiliza solamente las características básicas identificación debido al hecho de que es esencialmente un sistema de la capa 2 y ha limitado el línea-proceso de la potencia. Nuevo código de las Versiones de Cisco a tiempo para incluir las nuevas características aumentadas en los nuevos códigos. La versión 4.0 tiene las últimas características que incluyen la integración de un sistema LWAPP-basado de la red inalámbrica (WLAN) 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.

[Prerequisites](#)

Requisitos

Asegúrese de que usted cumpla estos requerimientos mínimos:

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

Componentes usados

Cisco WLC

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

- Cisco 2000 Series WLC
- Cisco 2100 Series WLC
- WLC de las Cisco 4400 Series
- Módulo de Servicios inalámbricos de Cisco (WiSM)
- Las Cisco Catalyst 3750G Series unificaron el switch de acceso
- Módulo inalámbrico del regulador LAN de Cisco (WLCM)

Puntos de acceso

- Cisco Aironet 1100 Puntos de acceso ligeros de la serie AG
- Cisco Aironet 1200 Puntos de acceso ligeros de la serie 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 identificación de Cisco - Encargado de dispositivo IDS de Cisco (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 identificación de Cisco (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.

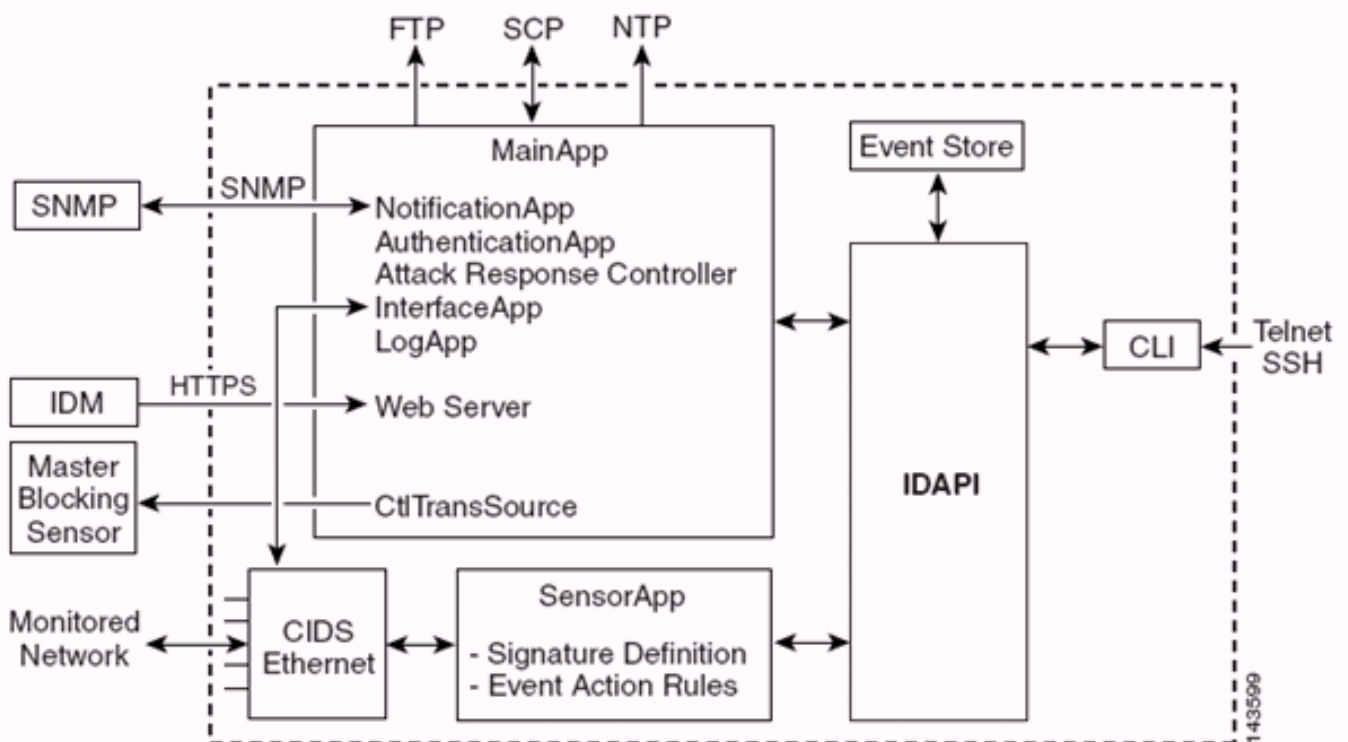
Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Descripción identificación de Cisco

Los componentes importantes de la identificación de Cisco (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 al 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 UI utilizan el módulo** — Proporciona a un CLI integrado y al IDM.
- **OS del sensor** — 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 mejoras. Contiene estos componentes:
 - Servidor de transacción del control** — Permite que los sensores envíen las transacciones del control que se utilizan para activar 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 del interfaz** — Las manijas desvían y las configuraciones físicas y definen los interfaces emparejados. Las configuraciones físicas consisten en la velocidad, el duplex, y los estados administrativos.
- **App del registro** — Escribe los mensajes de registro de la aplicación al archivo del registro y

de 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 a bloquear 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 GETs proporciona a la información sobre la salud de un sensor. **Servidor Web (servidor HTTP RDEP2)** — Proporciona a un interfaz del Web User. También proporciona a 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, ASDM, o RDEP.
- **App del sensor (motor del análisis)** — Realiza la captura de paquetes y el análisis.
- **CLI** — El interfaz se funciona con que cuando los usuarios se abren una 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 utilizó a la re-imagen la partición de aplicación del IDSM-2. Una re-imagen de la división del mantenimiento da lugar a las configuraciones perdidas.
- **División de la recuperación** — Una imagen del propósito especial usada para la recuperación del sensor. El arrancar en la división de la recuperación activa a los usuarios totalmente a la re-imagen la partición de aplicación. Se preservan las configuraciones de red, pero se pierden el resto de las configuraciones.

[Identificación y WLC de Cisco – Descripción de la integración](#)

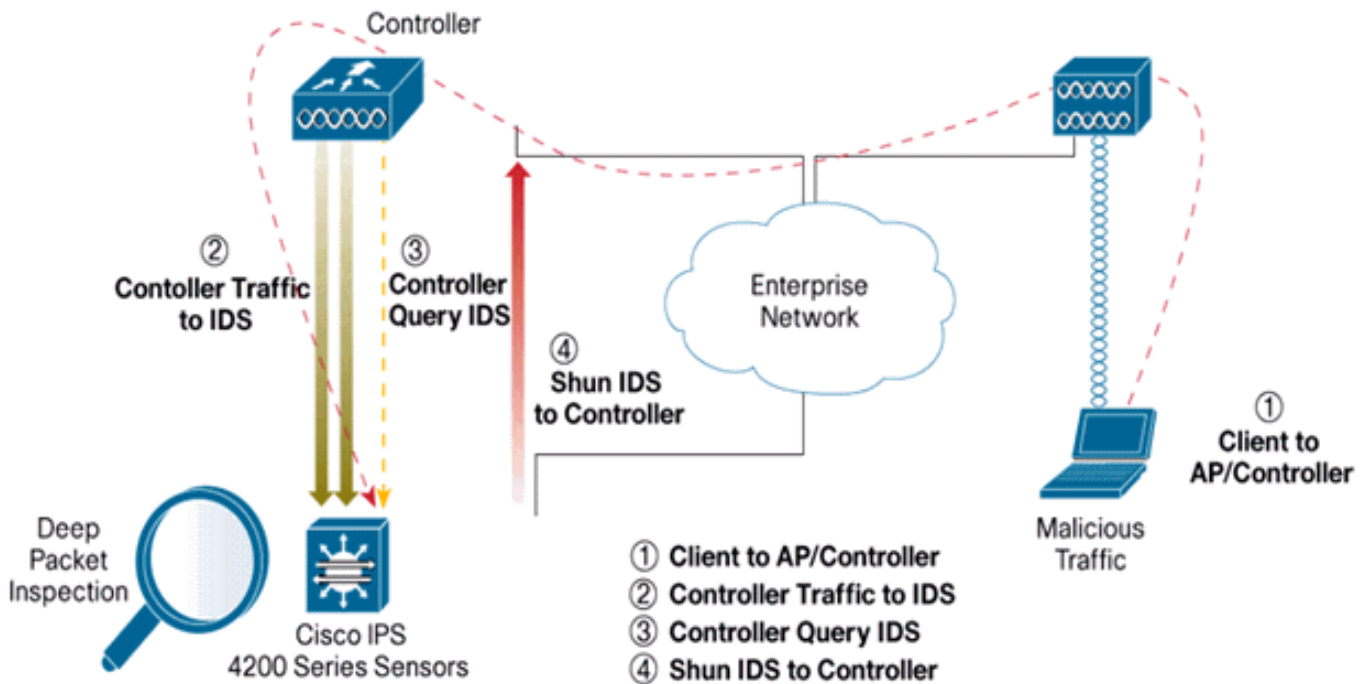
La versión 5.0 de la identificación de Cisco introduce la capacidad de configurar niega las acciones cuando se detectan las infracciones de la directiva (firmas). De acuerdo con la configuración de usuario en el sistema IDS/IPS, una petición del evitar se puede enviar a un Firewall, a un router, o a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

Con Cisco el Software Release 4.0 unificado de la red inalámbrica para los reguladores inalámbricos de Cisco, una petición del evitar necesita ser enviado a un WLC para accionar el cliente que pone o el comportamiento de la exclusión disponible en un regulador. El interfaz que el regulador utiliza para conseguir la petición del evitar es el comando y la interfaz de control en la identificación de Cisco.

- 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 identificación

El regulador pregunta al 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 cliente que la dirección IP 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 la identificación. 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.

Note: 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 para determinar que el cliente está poniendo en marcha 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.

Note: 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 la identificación para evite los eventos, la identificación envía la petición del evitar al regulador con la dirección IP A como la dirección IP de la blanco. 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), este cliente con una nueva dirección IP de B release/versión 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 de la dirección MAC 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 direccionamiento anterior del DHCP, 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 de la ayuda de los reguladores solamente a la identificación para el cliente que evita las peticiones que utilizan el puerto de administración en el regulador. El regulador conecta con la identificación para el examen del paquete vía los interfaces aplicables del VLA N que llevan el tráfico del cliente de red inalámbrica.

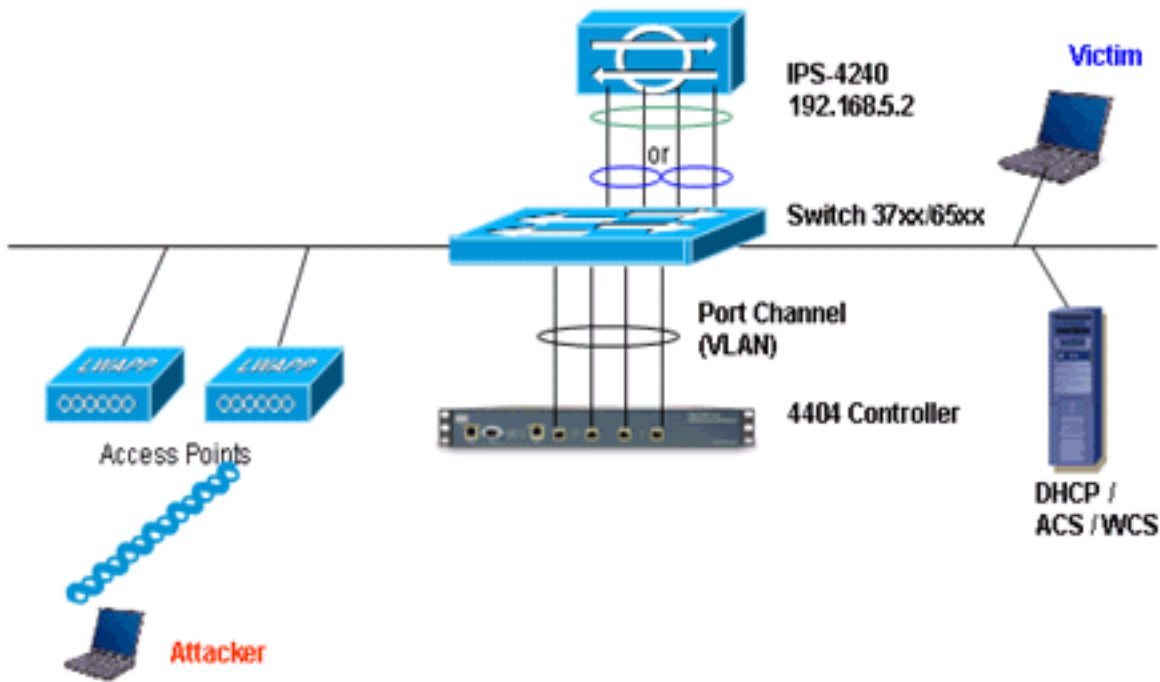
En el regulador, la página de los clientes de la neutralización muestra a cada cliente que se ha inhabilitado vía una petición del sensor IDS. El comando cli show también visualiza una lista de clientes puestos.

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

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

1. Instale y conecte el ids appliance en el mismo conmutador donde reside el regulador inalámbrico.
2. Duplique (SPAN) los puertos 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 la identificación 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. Se notifica un desvío es generado por el WLC y el WCS.
9. Quitar al usuario de la lista de la exclusión después del periodo de tiempo especificado.

[Diseño de la arquitectura de red](#)



Cisco WLC está conectado con las interfaces Gigabit en el catalizador 6500. Cree un Canal de puerto para las interfaces Gigabit y active 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 catalizador 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
```

Los interfaces de detección del sensor IPS pueden actuar individualmente en el **modo promiscuo** o usted puede emparejarlos para crear los 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 vigilado 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.

Note: [El diagrama de la arquitectura](#) es apenas una disposición del ejemplo de WLC y del IPS de arquitectura integrada. El ejemplo de configuración mostrado aquí explica la identificación que detecta el interfaz que actúa en el modo promiscuo. [El diagrama de la arquitectura](#) muestra los interfaces de detección que son emparejados junto para actuar en el modo en línea de los pares. Refiera al [modo en línea](#) para más información sobre el modo en línea del interfaz.

En esta configuración, se asume que el interfaz de detección actúa en el modo promiscuo. El interfaz de la supervisión del sensor IDS de Cisco está conectado con la interfaz Gigabit 5/3 en el catalizador 6500. Cree a una sesión de monitoreo en el catalizador 6500 donde está la fuente la interfaz de canal de puerto de los paquetes y el destino es la interfaz Gigabit donde el interfaz de la supervisión del sensor del IPS de Cisco está conectado. Esto replica todo el ingreso y tráfico de salida de los interfaces atados con alambre regulador a la identificación 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 IDS de Cisco](#)

La configuración inicial del sensor IDS de Cisco es hecha del puerto de la consola o conectando

un monitor y un teclado con el sensor.

1. Clave al dispositivo: Conecte un puerto de la consola con el sensor. Conecte un monitor y un teclado con el sensor.
2. Pulse su nombre de usuario y contraseña en el prompt de inicio de sesión. **Note:** El nombre de usuario y contraseña del valor por defecto es ambos Cisco. Le incitan cambiarlos la primera vez usted clave al dispositivo. Usted debe primero ingresar la contraseña de 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. **Note:** Ésta es el comando y la interfaz de control en la identificación usada para comunicar con el regulador. Este direccionamiento debe ser routable a la interfaz de administración del regulador. Los 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 de la identificación.

```
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
```

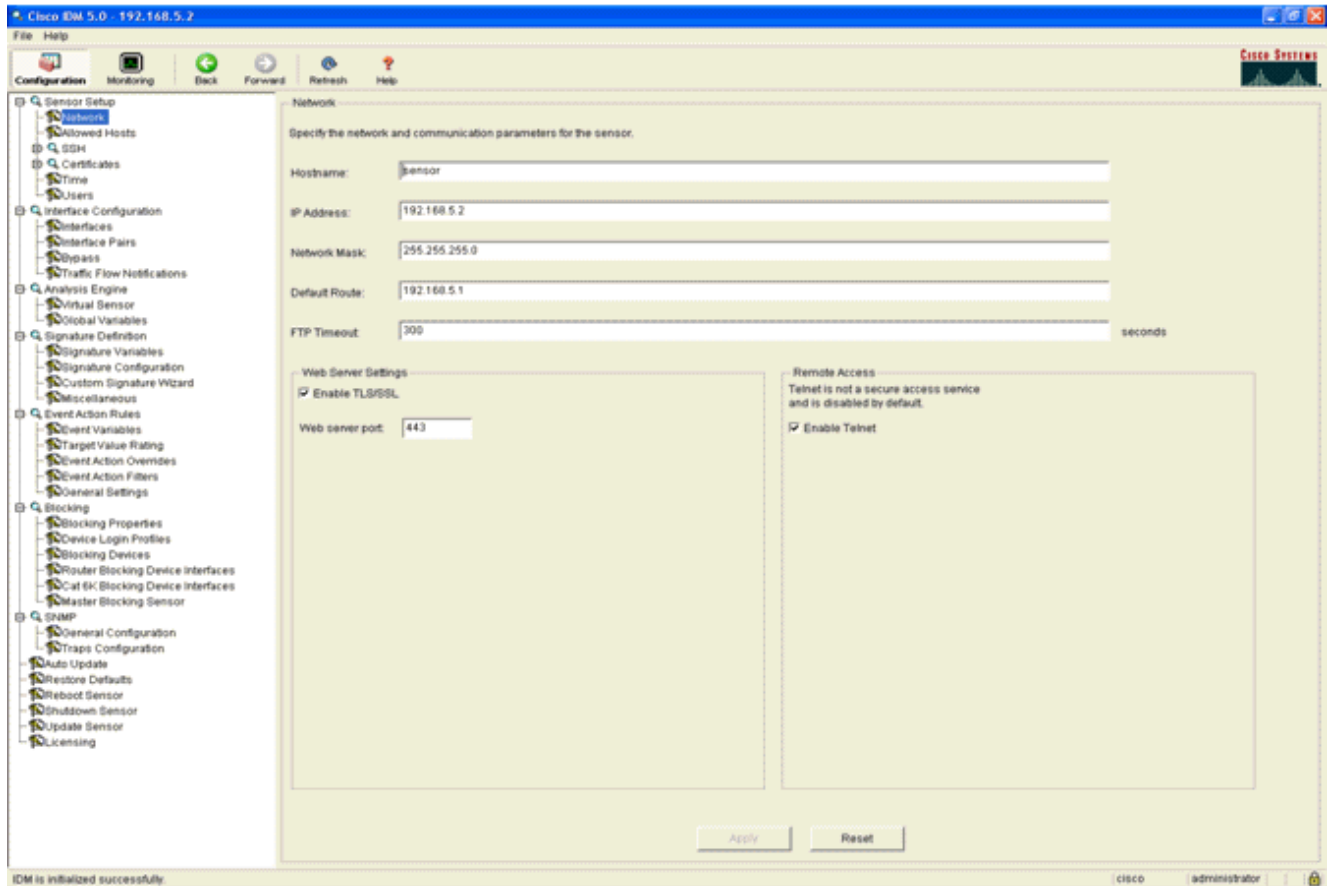
```
--- 192.168.5.1 ping statistics ---
```

```
4 packets transmitted, 4 packets received, 0% packet loss
```

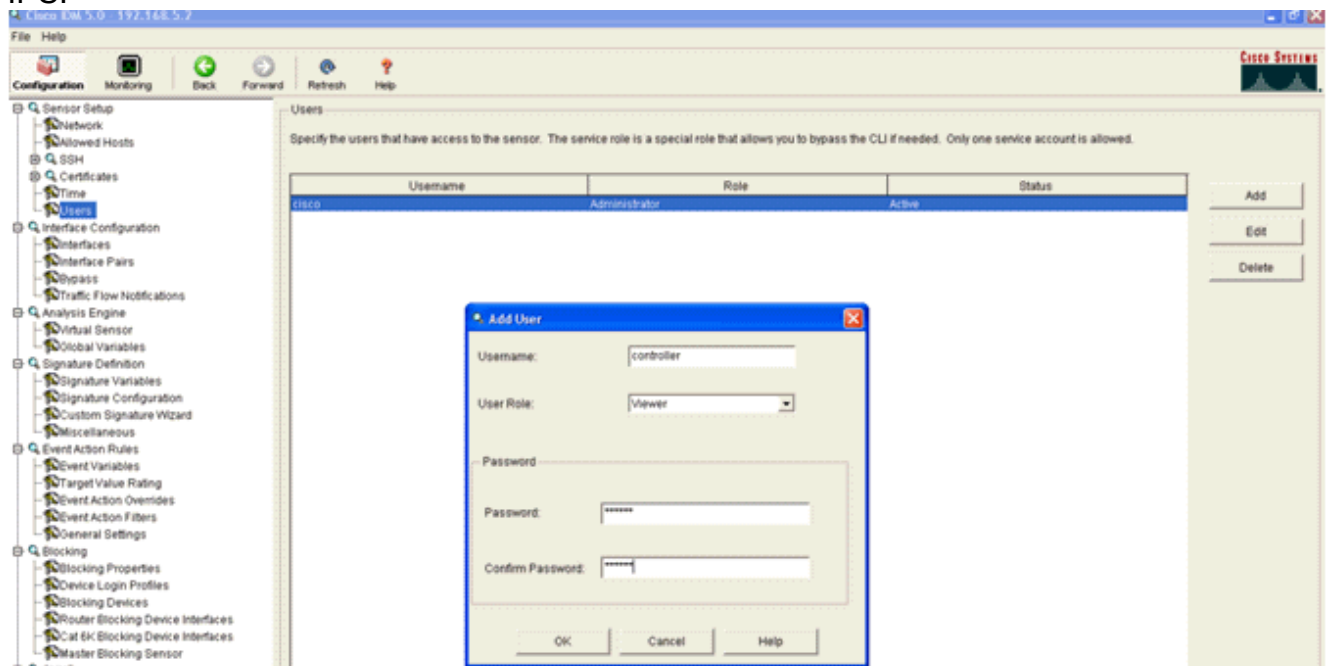
```
round-trip min/avg/max = 0.3/0.6/1.0 ms
```

sensor#

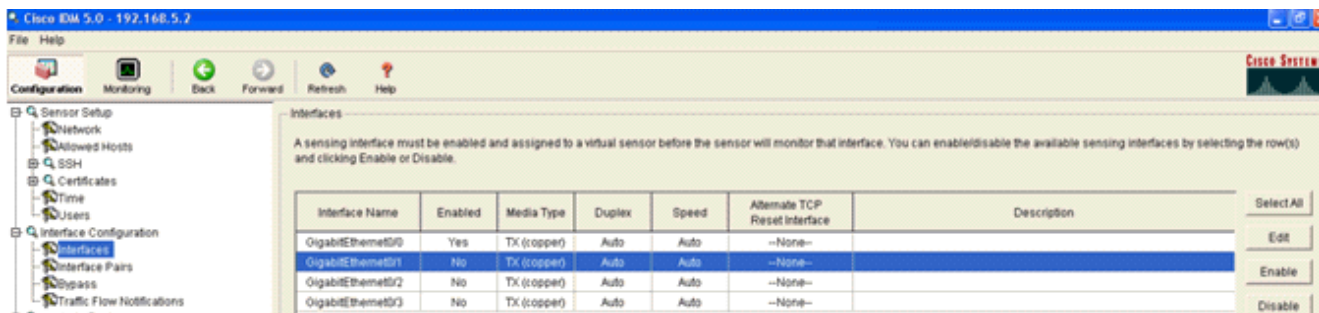
4. Usted puede ahora configurar el sensor IPS del GUI. Señale al navegador a la dirección IP de la Administración del sensor. Este visualizaciones de imágenes una muestra donde el sensor se configura con 192.168.5.2.



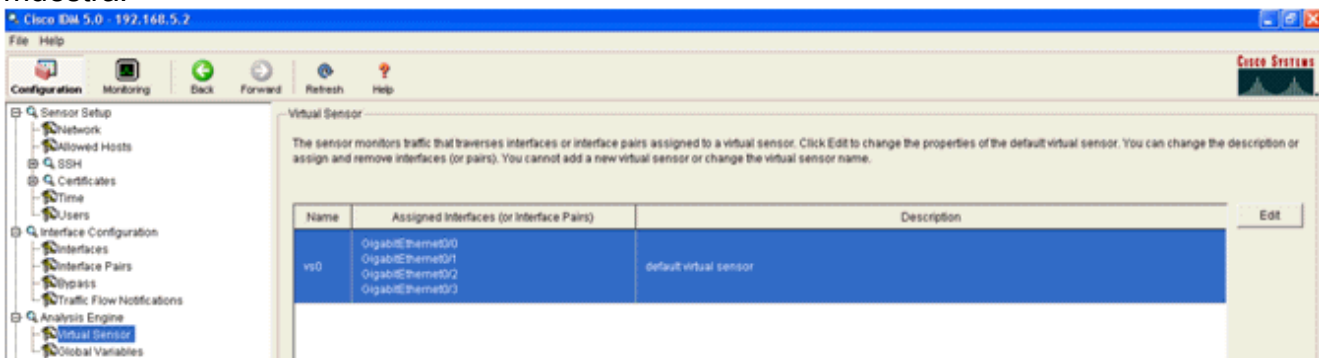
5. Agregue a un usuario que el WLC utilice para tener acceso a los eventos del sensor IPS.



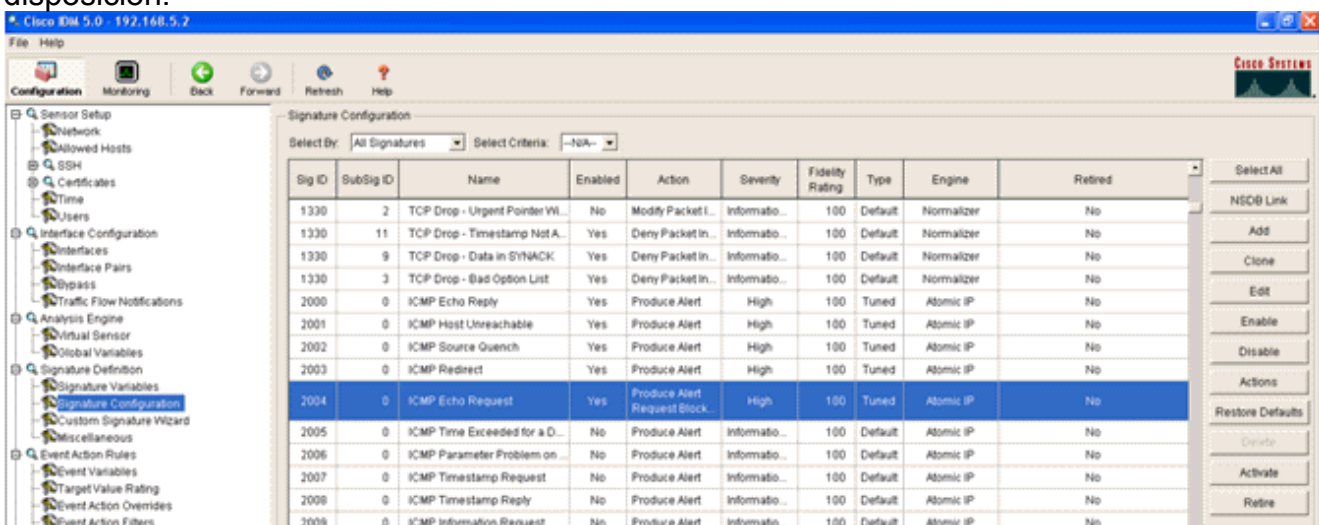
6. Active los interfaces de la supervisión.



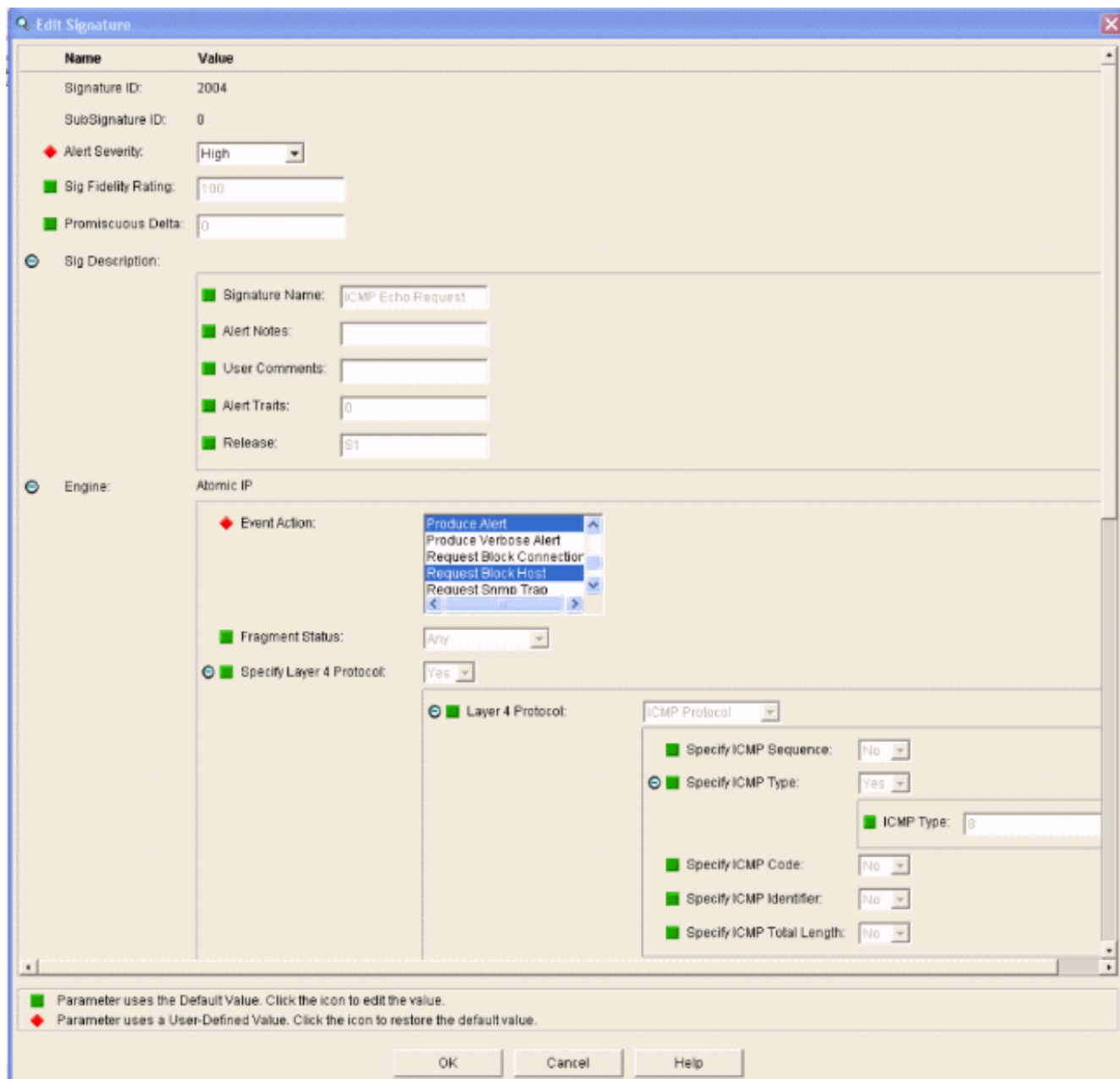
Los interfaces de la supervisión se deben agregar al motor del análisis, pues esta ventana muestra:



7. Seleccione la firma 2004 (petición de la generación de eco ICMP) para realizar una verificación rápida de la disposición.



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



Configure el WLC

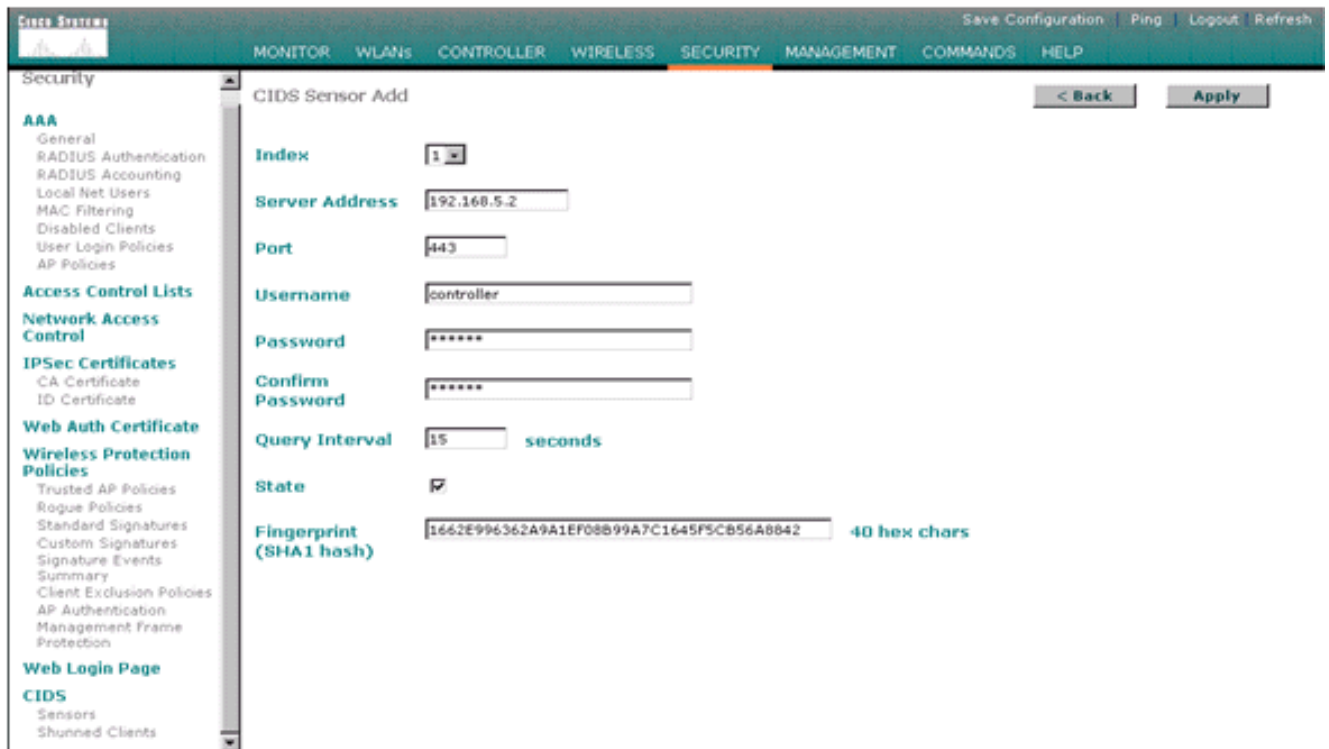
Complete estos pasos para configurar el WLC:

1. Una vez que el dispositivo IPS se configura y alista para ser agregado en el regulador, elija la **Seguridad > CIDS > 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-identificación.

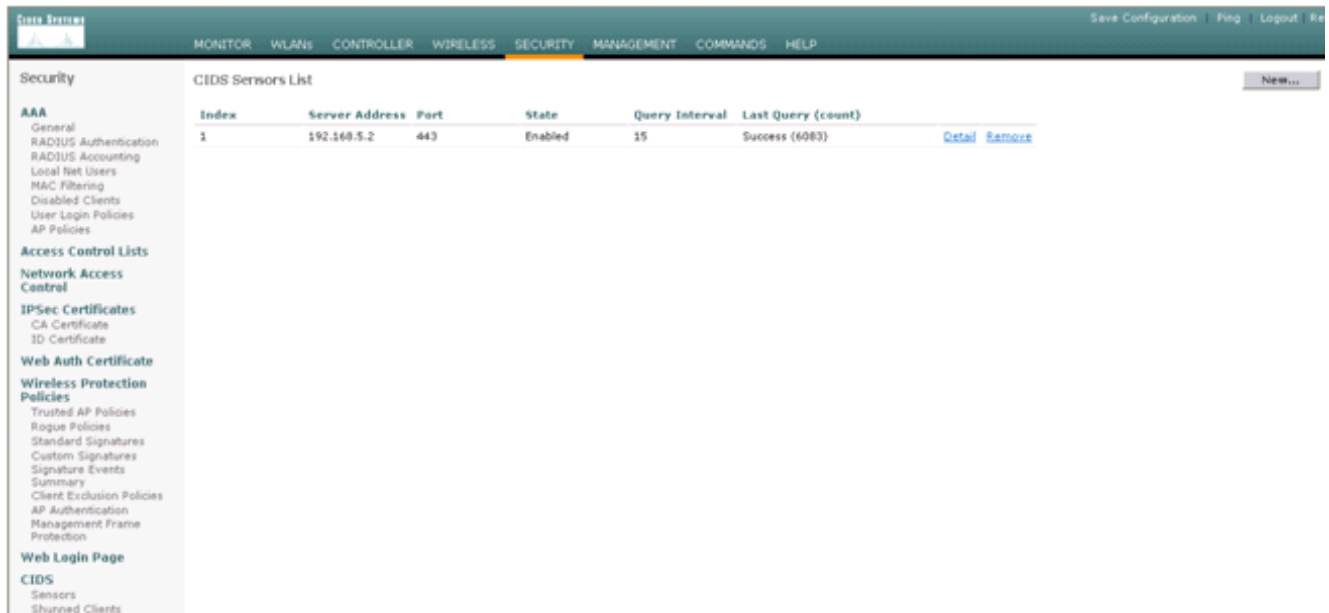
```
sensor#show tls fingerprint
```

```
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
```

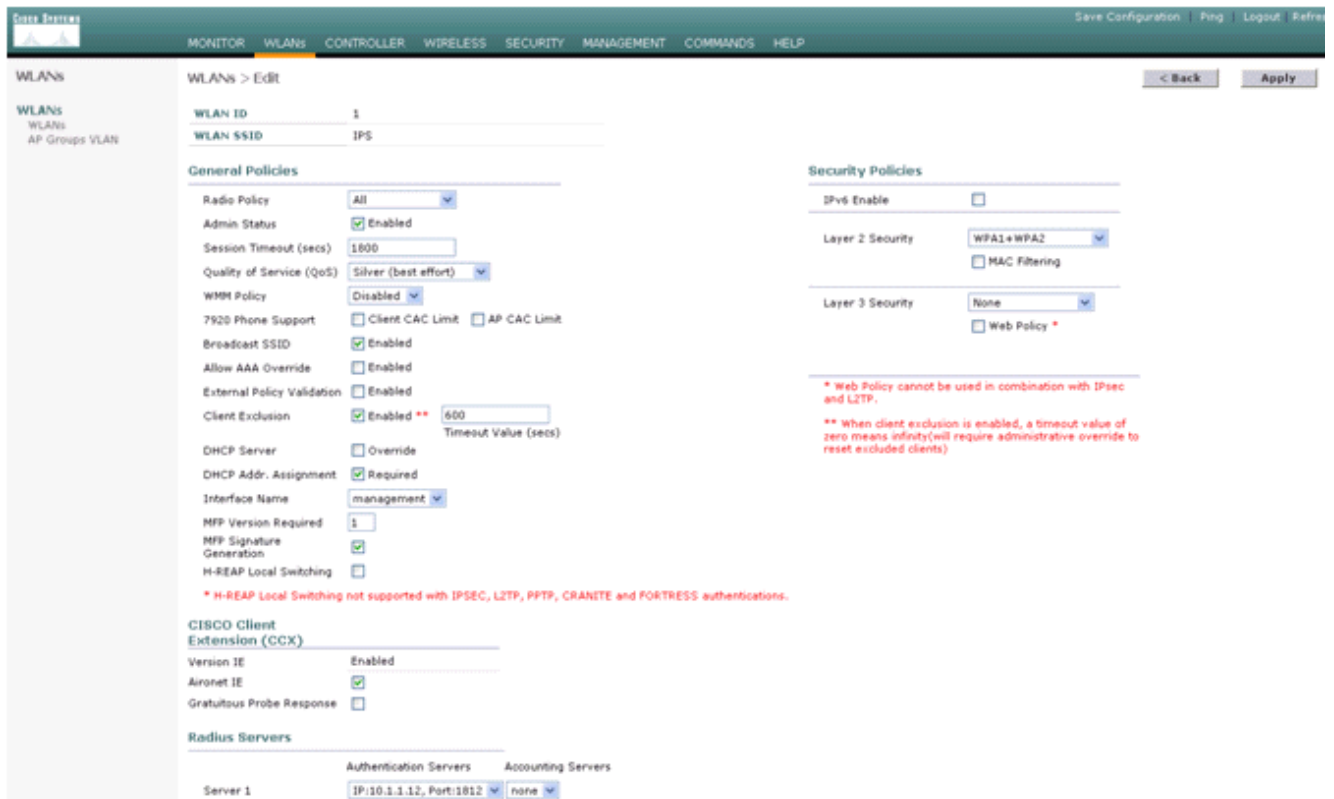
```
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



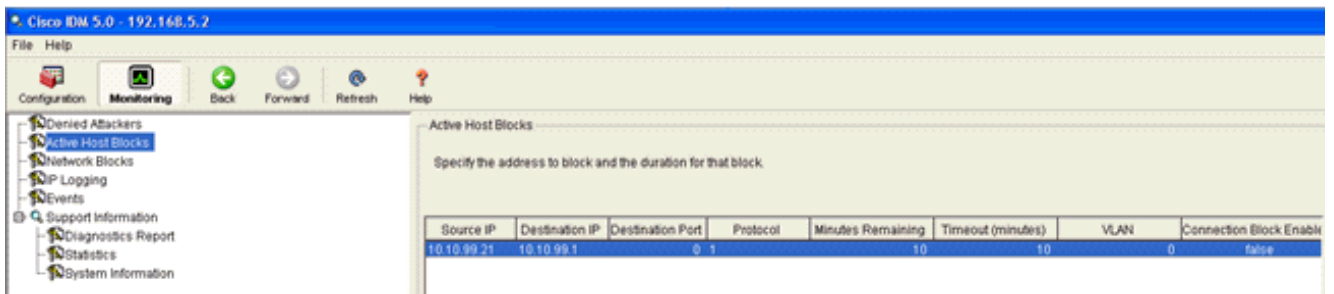
3. Controle el estatus de la conexión entre el sensor IPS y el WLC.



4. Una vez que usted establece la Conectividad con el sensor del IPS de Cisco, asegúrese de que la configuración de la red inalámbrica (WLAN) esté correcta y eso usted activa la **exclusión del cliente**. El valor de agotamiento del tiempo de la exclusión del cliente del valor por defecto 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 la identificación siga siendo activo. El tiempo del bloque del valor por defecto en la identificación 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 vigilados por el sensor del IPS de Cisco. Una vez que una alarma se acciona en el IPS de Cisco, vaya a los **bloques el vigilar y del host activo** para controlar los detalles sobre el host.



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

The screenshot shows the Cisco Systems Security interface. The left sidebar contains a navigation menu with categories like AAA, Access Control Lists, Network Access Control, IPsec Certificates, Web Auth Certificate, Wireless Protection Policies, and Web Login Page. The main content area is titled 'CIDS Shun List' and includes a 'Re-sync' button. Below the button is a table with the following data:

IP Address	Last MAC Address	Expire	Sensor IP / Index
10.10.99.21	00:40:96:ad:0d:1b	326979296	192.168.5.2 / 1

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

Agrega

The screenshot shows the 'Excluded Clients' page in the Cisco Systems interface. It features a search bar labeled 'Search by MAC address' and a 'Search' button. Below the search bar is a table with the following data:

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Exclusion Reason	Port	
00:40:96:ad:0d:1b	AP1242-2	00:14:1b:59:3e:10	IPS	802.11b	UnknownEnum:5	29	Detail Link Test Disable Remove

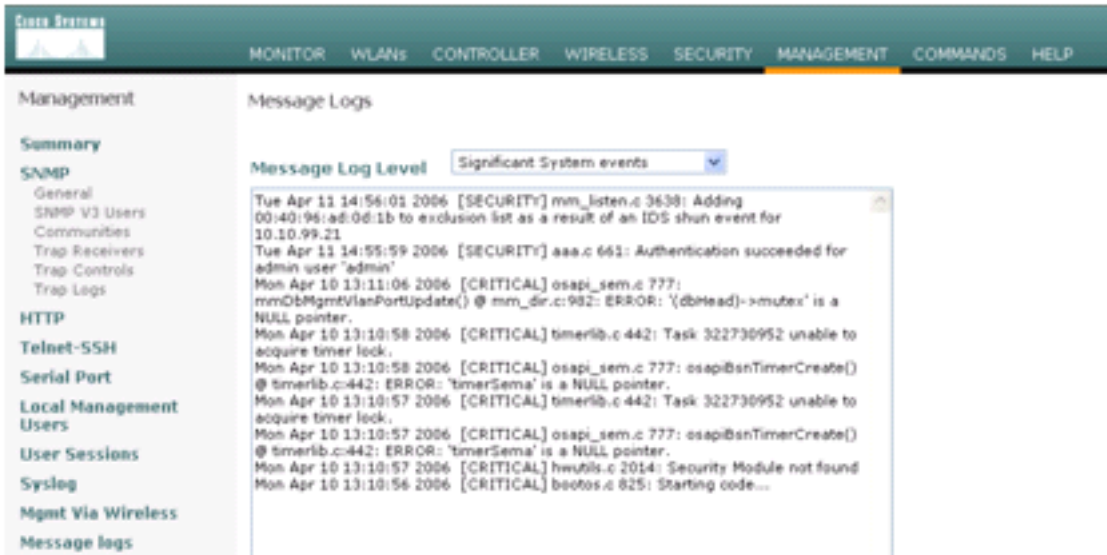
Se genera un registro del desvío mientras que agregan a un cliente a la lista del

The screenshot shows the 'Management' page in the Cisco Systems interface, displaying a log of events. The log entries are as follows:

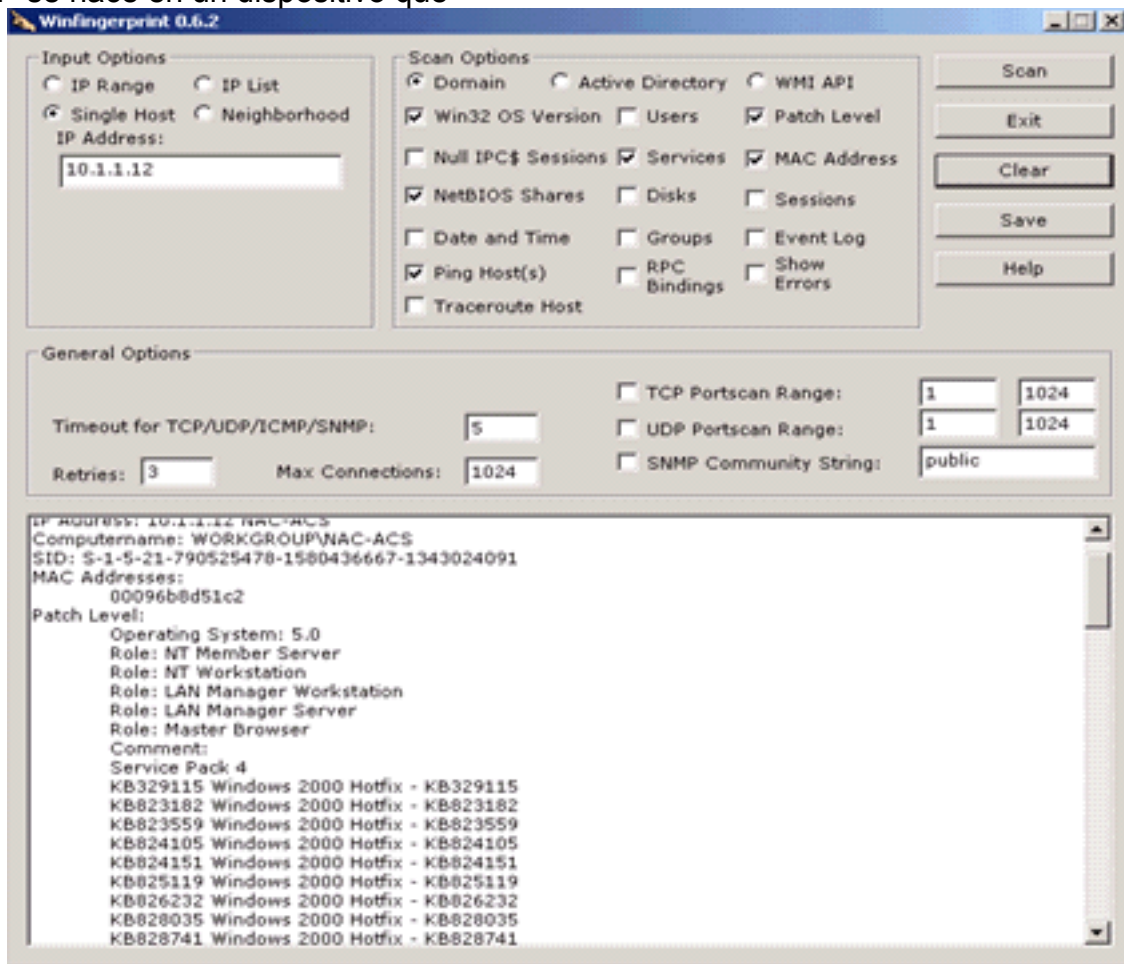
Event ID	Timestamp	Message
32	Tue Apr 11 14:41:00 2006	Rogue AP : 00:13:c7:82:03:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g) with RSSI: -83 and SNR: 6
33	Tue Apr 11 14:40:16 2006	New client at 10.10.99.21 requested to be shunned by Sensor at 192.168.5.2
34	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85:54:de:5d removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
35	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85:54:de:5e removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
36	Tue Apr 11 14:39:44	Rogue : 00:0b:85:54:de:5f removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)

evitar.
 registro de mensajes también se genera para el

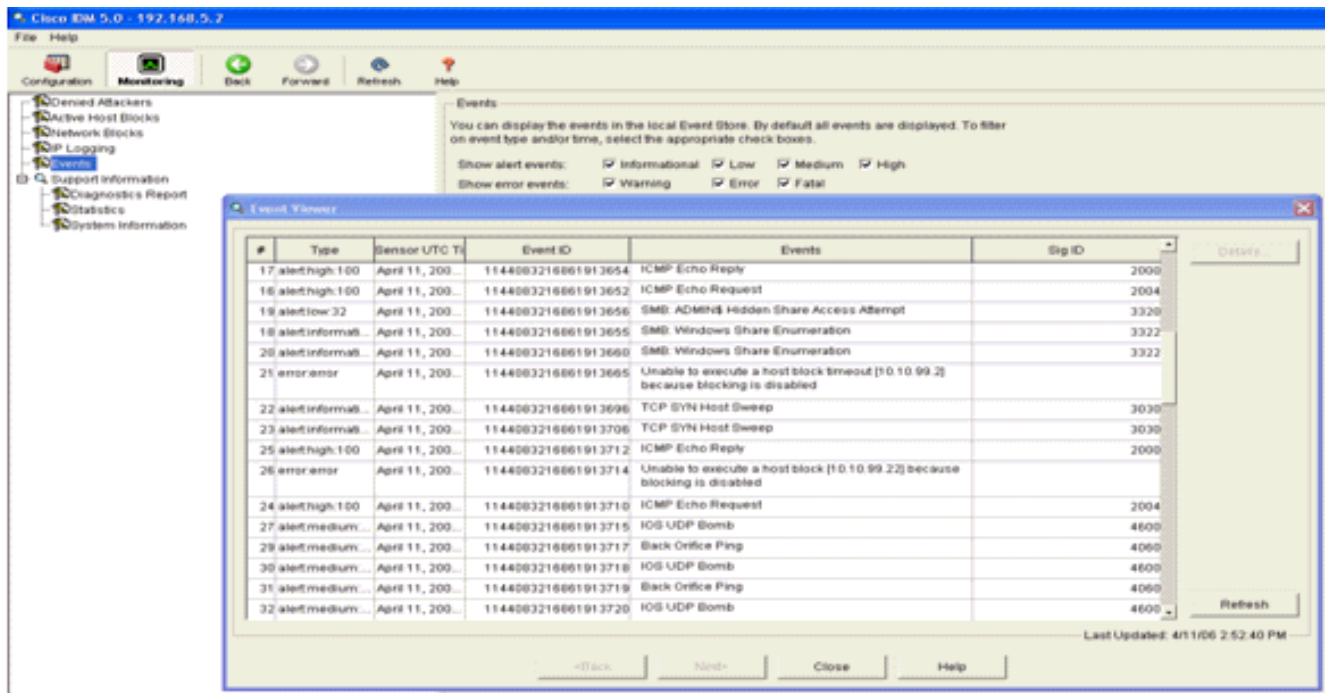
Un



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



vigila. Esta
 ventana muestra los eventos generados en el sensor del IPS de Cisco.



Configuración de muestra del sensor IDS de Cisco

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

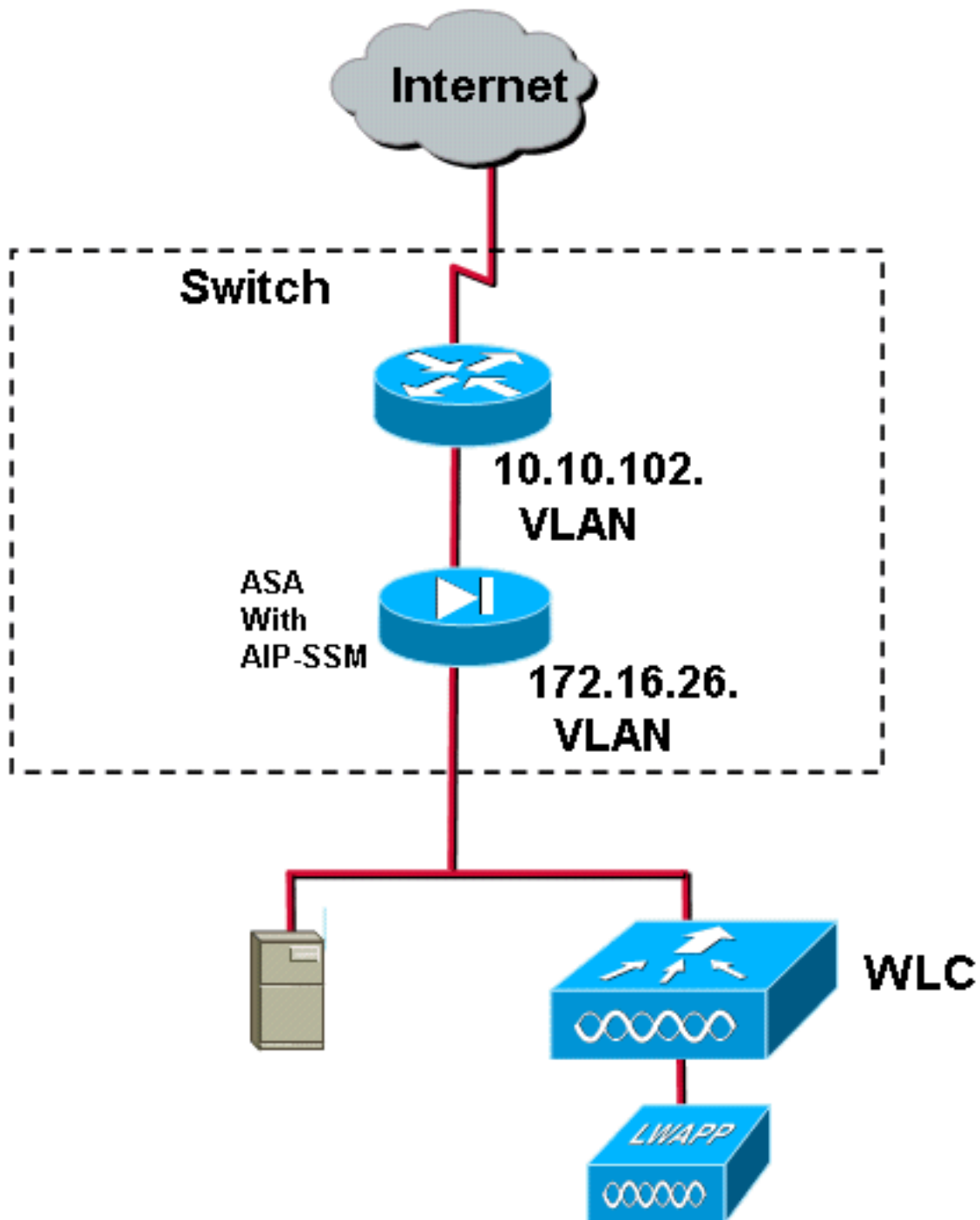
```

```
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 la identificación](#)

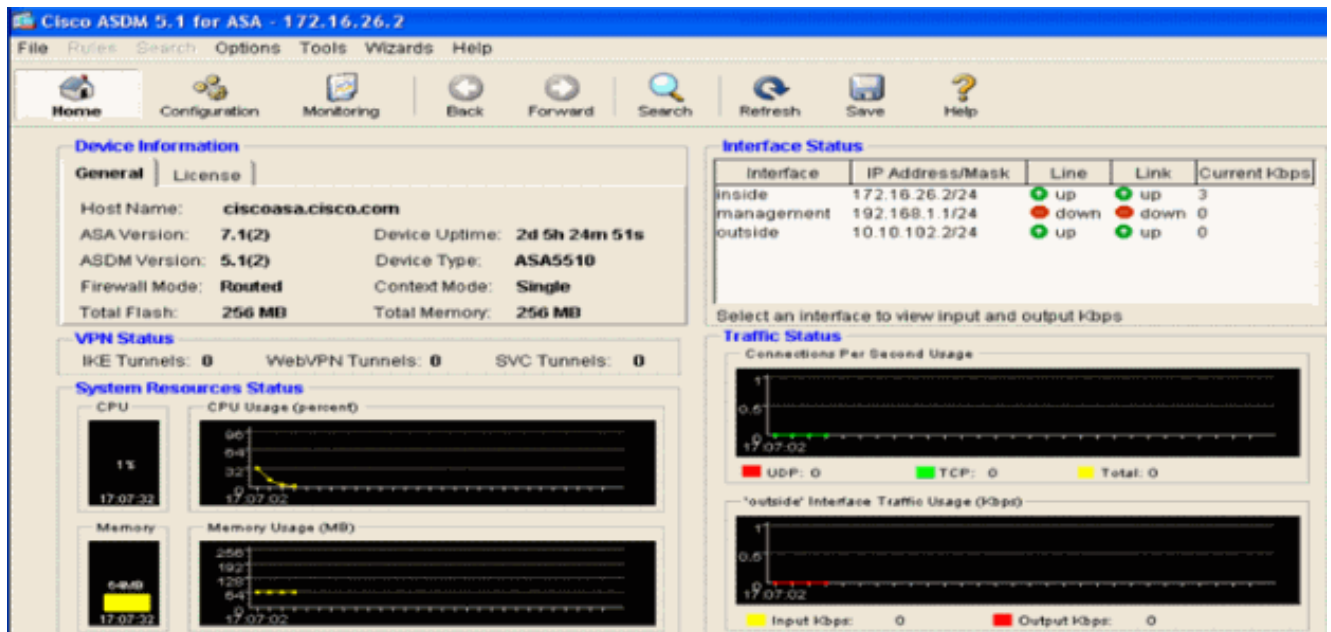
A diferencia de un sensor tradicional de la detección de intrusos, un ASA debe siempre estar en la trayectoria de datos. Es decir en vez de atravesar el tráfico de un puerto del switch encima a un

puerto pasivo el oler en el sensor, el ASA debe recibir los datos sobre un interfaz, lo procesa internamente, y después le remite hacia fuera otro puerto. Para la identificación, 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.

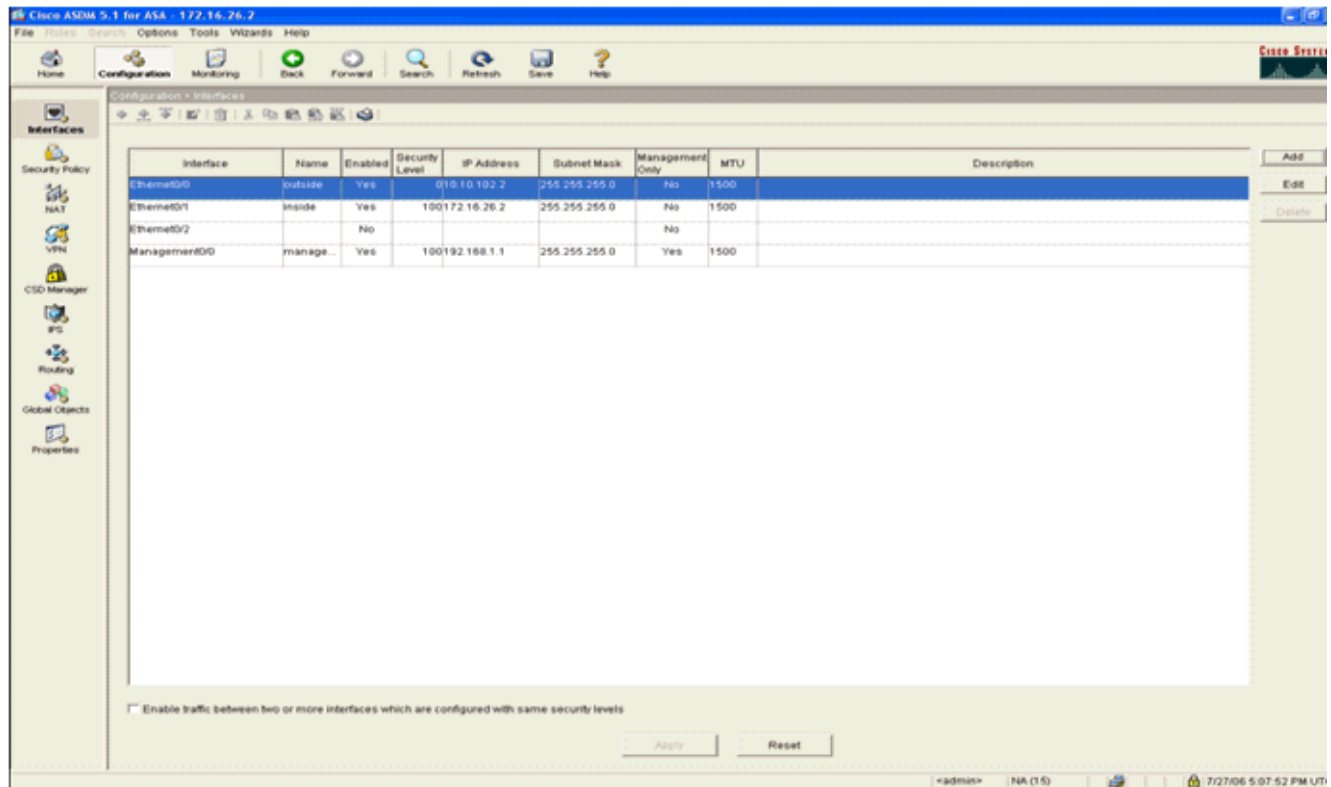


En este ejemplo, el ASA usado se pone y pasa ya el tráfico. Estos pasos demuestran cómo crear una directiva que envíe los datos al AIP-SSM.

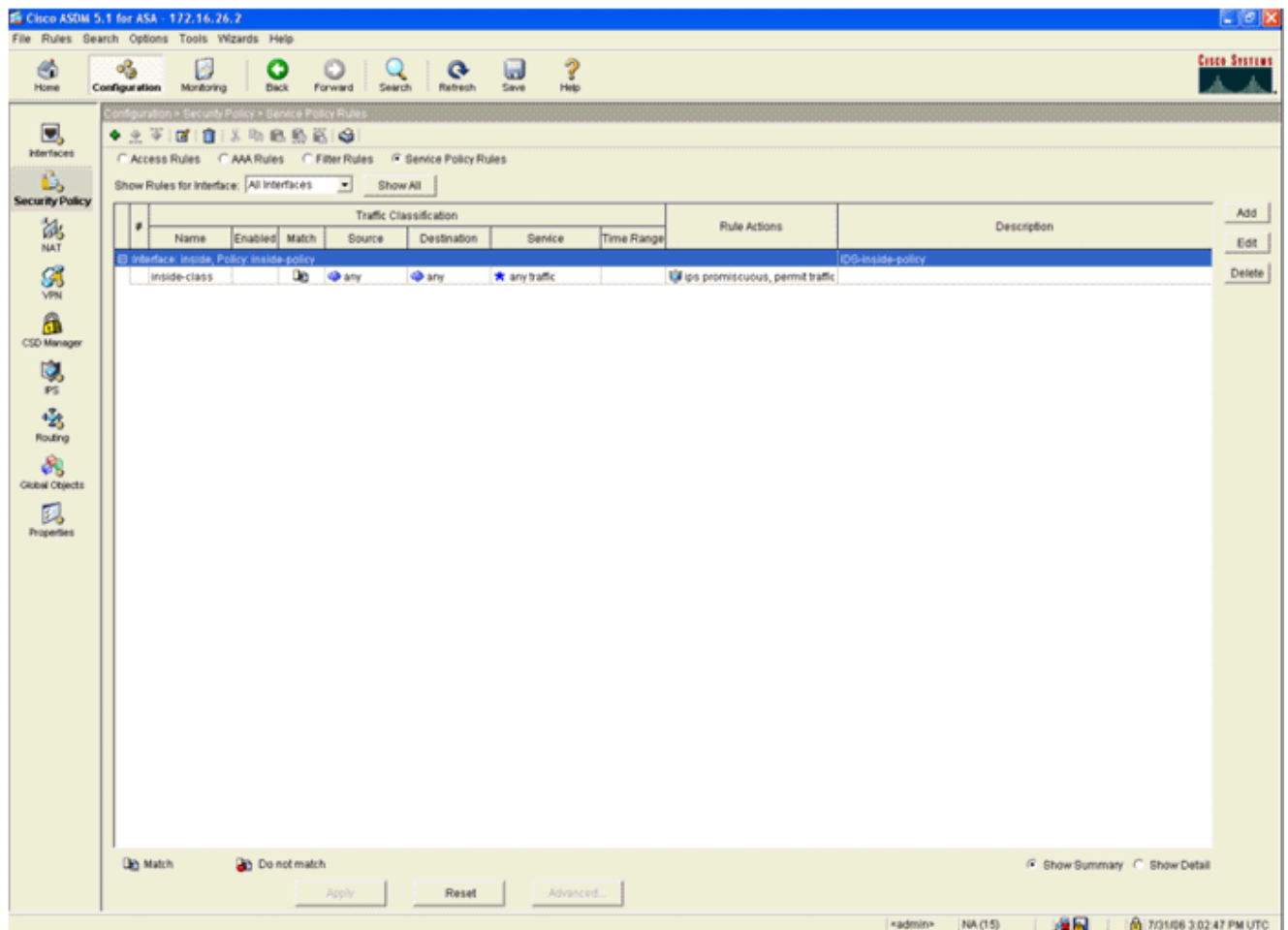
1. Registro en el ASA usando ASDM. Sobre la registración satisfactoria, la ventana del sistema principal ASA aparece.



2. Configuración del teclado en la cima de la página. La ventana cambia a una vista de los interfaces ASA.



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



4. El teclado **agrega** para crear una nueva directiva. El Asistente de la regla de la política de servicio del agregar lanza en una nueva ventana. Haga clic el **interfaz** y después elija el interfaz correcto de la lista desplegable para crear una nueva directiva que esté limitada a uno de los 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.

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a service policy and apply to:

Interface:

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

Description:

< Back Next > Cancel Help

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.

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic match criteria

Default Inspection Traffic

Source and Destination IP Address (uses ACL)

Tunnel Group

TCP or UDP Destination Port

RTP Range

IP DiffServ CodePoints (DSCP)

IP Precedence

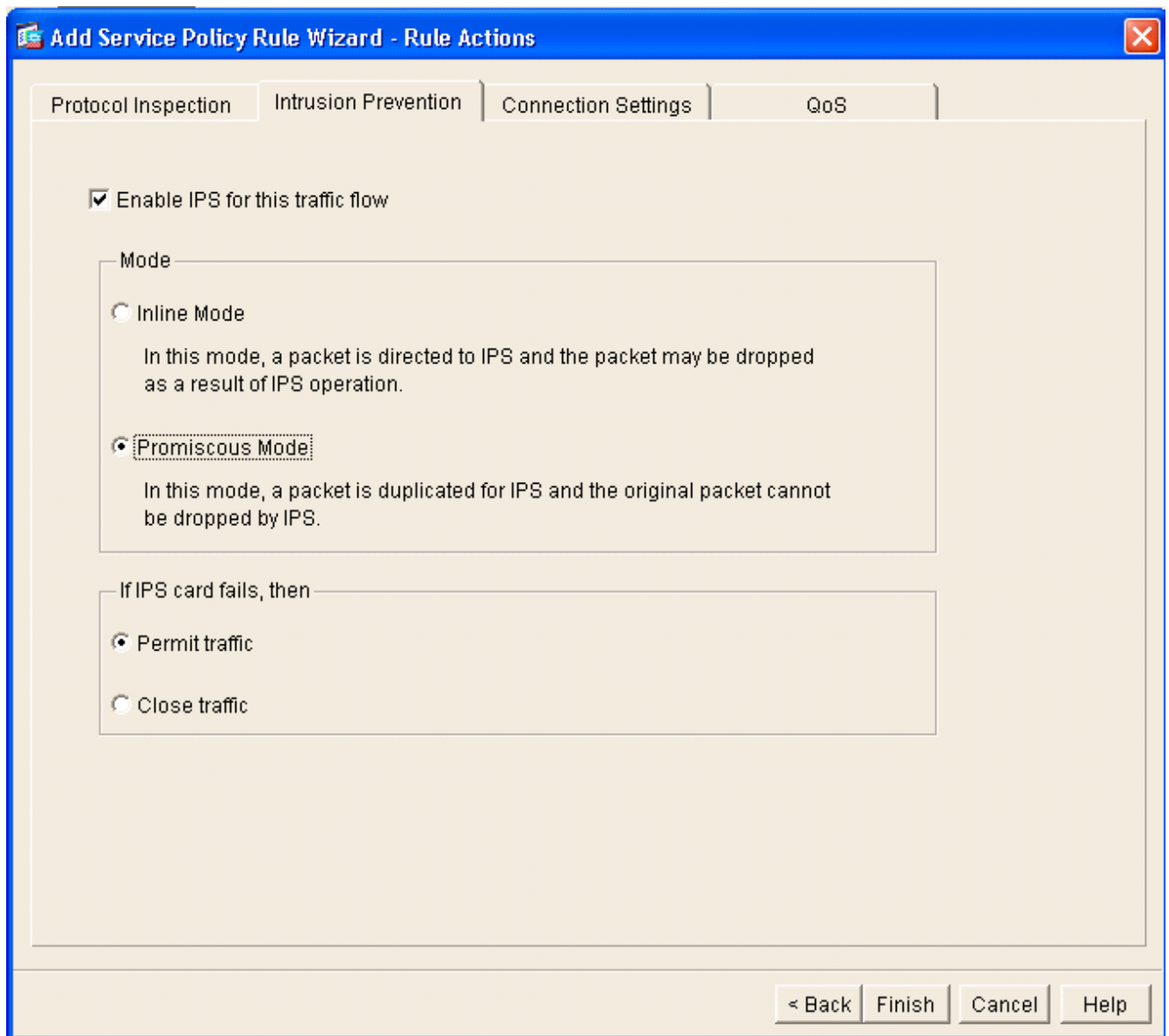
Any traffic

If traffic does not match a existing traffic class, then it will match the class-default traffic class.
Class-default can be used in catch all situation.

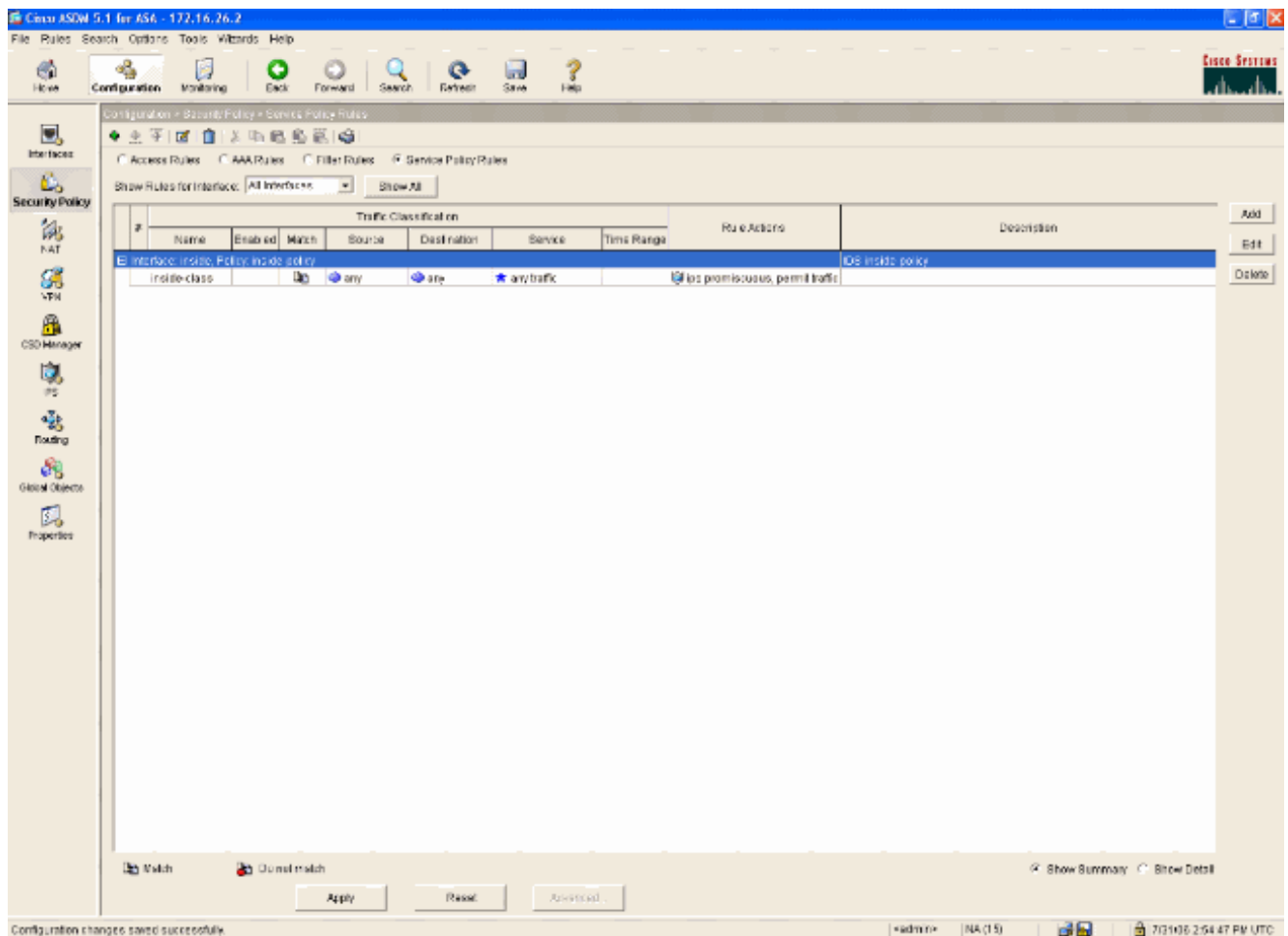
Use class-default as the traffic class.

< Back Next > Cancel Help

6. Complete estos pasos paradá instrucciones el ASA para dirigir el tráfico encima a su AIP-SSM. Controle el **permiso IPS para saber si hay este flujo de tráfico** para activar 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 ASA cambia a un estado fracaso-abierto en caso que el AIP-SSM falle. Clic en Finalizar para confiar el cambio.



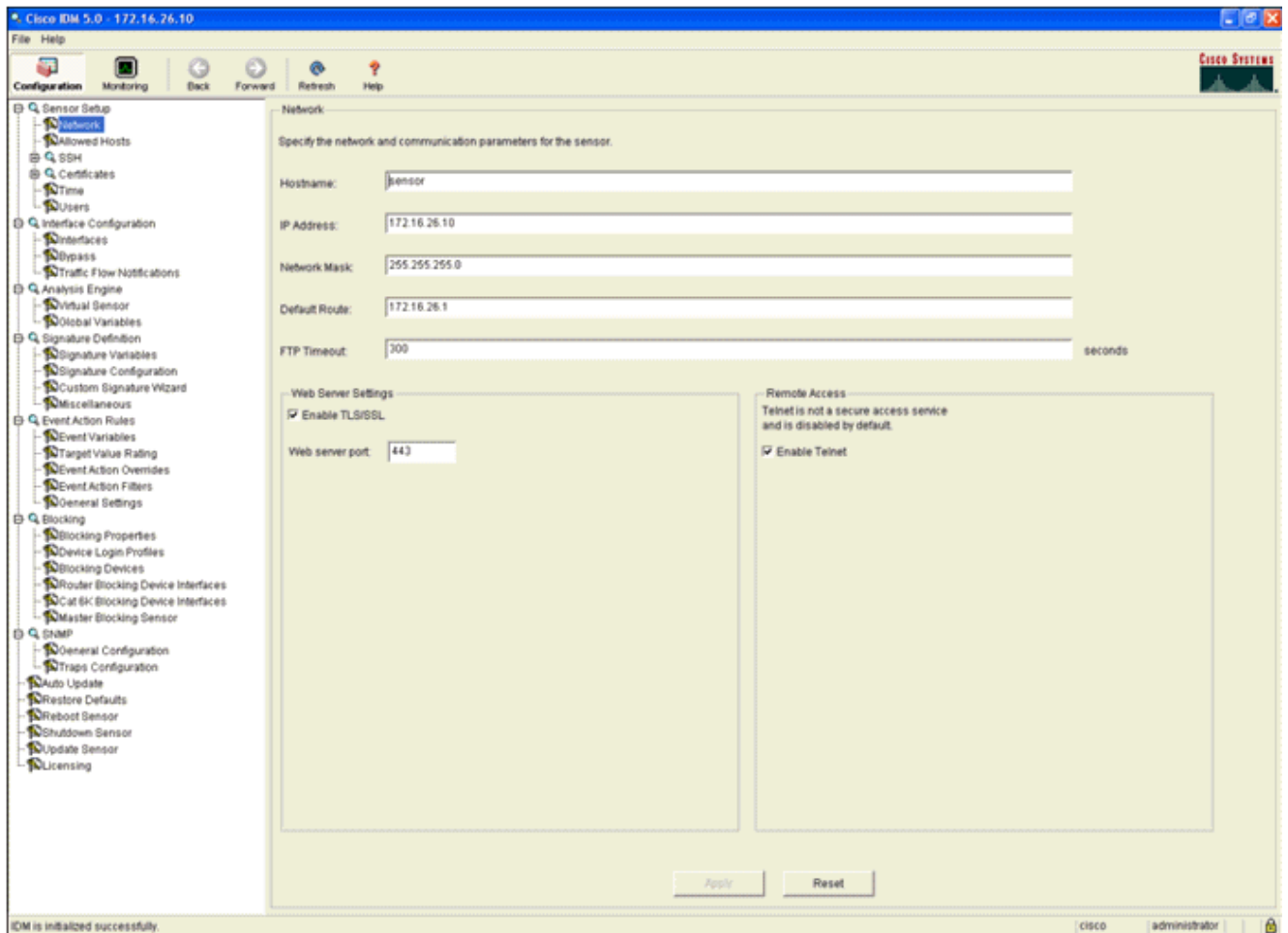
7. El ASA ahora se configura para enviar el tráfico al módulo ips. **Salvaguardia del teclado** en la fila superior para escribir los cambios al ASA.



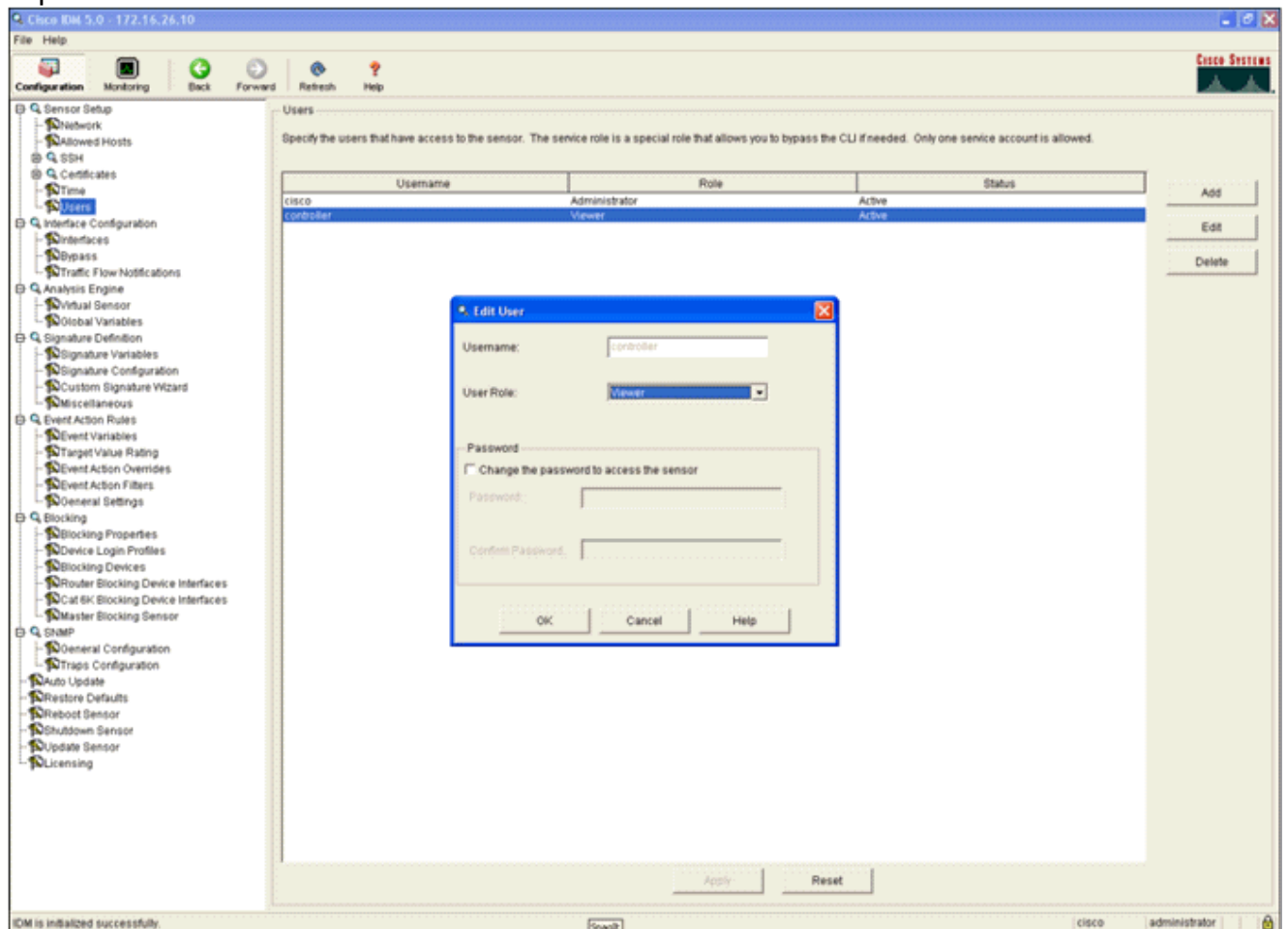
[Configure el AIP-SSM para el examen del tráfico](#)

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

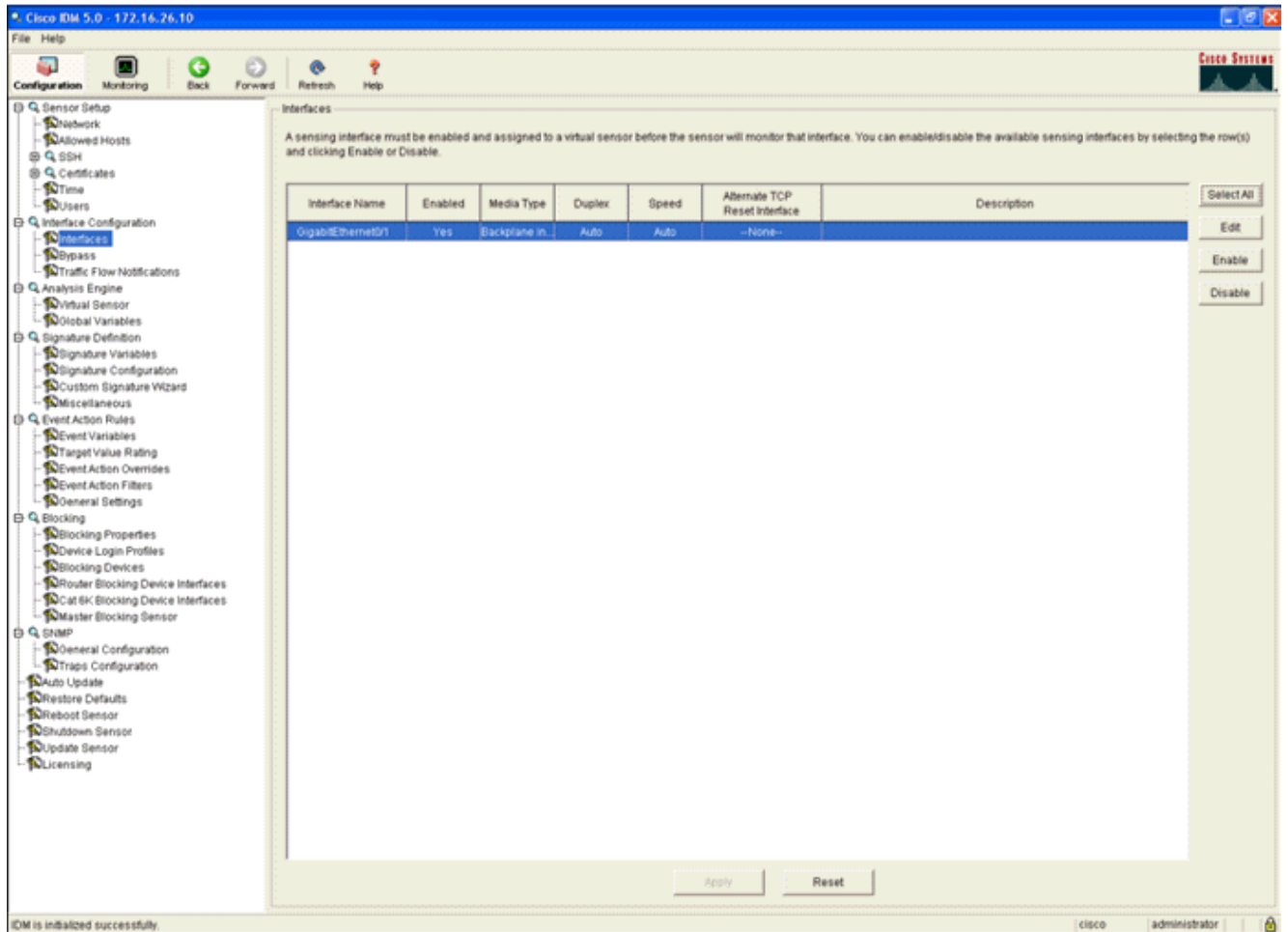
1. Ábrase una sesión al AIP-SSM usando el IDM.



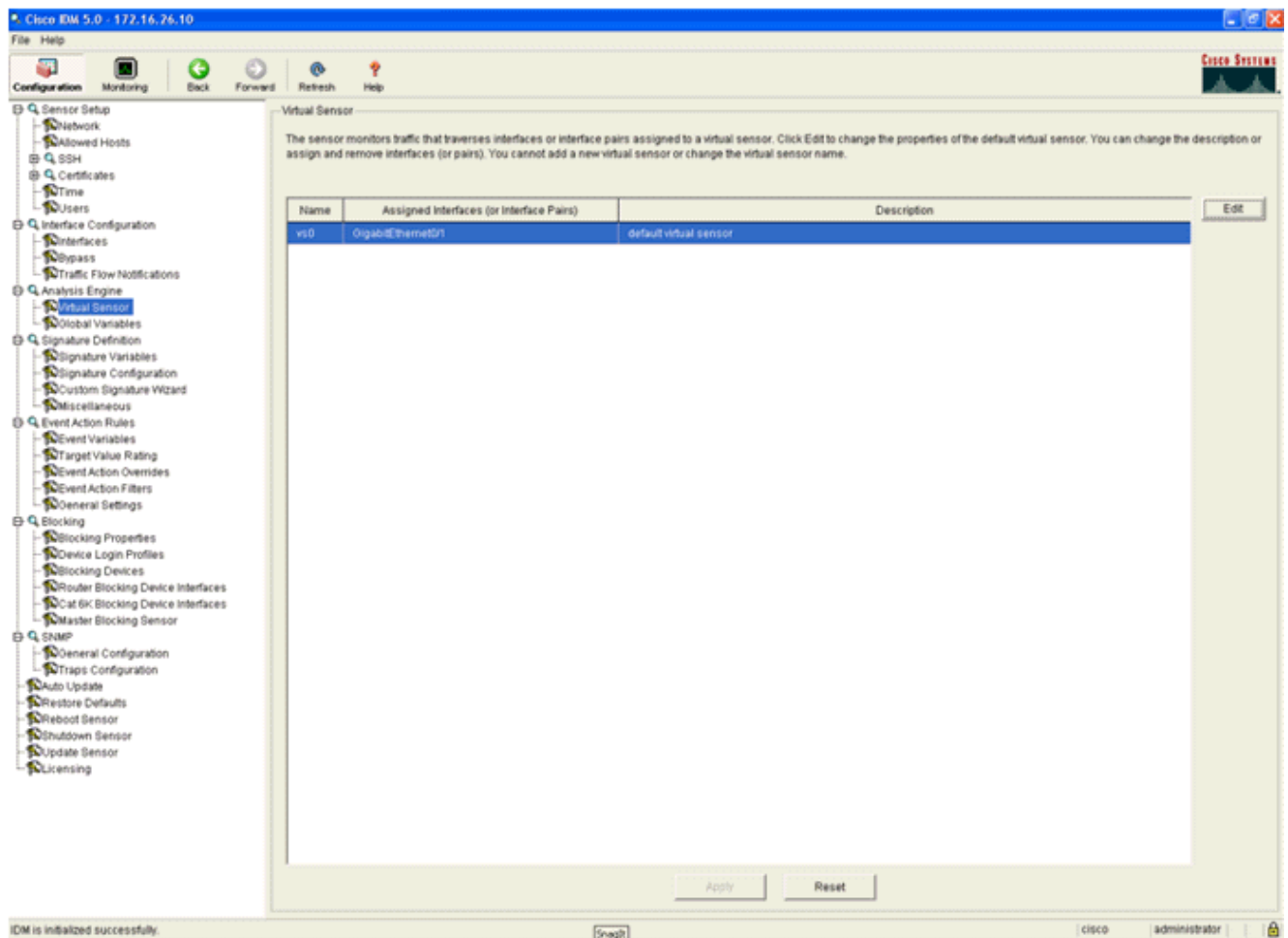
2. Agregue a un usuario con por lo menos los privilegios del espectador.



3. Habilite la interfaz.



4. Controle 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 > CIDS > 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-identificación.

```
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
```

The screenshot shows the Cisco Systems Security configuration page for CIDS Sensor Edit. The left sidebar contains a navigation menu with categories: AAA, Access Control Lists, IPSec Certificates, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area displays the configuration for a CIDS sensor with the following fields:

- Index:** 2
- Server Address:** 172.16.26.10
- Port:** 443
- Username:** controller
- Password:** *****
- State:**
- Query Interval:** 10 seconds
- Fingerprint (SHA1 hash):** 90C9969B4EFA74F8528092BBBC483C45B4876C55 (40 hex chars) (hash key is already set)
- Last Query (count):** Success (1400)

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

The screenshot shows the Cisco Systems Security configuration page for CIDS Sensors List. The left sidebar contains a navigation menu with categories: AAA, Access Control Lists, IPSec Certificates, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area displays a table of CIDS sensors:

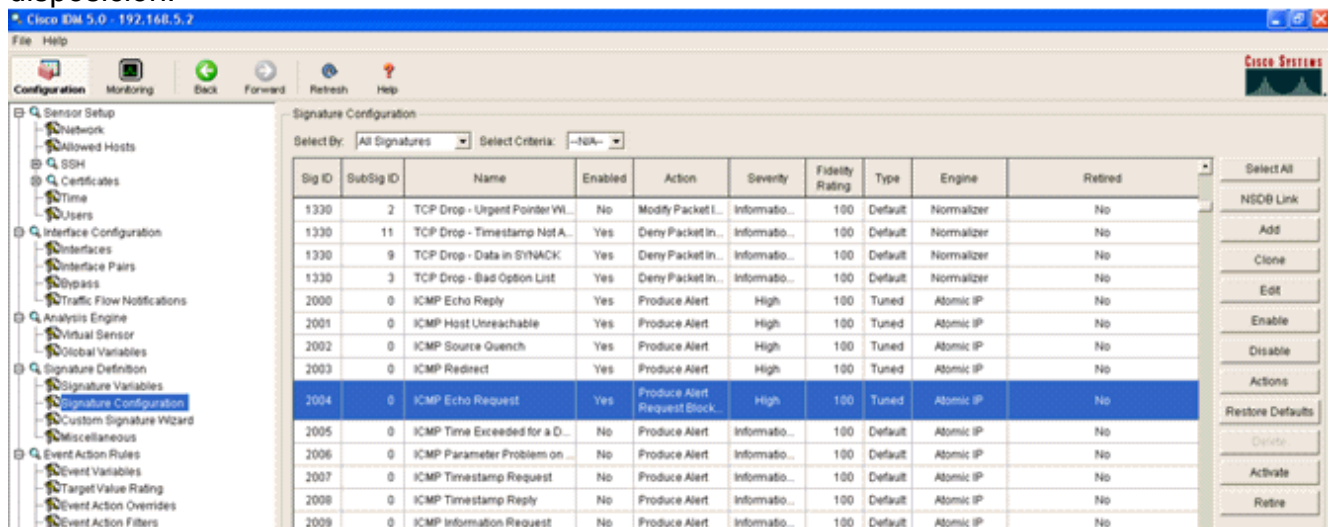
Index	Server Address	Port	State	Query Interval	Last Query (count)	
1	192.168.5.2	443	Enabled	15	Unauthorized (1)	Detail Remove
2	172.16.26.10	443	Enabled	10	Success (1444)	Detail Remove

[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** (petición de la generación de eco ICMP) para realizar una verificación rápida de la

disposición.



2. Active 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.

Edit Signature

Name	Value
Signature ID:	2004
SubSignature ID:	0
Alert Severity:	High
Sig Fidelity Rating:	100
Promiscuous Delta:	0

Sig Description:

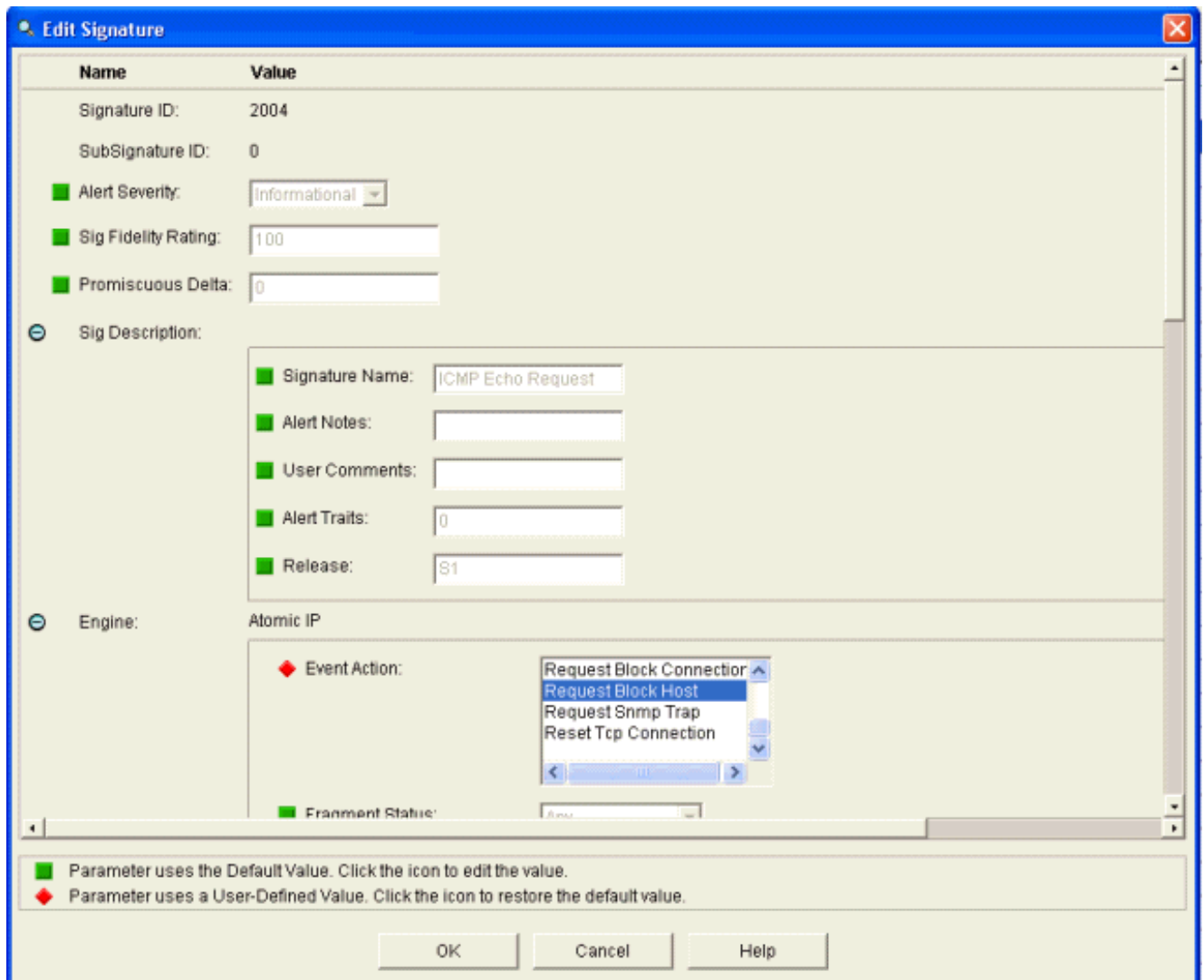
Signature Name:	ICMP Echo Request
Alert Notes:	
User Comments:	
Alert Traits:	0
Release:	B1

Engine: Atomic IP

Event Action:	<ul style="list-style-type: none"> Produce Alert Produce Verbose Alert Request Block Connector 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

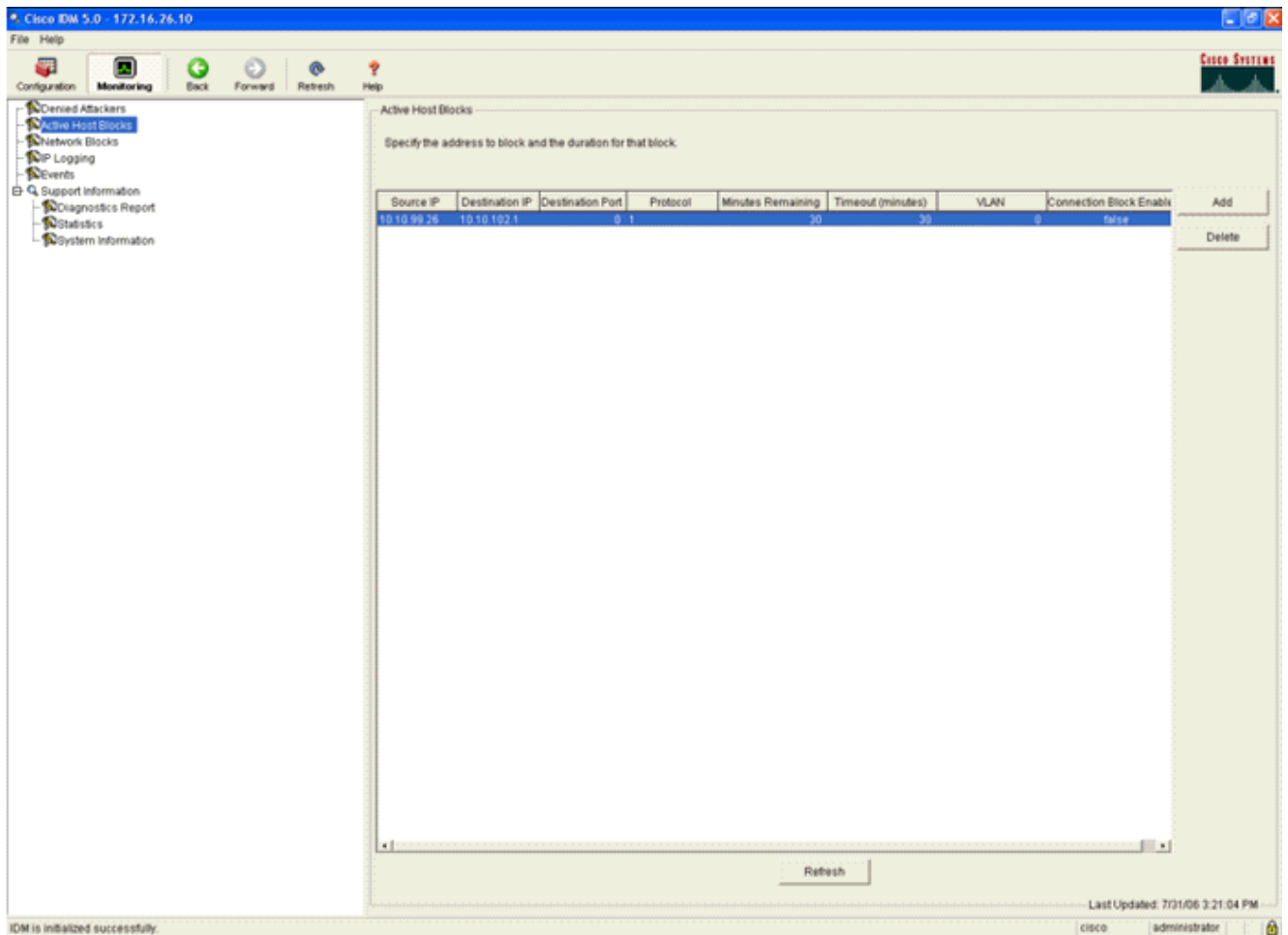


3. Haga clic la **AUTORIZACIÓN** para salvar la firma.
4. Verifique que la firma sea activa y que está fijada para realizar una acción de bloqueo.
5. El teclado **se aplica** para confiar la firma al módulo.

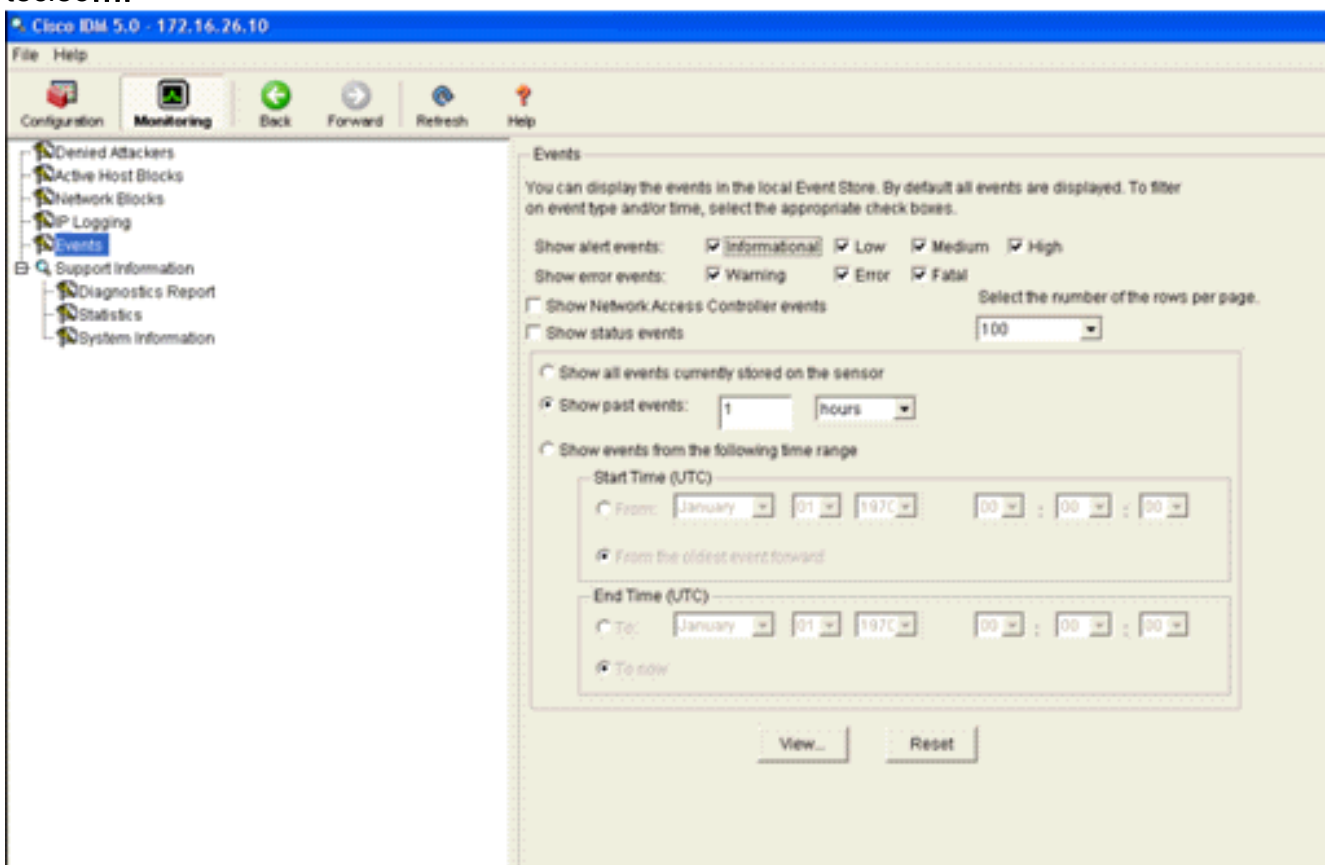
[Vigile el bloqueo y los eventos con el IDM](#)

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 items 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 valor por defecto que bloquea el tiempo 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 almacenador intermedio del evento AIP-SSM. De la página de la supervisión IDM, seleccione los **eventos** en la lista de los ítems en el lado izquierdo. La utilidad de la búsqueda de los eventos aparece. Fije los criterios de búsqueda y la **opinión** apropiados del teclado....



- El espectador del evento entonces aparece con una lista de eventos que hagan juego los criterios dados. El desplazamiento a través de la lista y encuentra la firma de la petición de la generación 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 identificación de los Sig.

#	Type	Sensor UTC Time	EventID	Events	Sig ID	Details...
1	error:error	July 31, 2006 2:59:52 PM U...	1145383740954940828	Unable to execute a host block [10.10.99.26] because blocking is not configured		
2	error:warning	July 31, 2006 3:16:51 PM U...	1145383740954941447	while sending a TLS warning alert close_notify, the following error occurred: socket error [3,32]		
3	alert:informati...	July 31, 2006 3:19:16 PM U...	1145383740954941574	ICMP Echo Request	2004	
4	error:error	July 31, 2006 3:19:16 PM U...	1145383740954941577	Unable to execute a host block [10.10.99.26] because blocking is not configured		
5	alert:informati...	July 31, 2006 3:19:46 PM U...	1145383740954941597	ICMP Echo Request	2004	

Last Updated: 7/31/06 3:22:39 PM

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

```

evIdsAlert: eventId=1145383740954941597 vendor=Cisco severity=informational
originator:
  hostId: sensor
  appName: sensorApp
  appInstanceId: 341
time: July 31, 2006 3:19:46 PM UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Request id=2004 version=31
  subsigId: 0
interfaceGroup:
  vlan: 0
participants:
  attacker:
    addr: 10.10.99.26 locality=OUT
  target:
    addr: 10.10.102.1 locality=OUT
summary: 4 final=true initialAlert=1145383740954941574 summaryType=Regular
alertDetails: Regular Summary: 4 events this interval ;
riskRatingValue: 25
interface: ge0_1
protocol: icmp
  
```

Los clientes evitados enumerados en el regulador se pueblan a este punto del tiempo con el IP y la dirección MAC del host.

The screenshot shows the 'Security' section of the Cisco Systems interface. The 'CIDS Shun List' is displayed with a 'Re-sync' button. Below the button is a table with the following data:

IP Address	Last MAC Address	Expire	Sensor IP / Index
10.10.99.26	00:40:96:ad:0d:1b	27	172.16.26.10 / 2

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

The screenshot shows the 'Monitor' section of the Cisco Systems interface. The 'Excluded Clients' page is displayed with a search bar and a 'Search' button. Below the search bar is a table with the following data:

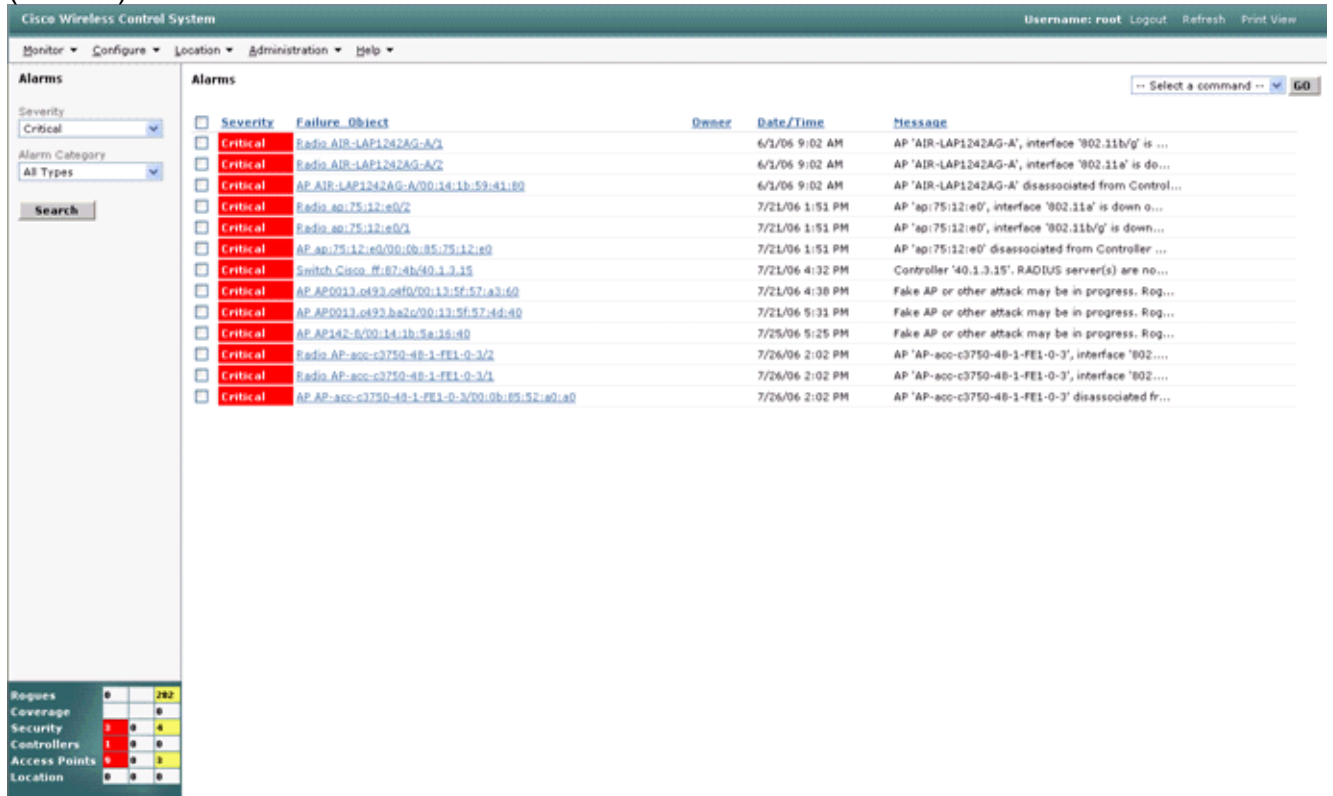
Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Exclusion Reason	Port	
00:40:96:ad:0d:1b	AP0014.6940.81ce	00:14:1b:5a:16:40	IPS	802.11a	UnknownEnum:5	29	Detail Link Text Disable Remove

Vigile los eventos en el WCS

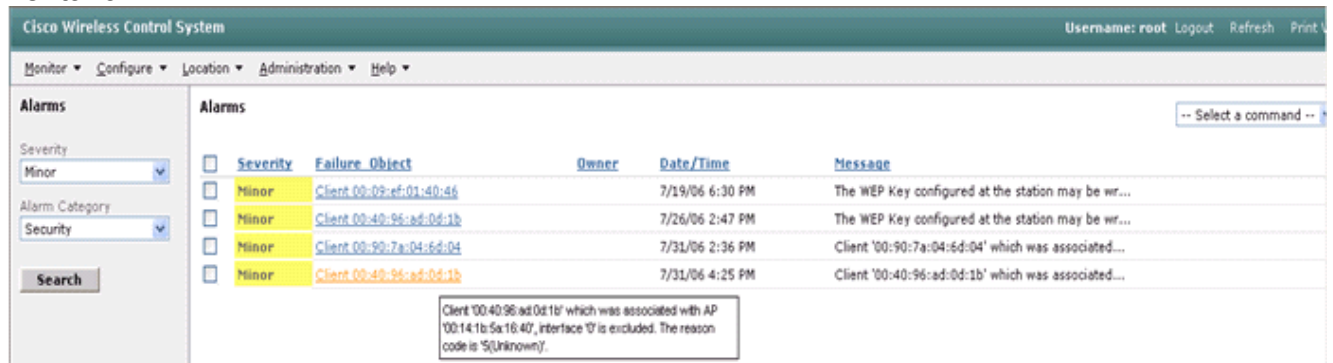
Eventos de seguridad que accionan un bloque dentro de la causa AIP-SSM el regulador para agregar el direccionamiento del delincuente a la lista de la exclusión del cliente. Un evento también se genera dentro del WCS.

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#
```

Verifique

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

Troubleshooting

No hay actualmente información disponible específica del troubleshooting para esta configuración.

Información Relacionada

- [Instalando y con al administrador de dispositivos 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 los interfaces](#)
- [Guía de configuración WLC 4.0](#)
- [Soporte técnico inalámbrico](#)
- [FAQ inalámbrico del regulador LAN \(WLC\)](#)
- [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](#)