Guía de integración de IPS y controlador de LAN inalámbrica

Contenido

Introducción **Prerequisites** Requirements Componentes Utilizados **Convenciones** Descripción general de Cisco IDS Cisco IDS y WLC - Descripción general de la integración Reducción de IDS Diseño de arquitectura de red Configuración del sensor IDS de Cisco Configurar la WLC Ejemplo de configuración del sensor IDS de Cisco Configure un ASA para IDS Configuración de AIP-SSM para la Inspección del Tráfico Configure un WLC para sondear el AIP-SSM para los blogues de clientes Agregar una firma de blogueo al AIP-SSM Supervisión de eventos y bloqueos con IDM Supervisión de la exclusión de clientes en un controlador inalámbrico Supervisar eventos en WCS Ejemplo de configuración de Cisco ASA Configuración de ejemplo del sensor del sistema de prevención de intrusiones de Cisco Verificación **Troubleshoot** 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. Cisco Unified IDS/IPS adopta un enfoque integral de la seguridad, en el perímetro inalámbrico, en el perímetro de la red por cable, en el perímetro de la WAN y a través del Data Center. Cuando un cliente asociado envía tráfico malintencionado a través de Cisco Unified Wireless Network, un dispositivo IDS con cables de Cisco detecta el ataque y envía solicitudes de rechazo a Cisco Wireless LAN Controllers (WLC), que luego desasocia el dispositivo cliente.

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

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

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

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

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

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

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos mínimos:

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

Componentes Utilizados

WLC de Cisco

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

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

Puntos de acceso

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

Administración

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

Plataformas Cisco Unified IDS/IPS

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

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

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco para obtener más información sobre las</u> <u>convenciones del documento.</u>

Descripción general de Cisco IDS

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

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



La aplicación Sensor (software IPS) consta de:

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

funciones de bloqueo cuando se produce un evento de alerta. ARC crea y aplica listas de control de acceso (ACL) en el dispositivo de red controlado o utiliza el comando **shun** (firewalls).

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

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

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

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

Cisco IDS y WLC - Descripción general de la integración

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

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

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



Reducción de IDS

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

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

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

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

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

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

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

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

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

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

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

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

Diseño de arquitectura de red



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

(Cisco Controller) >show interface summary

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

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

```
cat6506#show run interface gigabit 5/1
Building configuration...
Current configuration : 183 bytes
1
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
1
interface GigabitEthernet5/2
switchport
```

```
switchport trunk encapsulation dotlg
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
1
interface Port-channel99
switchport
switchport trunk encapsulation dotlq
switchport trunk native vlan 99
switchport mode trunk
no ip address
end
```

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

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

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

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

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

cat6506#**show monitor session 5**

Session 5	
Туре	: Local Session
Source Ports	:
Both	: Po99
Destination Ports	: Gi5/3
cat6506#	

Configuración del sensor IDS de Cisco

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

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

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

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

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

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

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

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

192.168.5.2.				
S Cisco IDM 5.0 - 192.168.5.2				1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
File Help				
Configuration Monitoring Dack Porwar	🚯 📍 Rathach Help			Cisco Serrier
Conformation Monitoring Deck Provide Notice Image: Status	Partnerh Partnerh extMonik extMonik extMonik extMonik extMonik implementation parameters for parameters for parameters ostname: jmencor Address: 192.168.5.2 etwork Mask: 255.255.255.0 etwork Mask: 192.168.5.1 IP Timeout 300 Web Server Bettings P P Table TLBRISE. Web server port:	* The sensor.	Remote Access Teletet is not a secure access service and is disable by default. If Enable Telnet	Seconds
		Apply	Reset	
IDM is initialized successfully.				cisco administrator 👔

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

CIRCULAR 1.0 177.166.3.7					
File Help					
Configuration Monitoring Eack Forward	nd Retresh Help				Cisco Sestia
G. Sensor Setup Sensor Setup Sensor Setup Sensor Setup Sensor Setup G. SSH G. SSH	Users Specify the users that have acc	ess to the sensor. The se	nice role is a special role that allows you to bypass the C	LI if needed. Only one service account is allowed.	
10 Certificates	Usema	me	Role	Status	1
Supers .	cisco		Administrator	Active	A00
G. Interface Configuration					Edt
- Dinterfaces					
- Dinterface Pairs					Delete
Traffic Flow Notifications					
E Q Analysis Engine		Add User	X		
- Ovirtual Sensor					
E Q. Signature Definition		Usemame:	controller		
- Signature Variables					
- Signature Configuration		User Role:	Viewer		
- DCustom Signature Wizard			· · · · · · · · · · · · · · · · · · ·		
Q Event Action Rules					
- Devent Variables		Password			
- STarget Value Rating					
Devent Action Overrides		Password:			
Someral Settings					
C G Blocking					
- Dilocking Properties		Confirm Password			
Device Login Profiles Selection Devices					
-SRouter Blocking Device Interfaces					
- Cat 6K Blocking Device Interfaces		OK	Cancel Help		
L-SMaster Blocking Sensor					
EL CLOUD					

6. Habilite las interfaces de supervisión.



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

ventana:

Cisco IDM 5.0 - 192.168.5.2				
File Help				
Configuration Monitoring Dack Forward	and Refresh	e Nob		Cisco Systems
G Q Sensor Setup In Diveback Noteback Question Question Question Question Question Question Question	Virtual Sensor The sensor assign and	or monitors traffic that traverses interfaces or interface pa remove interfaces (or pains). You cannot add a new vit	irs assigned to a virtual sensor. Click Edit to change the properties of the default virtual sensor. You can change the ual sensor or change the virtual sensor name.	description or
- NUsers	Name	Assigned Interfaces (or Interface Pains)	Description	Edit
G. Interface Configuration Sinterfaces Sinterface Pairs Sinterface Pairs Sinterface Pairs Sinterface Pairs Sinterface Pairs	¥\$0	OlgabelEthernet00 OlgabelEthernet01 OlgabelEthernet02 OlgabelEthernet00	default virtual sensor	
G. Analysis Engine C. Analysis Engine C. Michael Carried				

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

rápida.											
A Cisco IDM 5.0 - 192,168.5.2											20
File Help											
Configuration Montoring Dack Form	eard Retres	n Help									Cisco Sesters
Q. Sensor Setup Shietwork Shietwork Shietwork	Signature Select By	Configuration	on tures 💌 Belect Criteria: 🖡	-NA- 💌							_
B Q SSH B Q Certificates	Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity Rating	Type	Engine	Retired	Select All
- Nitime	1330	2	TCP Drop - Urgent Pointer WI	No	Modify Packet I	informatio	100	Default	Normalizer	No	NSCIE Link
() Q Interface Configuration	1330	11	TCP Drop - Timestamp Not A.	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Add
- Ninterfaces	1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Clone
- Ninterface Pairs	1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	
Traffic Flow Notifications	2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Edt
O Q Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	Enable
- DVirtual Sensor	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Disable
D 9 Signature Definition	2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	
- Signature Variables	2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	High	180	Tuned	Atomic IP	No	Actions Restore Defaults
Custom Signature Weard	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	
D Q Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Dente.
- Devent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Activate
- Target Value Rating	2008	0	ICMP Timestamp Reply	No	Produce Alert	informatio.	100	Default	Atomic IP	No	Rates
Sevent Action Filters	2009	0	ICMP Information Request	No	Produce Alert	Informatio	100	Default	Adormic IP	No	

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



Configurar la WLC

Complete estos pasos para configurar el WLC:

- 1. Una vez que el dispositivo IPS esté configurado y listo para ser agregado en el controlador, elija **Security > CIDS > Sensors > New**.
- Agregue la dirección IP, el número de puerto TCP, el nombre de usuario y la contraseña que creó anteriormente.Para obtener la huella dactilar del sensor IPS, ejecute este comando en el sensor IPS y agregue la huella digital SHA1 en el WLC (sin los dos puntos). Esto se utiliza para asegurar la comunicación de sondeo de controlador a IDS. sensor#show tls fingerprint MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19 SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42

Cases Systems	and the second second	and the second states	Surd and	in the second	And the second second	Save Co	nfiguration	Ping	Logout Refresh
March The Part of the	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		a she san and
Security	CIDS Sensor Add						< Back		Apply
General RADIUS Authentication RADIUS Accounting	Index	11							
Local Net Users MAC Filtering	Server Address	192.168.5.2							
Disabled Clients User Login Policies AP Policies	Port	443							
Access Control Lists	Username	controller							
Network Access Control	Password	•••••							
IPSec Certificates CA Certificate ID Certificate	Confirm Password								
Web Auth Certificate	Query Interval	15 sec	onds						
Policies Trusted AP Policies Rogue Policies	State	R							
Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection	Fingerprint (SHA1 hash)	1662E996362A9A	1EF08899A7C	1645F5C856A	8842 40 he	(chars			
Web Login Page									
CIDS Sensors Shunned Clients									

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

VVLC.								
Conce Statute								Ping Logout R
A.A. Same	MONITOR WLA	ANS CONTROLLER	R WIRELESS	SECURITY	MANAGEMENT COMM	MNDS HELP		
Security	CIDS Sensors L	ist						New
AAA	Index	Server Address	Port	State	Query Interval	Last Query (count)		
Centeral RADIUS Authentication RADIUS Accounting Local Net Users MAC Fibering Disabled Clients User Login Policies AP Policies	1	192.160.5.2	443	Enabled	15	Success (6083)	Ostail Esmore	
Access Control Lists								
Network Access Control								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trutbed AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authonication Nanagement Prame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

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

Conce Deserves									Save Config	puration Ping	Logout Refre
A.A.	MONITOR WLANS CO	ONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP					
WLANS	WLANs > Edit									< Back	Apply
WLANS	WLAN ID	1									
AP Groups VLAN	WLAN SSID	1PS									
	General Policies						Security Policies				
	Radio Policy	All 👻					IPv6 Enable				
	Admin Status	💽 Enabled									
	Session Timeout (secs)	1800					Layer 2 Security	WPA1+WPA2	~		
	Quality of Service (QoS)	Silver (best effort) 💌						HAC hitering			
	WMM Policy	Disabled 🛩					Layer 3 Security	None	¥		
	7920 Phone Support Client CAC Limit CAC Limit							Web Policy *			
	Broadcast SSID	🛃 Enabled									
	Allow AAA Override	Enabled									
	External Policy Validation	n 🔲 Enabled					 Web Policy cannot be and L2TP. 	used in combination	with IPsec		
	Client Exclusion	Enabled ** 600 Timeout	Value (secs)				** When client exclusion zero means infinity(will	n is enabled, a time: require administrativ	ut value of re override to		
	DHCP Server	C Override					reset excluded clients)				
	DHCP Addr. Assignment	Required									
	Interface Name	management 🛩									
	MFP Version Required	1									
	MFP Signature Generation										
	H-REAP Local Switching										
	* H-REAP Local Switching	g not supported with IPSEC,	L2TP, PPTP, C	RANITE and FORTI	RESS authentical	ions.					
	CISCO Client Extension (CCX)										
	Version IE	Enabled									
	Aironet IE	•									
	Gratuitous Probe Response										
	Radius Servers										
		Authentication Servers	Accounting 5	lervers							
	Server 1	IP:10.1.1.12, Port:1812	none 👻								

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

host.	
Cisco IDM 5.0 - 192.168.5.2	
File Help	
Configuration Monitoring Back Forward Refresh	₹ Help
Deried Attackers Dictive Host Blocks Dictive Host Blocks Dictive Blocks Diction Blocks	Active Host Blocks Specify the address to block and the duration for that block.
Support Information Statistics System Information	Source IP Destination IP Destination Port Protocol Minutes Remaining Timeout (minutes) VLAN Connection Block Enable 10.10.99.21 10.10.99.1 0 1 10 10 0 failse

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

A. A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shun List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users	Re-sync 1P Address La 10.10.99.21 00	st MAC Address 40:96:ad:0d:1b	Expire 326979296	Senso 192.10	or IP / Index 60.5.2 / 1		
MAC Eiltering Disabled Clients User Login Policies AP Policies							
Access Control Lists							
Network Access Control							
IPSec Certificates CA Certificate ID Certificate							
Web Auth Certificate							
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection							
Web Login Page							
CIDS Sensors Shunned Clients							

usuario se agrega a la lista de exclusión de

cliente.

A. A.	MONETOR WLA	NIS CONTROLLER	WIRELESS SEC	URITY MANAGEMENT	COMMANDS HELP		
Monitor	Excluded Client	s					
Summary	Search by MAC	address	Search	h			
Statistics Controller	Client MAC Add	r AP Name	AP NAC Adde	WLAN Type	Exclusion Reason	Port	
Wireless	00:40:95:ad:0d:1	15 AP1242-2	00:14:15:59:3e:10	IPS 802.1	1b UnknownEnum:5	29	Detail LinkTest Disable Remove

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

	And Second	MON	ITOR WLAN	S CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
	Management	32	14:41:00 2006	Rogue AP : 00:15: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
	Summary	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
	General SNMP V3 Users	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)
	Communities Trap Receivers Trap Controls	35	Tue Apr 11 14:39:44 2006	Regue : 00:0b:85:54:de:Se removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
rechazo.	Trap Logs	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 /o1

También se genera un registro de mensajes para el



evento.

Alguno

I and a set

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

	Scan Options		0	Scan
IP Range C IP List	Oomain Act	ive Directory	C WMI API	
Single Host C Neighborhood IP Address:	Vin32 OS Version	Users	Patch Level	Exit
10.1.1.12	Null IPC\$ Sessions	Services	MAC Address	Clear
	VetBIOS Shares	Disks	C Sessions	Save
	Date and Time	☐ Groups	Event Log	5410
	Ping Host(s)	E RPC Bindings	Errors	Help
	Traceroute Host			
ieneral Options				
		TCP Ports	ican Range: 1	1024
Timeout for TCP/UDP/ICMP/SNMP	5		Can Bannes 1	1024
	12	- ODP Port	rean Kange.	11
Retries: 3 Max Conne	octions: 1024	SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne	ections: 1024	SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10:1:1:12 NAC-ACS	ections: 1024	C SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10:1:1:12 NAC-ACS Semputername: WORKGROUP/NAC-	ACS	C SNMP Co	mmunity String: P	ublic .
Retries: 3 Max Conne Address: 10:1:1:12 NAC-ACS omputername: WORKGROUP\NAC-A D: S-1-S-21-790525478-15804366 AC Addresses	ACS 67-1343024091	SNMP Co	mmunity String: P	ublic _
Retries: 3 Max Conne Address: 10:1:1:12 NAC-ACS computername: WORKGROUP\NAC-J D: S-1-5-21-790525478-15804366 AC Addresses: 0009668d51c2	ACS 67-1343024091	SNMP Co	mmunity String: P	ublic 🔺
Retries: 3 Max Conne Address: 10.1.1.12 NAC-ACS omputername: WORKGROUP/NAC-J D: S-1-5-21-790525478-15804366 AC Addresses: 0009668d51c2 atch Level:	ACS 67-1343024091	C SNMP Co	mmunity String: P	ublic .
Retries: 3 Max Conne Address: 10:1:1:1 NAC-ACS omputername: WORKGROUP\NAC DD: S-1-S-21-790525478-15804366 AC Addresses: 0009668d51c2 tch Level: Operating System: 5.0	ACS 67-1343024091	SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10:11:12 NAC-ACS proputername: WORKGROUPNAC D: S-1-S-21-790525478-15804366 AC Addresses: 0009668d51c2 tch Level: Operating System: 5.0 Role: NT Member Server	ACS 67-1343024091	SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10.1.1.12 NAC-ACS computername: WORKGROUPNAC D: S-1-S-21-790525478-15804366 AC Addresses: 00096b8d51c2 tch Level: Operating System: 5.0 Role: NT Workstation	ACS 67-1343024091	SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10:1:1:12 NAC-ACS emputername: WORKGROUP\NAC-/ D: S-1-S-21-790525478-15804366 AC Addresses: 0009668d51c2 tch Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Workstat	ACS 67-1343024091	SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10:1:1:1: NAC-ACS omputername: WORKGROUP\NAC DD: S-1-S-21-790525478-15804366 AC Addresses: 0009668d51c2 tch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Workstat Role: LAN Manager Server Pole: LAN Manager Server Pole: LAN Manager Server	ACS 67-1343024091	SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10:1:1:1: NAC-ACS computername: WORKGROUPNAC ID: S-1-5-21-790525478-15804366 AC Addresses: 00096b8d51c2 itch Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server	ACS 67-1343024091	C SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10.1.1.12 NAC-ACS computername: WORKGROUPNAC (D: S-1-5-21-790525478-15804366 AC Addresses: 00096b8d51c2 itch Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4	ACS 67-1343024091	C SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10:1:1:12 NHC-ACS amputername: WORKGROUPNAC-/ D: 5-1-5-21-790525478-15804366 AC Addresses: 0009668051c2 tch Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Workstat Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hol	ACS 67-1343024091 ion	C SNMP Co	mmunity String: P	ubiic
Retries: 3 Max Conne Address: 10:11:12 NAC-ACS omputername: WORKGROUP\NAC D: S-1-S-21-790525478-15804366 AC Addresses: 0009668d51c2 ttch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Workstat Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hoi KB823182 Windows 2000 Hoi	tions: 1024	C SNMP Co	mmunity String: P	ubiic
Retries: 3 Max Conne Address: 10:1:1:1: NAC-ACS omputername: WORKGROUPNAC D: S-1-S-21-790525478-15804366 AC Addresses: 00096b8d51c2 tch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hot KB823559 Windows 2000 Hot KB823529 Windows 2000 Hot	tions: 1024	C SNMP Co	mmunity String: P	ubiic
Retries: 3 Max Conne Address: 10.11.12 NAC-ACS computername: WORKGROUPNAC-, D: S-1-S-21-790525478-15804366 AC Addresses: 00096b8d51c2 tch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hot KB823182 Windows 2000 Hot KB823559 Windows 2000 Hot KB823559 Windows 2000 Hot	tions: 1024	I SNMP Co	mmunity String: P	ublic
Retries: 3 Max Conne Address: 10:1:1:12 NHC-ACS omputername: WORKGROUPNAC-, ID: S-1-S-21-790525478-15804366 AC Addresses: 00096b8d51c2 stch Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Workstat Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hot KB823182 Windows 2000 Hot KB824105 Windows 2000 Hot KB824105 Windows 2000 Hot	tions: 1024 ACS 67-1343024091 ion fix - KB329115 fix - KB823182 fix - KB823182 fix - KB823182 fix - KB824105 fix - KB824151	C SNMP Co	mmunity String: P	ubiic
Retries: 3 Max Conne Address: 10:1:1:1: NHC-ACS computername: WORKGROUP\NAC ID: S-1-S-21-790525478-15804366. AC Addresses: 000966bd51c2 itch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Workstat Role: LAN Manager Server Role: Service Pack 4 KB329115 Windows 2000 Hoi KB823559 Windows 2000 Hoi KB824151 Windows 2000 Hoi KB824151 Windows 2000 Hoi KB824151 Windows 2000 Hoi	tions: 1024 ACS 67-1343024091 fix - KB329115 fix - KB823182 fix - KB823182 fix - KB823559 fix - KB824105 fix - KB824105 fix - KB824151 fix - KB825119	C SNMP Co	mmunity String: P	ubiic
Retries: 3 Max Conne Address: 10:1:1:12 NHC-ACS computername: WORKGROUPVNAC ID: S-1-S-21-790525478-15804366 AC Addresses: 00096b8d51c2 ttch Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Server Role: Windows 2000 Hot KB823519 Windows 2000 Hot KB825119 Windows 2000 Hot KB825119 Windows 2000 Hot KB825122 Windows 2000 Hot KB825122 Windows 2000 Hot KB825122 Windows 2000 Hot	tions: 1024 ACS 67-1343024091 ion tix - KB329115 tix - KB823182 tix - KB823182 tix - KB823182 tix - KB823182 tix - KB824105 tix - KB824151 tix - KB824151 tix - KB824151 tix - KB826232	C SNMP Co	mmunity String: P	ubiic
Retries: 3 Max Conne Address: 10.11.12 NAC-ACS computername: WORKGROUPNAC (D: S-1-5-21-790525478-15804366 AC Addresses: 00096b8d51c2 itch Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hot KB823182 Windows 2000 Hot KB823191 Windows 2000 Hot KB824105 Windows 2000 Hot KB824105 Windows 2000 Hot KB824151 Windows 2000 Hot KB824151 Windows 2000 Hot KB824151 Windows 2000 Hot KB828035 Windows 2000 Hot KB828035 Windows 2000 Hot KB828035 Windows 2000 Hot	tions: 1024 ACS 67-1343024091 fix - KB329115 fix - KB329115 fix - KB329182 fix - KB329182 fix - KB324105 fix - KB324105 fix - KB324151 fix - KB324151 fix - KB326232 fix - KB326035	C SNMP Co	mmunity String: P	ubiic

monitorea.

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

Denied Attackers Denied Attackers Dative Host Blocks Drietwork Blocks Die Logging	Dack Forward R	terirech Help P	vents u can display the events in t event type and/or time, see	he local Event Blore. Dy default all events are displayed. To file ct the appropriate check boxes.	,	
Cupperl Information			how alert events: P In how arour events: P W	formational D Low D Medium D High		
Ciagnostics Report	G. Local Theorem					
Soystem Information						
	# Type	Sensor UTC Ti	Event ID	Events	Sig ID 📩	
	17 alerthigh:100	April 11, 200	1144083216861913654	ICMP Echo Reply	2000	
	16 alerthigh:100	April 11, 200	1144003216861913652	ICMP Echo Request	2004	
	19 alertiow 32	April 11, 200	1144003216861913656	SMB: ADMINE Hidden Share Access Atlempt	3320	
	18 alertinformati	April 11, 200	1144003216861913655	SMB. Windows Share Enumeration	3322	
	20 alertinformati	April 11, 200	1144003216861913660	SMB: Windows Share Enumeration	3322	
	21 emprembr	April 11, 200	1144003216061913665	Unable to execute a host block timeout (10.10.99.2) because blocking is disabled		
	22 alert informati	April 11, 200	1144083216861913696	TCP SYN Host Sweep	3030	
	23 alertinformati	April 11, 200	1144083216661913706	TCP SYN Host Sweep	3030	
	25 alerthigh:100	April 11, 200	1144083216661913712	ICMP Echo Reply	2000	
	26 empriempr	April 11, 200	1144003216061913714	Unable to execute a host block (10.10.99.22) because blocking is disabled		
	24 alerthigh:100	April 11, 200	1144083216861913710	ICMP Echo Request	2004	
	27 alert medium.	April 11, 200	1144003216061913715	IOS UDP Bomb	4600	
	29 aletmedium	April 11, 200	1144083216861913717	Back Online Ping	4060	
	30 aletmedium	April 11, 200	1144083216861913718	IOS UDP Bomb	4600	
	31 alert medium:	April 11, 200	1144003216061913719	Back Orifice Ping	4060	
	32 alertmedium:	April 11, 200	1144083216861913720	IOS UDP Bomb	4600 .	Refesh

Ejemplo de configuración del sensor IDS de Cisco

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

sensor#**show config**

```
! ------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0/8
access-list 40.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------
service notification
exit
! ------
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
exit
signatures 2001 0
alert-severity high
status
enabled true
exit
```

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

Configure un ASA para IDS

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

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



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

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



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

43A.															_	
te Roles C	Search Options	Tools Wizard	is Help													.
Since 1	Configuration	Monitoring	O .	Orward	Search	Retresh	Save	2							Crace St	-
	Contracto • <u>+</u> ¥	n - Inderfaces I IIII ² I III I A (6 4												
Security Policy		Interface	Name	Enabled	Security Level	IP Address	Su	/briet Mask	Management	MTU		Descriptio	'n		Add	
als.	Cherned	0/0	outside	Yes	9	10.10.102.2	255.3	265.265.0	No	1500	1				Edit	
NAT	Ehernes	0/1	knolde	Yes	1001	172.16.26.2	255.2	255.255.0	140	1500					: Delet	
<u> </u>	Enemed	0/2		No					No							
- Ch	Manager	mentoro	manage.	Ves	100	192.160.1.1	255.3	255 255 0	Yes	1500						
in the second																
Routing																
Global Objects																
Properties																
	Enabl	e traffic between t	wo or more in	iterfacës w	hich are co	infigured with s	iame sei	curity levels								
									Alsty		Reset					
												-admin> N	uns 💕	1 1 1 10 7/	27/06 5 07 52 Pa	UT

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

📫 Cisco ASDM 1	5.1 for ASA - 172,16.2	26.2	
File Rules Se	arch Options Tools	Wizards Help	fores foresas
Home C	configuration Monitorin	ng Back Forward Search Refresh Seve Hep	
-	Configuration + Security	y Policy + Senice Policy Rules	
bierfaces	• 👷 🖗 🖬 📋	3 時 8 影 8 (9)	
8	Access Rules	AAA Rules Pilter Rules Policy Rules	
Security Policy	Show Rules for Interf	tace: All Interfaces Show All	
24		Traffic Classification Rule Actions Description	Add
NAT	E interface: inside, i	Enaded Match Source Lestination Service Inne Hange Policy Inside policy DO-Inside-policy	Edt
SK VEN	inside-class	Db @ any @ any ★ any traffic U\$ los promiscuous, permit traffic	Delete
<u>a</u>			
CSD Manager			
PS			
Routing			
A Constants			
Properties			
	De Match	🚯 Do not match 🕫 Show Summary 🔿 S	Show Detail
		Apply Reset Advanced	
	,		131/06 3:02:47 PM UTC

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

Add Service Policy F	Rule Wizard - Service Policy	×
Adding a new service p	olicy rule requires three steps:	
Step 1: Configure a se	rvice policy.	
Step 2: Configure the t	raffic classification criteria for the service policy rule.	
Step 3: Configure actio	ons on the traffic classified by the service policy rule.	
Create a service polic	cy and apply to:	
Interface:	inside - (create new service policy)	
Policy Name:	inside-policy	
Description:	DS-inside-policy	
C Global - applies t	to all interfaces	
Policy Name:	global-policy	
Description:		
	< Back Next > Cancel	Help

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

🗲 Add Service Policy Rule Wiz	ard - Traffic Classificatio	n Criteria			×
Create a new traffic class:	inside class				
ve create a new trainc class.					
Description (optional):					
Traffic match criteria					
🔲 Default Inspection T	raffic				
🔲 Source and Destina	tion IP Address (uses ACL)				
🗖 Tunnel Group					
TCP or UDP Destina	ation Port				
🗖 RTP Range					
🔲 IP DiffServ CodePoir	nts (DSCP)				
🔲 IP Precedence					
🔽 (Any traffic)					
If traffic does not match a existi Class-default can be used in c C Use class-default as the tra	ng traffic class, then it will ma atch all situation. ffic class.	atch the class-defau	ılt traffic class.		
		-	< Back Next >	Cancel	Help

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

🕵 Add Ser	vice Policy A	Rule Wizard - Rule Ac	tions		
Protocol	Inspection	Intrusion Prevention	Connection Settings	QoS]
IM E	nable IPS for t	his traffic flow			
	Inline Mode				
	In this mode as a result o	, a packet is directed to f IPS operation.	IPS and the packet may t	oe dropped	
Ģ	Promiscous	Mode			
	In this mode be dropped I	, a packet is duplicated by IPS.	for IPS and the original p	acket cannot	
_ If	IPS card fails	, then			
G	Permit traffic				
0	Close traffic				
				< Back Finish	Cancel Help

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

🖆 Cinco ASDM	5.1 for ASA - 172,16.3	26.2							- I ×
File Rules Se	sarch Options Tools	Wittands Help							
- Hove	Configuration Monitoria	ng Back Forward S	anch Refresh	🗐 ? Save Help				51	te serras
	Configuration + Baburd	V Folicy - Service Policy Rules							
	 	人生的现在分词							
C.	C Access Rules	C AAA Rules C Filler Rules	G Service Policy Ru	les					
Security Policy	Bhow Rules for Inter	face: All Interfaces 💌 🔠	iow All				-		
14	7	Tofic	Classification			Ru e Actions	D	seristion	Add
NAT	Name	Enalyed Match Source	Destination	Service	Tims Ranga				Edit
<u>88</u>	inside-class	De lang	🎱 any	🛪 any traffic		🗐 jos promiscuous, permit traffic	DS HSRD PORY		Delete
VPN									
CSD Marcader									
1									
190									
noting									
80									
Giolad Objects									
5.									
Properties									
	1								
	Den Walch	and match						@ Show Summary C. Show Detail	
		Apply	Reset	A16993	d .				
Configuration sh	anges saved successful	¥					sadmine (NA (15)	a 713108 2:54	47 PM UTC

Configuración de AIP-SSM para la Inspección del Tráfico

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

1. Inicie sesión en AIP-SSM con IDM.

Cisco IDM 5.0 - 172.16.26.10					e 🛯
File Help					
				Cisco Si	TETERS
Configuration Montoring Back Forwa	and Retresh He	•			\mathbf{A}
Configuration Montening Disk Form Configuration Status Disk Form Configuration Mitoweal Hosts Disk Form Configuration National Status Disk Form Configuration National Status Disk Form Configuration National Status Disk Status Configuration National Status Disk Status Configuration National Status Disk Status Disk Configuration National Status Disk Disk	vid Retresh He Network Specify the network Hostname: IP Address: Network Mask Default Route: FTP Timeout Vieb Server Setti IP Enable TLSISS Web server port.	ind communication parameters for the sensor. #ensor 172:16:26:10 1255:255:255:0 172:16:26:1 100 98	Remote Access Telnet is not a secure access service and is disabled by default. ✓ Enable Telnet	seconds	
IDM is initialized successfully.				cisco administrator	1 16

2. Agregue un usuario con al menos privilegios de

visor.



3. Habilite la

interfaz.

File Help Configuration Monitoring Configuration Monitoring Configuration Monitoring Retiresh Help Interfaces Interfaces Interfaces Interfaces Interfaces Interfaces Interfaces In	W(1)
Configuration Monitoring Back Forward Retresh Hop	STSTERS (1)
Configuration Monitoring Back Forward Retresh Help	w(1)
D No Sensor Detup	w(1)
- Diversion - Dive	w(s)
Assessing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enabledisable the available sensing interfaces by selecting the n and clinical finable finable or finable.	
O Q SSH And Clocking Endow of Unsace.	
er s central en la central de	the second
-Supers Interface Name Enabled Media Type Duplex Speed Rearbington Description	SCI ALI
Quinterface Configuration Quinterfacement/0 Vies Reconcision Auto Auto	dt
Perpass [1]	able
(b) Q. Analysis Engine Dr.	able
- Nvhuli Sensor	
- "polosoal vanasees	
- Dignature Variables	
- Nignature Configuration	
- Ducustom Signature Weated	
D Q Vent Action Rules	
- NEvent Variables	
- Straget value Raing	
Packweit Arbon Overnoes Second Arbon Olivers	
- Deneral Settings	
D Q Blocking	
Wellocking Properties Some local particular	
Polymore Logier roles Selection Devices	
- NRouter Blocking Device Interfaces	
- SCat K Bioching Device Interfaces	
- "Dwtaster slocking tiensor 15 Q. co.min	
- Doeneral Configuration	
Traps Configuration	
Decade Decade	
Providence Constants	
- Notrudown Sensor	
- Dubdate Sensor	
- wucening	
Apply Reset	
IDM is initialized successfully. [cisco administrator	1 10

4. Verifique la configuración del sensor virtual.



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

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

- 1. Elija Security > CIDS > Sensors > New en el WLC.
- 2. Agregue la dirección IP, el número de puerto TCP, el nombre de usuario y la contraseña que creó en la sección anterior.
- 3. Para obtener la huella dactilar del Sensor, ejecute este comando en el Sensor y agregue la huella digital SHA1 en el WLC (sin los dos puntos). Esto se utiliza para asegurar la comunicación de sondeo de controlador a IDS. sensor#show tls fingerprint MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E

SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55

Conce Services	MONITOR				GEOLIDITY	MANAGEMENT	COMMANDS	
Security	CIDS Sene	or Edit	CONTROLLER	WINELESS	SECONATI	PRODUCTION	0000000	HEEP
AAA General RADIUS Authentication	Index		2					
RADIUS Accounting Local Net Users MAC Filtering	Server Ad	Idress	172.16.26.10					
Disabled Clients User Login Policies	Port		443					
Access Control Lists	Usernam	0	controller					
IPSec Certificates CA Certificate ID Certificate	Password		•••••					
Web Auth Certificate	State							
Wireless Protection Policies	Query Int	erval	10 sec	conds				
Rogue Policies	Fingerprin	nt	90C996984EFA74	470528092888	C483C458487	6C55 40 her	k chars	
Custom Signatures	(SHA1 ha	sh)	(hash key is alre	ady set)				
Signature Events Summary Client Exclusion Policies AP Authentication / MPP Management Frame Protection	Last Quer (count)	Y	Success (1400)					
Web Login Page								
CIDS Sensors Shunned Clients								

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

WLC.								
Circo Station	MONITOR W	LANS CONTROLLE	R WIRELESS	SECURITY N	AANAGEMENT COMM	ANDS HELP		
Security	CIDS Sensors	List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users	Index 1 2	Server Address 192.168.5.2 172.16.26.10	443 443	State Enabled Enabled	Query Interval 15 10	Last Query (count) Unauthorized (1) Success (1444)	Detail Detail	Remove
MAC Filtering Disabled Clients User Login Policies AP Policies								
Access Control Lists								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

Agregar una firma de bloqueo al AIP-SSM

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

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

rápida.											
Cisco IDM 5.0 - 192,168.5.2											E 8 🗙
File Help											
Configuration Monitoring Eack Forward	Retret	9 sh Help									Cisco Sestions
⊕ Q, Sensor Setup	Signature	e Configurati	07								
- Network	Select B	All Sinna	Arres	A10. 1							
- SNAllowed Hosts	General D	. baraka	The second secon	1							
© Q Cesticates	Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity	Type	Engine	Retired	Select All
- STime	4.000		TOD Date: Upstel Databallit	No.	Martin Cashada	in the second second	namy	Curley R	No. of Concession, Name	No.	NSDB Link
L-SQUsers	1330	1	TCP Drop - Orgent Pointer WL	140	Modity Packet I	intormatio	100	Detaut	Normalizer	NO	
E Q Interface Configuration	1330	11	TCP Drop - Timestamp Not A.	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	A00
- Winterfaces	1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Clone
- Several - Seve	1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	
Traffic Flow Notifications	2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Edt
D Q Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Enable
- Wirtual Sensor	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	
- Toolobal Variables	2002		MR Deduct	Vac	Produce Alert	Link.	100	Tuned	Atomic 10	Rin	Disable
-Sisnature Variables	2005		Pomp Portunett	145	Produce Poen	righ	100	Toneo	Page 10	140	Actions
Signature Configuration Scustom Signature Withord	2004		ICMP Echo Request	Yes	Produce Alert Request Block	High	100	Tuned	Atomic IP	No	Restore Defaults
Miscellaneous	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Durine 1
Q. Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Univer-
- Sevent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio_	100	Default	Atomic IP	No	Activate
- STarget Value Rating	2008	0	ICMP Timestamp Reply	No	Produce Alert	informatio	100	Default	Atomic IP	No	Retre
- Sevent Action Filters	2009	0	ICMP Information Request	No	Produce Alert	informatio	100	Default	Atomic IP	No	

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

A ron signature				hitektektektektektektek
Name Value				
Signature ID: 2004				
SubSignature ID: 0				
Alert Severity: High	•			
Sig Fidelity Rating: 100				
Promiscuous Deita:				
Sig Description:				
Signature	Name: ICMP Echo Request			
Alert Note:	8			
User Com	nments:			
alart Traits	er [0			
Selection and	× 10			
Release.	181			
Engine: Atomic IP				
Event A	uction: Produce Al Produce Ve Request B Repuest B	tose Alert sck Connector		
	<	>		
Fragme	ent Status: Any	v		
😔 🔳 Specify	Layer 4 Protocol: Yes 💌			
	🖯 🖬 Laya	r 4 Protocol: ICMP. Protocol	-	
		Specify	CMP Sequence: No -	
		🕒 🔳 Specify	CMP Type: Yes 💌	
				Type:
		Specify 1	CMP Code: No	
		Specify	CMP Identifier.	
		Specify	CMP Total Length: No. V	
Parameter uses the Default Value. Clin	ck the icon to edit the value			
Parameter uses a User-Defined Value	a. Click the icon to restore the defau	tvalue.		
	0K	Cancel Help	1	

🤏 Edi	it Signature					×
	Name	Value				<u>-</u>
	Signature ID:	2004				
	SubSignature ID:	0				
	Alert Severity:	Informational 💌				
	Sig Fidelity Rating:	100	_			
	Promiscuous Delta:	0	-			
Θ	Sig Description:					
		Signature Name:	ICMP Echo Request			
		Alert Notes:				
		User Comments:				
		Alert Traits:	0			
		Release:	81			
Θ	Engine:	Atomic IP				
		Event Action:	Request Bi Request Bi Request Si Reset Top	lock Connectior A lock Host nmp Trap Connection		
•		Franment Status	r Dow			<u>*</u>
•	Parameter uses the D Parameter uses a Use	efault Value. Click the ico er-Defined Value. Click th	n to edit the value. e icon to restore the defau	it value.		
			OK Cancel	I Help]	

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

Supervisión de eventos y bloqueos con IDM

Complete estos pasos:

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



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

Ver....

Cisco IDM 5.0 - 172.16.26.10	
File Help	
Configuration Monitoring Back Forward Retresh	📍 Help
Denied Attackers Active Host Blocks Network Blocks Program Support Information Diagnostics Report Statistics Psystem Information	Events You can display the events in the local Event Store. By default all events are displayed. To filter overent type analytic time, select the appropriate check boxes. Show rater events: Show reverts in the local Event Store. By default all events are displayed. To filter over all events: Show reverts: Show reverts: <t< td=""></t<>

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

¶ ₽	ent Viewer					
[t Type	Sensor UTC Time	Event ID	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	
						Refresh
Ľ					Last Updated: 7/	31/06 3:22:39 PM-
			<back nex<="" td=""><td>Close Help</td><td></td><td></td></back>	Close Help		

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

```
Details for 1145383740954941597
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=S1
   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
```

Supervisión de la exclusión de clientes en un controlador inalámbrico

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

Constantino A. A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shu	n List						
AAA General RADIUS Authentication	Re-sync	Ш я ц	st MAC Address	Expire	Sent	sor IP / Index		
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	10.10.99.20	6 00	0:40:96:ad:0d:1b	27	172.	16.26.10 / 2		
Access Control Lists								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MPP Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

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

	MONITOR WLAN	s CONTROLLER	WIRELESS SE	CURITY MAN	AGEMENT C	OMMANDS HELP		
Monitor Summary Statistics Controller Ports Wireless Rogue APs Known Rogue APs Rogue Clents Adhoc Rogues 802.11 Radios 802.11 Radios 802.11 July Radios Clients	Excluded Clients Search by NAC a Client NAC Addr 00:40:96:ad:0d:1b	AP Name AP0014.6940.81c	AP NAC Addr e 00:14:15:5a:16:44	WLAN D IPS	Type 802.11e	Exclusion Reason UnknownEnum:5	Port 29	Detail UnkTest Disable Remove

Supervisar eventos en WCS

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

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

(Buscar).

Cisce Wireless Control S	istem			Username: root Logout Refresh Print View
Monitor • Configure •	ocation - Administration - Help -			
Alarms	Alorms			Select a command 💌 GO
Severity	C formation failure Object	0	Date (Time	
Critical	Conseal Participation Management	Uwner	6/1/06 9:02 AM	AP (AIR-J AP12424/G-8) interface (802 31b/o) in
Alarm Category	Contract Registration Provided All Contract Cont		6/1/06 9:02 AM	AP ALC-API242ACAA, Interface (002.1107g is
All Types 💌	Critical AP AIR-LAR124/24/C-4/00/14/15/59/41/80		6/1/06 9:02 AM	AP 'AIR-LAP12424G-8' disassociated from Control
and the second sec	Critical Radia an 75:12:a0/2		7/21/06 1:51 PM	AP 'ao 75 12 a0', interface '802 11 a' is down o
Search	Critical Radio apr7512:e0/3		7/21/06 1:51 PM	AP 'ap:75:12:e0', interface '802.11b/o' is down
	Critical AP ap://5:12:e0/00:0b:85:75:12:e0		7/21/06 1:51 PM	AP 'ao:75:12:e0' disassociated from Controller
	Critical Switch Cisco #187:45/40.3.3.35		7/21/06 4:32 PM	Controller '40.1.3.15', RADIUS server(s) are no
	Critical AP AP0013.0493.0460/00:13:5f:57:a3:60		7/21/06 4:38 PM	Fake AP or other attack may be in progress. Rog
	Critical AP AP0013.0493.ba20/00:13:5f:57:4d:40		7/21/06 5:31 PM	Fake AP or other attack may be in progress. Rog
	Critical AP.AP142-0/00:14:15:5a:16:40		7/25/06 5:25 PM	Fake AP or other attack may be in progress. Rog
	Critical Radio AP-acc-c3750-48-1-FE1-0-3/2		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3', interface '802
	Critical Radio AP-acc-c3750-48-1-FE1-0-3/1		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3', interface '802
	Critical AP.AP-acc-c0750-40-1-FE1-0-3/00:05:05:52:a0:a0		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3' disassociated fr
Reques 0 202 Coverage 0 Security 0 4 Costrollers 1 0 0 Access Points 0 0				

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

Cisco Wireless Cor	itrol S	ystem							Username: roo	at Logout Re	fresh	Print V
Monitor • Configur	e = j	ocation	• • <u>A</u> dminis	tration • Help •								
Alarms		Alar	ms							Select a	comma	nd
Severity	v		Severity	Failure Object		Owner	Date/Time		Message			
(the second sec			Minor	Client 00:09:ef:01:40	:46		7/19/06 6:30	PM	The WEP Key configured at the station may be wr			
Alarm Category			Minor	Client 00:40:96:ad:00	<u>:1b</u>		7/26/06 2:47	PM	The WEP Key configured at the station may be wr			
accord			Minor	Client 00:90:7a:04:60	1:04		7/31/06 2:36	PM	Client '00:90:7a:04:6d:04' which was associated			
Search			Minor	Client 00:40:95:ad:0	11b		7/31/06 4:25	PM	Client '00:40:96:ad:0d:1b' which was associated			
					Client 100:40:96:ad.0d:16/ 100:14:16:56:16:40', interfe code is 'S(Unknown)'.	which was as: ace 10 is exclu	sociated with AP ded. The reason					

Ejemplo de configuración de Cisco ASA

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

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

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

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

```
sensor#show config
! ------
! Version 5.0(2)
! Current configuration last modified Tue Jul 25 12:15:19 2006
! ------
service host
network-settings
host-ip 172.16.26.10/24,172.16.26.1
telnet-option enabled
access-list 10.0.0/8
access-list 40.0.0/8
exit
exit
! ------
service notification
exit
! ------
service signature-definition sig0
signatures 2004 0
engine atomic-ip
event-action produce-alert | request-block-host
exit
status
enabled true
exit.
exit
exit
! ------
service event-action-rules rules0
exit
! ------
service logger
exit.
! ------
service network-access
exit
! ------
service authentication
exit
! _____
service web-server
exit
! ------
service ssh-known-hosts
exit
! ------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/1
exit
```

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

Verificación

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

Troubleshoot

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

Información Relacionada

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