

Cómo verificar las alertas del examen y de la firma del tráfico IPS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Comunicaciones internas, del externo y de Administración](#)

[Verifique el examen del tráfico](#)

[Verifique los fuegos de la firma](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona los pasos para utilizar para verificar la operación de las opciones de un sensor del Sistema de prevención de intrusiones (IPS) y de la prueba de la firma en un entorno de producción.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en estas versiones de software:

- Versión 6.2(x)E4 del sistema de prevención de intrusiones
- Versión 7.0(x)E4 del sistema de prevención de intrusiones
- Versión 7.1(x)E4 del sistema de prevención de intrusiones

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las

convenciones del documento.

Comunicaciones internas, del externo y de Administración

Utilice estos pasos para verificar el acceso y la disposición de la Administración de IPS:

- Acceda a la consola en el IPS. Si esto es un problema del módulo, después ingrese: **sesión 1 de las 5500 y 5585 Series adaptantes del dispositivo de seguridad (ASA), sesión IPS de un 5500x, la sesión del /port del slot del sensor IDS del módulo de servicio** sobre un módulo de red aumentó el módulo (NME), **sessionslot_number** en CatOS, **y procesador 1 del module_number del slot de la sesión** en el IOS para el sistema de la detección de intrusos (IDSM) y los módulos (de segunda generación) IDSM-2.
- Inicie sesión con el nombre de usuario y contraseña que fue configurado en la configuración inicial. El nombre de usuario predeterminado y la contraseña es "Cisco". Refiera a la [guía de la configuración](#) para la versión apropiada para más detalles.
- Si la configuración es ya completa, después proceda a la conectividad del IP de la prueba a la Administración de IPS.
- Ingrese el **comando host de las estadísticas de la demostración**, e intente hacer ping y obtener el acceso del Secure Shell (SSH) al IP Address de la Administración de IPS. Si esto trabaja, después continúe al siguiente paso. Si no, entonces resuelva problemas los problemas de conectividad con la [guía de configuración](#) para la versión apropiada.
- Ingrese el **comando show version**. Verifique la versión de software es actual, eso una licencia está instalada, la versión de firma es la más última, todos los motores son operativos, y ése el certificado del host es válido.
- Si se validan todos los pasos anteriores, después acceda a la dirección de administración del IPS vía el HTTPS y inicie el IDM. Las Javas 6 deben ser instaladas. Si la Java 6 no está disponible, después instale al administrador IPS expreso (IME) de la página web IPS. **Nota:** La Java 7 no se soporta para iniciar al administrador de dispositivo IPS (IDM) o para acceder las opciones IPS en el Administrador de dispositivos de seguridad adaptante (ASDM) ahora.
- Si la Conectividad es acertada, después en el IDM, vaya a la **Administración de la configuración > del sensor > autorizando y ponga al día la licencia del cisco.com**. Incluso si existe una licencia válida, ésta confirma la Conectividad a Internet.
- Si es acertada, después van a la **configuración > a las directivas > la correlación > el examen/la reputación globales** y hacen clic en la **correlación global de la prueba** para asegurarse los trabajos DNS. Para marcar esto, ir a **monitorear > Events** y seleccionar solamente el **cuidado, el error y fatal** y confirmar si las actualizaciones **globales de la correlación** fallan. **Nota:** La correlación global no está disponible en el software IPS anterior que la versión 7.0 IPS.

Verifique el examen del tráfico

Después de que usted verifique las comunicaciones con el IPS, usted puede verificar el examen del tráfico con estos pasos.

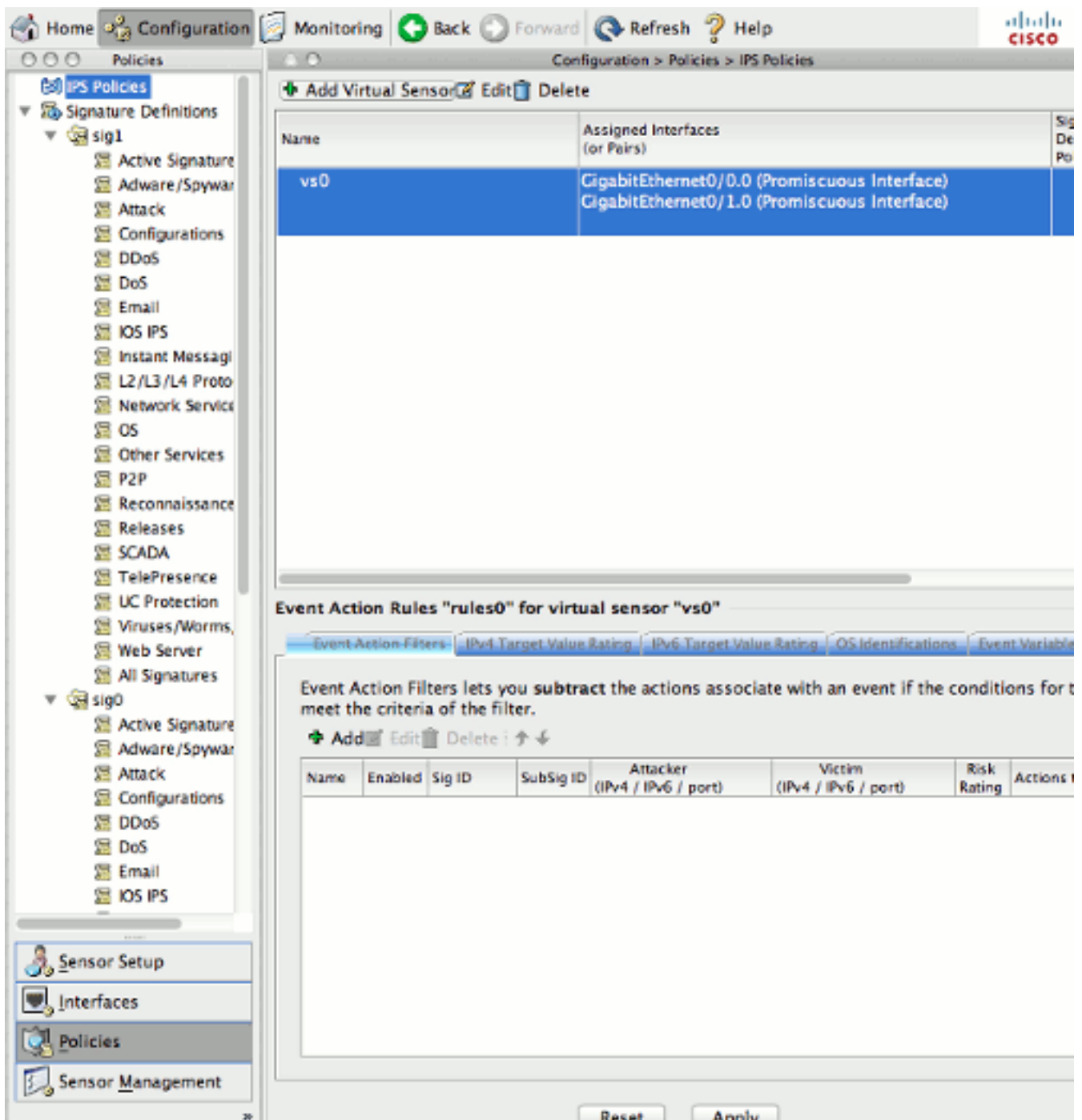
- Verifique que el sensor que detecta el estado de link de la interfaz sea **ascendente** y reciba el tráfico. Inicie sesión a la interfaz del sensor y ingrese estos comandos:

sensor# **show interface** !! In the output, find the applicable section for the sensing interface(s) in !! question and confirm that the Link Status value is "Up". If so, note the !! value shown for the Total Packets Received counter. After a few seconds, !! run the command again and compare the current value to the previous. !! If the value has increased, the sensing interface(s) in-question is Up !! and receiving traffic. Example: sensor# **show interface** MAC statistics from interface GigabitEthernet0/0 Interface function = Sensing interface Link Status = Up Total Packets Received = 100 sensor# **show interface** MAC statistics from interface GigabitEthernet0/0 Interface function = Sensing interface Link Status = Up Total Packets Received = 150 !! If a sensing interface's Link Status value is expected to be "Up", but is !! not, verify that it is properly and physically connected to a switchport or !! other network device. If so, verify that the switchport or other network !! device is configured properly and the remote interface (the switchport or !! NIC on the other network device) is not administratively-disabled !! ("shutdown"). If needed, try to swap cables with another that is known !! to be good. !! If a sensing interface's Total Packets Received counter does not increment, !! check the configuration of the switchport or other network device to which !! the sensing interface is connected. If the sensing interface is supposed to !! be the destination of a SPAN/monitor session, verify the SPAN/monitor !! configuration on the switch the sensing interface is connected.

- Alternativamente en el IDM, verifique todas las interfaces de la supervisión visualizan un valor del link del **estatus directo ascendente del hogar > de la interfaz.**

Interface	Link	Enabled	Speed (Mbps)	Mode	Received Packets	Transmitted Packets
GigabitEthernet0/0	down	Yes	100	unpaired	0	0
GigabitEthernet0/1	up	Yes	100	unpaired	73,403	0
GigabitEthernet0/2	down	Yes	100	unpaired	0	0
GigabitEthernet0/3	down	Yes	100	unpaired	0	0
Management0/0	up	Yes	100	unpaired	5,323	3,401

- Verifique que el sensor del sensor tenga por lo menos una interfaz de detección asignada y examina el tráfico. Inicie sesión al sensor y ingrese este comando. sensor# **show stat virtual** !! In the output, find the List of interfaces monitored by this virtual !! sensor line and confirm that at least one (1) sensing interface(s) is !! listed. Additionally, find the Total packets processed since reset !! line/counter and confirm its value is greater-than (>) zero (0). !! Example: sensor# **show stat virtual** Statistics for Virtual Sensor vs0 List of interfaces monitored by this virtual sensor = GigabitEthernet0/0 General Statistics for this Virtual Sensor Total packets processed since reset = 200 !! If there are no sensing interface(s) listed (or, if additional sensing !! interfaces need to be assigned), login to the sensor using an !! administrative account and issue the following commands !! (**NOTE:** In the example provided, the GigabitEthernet0/0 sensing interface !! is assigned to virtual-sensor vs0. Replace that particular configuration !! line accordingly with the actual sensing interface you wish to assign to !! the virtual-sensor. If you need to assign multiple sensing interfaces, !! repeat that line (one per sensing interface)): sensor# **conf t** sensor(config) # **service analysis-engine** sensor(config-ana) # **virtual-sensor vs0** sensor(config-ana-vir)# **physical-interface GigabitEthernet0/0** sensor(config-ana-vir)# **exit** sensor(config-ana)# **exit** Apply Changes?[yes]: yes !! **NOTE:** The above example assigns a Promiscuous sensing interface to the vs0 !! virtual-sensor. Inline sensing interfaces must first be "paired" together !! and then the logical pair assigned to a virtual-sensor. Details can be !! found in the official product configuration guide's Configuring !! Interfaces section.
- Alternativamente, verifique que las interfaces estén asignadas a vs0 en el IDM bajo la **configuración > las directivas > directivas IPS.**



- Ingrese el SSH al IPS y ingrese el comando del /port del slot de interfaz de la visualización del paquete y verifique el tráfico se ve en la interfaz. **Nota:** La palabra clave de la *expresión* permite que el uso de las expresiones del *tcpdump* para visualizar solamente el tráfico que hace juego la expresión usada. `sensor# packet display gigabitEthernet0/1 expression ip host 198.51.100.1` Warning: This command will cause significant performance degradation `tcpdump: WARNING: ge0_1: no IPv4 address assigned tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes 18:32:24.247864 IP 198.51.100.1.2000 > 192.0.2.1.2000: UDP, length 172 18:32:24.247868 IP 198.51.100.1.2000 > 192.0.2.1.2000: UDP, length 172 18:32:24.257249 IP 198.51.100.1.2000 > 192.0.2.1.16384: UDP, length 172 !! Alternatively, in the case of VLAN tagging: sensor# packet display gigabitEthernet0/1 expression vlan 20 and ip host 192.51.100.1`

Verifique los fuegos de la firma

- Los eventos de la firma se pueden ver en la sección de la supervisión.

Home Configuration Monitoring Back Forward Refresh Help

Sensor Monitoring Monitoring > Sensor Monitoring > Events

Events

- Dynamic Data
 - Anomaly Detection
 - OS Identifications
- Properties
 - Clear Flow States
 - Reset Network Security
- Support Information
 - Diagnostics Report
 - Statistics
 - System Information

You can display the events in the sensor Event Store. To filter on event type and/or time, select the appropriate check boxes.

Show Alert Events

Informational Low Medium High

Min Max

Threat Rating (0-100): -

Show Error Events

Warning

Error

Fatal

Show Attack Response Controller events

Show status events

Select the number of the rows per page:

Show all events currently stored on the sensor

Show past events:

Show events from the following time range

Start Time (UTC)

From: : :

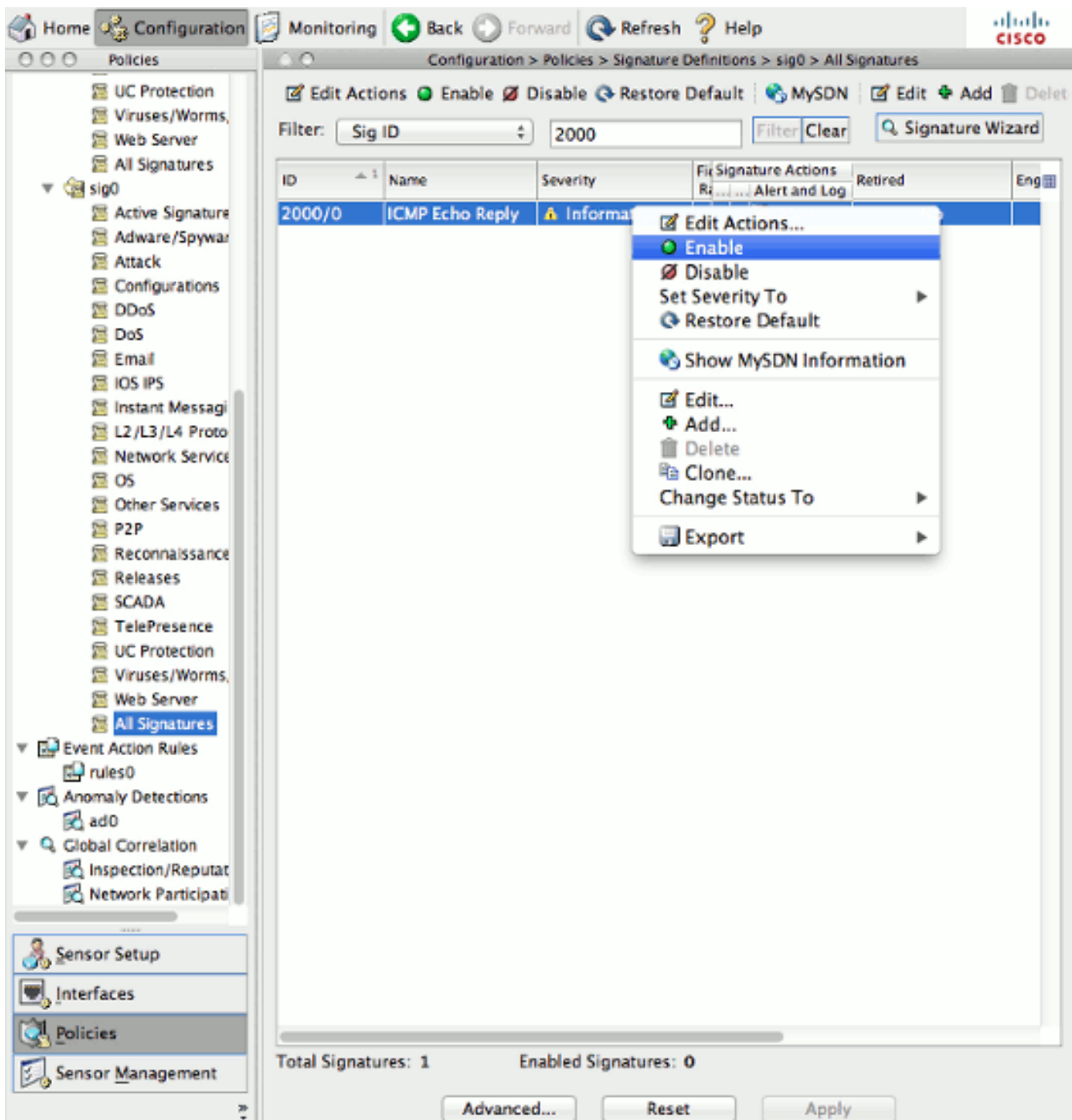
From the oldest event forward

End Time (UTC)

To: : :

To now

- Las firmas se pueden modificar bajo configuración > todas las firmas.



- Firmas 2000/0 y 2004/0 del permiso (respuesta de eco del Protocolo de mensaje de control de Internet (ICMP) y pedido de eco ICMP); inicie un ping a través del sensor, y marque el registro de acontecimientos en la lengüeta de la supervisión. Si se bloquea el ICMP: Para 1107/0, refiera al RFC1918 - *Dirija visto*. Para accionar esta firma, el conjunto **se retira a falso** y al **permiso para verdad** en esta firma y para mirar los IP en los rangos del RFC 1918 accionar las firmas. Estos direccionamientos son 10.0.0.0/8, 172.16.0.0-172.31.255.255, 192.168.0.0/16. Esto no se puede ver en un SSC-5 porque se requiere para que la firma unretired. Para 3409/0, telnet al puerto 80. Con la configuración del servidor Web, el puerto 80 está abierto y el telnet es acertado. Cuando el telnet es acertado, los fuegos del evento en el IPS. Un apretón de manos de tres vías TCP se requiere para que el sensor siga la conexión TCP válida. En el caso del Asymmetric Routing o de una respuesta de una captura del paquete parcial, el tráfico no causa un fuego de la firma.

Después de que la prueba sea completa, restablezca los valores por defecto a cualquier firma modificada:

The screenshot displays the Cisco IPS configuration interface. The left-hand navigation pane shows a tree structure under 'Policies' > 'Signature Definitions' > 'sig0', with 'All Signatures' selected. The main content area shows a table of signatures with the following data:

ID	Name	Enabled	Severity	Fidelity Rating	Signature Actions			Retired
					Deny	Other	Alert and Log	
2000/0	ICMP Echo Reply	<input checked="" type="checkbox"/>	Informational	100			Alert	Yes

At the bottom of the interface, the status bar indicates 'Total Signatures: 1' and 'Enabled Signatures: 1'. There are buttons for 'Advanced...', 'Reset', and 'Apply'.

Información Relacionada

- [Escenarios de configuración de la Administración de IPS en un módulo ips 5500x](#)
- [Guía de configuración CLI del sensor de Cisco Intrusion Prevention System para IPS 7.0](#)
- [Guía de configuración CLI del sensor de Cisco Intrusion Prevention System para IPS 7.1](#)
- [Administrador IPS expreso](#)
- [Secure Shell \(SSH\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)