

Recopilación de estadísticas de rendimiento mediante la opción "Monitor de rendimiento de 1 segundo"

Contenido

[Introducción](#)

[Monitor de rendimiento de 1 segundo](#)

[Activar en la versión 5.4 o posterior](#)

[Activar versiones anteriores a 5.4](#)

[Documentos Relacionados](#)

Introducción

En un dispositivo que ejecute el software Sourcefire, puede configurar los parámetros básicos que supervisan y generan informes sobre su propio rendimiento. La estadística de rendimiento es crítica para resolver problemas relacionados con el rendimiento en un dispositivo que ejecuta Snort. Este documento proporciona los pasos para habilitar esta función mediante FireSIGHT Management Center.

Advertencia: si su red está activa y habilita un rendimiento de 1 segundo en un sistema de producción, puede afectar al rendimiento de la red. Debe activar esto sólo si el Soporte Técnico de Cisco lo solicita con el fin de solucionar problemas.

Nota: La información de este documento se creó a partir de los dispositivos en un entorno de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration.

Monitor de rendimiento de 1 segundo

La función *Monitor de rendimiento de 1 segundo* permite especificar los intervalos en los que el sistema actualiza las estadísticas de rendimiento en sus dispositivos mediante la configuración de lo siguiente:

- Número de segundos
- Número de paquetes analizados

Cuando ha transcurrido el número de segundos especificado desde la última actualización de las estadísticas de rendimiento, el sistema verifica que se haya analizado el número especificado de paquetes. Si es así, el sistema actualiza las estadísticas de rendimiento. Si no es así, el sistema

espera hasta que se haya analizado el número especificado de paquetes.

Activar en la versión 5.4 o posterior

Paso 1: Seleccione **Policies > Access Control**. Aparecerá la página Directiva de control de acceso.

Paso 2: Haga clic en el icono *del lápiz* junto a la política de control de acceso que desea editar.

Paso 3: Seleccione la ficha **Advanced** (Opciones avanzadas). Aparecerá la página de configuración avanzada de la directiva de control de acceso.

Overview Analysis **Policies** Devices Objects AMP

Access Control Intrusion Files Network Discovery SSL

Default Access Control

Enter a description

Rules Targets Security Intelligence HTTP Responses **Advanced**

Paso 4: Haga clic en el icono *del lápiz* junto a **Performance Settings**.

Performance Settings


Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet	5
Performance Statistics - Sample Time (seconds)	300
Regular Expression - Limit	Default
Regular Expression - Recursion Limit	Default
Intrusion Event Logging Limits - Max Events Stored Per Packet	8

Paso 5: Seleccione la ficha **Estadísticas de rendimiento** en la ventana emergente que aparece. Modifique la hora de muestra o el número mínimo de paquetes como se describe anteriormente.

Performance Settings

Pattern Matching Limits **Performance Statistics** Regular Expression Limits Intrusion Event Logging Limits

Sample time (seconds)	300
Minimum number of packets	10000

Troubleshooting Options 

Revert to Defaults OK Cancel

Paso 6: *Opcionalmente*, expanda la sección **Opciones de Troubleshooting** y modifique esas opciones sólo si Cisco TAC se lo solicita.

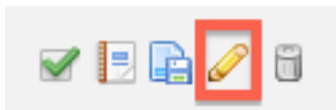
Paso 7: Click OK.

Paso 8: Debe guardar y aplicar la política de control de acceso para que los cambios surtan efecto.

Activar versiones anteriores a 5.4

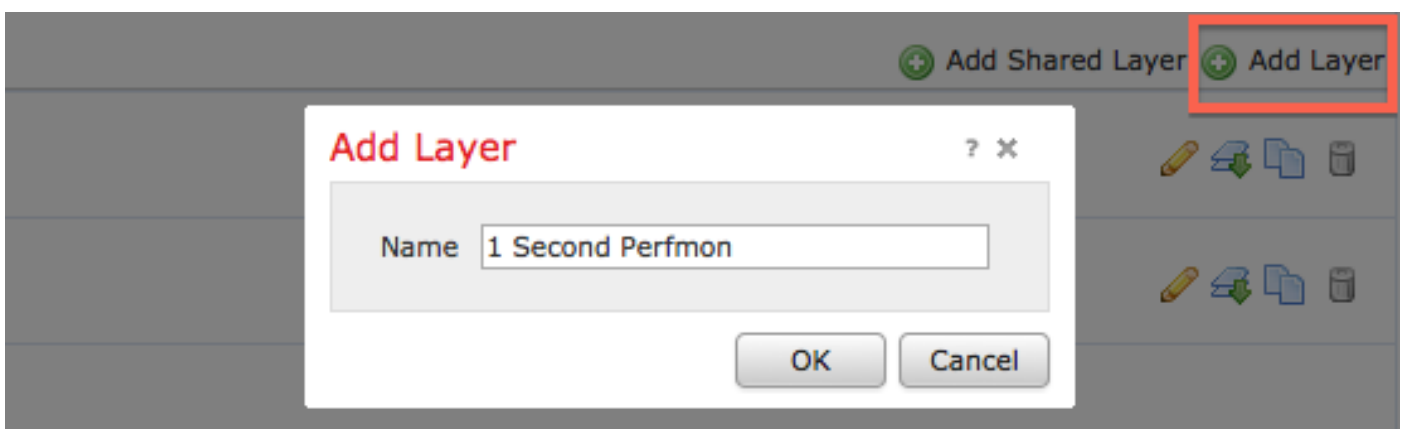
Paso 1: Vaya a la página Política de intrusiones. Inicie sesión en FireSIGHT Management Center. Vaya a **Políticas > Intrusión > Política de intrusiones**.

Paso 2: Edite la política de intrusiones que desee aplicar. Haga clic en el icono *del lápiz* para editar la directiva.

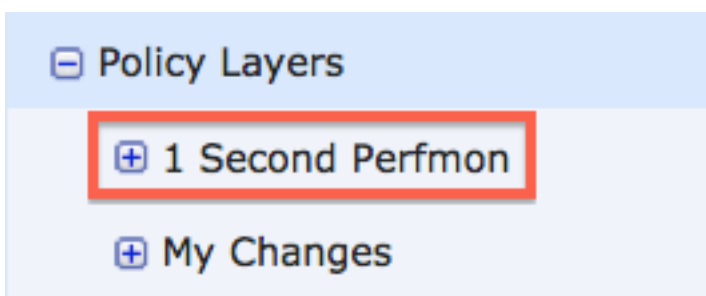


Nota: Debido al diseño de esta configuración avanzada, sólo debe modificar esta configuración dentro de una política de intrusiones que se está utilizando como acción predeterminada de su política de control de acceso.

Paso 3: Agregue una capa de políticas. Haga clic en **Capas de política** y, a continuación, **Agregar capa**. Nombre la capa "*1 Second Perfmon*".









Verifique las **capas de políticas** en el panel izquierdo, y asegúrese de que la nueva capa "*1 Segundo Perfmon*" esté por encima de todas las demás capas.



Paso 4: Habilite la configuración de estadísticas de rendimiento. En **Performance Settings**, seleccione el botón de opción **Enabled** junto a **Performance Statistics Configuration** y haga clic en Edit.

Performance Settings

Event Queue Configuration	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Latency-Based Packet Handling	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Latency-Based Rule Handling	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Performance Statistics Configuration	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Regular Expression Limits	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Rule Processing Configuration	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit

Paso 5: Modifique el tiempo de muestra predeterminado a 1 segundo y el número mínimo de paquetes a 100 paquetes.

Performance Statistics Configuration

Settings

Sample time	<input type="text" value="1"/>	seconds
Minimum number of packets	<input type="text" value="100"/>	

Paso 6: Haga clic en **Información de política** en el panel izquierdo, confirme los cambios y aplique la política actualizada a los dispositivos que desea perfilar.

Policy Information

- Variables
- Rules
- FireSIGHT Recommendations
- Advanced Settings

Paso 7: Revertir la configuración después de recopilar los datos. Para revertir, simplemente elimine la capa de política "1 Second Perfmon".

Precaución: No olvide revertir la configuración. De lo contrario, puede causar problemas de

rendimiento.

Documentos Relacionados

- [Visualización del rendimiento de los eventos de intrusión](#)
- [Generación de Gráficos de Estadísticas de Rendimiento de Eventos de Intrusión](#)