Configure un sistema de FireSIGHT para enviar las alertas a un servidor Syslog externo

Contenido

Introducción

Mientras que un sistema de FireSIGHT proporciona las diversas vistas de los eventos dentro de él es la interfaz Web, usted puede querer configurar la notificación del evento externo para facilitar la supervisión constante de los sistemas críticos. Usted puede configurar un sistema de FireSIGHT para generar las alertas que le notifican vía el correo electrónico, el SNMP trap, o el Syslog cuando uno del siguiente se genera. Este artículo describe cómo configurar un centro de administración de FireSIGHT para enviar las alertas en un servidor Syslog externo.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento en el Syslog y el centro de administración de FireSIGHT. También, el puerto de Syslog (el valor por defecto es 514) se debe permitir en su Firewall.

Componentes Utilizados

La información en este documento se basa en la versión de software 5.2 o más adelante.

> Precaución: La información sobre este documento se crea de un dispositivo en un ambiente de laboratorio específico, y se comienza con una configuración despejada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener

cualquier comando.

Envío de las alertas de la intrusión

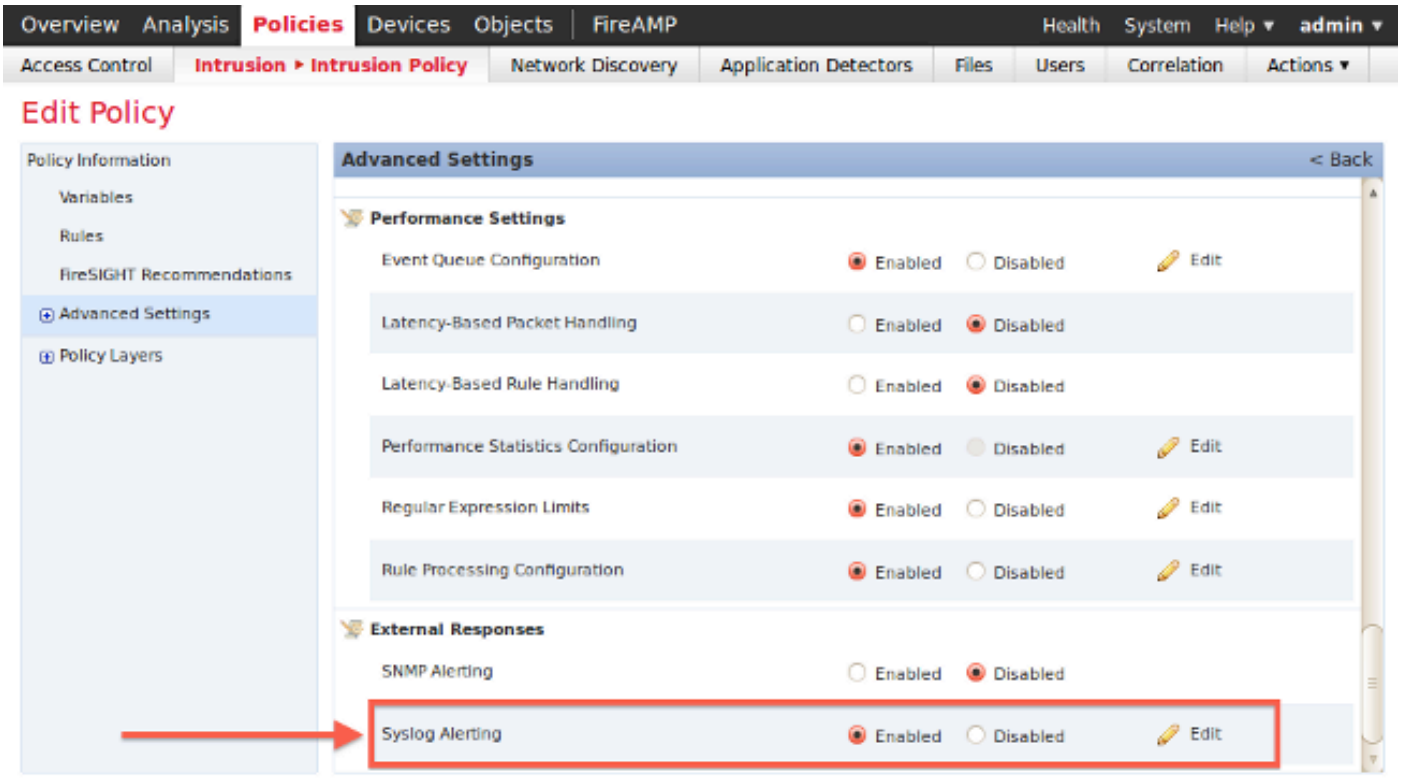
1. Registro en la interfaz del Web User de su centro de administración de FireSIGHT.

2. Navegue a las **directivas** > a la **intrusión** > a la **directiva de la intrusión**.

3. El tecleo **edita** al lado de la directiva que usted quiere aplicarse.

4. Haga clic en las **configuraciones avanzadas**.

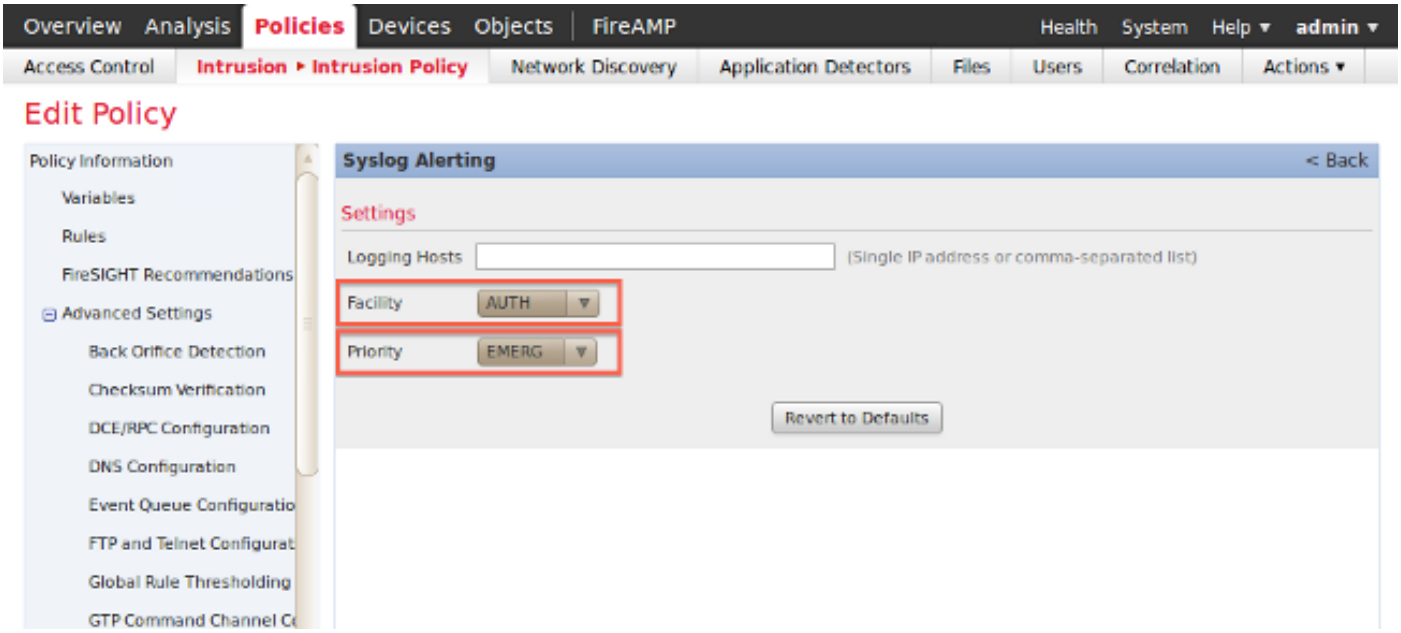
5. Localice el **Syslog que alerta** en la lista y fíjelo a **habilitado**.



6. El tecleo **edita** al lado de la derecha de **alertar del Syslog**.

7. Teclee la dirección IP de su servidor de Syslog en el campo de los **host de registro**.

8. Elija un **recurso** y una **gravedad** apropiados del menú desplegable. Éstos se pueden dejar en los valores predeterminados a menos que configuren a un servidor de Syslog para validar las alertas para un cierto recurso o gravedad.



9. Haga clic en la **información de política** cerca de la superior izquierda de esta pantalla.

10. Haga clic el botón de los **cambios del cometer**.

11. Reaplique su directiva de la intrusión.

> Nota: Para que las alertas sean generadas, utilice esta directiva de la intrusión en la regla del control de acceso. Si no hay regla del control de acceso configurada, después fije esta directiva de la intrusión que se utilizará como la acción predeterminada de la directiva del control de acceso, y reaplique la directiva del control de acceso.

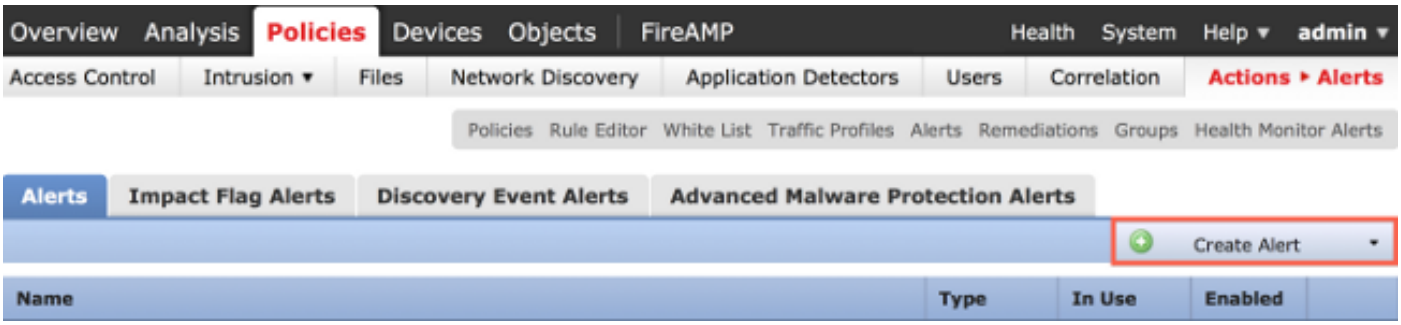
Ahora si un evento de la intrusión se acciona en esa directiva, una alerta también será enviada al servidor de Syslog que se configura en la directiva de la intrusión.

Envío de las alertas de la salud

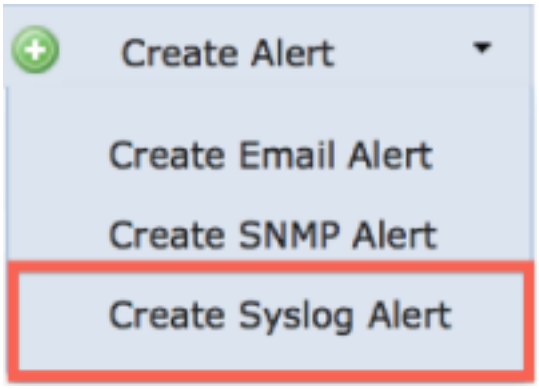
Parte 1: Cree una alerta del Syslog

1. Registro en la interfaz del Web User de su centro de administración de FireSIGHT.

2. Navegue a las **directivas > a las acciones > a las alertas**.



3. Selecto **cree la alerta**, que está en el Lado derecho de la interfaz Web.



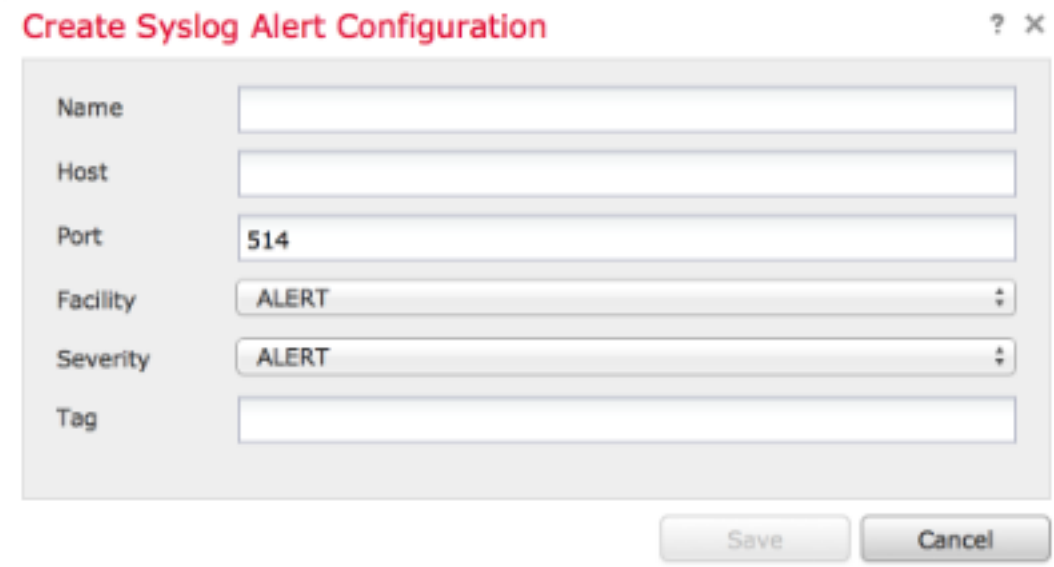
4. El tecleo **crea la alerta del Syslog**. Una ventana emergente de la configuración aparece.

5. Proporcione un nombre para la alerta.

6. Complete la dirección IP de su servidor de Syslog en el campo del **host**.

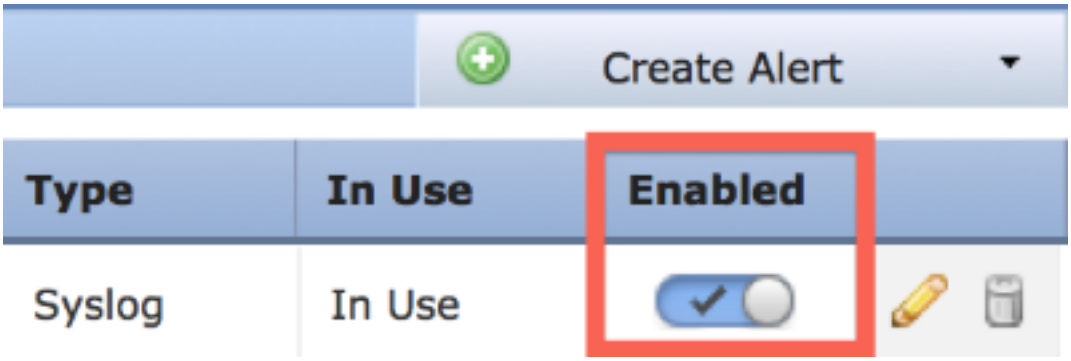
7. Cambie el puerto si es necesario por su servidor de Syslog (el puerto predeterminado es 514).

8. Seleccione un **recurso** y una **gravedad** apropiados.



9. Haga clic el **botón Save Button**. Usted volverá a la página de las **directivas > de las acciones > de las alertas**.

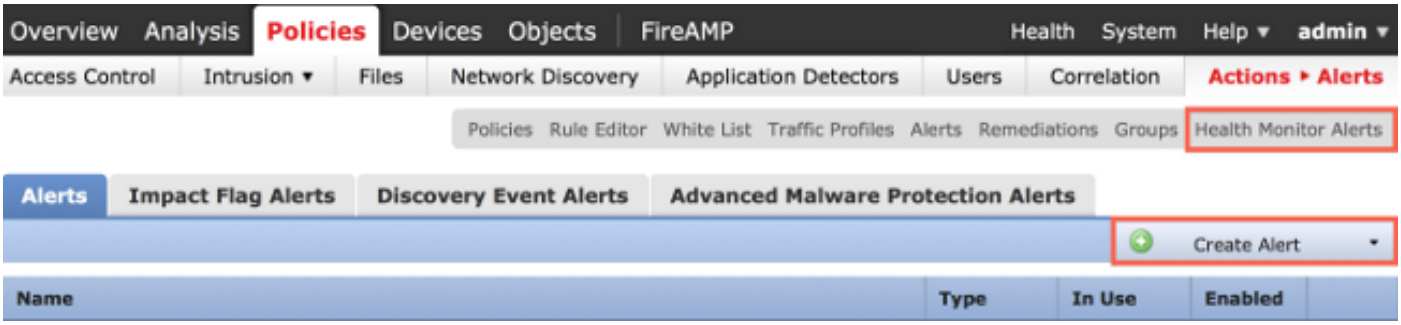
10. Habilite la configuración de syslog.



Parte 2: Cree las alertas del control de salud

La instrucción siguiente describe los pasos para configurar las **alertas del control de salud** que utiliza la alerta del Syslog que usted acaba de crear (en la sección anterior):

1. Vaya a la página de las **directivas > de las acciones > de las alertas**, y elija las **alertas del control de salud**, que está cerca del top de la página.



2. Dé a alerta de la salud un nombre.

3. Elija una **gravedad** (que mantiene la tecla CTRL mientras que el hacer clic se puede utilizar para seleccionar más de un tipo de la gravedad).

4. Del columnm del **módulo** elija los módulos de la salud para los cuales usted quisiera enviar las alertas al servidor de Syslog (por ejemplo, uso del disco).

5. Seleccione la alerta previamente creada del Syslog de la columna de las **alertas**.

6. Haga clic el **botón Save Button**.

Enviando el indicador del impacto, descubra el evento y las alertas de Malware

Usted puede también configurar un centro de administración de FireSIGHT para enviar las alertas del Syslog para los eventos con un indicador específico del impacto, tipo específico de eventos de la detección y de eventos del malware. Para hacer eso, usted tiene que la parte 1: Cree una alerta del Syslog y después configure el tipo de eventos que usted quiera enviar a su servidor de Syslog. Usted puede hacer eso navegando a la página de las **directivas > de las acciones > de las alertas**, y después seleccionando una lengueta para el tipo alerta deseado.