Configuración de un sistema FireSIGHT para enviar alertas a un servidor Syslog externo

Contenido

Introducción

Si bien un sistema FireSIGHT proporciona varias vistas de eventos dentro de su interfaz web, es posible que desee configurar la notificación de eventos externos para facilitar la supervisión constante de los sistemas críticos. Puede configurar un sistema FireSIGHT para generar alertas que le notifiquen por correo electrónico, captura SNMP o registro del sistema cuando se genere una de las siguientes opciones. En este artículo se describe cómo configurar FireSIGHT Management Center para enviar alertas en un servidor Syslog externo.

Prerequisites

Requirements

Cisco recomienda tener conocimientos sobre Syslog y FireSIGHT Management Center. Además, se debe permitir el puerto syslog (el predeterminado es 514) en el firewall.

Componentes Utilizados

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

> **Precaución:** La información de este documento se crea a partir de un dispositivo en un entorno de laboratorio específico y se inicia con una configuración desactivada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Envío de alertas de intrusión

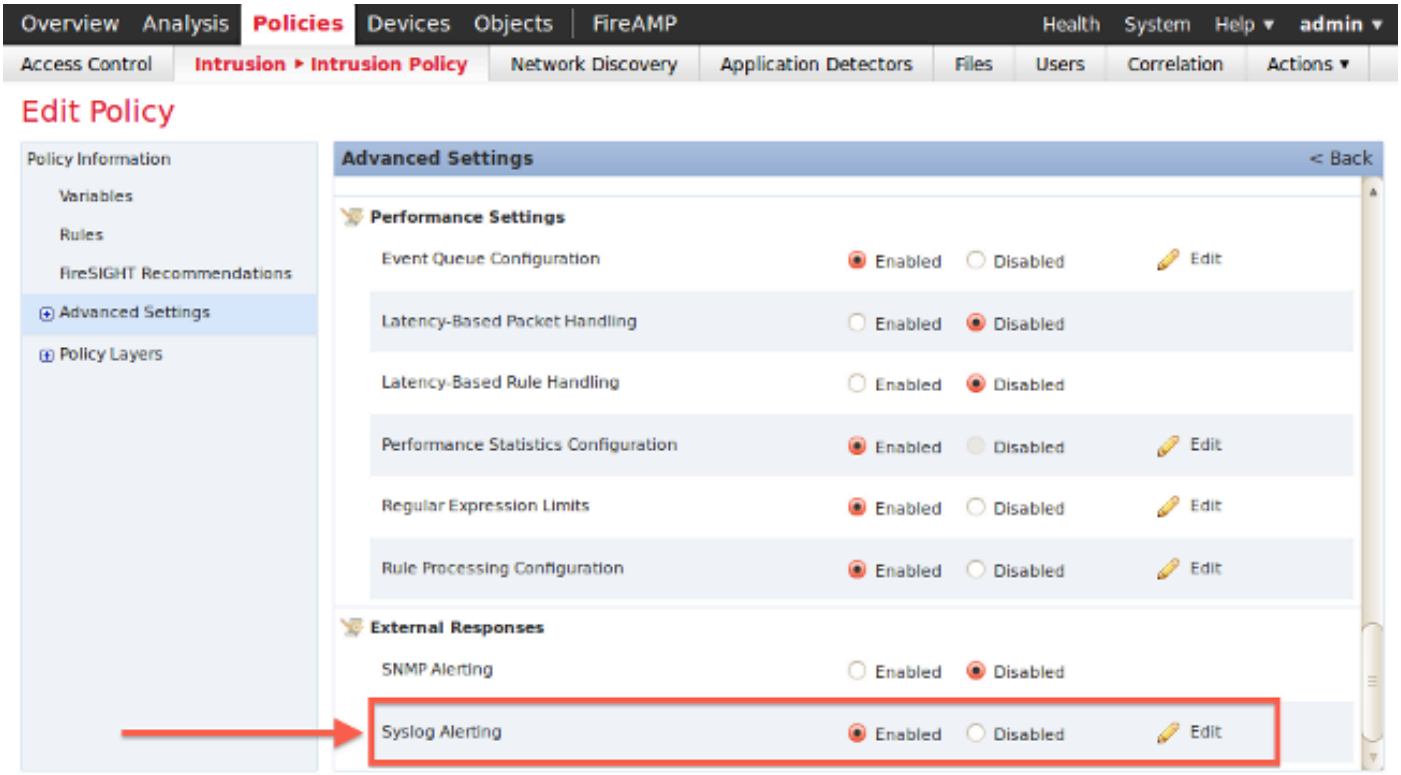
1. Inicie sesión en la interfaz de usuario web de FireSIGHT Management Center.

2. Navegue hasta **Políticas > Intrusión > Política de intrusión**.

3. Haga clic en **Editar** junto a la política que desea aplicar.

4. Haga clic en **Advanced Settings**.

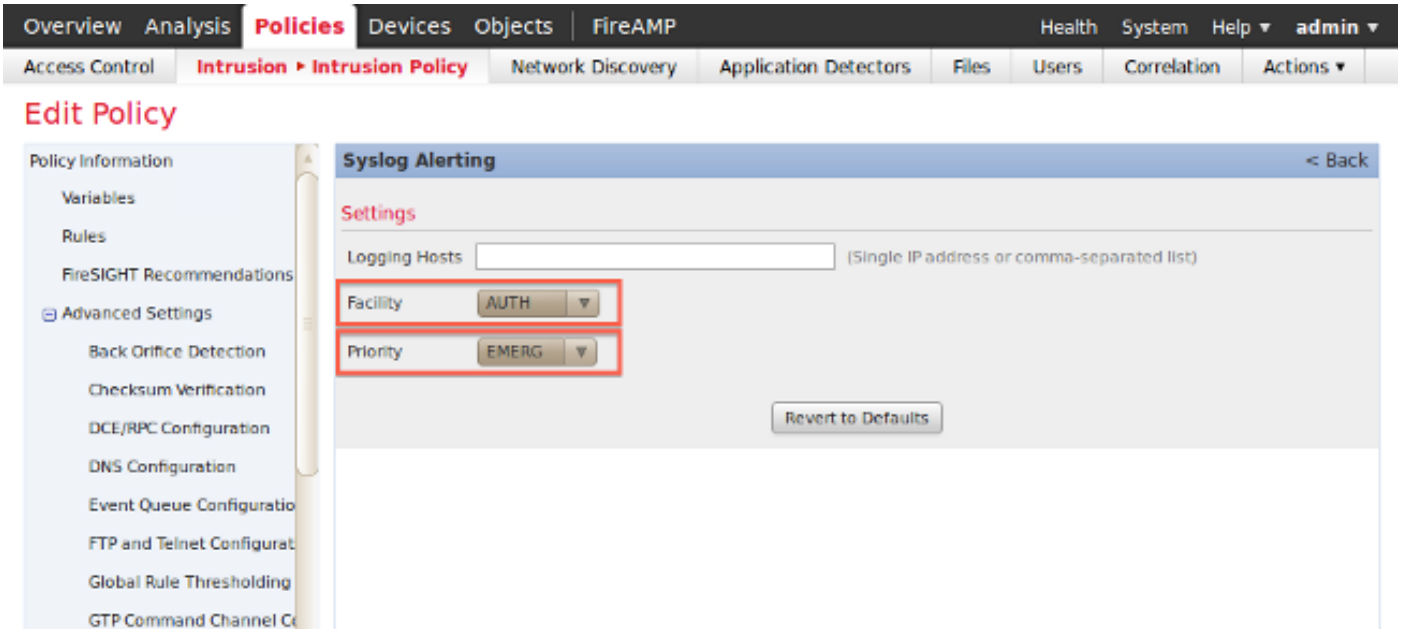
5. Localice **Alertas de Syslog** en la lista y establézcalo en **Activado**.



6. Haga clic en **Editar** junto a la derecha de **Alertas de Syslog**.

7. Escriba la dirección IP del servidor syslog en el campo **Hosts de Registro**.

8. Seleccione una **instalación** adecuada y **Gravedad** en el menú desplegable. Estos pueden dejarse en los valores predeterminados a menos que un servidor syslog esté configurado para aceptar alertas para un servicio o gravedad determinados.



9. Haga clic en **Policy Information** (**Información de política)** cerca de la parte superior izquierda de esta pantalla.

10. Haga clic en el botón **Confirmar Cambios**.

11. Vuelva a aplicar la política de intrusiones.

> **Nota:** Para que se generen las alertas, utilice esta política de intrusión en la regla de control de acceso. Si no hay ninguna regla de control de acceso configurada, establezca esta directiva de intrusiones para que se utilice como acción predeterminada de la directiva de control de acceso y vuelva a aplicar la directiva de control de acceso.

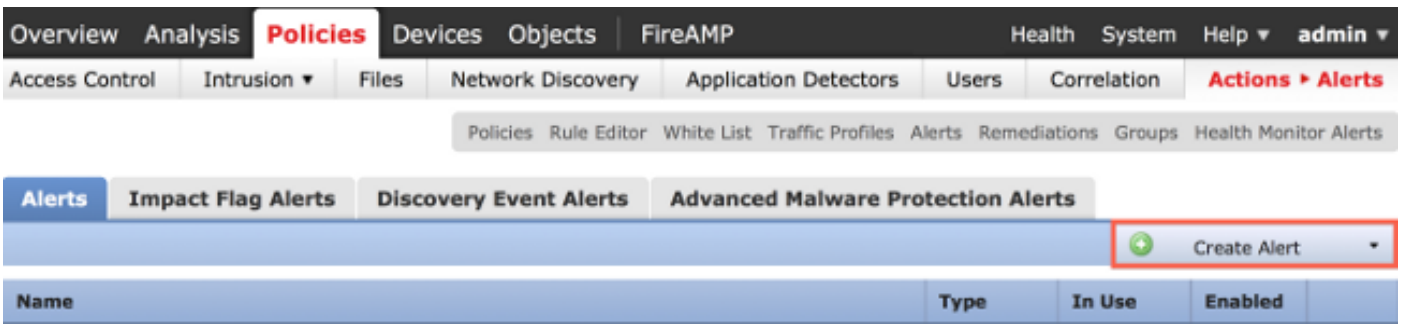
Ahora, si se activa un evento de intrusión en esa política, también se enviará una alerta al servidor syslog configurado en la política de intrusiones.

Envío de alertas de estado

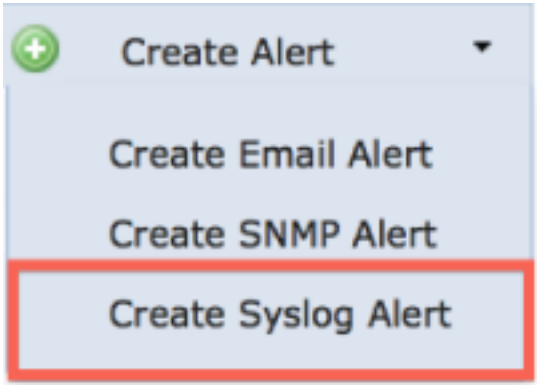
Parte 1: Crear una alerta de Syslog

1. Inicie sesión en la interfaz de usuario web de FireSIGHT Management Center.

2. Acceda a **Políticas > Acciones > Alertas**.



3. Seleccione **Crear alerta**, que se encuentra en el lado derecho de la interfaz Web.



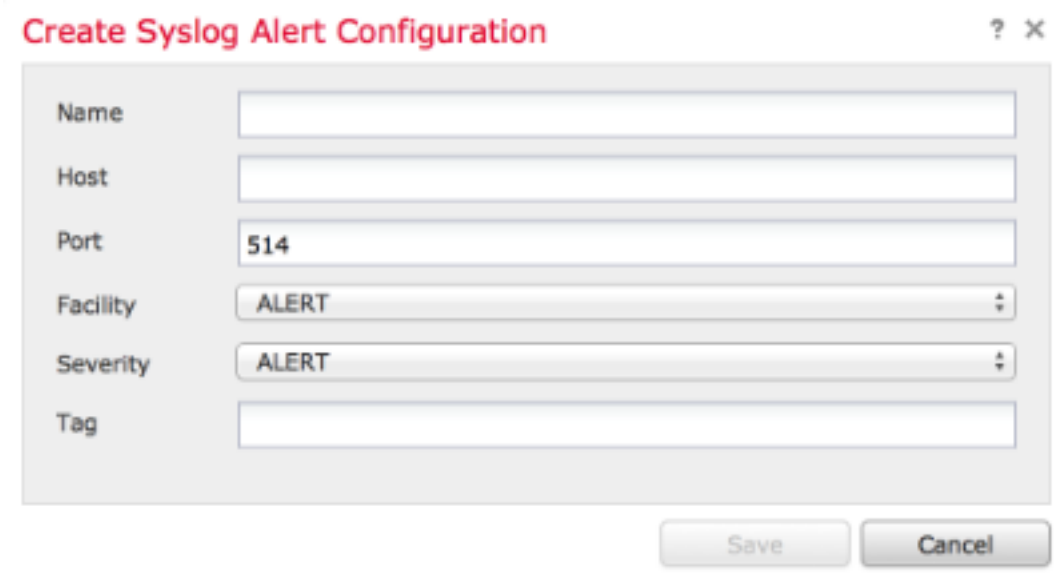
4. Haga clic en **Create Syslog Alert**. Aparecerá una ventana emergente de configuración.

5. Proporcione un nombre para la alerta.

6. Introduzca la dirección IP del servidor syslog en el campo **Host**.

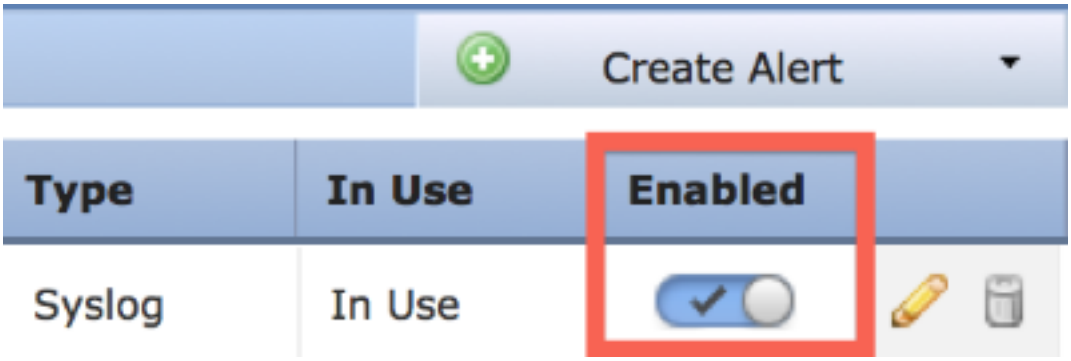
7. Cambie el puerto si lo necesita el servidor syslog (el puerto predeterminado es 514).

8. Seleccione una **instalación** y una **gravedad** adecuadas.



9. Haga clic en el botón **Guardar**. Volverá a la página **Políticas > Acciones > Alertas**.

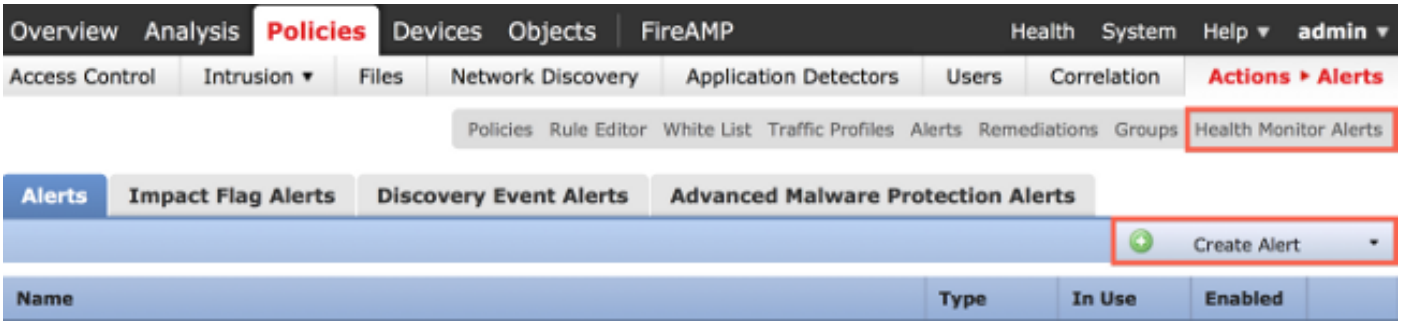
10. Active la configuración de Syslog.



Parte 2: Crear alertas de Health Monitor

La siguiente instrucción describe los pasos para configurar **Health Monitor Alerts** que utiliza la alerta syslog que acaba de crear (en la sección anterior):

1. Vaya a la página **Políticas > Acciones > Alertas** y elija **Alertas de Health Monitor**, que se encuentra cerca de la parte superior de la página.



2. Dé un nombre a la alerta médica.

3. Seleccione una **gravedad** (mantenga pulsada la tecla CTRL mientras pulsa para seleccionar más de un tipo de gravedad).

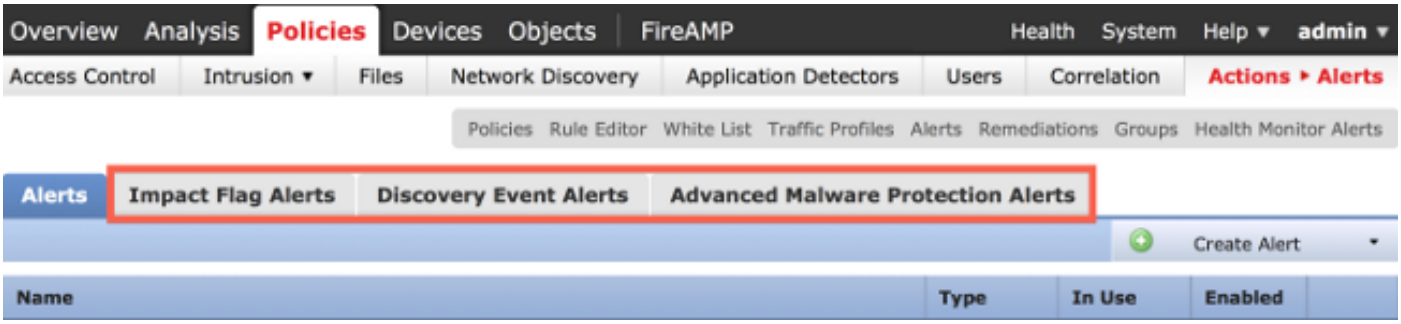
4. En la columna **Módulo**, seleccione los módulos de estado para los que desea enviar alertas al servidor syslog (por ejemplo, Uso de Disco).

5. Seleccione una alerta de registro del sistema creada anteriormente en la columna **Alertas**.

6. Haga clic en el botón **Guardar**.

Envío de indicadores de impacto, detección de eventos y alertas de malware

También puede configurar un FireSIGHT Management Center para enviar alertas de registro del sistema para eventos con un indicador de impacto específico, un tipo específico de eventos de detección y eventos de malware. Para ello, debe consultar la Parte 1: Cree una alerta Syslog y, a continuación, configure el tipo de eventos que desea enviar al servidor syslog. Para ello, vaya a la página **Políticas > Acciones > Alertas** y seleccione una ficha para el tipo de alerta deseado.



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).