

Configurar um sistema FireSIGHT para enviar alertas a um servidor syslog externo

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Enviando alertas de intrusão](#)

[Enviando alertas de integridade](#)

[Parte 1: Criar um alerta de Syslog](#)

[Parte 2: Criar Alertas do Monitor de Integridade](#)

[Enviando sinalizador de impacto, eventos de descoberta e alertas de malware](#)

Introduction

Embora um sistema FireSIGHT forneça várias visualizações de eventos em sua interface da Web, você pode querer configurar a notificação de eventos externos para facilitar o monitoramento constante de sistemas críticos. Você pode configurar um sistema FireSIGHT para gerar alertas que o notificam por e-mail, trap SNMP ou syslog quando um dos itens a seguir é gerado. Este artigo descreve como configurar um FireSIGHT Management Center para enviar alertas em um servidor Syslog externo.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento sobre Syslog e FireSIGHT Management Center. Além disso, a porta syslog (o padrão é 514) deve ser permitida em seu firewall.

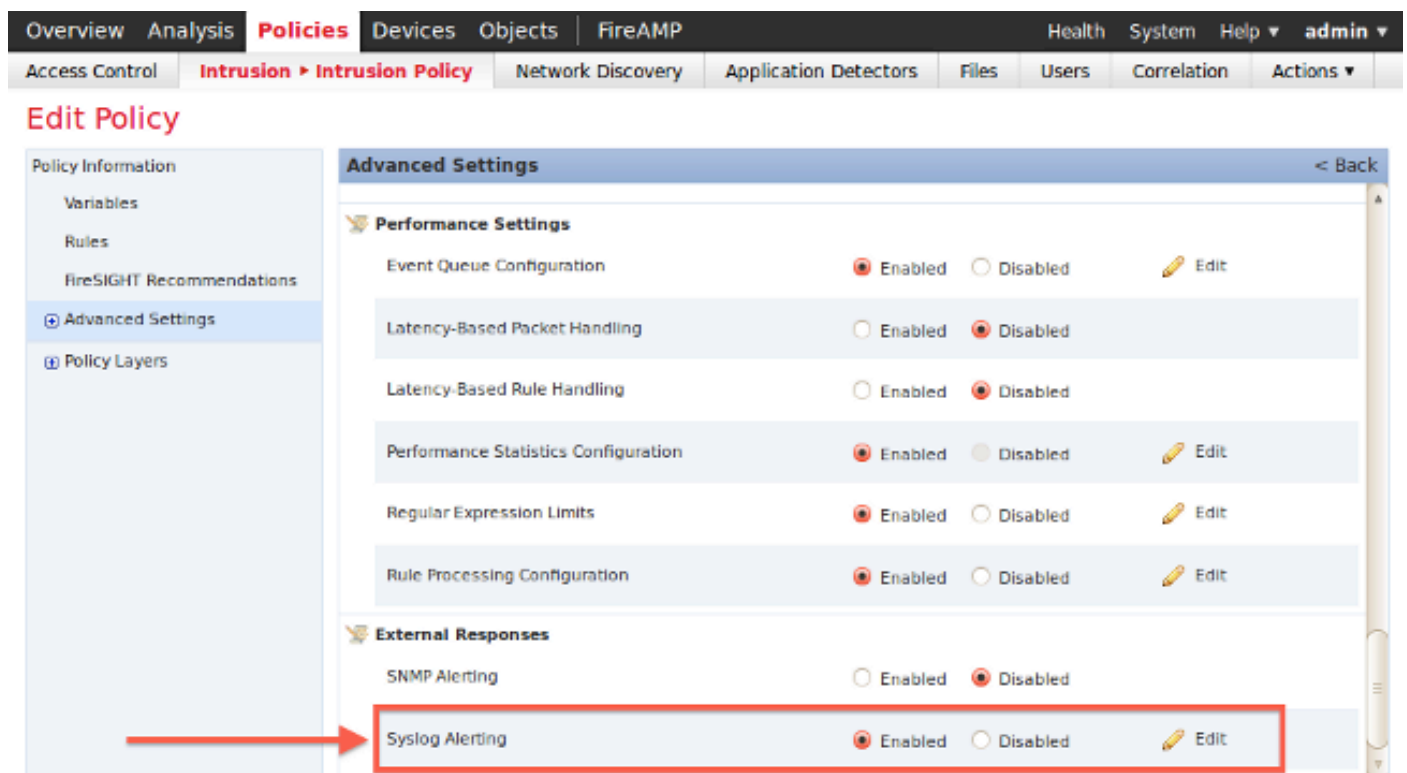
Componentes Utilizados

As informações neste documento são baseadas na versão de software 5.2 ou posterior.

Caution: As informações neste documento são criadas a partir de um dispositivo em um ambiente de laboratório específico e iniciadas com uma configuração limpa (padrão). If your network is live, make sure that you understand the potential impact of any command.

Enviando alertas de intrusão

1. Faça login na interface de usuário da Web do FireSIGHT Management Center.
2. Navegue até **Policies > Intrusion > Intrusion Policy**.
3. Clique em **Editar** ao lado da política que deseja aplicar.
4. Clique em **Advanced Settings**.
5. Localize **Syslog Alerting** na lista e defina-o como **Enabled**.



The screenshot shows the 'Edit Policy' interface in the FireSIGHT Management Center. The navigation menu at the top includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The 'Policies' section is active, and the 'Intrusion > Intrusion Policy' path is selected. The 'Advanced Settings' section is expanded, showing various configuration options. The 'Syslog Alerting' option is highlighted with a red box, and a red arrow points to it. The 'Syslog Alerting' option is currently set to 'Enabled'.

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

6. Clique em **Editar** à direita de **Alerta de Syslog**.
7. Digite o endereço IP do servidor syslog no campo **Logging Hosts**.
8. Escolha uma **Facilidade** e **Severidade** apropriadas no menu suspenso. Eles podem ser deixados com os valores padrão, a menos que um Servidor syslog esteja configurado para aceitar alertas para um determinado recurso ou gravidade.

The screenshot shows the 'Edit Policy' page for 'Syslog Alerting'. The left sidebar contains a 'Policy Information' menu with 'Advanced Settings' expanded. The main content area shows 'Settings' for 'Syslog Alerting' with a 'Logging Hosts' field and two dropdown menus: 'Facility' (set to 'AUTH') and 'Priority' (set to 'EMERG'). A 'Revert to Defaults' button is located below the dropdowns.

9. Clique em **Policy Information** (Informações da política) próximo à parte superior esquerda desta tela.

10. Clique no botão **Confirmar Alterações**.

11. Reaplique sua política de intrusão.

Note: Para que os alertas sejam gerados, use essa política de intrusão na regra de Controle de Acesso. Se não houver uma regra de controle de acesso configurada, defina essa política de intrusão para ser usada como a ação padrão da política de controle de acesso e reaplique a política de controle de acesso.

Agora, se um evento de intrusão for disparado nessa política, um alerta também será enviado para o Servidor syslog configurado na política de intrusão.

Enviando alertas de integridade

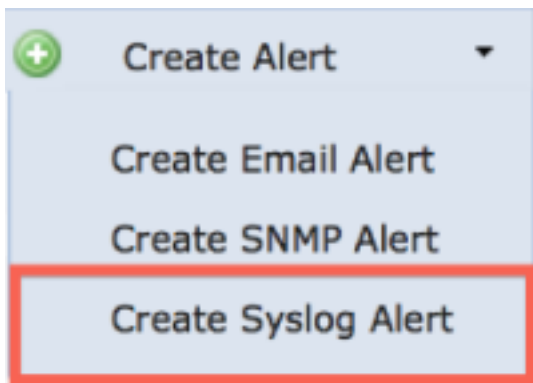
Parte 1: Criar um alerta de Syslog

1. Faça login na interface de usuário da Web do FireSIGHT Management Center.

2. Navegue até **Policies > Actions > Alerts**.

The screenshot shows the 'Alerts' page in the FireSIGHT Management Center. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The 'Alerts' page has a sub-navigation bar with 'Alerts', 'Impact Flag Alerts', 'Discovery Event Alerts', and 'Advanced Malware Protection Alerts'. A 'Create Alert' button with a green plus icon is highlighted with a red box. Below the navigation bar is a table with columns: 'Name', 'Type', 'In Use', and 'Enabled'.

3. Selecione **Criar Alerta**, que está no lado direito da interface da Web.



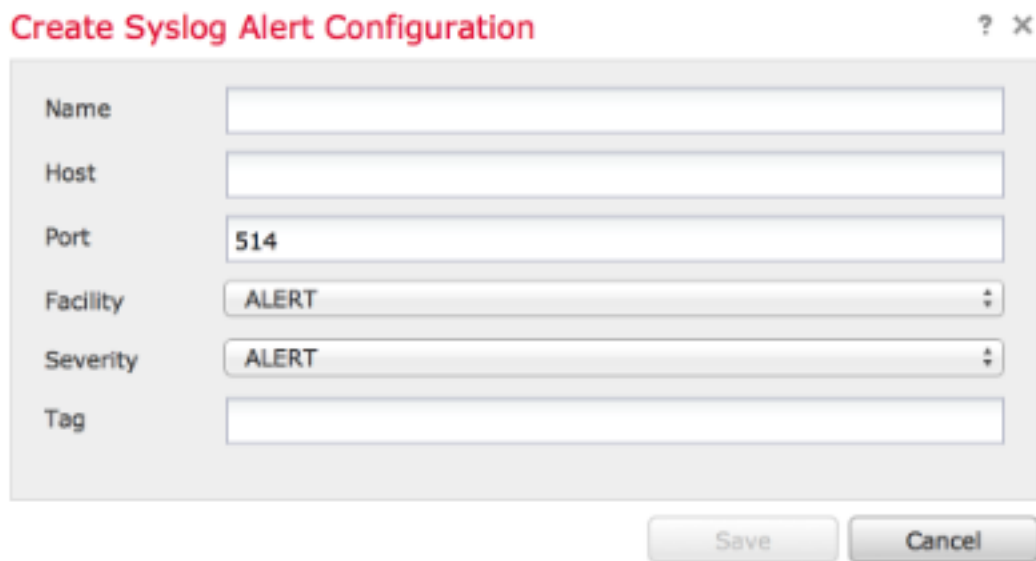
4. Clique em **Create Syslog Alert**. Uma janela pop-up de configuração é exibida.

5. Forneça um nome para o alerta.

6. Preencha o endereço IP do seu Servidor syslog no campo **Host**.

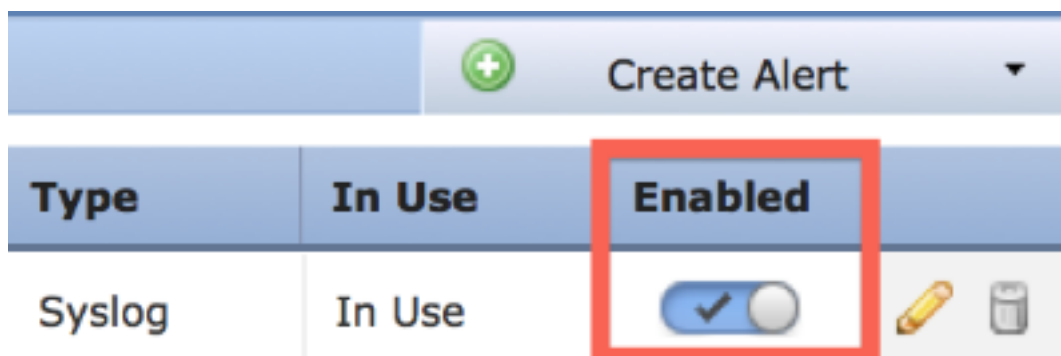
7. Altere a porta, se necessário, pelo servidor syslog (a porta padrão é 514).

8. Selecione uma **Instalação** e **Gravidade** apropriadas.

A screenshot of a 'Create Syslog Alert Configuration' dialog box. The dialog has a title bar with a question mark and a close button. It contains several input fields: 'Name' (empty), 'Host' (empty), 'Port' (514), 'Facility' (ALERT), 'Severity' (ALERT), and 'Tag' (empty). Below the fields are 'Save' and 'Cancel' buttons.

9. Clique no botão **Salvar**. Você retornará à página **Políticas > Ações > Alertas**.

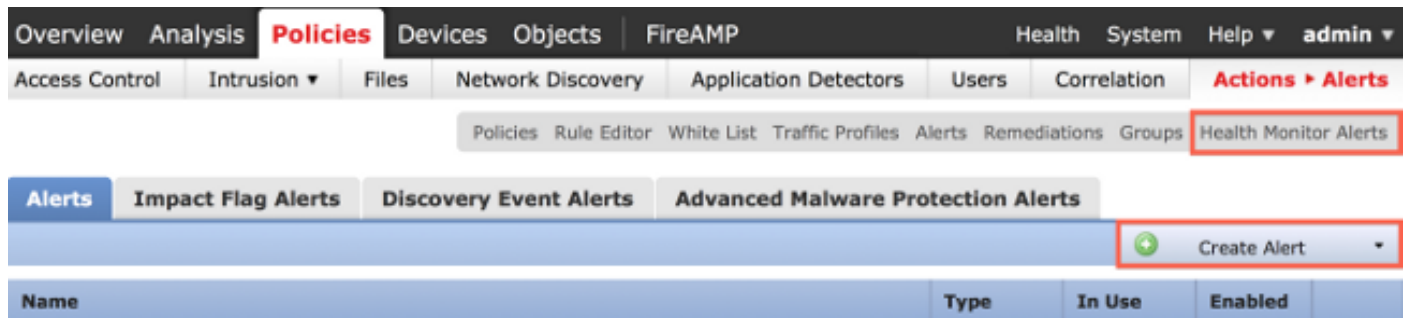
10. Ative a configuração de Syslog.



Parte 2: Criar Alertas do Monitor de Integridade

As instruções a seguir descrevem as etapas para configurar os alertas do Health Monitor que usam o alerta de syslog que você acabou de criar (na seção anterior):

1. Vá para a página **Políticas > Ações > Alertas** e escolha **Health Monitor Alerts**, que está próxima da parte superior da página.



2. Dê um nome ao alerta de integridade.

3. Escolha uma **Severidade** (mantendo pressionada a tecla CTRL enquanto clica em pode ser usada para selecionar mais de um tipo de severidade).

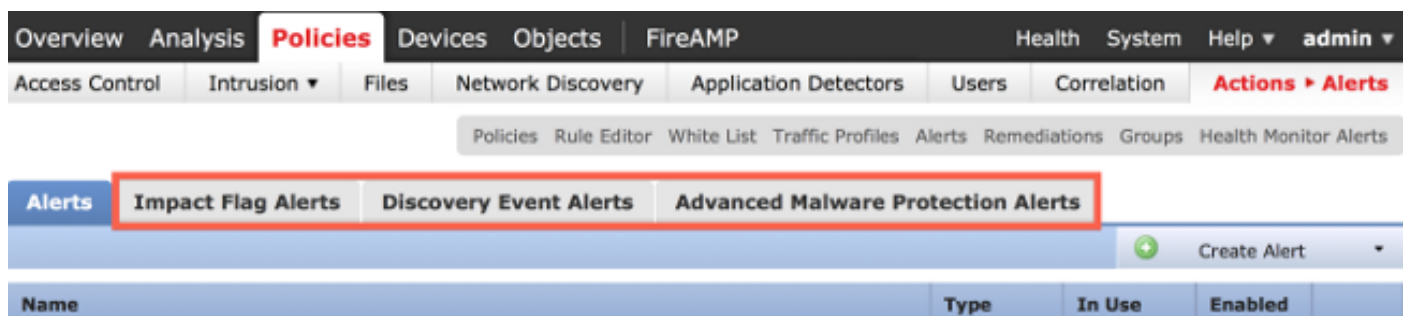
4. Na coluna **Module**, escolha os módulos de funcionamento para os quais você deseja enviar alertas ao Servidor syslog (Por exemplo, Disk Usage).

5. Selecione o alerta de syslog criado anteriormente na coluna **Alertas**.

6. Clique no botão **Salvar**.

Enviando sinalizador de impacto, eventos de descoberta e alertas de malware

Você também pode configurar um FireSIGHT Management Center para enviar alertas de syslog para eventos com um sinalizador de impacto específico, tipo específico de eventos de descoberta e eventos de malware. Para fazer isso, você precisa fazer a [Parte 1: Crie um alerta de syslog](#) e configure o tipo de evento que deseja enviar ao servidor syslog. Para fazer isso, navegue até a página **Políticas > Ações > Alertas** e selecione uma guia para o tipo de alerta desejado.



Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.