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

Índice

Introdução

Quando um sistema de FireSIGHT fornecer várias ideias dos eventos dentro dele é a interface da WEB, você pode querer configurar a notificação de evento externo para facilitar a monitoração constante dos sistemas críticos. Você pode configurar um sistema de FireSIGHT para gerar os alertas que o notificam através do email, da armadilha de SNMP, ou do Syslog quando um do seguinte é gerado. Este artigo descreve como configurar um centro de gerenciamento de FireSIGHT para enviar alertas em um servidor syslog externo.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento no Syslog e no centro de gerenciamento de FireSIGHT. Também, a porta de SYSLOG (o padrão é 514) deve ser permitida em seu Firewall.

Componentes Utilizados

A informação neste documento é baseada a versão de software em 5.2 ou em mais atrasado.

> Cuidado: A informação neste documento é criada de um dispositivo em um ambiente de laboratório específico, e começada com uma configuração esclarecida (PADRÃO). Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Enviando alertas da intrusão

1. Log na relação de usuário de web de seu centro de gerenciamento de FireSIGHT.

2. Navegue às **políticas** > à **intrusão** > à **política da intrusão**.

3. O clique **edita** ao lado da política que você quer se aplicar.

4. Clique **ajustes** sobre **avançados**.

5. Encontre o **Syslog que alerta na** lista e ajuste-o ao **permitido**.

6. O clique **edita** ao lado do direito da **alerta do Syslog**.

7. Datilografe o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu servidor de SYSLOG no campo dos **logging host**.

8. Escolha uma **facilidade** e uma **severidade** apropriadas do menu suspenso. Estes podem ser deixados nos valores padrão a menos que um servidor de SYSLOG for configurado para aceitar alertas para alguma facilidade ou severidade.

9. Clique sobre a **informação sobre a política** perto do esquerdo superior desta tela.

10. Clique o botão das **mudanças comprometer**.

11. Reaplique sua política da intrusão.

> Nota: Para que os alertas sejam gerados, use esta política da intrusão na regra do controle de acesso. Se não há nenhuma regra do controle de acesso configurada, a seguir ajuste esta política da intrusão a ser usada como a ação padrão da política do controle de acesso, e reaplique a política do controle de acesso.

Agora se um evento da intrusão é provocado nessa política, um alerta será enviado igualmente ao servidor de SYSLOG que é configurado na política da intrusão.

Enviando alertas da saúde

Parte 1: Crie um alerta do Syslog

1. Log na relação de usuário de web de seu centro de gerenciamento de FireSIGHT.

2. Navegue às **políticas > às ações > aos alertas**.

3. Seleto **crie o alerta**, que está no lado direito da interface da WEB.

4. O clique **cria o alerta do Syslog**. Uma janela pop-up da configuração aparece.

5. Forneça um nome para o alerta.

6. Preencha o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu servidor de SYSLOG no campo do **host**.

7. Mude a porta se necessário por seu servidor de SYSLOG (a porta padrão é 514).

8. Selecione uma **facilidade** e uma **severidade** apropriadas.

9. Clique o **botão Save Button**. Você retornará à página das **políticas > das ações > dos alertas**.

10. Permita a configuração do Syslog.

Parte 2: Crie alertas do monitor de funcionamento

A seguinte instrução descreve as etapas para configurar **alertas do monitor de funcionamento** que usa o alerta do Syslog que você apenas criou (na seção anterior):

1. Vá à página das **políticas > das ações > dos alertas**, e escolha **alertas do monitor de funcionamento**, que está perto da parte superior da página.

2. Dê ao alerta da saúde um nome.

3. Escolha uma **severidade** (que mantém a chave CTRL quando clicar puder ser usado para selecionar mais de um tipo da severidade).

4. Do columnm do **módulo** escolha os módulos da saúde para que você gostaria de enviar alertas ao servidor de SYSLOG (por exemplo, uso de disco).

5. Selecione o alerta previamente criado do Syslog da coluna dos **alertas**.

6. Clique o **botão Save Button**.

Enviando a bandeira do impacto, descubra o evento e os alertas do malware

Você pode igualmente configurar um centro de gerenciamento de FireSIGHT para enviar alertas do Syslog para eventos com uma bandeira específica do impacto, tipo específico de eventos da descoberta e de eventos do malware. A fim fazer isso, você tem que a parte 1: Crie um alerta do Syslog e configurar então o tipo de eventos que você quer enviar a seu servidor de SYSLOG. Você pode fazer aquele navegando à página das **políticas > das ações > dos alertas**, e então selecionando uma aba para o tipo alerta desejado.