目次

概要

FireSIGHT システムがその中のイベントのさまざまな概観を提供する間、Webインターフェイスは、重要なシステムの一定したモニタリングを促進するために外部イベント通知を設定したいと思う場合もありますあります。 次のいずれかが生成されるとき電子メール、SNMPトラップ、または syslog によって知らせるアラートを生成するために FireSIGHT システムを設定できます。 この技術情報は送信 するために FireSIGHT Management Center を設定する方法を警告 します 外部 の syslog サーバの記述します。

前提条件

要件

Cisco は Syslog および FireSIGHT Management Center のナレッジがあることを推奨します。 また、syslogポート（デフォルトはファイアウォールで 514）必要があります許すあります。

使用するコンポーネント

この文書に記載されている情報はソフトウェア バージョン 5.2 またはそれ以降に基づいています。

> **注意**： この資料の情報は特定のラボ 環境のアプライアンスから作成され、初期（デフォルト）設定と開始します。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

不正侵入アラートの送信

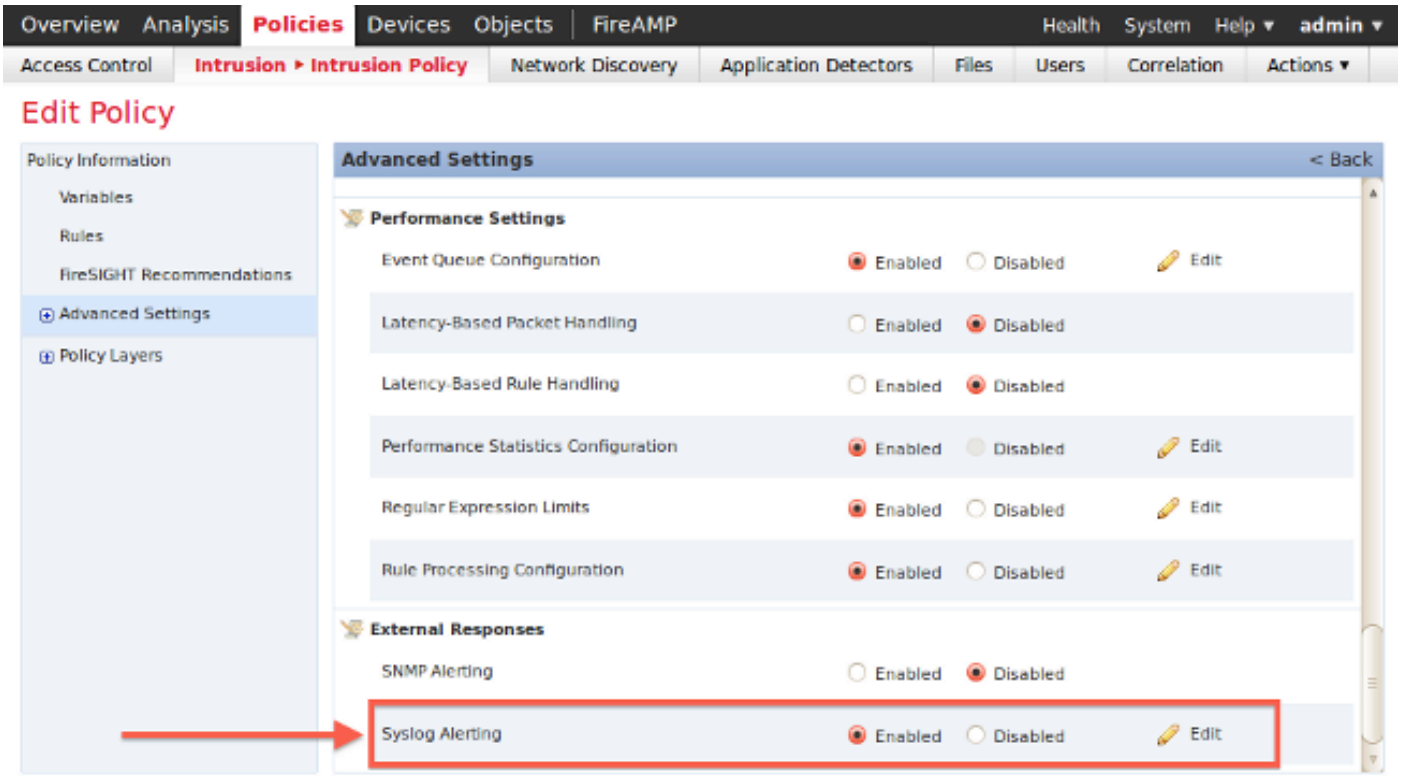
1. FireSIGHT Management Center の Web ユーザ ユーザー・ インターフェースにログイン して下さい。

2. **ポリシー > 不正侵入 > 不正侵入 ポリシー**へのナビゲート。

3. 適用したいと思うポリシーの隣で『Edit』 をクリック して下さい。

4. **設定を**『Advanced』 をクリック して下さい。

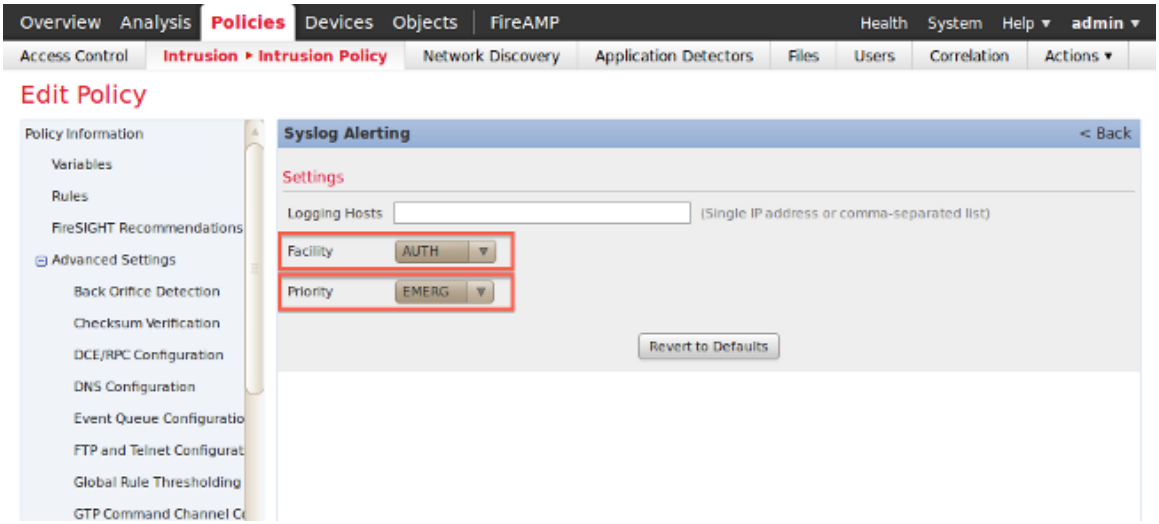
5. **警告 する Syslog を**リストで見つけ、**イネーブルになった**に設定 して下さい。



6. **Syslog 警告**の権限の隣で『Edit』 をクリック して下さい。

7. **ロギング Hosts フィールド**の syslog サーバの IP アドレスをタイプして下さい。

8. ドロップダウン メニューから適切な**ファシリティ**および**重大度を**選択して下さい。 これらはデフォルト値である特定のファシリティまたは重大度のためのアラートを受け入れるために syslog サーバが設定されなければ残すことができます。



9. この画面の左上の近くで**ポリシー情報を**クリックして下さい。

10. **託変更**ボタンをクリックして下さい。

11. 不正侵入 ポリシーを再適用して下さい。

> **注** 生成されるべきアラートのためにアクセスコントロール ルールでこの不正侵入 ポリシーを使用して下さい。 設定される、アクセスコントロール ポリシーのデフォルト アクションとして使用されるべきこの不正侵入 ポリシー 設定 される アクセスコントロール ルールがないしアクセスコントロール ポリシーを再適用すれば。

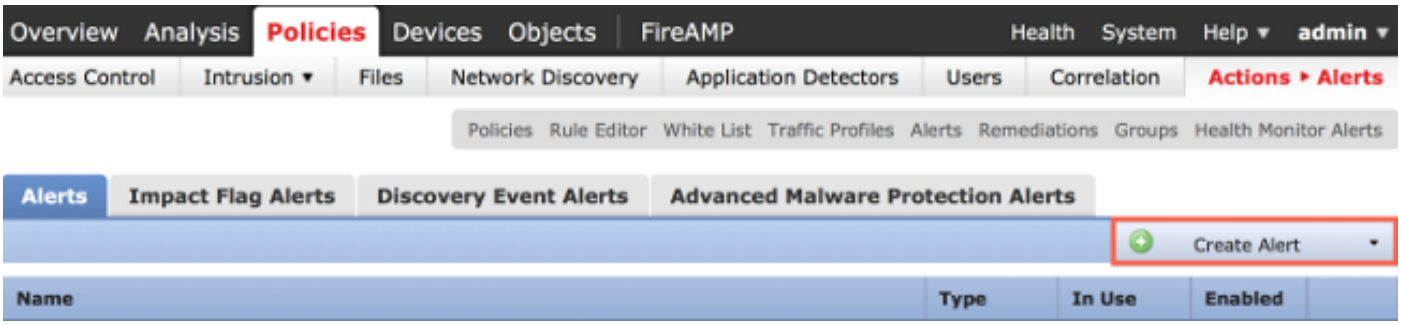
この場合不正侵入 イベントがそのポリシーで引き起こされれば、アラートはまた不正侵入 ポリシーで設定される syslog サーバに発信されます。

健全性アラートの送信

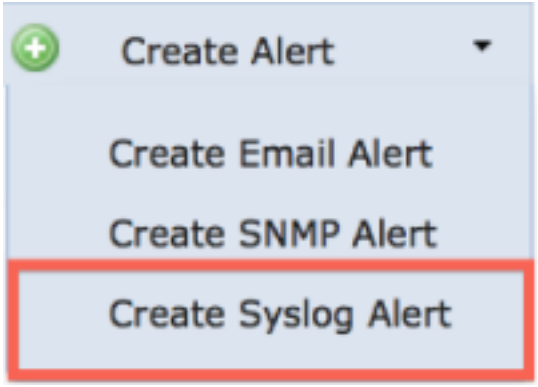
パート 1： Syslog アラートを作成して下さい

1. FireSIGHT Management Center の Web ユーザ ユーザー・ インターフェースにログイン して下さい。

2. **ポリシー > 操作 > アラート**へのナビゲート。



3. **アラートを**『Create』 を選択 して下さい、Webインターフェイスの右側にある。



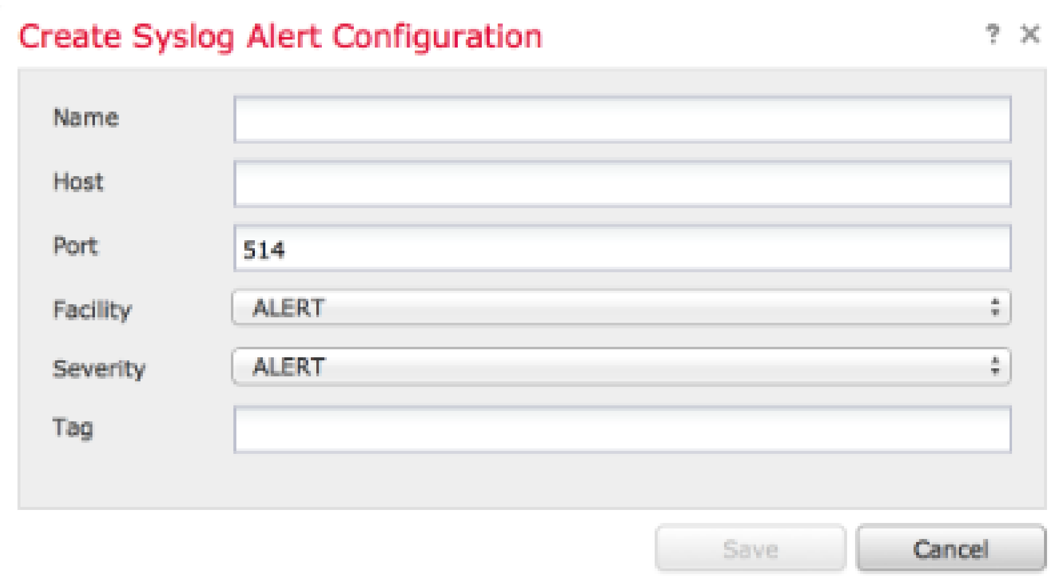
4. **Syslog アラートを**『Create』 をクリック して下さい。 設定 ポップアップウィンドウは現われます。

5. アラートに名前をつけて下さい。

6. **[Host] フィールド**の syslog サーバの IP アドレスを記入して下さい。

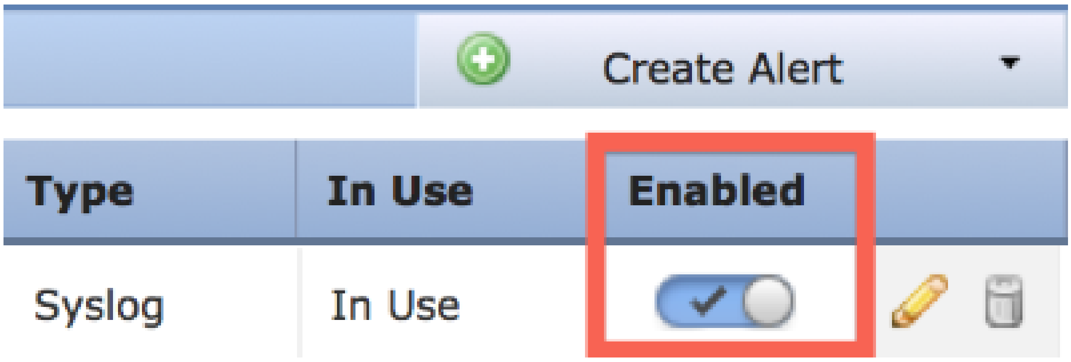
7. syslog サーバによってポートをもし必要なら変更して下さい（デフォルトポートは 514）あります。

8. 適切な**ファシリティ**および**重大度を**選択して下さい。



9. [Save] ボタンをクリックします。 **ポリシー > アクションに > Alerts ページ**戻ります。

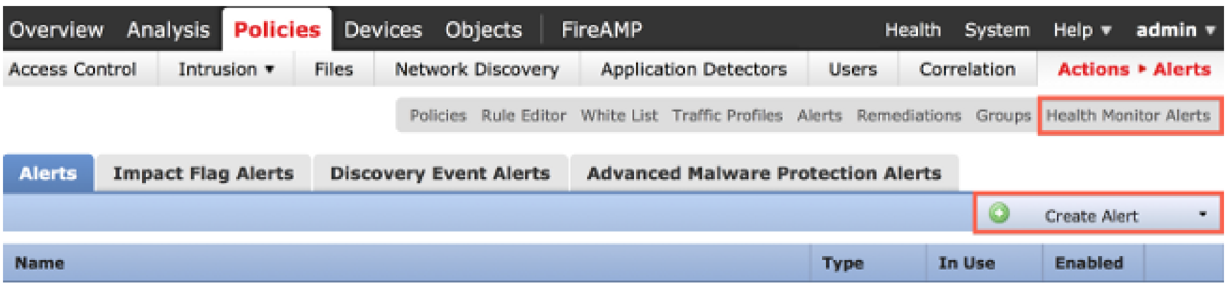
10. Syslog 設定を有効に して下さい。



パート 2： ヘルス モニタ アラートを作成して下さい

ちょうど作成した syslog アラートを使用する次の手順は**ヘルス モニタ アラートを**設定するためにステップを記述します（前のセクションで）:

1. **ポリシー > アクションに > Alerts ページ**行き、**ヘルス モニタ アラートを**選択して下さい、ページの上の近くにある。



[illegible]

影響フラグを送信して、イベントおよび Malware アラートを検

出して下さい

またディスカバリ イベントおよび malware イベントの特定の種類特定の影響フラグのイベントのための syslog アラートを発信するために FireSIGHT Management Center を設定できます。 それをするために、Part 1 なります: Syslog アラートを作成し、次に syslog サーバに送ってほしいイベントの種類を設定して下さい。 **> Alerts ページ ポリシー > アクション**へのナビゲート し、望ましいアラート タイプにタブを選択することによってそれをすることができます。