FireSIGHT システムの初期設定手順

目次

概要

FireSIGHT Management Center または FirePOWER デバイスのイメージ変更が完了したら、システムが完全に機能し、侵入イベントのアラートを生成できるようにするための手順を実行する必要があります（ライセンスのインストール、アプライアンスの登録、正常性ポリシー、システム ポリシー、アクセス コントロール ポリシー、侵入ポリシーの適用など）。 このドキュメントは、FireSIGHT システムのインストール ガイド ガイドの補足です。

前提条件

このドキュメントは、FireSIGHT システムのインストール ガイドを読んでいることを前提としています。

設定

ステップ 1： 初期設定

FireSIGHT Management Center で Web インターフェイスにログインし、次に示すセットアップ ページで初期設定オプションを指定して、セットアップ プロセスを完了する必要があります。 こ

のページで、管理者パスワードを変更する必要があります。また、ドメインや DNS サーバなどのネットワーク設定や時刻設定を指定することもできます。

任意で、繰り返しルール、位置情報更新、および自動バックアップを設定できます。 機能ライセンスもこの時点でインストールできます。

このページでは、デバイスを FireSIGHT Management Center に登録し、検出モードを指定することもできます。 登録中に選択された検出モードとその他のオプションによって、システムで作成されるデフォルト インターフェイス、インライン セット、およびゾーンだけでなく、管理対象デバイスに最初に適用されるポリシーも決定されます。

ステップ 2： ライセンスのインストール

初期設定のページでライセンスをインストールしていない場合は、次の手順に従ってこの作業を実行できます。

- 次のページに移動します： [System] .> [Licenses]
- [Add New License] をクリックします。

ライセンスを受け取っていない場合は、お客様のアカウント担当のセールス担当者にお問い合わせください。

手順 3： システム ポリシーの適用

システム ポリシーは、FireSIGHT Management Center および管理対象デバイス間の時刻同期と認証プロファイルの設定を指定します。 システム ポリシーを設定または適用するには、[System] > [Local] > [System Policy] に移動します。 デフォルトのシステム ポリシーが提供されますが、このデフォルト ポリシーをすべての管理対象デバイスに適用する必要があります。

ステップ 4： 正常性ポリシーの適用

正常性ポリシーは、管理対象デバイスが各自のヘルス ステータスを FireSIGHT Management Center に報告する方法を設定するのに使用されます。 正常性ポリシーを設定または適用するには、[Health Policy] に移動します。 デフォルトの正常性ポリシーが提供されますが、このデフォルト ポリシーをすべての管理対象デバイスに適用する必要があります。

ステップ 5： 管理対象デバイスの登録

初期設定ページでデバイスを登録しなかった場合は、このドキュメントを読み、FireSIGHT Management Center へのデバイスの登録手順を確認してください。

ステップ 6： インストールされているライセンスの有効化

アプライアンスで機能ライセンスを使用するには、各管理対象デバイスで機能ライセンスを有効にしておく必要があります。

1. 次のページに移動します： [Devices] > [Device Management]
2. ライセンスを有効にするデバイスをクリックし、[Device] タブを表示します。
3. [License] の横の [Edit]（*鉛筆* アイコン）をクリックします。

このデバイスに必要なライセンスを有効にし、[Save] をクリックします。

右上隅に「*You have unapplied changes*」というメッセージが表示されます。 この警告は、デバイス管理ページから移動した後でも、[Apply Changes] ボタンをクリックするまではアクティブなままになります。

ステップ 7： 検知インターフェイスの設定

1. [Devices] > [Device Management] ページに移動します。
2. 該当するセンサの [Edit]（鉛筆）アイコンをクリックします。
3. [Interfaces] タブで、該当するインターフェイスの [Edit] アイコンをクリックします。

パッシブ インターフェイス設定またはインライン インターフェイス設定を選択します。 スイッチド インターフェイスおよびルーテッド インターフェイスは、この記事では扱いません。

ステップ 8： 侵入ポリシーの設定

- 次のページに移動します： **[Policies] > [Intrusion] > [Intrusion Policy]**
- [Create Policy] をクリックします。次のダイアログボックスが表示されます。

名前を割り当て、使用するベース ポリシーを定義します。 導入環境によっては、[Drop when Inline] オプションを有効にできます。 誤検出を削減し、システムのパフォーマンスを改善するために保護するネットワークを定義します。

[Create Policy] をクリックすると、設定が保存され、IPS ポリシーが作成されます。 侵入ポリシーを変更する場合は、代わりに [Create and Edit Policy] を選択できます。

> **注:** 侵入ポリシーは、アクセス コントロール ポリシーの一部として適用されます。 侵入ポリシーの適用後に [Reapply] ボタンをクリックすると、アクセス コントロール ポリシー全体を再適用せずに変更を適用できます。

ステップ 9： アクセス コントロール ポリシーの設定と適用

1. [Policies] > [Access Control] に移動します。

2. [New Policy] をクリックします。

3. [Name] にポリシーの名前を入力し、[Description] に説明を入力します。

4. [Default Action] で、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 [Intrusion Prevention] を選択します。

5. 最後に [Targeted Devices] で、アクセス コントロール ポリシーを適用する対象デバイスを選択し、[Save] をクリックします。

6. デフォルト アクションの侵入ポリシーを選択します。

7. 接続イベントを生成するには、接続ロギングを有効にしておく必要があります。 [Default Action] の右側にあるドロップダウン メニューをクリックします。

8. 接続の開始時または終了時に接続をログに記録することを選択します。 イベントは FireSIGHT Management Center または Syslog ロケーションでログに記録されるか、または SNMP 経由でログに記録されます。

> **注:** 接続の開始時と終了時の両方で記録すると、ブロックされている接続を除くすべての接続が 2 回ログに記録されるため、両側で記録することは推奨されません。 開始時に記録すると、ブロックされる接続の場合に役立ち、終了時に記録すると、その他の接続の場合に役立ちます。

9. [OK] をクリックします。 ロギング アイコンの色が変化することに注意してください。

10. この時点で**アクセス コントロール ルール**を追加できます。 使用できるオプションは、インストールされているライセンスの種類に応じて異なります。

11. 変更が完了したら、 [Save and Apply] ボタンをクリックします。 このボタンをクリックするまで、ポリシーの変更が未保存であることを示すメッセージが右上隅に表示されています。

変更を**保存**するだけか、または**保存して適用**することを選択できます。 後者を選択すると、次のウィンドウが表示されます。

12. [Apply All] は、アクセス コントロール ポリシーと関連するすべての侵入ポリシーをターゲット デバイスに適用します。

> **注:** 侵入ポリシーが初めて適用される場合、このポリシーを選択解除することはできません。

13. タスクのステータスをモニタするには、ページ上部に表示されている通知で [Task Status] リンクをクリックするか、または、 **[System] > [Monitoring] > [Task Status] に移動します。**

14. [Task Status] リンクをクリックして、アクセス コントロール ポリシーの適用の進行状況をモニタします。

ステップ 10： FireSIGHT Management Center がイベントを受信するかどうかの確認

アクセス コントロール ポリシーの適用が完了すると、接続イベントが表示され、トラフィック侵入イベントを利用できるようになります。

その他の推奨事項

システムでは次の追加機能も設定できます。 実装の詳細については、ユーザ ガイドを参照してください。

- スケジュール バックアップ
- 自動ソフトウェア アップデート、SRU、VDB、および GeoLocation ダウンロード/インストール。
- LDAP または RADIUS を使用した外部認証