修復モジュールの設定

次のセクションでは、修復モジュールを設定する手順について説明します。

- 設定（Configure） （1 ページ）

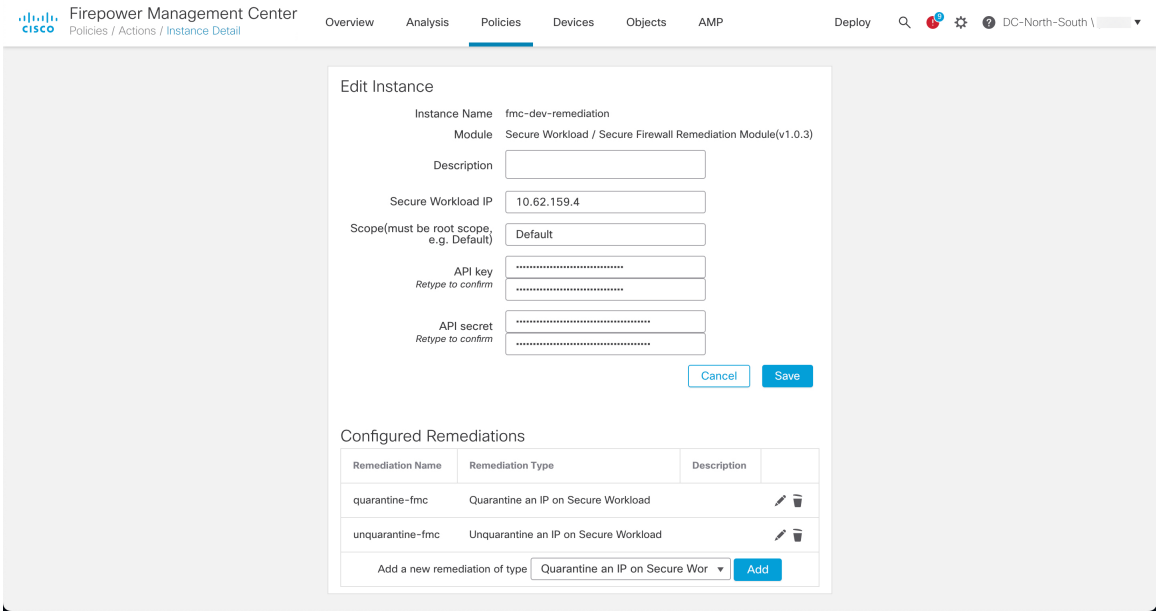
設定（Configure）

FMC にインストールされた修復モジュールを設定するには、次の手順を実行します。

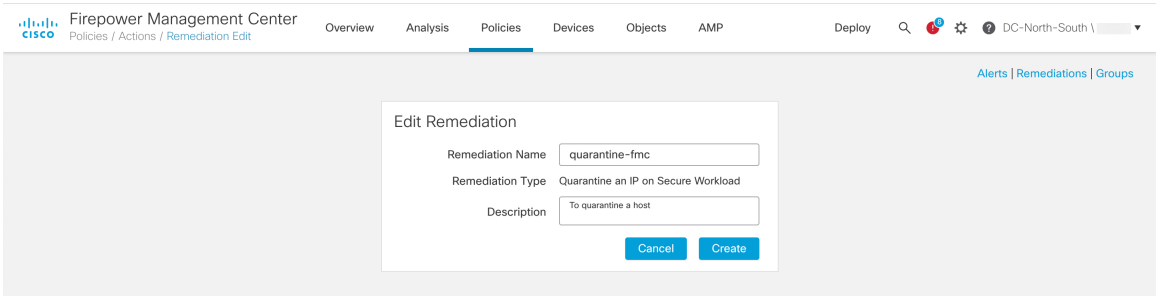
ステップ 1 FMC で、ネットワーク内の Cisco Secure Workload クラスタごとに修復モジュールのインスタンスを作成します。

1. [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）] に移動します。
2. ドロップダウン リストから修復モジュールを選択し、[追加（Add）] をクリックします。
3. [インスタンス名（Instance Name）] を入力します（この例では **`fmc-dev-remediation`**）。
4. Cisco Secure Workload サーバーの IP アドレス、API キー、API シークレット、および問題がある可能性のあるホストが含まれる範囲を入力します。[作成（Create）] をクリックします。

   （注） API キーとシークレットは、この時点では Cisco Secure Workload サーバーに対して検証されません。サイト管理者、カスタマーサポート、またはルート スコープ オーナー ロールは、API キーとシークレットを Cisco Secure Workload で最初に作成しておく必要があります。ここで使用する情報をコピーします。詳細については、関連資料を参照してください。



5. [設定されている修復（Configured Remediations）] で、修復のタイプ（この例では「**Quarantine an IP on Secure Workload**」）を選択し、[追加（Add）] をクリックして新しい修復を追加します。
6. [修復名（Remediation Name）]（この例では **quarantine-fmc**）を入力し、[作成（Create）] をクリックします。



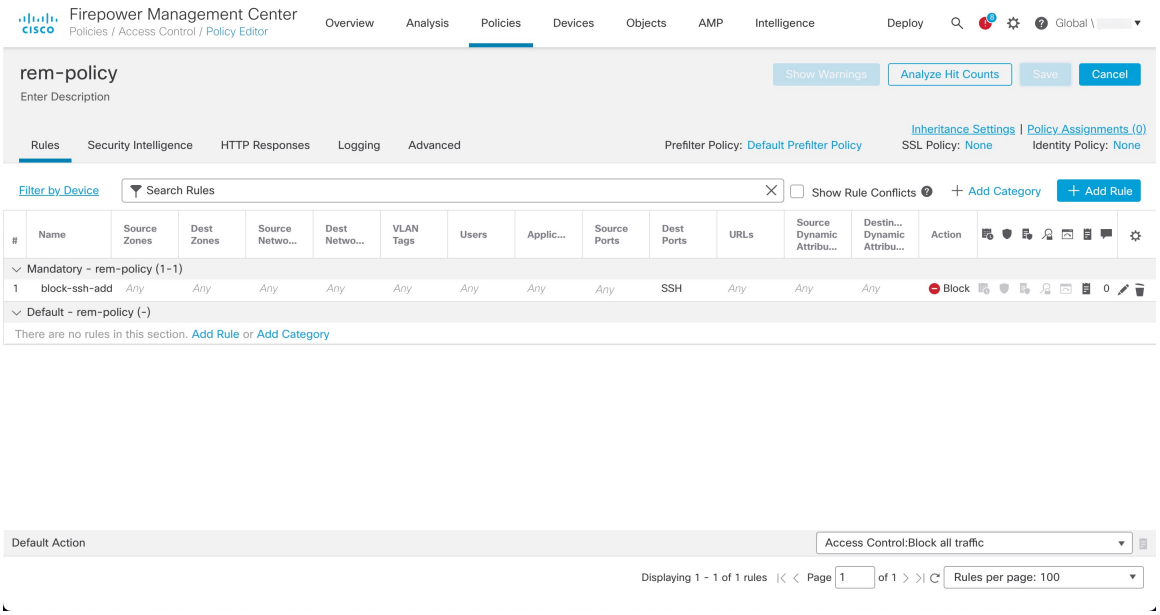
7. 設定した修復がテーブルに表示されます。[保存（Save）] をクリックします。

ステップ 2 アクセス制御ポリシーを設定します（この例では、**rem-policy**）。

1. [ポリシー（Policies）] > [アクセス制御（Access Control）] を選択し、アクセス コントロール ポリシーの [編集（Edit）] アイコンをクリックしてルールを追加します。
2. [ルールの追加（Add Rule）] をクリックし、名前（この例では **block-ssh-add-tag**）を入力します。
3. [アクション（Action）] で [ブロック（Block）] を選択します。
4. [ポート（Ports）] タブで、宛先ポートのプロトコルの一覧から [SSH（SSH）] を選択します。
5. [ロギング（Logging）] タブで、[接続開始時のログ（Log at Beginning of Connection）] を選択します。

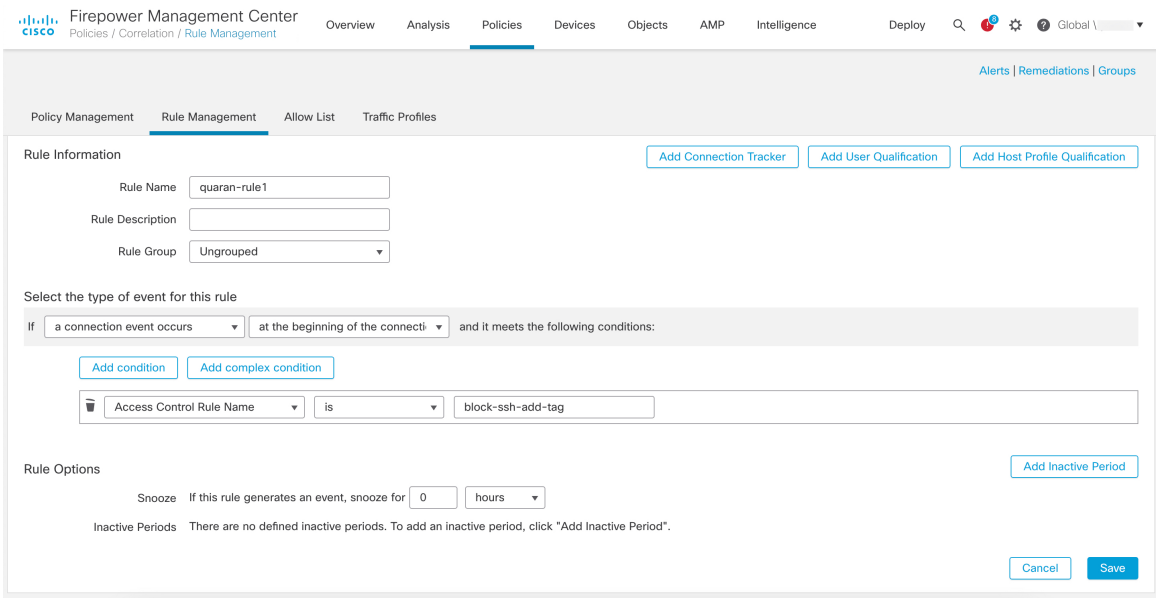
   重要 アクセスルールでロギングが有効になっていることを確認します。これにより、FMC はイベント通知を受信します。確認したら [追加（Add）] をクリックします。

6. [保存（Save）] をクリックします。



ステップ 3 相関ルールを設定します。

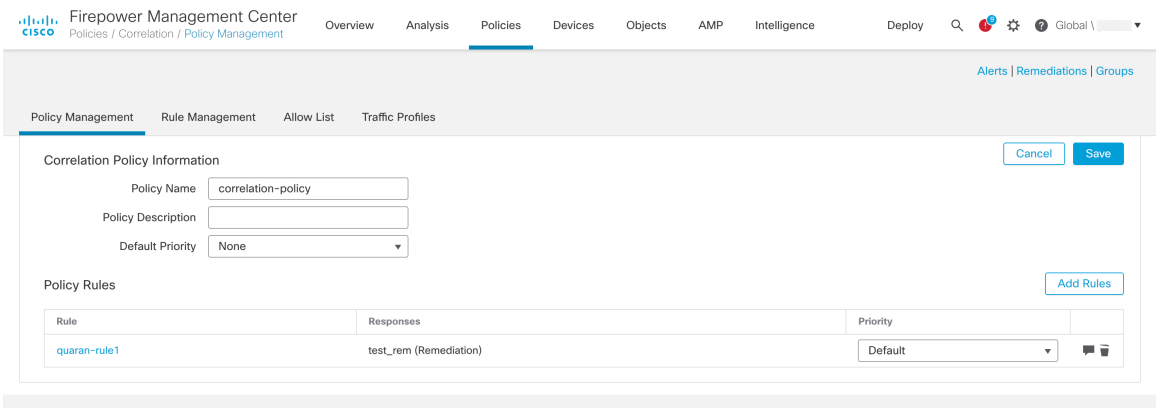
1. [ポリシー（Policies）] > [相関（Correlation）] > [ルールの管理（Rule Management）] に移動します。
2. [ルールの作成（Create Rule）] をクリックします。
3. [ルール名（Rule Name）] を入力し（この例では、**`quaran-rule1`**）、説明（オプション）を入力します。
4. [このルールのイベントタイプの選択（Select the type of event for this rule）] セクションで、[接続イベントの発生（a connection event occurs）] および [接続の開始時または終了時（at either the beginning or the end of the connection）] を選択します。
5. [条件を追加（Add condition）] をクリックし、演算子を **OR** から **AND** に変更します。
6. ドロップダウンリストで、[アクセスコントロールルール名（Access Control Rule Name）]、[は（is）] を選択し、ステップ 2 で設定したアクセス コントロール ルールの名前を入力します（この例では、**`block-ssh-add-tag`**）。



7. [保存（Save）] をクリックします。

ステップ 4 相関ルールに、修復モジュールのインスタンスを応答としてアソシエートします。

1. [ポリシー（Policies）]>[相関（Correlation）]>[ポリシーの管理（Policy Management）] に移動します。
2. [ポリシーの作成（Create Policy）] をクリックします。
3. [ポリシー名（Policy Name）] を入力し（この例では、**correlation-policy**）、説明（オプション）を入力します。
4. [ディフォルトのプライオリティ（Default Priority）] ドロップダウン リストから、ポリシーのプライオリティを選択します。[なし（None）] を選択して、ルールのプライオリティのみ使用します。
5. [ルールの追加（Add Rules）] をクリックし、ステップ 3 で設定した相関ルールを選択し（この例では、**quaran-rule1**）、[追加（Add）] をクリックします。
6. ルールの横にある [応答（Responses）] アイコンをクリックし、ルールに応答（この例では **test_rem**）を割り当てます。[更新（Update）] をクリックします。



7. [保存（Save）] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。