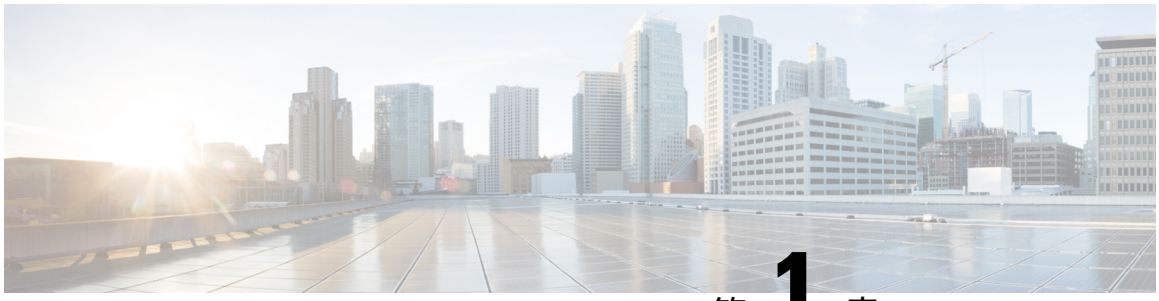
Cisco Secure Workload 向け Cisco Secure Firewall Management Center 修復モジュール クイックスタートガイド

初版：2022 年 6 月 6 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



第 1 章

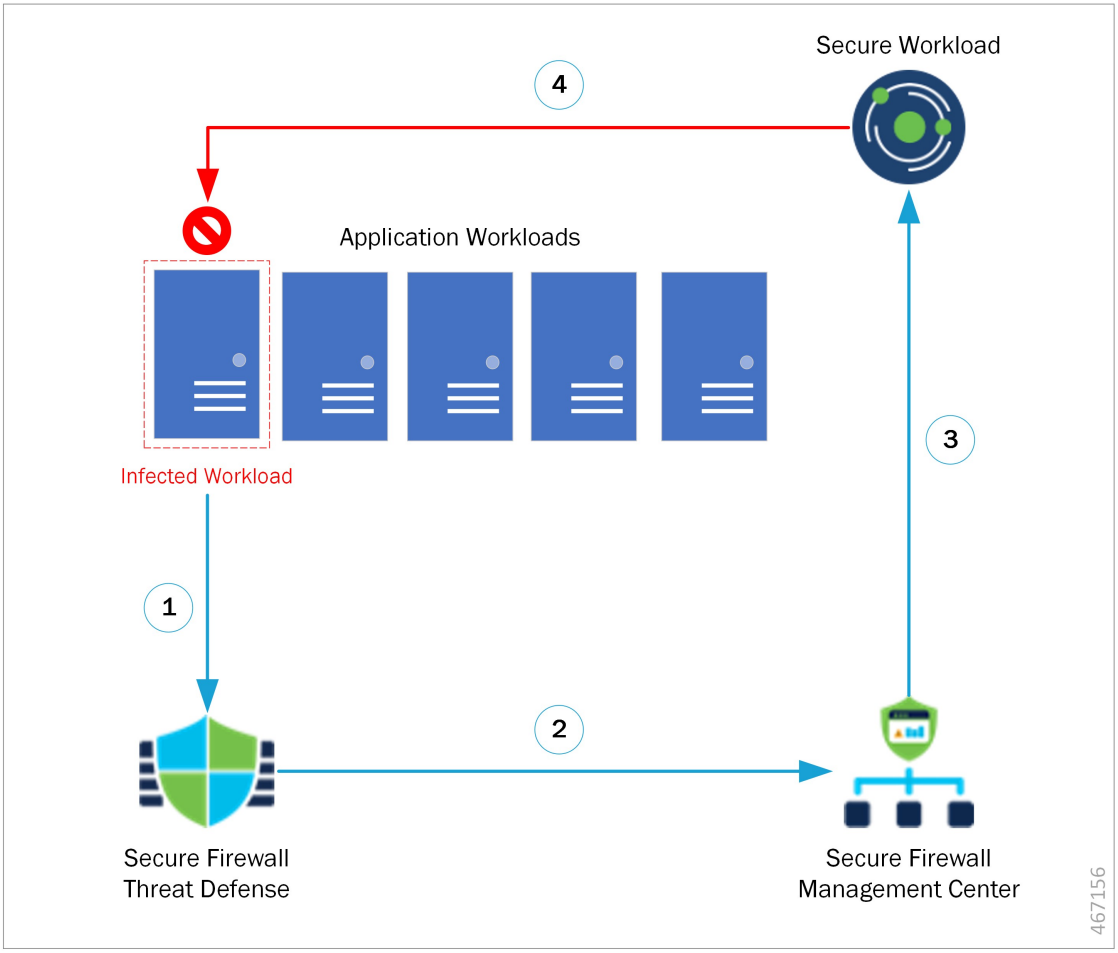
はじめに

Cisco Secure Workload（旧 Cisco Tetration）向け Cisco Secure Firewall Management Center 修復モジュールは、ネットワークの状況が関連する相関ポリシーに違反したときに Cisco Secure Firewall Management Center を自動的に起動する修復を作成するのに役立ちます。たとえば、ホストの状況を評価し、Cisco Secure Workload 適用エージェントで問題のあるホストを隔離するために、送信元または宛先 IP アドレスのデバイスでトラフィックをブロックできます。ポリシー内の複数のルールがトリガーされた場合、Cisco Secure Firewall Management Center でルールごとに応答を起動できます。修復モジュールは、応答を実行するために Cisco Secure Firewall Management Center にインストールするファイルのパッケージです。

概要

Cisco Secure Workload（旧 Cisco Tetration）向け Cisco Secure Firewall Management Center（FMC）修復モジュールを使用すると、感染したホストからのネットワークへの攻撃が FMC によって検出された場合に、Cisco Secure Workload 適用エージェントによって問題のあるホストを隔離し、そのホストに対する以降のトラフィックの出入りを禁止できます。次の図は、この修復モジュールをインストールした場合の FMC と Cisco Secure Workload の関係を示しています。

図 *1 : Cisco Secure Firewall Management Center* による *Cisco Secure Workload* への脅威の迅速な封じ込め



1	Threat Defense により、感染したワークロードから悪意のあるトラフィックが検出されます。
2	Threat Defense から Management Center に悪意のあるトラフィックの詳細を含むイベントが送信されます。
3	感染したワークロードを隔離するために修復モジュールがトリガーされます。
4	Cisco Secure Workload から適用エージェントにワークロードの隔離要求が送信されます。

ネットワーク攻撃を隔離するプロセスは次のとおりです。

ステップ 1 感染したワークロードにより、ネットワーク内に悪意のあるトラフィックが送信されます。Cisco Secure Firewall デバイス（物理または仮想）で実行されている Cisco Secure Firewall Threat Defense（FTD）によって、悪意のあるトラフィックが検出されます。

ステップ 2 悪意のあるトラフィックに関する情報を含むイベントが生成され、FTD を管理する FMC に報告されます。

ステップ 3 FMC で修復モジュールがトリガーされ、Cisco Secure Workload REST API を使用して、感染したワークロードを隔離するように Cisco Secure Workload に対して要求が送られます。

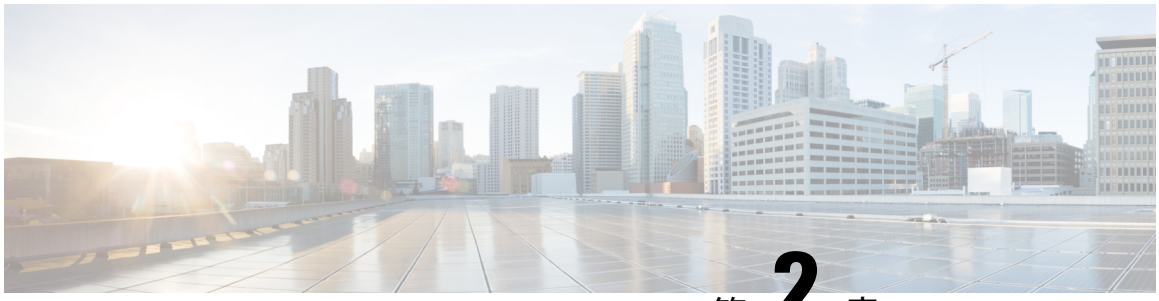
ステップ 4 Cisco Secure Workload は、適用エージェントに感染したワークロードの隔離要求を送信することで、感染したワークロードをすばやく封じ込めます。

前提条件

- 「quarantine」という注釈が付けられたホストに出入りするすべてのトラフィックをドロップするために、Cisco Secure Workload で絶対ポリシーを事前定義します。部分隔離が必要な場合は、Cisco Secure Workload でポリシーをカスタマイズして、すべてではなく一部のタイプのトラフィックのみ拒否するようにします。詳細については、関連資料 （3 ページ）を参照してください。
- Cisco Secure Workload エージェントは、Linux、Windows などのホスト オペレーティング システム内で実行されるソフトウェアです。エンフォースメントエージェントとして、インストールされているホストに対してファイアウォール ルールを設定する機能があります。保護するネットワーク ホストに、エンフォースメント エージェントをインストールします。詳細については、関連資料 （3 ページ）を参照してください。

関連資料

- Cisco Secure Firewall Management Center 設定ガイド
- Cisco Secure Workload Web インターフェイスから入手できるユーザーガイド。
- Cisco Secure Workload ドキュメント



第 2 章

修復モジュールのダウンロードとインストール

次のセクションでは、Cisco Secure Workload（旧 Cisco Tetration）向け FMC 修復モジュールをダウンロードしてインストールする手順について説明します。

修復モジュールのインストール

ステップ 1 Web ブラウザを使用して、この修復モジュールをダウンロードします。
https://software.cisco.com/download/home/286259687/type

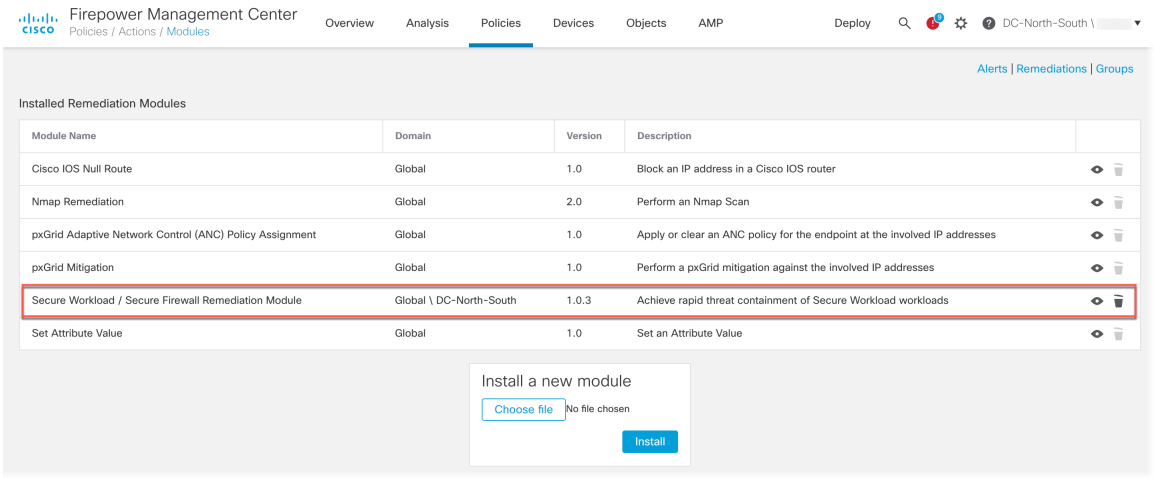
ステップ 2 FMC にこの修復モジュールをインストールします。

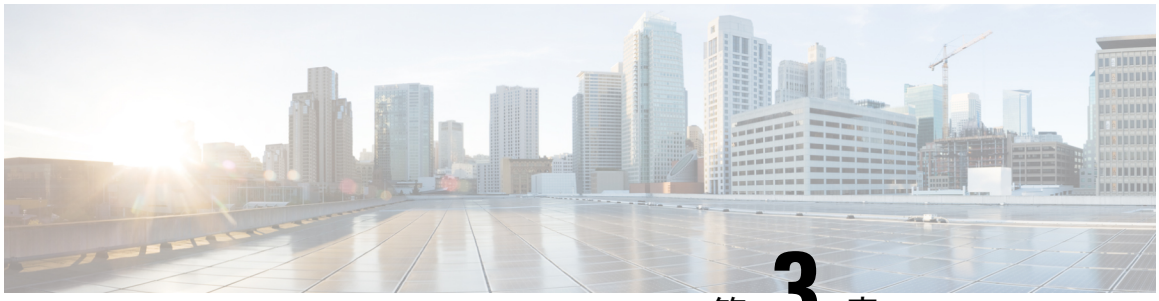
1. FMC Web インターフェイスで、[ポリシー（Policies）] > [アクション（Actions）] > [モジュール（Modules）] に移動します。
2. [新しいモジュールのインストール（Install a new module）] ダイアログボックスで、[ファイルの選択（Choose File）] をクリックします。
3. ステップ 1 でダウンロードした修復モジュールのファイルを選択します。
4. [Install（インストール）] をクリックします。

   （注） アクセス エラーメッセージを受信した場合、エラー メッセージをクリアし、ステップ 2 を繰り返します。

インストールが成功すると、インストールされている修復モジュールの一覧に Cisco Secure Workload 向け Cisco Secure Firewall Management Center 修復モジュールが表示されます。

修復モジュールのインストール





第 3 章

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。

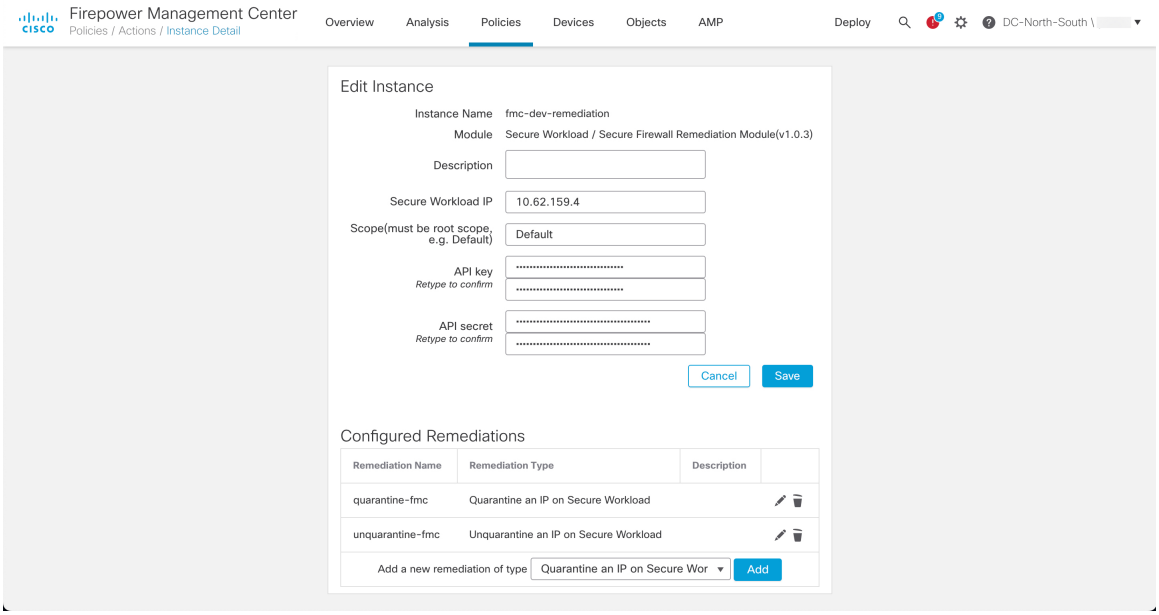
設定（Configure）

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。

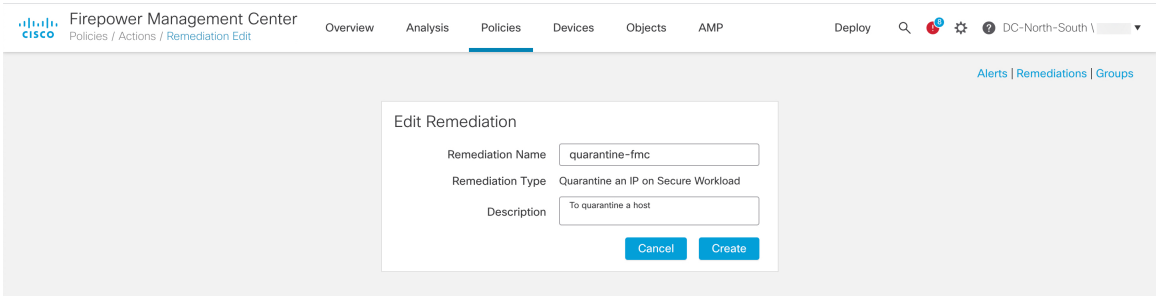
ステップ 1 FMC で、ネットワーク内の Cisco Secure Workload クラスタごとに修復モジュールのインスタンスを作成します。

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 （3 ページ）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。



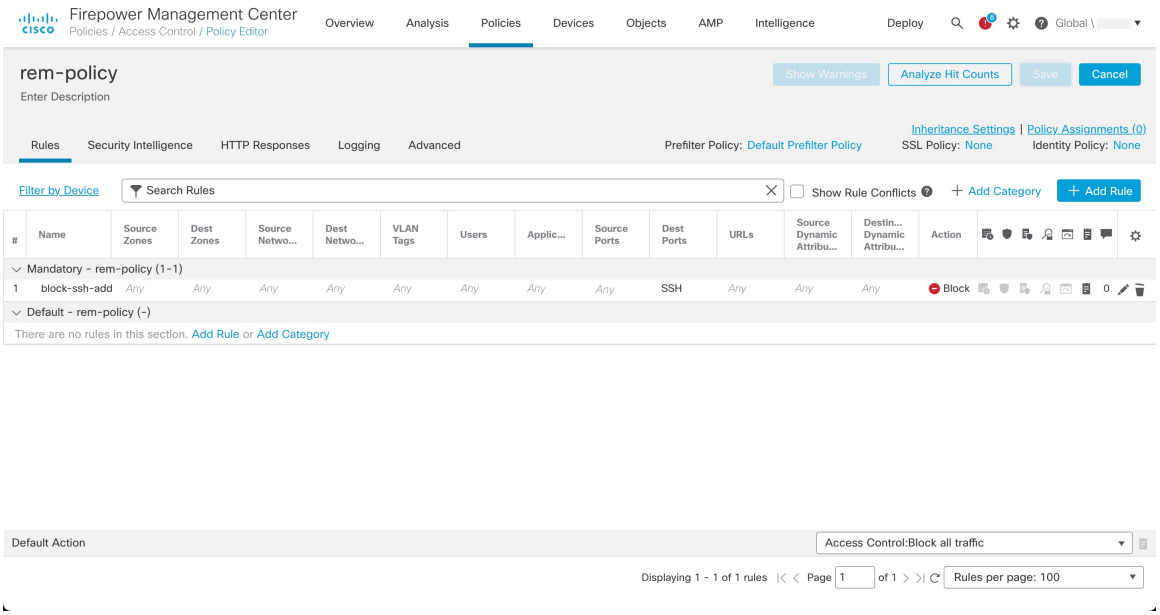
7. 設定した修復がテーブルに表示されます。[保存（Save）] をクリックします。

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。

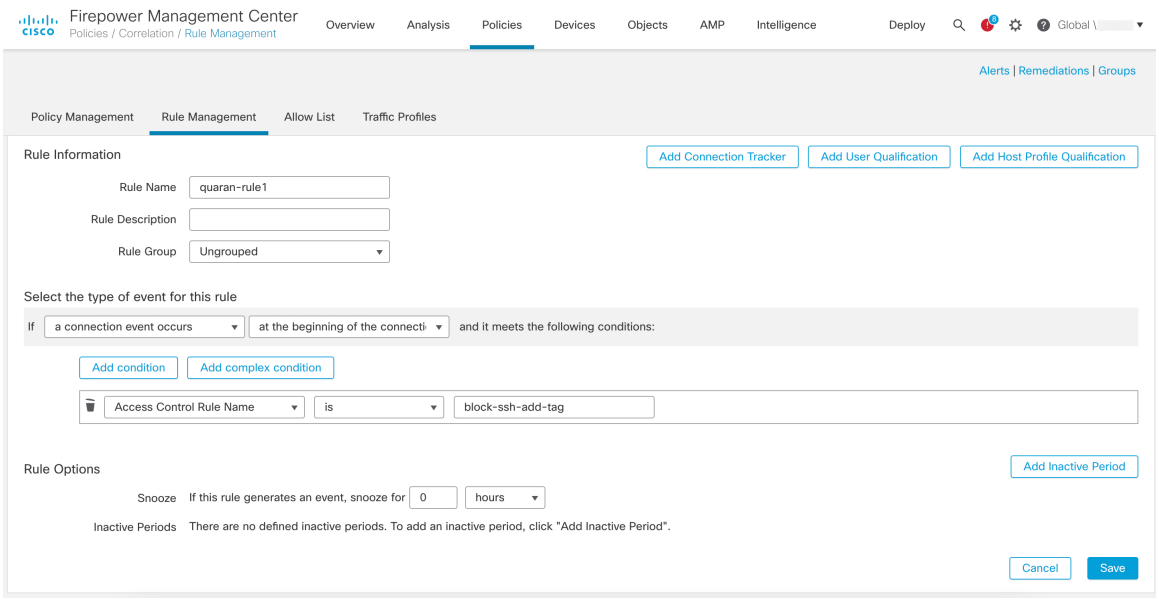
   重要 アクセスルールでロギングが有効になっていることを確認します。これにより、FMC はイベント通知を受信します。確認したら [追加（Add）] をクリックします。

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。

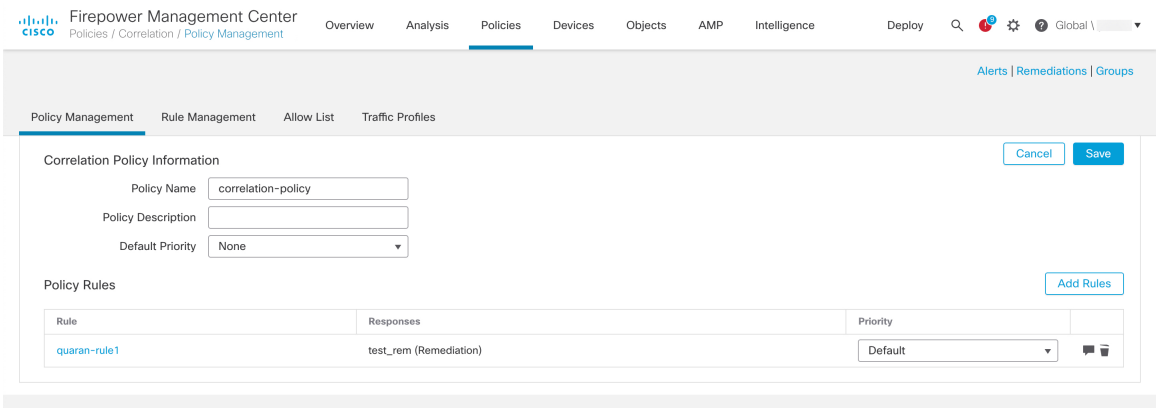
1. [ポリシー（Policies）] > [相関（Correlation）] > [ルールの管理（Rule Management）] に移動します。
2. [ルールの作成（Create Rule）] をクリックします。
3. [ルール名（Rule Name）] を入力し（この例では、**`quaran-rule1`**）、説明（オプション）を入力します。
4. [このルールのイベントタイプの選択（Select the type of event for this rule）] セクションで、[接続イベントの発生（a connection event occurs）] および [接続の開始時または終了時（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`**）。



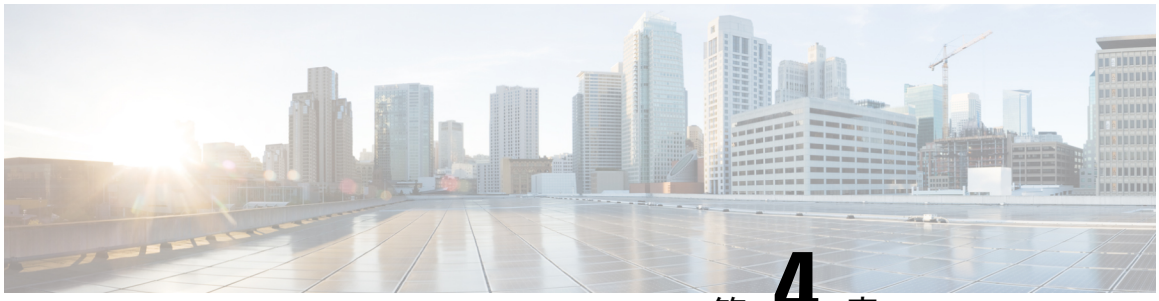
7. [保存（Save）] をクリックします。

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。



第 4 章

修復の検証

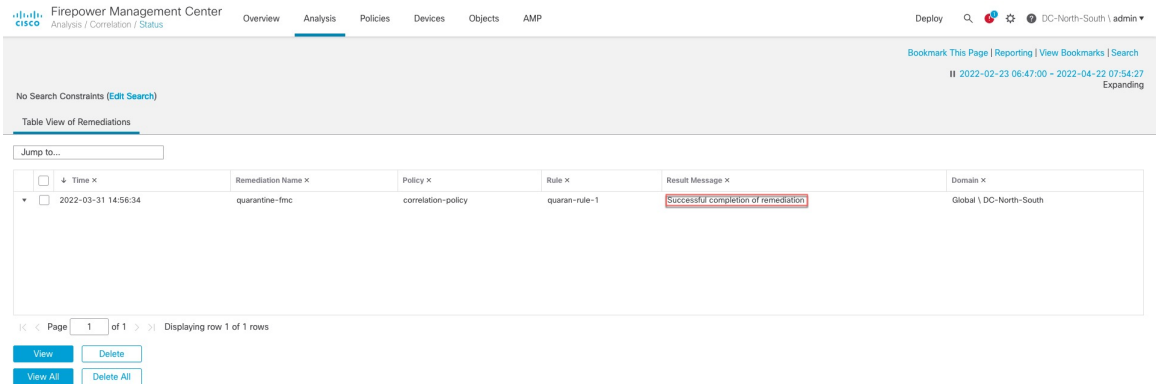
次のセクションでは、修復プロセスが成功したかどうかを確認する手順について説明します。

修復の検証

修復はさまざまな理由で失敗することがあるため、次の手順を実行して、修復が成功したことを確認します。

ステップ 1 修復モジュールが関連付けられている相関ルールによってトリガーされた後、修復実行のステータスを確認します。FMC Web インターフェイスで、[分析（Analysis）]>[相関（Correlation）]>[ステータス（Status）] に移動します。

ステップ 2 [修復ステータス（Remediation Status）] テーブルで、ポリシーの行を見つけ、結果のメッセージを確認します。

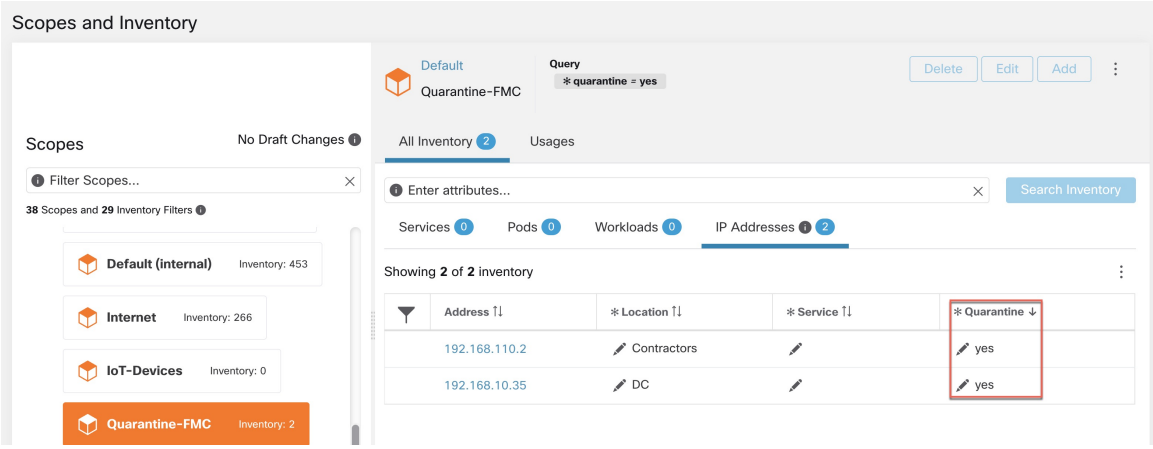


ステップ 3 修復が完了したら、次の手順を実行します。

1. Cisco Secure Workload ユーザーインターフェイスで、[可視性（Visibility）]>[インベントリ検索（Inventory Search）] に移動します。
2. 感染したホストの IP アドレスを入力し、[検索（Search）] をクリックします。

修復の検証

3. [ユーザー注釈（User Annotations）] で、感染したホストの IP アドレスに「**quarantine = yes**」という注釈が付けられていることを確認します。



次のタスク

隔離されたホストをクリーンアップし、感染がなくなったら、次のいずれかのアクションを実行して隔離の注釈を削除できます。

- （**推奨**）Secure Workload を使用して、「**quarantine = yes**」という注釈を「**quarantine = no**」に戻します。

  1. たとえば、感染がなくなった隔離されたホストが 172.21.208.11 で、デフォルトの範囲内であれば、次のような CSV ファイルを作成します。

     ```
     IP,VRF,quarantine
     172.21.208.11,Default,no
     ```

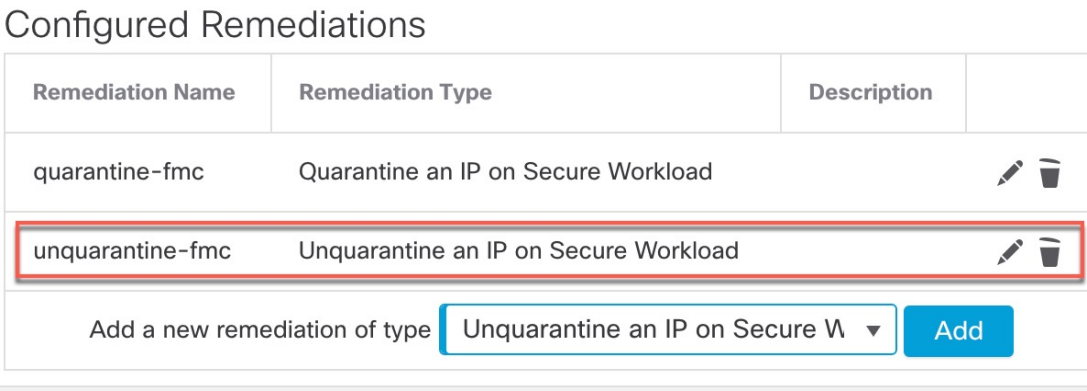
  2. **[アプリケーション（Applications）]>[インベントリアップロード（Inventory Upload）]** に移動し、Cisco Secure Workload に CSV ファイルをアップロードします。Cisco Secure Workload に CSV ファイルをアップロードする方法の詳細については、関連資料 （3 ページ） のセクションを参照してください。

- FMC 修復モジュールを使用して隔離の注釈を削除します。

重要 この方法は、セキュリティ上の懸念から、実稼働ネットワークでは推奨されません。

1. （「設定」セクションのステップ 1 を参照）隔離解除タイプの修復を使用する新しい修復を追加します。同じインスタンスを編集し、[設定されている修復（Configured Remediations）] で隔離解除タイプの修復（この例では **unquarantine-fmc**）を選択して追加します。

修復の検証



2. （「設定」セクションのステップ 2 を参照）隔離解除修復をトリガーするために使用できるアクセスコントロールルール（この例では**remove-tag**）を同じポリシー（この例では **rem-policy**）に追加します。
3. （「設定」セクションのステップ 3 を参照）アクセスコントロールルール（この例では **remove-tag**）を使用する相関ルール（この例では **unquaran-rule1**）を追加します。
4. （「設定」セクションのステップ 4ß を参照）隔離解除応答（この例では **un-quaran-rem**）を相関ルール（この例では**unquaran-rule1**）に割り当てます。
5. このルールに一致すると、隔離解除修復がトリガーされ、隔離の注釈が削除されます。

修復の検証

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。