



Cisco Firepower Management Center Remediation Module for Tetration バージョン 1.0.1 クイック スタート ガイド

初版 : 2018 年 8 月 1 日

最終更新 : 2018 年 8 月 20 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/>



第 1 章

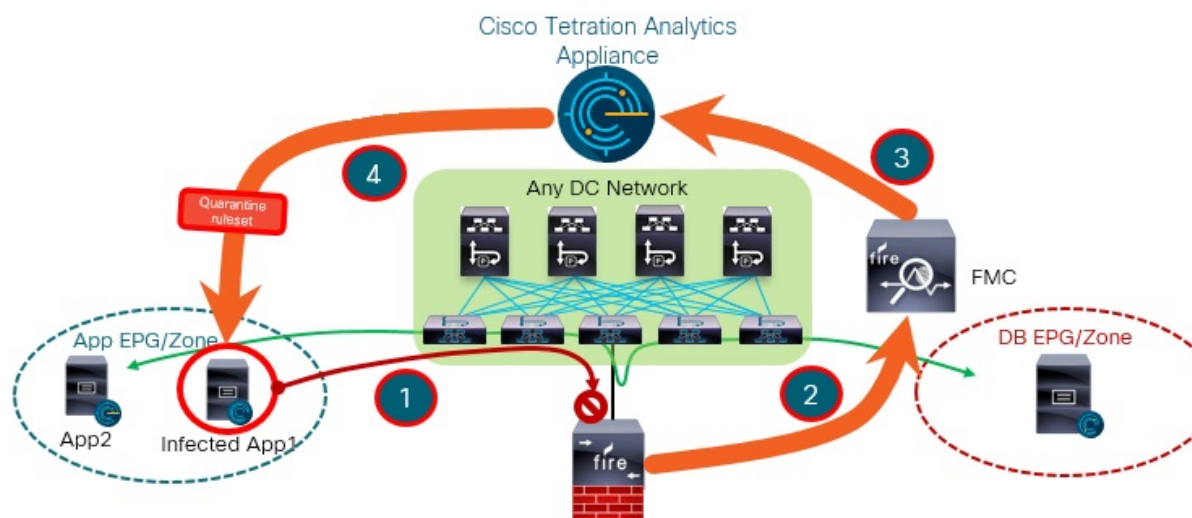
はじめに

- 概要 (1 ページ)
- 前提条件 (2 ページ)
- 関連資料 (2 ページ)

概要

Cisco Firepower Management Center (FMC) Remediation Module for Tetration を使用すると、感染したホストからネットワークへの攻撃が FMC によって検出された場合に、Tetration Analytics (TA) エンフォースメント エージェントによって問題のあるホストを隔離でき、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 Tetration の関係を示しています。

FMC to Tetration Rapid Threat Containment



この図は、ネットワーク攻撃を隔離する全体的なプロセスも示しています。

-
- ステップ 1** 感染したアプリケーションがあるホストは、ネットワークへの攻撃を開始します。攻撃は、Firepower デバイス（物理または仮想）で実行されている Cisco Firepower Threat Defense (FTD) によってインラインでブロックされます。
- ステップ 2** 感染に関する情報を含む侵入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** 攻撃によって、FMC 上の修復モジュールがトリガーされ、ノースバウンド API を使用して、感染したホストを隔離するよう Tetration に対して要求が送られます。
- ステップ 4** Tetration は、感染したホスト上のエンフォースメント エージェントに隔離要求を送信することで、感染したアプリケーションのワークロードをすばやく封じ込めます。
-

前提条件

- 「隔離」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、TA で絶対ポリシーを事前定義します。部分隔離を希望する場合は、TA 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、TA GUI で [ユーザ ガイド](#) を参照してください。
- Tetration 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、『[Cisco Tetration Analytics for the Software Agent Installation Guide](#)』を参照してください。

関連資料

- [Firepower Management Center 設定ガイド](#)
- [Cisco Tetration Analytics](#)



第 2 章

インストール (Install)

・インストール (3 ページ)

インストール

Cisco Firepower Management Center Remediation Module for Tetration をダウンロードしてインストールするには、次の手順を実行します。

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 GUI 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. 以下に示されているように、[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、Cisco Firepower Management Center Remediation Module for Tetration が、インストールされている修復モジュールの一覧に表示されます。

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Display', 'System', 'Help', and 'admin'. Below this, a secondary navigation bar shows 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions > Modules'. Under 'Actions > Modules', there are sub-tabs for 'Alerts', 'Remediations', and 'Groups'. The main content area is titled 'Installed Remediation Modules' and contains a table with the following data:

Module Name	Version	Description
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Nmap Remediation	2.0	Perform an Nmap Scan
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses
Set Attribute Value	1.0	Set an Attribute Value
Tetration/FirePOWER Remediation Module	1.0.1	Achieve rapid threat containment of Tetration workloads

Below the table, a modal dialog titled 'Install a new module' is open. It contains a file selection field with the text 'Choose File' and 'No file chosen', and an 'Install' button.



第 3 章

設定 (Configure)

• 設定 (5 ページ)

設定

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、FMC GUI で次の手順を実行します。

ステップ 1 ネットワーク内の Tetration Analytics (TA) サーバ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。

The screenshot shows the Cisco FMC GUI interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies' (selected), 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and 'System'. Below this, there are sub-tabs: 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', 'Actions', and 'Instances' (selected). The main content area is titled 'Configured Instances' and contains a table with columns 'Instance Name', 'Module Name', and 'Version'. The table is currently empty, with the text 'No instances configured' displayed below it. Below the table, there is a section titled 'Add a New Instance' with a dropdown menu labeled 'Select a module type' showing 'Tetration/FirePOWER Remediation Module(v1.0.1)' and an 'Add' button.

3. [インスタンス名 (Instance Name)] を入力します (この例では、**rem-instance**) 。

4. TA サーバの IP アドレス、API キー、API シークレット、および問題の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 TA サーバ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 TA 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、『[TA API Configuration Guide](#)』を参照してください。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System

Access Control ▾ Network Discovery Application Detectors Correlation **Actions ▶ Instance**

Alerts Remediations

✔ Success ✕
 Created new instance rem-instance

Edit Instance

Instance Name: rem-instance

Module: Tetration/FirePOWER Remediation Module(v1.0.1)

Description:

Tetration Analytics IP:

Scope(e.g. Default):

API key
Retype to confirm:

API secret
Retype to confirm:

Configured Remediations

Remediation Name	Remediation Type	Description
No configured remediations available		

Add a new remediation of type

5. [設定されている修復 (Configured Remediations)]で、修復のタイプを選択し (この例では、**Quarantine an IP on Tetration Analytics**)、[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)] を入力し (この例では、**quaran-rem**)、[作成 (Create)] をクリックします。

The screenshot shows the 'Edit Remediation' form in the Cisco Firepower Management Center Remediation Module for Tetration. The navigation bar at the top includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and 'System'. Below this, there are sub-menus for 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions > Instances'. The main form area is titled 'Edit Remediation' and contains the following fields:

- Remediation Name:** A text input field containing 'quaran-rem'.
- Remediation Type:** A dropdown menu with the selected option 'Quarantine an IP on Tetration Analytics'.
- Description:** A text area containing the text 'To quarantine a host'.

At the bottom of the form, there are two buttons: 'Create' and 'Cancel'.

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。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System

Access Control ▾ Network Discovery Application Detectors Correlation **Actions ▶ Instance**

Alerts Remediations Group

Edit Instance

Instance Name rem-instance

Module Tetration/FirePOWER Remediation Module(v1.0.1)

Description

Tetration Analytics IP 172.26.46.68

Scope(e.g. Default) SBG

API key
Retype to confirm

API secret
Retype to confirm

Save Cancel

Configured Remediations

Remediation Name	Remediation Type	Description
quaran-rem	Quarantine an IP on Tetration Analytics	To quarantine a host

Add a new remediation of type Unquarantine an IP on Tetration Analytics ▾ Add

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)] > [ルール (Rules)] に移動します。
2. [ルールの追加 (Add Rule)] をクリックします（たとえば、**block-ssh-add-tag**）。
3. [アクション (Action)] で [ブロック (Block)] を選択します。

- [ポート (Ports)] タブで、宛先ポートのプロトコルの一覧から [SSH] を選択し、[追加 (Add)] をクリックします。
- [保存 (Save)] をクリックします。
- [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。
- [保存 (Save)] をクリックします。

The screenshot shows the FMC interface for configuring a policy named 'rem-policy'. The 'Rules' tab is active, showing a table of rules. The table has columns for #, Name, Source Zones, Dest Zones, Source..., Dest..., VLAN Tags, Users, Apps, Source Ports, Dest Ports, URLs, ISE/..., and Action. The rules listed are:

#	Name	Source Zones	Dest Zones	Source...	Dest...	VLAN Tags	Users	Apps	Source Ports	Dest Ports	URLs	ISE/...	Action
▼ Mandatory - rem-policy (1-2)													
1	remove-tag	external-zone internal-zone	internal-zone external-zone	Any	Any	Any	Any	Any	Any	TCP (6):500C	Any	Any	Allow
2	block-ssh-add-tag	external-zone internal-zone	internal-zone external-zone	Any	Any	Any	Any	Any	Any	SSH	Any	Any	Block
▼ Default - rem-policy (3-3)													
3	allow-any	external-zone internal-zone	internal-zone external-zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow

ステップ3 関連ルールを設定します。

- [ポリシー (Policies)] > [関連 (Correlation)] > [ルールの管理 (Rule Management)] に移動します。
- [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。
- [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。
- [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。
- 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名を入力します (この例では、**block-ssh-add-tag**) 。

The screenshot displays the 'Policies' section of the Cisco Firepower Management Center Remediation Module for Tetration. The 'Rule Management' tab is active, showing the configuration for a new rule named 'quaran-rule1'. The rule description is 'add tag' and it is currently ungrouped. The event type is set to 'a connection event occurs' at 'either the beginning or the end of the connection'. A condition is added: 'Access Control Rule Name' is 'block-ssh-add-tag'. The rule options include a snooze duration of 0 hours and no inactive periods defined.

Rule Information

Rule Name:

Rule Description:

Rule Group:

Select the type of event for this rule

If at either the beginning or the end of the connection and it meets the following conditions:

is

Rule Options

Snooze: If this rule generates an event, snooze for hours

Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

6. [保存 (Save)] をクリックします。

ステップ 4 関連ルールに、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. [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. [ルール追加 (Add Rules)] をクリックし、ステップ3で設定した関連ルールを選択し (この例では、**quaran-rule1**)、[追加 (Add)] をクリックします。

The screenshot shows the 'Policies' configuration page. The 'Correlation Policy Information' section contains the following details:

- Policy Name: correlation-policy
- Policy Description: correlation policy for testing
- Default Priority: None

The 'Policy Rules' section displays a table with the following data:

Rule	Responses	Priority
<u>quaran-rule1</u> add tag	This rule does not have any responses.	Default

6. ルールの横にある [応答 (Responses)] アイコンをクリックし、ルールに応答を割り当てます (この例では、**quaran-rem**)。[更新 (Update)] をクリックします。

The screenshot shows the 'Policies' configuration page. The 'Correlation Policy Information' section contains the following details:

- Policy Name: correlation-policy
- Policy Description: correlation policy for testing
- Default Priority: None

The 'Policy Rules' section displays a table with the following data:

Rule	Responses	Priority
<u>quaran-rule1</u> add tag	quaran-rem (Remediation)	Default

7. [保存 (Save)]をクリックします。
-



第 4 章

検証

- 検証 (15 ページ)

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、FMC GUI で修復実行のステータスを確認します。
- ステップ 2** [分析 (Analysis)]> [相関 (Correlation)]> [ステータス (Status)]に移動します。
- ステップ 3** [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。

Overview **Analysis** Policies Devices Objects AMP Intelligence Deploy System Help ▾

Context Explorer Connections ▾ Intrusions ▾ Files ▾ Hosts ▾ Users ▾ Vulnerabilities ▾ **Correlation ▸ Status** Custom ▾ Lookup ▾

Remediation Status

Table View of Remediations 2018-07-28 01:22:27 - 2018-07-28 02:41:29 Expanding

No Search Constraints ([Edit Search](#))

Jump to... ▾

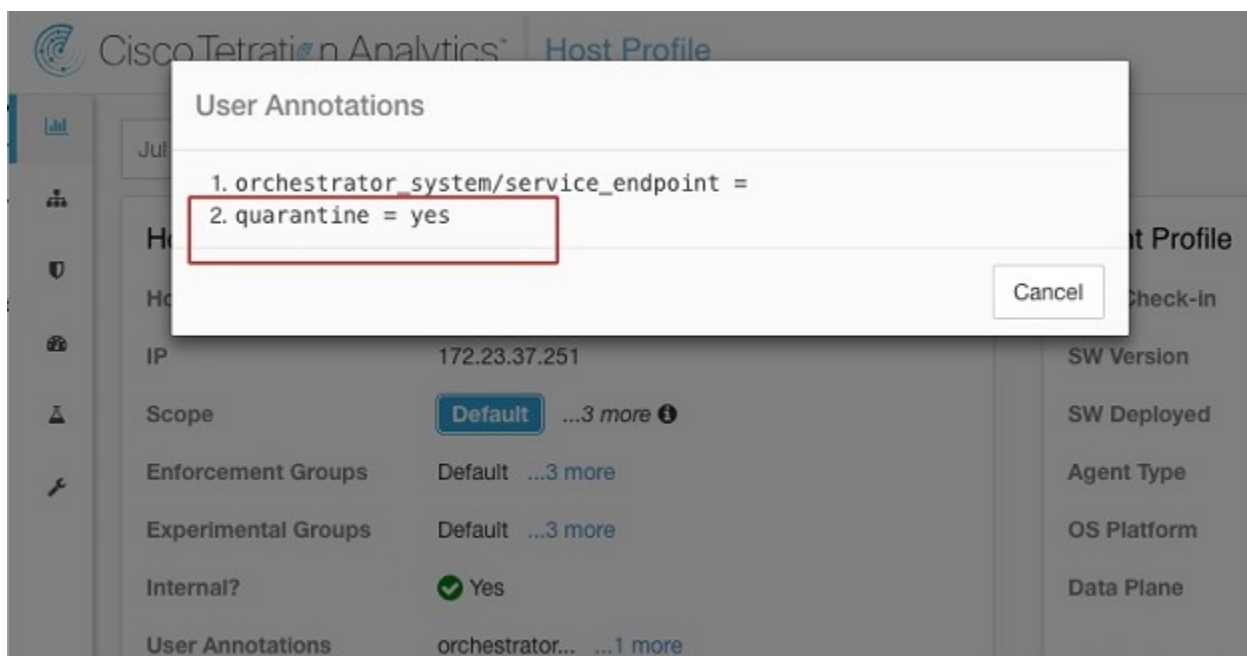
Time ×	Remediation Name ×	Policy ×	Rule ×	Result Message ×
2018-07-28 02:26:09	guaran-rem	correlation-policy	guaran-rule1	Successful completion of remediation

Page 1 of 1 | Displaying row 1 of 1 rows

View Delete

- ステップ 4** 修復が完了した後、TA GUI に移動します。
1. [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。

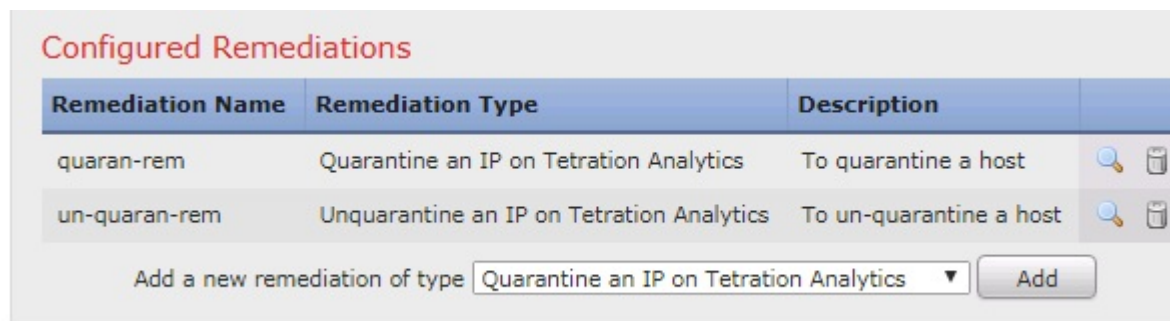
3. [ユーザ注釈 (User Annotations)] で、感染したホストの IP アドレスに **quarantine = yes** という注釈が付けられていることを確認します。



次のタスク

隔離されたホストをクリーンにし、感染がなくなった後、TA GUI (推奨) を使用して **quarantine = yes** という注釈を **quarantine = no** に変更するか、または FMC 修復モジュールを使用して次のように隔離を解除します (セキュリティの問題のため、実稼働ネットワークでは非推奨)。

- (「設定: 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を選択し、追加します (この例では、**un-quaran-rem**)。



- (「設定：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。
- (「設定：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。
- (「設定：ステップ 4」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。

Policy Rules

Rule	Responses
<u>quaran-rule1</u> add tag	quaran-rem (Remediation)
<u>unquaran-rule1</u> removing tag	un-quaran-rem (Remediation)

- このルールに一致すると、隔離解除修復がトリガーされ、隔離注釈が削除されます。

