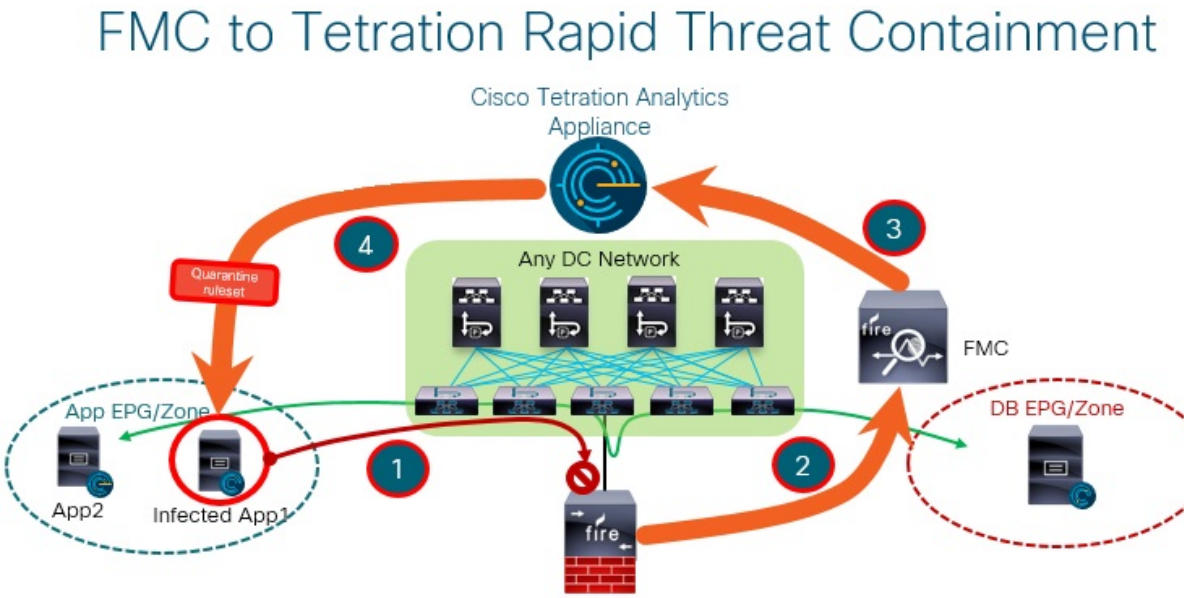
はじめに

- 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。



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