はじめに

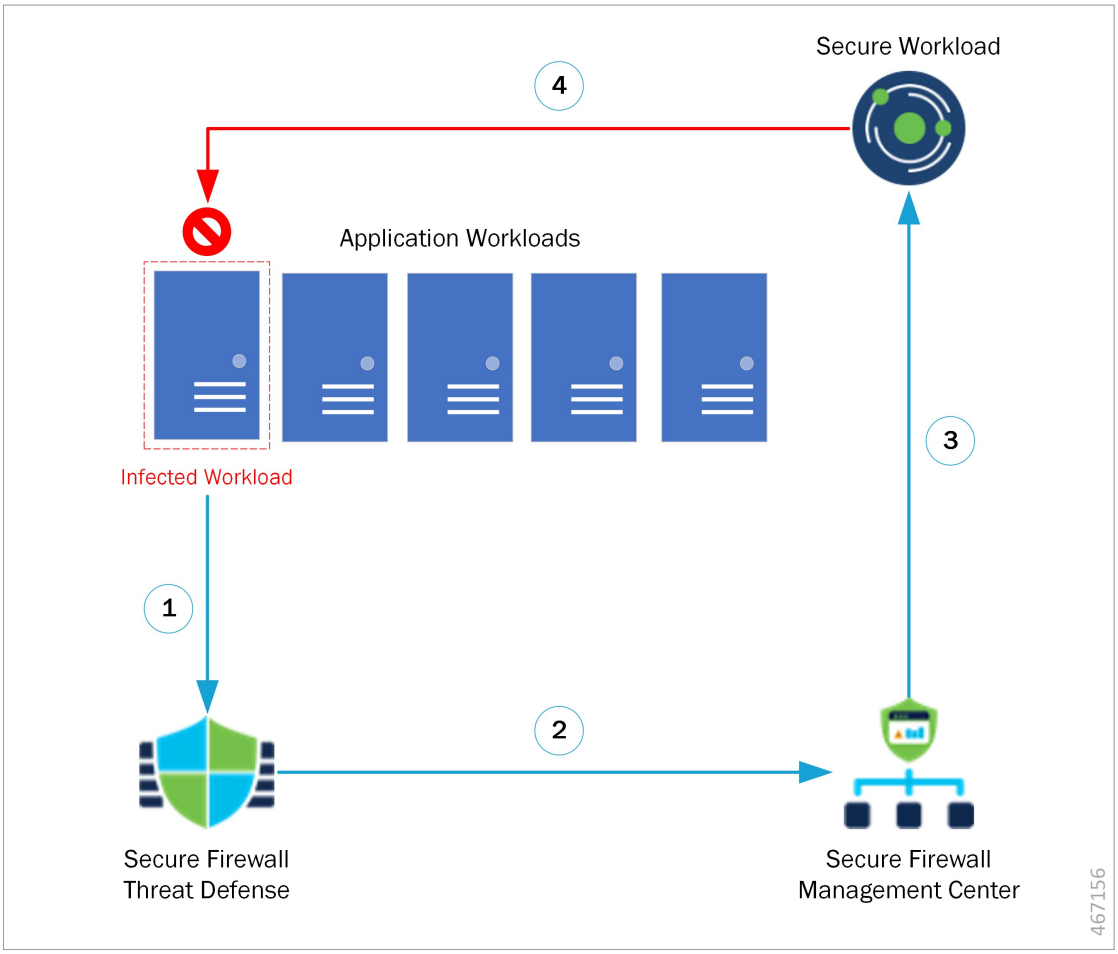
Cisco Secure Workload（旧 Cisco Tetration）向け Cisco Secure Firewall Management Center 修復モジュールは、ネットワークの状況が関連する相関ポリシーに違反したときに Cisco Secure Firewall Management Center を自動的に起動する修復を作成するのに役立ちます。たとえば、ホストの状況を評価し、Cisco Secure Workload 適用エージェントで問題のあるホストを隔離するために、送信元または宛先 IP アドレスのデバイスでトラフィックをブロックできます。ポリシー内の複数のルールが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 （1 ページ）
- 前提条件 （3 ページ）
- 関連資料 （3 ページ）

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

関連資料

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。