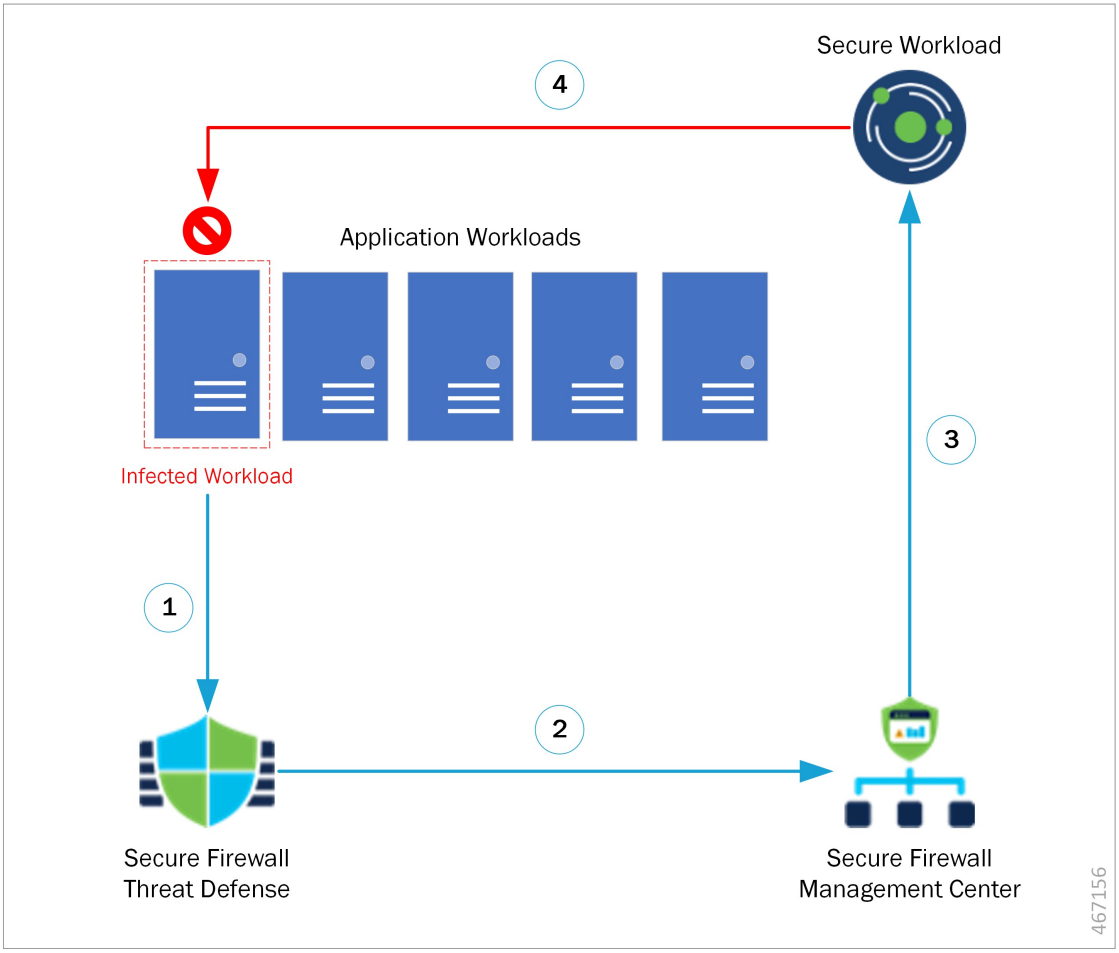
Introduction

The Cisco Secure Firewall Management Center remediation module for Cisco Secure Workload (formerly known as Tetration) helps to create remediations that your Secure Firewall Management Center can automatically launch when conditions on your network violate the associated correlation policy. For example, to assess the host status, and quarantine an offending host with the Secure Workload enforcement agent, you can block traffic at a device on the source or destination IP address. If multiple rules in a policy trigger, the Secure Firewall Management Center can launch responses for each rule. A remediation module is the package of files you install on the Secure Firewall Management Center to perform the response.

Overview

With the Cisco Secure Firewall Management Center (FMC) Remediation Module for Cisco Secure Workload (formerly known as Tetration), when an attack on your network from an infected host is detected by the FMC, the offending host can be quarantined by a Secure Workload enforcement agent so that no further traffic is allowed to go in or out of that host. The following illustration shows the relationship between the FMC and Secure Workload when the remediation module is installed:

Figure 1: Secure Firewall Management Center to Secure Workload Rapid Threat Containment



1	Threat Defense detects malicious traffic from infected workload.
2	Threat Defense sends an event with malicious traffic details to the Management Center.
3	Remediation module is triggered to quarantine infected workload.
4	Secure Workload sends quarantine request to the enforcement agent on workload.

The process of quarantining the network attack is as follows:

Step 1 An infected workload sends malicious traffic within the network. The malicious traffic is detected by Secure Firewall Threat Defense (FTD) running on a Secure Firewall device (physical or virtual).

Step 2 An event that includes information about the malicious traffic is generated and reported to the FMC managing the FTD.

Step 3 The action triggers the remediation module on the FMC to use the Secure Workload REST API to request that Secure Workload quarantine the infected workload.

Step 4 Secure Workload quickly contains the infected workload by sending a quarantine request to the enforcement agent on the infected workload.

Prerequisites

- Pre-define absolute policies in Secure Workload to drop all traffic from and to any host annotated with 'quarantine.' If a partial quarantine is what you want, customize the policy in Secure Workload to deny only some, but not all, types of traffic. For more information, see Related Documentation, on page 3.
- Secure Workload agents are software that runs within a host operating system, such as Linux or Windows. As enforcement agents, they have the capability to set firewall rules on installed hosts. Install enforcement agents on network hosts you want to protect. For more information, see Related Documentation, on page 3.

Related Documentation

- Secure Firewall Management Center Configuration Guides
- The user guide available from the Secure Workload web interface.
- Cisco Secure Workload Documentation