About the Remediation Module

About the Remediation Module

With the APIC/Secure Firewall Remediation Module, when an attack on your network is detected by the Management Center, the offending endpoint can be completely quarantined in the Application Policy Infrastructure Controller (APIC) so that no further traffic is allowed to go in or out of that endpoint. The following figure shows the relationship between the Management Center and the APIC when the remediation module is installed.

Compatibility

The following table shows the compatibility between the APIC/Secure Firewall Remediation Module, Management Center, and APIC.

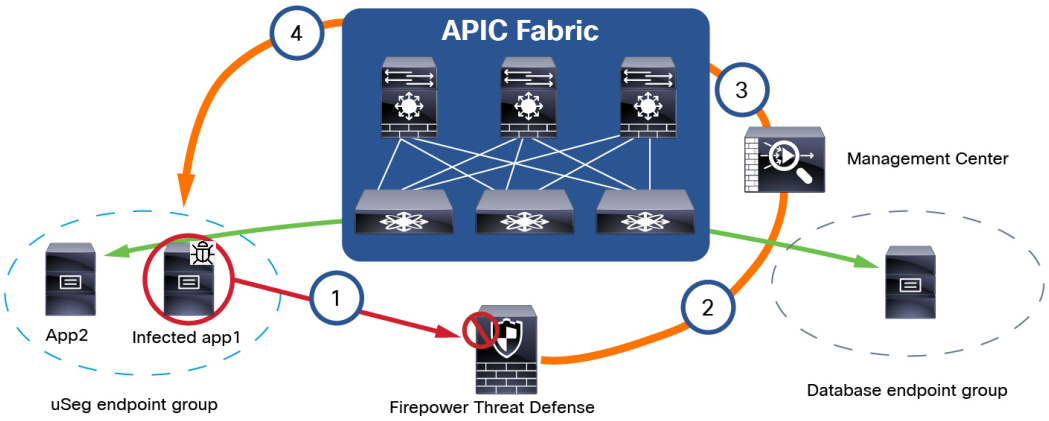
Table 1: Compatibility with the remediation module, Management Center and APIC

Remediation module version compatible with....	Management Center version	APIC version
2.0.2	7.0 and later	5.1(1h)

Infected endpoint

The following figure shows how the APIC/Secure Firewall Remediation Module reacts when an infected endpoint is detected.

About the Remediation Module



The process is as follows:

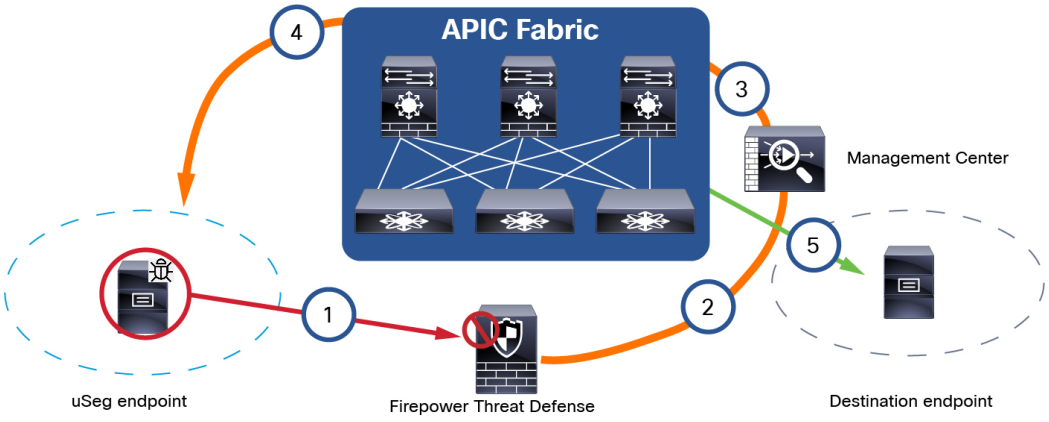
1. An endpoint with an infected application in an endpoint group (endpoint group on the left) launches an attack on another endpoint in Database EPG. The attack is blocked inline by a managed device (such as a physical or virtual device running Firepower Threat Defense).
2. An attack event is generated and sent to the Management Center. The attack event includes information about the infected endpoint.
3. The attack event triggers the remediation module for APIC, which used the APIC northbound (NB) API to contain the infected endpoint in the ACI fabric.
4. The APIC quickly contains or quarantines the infected application workload into an isolated microsegment (uSeg) EPG.

   Because App2 is not infected, it can still communicate on the network.

   You can quarantine a source endpoint, a destination endpoint, or both, as the next section shows.

Quarantine source and/or destination endpoints

On detection of an infected endpoint, you can optionally quarantine either the source endpoint, the destination endpoint, or both, as the following figure shows.



The figure shows the following process:

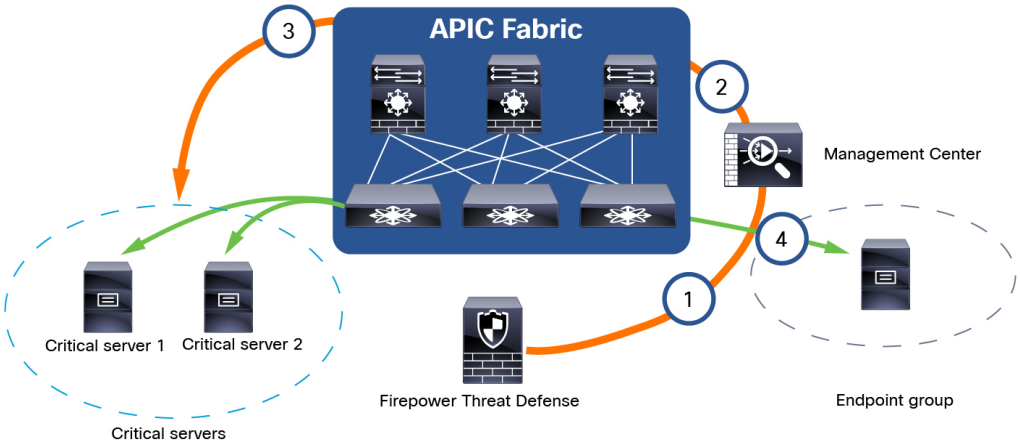
1. An endpoint with an infected application in an endpoint group (EPG) launches an attack on another endpoint in another EPG. The attack is blocked inline by a managed device (such as a physical or virtual device running Firepower Threat Defense).
2. An attack event is generated and sent to the Management Center. The attack event includes information about the infected endpoint.
3. The attack event triggers the remediation module for APIC, which used the APIC northbound (NB) API to contain the infected endpoint in the ACI fabric.
4. The APIC quickly contains or quarantines the infected application workload into an isolated microsegment (uSeg) EPG.
5. Depending on the configuration, the source endpoint can be quarantined, the destination endpoint can be quarantined, or both endpoints can be quarantined.

   The example shown in the figure quarantines the uSeg (source) endpoint but not the destination endpoint.

Always allow traffic to critical servers

You can allow traffic to and from critical servers, even if those servers are passing traffic that could be considered suspicious. *Use this option with caution* but it can be useful in situations where you always want to allow this traffic.

The following figure shows an example.



The figure shows the following process:

1. An endpoint in `Endpoint group` sends traffic to servers designated as `Critical Servers`. (You specify these servers by IP address.)
2. The Management Center ignores this traffic, even if it matches correlation rules.
3. Traffic is always allowed to and from the critical servers in `Endpoint group` and `Critical Servers`, regardless of what the traffic contains.

Supported Features

This release enables you to quarantine offending endpoints that are detected by the APIC/Secure Firewall Remediation Module, using APIC version 5.1(1h). For version 2.0.2 of the remediation module, the supported behavior when endpoints are quarantined is described in the following table:

	VMware Distributed Virtual Switch (DVS)	Bare metal
Verified in IPS inline mode	Yes	Yes
EPG bridge mode	Yes	Yes
EPG routed mode	No	No
Multiple IP to one MAC checking	Yes	Yes
Create only an IP address filter uSeg attribute	No	No
Create both an IP address filter and a MAC address filter uSeg attribute	Yes	Yes
Quarantine source and destination endpoints	Yes	Yes
Apply a predefined management contract to source and destination endpoints	Yes	Yes
Always allow traffic to critical servers	Yes	Yes