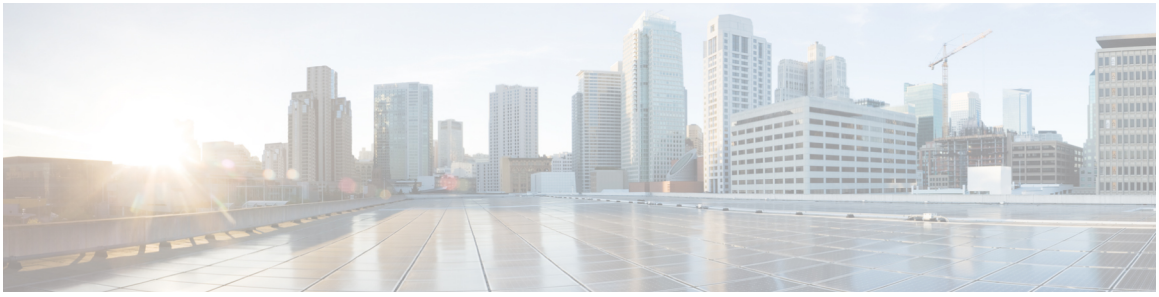


APIC/Secure Firewall Remediation Module 3.0

First Published: 2022-08-23

Last Modified: 2025-09-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 **About the Remediation Module** 1

About the Remediation Module 1

Supported Features 4

CHAPTER 2 **Download and Install the APIC/Secure Firewall Remediation Module** 5

Download and Install the APIC/Secure Firewall Remediation Module 5

CHAPTER 3 **Remediation and Quarantine** 7

The Remediation and Quarantine Process 7

How to Remediate and Quarantine 7

Create an Optional Management Contract and Contract EPG 9

Prerequisites for Creating an Optional Management Contract and Contract EPG 9

Optionally Create a Management Contract and Contract EPG 10

Create a Remediation Module Instance and Type 12

Configure an Access Control Rule for the Remediation 15

Configure a Correlation Rule for the Remediation 17

Associate the Correlation Rule with the Remediation Module Instance 18

Verify the Remediation in the Firewall Management Center 18

Verify the Quarantine in APIC 19

CHAPTER 4 **Manually Quarantine an IP Address** 21

Overview of Manually Quarantining an IP Address 21

Find an IP Address to Quarantine 21

Create a uSeg EPG Attribute 22

Verify the Manual IP Address Quarantine 23

CHAPTER 5 **Related Documentation** 25

Related Documentation 25

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

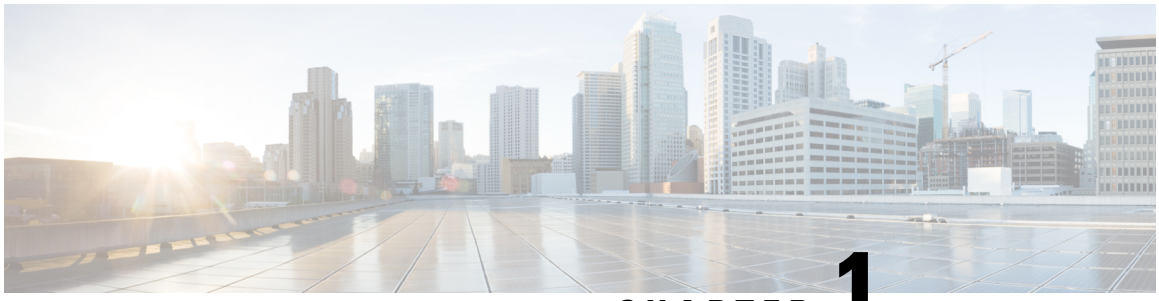
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

About the Remediation Module

- About the Remediation Module, on page 1
- Supported Features, on page 4

About the Remediation Module

With the APIC/Secure Firewall Remediation Module, when an attack on your network is detected by the Firewall 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 Firewall 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, Firewall Management Center, and APIC.

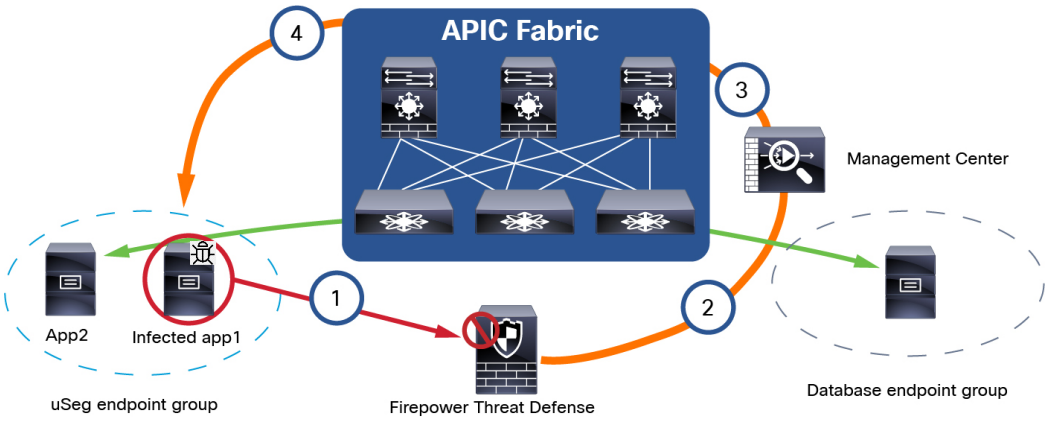
Table 1: Compatibility with the remediation module, Firewall Management Center and APIC

Remediation module version compatible with....	Firewall Management Center version	APIC version
3.0	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:

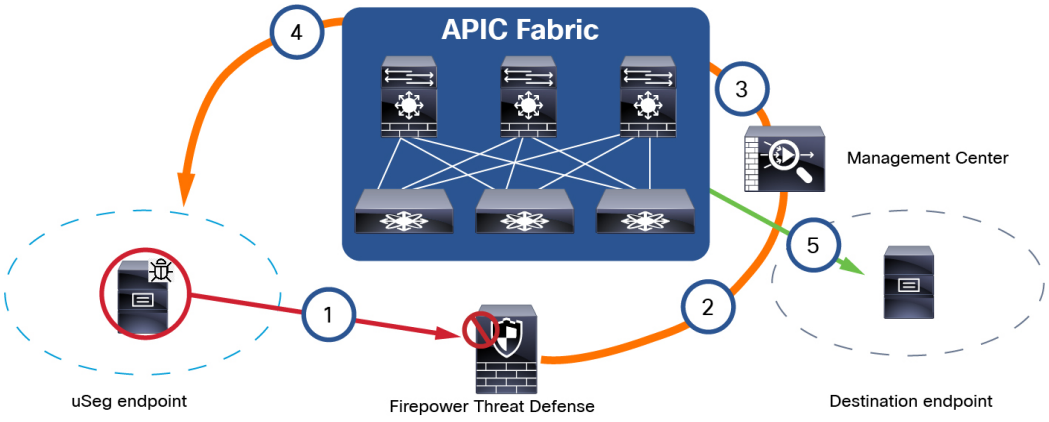
1. An endpoint with an infected application in an endpoint group (endpoint group on the left) launches an attack on another endpoint in Database EPG. The attack is blocked inline by a managed device (such as a physical or virtual device running Firepower Threat Defense).
2. An attack event is generated and sent to the Firewall 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:

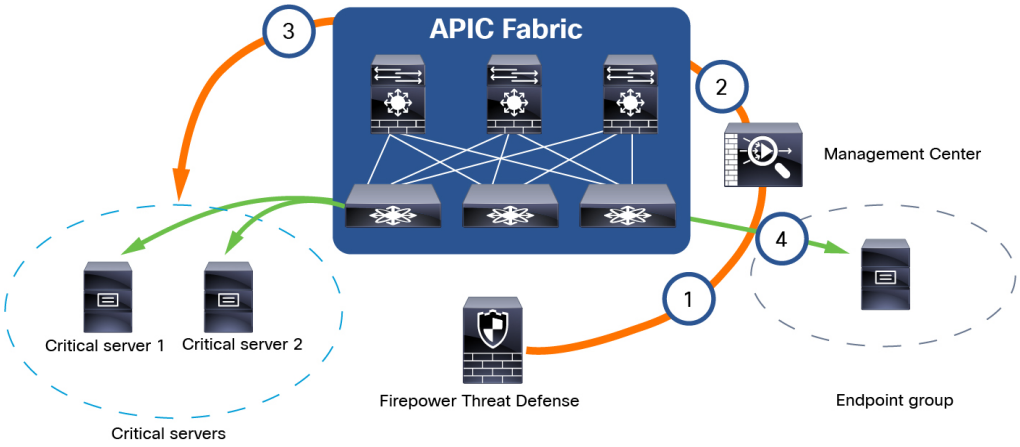
1. An endpoint with an infected application in an endpoint group (EPG) launches an attack on another endpoint in another EPG. The attack is blocked inline by a managed device (such as a physical or virtual device running Firepower Threat Defense).
2. An attack event is generated and sent to the Firewall 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.



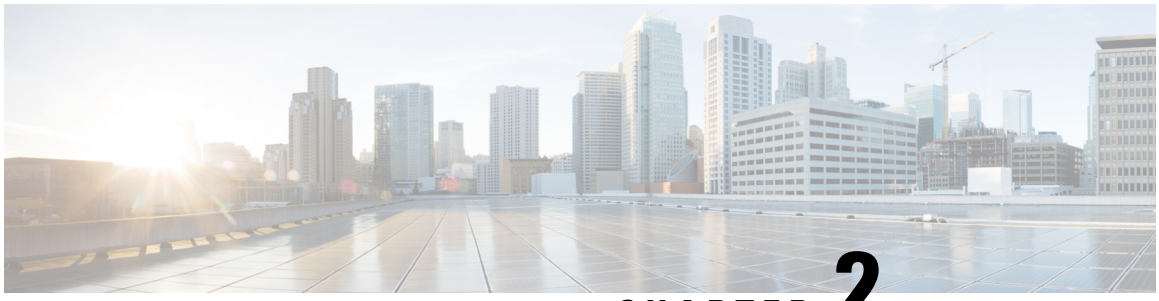
The figure shows the following process:

1. An endpoint in `Endpoint group` sends traffic to servers designated as `Critical Servers`. (You specify these servers by IP address.)
2. The Firewall 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 3.0 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
Allow traffic from a quarantined endpoint to an L3Out endpoint group	Yes	Yes
Allow audit only	Yes	Yes
Always allow traffic to critical servers	Yes	Yes



CHAPTER 2

Download and Install the APIC/Secure Firewall Remediation Module

Download the APIC/Secure Firewall Remediation Module and install it in theSecure Firewall Management Center as discussed in the next section.

• Download and Install the APIC/Secure Firewall Remediation Module, on page 5

Download and Install the APIC/Secure Firewall Remediation Module

Before you begin

Make sure you're using compatible versions as shown in the following table.

Table 2: Compatibility with the remediation module, Firewall Management Center and APIC

Remediation module version compatible with....	Firewall Management Center version	APIC version
3.0	7.0 and later	5.1(1h)

Procedure

Step 1 Download the APIC/Secure Firewall Remediation Module to a machine on which you'll connect to the Firewall Management Center.

- FMC: https://software.cisco.com/download/home/278875421. Choose your model, choose **Firepower Management Center Remediation Modules**, and then choose **ACI**.
- FMCv: https://software.cisco.com/download/home/286259687/type/286311510/release/Tetration. Choose **ACI**

Step 2 If you haven't done so already, log in to the Firewall Management Center.

Step 3 Click **Policies** > **Actions** > **Modules**.

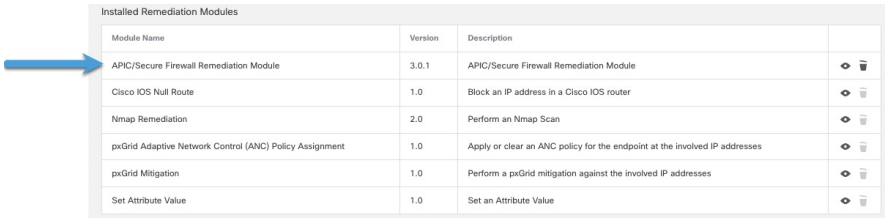
Download and Install the APIC/Secure Firewall Remediation Module

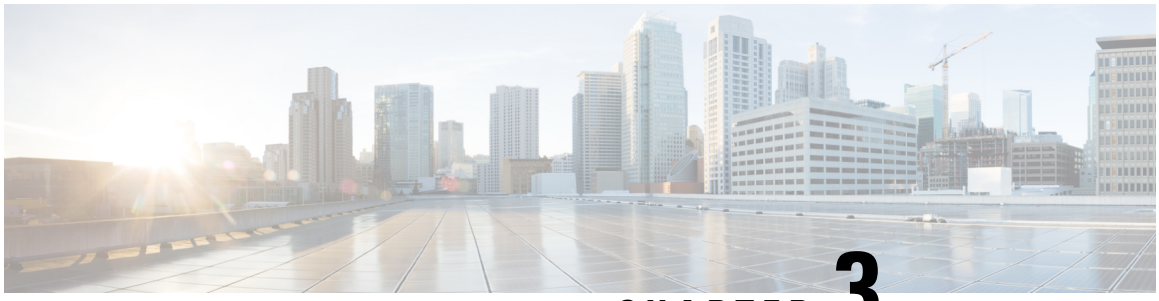
Step 4 In the Install a New Module section, click **Browse**.

Step 5 Follow the prompts to upload the remediation module.

Step 6 Click **Install**.

Step 7 When successfully installed, the APIC/Secure Firewall Remediation Module is displayed in the list of installed remediation modules:





CHAPTER 3

Remediation and Quarantine

This chapter discusses tasks you must perform in APIC and in the Secure Firewall Management Center to create rules to remediate and quarantine an endpoint.

- The Remediation and Quarantine Process, on page 7
- Create an Optional Management Contract and Contract EPG, on page 9
- Create a Remediation Module Instance and Type, on page 12
- Configure an Access Control Rule for the Remediation, on page 15
- Configure a Correlation Rule for the Remediation, on page 17
- Associate the Correlation Rule with the Remediation Module Instance, on page 18
- Verify the Remediation in the Firewall Management Center, on page 18
- Verify the Quarantine in APIC, on page 19

The Remediation and Quarantine Process

Remediation (definining the circumstances under which an endpoint should be quarantined) and *quarantine* (isolating an endpoint so it cannot communicate on the network) is a multi-step process summarized in the next section, How to Remediate and Quarantine, on page 7.

How to Remediate and Quarantine

The following summarizes the tasks required to remediate and quarantine an endpoint. You perform some tasks in APIC and some in the Firewall Management Center.

Before you begin

Consult a reference such as the *Endpoint Groups (EPG) Usage and Design* whitepaper or the *Cisco APIC Basic Configuration Guide* to understand APIC-related concepts.

SUMMARY STEPS

1. Optionally create a management contract and management contract endpoint group (EPG).
2. Create a remediation module instance and type.
3. Configure an access control rule that determines the conditions under which an endpoint should be quarantined.
4. Associate the correlation rule with the remediation policy.

5. Verify the quarantine and remediation.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Optionally create a management contract and management contract endpoint group (EPG).	Perform this task in APIC. APIC uses an allow-list model where we explicitly define what traffic should be permitted. A *contract* is a policy construct used to define communication between EPGs. This optional configuration enables you to initiate a connection to the quarantined uSeg EPG. For more information, see Optionally Create a Management Contract and Contract EPG, on page 10.
Step 2	Create a remediation module instance and type.	Perform this task in the Firewall Management Center. The remediation module creates, on APIC, the EPG that enables you to view and work with quarantined endpoints. The remediation module can: • Quarantine source endpoint, destination endpoint, or both • Reference a management EPG • Audit remediation activity only without triggering remediation or affecting production traffic For more information, see Create a Remediation Module Instance and Type, on page 12.
Step 3	Configure an access control rule that determines the conditions under which an endpoint should be quarantined.	Perform this task in the Firewall Management Center. Determine the conditions under which you want an endpoint quarantined; for example, passing unsecure traffic. Set up an access control rule that in turn triggers the remediation policy you set up previously. For more information, see Configure an Access Control Rule for the Remediation, on page 15.
Step 4	Associate the correlation rule with the remediation policy.	Perform this task in the Firewall Management Center. This triggers the quarantine on APIC. For more information, see Associate the Correlation Rule with the Remediation Module Instance, on page 18.
Step 5	Verify the quarantine and remediation.	Verify the *quarantine* in APIC and verify the *remediation* in the Firewall Management Center.

	Command or Action	Purpose
		For more information, see Verify the Quarantine in APIC, on page 19 and Verify the Remediation in the Firewall Management Center, on page 18.

What to do next

Create an Optional Management Contract and Contract EPG, on page 9

Create an Optional Management Contract and Contract EPG

You can optionally predefine an APIC traffic filtering contract in the common tenant and a management EPG in the mgmt tenant to initiate a connection to the quarantined uSeg EPG. To use this optional configuration, you *must* define a management EPG in APIC in its **mgmt** tenant, and you *must* define a contract in the **common** tenant.

For more information, see the *Cisco APIC Basic Configuration Guide*.

What To Do Next

Prerequisites for Creating an Optional Management Contract and Contract EPG, on page 9.

Prerequisites for Creating an Optional Management Contract and Contract EPG

This task discusses how to do the following before you configure an optional management contract and contract EPG:

- Create an application ESG.
- Create a filter for the quarantine you wish to perform; in this example, the filter is for SSH2 traffic.

Procedure

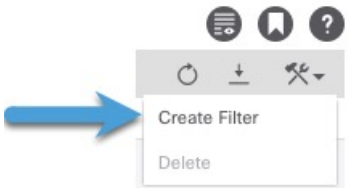
Step 1 Log in to APIC.

Step 2 Click **Tenants**.

Step 3 Double-click **common**.

Step 4 In the left pane, expand **Contracts** > **Filters**.

Step 5 In the right pane, click **Create Filter**.



Step 6 Give the filter a **Name** like **SSHv2**.

Step 7 Click **Submit**.

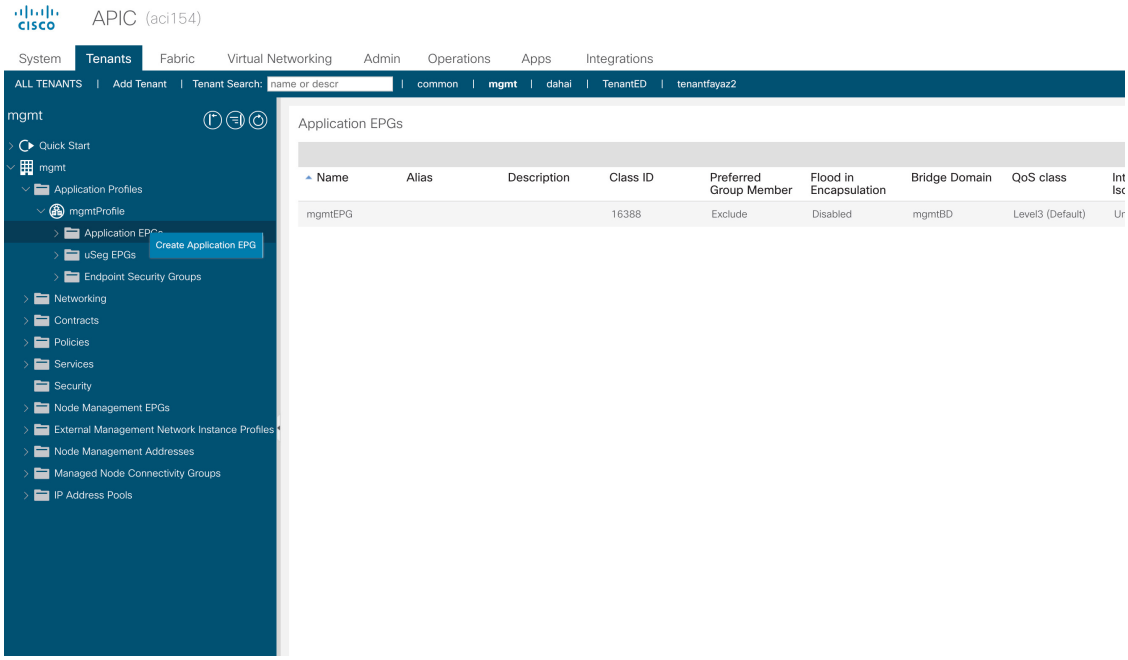
Step 8 In the left pane, click **Tenants** > **ALL TENANTS**.

Step 9 Click **mgmt**.

Step 10 Expand **Application Profiles** > **mgmt profile**.

Step 11 Right-click **Application EPGs** and click **Create Application EPG**.

The following figure shows an example.



Step 12 Give the EPG a **Name**.

Step 13 From the **Bridge Domain** list, click WHICH BRIDGE DOMAIN.

Step 14 Click **Finish**.

What to do next

Optionally Create a Management Contract and Contract EPG, on page 10

Optionally Create a Management Contract and Contract EPG

If you do not wish to create contracts, skip this section and continue with Create a Remediation Module Instance and Type, on page 12.

Procedure

Step 1 Log in to APIC.

Step 2 Click **ALL TENANTS**.

Step 3 Double-click **common**.

Step 4 Expand **Contracts** > **Standard**.

Step 5 Right-click **Standard** and then click **Create Contract**.

Step 6 In the **Name** field, enter **`useg_filter_contract`**.

Step 7 From the **Scope** list, click **Global**.

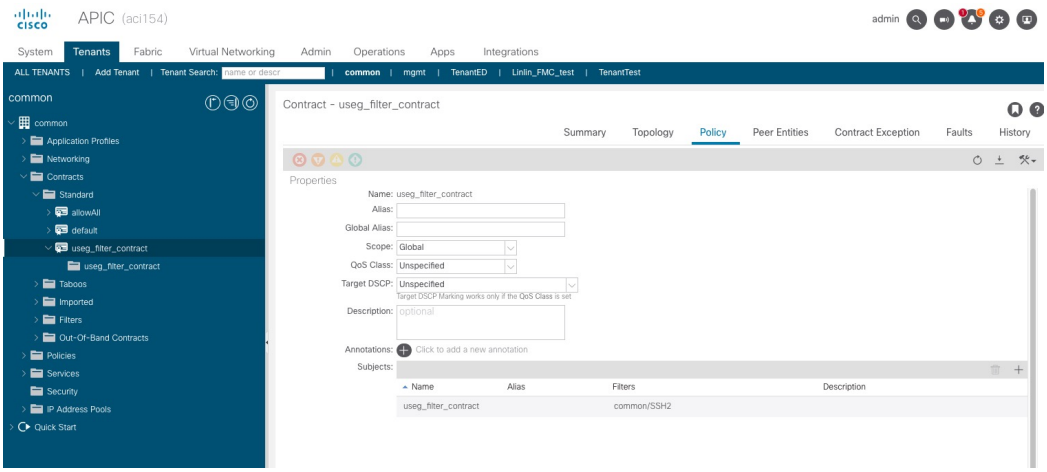
Step 8 Make other selections as desired.

Step 9 Click **Submit**.

Step 10 Click **useg_filter_contract**.

Step 11 In the right pane, click the **Policy** tab.

The following figure shows an example.



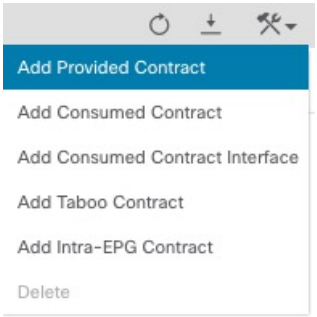
Step 12 Click **ALL TENANTS**.

Step 13 Double-click **mgmt**.

Step 14 Expand **mgmt** > **Application Profiles** > **mgmtProfile** > **Application EPGs** > **mgmtEPG** > **.**

Step 15 Click **Contracts**.

Step 16 Click **Add Provided Contract**.



Step 17 From the **Contract** list, click **useg_filter_contract**.

Step 18 Click **Submit**.

What to do next

See Create a Remediation Module Instance and Type, on page 12.

Create a Remediation Module Instance and Type

For the Secure Firewall Management Center to be able to detect threats and inform APIC to quarantine them, you must configure on the Secure Firewall Management Center a remediation module instance and type. For more information about remediations, see the Cisco Secure Firewall Management Center Administration Guide. You can optionally choose to quarantine the source endpoint, the destination endpoint, or both.

You can also choose to only audit endpoints without quarantining them.

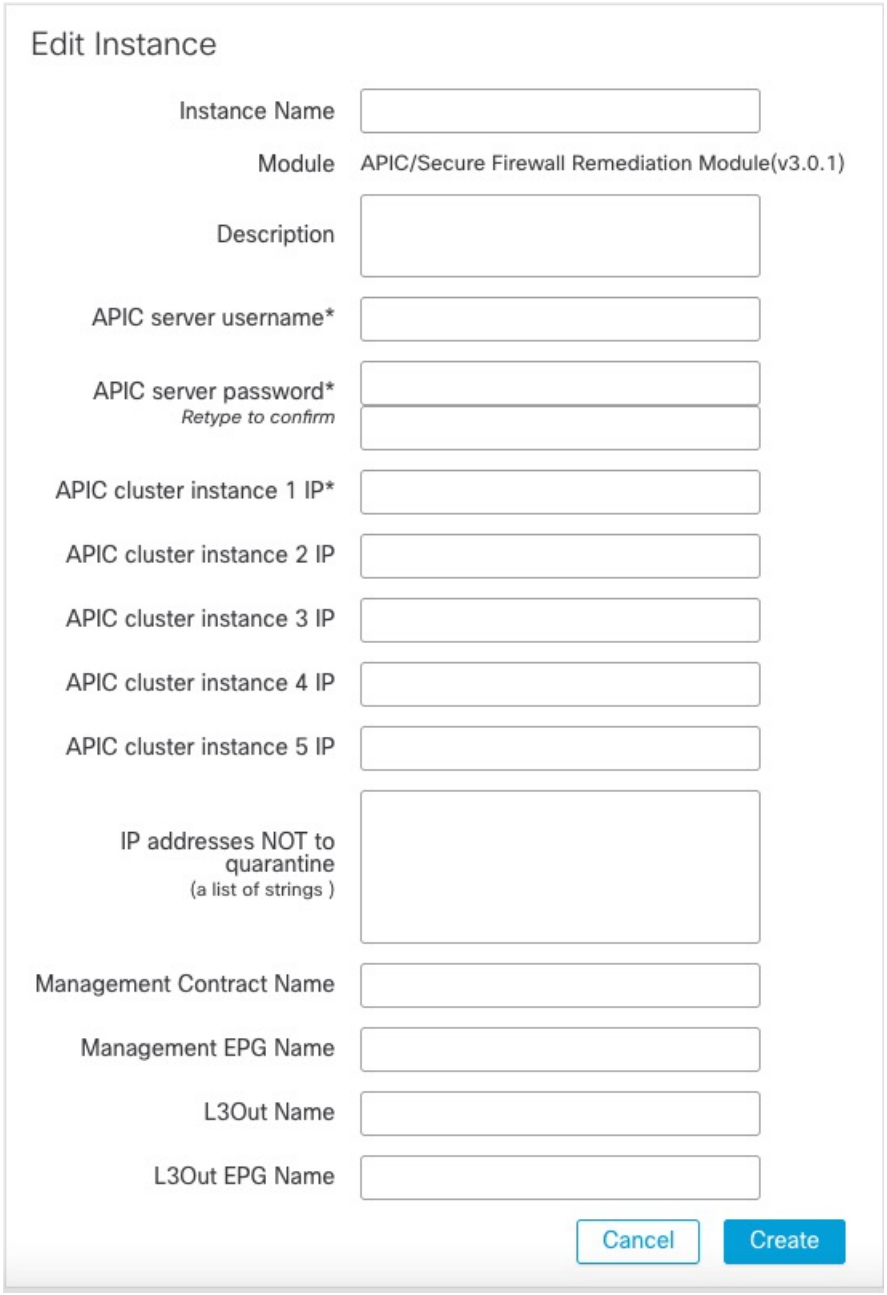
Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

Step 2 Click **Policies** > **Actions** > **Instances**.

Step 3 From the **Select a module type** list, click **APIC/Secure Firewall Remediation Module (3.0.1)**.

Step 4 Click **Add**.
The Edit Instance page is displayed as follows.



Step 5 Enter the following information:

Item	Description
Instance name	Enter a name to identify this instance. (Spaces are not allowed in the name.)
Description	(Optional.) Enter a description.
APIC server username	Enter the user name of an APIC user with admin privileges.
APIC server password	Enter and re-enter the user's password

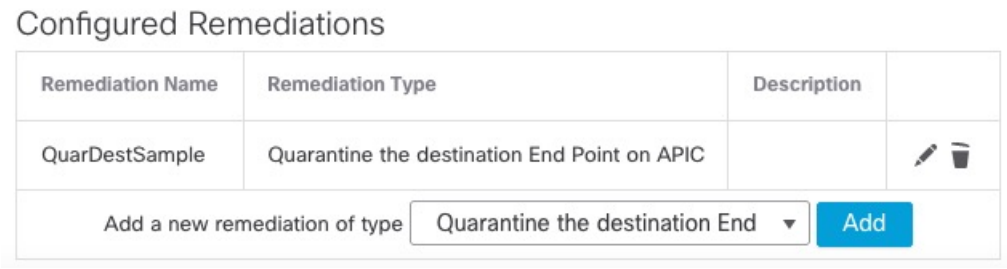
Item	Description
APIC cluster instance 1 IP	Enter the IP address of the APIC server or of the first server in the cluster.
APIC cluster instance x IP	(Optional.) If your APIC cluster has more than one server, enter additional IP addresses in the provided fields.
IP addresses NOT to quarantine	(Optional.) Enter a list of individual IP addresses to always exclude from the quarantine. Separate IP addresses with Enter. You cannot specify subnet masks.
Management Contract Name	(Optional.) Enter the name of the management contract you created in APIC. For more information, see Create an Optional Management Contract and Contract EPG, on page 9.
Management EPG Name	(Optional.) Enter the name of the EPG with which the management contract is associated. For more information, see Create an Optional Management Contract and Contract EPG, on page 9.
L3Out Name	(Optional.) The name of an L3Out target configured on APIC. If you enter a value in **L3Out Name**, you must also enter a value in **L3Out EPG Name**. Drops traffic between a quarantined endpoint in an L3Out target and the source endpoint group while allowing traffic from the quarantined endpoint for forensic analysis purposes.
L3Out EPG Name	(Optional.) The name of an L3Out endpoint group (EPG) configured on APIC. If you enter a value in **L3Out EPG Name**, you must also enter a value in **L3Out Name**.
Audit-only	**Off** (default): Quarantines an infected endpoint and sends correlation status messages to the Firewall Management Center. **On**: Does not quarantine an infected endpoint; instead, sends correlation status messages to the Firewall Management Center (**Analysis** > **Correlation** > **Correlation Events**).

Step 6 In the Configured Remediation section at the bottom of the page, click one of the following then click **Add**:

- **Quarantine the destination End Point on APIC**
- **Quarantine the source End Point on APIC**

The remediation name cannot include a space.

Following is an example of the Configured Remediation section showing a remediation.



Step 7 On the Edit Remediation page, enter the following information:

- **Remediation Name**: Enter a name to identify the remediation instance.
- (Optional.) **Description**: Enter a description of the remediation instance.

Step 8 Click **Create**.

Step 9 Click **Done**.

Step 10 On the Edit Instance page, optionally configure another remediation.

What to do next

See Configure an Access Control Rule for the Remediation, on page 15.

Configure an Access Control Rule for the Remediation

This example shows how to create an access control rule that blocks the SSH protocol. After creating this rule, any endpoint that attempts to SSH to another endpoint in an monitored EPG, the offending node or nodes are quarantined.

Procedure

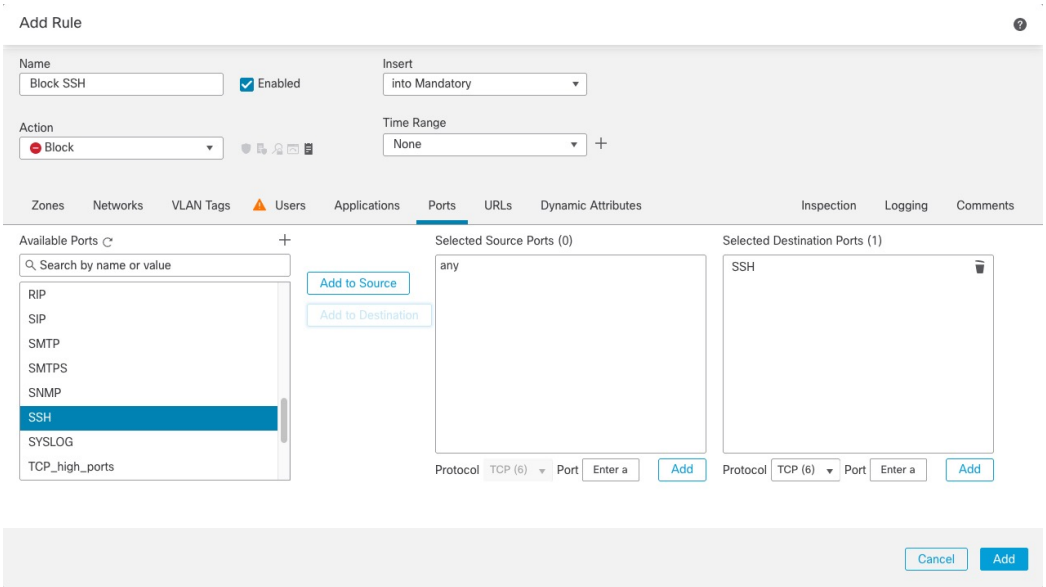
Step 1 If you haven't done so already, log in to the Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Access Control**.

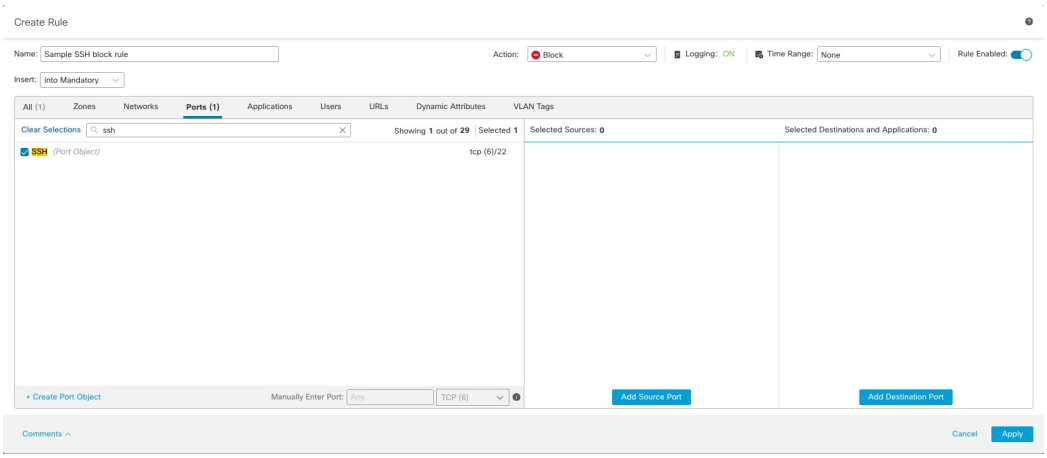
Step 3 Create a new access control policy or click **Edit** (✎) to edit an existing policy.

Step 4 If you're editing an exising policy, click **Add Rule** to add a rule.

Enter the following information (Firewall Management Center version 7.2 and earlier).



Enter the following information (Firewall Management Center version 7.3 and later).



Item	Description
Name field	Enter a name to identify this rule. *Write down* the name because you'll need it later.
Action list	Click **Block**.
Ports tab page	From the **Available Ports** list, scroll to SSH and click **Add to Destination**.
Logging tab page	Select the **Log at Beginning of Connection** check box.

For more information about access control rules, see the Cisco Secure Firewall Management Center Device Configuration Guide.

Step 5 Click **Add**.

Step 6 At the top of the page, click **Save**.

What to do next

See Configure a Correlation Rule for the Remediation, on page 17.

Configure a Correlation Rule for the Remediation

A correlation rule provides conditions in which the system responds to threats. The following task discusses how to set up a correlation rule that is triggered at any point in the connection when your access control rule conditions are met. In particular, the sample access control policy and rule are triggered when SSH traffic is passed between a source and destination endpoint.

For more information about correlation policies and rules, see the Cisco Secure Firewall Management Center Administration Guide.

Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

Step 2 Click **Policies** > **Correlation**.

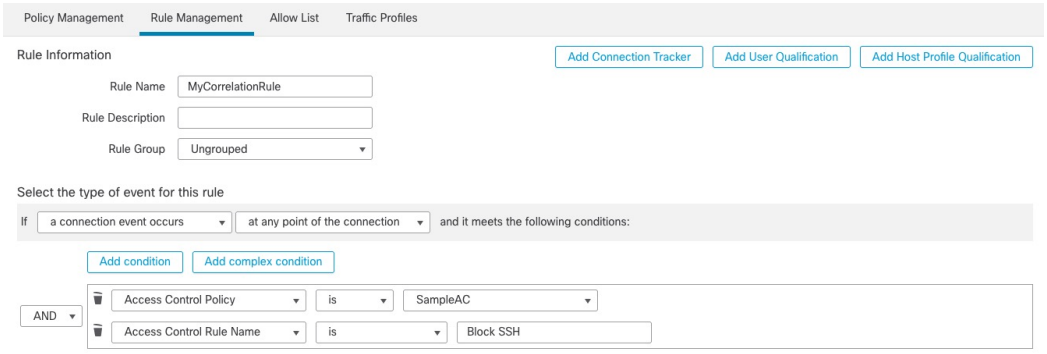
Step 3 Click the **Rule Management** tab.

Step 4 Click **Create Rule**.

Step 5 Enter a name to identify the rule and an optional description.

Step 6 In the Select the type of event for this rule section, click **a connection event occurs** and **at any point of the connection**.

Step 7 Set up the rest of the rule as shown in the following figure.



Substitute the name of your access control policy and rule name for those shown in the preceding figure.

Step 8 Set other options as desired and click **Save**.

What to do next

See Associate the Correlation Rule with the Remediation Module Instance, on page 18.

Associate the Correlation Rule with the Remediation Module Instance

The final step in configuring the Firewall Management Center for remediation and quarantine is to associate your correlation rule with your remediation policy. After you do this, when the Firewall Management Center detects a threat, the offending endpoints are quarantined in APIC.

Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

Step 2 Click **Policies** > **Correlation**.

Step 3 Click the **Policy Management** tab.

Step 4 Click **Create Policy**.

Step 5 Enter a policy name and optional policy description.

Step 6 Do not change **Default Priority**.

Step 7 Click **Add Rules**.

Step 8 Select the check box next to the name of the correlation rule you created earlier.

Step 9 Click **Add**.

Step 10 Click **Responses** ( ).

Step 11 From the **Unassigned Responses** list, double-click the name of your remediation policy to move it to **Assigned Responses**.

If the name of your remediation policy is not displayed, go back to the correlation rule and make sure the name of both the access control policy and access control rule are correct.

Step 12 Click **Update**.

Step 13 At the top of the page, click **Save**.

Step 14 Move the slider for the remediation policy to **Slider enabled** ( ).

Verify the Remediation in the Firewall Management Center

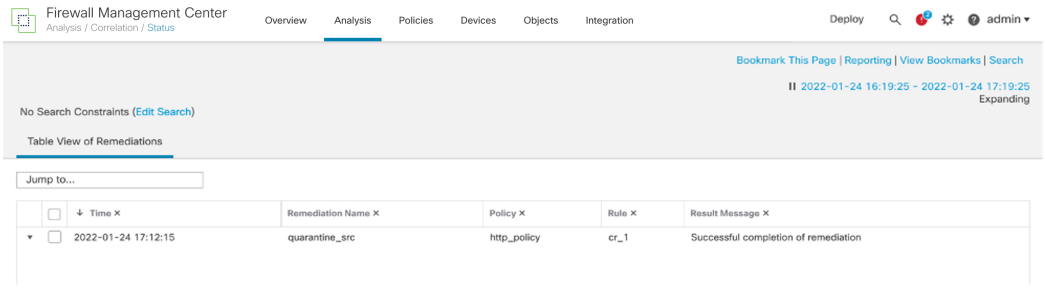
Because remediations can fail for various reasons, complete the following steps to verify that no error messages are listed for the remediation status on the Firewall Management Center.

Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

Step 2 Click **Analysis** > **Correlation** > **Status**.

Step 3 In the Remediation Status table, find the row for your policy and view the result message.
The following figure shows an example



Step 4 If the remediation was successful, see Verify the Quarantine in APIC, on page 19.

Step 5 If an error is displayed, the endpoint might still be quarantined if subsequent remediation events are successful.

Step 6 If you see an error, see Verify the Quarantine in APIC, on page 19 to verify whether or not the quarantine was successful. If the quarantine was eventually successful, you can ignore all of its error messages.

What to do next

See Verify the Quarantine in APIC, on page 19.

Verify the Quarantine in APIC

Before you begin

Complete the tasks discussed in Verify the Remediation in the Firewall Management Center, on page 18.

Procedure

Step 1 Log in to APIC.

Step 2 Click the **Tenants** tab page.

Step 3 Click **ALL TENANTS**.

Step 4 Double-click the name of the tenant that is infected.

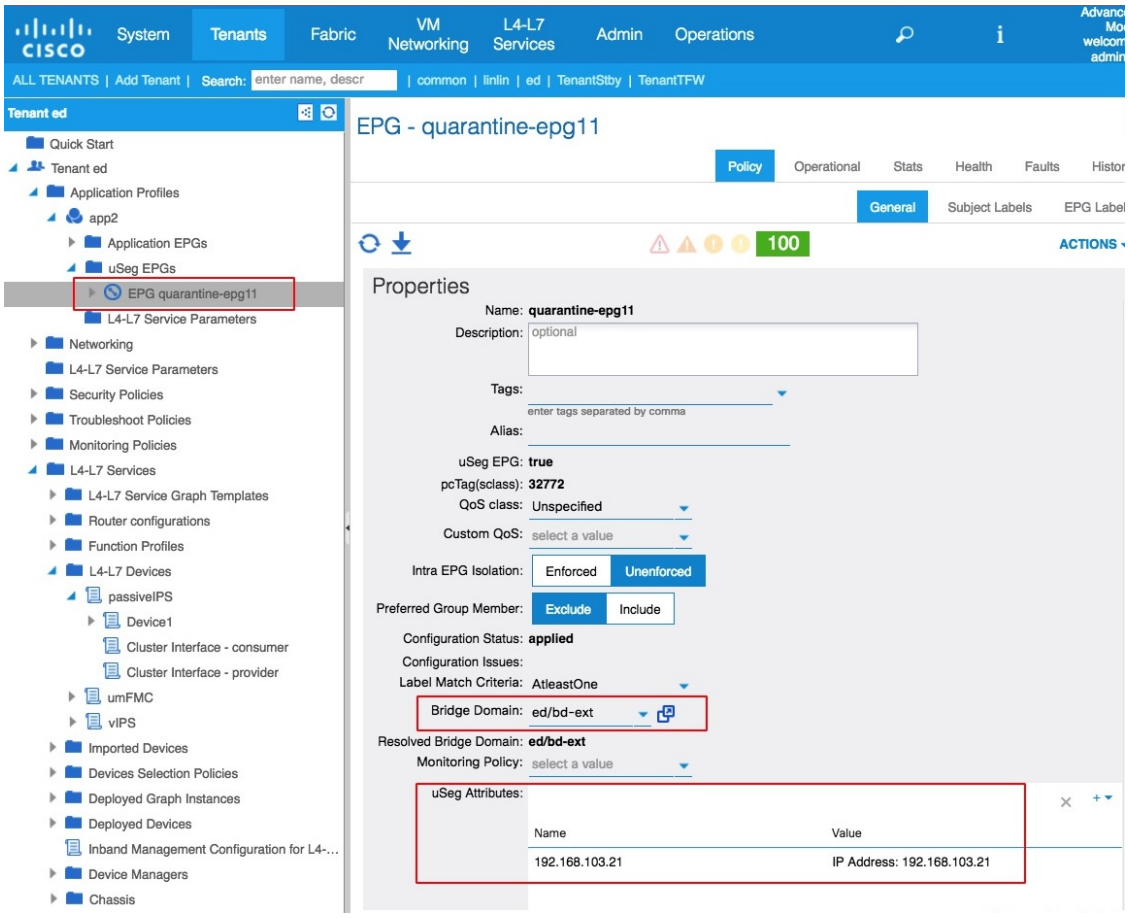
Step 5 Expand the infected application in the left pane.

Step 6 Click **uSeg EPGs**

Step 7 Click the EPG quarantine for the quarantined endpoint.

Step 8 In the right panel, click **Policy** > **General**.

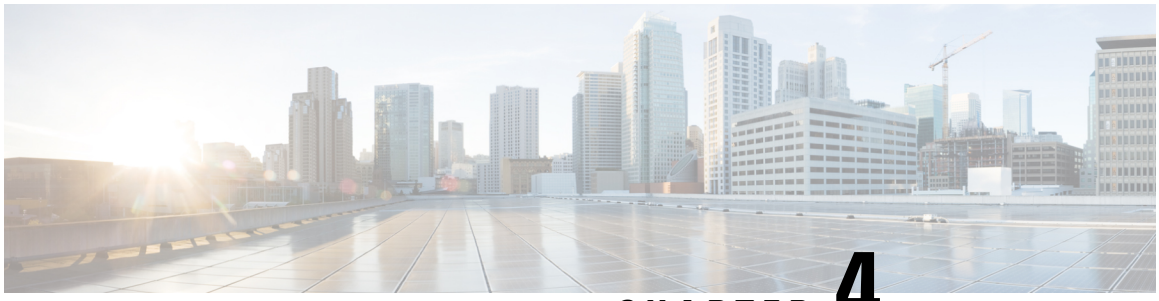
Step 9 Verify that one or more uSeg attributes were created on the APIC server.
The following figure shows an example.



The figure shows that a device at IP address 192.168.103.21 has been quarantined.

Note
For VMware DVS and Bare Metal (in bridged mode), two attributes (filters) are automatically created when an endpoint is quarantined, one attribute for the IP address and one attribute for the MAC address. Therefore, to remove the quarantine, you must delete both attributes.

Step 10 If no uSeg attributes were created, but you know that the conditions set by a correlation rule were met, the quarantine failed. To manually quarantine the IP address, see Overview of Manually Quarantining an IP Address, on page 21.



CHAPTER 4

Manually Quarantine an IP Address

In the event your quarantine fails, you can manually quarantine one or more IP addresses as discussed in the followint topics.

- Overview of Manually Quarantining an IP Address, on page 21
- Find an IP Address to Quarantine, on page 21
- Create a uSeg EPG Attribute, on page 22
- Verify the Manual IP Address Quarantine, on page 23

Overview of Manually Quarantining an IP Address

If a quarantine fails as discussed in earlier sections in this guide, you can manually quarantine that IP address. You must find the IP address and MAC address to quarantine. The IP address is shown in the Secure Firewall Management Center and the MAC address is shown in APIC.

Find an IP Address to Quarantine

This topic discusses how to look at correlation logs in the Firewall Management Center to find an IP address to quarantine.

Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

Step 2 Click **Analysis** > **Correlation** > **Status**.

Step 3 Find the timestamp of entry for the unsuccessful quarantine and make note of the source IP address.

Step 4 Log in to APIC if you haven't already done so.

Step 5 On the Operations tab page, click **EP Tracker**, enter the IP address, and press Enter.

Step 6 If no information is displayed, the endpoint cannot be quarantined. If more than one IP address is displayed, look for the one in the offending tenant.

What to do next

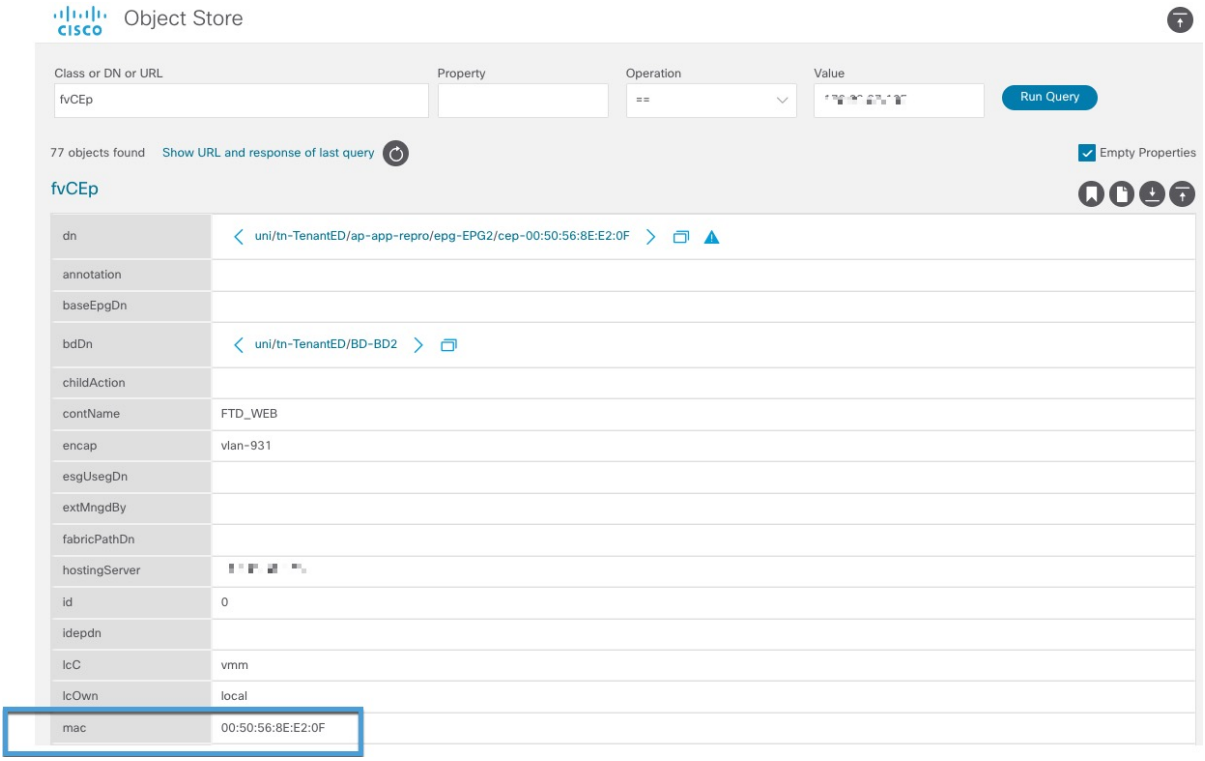
Create a uSeg EPG Attribute, on page 22

Create a uSeg EPG Attribute

If you can identify the EPG of the endpoint that you want to quarantine, create a uSeg EPG attribute corresponding to this endpoint.

Procedure

Step 1 To find the MAC address of the IP address to quarantine, go to the APIC Object Store Browser at https://*apic_IP_address*/**visore.html**. Use the IP address of the endpoint to run a query and display the MAC address. The following figure shows an example.



Step 2 Log in to APIC if you haven't already done so.

Step 3 Click **Tenants** > **ALL TENANTS**.

Step 4 Double-click the tenant that contains the endpoint to be quarantined.

Step 5 Expand **Networking** > **Bridge Domains**.

Step 6 Make note of the EPG bridge domain.

Step 7 Expand **Application Profiles** > ***profile-name*** > **Application EPGs** > ***epg-name*** and make note of the domain profile name.

Step 8 Expand **Application Profiles** and right-click **uSeg EPG**.

Step 9 Click **Create uSeg EPG**.

Step 10 Enter a name for the uSeg EPG, in the format **uSegEPG***endpoint-name*. (For example, **uSegEPG-EPG1**.)

Step 11 From the **Bridge Domain** list, click the EPG's bridge domain.

Step 12 Click **Next**.

Step 13 On the Domains page, click **Add** (+).

Step 14 From the **Domain Profiles** list, click the domain profile.

Step 15 Set **Deployment Immediacy** to **Immediate**.

Step 16 Set **Resolution Immediacy** to **Immediate**.

Step 17 Add an IP filter attribute by clicking **Add** (+) on the lower right and entering the IP address for the name and filter.

Step 18 Click **Update** and then click **Finish**.

If the uSeg EPG is not displayed, refresh your browser page.

Step 19 Click **uSeg Attributes**.

Step 20 Click **Add** (+)

Step 21 Add attributes for the quarantined host's IP address and MAC address with an operator of **Match Any**.

For the IP filter, use the IP address as the name. For MAC filter, use the IP address plus an underscore and the last three octets of the MAC address as a name.

Step 22 Right-click **Domains** (VMs and Bare Metals) under the newly created uSeg EPG, and add a domain association with the same name and domain type as the original EPG.

Step 23 For Bare Metal, right-click **Static Leafs**, and click **Statically Link With Node**.

Step 24 Click **Submit**.

What to do next

Verify the Manual IP Address Quarantine, on page 23

Verify the Manual IP Address Quarantine

Verify that no traffic can go into or out from the quarantined endpoint.

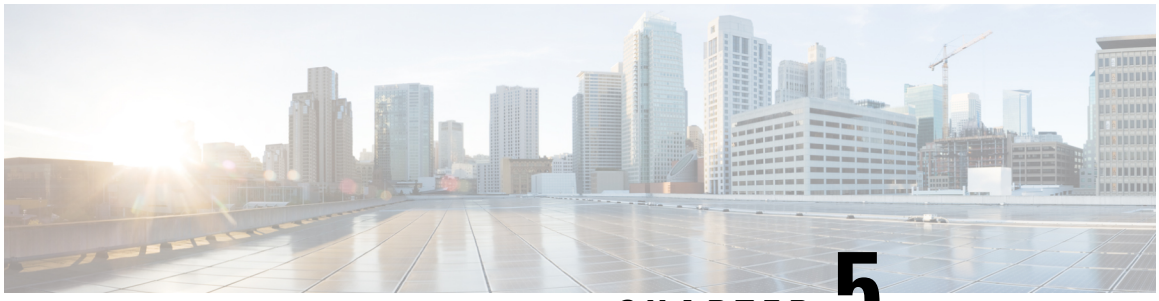
Before you begin

Procedure

Step 1 Perform some task such as pinging a quarantined IP address.

The operation should fail.

Step 2 If the ping succeeds, verify the IP and MAC addresses of the endpoint to quarantine and try again.



CHAPTER 5

Related Documentation

- Related Documentation, on page 25

Related Documentation

For additional information about the Cisco APIC/Secure Firewall Remediation Module, see the appropriate guide.

For additional information about the Cisco APIC and ACI, see APIC Documentation.

For information on using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see the Support Case Manager.

Related Documentation