cisco.



Cisco Secure Firewall Management Center Remediation Module for Cisco Secure Workload, Quick Start Guide

First Published: 2022-06-06

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 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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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.



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, on page 1
- Prerequisites, on page 3
- Related Documentation, on page 3

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



Downloading and Installing the Remediation Module

The following section provides the steps to download and install the FMC remediation module for Secure Workload (formerly Tetration).

• Install the Remediation Module, on page 5

Install the Remediation Module

Step 1 Use a web browser to download the remediation module: https://software.cisco.com/download/home/286259687/type

- Step 2 Install the remediation module onto the FMC:
 - a. In the FMC web interface, navigate to Policies > Actions > Modules.
 - b. In the Install a new module dialog box, click Choose File.
 - Select the file for the remediation module that was downloaded in Step 1. c.
 - d. Click Install.

Note If you receive an access error message, clear the error message and repeat Step 2.

When successfully installed, the Secure Firewall Management Center Remediation Module for Secure Workload is displayed in the list of installed remediation modules:

Firepower Management Center Over	view Analysis	Policies	Devices	Objects	AMP	Deploy	Q	¢	¢	2 DC-North-South	th \	•
										Alerts Remediation	ıs Gro	oups
Installed Remediation Modules												
Module Name	Domain		Version	Descriptio	on							
Cisco IOS Null Route	Global		1.0	Block an I	P address in a Cisc	co IOS router					•	
Nmap Remediation	Global		2.0	Perform a	n Nmap Scan						•	i
pxGrid Adaptive Network Control (ANC) Policy Assignment	Global		1.0	Apply or o	clear an ANC policy	/ for the endpoint at the	e involv	ed IP a	addre	sses	•	T.
pxGrid Mitigation	Global		1.0	Perform a	pxGrid mitigation a	against the involved IP	addres	ses			•	W
Secure Workload / Secure Firewall Remediation Module	Global \ DC	-North-South	1.0.3	Achieve ra	apid threat contain	ment of Secure Worklo	ad wor	kloads			•	1
Set Attribute Value	Global		1.0	Set an Att	tribute Value						•	Ì.
		Install a Choose fi	new modu le No file cho:	Ile ^{sen} Install								



Configuring the Remediation Module

The following section provides the steps for configuring the remediation module.

• Configure, on page 7

Configure

To configure the remediation module installed on the FMC, complete the following procedure:

Step 1 In FMC, create an instance of the remediation module for each Secure Workload cluster in your network:

- a. Navigate to Policies > Actions > Instances.
- b. Select the remediation module in the drop-down list, and click Add.
- c. Enter an Instance Name (in this example, fmc-dev-remediation).
- d. Enter the Secure Workload server's IP address, API key, API secret, and scope containing the potentially offending host. Click Create.
 - **Note** The API key and secret are not validated against the Secure Workload server at this point. The API key and secret must first be created in Secure Workload by a site admin, customer support, or a root scope owner role. Copy that information for use here. For more details, see Related Documentation, on page 3.

Firepower Management Center Policies / Actions / Instance Detail	Overview Analysis Pol	licies Devices Objects	AMP	Deploy Q	🥵 🌣 👩 DC-North-South \ 📃 🔻
	Edit Instance				
	Instance Name	fmc-dev-remediation			
	Module	Secure Workload / Secure Firewall I	Remediation Module(v1.0.3)		
	Description				
	Secure Workload IP	10.62.159.4			
	Scope(must be root scope, e.g. Default)	Default			
	API key				
	Retype to confirm				
	API secret				
	hetype to obtainin				
			Cancel Save		
	Configured Remediat	ions			
	Remediation Name Reme	diation Type	Description		
	quarantine-fmc Quara	antine an IP on Secure Workload	/1		
	unquarantine-fmc Unqua	arantine an IP on Secure Workload	/1		
	Add a new remediation of	of type Quarantine an IP on Secur	e Wor 🔻 🛛 Add		

- e. Under Configured Remediations, select a type of remediation (in this example, Quarantine an IP on Secure Workload), and click Add to add a new remediation.
- f. Enter a Remediation Name (in this example, quarantine-fmc), and click Create.

cisco Policie	power Management Center ies / Actions / Remediation Edit	Overview	Analysis	Policies	Devices	Objects	AMP		Deploy	Q	6	₽	DC-North-South \
													Alerts Remediations Groups
			Edit Reme	diation									
			Ren	nediation Name	quarant	ine-fmc							
			Re	mediation Type	e Quarantine	an IP on Secu	re Workload						
				Description	n To quarant	tine a host							
						Cancel	Create						

- g. The remediation you just configured then shows up in the table. Click Save.
- **Step 2** Configure an access control policy (in this example, **rem-policy**):
 - a. Navigate to Policies > Access Control and click the Edit icon of the access control policy to add rules.
 - b. Click Add Rule and enter a name (for example, block-ssh-add-tag).
 - c. Select Block for the Action.
 - d. On the Ports tab, select SSH from the list of protocols for the destination port.
 - e. On the Logging tab, select Log at Beginning of Connection.

Important Ensure that logging is enabled on the access rule, so that the FMC receives event notifications, and click Add

f. Click Save.

i c	Firepo	wer Man Access Cor	agement htrol / Policy E	Center	Overview	Analysis	Policie	es Devic	es Obj	ects AM	1P Intelli	gence	Deploy	, Q	6 🌣	0	Global	١.	Ŧ
n E	em-policy												gs Ana	lyze Hit C	ounts		e	Canc	el
	Rules Secu	rity Intelliger	nce HTTI	P Responses	Logging	Advanc	ed			Prefilter P	olicy: Default	Prefilter Polic	sy SSL	heritance Policy: N	<u>Settings</u> one	<u>Polic</u> Ider	<u>y Assig</u> ntity Pol	inmen licy: N	<u>ts (0)</u> Ione
Ei	Iter by Device	T Searc	h Rules								×	Show R	ule Conflicts	0 + /	Add Cate	gory	+ 4	Add Ri	ule
#	Name	Source Zones	Dest Zones	Source Netwo	Dest Netwo	VLAN Tags	Users	Applic	Source Ports	Dest Ports	URLs	Source Dynamic Attribu	Destin Dynamic Attribu	Action	F6 🛡	6 A		-	¢
\sim	Mandatory - rem	-policy (1-1)																
1	block-ssh-add	Any	Any	Any	Any	Any	Any	Any	Any	SSH	Any	Any	Any	Block	B 🛡	B 2		0	1
\sim	Default - rem-po	licy (-)																	
Th	ere are no rules	n this sectio	on. Add Rule	or Add Categ	ory														

Default Action	Access Control:Block all traffic	•
	Displaying 1 - 1 of 1 rules < < Page 1 of 1 > > C _ Rules per page: 100	¥

Step 3 Configure a correlation rule:

- a. Navigate to Policies > Correlation > Rule Management.
- b. Click Create Rule.
- c. Enter a Rule Name (in this example, quaran-rule1) and description (optional).
- **d.** In the Select the type of event for this rule section, select a connection event occurs and at either the beginning or the end of the connection.
- e. Click Add condition, and change the operator from OR to AND.
- f. In the drop-down list, select Access Control Rule Name, is, and enter the name of the access control rule that you previously configured in Step 2 (in this example, block-ssh-add-tag).

Firepower Management Center CISCO Policies / Correlation / Rule Management Overview	Analysis Policies	Devices Of	ojects AMP	Intelligence	Deploy 0	ર 🔮 🌣	Global \
						Alerts Re	emediations Groups
Policy Management Rule Management Allow List Traffic	Profiles						
Rule Information			Add Connectio	n Tracker Add Use	r Qualification	Add Host F	Profile Qualification
Rule Name quaran-rule1							
Rule Description							
Rule Group Ungrouped 🔻							
Select the type of event for this rule							
If a connection event occurs • at the beginning of the cor	and it meets the	he following conditio	ns:				
Add condition Add complex condition							
CAccess Control Rule Name	▼ block-ssh-ad	ld-tag					
Rule Options						A	dd Inactive Period
Snooze If this rule generates an event, snooze for	or 0 hours	•					
Inactive Periods There are no defined inactive periods. T	o add an inactive period, o	click "Add Inactive Pe	eriod".				
						С	ancel Save

g. Click Save.

Step 4 Associate the instance of the remediation module as a response with a correlation rule:

- a. Navigate to Policies > Correlation > Policy Management.
- b. Click Create Policy.
- c. Enter a Policy Name (in this example, correlation-policy) and description (optional).
- d. From the Default Priority drop-down list, select a priority for the policy. Select None to use rule priorities only.
- e. Click Add Rules, select the correlation rule you previously configured in Step 3 (in this example, quaran-rule1), and click Add.
- f. Click the Responses icon next to the rule and assign a response (in this example, test_rem) to the rule. Click Update.

, i	Firepower Management Center Policies / Correlation / Policy Management	riew Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	Q	6 9 🌣	0	Global \	•
										Alerts	Remedia	ations Gro	oups
	Policy Management Rule Management Allow List	Traffic Profiles											
	Correlation Policy Information										Cancel	Save	
	Policy Name correlation-policy												
	Policy Description												
	Default Priority None	Ŧ											
	Policy Rules										C	Add Rules	۶
	Rule	Responses						Priority					
	quaran-rule1	test_rem (Remediat	tion)					Default			•		

g. Click Save.



Verifying Remediation

The following section provides the steps to verify if the remediation process is successful.

• Verify Remediation, on page 11

Verify Remediation

Eirenower Management Center

Because remediations can fail for various reasons, perform the following steps to verify that a remediation is successful.

Step 1After the remediation module is triggered by an associated correlation rule, check the status of the remediation execution.
In the FMC web interface, navigate to Analysis > Correlation > Status.

Step 2 In the Remediation Status table, find the row for your policy and view the result message.

cisco Analysis / Correlation / Status	Overview Analysis Policies	Devices Objects AMF	5	Deploy	Q 💕 🌣 🞯 DC-North-South∖admin▼
No Search Constraints (Edit Search)				Bookmart	k This Page Reporting View Bookmarks Search III 2022-02-23 06:47:00 - 2022-04-22 07:54:27 Expanding
Jump to					
□ ↓ Time ×	Remediation Name ×	Policy ×	Rule ×	Result Message ×	Domain ×
 2022-03-31 14:56:34 	quarantine-fmc	correlation-policy	quaran-rule-1	Successful completion of remediation	Global \ DC-North-South
$ <\ <\ Page$ 1 of 1 $>\ > $ Displaying row 1	of 1 rows				
View Delete					
May All Delate All					

- **Step 3** Once the remediation is complete, perform the following steps:
 - a. In the Secure Workload user interface, navigate to Visibility > Inventory Search.
 - **b.** Enter the IP address of the infected hosts, and click **Search**.
 - c. In User Annotations, you should see quarantine = yes annotated to the IP address of the infected hosts.

Scopes and Inventory					
	Query Quarantine-FMC	uarantine = yes		Delete Edit Ac	id :
Scopes No Draft Changes	All Inventory 2 Usages				
● Filter Scopes ×	Enter attributes			× Search	Inventory
38 Scopes and 29 Inventory Filters ()	Services O Pods O	Workloads 0 IP Ac	ddresses 🕕 2		
Default (internal) Inventory: 453	Showing 2 of 2 inventory				:
1 Internet Inventory: 266	▼ Address 1↓	* Location Î↓	* Service 1↓	* Quarantine ↓	
	192.168.110.2	J Contractors	1	🖋 yes	
V IoT-Devices Inventory: 0	192.168.10.35	ø DC	/	💉 yes	
Quarantine-FMC Inventory: 2					

What to do next

Once you clean the quarantined host and it is no longer infected, you can perform either of the following actions to remove the quarantine annotation:

- (**Recommended**) Use Secure Workload to change the **quarantine** = **yes** annotation back to **quarantine** = **no**.
- 1. For example, if the quarantined host that is no longer infected is 172.21.208.11 and within the **Default** scope, create a CSV file such as:

```
IP,VRF,quarantine
172.21.208.11,Default,no
```

- Navigate to Applications > Inventory Upload, and then upload the CSV file to Secure Workload. For more information on how to upload a CSV file to Secure Workload, see the Related Documentation, on page 3 section.
- Use FMC Remediation Module to remove the quarantine annotation.

G

Important This method is not recommended in production networks due to security concerns.

1. (In the Configure section, see Step 1) Add a new remediation that uses the un-quarantine type of remediation. Edit the same instance, and under **Configured Remediations**, select and add the un-quarantine type of remediation (in this example, **unquarantine-fmc**).

Configured Remediations

Remediation Name	Remediation Type	Description	
quarantine-fmc	Quarantine an IP on Secure Workload		
unquarantine-fmc	Unquarantine an IP on Secure Workload		1
Add a new reme	diation of type Unquarantine an IP on Sec	ure W 🔻 🛛 Ad	d

- 2. (In the Configure section, see Step 2) Add an access control rule (For example, **remove-tag**) to the same policy (For example, **rem-policy**) which can be used to trigger the un-quarantine remediation.
- 3. (In the Configure section, see Step 3) Add a correlation rule (For example, unquaran-rule1) that uses the access control rule (in this example, remove-tag).
- 4. (In the Configure section, see Step 4B) Assign the un-quarantine response (For example, un-quaran-rem) to the correlation rule (For example, unquaran-rule1).
- 5. After the rule is matched, the un-quarantine remediation will be triggered to remove the quarantine annotation.