



Kemp Flowmon ADS Script for Check Point Quarantine

This document describes how to use a mitigation script to automatically quarantine suspicious IP addresses on a Check Point firewall based on triggers initiated by Kemp Flowmon ADS.

Introduction

The purpose of integrating Kemp Flowmon and Check Point is to automatically respond to threats detected by Kemp Flowmon ADS by blocking malicious traffic at a Check Point firewall. When Kemp Flowmon ADS detects a critical event, an automated action is triggered via Check Point API to block all network traffic of the event source – a compromised device or any adversary activity in the network. This ensures that the device is no longer able to reach other network zones (e.g. A data center or company servers) on the Internet. This is an effective way to minimize the impact, prevent data exfiltration or terminate covered communication channels.

The integration script was tested on the Check Point Gaia R81 (Build 959) firewall and is using SAM (Suspicious Activity Monitoring) rules to restrict access without the need to install a policy.

Check Point API doesn't have a method to call for direct IP address blocking. So instead, the script calls the method "run-script" after opening a connection on Check Point, which includes the parameter "script" that is basically the command you want to run on the Check Point cli. In this case, the command (fw sam) is the one that puts the IP address into the quarantine.

For more info check the official [Check Point API Reference website](#).

Configuration Steps

Firstly, make sure your API interface is up and running on Gaia Clish by entering 'api status' in the prompt. This is required in order to make the integration work.

```
gw-bfba64> api status

API Settings:
-----
Accessibility:                Require all granted
Automatic Start:              Enabled

Processes:

Name      State    PID      More Information
-----
API       Started  8369
CPM       Started  8369     Check Point Security Management Server is running
and ready
FWM       Started  7857
APACHE   Started  10100

Port Details:
-----
JETTY Internal Port:          61724
JETTY Documentation Internal Port: 52162
APACHE Gaia Port:             443

Profile:
-----
Machine profile:              Small Medium env resources profile
CPM heap size:                 1280m

                                Apache port retrieved from: httpd-ssl.conf

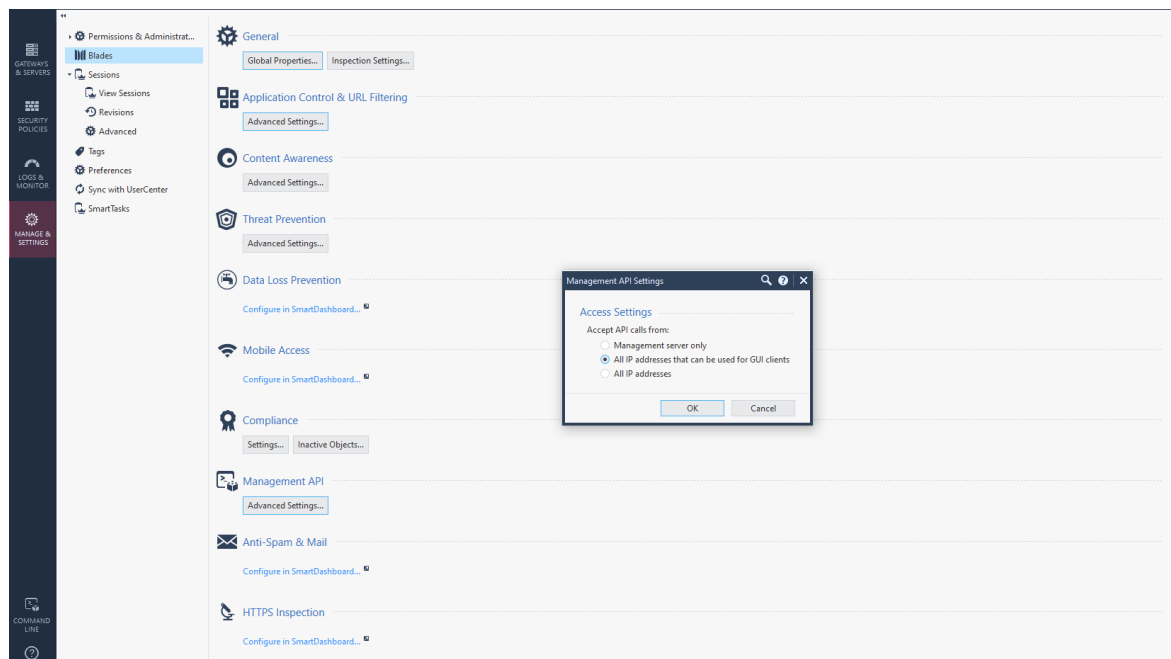
-----
Overall API Status: Started
-----

API readiness test SUCCESSFUL. The server is up and ready to receive connections

Notes:
-----
To collect troubleshooting data, please run 'api status -s <comment>'

gw-bfba64> █
```

Configure the Kemp Flowmon IP address in the SmartConsole to allow the Check Point firewall to accept API calls from Kemp Flowmon.



The script itself contains default configuration parameters such as login credentials and the firewall IP address for Check Point API authentication. You also need to specify the firewall hostname, and optionally, you may amend the expiration of the blocking rule.

```

8 #Default values
9 default_user="admin"
10 default_password="admin123"
11 default_ipaddress="192.168.47.78"
12 default_target="gw-bfba64"
13 default_expiration="3600"
    
```


These settings do not have to be configured in the script source code as they can be configured in Kemp Flowmon ADS script settings.

Upload the integration script to Kemp Flowmon ADS in Settings > System settings > Custom scripts. Click New Custom Script, type a name and upload the script source code file. Provide all the above-mentioned configuration parameters:






- user
- password
- ipaddress
- hostname
- expiration


New custom script ✕

Name

File 

Parameters

Name	Value	
<input type="text" value="--user"/>	<input type="text" value="admin"/>	
<input type="text" value="--password"/>	<input type="text" value="admin123"/>	
<input type="text" value="--ipaddress"/>	<input type="text" value="192.168.47.78"/>	
<input type="text" value="--target"/>	<input type="text" value="gw-bfba64"/>	
<input type="text" value="--expiration"/>	<input type="text" value="7200"/>	



SAVE **CLOSE**

If a configuration parameter is not set via the graphical user interface as described here, the default configuration parameter from the script source code will be used.

Next step is to set up a custom script action in Kemp Flowmon ADS in Settings > Processing > Custom scripts for the desired perspective and the minimum required priority of detected events.

Edit custom script action
✕

Name

Script script ▼

Parameters	Name	Value
	--user	<input style="width: 100%;" type="text" value="admin"/>
	--password	<input style="width: 100%;" type="text" value="admin123"/>
	--ipaddress	<input style="width: 100%;" type="text" value="192.168.47.78"/>
	--target	<input style="width: 100%;" type="text" value="gw-bfba64"/>
	--expiration	<input style="width: 100%;" type="text" value="7200"/>

Perspective Operational issues ▼

Active

Do not send empty reports

Minimal priority to be reported Informational ▼

Owner Michal Zakarovsky ▼

SAVE

+ SAVE AS NEW

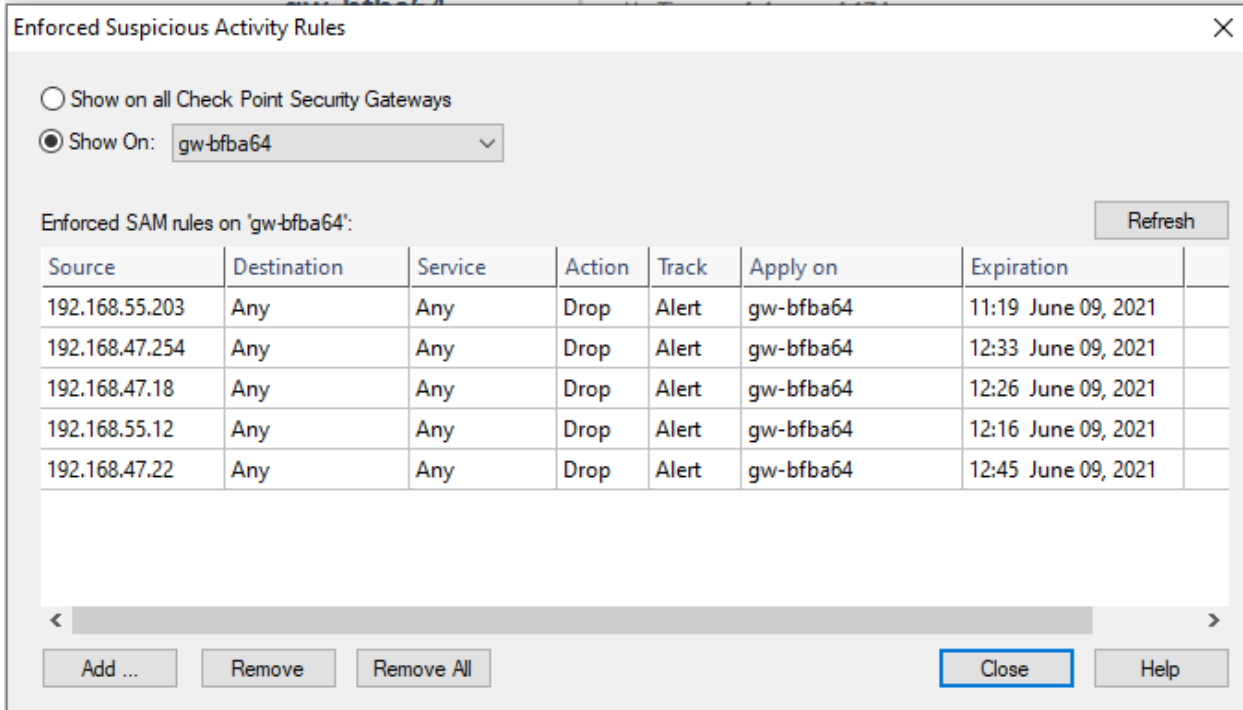
CLOSE

After that, make sure that the custom script trigger is active.

Custom scripts					
ACTIVE	NAME	OWNER	SCRIPT	PARAMETERS	PERSPECTIVE
<input checked="" type="checkbox"/> Yes	script	zakarovsky	script		Operational Issues ✎ ☰

Operation

In the Checkpoint SmartView Monitor you can display Suspicious Activity Rules (the icon is located in the panel at the top of the window). Suspicious Activity Rules will display all IP addresses the firewall is configured to block.



Enforced Suspicious Activity Rules

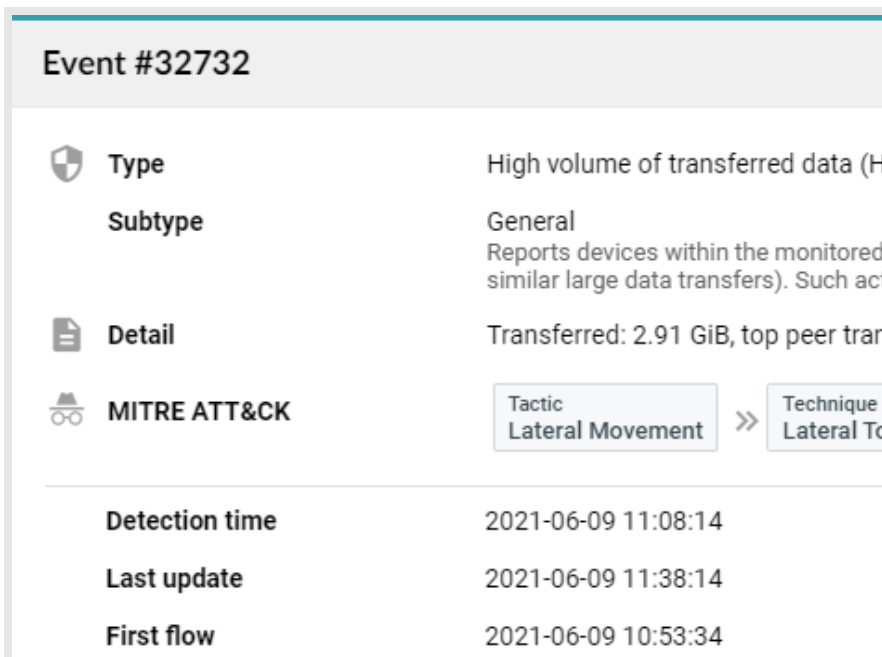
Show on all Check Point Security Gateways
 Show On: gw-bfba64

Enforced SAM rules on 'gw-bfba64': Refresh

Source	Destination	Service	Action	Track	Apply on	Expiration
192.168.55.203	Any	Any	Drop	Alert	gw-bfba64	11:19 June 09, 2021
192.168.47.254	Any	Any	Drop	Alert	gw-bfba64	12:33 June 09, 2021
192.168.47.18	Any	Any	Drop	Alert	gw-bfba64	12:26 June 09, 2021
192.168.55.12	Any	Any	Drop	Alert	gw-bfba64	12:16 June 09, 2021
192.168.47.22	Any	Any	Drop	Alert	gw-bfba64	12:45 June 09, 2021

Additional tips and tricks

The Kemp Flowmon script is only triggered once Kemp Flowmon ADS detects a new event (“Detection time”, see below). Updating the event (“Last update”, see below) will not trigger the script.



Event #32732

Type High volume of transferred data (H
Subtype General
 Reports devices within the monitored similar large data transfers). Such act

Detail Transferred: 2.91 GiB, top peer tran

MITRE ATT&CK
Tactic
Lateral Movement >> Technique
Lateral To

Detection time 2021-06-09 11:08:14
Last update 2021-06-09 11:38:14
First flow 2021-06-09 10:53:34

For this reason, you may consider quarantining the IP address indefinitely by configuring the expiration to “never”. To manually remove an IP address from the quarantine, use the Checkpoint SmartView Monitor.

```
8 user="admin"  
9 password="admin123"  
10 ipaddress="192.168.47.78"  
11 target="gw-bfba64"  
12 expiration="never"
```

You may also prevent the Kemp Flowmon device from accessing the Check Point appliance by putting the Kemp Flowmon IP address into the quarantine. Thus, you won't be able to revoke API calls anymore.