

ADS Script for Fortigate Quarantine

This document describes how to use the mitigation script for blocking suspicious stations automatically on Fortigate firewalls. It's using the new functionality of FortiOS 6.4.0 for webhook automation stitches. Unblocking needs to be performed manually on a Fortigate device once the threat is mitigated. This new version allows mitigation also on the access layer.

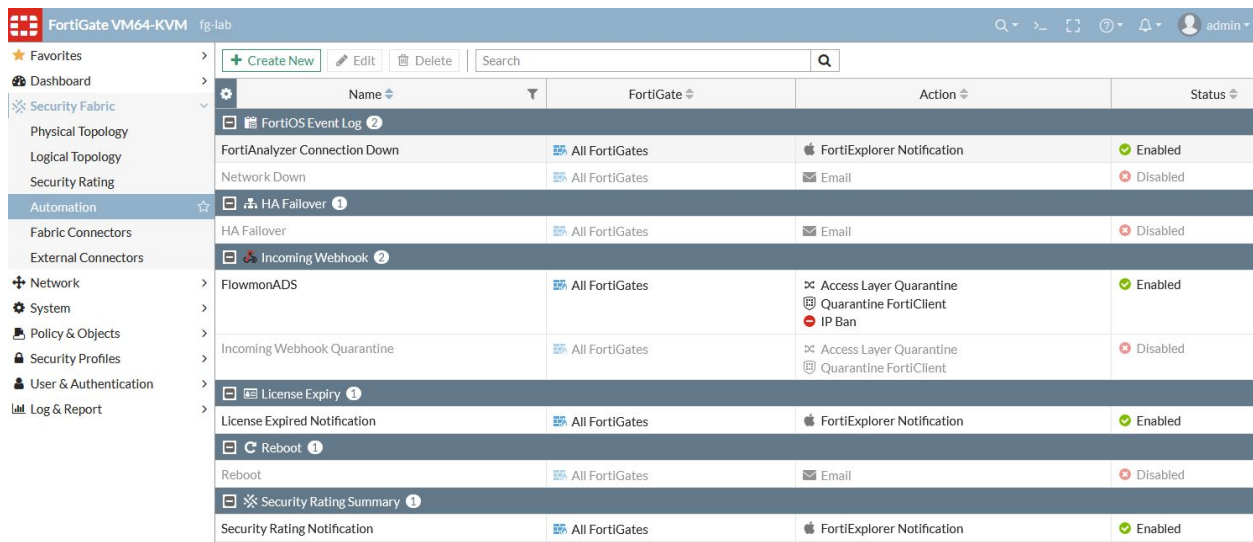
Configuration

The script contains configuration such as username, password for Flowmon API authentication in case you would like to enable access layer (MAC address) mitigation, firewall IP address, API key and option to provide name of custom webhook and turn on the access layer mitigation. These parameters can be provided by Flowmon ADS when the script is triggered or hardcoded in the script itself based on the user preference. You can open and adjust the script before uploading to Flowmon ADS by editing values on lines 13,14,16,17,18 and 19.

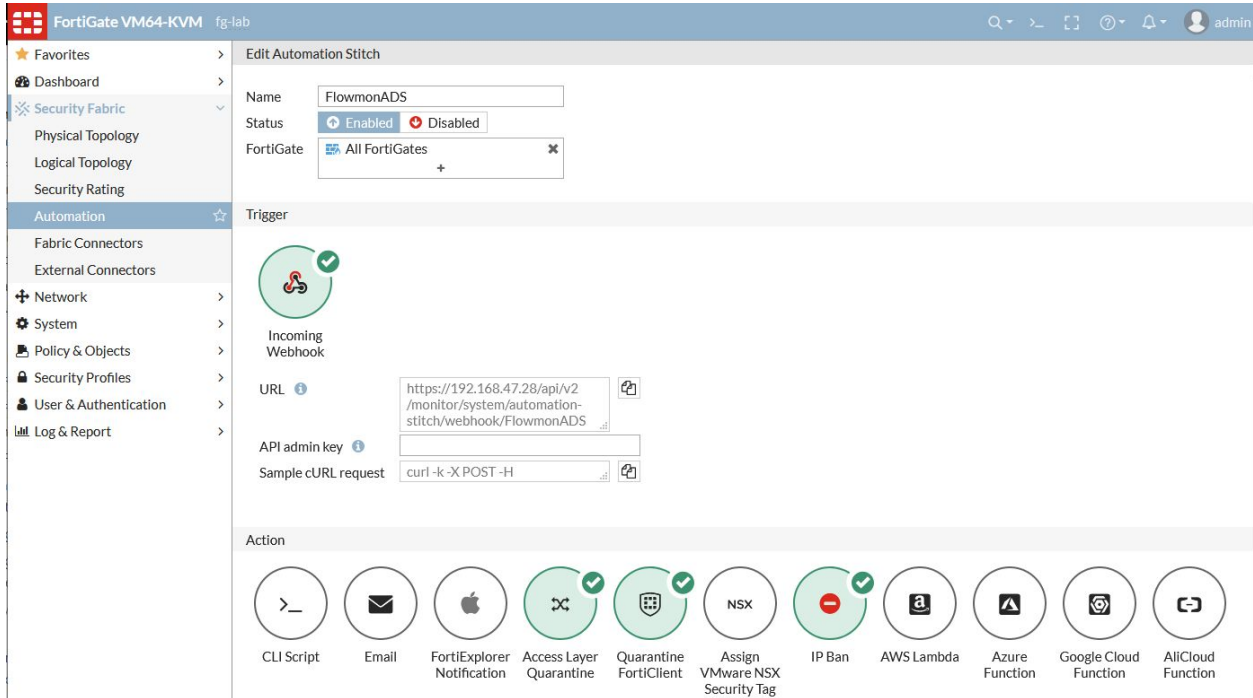
```

12 # Flowmon API access
13 USER='admin'
14 PASS='admin'
15 # Management IP/hostname of Firewall/ Core device
16 IP='192.168.47.28'
17 WEBHOOK='FlowmonADS'
18 API_KEY='fp8114zdNpjp8Qf8zN4Hdp57dhgjff'
19 MAC=0
  
```

On a Fortigate device you need to add in Security Fabric new Automation.

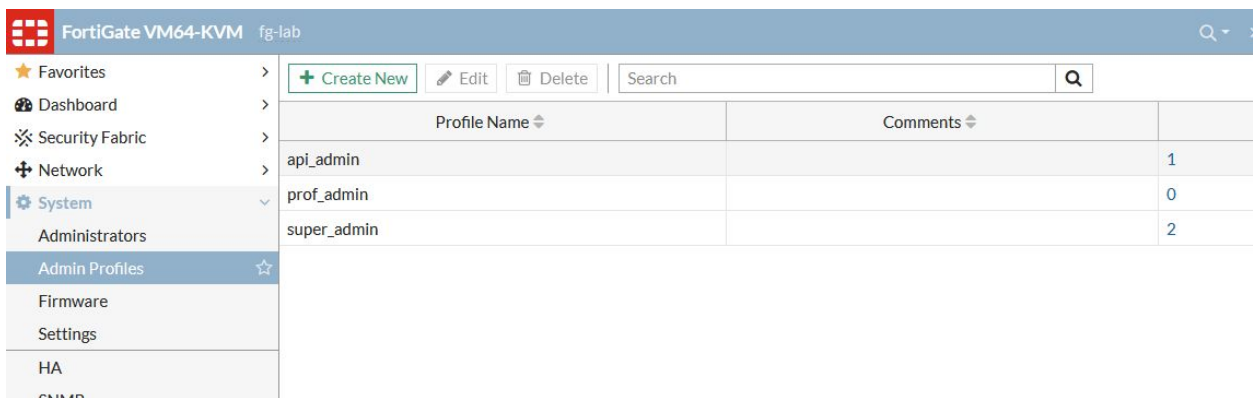


It's recommended to name it FlowmonADS as this way you don't need to change this name in a script. Then you can select which Action is going to be taken. Our script is able to fill an IP address and MAC address so you can use Access Layer Quarantine, Quarantine FortiClient and IP Ban action.

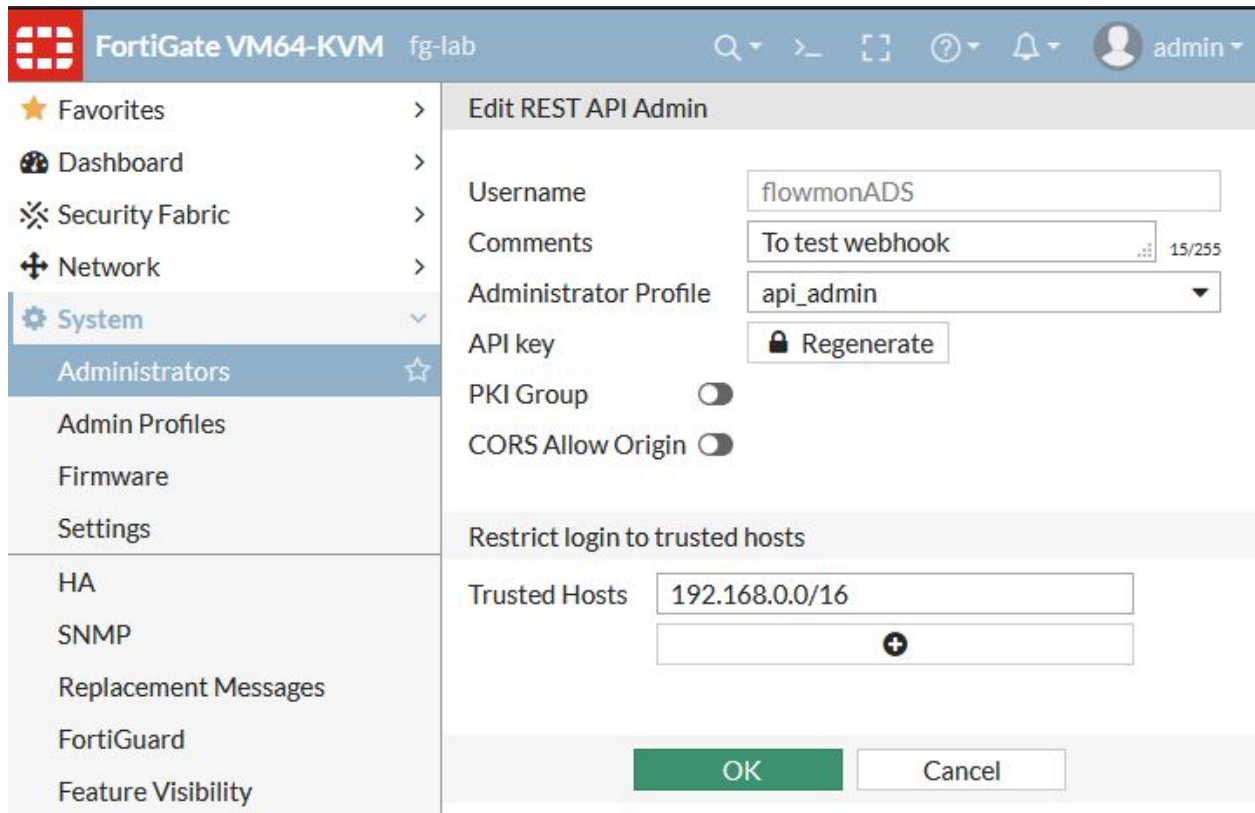


Now, you would need to create an admin profile which would allow API access to configure IP Ban and quarantines and API administration access.

So, you can use a predefined profile or create own for API access in System > Admin Profiles.



Then in System > Administrator create a New REST API Admin, you can limit networks/IP addresses which have access to API just to Flowmon appliance IP/network.



FortiGate VM64-KVM fg-lab

admin

- Favorites
- Dashboard
- Security Fabric
- Network
- System
 - Administrators
 - Admin Profiles
 - Firmware
 - Settings
- HA
- SNMP
- Replacement Messages
- FortiGuard
- Feature Visibility

Edit REST API Admin

Username: flowmonADS

Comments: To test webhook (15/255)

Administrator Profile: api_admin

API key:

PKI Group:

CORS Allow Origin:

Restrict login to trusted hosts

Trusted Hosts: 192.168.0.0/16


This step will generate for you an API key you need to include in script or ADS configuration. Or you would need to regenerate it later. User name you can use any string to understand that it was this key triggering API key.

If you would like to configure this in CLI then you can have a look at the reference [\[1\]](#) link.

Now you are ready to add new action in Flowmon ADS (details are available in Flowmon ADS User Guide). Upload the script in Settings > System settings > Custom scripts. If you have hard coded parameters in the script you do not need to provide any additional parameters. Otherwise configure add username (user), password (pass), firewall IP address (ip), API key (key) and if you wish to use Access Layer mitigation (mac)parameters to script configuration. IT would look similar to the setup you can see on below screenshot.

Edit custom script ✕

Name

File No file selected. 

Parameters

Name	Value
<input type="text" value="-fw"/>	<input type="text" value="192.168.47.28"/>
<input type="text" value="-key"/>	<input type="text" value="fp8114zdNpjp8Qf8zN4Hdp"/>
<input type="text" value="-mac"/>	<input type="text"/>
<input type="text" value="-pass"/>	<input type="text" value="admin"/>
<input type="text" value="-user"/>	<input type="text" value="admin"/>

Now you can set up blocking via Fortigate as custom action in Settings > Processing > Custom scripts for desired perspective and priority of events. Here you can modify parameters if you would like to.

Edit custom script action ✕

Name

Script

Parameters	Name	Value
	--fw	<input type="text" value="192.168.47.28"/>
	--key	<input type="text" value="fp8114zdNpjp8Qf8zN4Hdp"/>
	--mac	<input type="text" value="1"/>
	--pass	<input type="text" value="admin"/>
	--user	<input type="text" value="admin"/>

Perspective

Active

Do not send empty reports

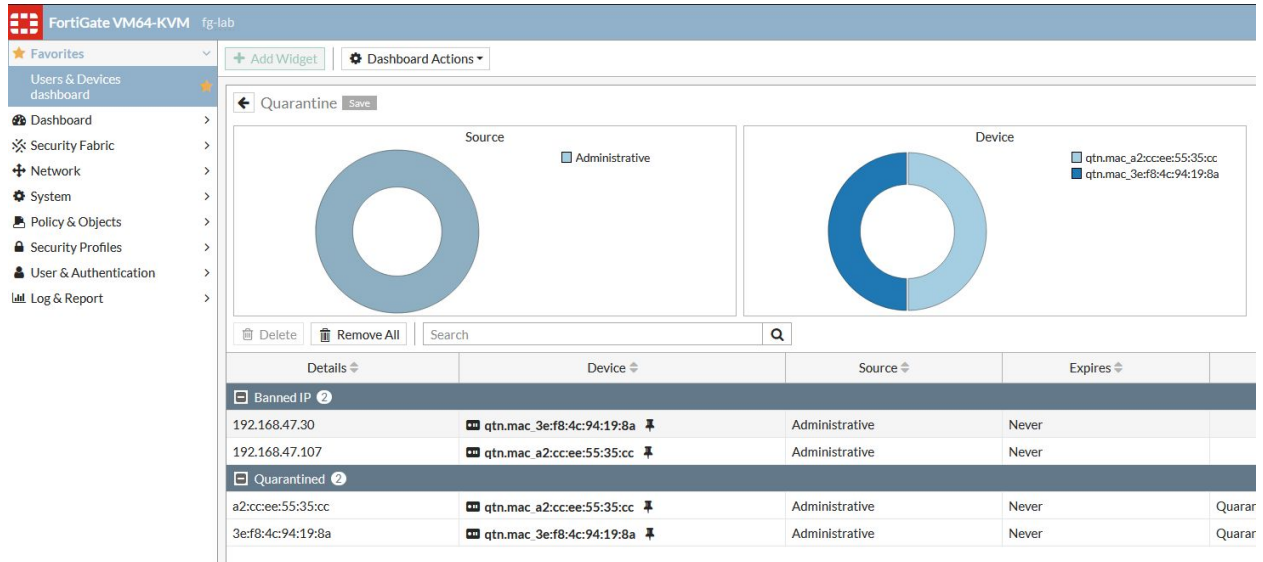
Minimal priority to be reported

Owner

SAVE **+ SAVE AS NEW** **CLOSE**

Operation

In Fortigate GUI you can see blocked IPs in Dashboard > User & Devices and widget Quarantine.



Details	Device	Source	Expires	
Banned IP				
192.168.47.30	qtn.mac_3e:f8:4c:94:19:8a	Administrative	Never	
192.168.47.107	qtn.mac_a2:cc:ee:55:35:cc	Administrative	Never	
Quarantined				
a2:cc:ee:55:35:cc	qtn.mac_a2:cc:ee:55:35:cc	Administrative	Never	Quarar
3e:f8:4c:94:19:8a	qtn.mac_3e:f8:4c:94:19:8a	Administrative	Never	Quarar

Or use a command in CLI.

```
diagnose user quarantine list
```

You would need to delete quarantined IPs manually when a particular threat is mitigated and blocking is no longer needed.

If you enable FortiClient Quarantine, then you would need to remove the device from quarantine there as well.

Reference:

[1] <https://docs.fortinet.com/document/fortigate/6.4.0/new-features/921236/automation-stitches>