

Phantom Integration with Check Point R80.10

Author: Richard Devera

Reviewer: Calvin Joy;

Version: 0.9

Version Date:

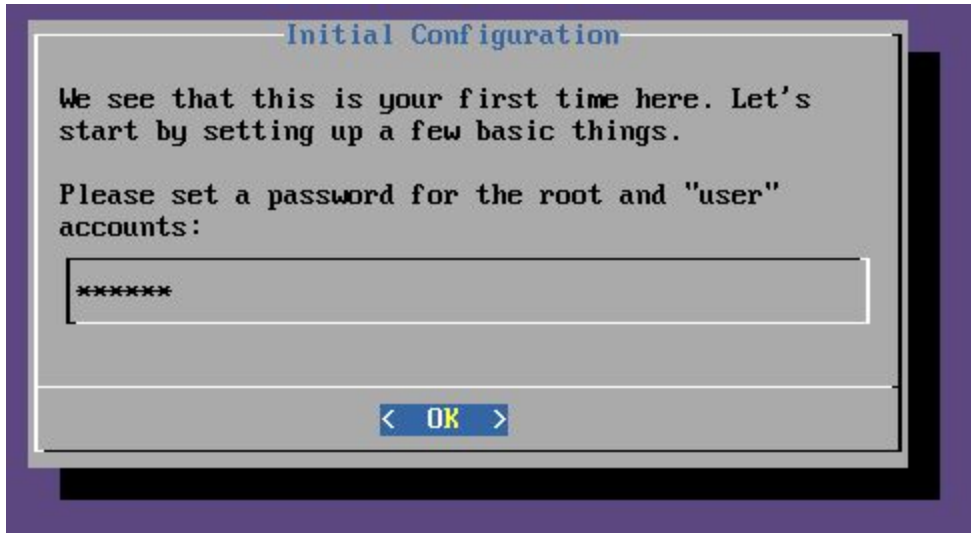
Purpose: Demonstrate the API integration between Phantom and Check Point R80.10. This document does not cover all the automation features of Phantom (ie Playbooks).

Prerequisite:

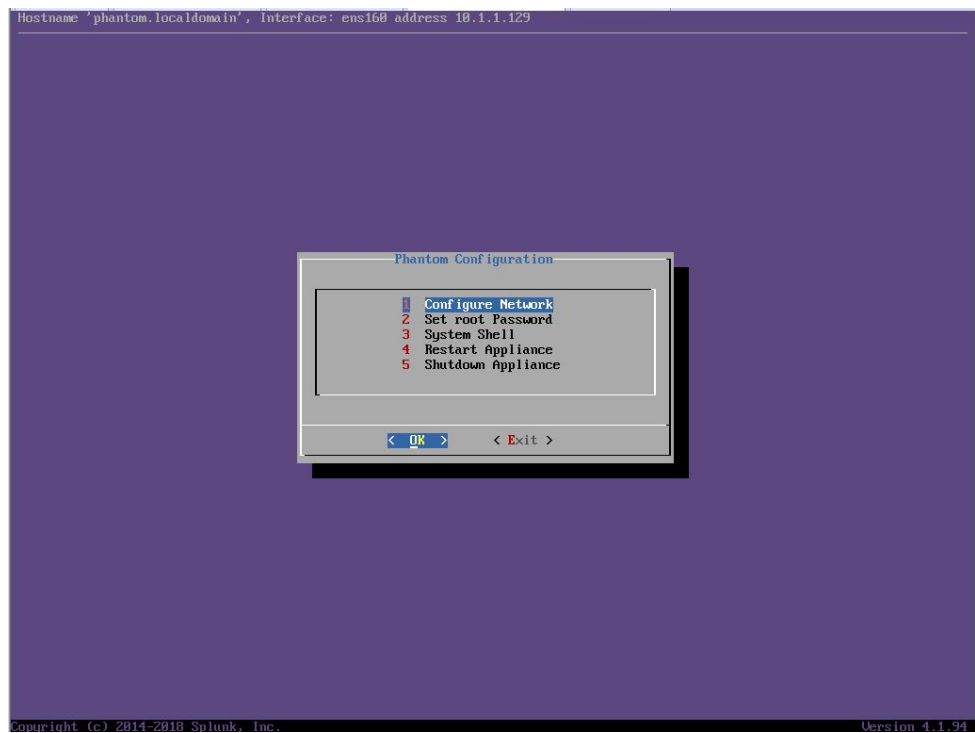
1. R80.10 SmartCenter VM installed (Configured to allow API on all interfaces)
 - a. IP: 10.1.1.101
 - b. username/password: root/vpn123
2. R80.10 Gateway
 - a. Internal IP: 10.1.1.254
 - b. External IP: NAT or Bridge IP
 - c. username/password: root/vpn123
3. Routable to the internet with DNS enabled
4. Download Phantom Playbook samples from this URL
<https://github.com/rickdevera/phantom-checkpoint>

Steps

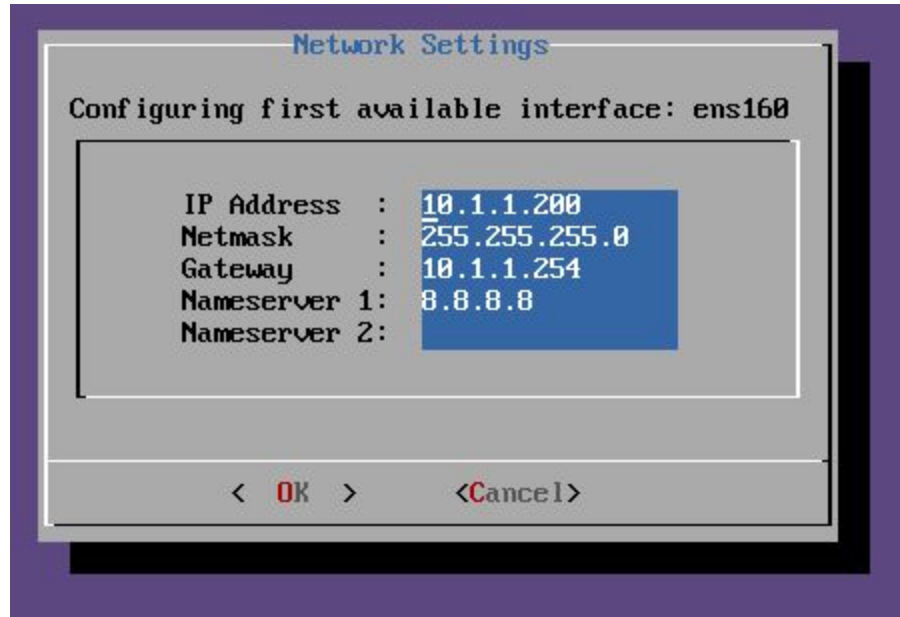
1. Download Splunk Phantom and import Phantom OVA on VMware Workstation
2. After import, attach Phantom VM network adapter to the same network as the Smart Center.
3. Startup Phantom and login into the console
 - a. Enter a new Password - 'vpn123'



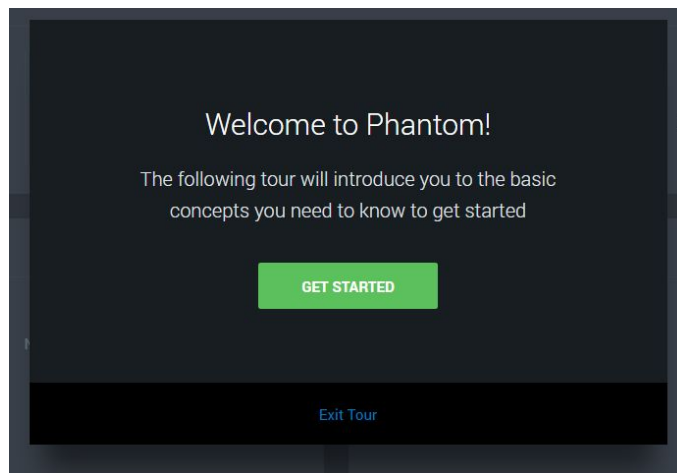
b. Phantom Configuration



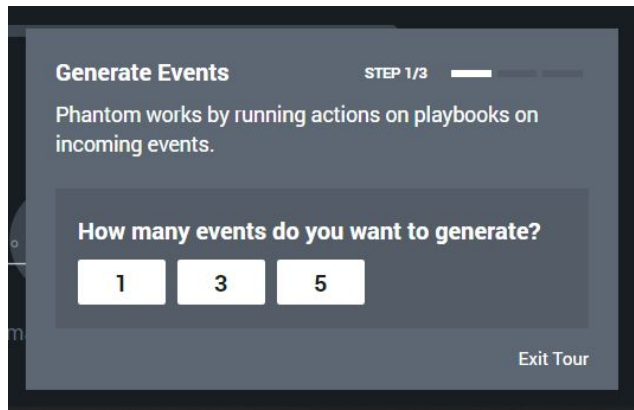
- i. Select Configure Network
- ii. Enter the following network information:



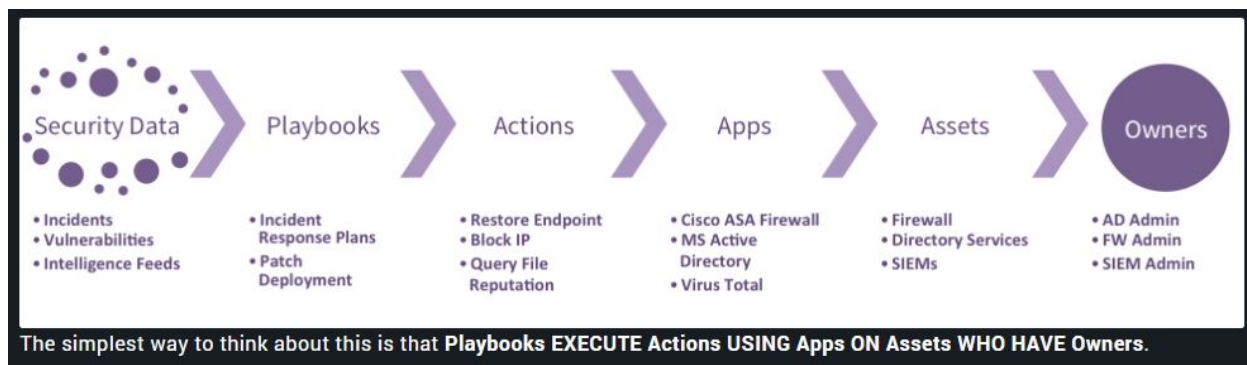
- iii.
- iv. Select 'OK'
- v. Be sure the Phantom server can access the internet to download the latest updates. Otherwise, offline updates will be required.
- vi. Using your web browser, go to <https://10.1.1.200>
- vii. Login with username/password: **admin/password**. (This is the default for new installations.)
- viii. Accept license agreement (must scroll through the entire agreement)



- ix. To simplify installation and learn about phantom, Click on Get Started, otherwise, Exit Tour. The Getting Started wizard can be restarted again.
- x. Select 1 event, and View the event.

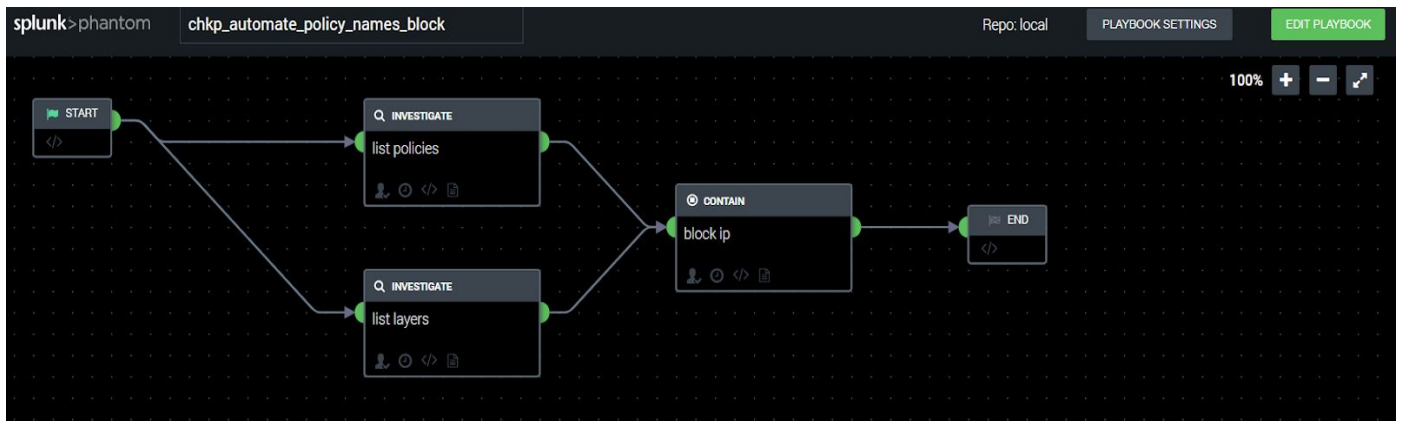


- xi. The events are generated for demo use.
- xii. Click on RUN PLAYBOOK
- xiii. Click on View the Playbook
 1. This document doesn't cover the details of Playbooks. Playbooks is a logical collection of actions that are executed from importing your data source. Notice each action (ie Investigate blocks). The information is basically in block diagram format. Playbooks execute actions using apps on assets who have owners. (Splunk->Phantom Documentation)



Below is the block diagram example of a playbook.

Using the Check Point R80 API, the playbook queries for the policy name and layer name, populates the containment action, block ip, with the information and executes a policy change on the SmartCenter. The SmartCenter, builds the objects, policies, and installs the policy automatically.



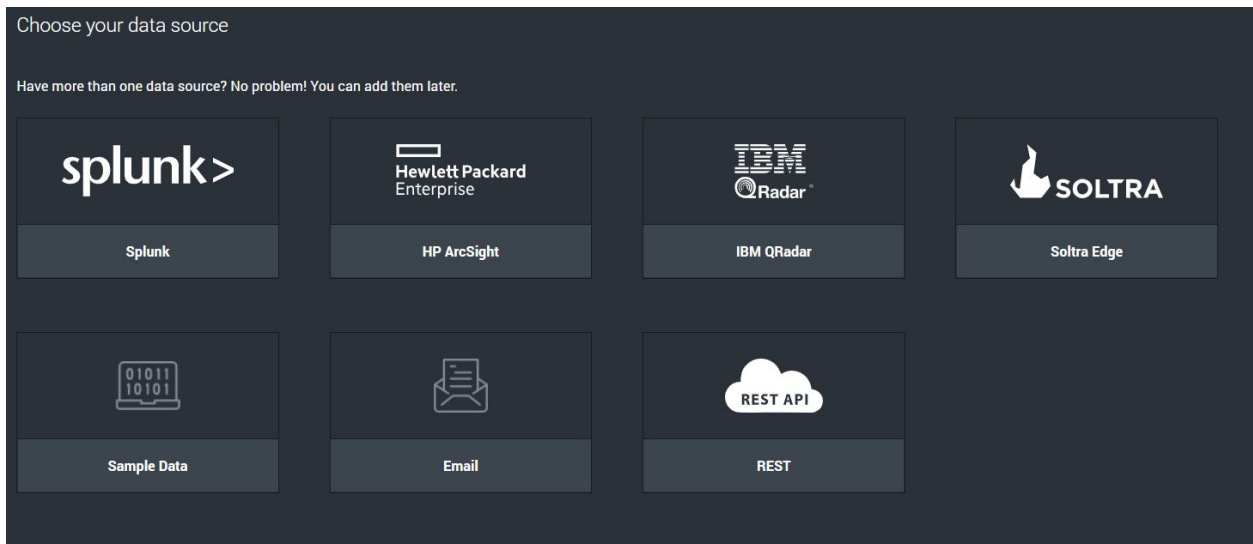
- xiv. Click on the CONFIGURE PHANTOM button
- xv. This will take you to the “Getting setup with Phantom” wizard.
 - 1. Enter the Company Name (ie Check Point) and click on SAVE and CONTINUE.
- xvi. Configure Data Source
- xvii. Continue from Basic Settings configuration
 - 1. For demo and connections email information is not required

The screenshot shows the 'Getting set up with Phantom' wizard, specifically the 'Basic Settings' tab. The interface includes the following elements:

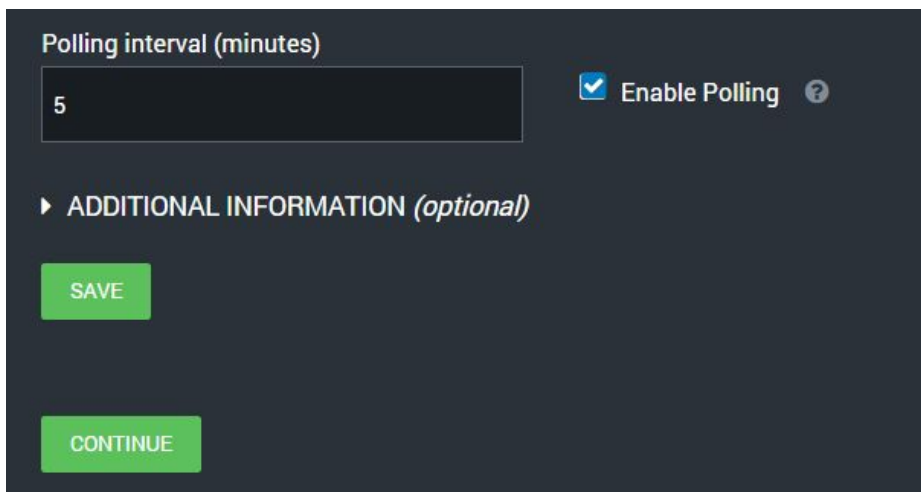
- Header:** 'Getting set up with Phantom', 'Basic Settings', and 'Data Sources'.
- Text:** 'Phantom requires an email server to send users email for action approvals, when SLAs are breached, and when items that they are tracking change. You can configure a server now or skip this and configure one later.'
- Section:** 'Configure'.
- ASSET SETTINGS:**
 - Asset name:** A dropdown menu with 'smtp' selected.
 - Server IP/Hostname:** An empty text input field.
 - SSL Method:** A dropdown menu with 'None' selected.
- ADDITIONAL INFORMATION (optional):** A section header with a right-pointing arrow.
- Buttons:** A green 'SAVE AND CONTINUE' button at the bottom.

- 2. Click on Save and Continue

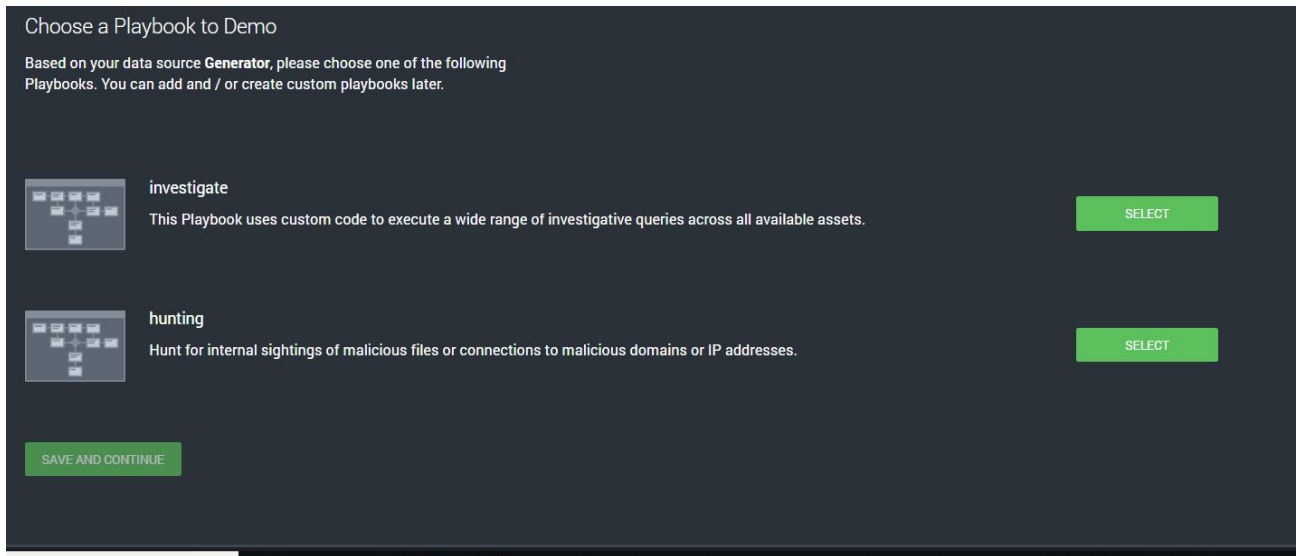
- xviii. Data Source configuration
 - 1. Choose Sample Data



- 2. Scroll down enter 5 minutes and check Enable Polling



- 3. click SAVE and CONTINUE
- xix. Playbook configuration
 - 1. Select **hunting**

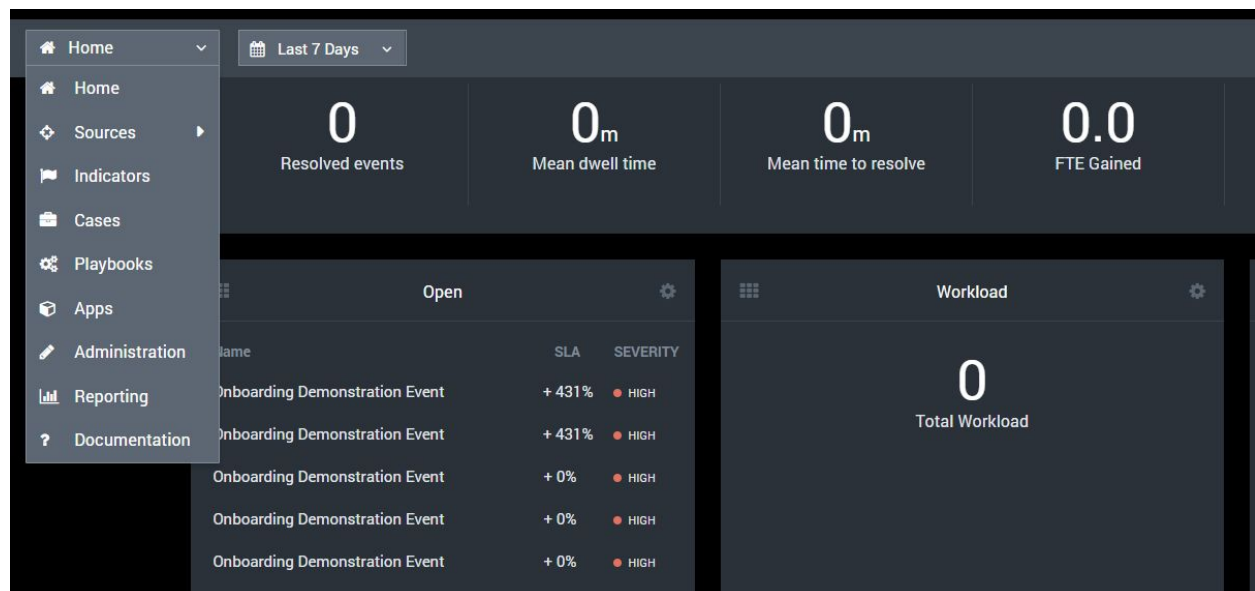


2. Click on **SAVE AND CONTINUE**

xx. Apps and Assets

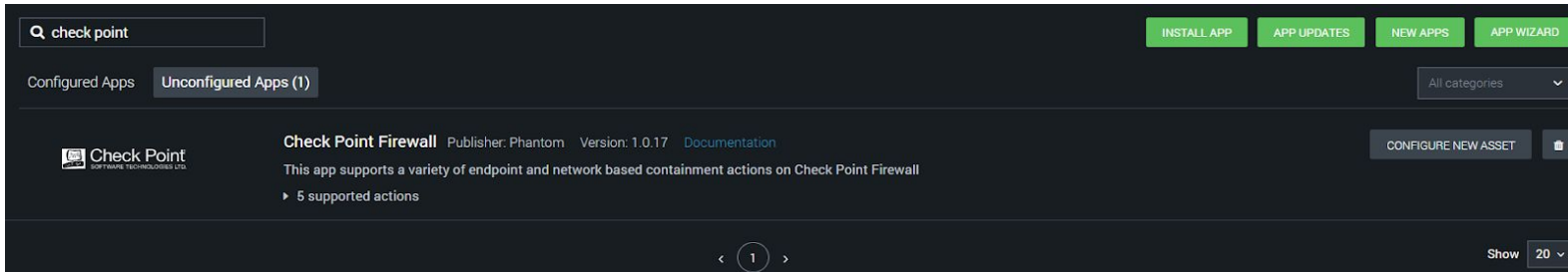
1. Choose SKIP REMAINING

xxi. After configuration select Home->Apps



xxii. Under Apps configuration,

1. select the Unconfigured Apps tab
2. In the Search box type in 'check point'
3. Click on **CONFIGURE NEW ASSET**



- xxiii. Asset Configuration
1. Goto -> Asset Info

Apps ▾

Description

This app supports a variety of endpoint and network based containment actions on Check Point

ASSET CONFIGURATION

CONFIGURE NEW ASSET

Asset (0)

Select existing asset ▾

Asset Info Asset Settings Approval Settings Access Control

Asset name

checkpoint

Asset description

Data Center firewall

Product vendor

Check Point Software Technologies

Product name

Check Point Firewall

- xxiv. Configure Asset Settings
 - 1. Select ->Asset Settings
 - a. Enter url of the WebUI of the Smart Center/Management Server
 - i. `https://10.1.1.10`
 - b. Enter the Administration Username and Password

Asset (1)

checkpoint

Asset Info **Asset Settings** Approval Settings Access Control

Management Server URL with port (e.g. https://10.10.10.10:443)

https://10.1.1.101/ Verify server certificate

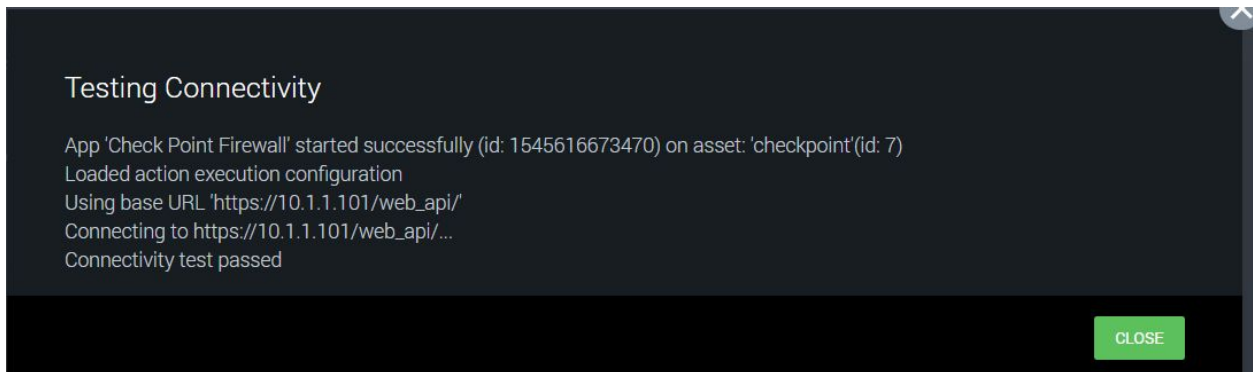
Username admin **Password**

Domain Optional

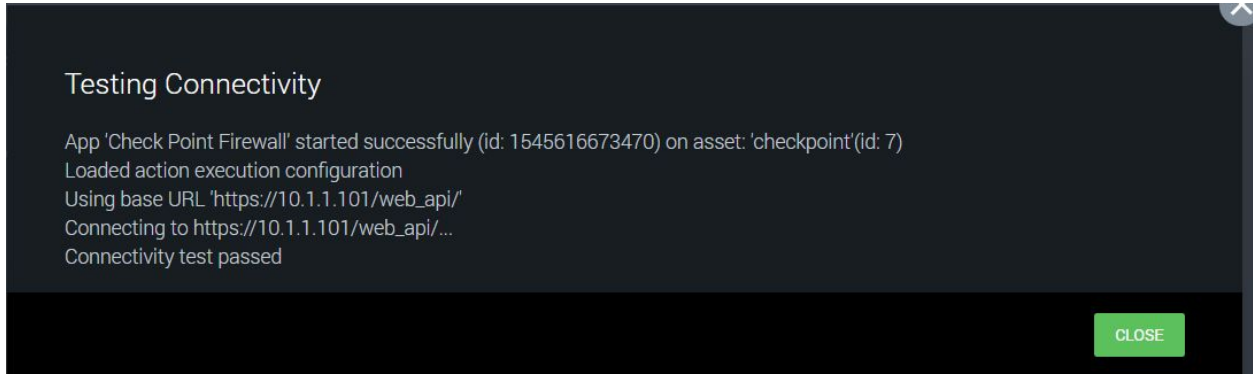
▶ Advanced

EDIT TEST CONNECTIVITY

- c. Click on Save and Click on Test Connectivity. The result should look like the following
- d.



- xxv. Get the name of the Check Point Policy and Policy Layer This can be done two ways,
 1. Open the SmartConsole and
- xxvi. .

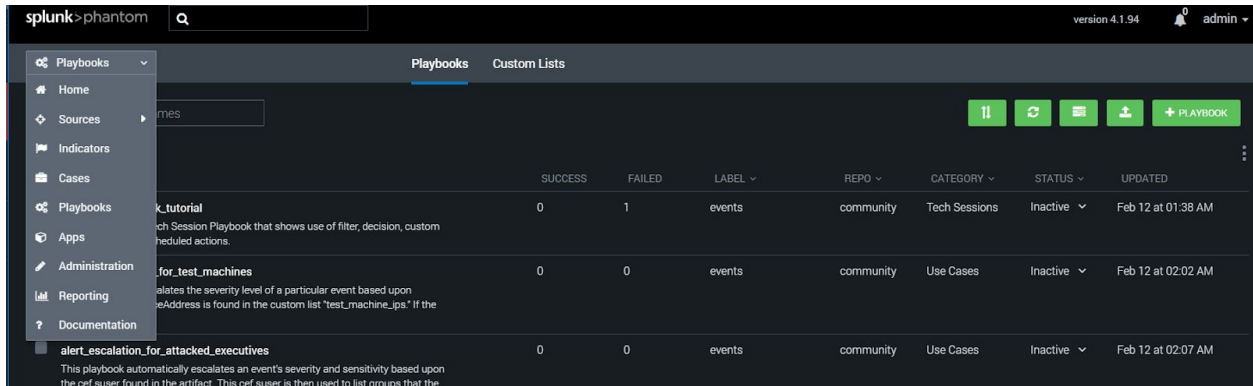


- c. Startup the SmartConsole
- 4.
 - a. Verify the policy.

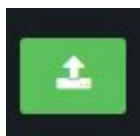
No.	Name	Source	Destination	VPN	Services & Application
1	For connectivity testing	A-SMS	A-GW	* Any	* Any
2		Net_10.1.1.0	* Any	* Any	* Any
3	Cleanup rule	* Any	* Any	* Any	* Any

- b. In the Phantom Portal, create a Playbook.
For this document, we will import a Playbook.

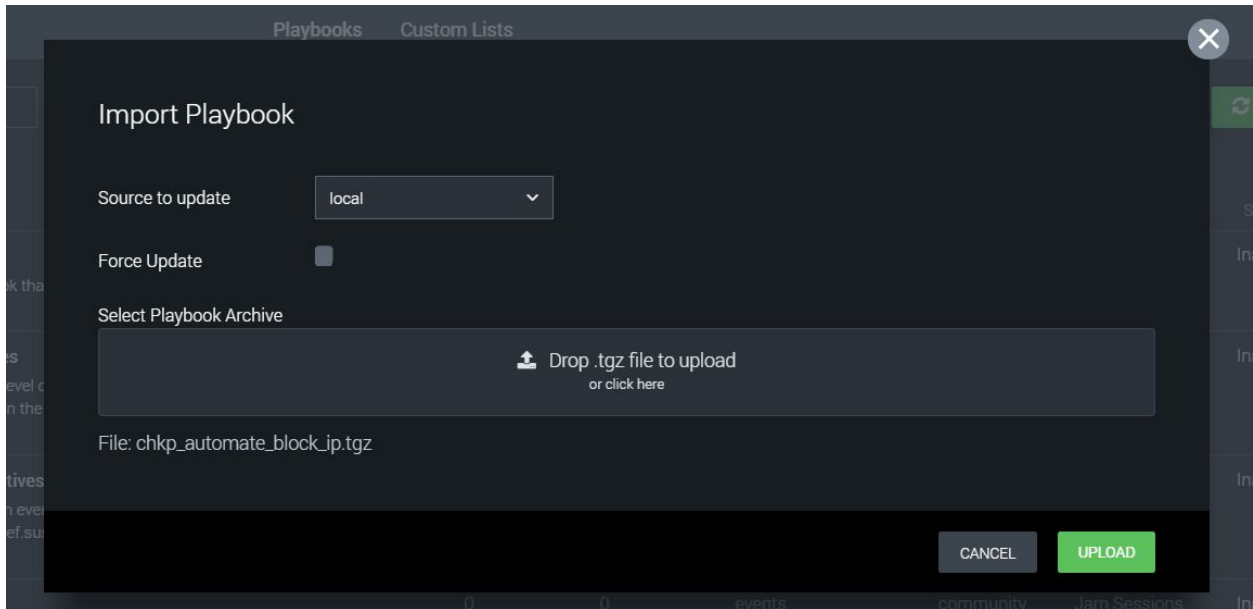
- c. Select Playbook on from the Main pulldown menu



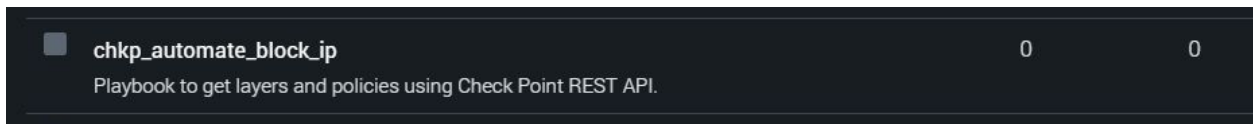
- d. Select the icon to import a playbook



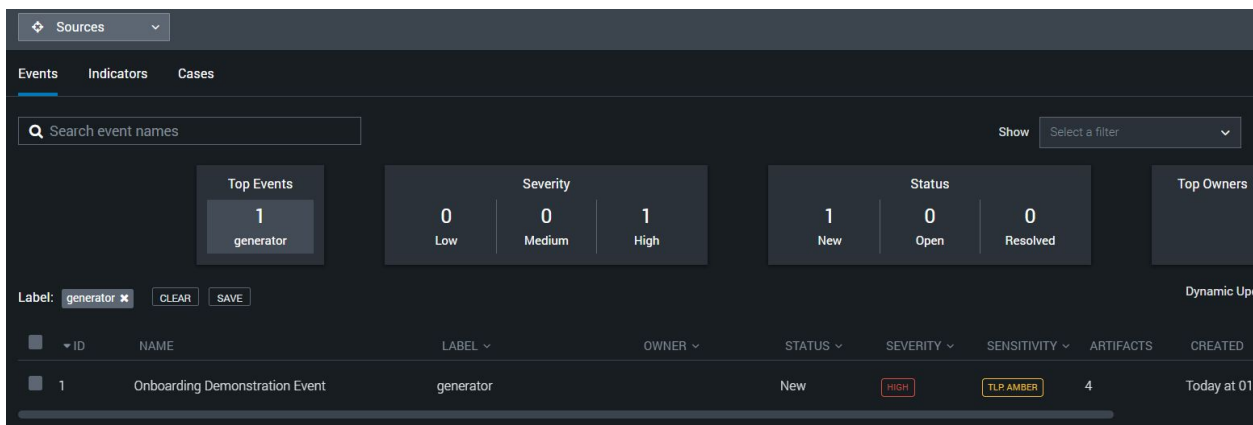
- e. From the Import Playbook screen, enter the following information
 - i. Source to update: local
 - ii. Force Update: unchecked
 - iii. File: chkp_automate_block_ip.tgz
- f. Click Upload



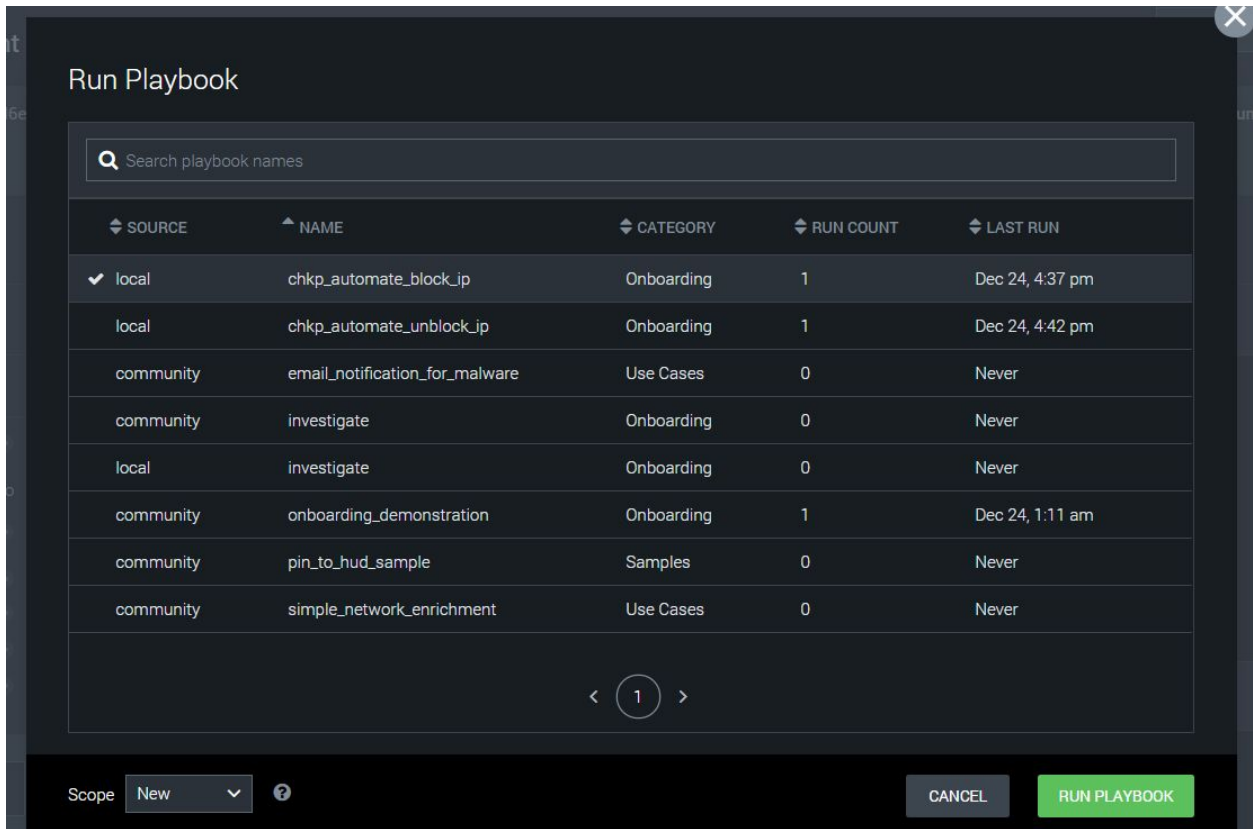
- g. Click DIMISS to continue
- h. Verify a the imported Playbook.



- i. From the Main Menu pulldown, select Sources->Generator



- j. Click on Onboarding Demonstration Event checkbox
- k. Click on Playbook on the right of the Display to Run a Playbook
- l. Select *chkp_automate_block_ip* and click on **RUN PLAYBOOK**



- m. After selection goto the Smart Console and verify the policy and object updates.

No.	Name	Source	Destination	VPN	Services & Application
1	phantom - 60.163.90.8/32	* Any	phantom - 60.163.90.8/32	* Any	* Any
2	For connectivity testing	A-SMS	A-GW	* Any	* Any
3		Net_10.1.1.0	* Any	* Any	* Any
4	Cleanup rule	* Any	* Any	* Any	* Any

Hosts 2

- phantom
- phantom - 60.163.90.8/32

- 5. Optional: Run an Action to remove update rule.

6.