

Project Summary

- 1) Assist in Setting up Python on a Windows 7 Workstation. python-3.7.4-amd64.exe is installed on the machine but will require assistance with any additional configurations needed for this project.
- 2) Assist in setting up Authentication, on the Windows 7 Workstation, to allow the Scripts to execute successfully.
- 3) Create Python Scripts based on the 2 scenarios detailed below in the “Project Details” section.
- 4) Provide the matching configurations of the Python scripts that were create in step #3 that can be used to verify the functionality using POSTMAN.

Resource

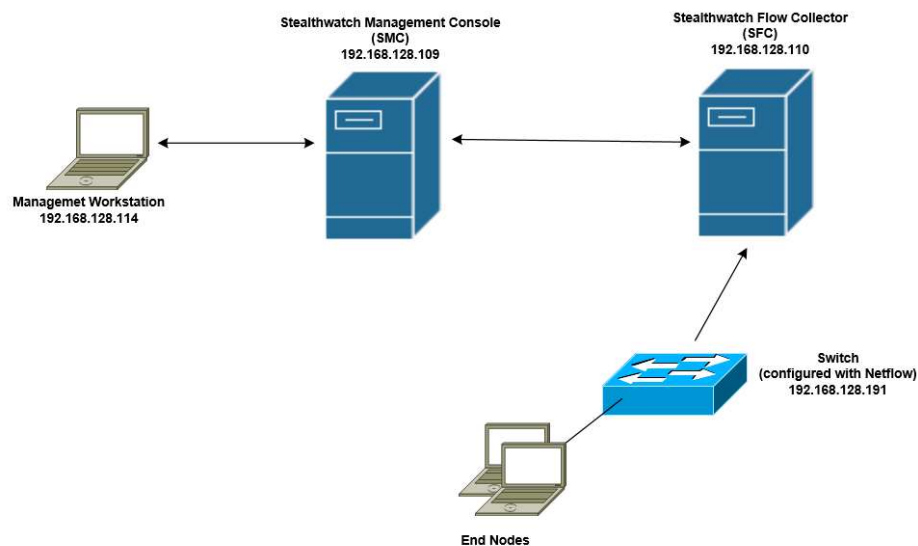
- Attached Document

Test Environment Details

- Workstation running Windows 7 with python-3.7.4-amd64.exe & Postman-win64-7.7.3-Setup.exe for testing if needed.
- Cisco Stealthwatch Management Console and Stealthwatch Flow Collector installed and configured.
- The systems will be configured with TFTP/IP and all necessary initialization.

Project Details

To be determined



Access Information

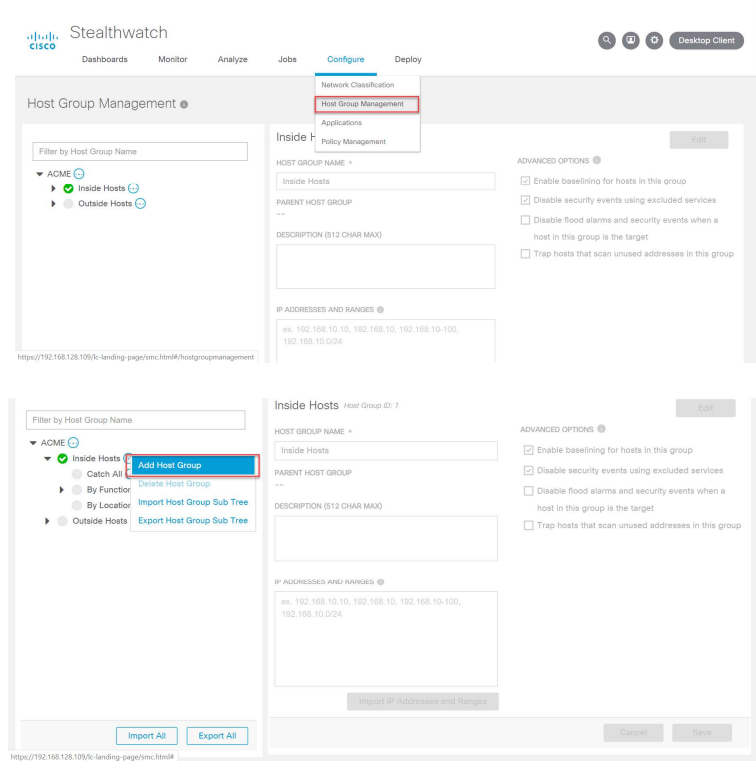
SMC GUI – username: admin / Password: WWTwwt1!
SFC GUI – username: admin / Password: WWTwwt1!
Switch SSH – username: admin / Password: WWTwwt1!
Switch – enable password: WWTwwt1!

Configuration Example

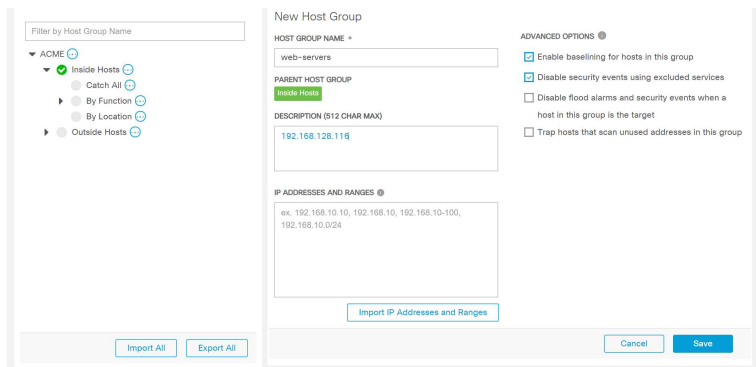
This scenario will use only the Web Interface.

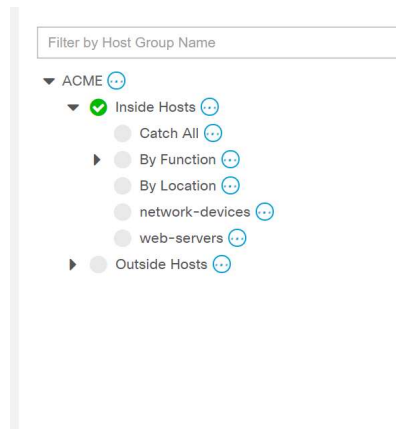
The starting point configuration will have two group network-devices and web-servers and a “Custom Policy” that restricts web-servers from communicating with network-devices.

Create a Host group.

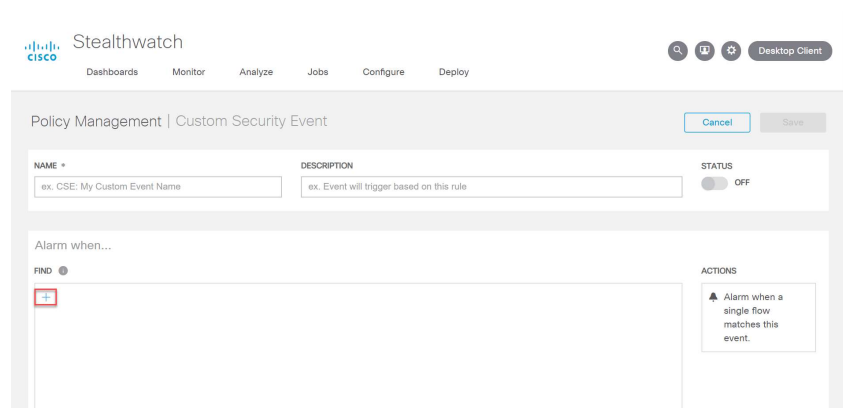
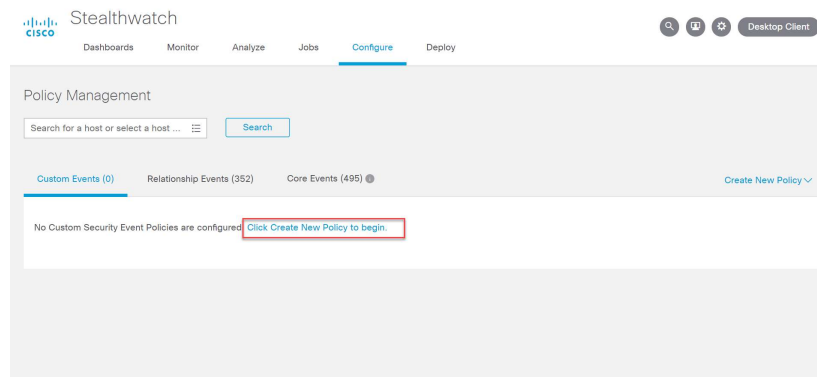
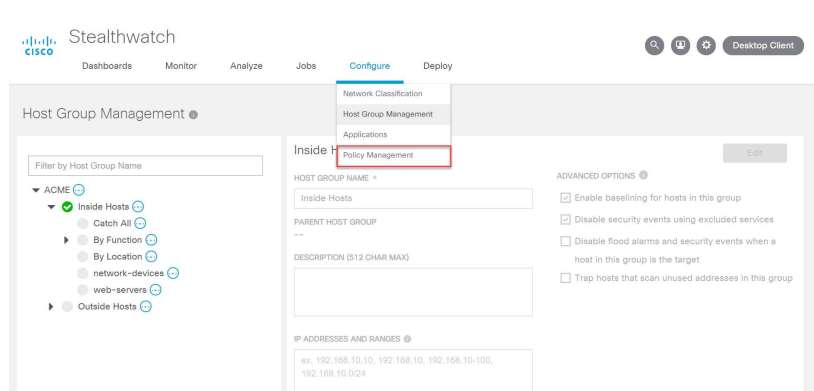


Add an IP address to the Host Group.





Create a Policy



Stealthwatch

Dashboards Monitor Analyze Jobs Configure Deploy

Policy Management | Custom Security Event

NAME *
Alarm_Web_Server_to_Network_Device

DESCRIPTION
ex. Event will trigger based on this rule

STATUS
OFF

Alarm when...

FIND

ACTIONS
Alarm when a single flow matches this event.

Stealthwatch

Dashboards Monitor Analyze Jobs Configure Deploy

Policy Management | Custom Security Event

NAME *
Alarm_Web_Server_to_Network_Device

DESCRIPTION
ex. Event will trigger based on this rule

STATUS
OFF

Alarm when...

FIND

ACTIONS
Alarm when a single flow matches this event.

Subject Host Groups

Search

☒ Include (1 click) ☐ Exclude (2 clicks) ☐ Clear (3 clicks)

☒ Inside Hosts

☐ By Function

☐ By Location

☐ Catch All

☐ network-devices

☒ web-servers

☐ Outside Hosts

Cancel Apply

Configure Deploy

DESCRIPTION
ex. Event will trigger based on this rule

STATUS
OFF

ACTIONS
Alarm when a single flow matches this event.

Stealthwatch

Dashboards Monitor Analyze Jobs Configure Deploy

Policy Management | Custom Security Event

NAME *
Alarm_Web_Server_to_Network_Device

DESCRIPTION
ex. Event will trigger based on this rule


STATUS
OFF

When any host within **web-servers** communicates with any **peer host**, an alarm is raised.

FIND

SUBJECT HOST GROUPS
web-servers

ACTIONS
Alarm when a single flow matches this event.

Stealthwatch

Search

Help

Settings

Desktop Client

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

Policy Management | Custom Security Event

CancelSave

NAME *

Alarm_Web_Server_to_Network_Device

DESCRIPTION

ex. Event will trigger based on this rule

STATUS

OFF

When any host within **web-servers** communicates with any host within **network-devices**, an alarm is raised.

FIND

SUBJECT HOST GROUPS

web-servers


AND

PEER HOST GROUPS

network-devices

ACTIONS

Alarm when a single flow matches this event.

Stealthwatch

Search

Help

Settings

Desktop Client

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

Policy Management

Search for a host or select a host... Search

Custom Events (1)

Relationship Events (352)

Core Events (495)


Create New Policy

EVENT	DESCRIPTION	DATE MODIFIED	SUBJECT	PEER	STATUS	ACTIONS
<div>Ex. Data Event</div>	<div>Ex. Data Center</div>	<div>Ex. 01/28/2018 12:00</div>	<div>Ex. Inside Hosts</div>	<div>Ex. Inside Hosts</div>	<div>Ex. On</div>	
Alarm_Web_Server_to_Network_Device		10/25/2019 10:45 PM	web-servers	network-devices	Off	

10

Items per page

1 - 1 of 1 items

Stealthwatch

Search

Help

Settings

Desktop Client

Dashboards

Monitor

Analyze

Jobs

Configure

Deploy

Policy Management

Search for a host or select a host... Search

Custom Events (1)

Relationship Events (352)

Core Events (495)

Create New Policy

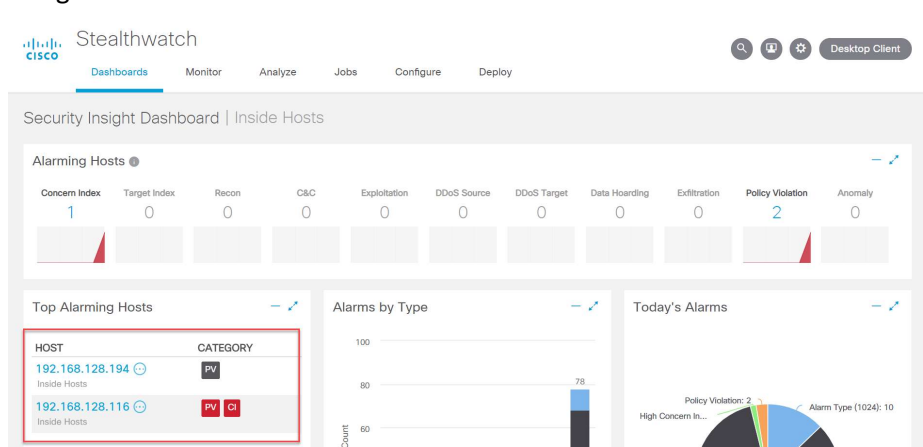
EVENT	DESCRIPTION	DATE MODIFIED	SUBJECT	PEER	STATUS	ACTIONS
<div>Ex. Data Event</div>	<div>Ex. Data Center</div>	<div>Ex. 01/28/2018 12:00</div>	<div>Ex. Inside Hosts</div>	<div>Ex. Inside Hosts</div>	<div>Ex. On</div>	
Alarm_Web_Server_to_Network_Device		10/25/2019 10:45 PM	web-servers	network-devices	On	

10

Items per page

1 - 1 of 1 items

View top Alarming Hosts



The scrip will build on the existing configuration.

The script will add a group named db-servers, add a host IP address to the db-servers group and create a policy to generate an alarm if db-servers group communicates with network-devices group and turns the policy on.

The script will also allow the user to get a recent list of “Top Alarming” hosts on the screen and another script will save the “Top Alarming” hosts to a .cv file.