Cisco ASA Playbook Document

MANNAI TRADING CO. WLL

Member of Mannai Corporation QPSC

MICROSOFT SOLUTIONS

Your Complete Guide to achieve Digital Transformation

Contents

1. Overview

Cisco Adaptive Security Appliance (ASA) Software is the core operating system for the Cisco ASA Family. It delivers enterprise-class firewall capabilities for ASA devices in an array of form factors - standalone appliances, blades, and virtual appliances - for any distributed network environment. ASA Software also integrates with other critical security technologies to deliver comprehensive solutions that meet continuously evolving security needs.

This integration allows to automate response to Microsoft Sentinel incidents which contain IPs. It contains the basic connector component, with which you can create your own playbooks that interact with Cisco ASA. It also contains 3 playbook templates, ready to quick use, that allow direct response on Cisco ASA from Microsoft Teams.

Using Logic Apps gateway

On a server in your network install the on-premises data gateway, see Install on-premises data gateway for Azure Logic Apps. The server on which the data gateway is installed needs to be able to reach the Cisco ASA REST API. Also the SSL certificate used by the Cisco ASA REST API needs to be able to be validated on the server, including the certificate chain. When deploying the Cisco ASA connector choose the option via on-premises data gateway. When using the connector you will be asked to select the data gateway you want to use.

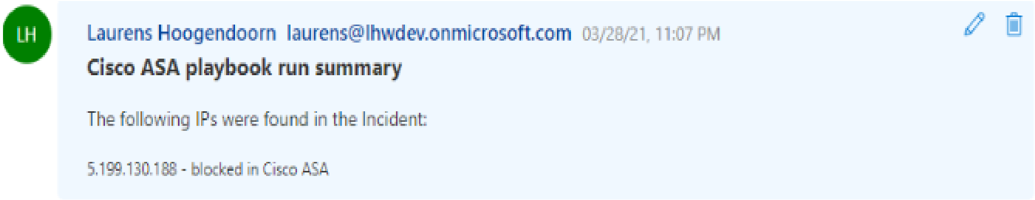
2. Block IP – Cisco ASA

Purpose: This playbook allows blocking/allowing of IPs in Cisco ASA, using a **Network Object Group**. This allows making changes to a Network Object Group members, instead of making Access Control Entries. The Network Object Group itself should be part of an Access Control Entry.

Type: Sentinel Trigger

Uses: When a new Sentinel incident is created, this playbook gets triggered and performs below actions

1. For the IPs we check if the IP are already a member of the Network Object Group
2. An adaptive card is sent to a Teams channel with information about the incident and giving the option to ignore an IP, or depending on its current status block it by adding it to the Network Object Group or unblock it by removing it from the Network Object Group.
3. Comment is added to Microsoft Sentinel incident.



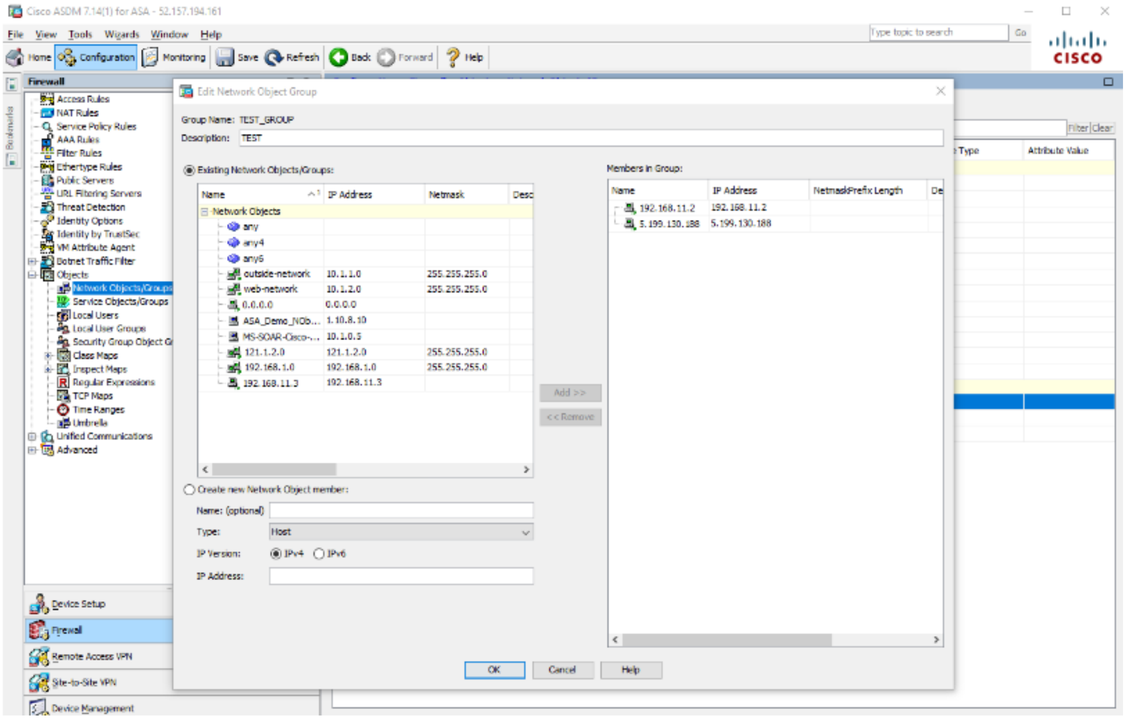
Laurens Hoogendoorn laurens@lhwdev.onmicrosoft.com 03/28/21, 11:07 PM

Cisco ASA playbook run summary

The following IPs were found in the Incident:

5.199.130.188 - blocked in Cisco ASA

IP is added to Cisco ASA object group:



Edit Network Object Group

Group Name: TEST_GROUP

Description: TEST

● Existing Network Objects/Groups:

Name	IP Address	Netmask	Desc
Network Objects			
any			
any4			
any6			
outside-network	10.1.1.0	255.255.255.0	
web-network	10.1.2.0	255.255.255.0	
0.0.0.0	0.0.0.0		
ASA_Demo_NOb...	1.10.8.10		
MS-SOAR-Cisco-...	10.1.0.5		
121.1.2.0	121.1.2.0	255.255.255.0	
192.168.1.0	192.168.1.0	255.255.255.0	
192.168.11.3	192.168.11.3		

Members in Group:

Name	IP Address	Netmask/Prefix Length	De
192.168.11.2	192.168.11.2		
5.199.130.188	5.199.130.188		

○ Create new Network Object member:

Name: (optional)

Type: Host

IP Version: ● IPv4 ○ IPv6

IP Address:

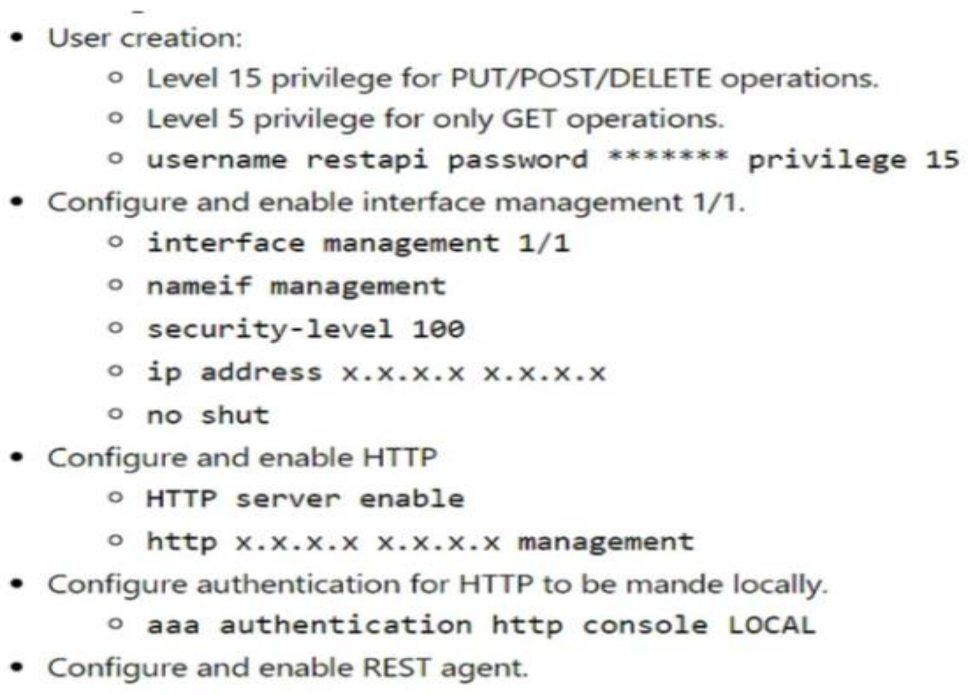
Prerequisites

1. **This playbook template is based on Microsoft Sentinel Incident Trigger which is currently in Private Preview (Automation Rules).** You can change the trigger to the Sentinel Alert trigger in cases you are not part of the Private Preview.
2. Cisco ASA custom connector needs to be deployed prior to the deployment of this playbook, in the same resource group and region. Relevant instructions can be found in the connector doc page.
3. In Cisco ASA there needs to be a Network Object Group. You can create a Network Object Group using Cisco ASDM, Configure a Network Object Group, or using the CLI, Configuring a Network Object Group. The Network Object Group can be blocked using an access rule, Configure Access Rules

Note: In Cisco ASA create a local user and allow it to use the REST API. Depending on the playbook used the user needs to be able to add members to a network object group or create access control entries, by default that requires privilege level 15.

https://medium.com/@daniela.mh20/rest-api-for-cisco-asa-3374a22d2e24

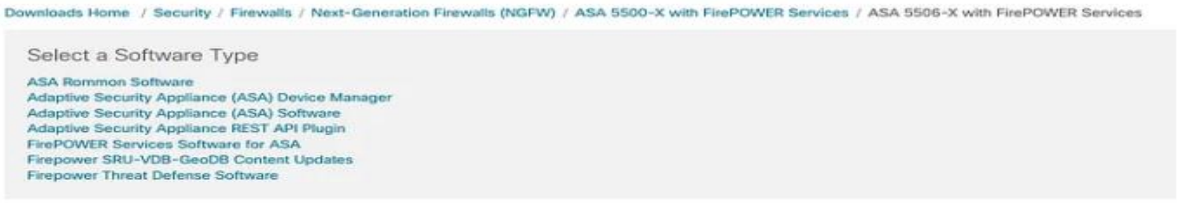
[Cisco ASA REST API Quick Start Guide]()



- User creation:
  - Level 15 privilege for PUT/POST/DELETE operations.
  - Level 5 privilege for only GET operations.
  - `username restapi password ******* privilege 15`
- Configure and enable interface management 1/1.
  - `interface management 1/1`
  - `nameif management`
  - `security-level 100`
  - `ip address x.x.x.x x.x.x.x`
  - `no shut`
- Configure and enable HTTP
  - `HTTP server enable`
  - `http x.x.x.x x.x.x.x management`
- Configure authentication for HTTP to be mande locally.
  - `aaa authentication http console LOCAL`
- Configure and enable REST agent.

REST API AGENT

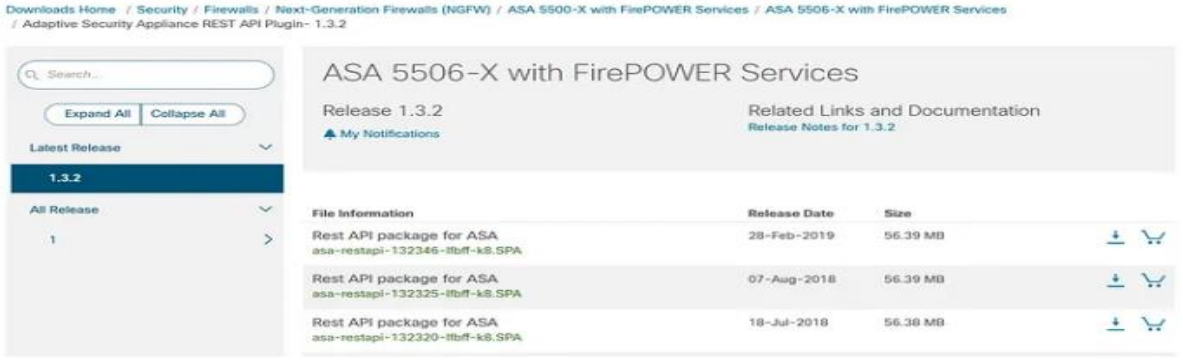
From Cisco software web page, download .SPA file, transfer the file to your ASA and enable it.



Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / ASA 5500-X with FirePOWER Services / ASA 5506-X with FirePOWER Services

Select a Software Type

ASA Rommon Software
Adaptive Security Appliance (ASA) Device Manager
Adaptive Security Appliance (ASA) Software
Adaptive Security Appliance REST API Plugin
FirePOWER Services Software for ASA
Firepower SRU-VDB-GeoDB Content Updates
Firepower Threat Defense Software



Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / ASA 5500-X with FirePOWER Services / ASA 5506-X with FirePOWER Services / Adaptive Security Appliance REST API Plugin- 1.3.2

ASA 5506-X with FirePOWER Services

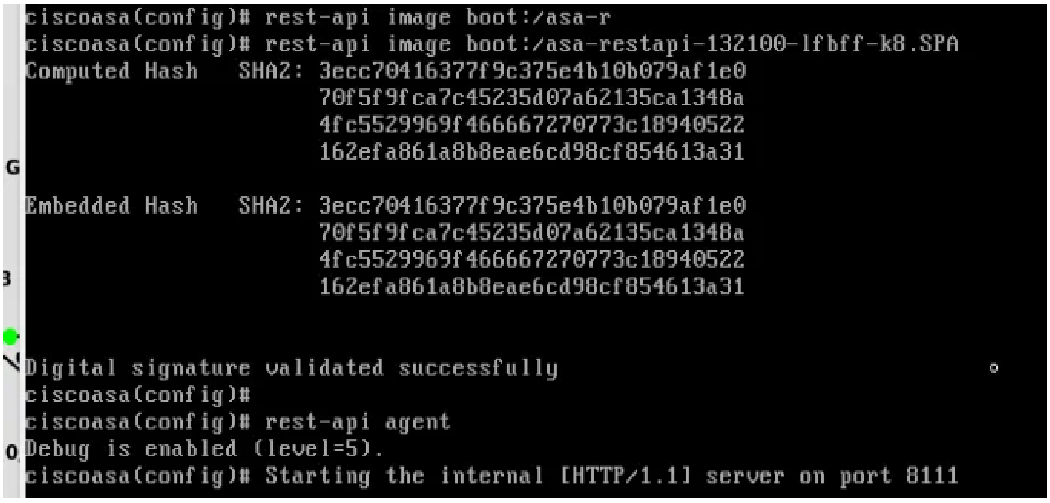
Release 1.3.2
My Notifications

Related Links and Documentation
Release Notes for 1.3.2

File Information	Release Date	Size
Rest API package for ASA asa-restapi-132346-lfbff-k8.SPA	28-Feb-2019	56.39 MB
Rest API package for ASA asa-restapi-132325-lfbff-k8.SPA	07-Aug-2018	56.39 MB
Rest API package for ASA asa-restapi-132320-lfbff-k8.SPA	18-Jul-2018	56.38 MB

Global config mode:

- **rest-api image disk0:/asa-restapi-xxxxx.**
- **rest-api agent.**



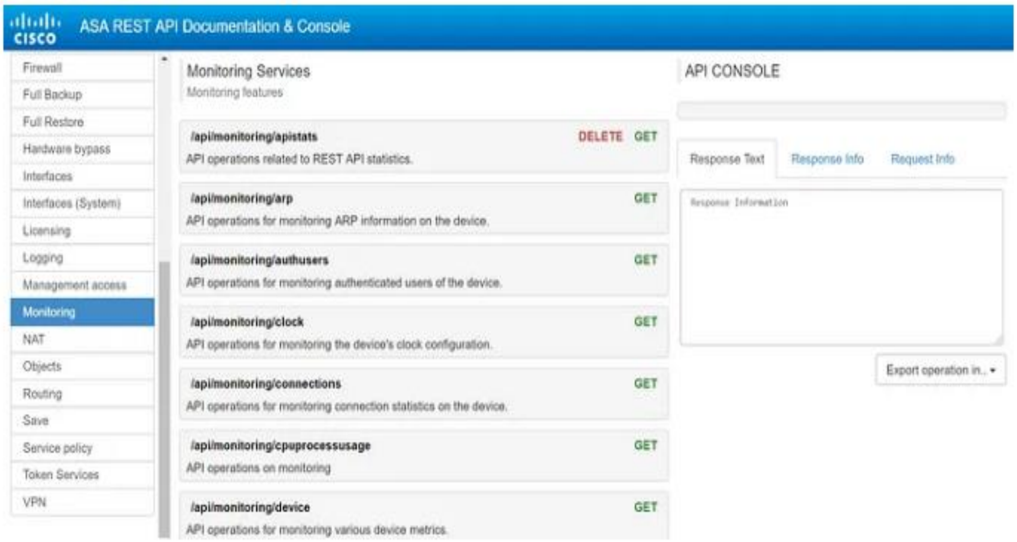
```
ciscoasa(config)# rest-api image boot:/asa-r
ciscoasa(config)# rest-api image boot:/asa-restapi-132100-lfbff-k8.SPA
Computed Hash   SHA2: 3ecc70416377f9c375e4b10b079af1e0
                      70f5f9fca7c45235d07a62135ca1348a
                      4fc5529969f466667270773c18940522
                      162efa861a8b8eae6cd98cf854613a31

Embedded Hash   SHA2: 3ecc70416377f9c375e4b10b079af1e0
                      70f5f9fca7c45235d07a62135ca1348a
                      4fc5529969f466667270773c18940522
                      162efa861a8b8eae6cd98cf854613a31


Digital signature validated successfully
ciscoasa(config)#
ciscoasa(config)# rest-api agent
Debug is enabled (level=5).
ciscoasa(config)# Starting the internal [HTTP/1.1] server on port 8111
```

To validate web Documentation.

The actual documentation WEB page for Cisco's ASA apis, are accesible trough the following URL:

URL: https://[YOUR MANAGMENT IP ADDREES]/doc

Here you can check all the requests you can do and the URL's to get them done.



Monitoring Services
Monitoring features

/api/monitoring/apistats DELETE GET
API operations related to REST API statistics.

/api/monitoring/arp GET
API operations for monitoring ARP information on the device.

/api/monitoring/authusers GET
API operations for monitoring authenticated users of the device.

/api/monitoring/clock GET
API operations for monitoring the device's clock configuration.

/api/monitoring/connections GET
API operations for monitoring connection statistics on the device.

/api/monitoring/cpuprocessusage GET
API operations on monitoring

/api/monitoring/device GET
API operations for monitoring various device metrics.