FortiGate integration for input traffic blocking

Use case for this script integration is to block some input traffic by firewall rule or policy.

Use-case

Use case for this script integration is to block some input traffic by firewall rule or policy. To achieve it we have a script which does create an address object and add it to a predefined address group which is then used to block traffic. This is now designed to work only for IPv4 addresses.

As it's described in the https://kb.fortinet.com/kb/documentLink.do?externalID=FD45208 we can revert this to block certain traffic assigned to the group.

There is a limitation to this which would depend on a platform (https:/docs.fortinet.com/max-value-table) as it has a maximum of 600 members in the address group for the policy.

These scripts were tested on Flowmon 11 with ADS 11 and FortiOS 6.4.3 but they should work also on the older version. However, they might require some additional Python packages which aren't available on the older versions. It's recommended to use version 12.4 or newer.

FortiGate configuration

First, we need to create an address group

```
config firewall addrgrp
   edit "ads_detected"
        set member "none"
    next
end
```

This group has one member which special address 0.0.0.0/32 which doesn't block anything.

```
config firewall local-in-policy
    edit 1
        set intf "port1"
        set srcaddr "ads_detected"
        set dstaddr "WAN_IP"
        set service "ALL_ICMP"
       set action deny
        set schedule "always"
    next
end
```

So, in my example I created a local policy to drop all ICMP traffic incoming to my WAN interface (port1) with IP address WAN_IP, this is happening always when the source address is in a group of ads_detected.

This is all that we need to do at FortiGate firewall site. In a similar way you can set up this script to use this address group in some firewall policy.

Script and Flowmon ADS configuration

This guide assumes that you have Flowmon ADS configured with active Data Feeds and basic tuning completed. More details about configuration of the Flowmon system are in the User guide, which is included in every Flowmon appliance, or alternatively at the following location: https://docs.progress.com/.

There are two scripts, first called **ag-mitigation.py** is to be imported to Flowmon ADS and is adding the IP address to the group used for blocking. The **ag-timeout.py** is the part responsible for removing after a certain time the record from the address group and thus from blocking.

The scripts are part of the ZIP file which can be extracted to /home/flowmon/fgt-mitigation/ directory and where it would by default place it's database and expects the configuration.

If you wish to use a different directory you would need to modify the scripts and specify the location.

Cron configuration for the ag-timeout.py

There is a script prepared for removal of blocked IP addresses to make sure the group would be able to handle a new request. On SSH console access you can run a command crontab -e to edit a cron table and add to the last line something like

```
# Adress group address removal
0 * * * * /home/flowmon/fgt-mitigation/ag-timeout.py 2>&1
```

If you want to use a different schedule, then you can find some help on the first parameter https://cron.help/every-hour

Script configuration

The script configuration is placed in /home/flowmon/fgt-mitigation/etc where are two INI files. One for the script parameters and another for the logging.

You can modify them directly on the Flowmon appliance using vim i.e. **vim /home/flowmon/fgt-mitigation/etc/ag-config.ini**

```
# Configuration Section for connection to the FortiGate Firewall
[FortiGate]
# IP or hostname of the firewall
IP = 192.168.47.28
# web management port
HTTPS = 443
# API key to allow controll of addreses and groups
API_KEY = fp8114zdNpjp8Qf8zN4Hdp57dhgjjf
# name for address group for the script
GROUP = FlowmonADS
# is TLS certificate to be verified
# set yes if not using the self-signed one
verify = no

[script]
script_dir = /data/components/fgt-mitigation
# Location of the database to keep track of IPs
DBFILE = %(script_dir)s/data.db
# Time to live of record for ban in minutes
TTL = 360
# Time to decrease from TTL
# this should be set up based on how often timeout script is started.
decrease = 60
"/data/components/fgt-mitigation/etc/ag-config.ini" 25L, 708C
```

Script configuration open with vim

Where you can set up an IP address or hostname for the FortiGate device and its web interface port. Then API_KEY created in FortiGate with access to API to allow creation of address and modification of groups. Also, TTL and decrease could be changed if needed. Default is 6 hours and to be decreased by 60 minutes as the timeout script is to run every hour.

Those parameters may be also provided as script parameters.

Optional:
- --fw IP / hostname of FortiGate firewall
- --port HTTPS port on the FortiGate firewall
- --group Name of Address group
- --key FortiGate API key

Create Perspective(s)

Create one or more Perspectives to categorize anomalies on the network.

This guide gives an example only. In production, you must find what traffic your organization would like to enable alerts and triggers on.

1. Within the ADS module, go to **Settings** > **Processing** > **Perspectives**.
2. Click **+ NEW PERSPECTIVE**.

    a) Provide a **Name**.

    b) Select the relevant **Filter**.

    c) Select the relevant **Data feed**.

    d) Select the priority (Critical, High, Medium, Low, and Informational) and add the relevant detection methods to each priority.

    e) Click **SAVE**.

Create a Custom Script (API trigger)

In Flowmon ADS, custom scripts are used to automate actions when anomalous events are detected according to the configured Perspective. Each custom script must be bound to exactly one Perspective. A script can be in the active or inactive state.

1. Within the ADS Module, go to **Settings > System Settings > Custom scripts**.
2. Click **+ NEW CUSTOM SCRIPT**.
3. Provide a **Name** for the script.
4. Under **File**, click **Choose file** and select the custom script to trigger FortiGate mitigation action.
5. Click **SAVE**.
6. Within the ADS Module, go to **Settings > Processing > Custom scripts**.
7. Click **+ NEW CUSTOM SCRIPT ACTION**.
8. Provide a **Name** for the action.

   Select the **Perspective**.
9. Tick the box to make the action **Active**.
10. Set the **Minimum priority to be reported**.
11. Click **SAVE**.

Perspective Methods

Methods outlined within the perspectives shown are recommendations and should be adjusted as relevant to your network access details. Progress Flowmon engineers are available to assist with determining which methods should be leveraged and we recommend the testing of triggers to ensure all is working as expected before enabling the actions taken by this script in production.

As a good starting point leveraging the methods: SCANS, RANDOMDOMAIN, BPATTERNS, DICTATTACK, SSHDICT, RDPDICT, and BLACKLIST (BotnetActivities, MalwareDomains and BotnetDomains) will provide detection of hosts that are carrying out anomalous actions.