FortiGate integration for input traffic

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 particular 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. The package can be installed only on version 10.3.9 and newer.

FortiGate configuration

First we need to create a 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
```

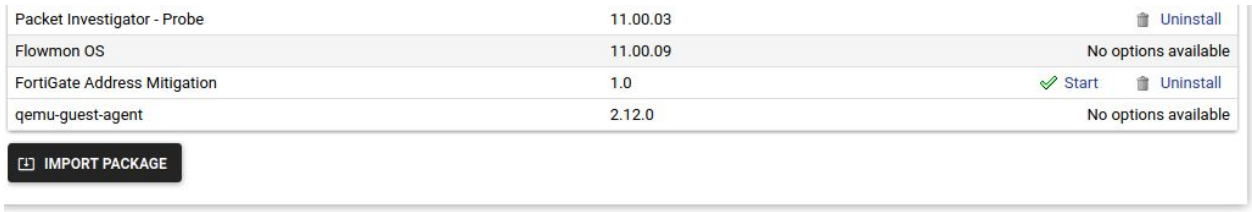
So, in my example I created a local policy to drop all ICMP traffic incoming to my WAN interface (port1) with IP address WAN_IP, this is happening always when the source address is in a group of ads_detected.

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 configuration

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.

Those scripts are both at the integration package ag-mitigation.tar.gz which is just a standard Flowmon package and it's to be installed by Configuration Centre like any other package.



The only two actions are to start the script which will add the call for ag-timeout.py to the cron scheduler for Flowmon user and uninstall which is going to remove it from the appliance.

Scripts are located at directory */data/components/fgt-mitigation/* and configuration is at file */data/components/fgt-mitigation/etc/ag-config.ini* and can be edited for instance by vim like **vim /data/components/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
```

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.
I recommend to use the decrease based on value set to cron how often this should be checked.

The configuration for logging in in the second file and probably won't need to be changed.

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

To configure the ADS with a custom script you can find at ADS user guide or in the previous guide for mitigation with FortiGate.