SOC Duck


Description:

Build your own visual alert DUCKhickey that integrates with the Palo Alto Networks platform using the HTTP Log Forwarding feature in PAN-OS 8.X and above. I configured the SOC Duck in the Black Hat NOC to trigger and light up with threat alerts. The alerts are configurable for how and when the SOC Duck is triggered.

Purpose:

This is for experimental purposes only - to create a cool *thing*. This is not intended to be used in a production environment and is supported as best effort. If you happen to make this production ready or utilize this in your Operations Center please let us know!

Components List:

If you attended the Black Hat USA conference in 2019, then you would have received a kit of components from the Palo Alto Networks booth in the Expo Hall. If you want to build your own then here is what you will need to get started:

- Sacrificial Rubber Ducky
- ESP32 Development Board
- LEDs
- Arduino IDE Open-source Software

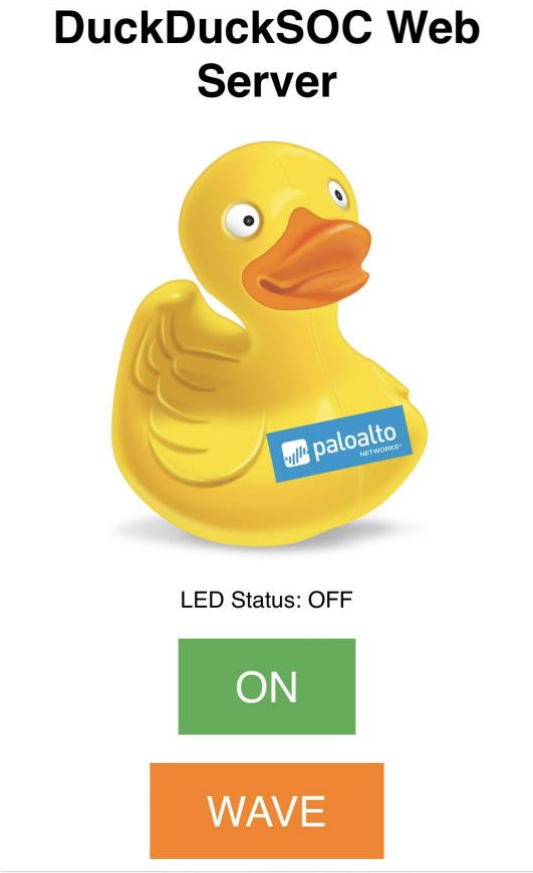
Getting Started:

If you are brand new to Arduino and need a kick-start on how to get the things to connect START HERE.

Official Documentation for ESP-IDF (Espressif IoT Development Framework)

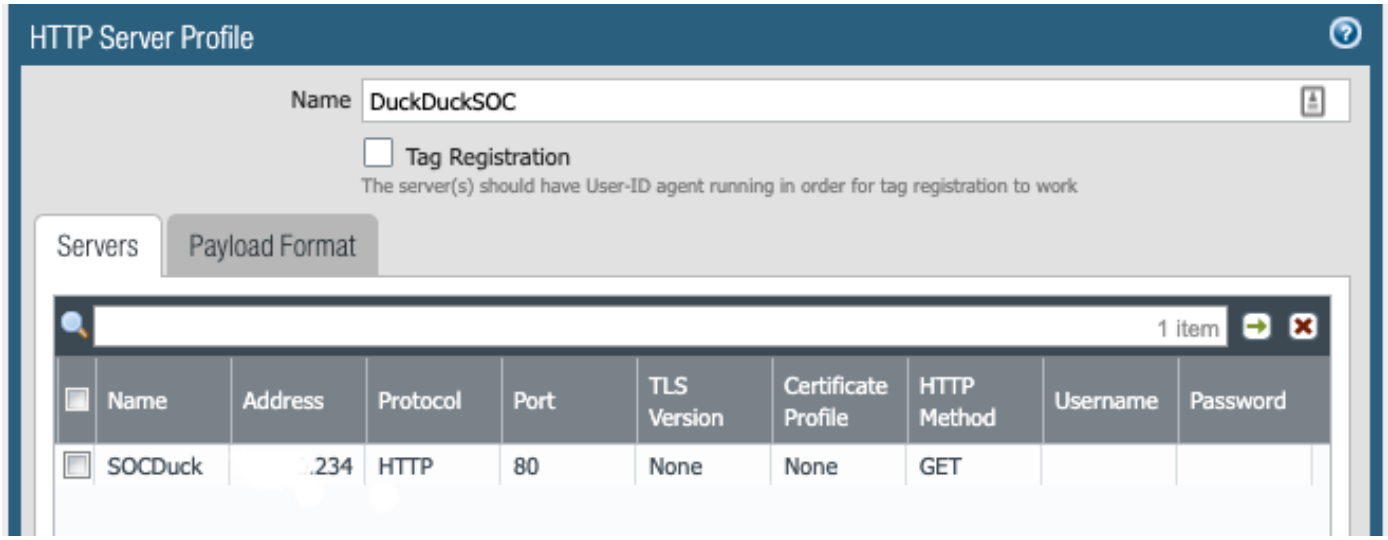
Flash the Firmware:

Once you are able to establish communication with your ESP32 development board then upload this firmware to it. This will set up the ESP32 as an HTTP web server. Follow the README in order to get this set up successfully.



PAN-OS Configuration:

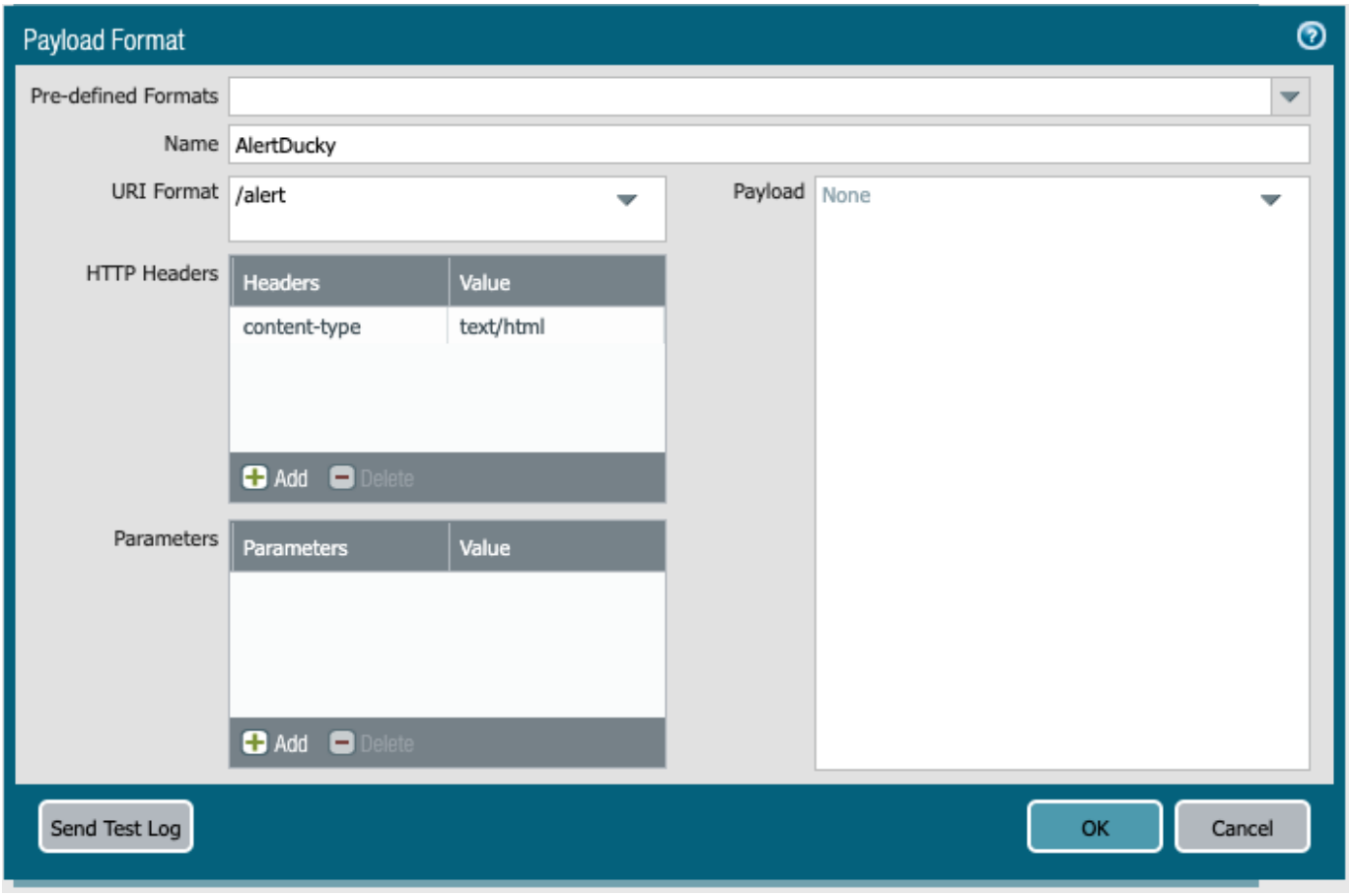
Within the Palo Alto Networks GUI navigate to **Device > HTTP** and add an HTTP Server Profile:



Name: Give it a wicked cool name or you can use what I have ☺
Address: You will input the IP address that the ESP32 displays within the IDE serial monitor
Protocol: HTTP
Port: 80
TLS: None
Certificate Profile: None
HTTP Method: GET

After this is complete make sure to 'Test Server Connection' to verify your configuration information is correct.

Click the Tab for Payload Format
You can choose any log type listed. The payload format will be the same for any log type you choose to configure.

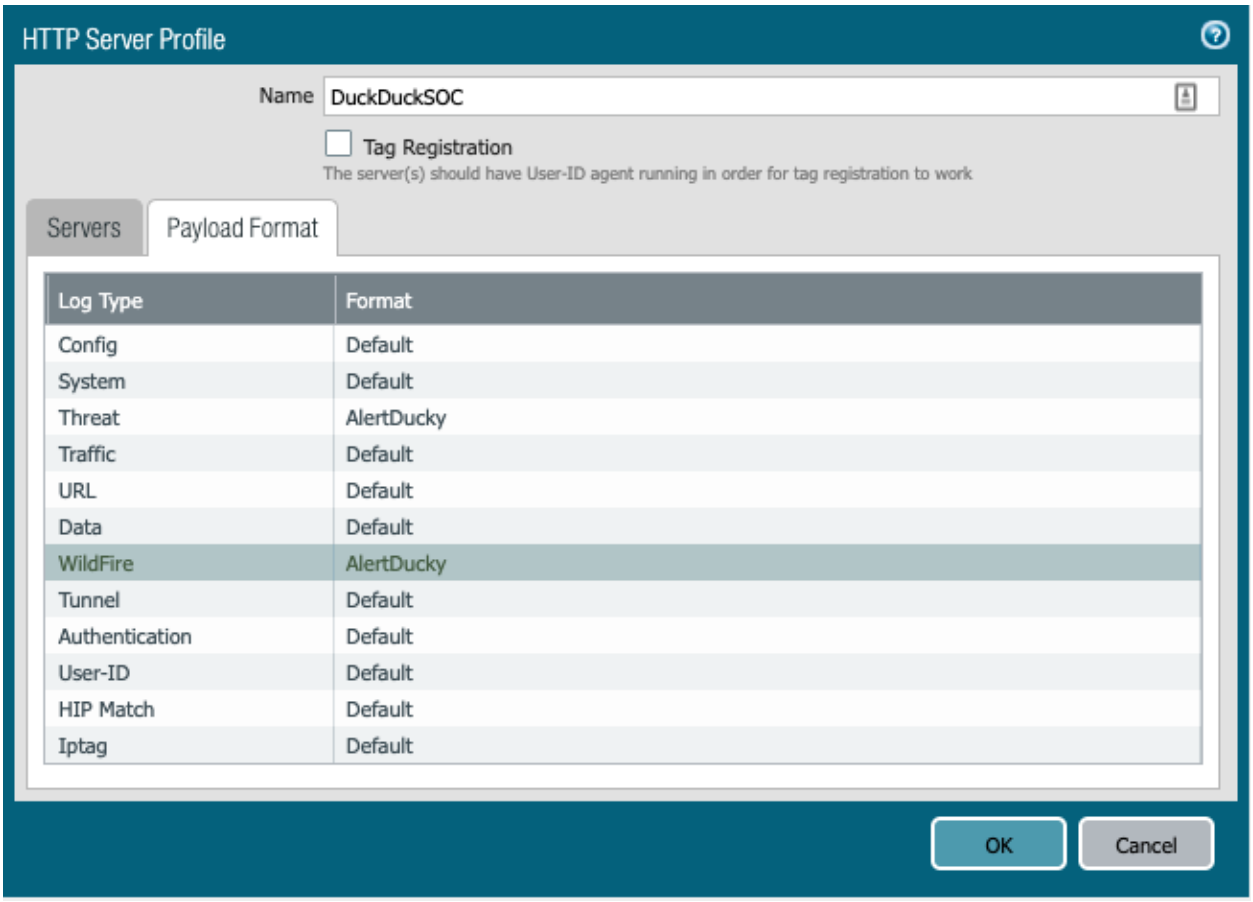


Name: Again, cool name or stick with mine
URI Format: This will be the URL path that you want triggered. '/alert' is the default
Note: *If you want to add some security you can update the '/alert' URI and add random characters into the URI. Example: '/HiS99s0aPeUNrWns/alert'. This will need to be updated within the .ino file (the firmware you loaded onto your SOC Duck) as well as in the URI Format in the PAN-OS GUI.*
HTTP Headers: content-type
Value: text/html

Payload is left blank on purpose.

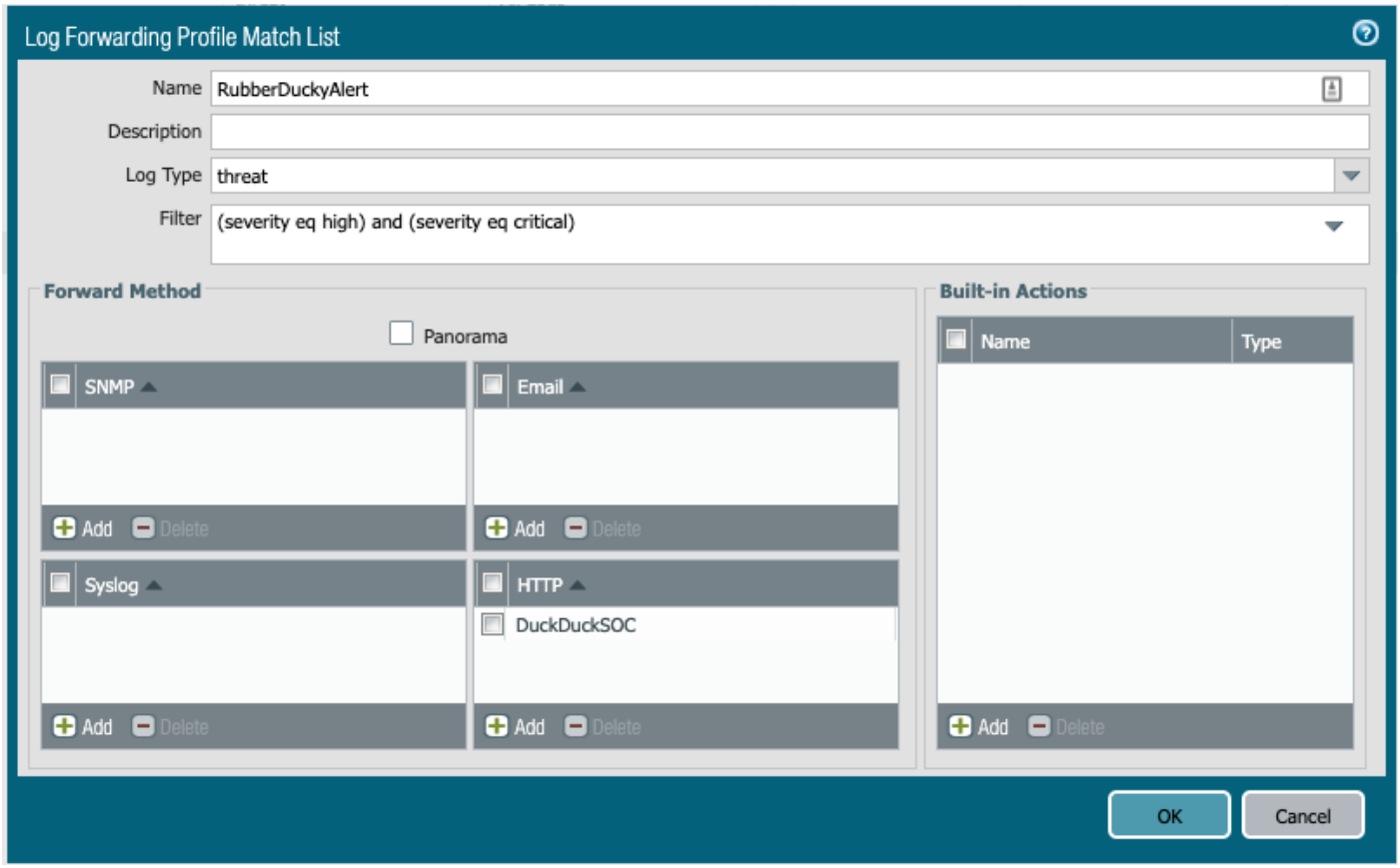
Click OK

Repeat these steps for each log type you want to define.

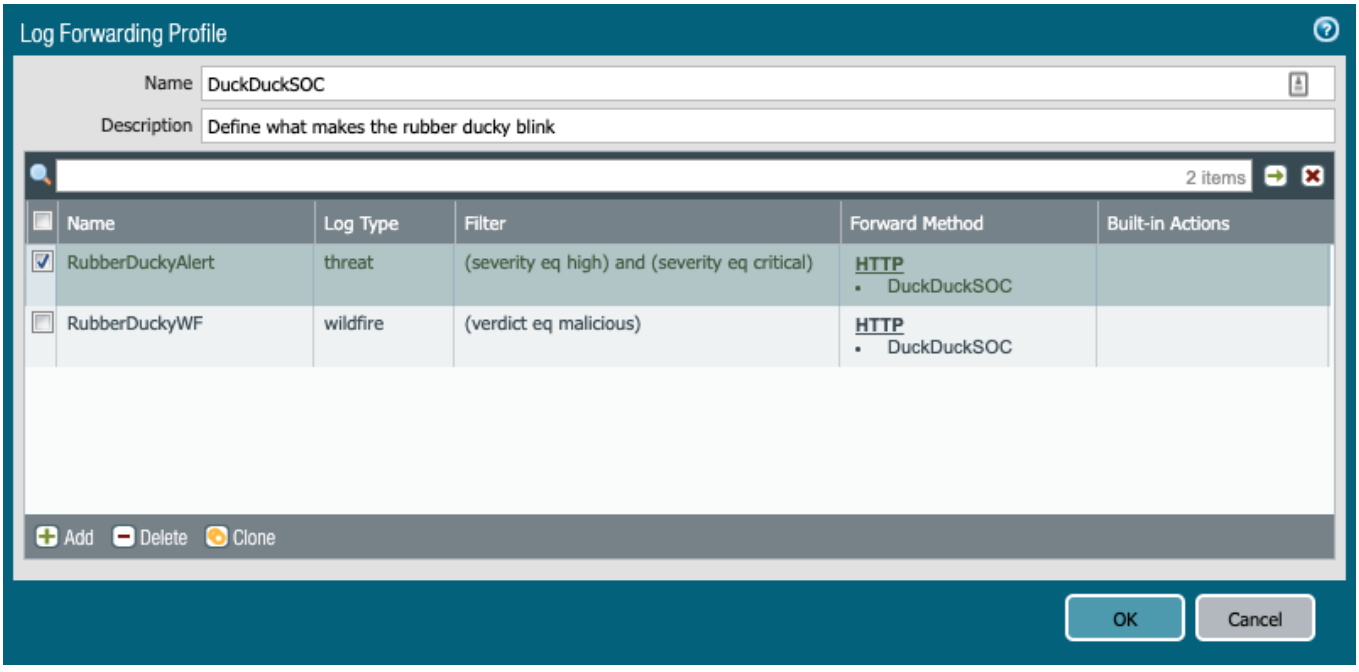


Click OK

Navigate to Objects > Log Forwarding and add a Log Forwarding Profile



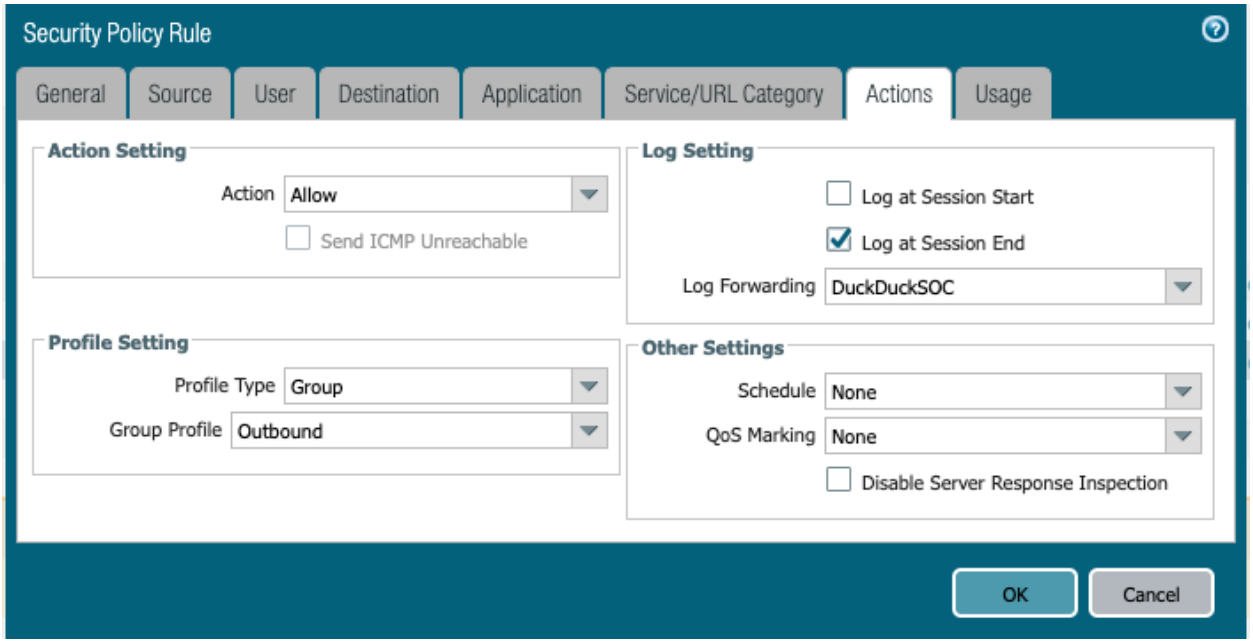
Create the log forwarding profile match list. This is where you will configure the log type(s) that will trigger the SOC Duck. Attach the HTTP Server Profile that you created in the previous step here.



Repeat steps if you want to add additional filters. For my use case I am filtering on threat logs with a high and critical severity as well as malicious WildFire verdicts.

Click OK

Navigate to Policies > Security > Security Policy Rule you want to attach the Log Forwarding Profile to **> Actions > Log Setting**



Click OK

Commit Changes

If all went well the log type and filter you defined should now trigger your SOC Duck!

Written By: Sandra Wenzel & Dan Ward, Consulting Engineers for Palo Alto Networks