Pacific Northwest
NATIONAL LABORATORY

IoTCOE
INTERNET OF THINGS
COMMON OPERATING
ENVIRONMENT
@PNNL

Smart Home Intrusion Detection System

12 January 2025

Ernest Allard
Post Bachelor’s Research Assistant

U.S. DEPARTMENT OF ENERGY BATTELLE

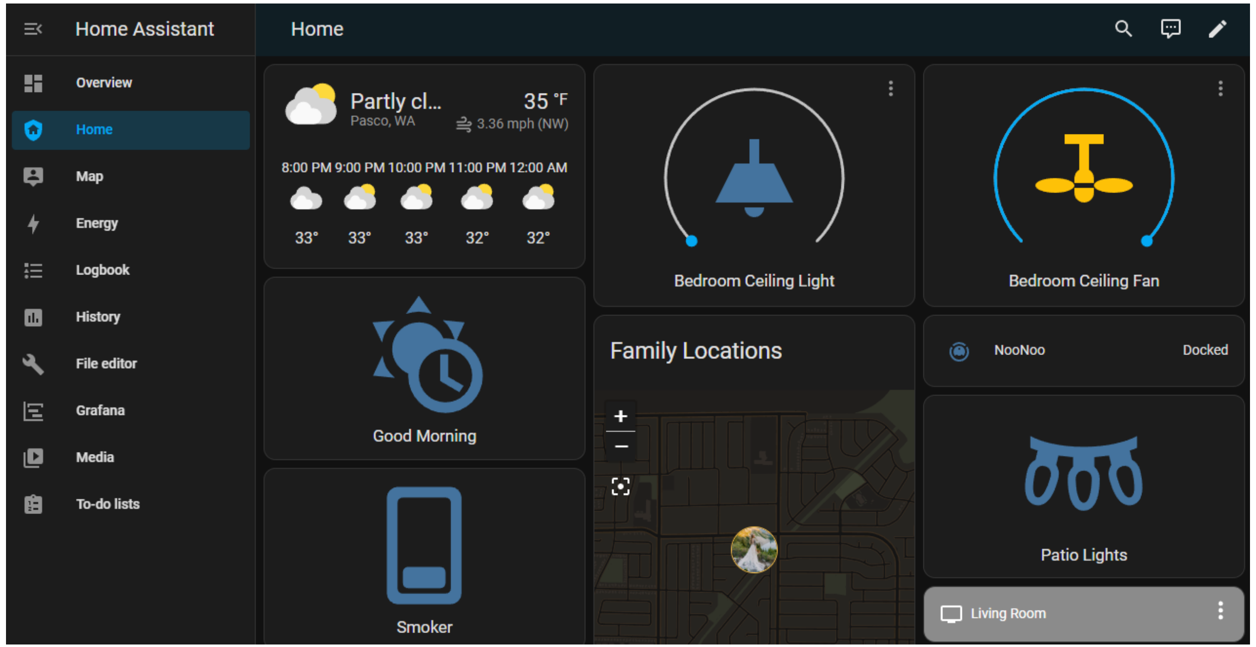
PNNL is operated by Battelle for the U.S. Department of Energy

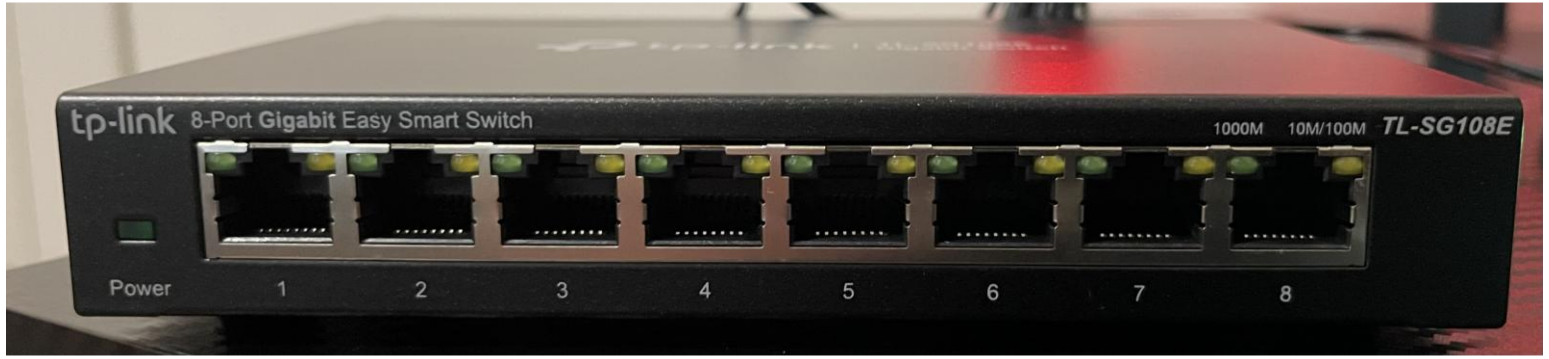
About Me:

- Husband
- Father
- Veteran
- Brother

What do we need?

- Home Assistant
- Managed Switch (TL-SG108E)
- Raspberry Pi
- Smartphone
- Suricata
  - Tcpdump
  - SSH





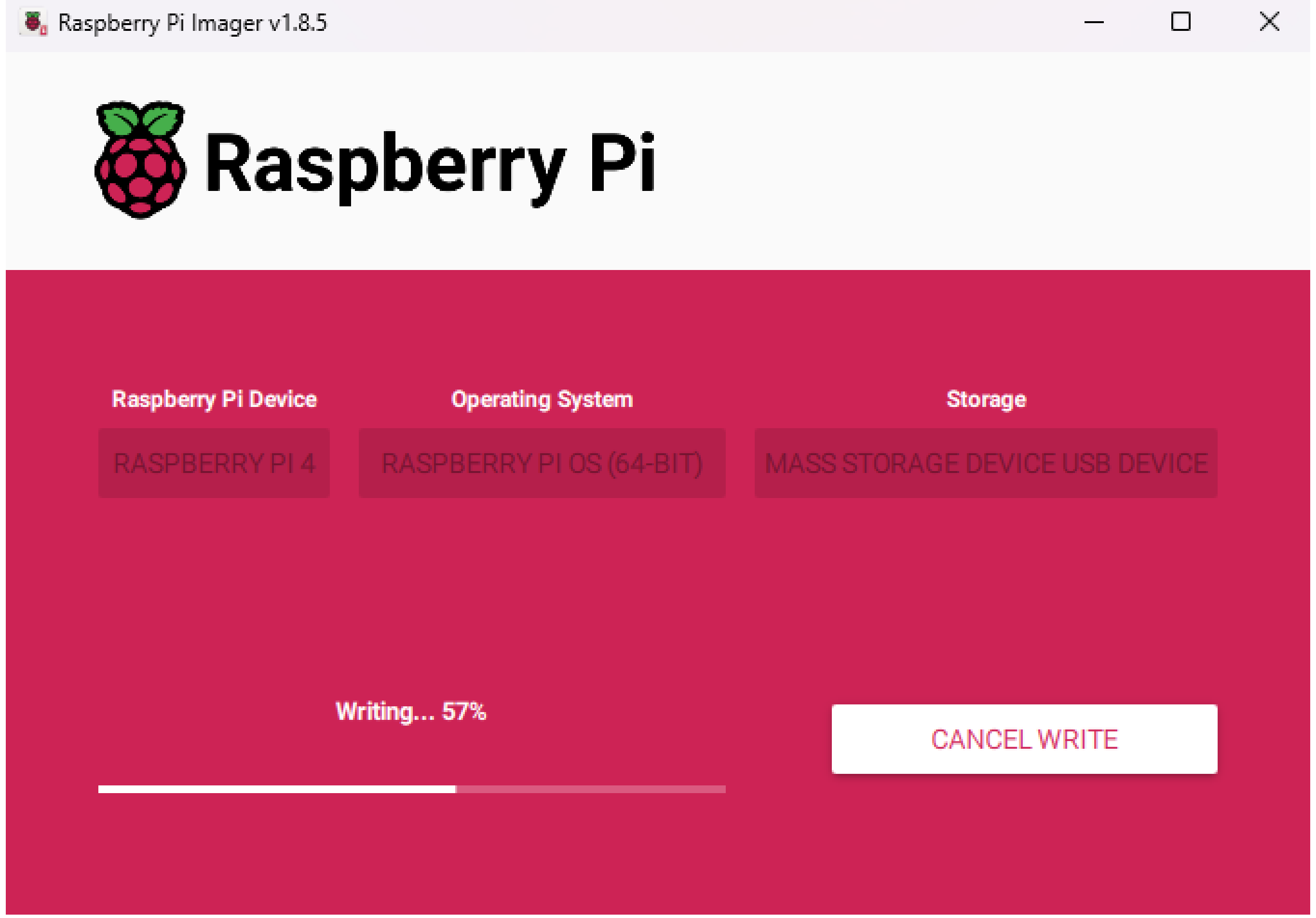
Goals/Purpose:

- Enable SSH between Home PC / Suricata Raspberry Pi / Home Assistant Raspberry Pi.
- Create a Mirror Port on my managed switch.
- Ensure that the Suricata Pi is monitoring the network.
- Send alerts to Home Assistant.
- Enable Mobile Notification on Home Assistant.

Pacific Northwest
NATIONAL LABORATORY

Suricata Pi Setup

- Flash Raspberry Pi OS to microSD card.
- Setup Process.
- Conduct Updates to packages.



Raspberry Pi Imager v1.8.5

Raspberry Pi Device: RASPBERRY PI 4

Operating System: RASPBERRY PI OS (64-BIT)

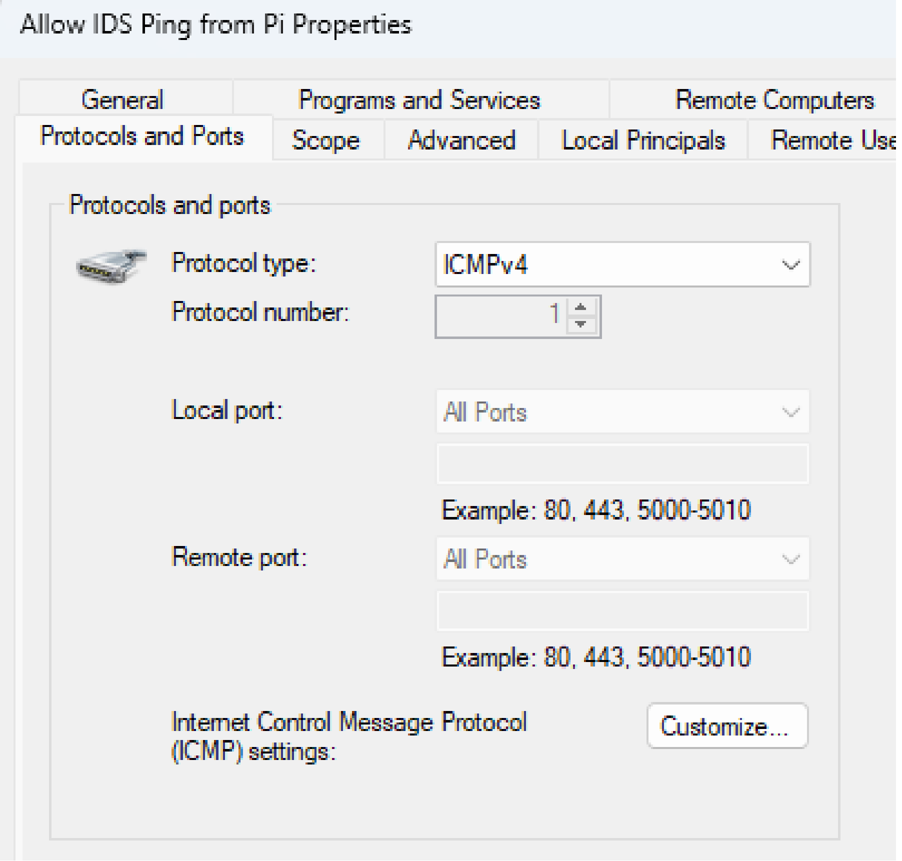
Storage: MASS STORAGE DEVICE USB DEVICE

Writing... 57%

Pacific Northwest
NATIONAL LABORATORY

Hello? Are you there?

- Windows Firewall Rules
- From Windows – Suricata Pi, Suricata Pi – Windows.
- Enable SSH
- Success!



Allow IDS Ping from Pi Properties

Protocols and ports

Protocol type: ICMPv4

Protocol number: 1

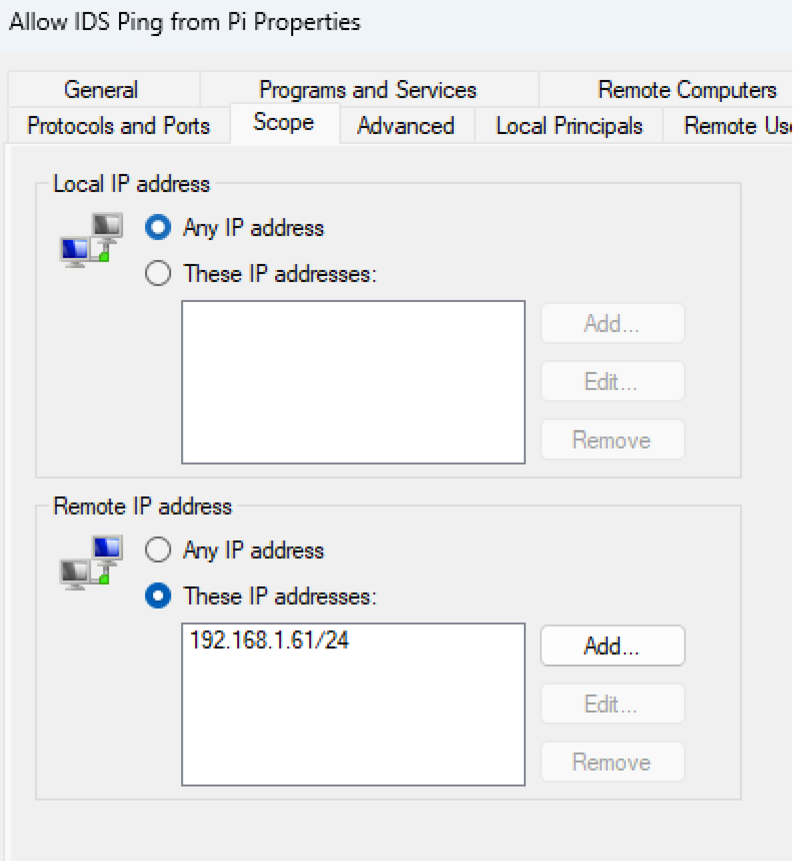
Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...



Allow IDS Ping from Pi Properties

Local IP address

● Any IP address

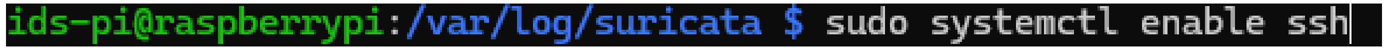
○ These IP addresses:

Remote IP address

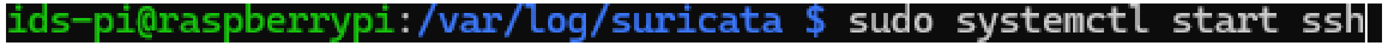
○ Any IP address

● These IP addresses:

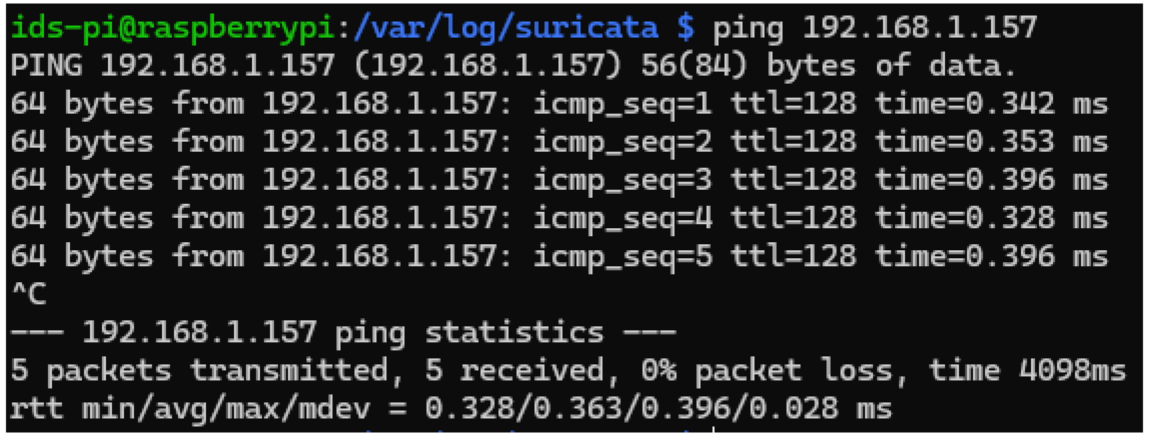
192.168.1.61/24



```
ids-pi@raspberrypi:/var/log/suricata $ sudo systemctl enable ssh
```



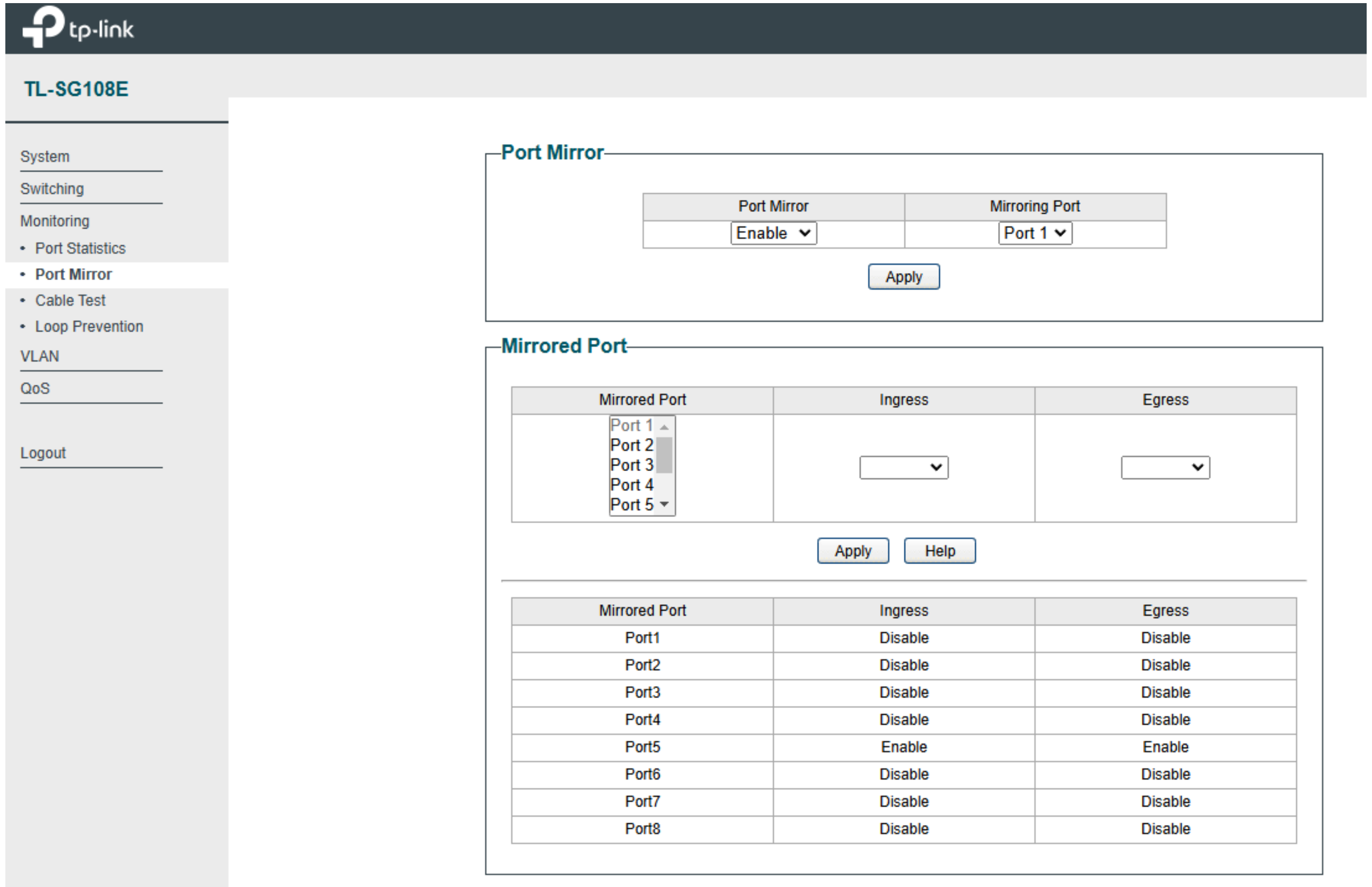
```
ids-pi@raspberrypi:/var/log/suricata $ sudo systemctl start ssh
```



```
ids-pi@raspberrypi:/var/log/suricata $ ping 192.168.1.157
PING 192.168.1.157 (192.168.1.157) 56(84) bytes of data.
64 bytes from 192.168.1.157: icmp_seq=1 ttl=128 time=0.342 ms
64 bytes from 192.168.1.157: icmp_seq=2 ttl=128 time=0.353 ms
64 bytes from 192.168.1.157: icmp_seq=3 ttl=128 time=0.396 ms
64 bytes from 192.168.1.157: icmp_seq=4 ttl=128 time=0.328 ms
64 bytes from 192.168.1.157: icmp_seq=5 ttl=128 time=0.396 ms
^C
--- 192.168.1.157 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4098ms
rtt min/avg/max/mdev = 0.328/0.363/0.396/0.028 ms
```

Switch Configuration

- Plug in my ethernet devices
- Use web UI to enable mirror port
- Connect Suricata Pi to the mirror port via Cat6



Port Mirror

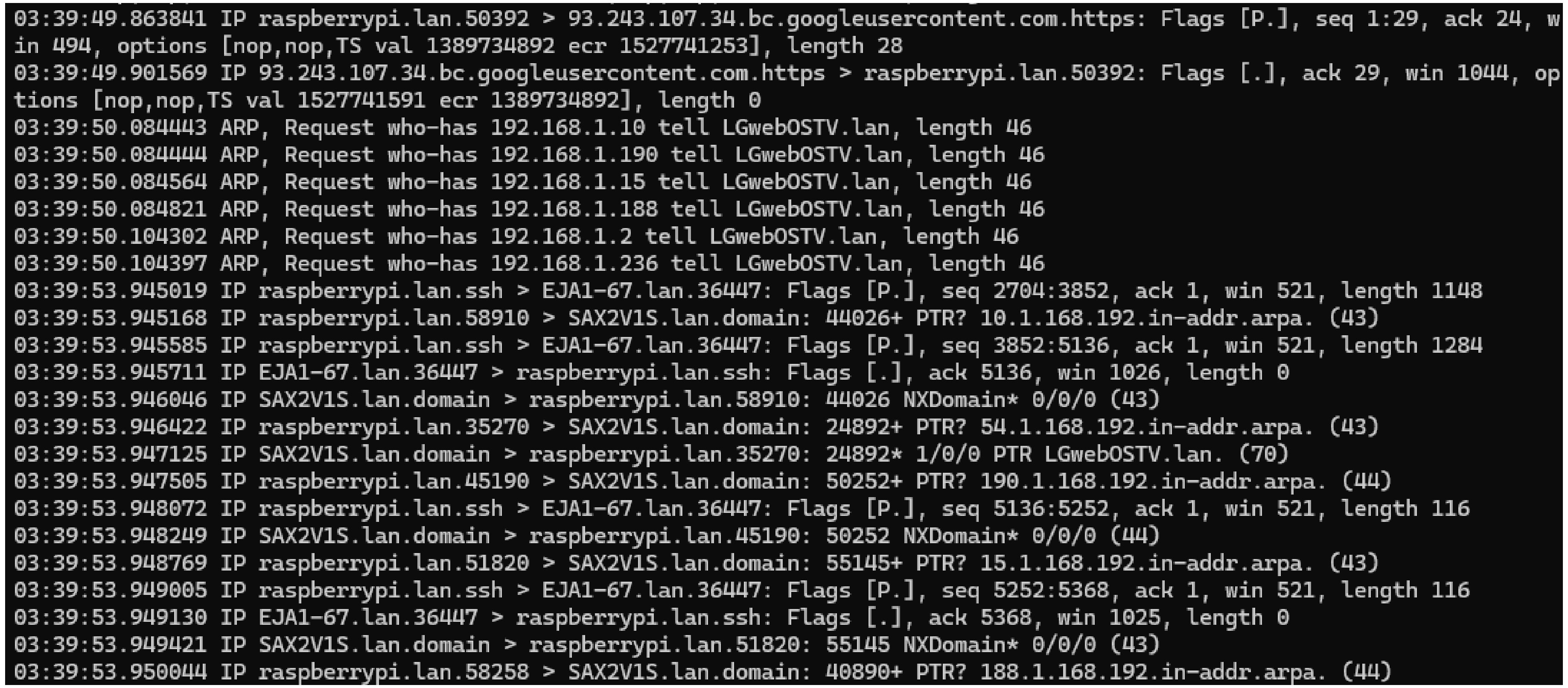
Port Mirror	Mirroring Port
Enable	Port 1

Mirrored Port

Mirrored Port	Ingress	Egress
Port1	Disable	Disable
Port2	Disable	Disable
Port3	Disable	Disable
Port4	Disable	Disable
Port5	Enable	Enable
Port6	Disable	Disable
Port7	Disable	Disable
Port8	Disable	Disable

Can We See traffic?

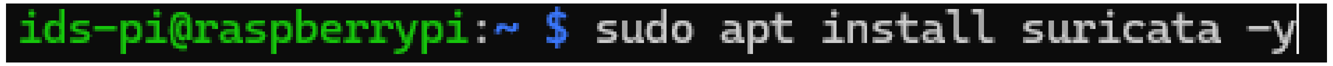
- Yes we can!
- tcpdump –i eth0



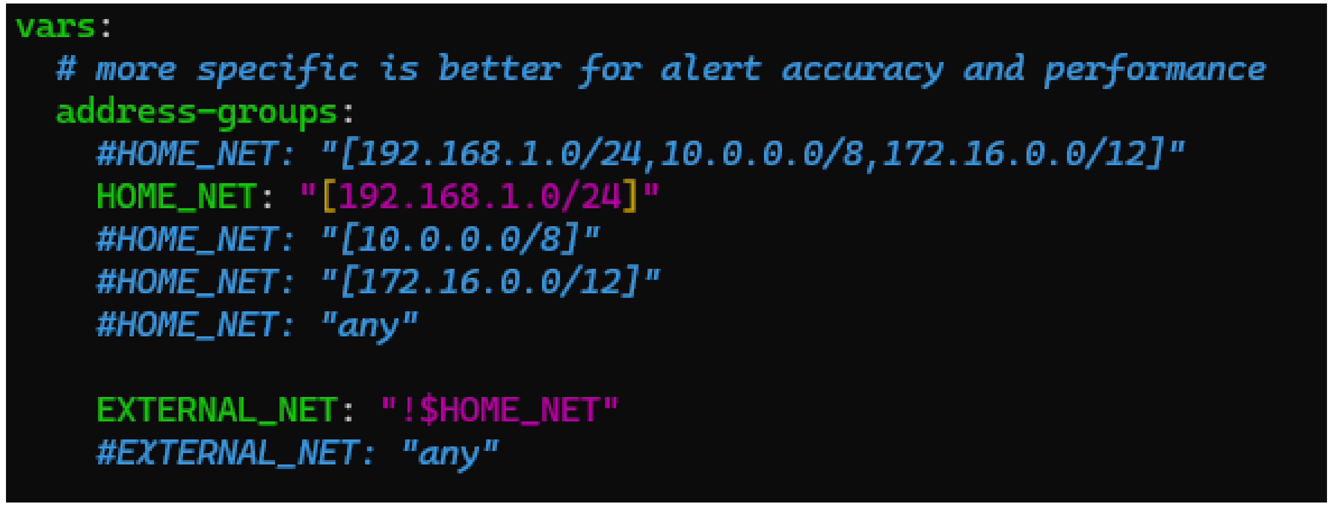
```
03:39:49.863841 IP raspberrypi.lan.50392 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], seq 1:29, ack 24, w
in 494, options [nop,nop,TS val 1389734892 ecr 1527741253], length 28
03:39:49.901569 IP 93.243.107.34.bc.googleusercontent.com.https > raspberrypi.lan.50392: Flags [.], ack 29, win 1044, op
tions [nop,nop,TS val 1527741591 ecr 1389734892], length 0
03:39:50.084443 ARP, Request who-has 192.168.1.10 tell LGwebOSTV.lan, length 46
03:39:50.084444 ARP, Request who-has 192.168.1.190 tell LGwebOSTV.lan, length 46
03:39:50.084564 ARP, Request who-has 192.168.1.15 tell LGwebOSTV.lan, length 46
03:39:50.084821 ARP, Request who-has 192.168.1.188 tell LGwebOSTV.lan, length 46
03:39:50.104302 ARP, Request who-has 192.168.1.2 tell LGwebOSTV.lan, length 46
03:39:50.104397 ARP, Request who-has 192.168.1.236 tell LGwebOSTV.lan, length 46
03:39:53.945019 IP raspberrypi.lan.ssh > EJA1-67.lan.36447: Flags [P.], seq 2704:3852, ack 1, win 521, length 1148
03:39:53.945168 IP raspberrypi.lan.58910 > SAX2V1S.lan.domain: 44026+ PTR? 10.1.168.192.in-addr.arpa. (43)
03:39:53.945585 IP raspberrypi.lan.ssh > EJA1-67.lan.36447: Flags [P.], seq 3852:5136, ack 1, win 521, length 1284
03:39:53.945711 IP EJA1-67.lan.36447 > raspberrypi.lan.ssh: Flags [.], ack 5136, win 1026, length 0
03:39:53.946046 IP SAX2V1S.lan.domain > raspberrypi.lan.58910: 44026 NXDomain* 0/0/0 (43)
03:39:53.946422 IP raspberrypi.lan.35270 > SAX2V1S.lan.domain: 24892+ PTR? 54.1.168.192.in-addr.arpa. (43)
03:39:53.947125 IP SAX2V1S.lan.domain > raspberrypi.lan.35270: 24892* 1/0/0 PTR LGwebOSTV.lan. (70)
03:39:53.947505 IP raspberrypi.lan.45190 > SAX2V1S.lan.domain: 50252+ PTR? 190.1.168.192.in-addr.arpa. (44)
03:39:53.948072 IP raspberrypi.lan.ssh > EJA1-67.lan.36447: Flags [P.], seq 5136:5252, ack 1, win 521, length 116
03:39:53.948249 IP SAX2V1S.lan.domain > raspberrypi.lan.45190: 50252 NXDomain* 0/0/0 (44)
03:39:53.948769 IP raspberrypi.lan.51820 > SAX2V1S.lan.domain: 55145+ PTR? 15.1.168.192.in-addr.arpa. (43)
03:39:53.949005 IP raspberrypi.lan.ssh > EJA1-67.lan.36447: Flags [P.], seq 5252:5368, ack 1, win 521, length 116
03:39:53.949130 IP EJA1-67.lan.36447 > raspberrypi.lan.ssh: Flags [.], ack 5368, win 1025, length 0
03:39:53.949421 IP SAX2V1S.lan.domain > raspberrypi.lan.51820: 55145 NXDomain* 0/0/0 (43)
03:39:53.950044 IP raspberrypi.lan.58258 > SAX2V1S.lan.domain: 40890+ PTR? 188.1.168.192.in-addr.arpa. (44)
```

Suricata Install/Configurations

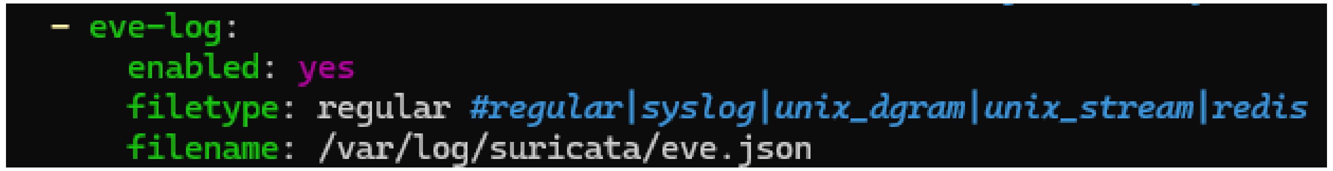
- sudo apt install suricata -y
- sudo nano /etc/suricata/suricata.yaml
- Eve.json



```
ids-pi@raspberrypi:~ $ sudo apt install suricata -y
```



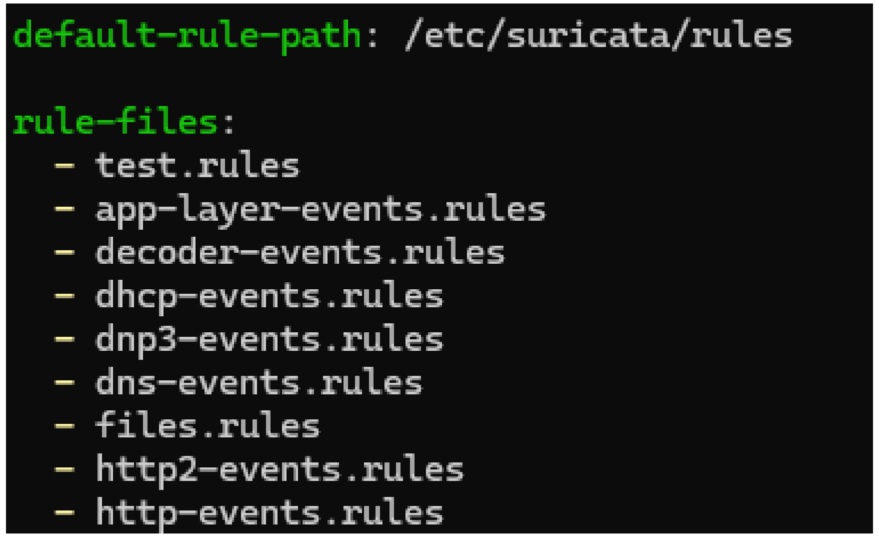
```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    #HOME_NET: "[192.168.1.0/24,10.0.0.0/8,172.16.0.0/12]"
    HOME_NET: "[192.168.1.0/24]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"
```



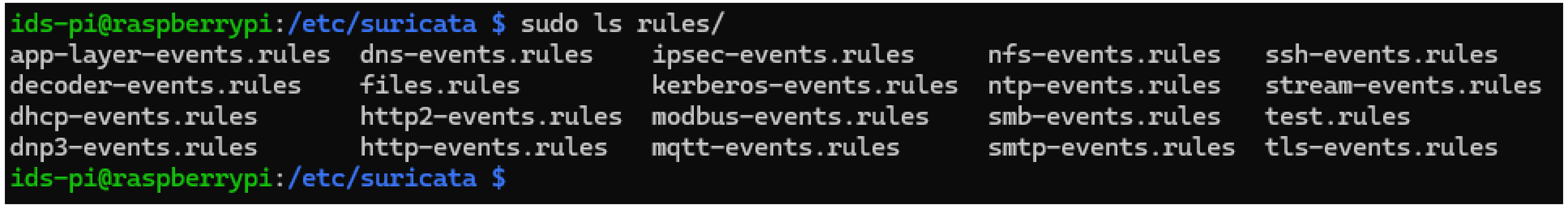
```
  - eve-log:
      enabled: yes
      filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
      filename: /var/log/suricata/eve.json
```

Suricata Rule Files/Location

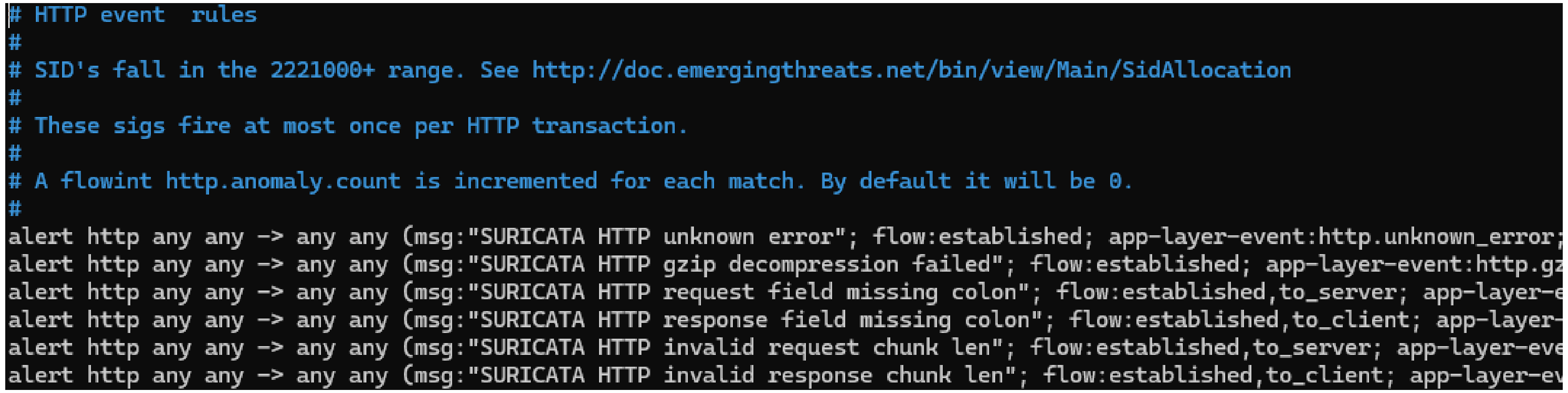
- Located at /etc/suricata/rules
- Can use rulesets found online or custom rulesets.
- Include any rules within suricata.yaml



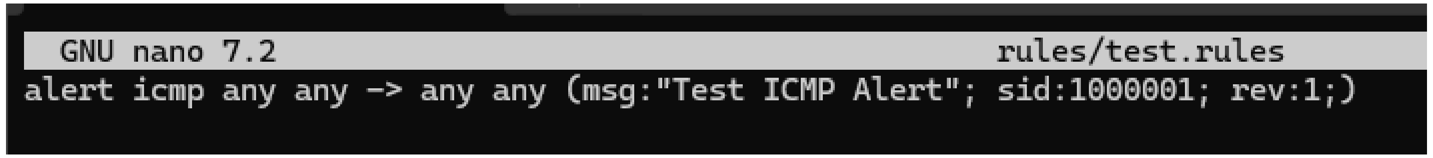
```
default-rule-path: /etc/suricata/rules

rule-files:
  - test.rules
  - app-layer-events.rules
  - decoder-events.rules
  - dhcp-events.rules
  - dnp3-events.rules
  - dns-events.rules
  - files.rules
  - http2-events.rules
  - http-events.rules
```



```
ids-pi@raspberrypi:/etc/suricata $ sudo ls rules/
app-layer-events.rules  dns-events.rules     ipsec-events.rules     nfs-events.rules    ssh-events.rules
decoder-events.rules    files.rules          kerberos-events.rules  ntp-events.rules    stream-events.rules
dhcp-events.rules       http2-events.rules   modbus-events.rules    smb-events.rules    test.rules
dnp3-events.rules       http-events.rules    mqtt-events.rules      smtp-events.rules   tls-events.rules
ids-pi@raspberrypi:/etc/suricata $
```



```
# HTTP event  rules
#
# SID's fall in the 2221000+ range. See http://doc.emergingthreats.net/bin/view/Main/SidAllocation
#
# These sigs fire at most once per HTTP transaction.
#
# A flowint http.anomaly.count is incremented for each match. By default it will be 0.
#
alert http any any -> any any (msg:"SURICATA HTTP unknown error"; flow:established; app-layer-event:http.unknown_error;
alert http any any -> any any (msg:"SURICATA HTTP gzip decompression failed"; flow:established; app-layer-event:http.gz
alert http any any -> any any (msg:"SURICATA HTTP request field missing colon"; flow:established,to_server; app-layer-e
alert http any any -> any any (msg:"SURICATA HTTP response field missing colon"; flow:established,to_client; app-layer-
alert http any any -> any any (msg:"SURICATA HTTP invalid request chunk len"; flow:established,to_server; app-layer-eve
alert http any any -> any any (msg:"SURICATA HTTP invalid response chunk len"; flow:established,to_client; app-layer-ev
```

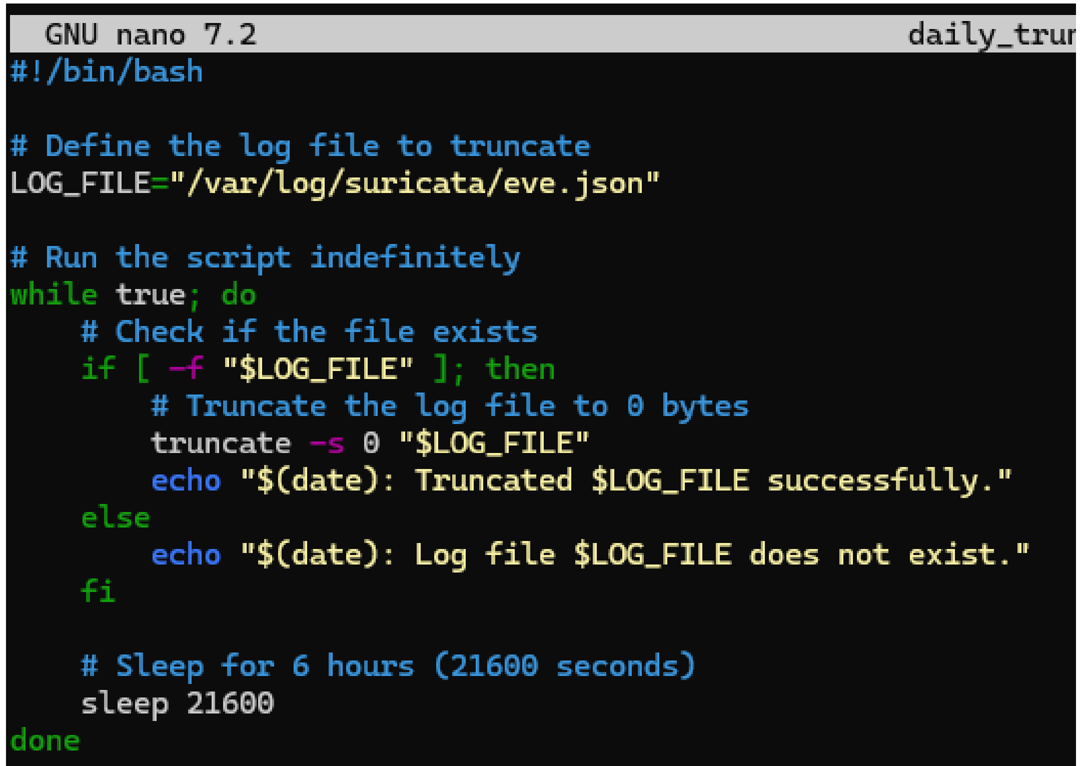


```
 GNU nano 7.2                                         rules/test.rules
alert icmp any any -> any any (msg:"Test ICMP Alert"; sid:1000001; rev:1;)
```

Scripts In Use: Suricata Pi

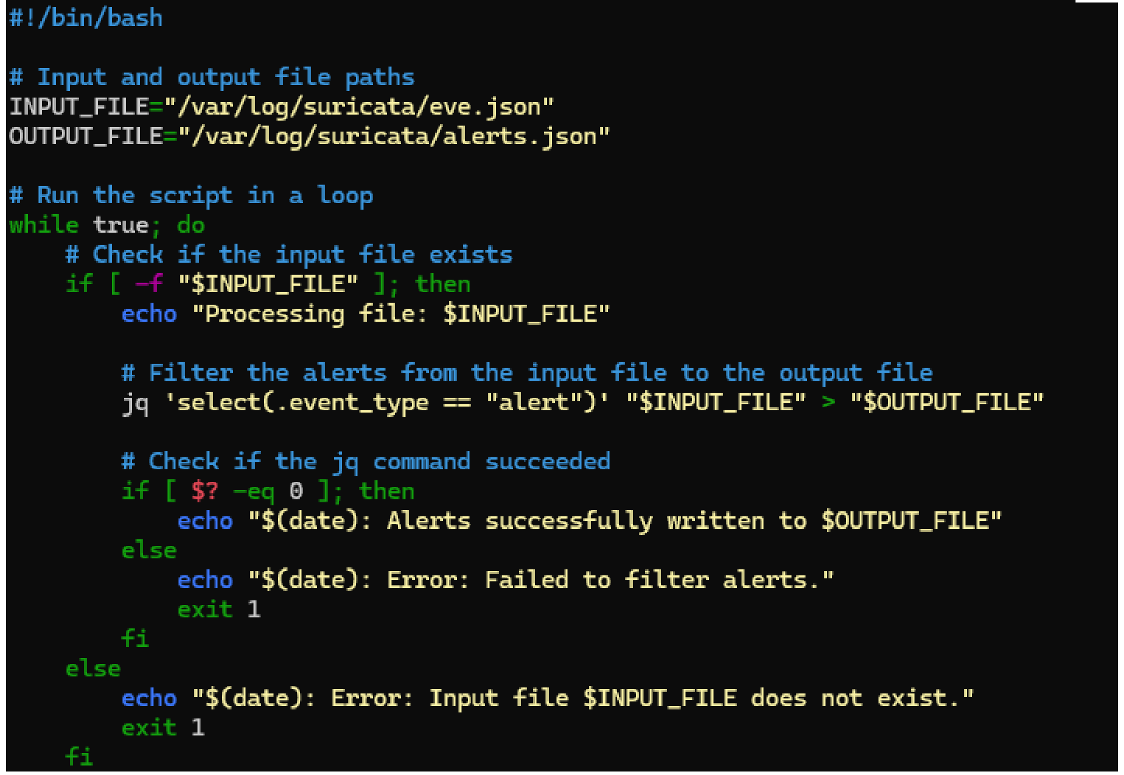
- Trunicate eve.log every 6 hours
- Pull alerts from eve.log every X minutes
- Explain the scripts.

daily_trunicate_eve.sh



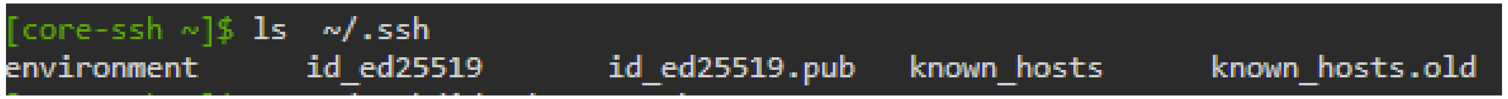
```
#!/bin/bash

# Define the log file to truncate
LOG_FILE="/var/log/suricata/eve.json"

# Run the script indefinitely
while true; do
    # Check if the file exists
    if [ -f "$LOG_FILE" ]; then
        # Truncate the log file to 0 bytes
        truncate -s 0 "$LOG_FILE"
        echo "$(date): Truncated $LOG_FILE successfully."
    else
        echo "$(date): Log file $LOG_FILE does not exist."
    fi

    # Sleep for 6 hours (21600 seconds)
    sleep 21600
done
```

filter.sh

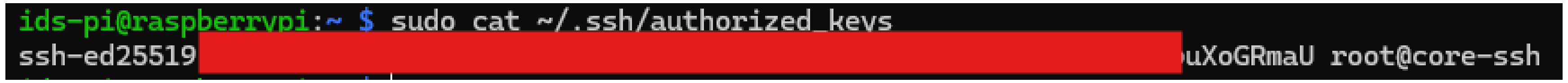


```
#!/bin/bash

# Input and output file paths
INPUT_FILE="/var/log/suricata/eve.json"
OUTPUT_FILE="/var/log/suricata/alerts.json"

# Run the script in a loop
while true; do
    # Check if the input file exists
    if [ -f "$INPUT_FILE" ]; then
        echo "Processing file: $INPUT_FILE"

        # Filter the alerts from the input file to the output file
        jq 'select(.event_type == "alert")' "$INPUT_FILE" > "$OUTPUT_FILE"

        # Check if the jq command succeeded
        if [ $? -eq 0 ]; then
            echo "$(date): Alerts successfully written to $OUTPUT_FILE"
        else
            echo "$(date): Error: Failed to filter alerts."
            exit 1
        fi
    else
        echo "$(date): Error: Input file $INPUT_FILE does not exist."
        exit 1
    fi
```

SSH Key Between Home Assistant Pi & Suricata Pi

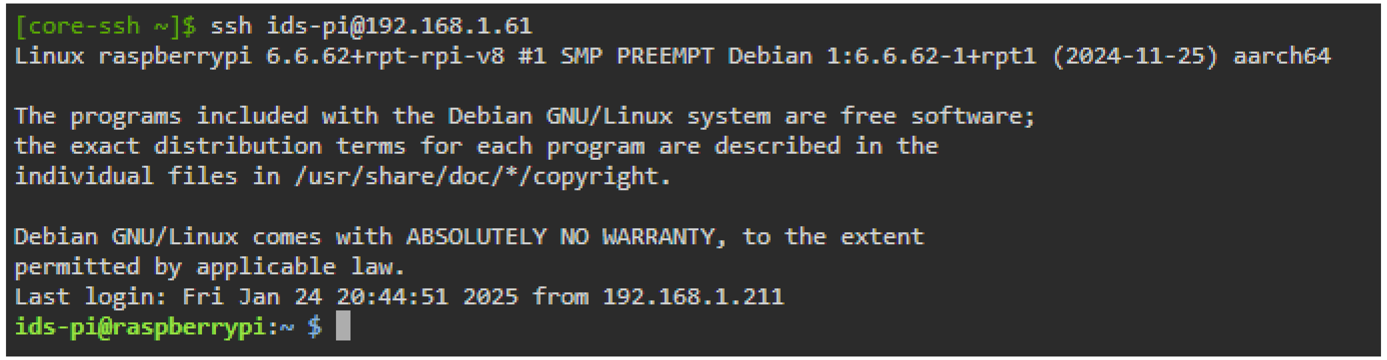


```
[core-ssh ~]$ ls  ~/.ssh
environment       id_ed25519        id_ed25519.pub    known_hosts       known_hosts.old
```



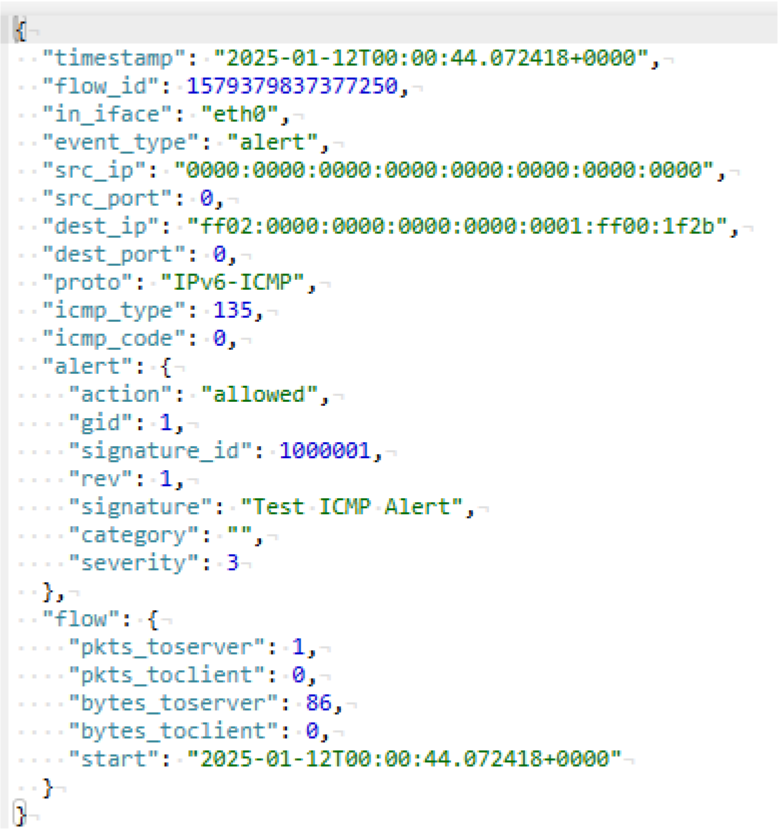
```
ids-pi@raspberrypi:~ $ sudo cat ~/.ssh/authorized_keys
ssh-ed25519 [redacted]uXoGRmaU root@core-ssh
```

- ssh-keygen
- ssh-copy-id ids-pi@192.168.1.61



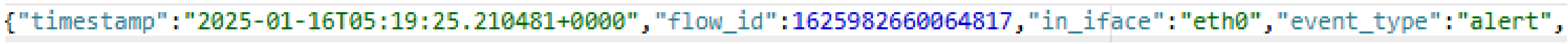
```
[core-ssh ~]$ ssh ids-pi@192.168.1.61
Linux raspberrypi 6.6.62+rpt-rpi-v8 #1 SMP PREEMPT Debian 1:6.6.62-1+rpt1 (2024-11-25) aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jan 24 20:44:51 2025 from 192.168.1.211
ids-pi@raspberrypi:~ $
```

Home Assistant Script:



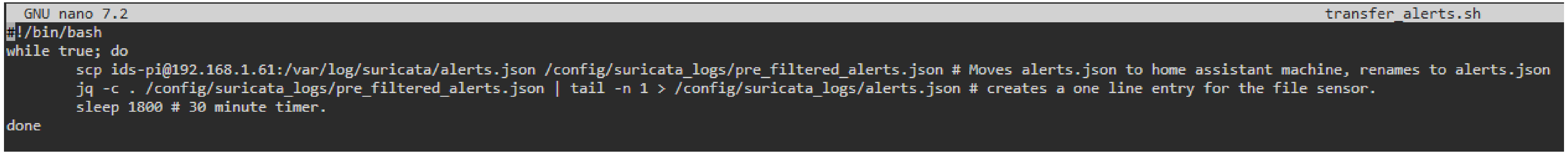
```
{
  "timestamp": "2025-01-12T00:00:44.072418+0000",
  "flow_id": 1579379837377250,
  "in_iface": "eth0",
  "event_type": "alert",
  "src_ip": "0000:0000:0000:0000:0000:0000:0000:0000",
  "src_port": 0,
  "dest_ip": "ff02:0000:0000:0000:0000:0001:ff00:1f2b",
  "dest_port": 0,
  "proto": "IPv6-ICMP",
  "icmp_type": 135,
  "icmp_code": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 1000001,
    "rev": 1,
    "signature": "Test ICMP Alert",
    "category": "",
    "severity": 3
  },
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 0,
    "bytes_toserver": 86,
    "bytes_toclient": 0,
    "start": "2025-01-12T00:00:44.072418+0000"
  }
}
```

- Retrieve the unfiltered alert log
- Use JQ to get the most recent alert, what's the purpose of this?



```
{"timestamp":"2025-01-16T05:19:25.210481+0000","flow_id":1625982660064817,"in_iface":"eth0","event_type":"alert",
```

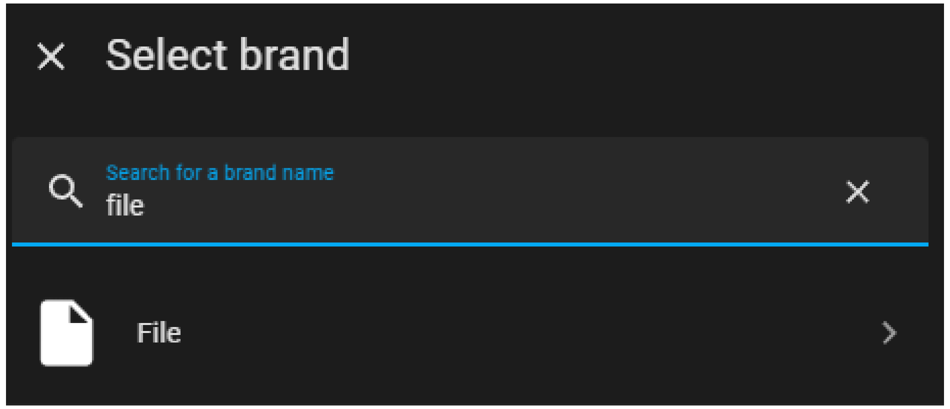
transfer_alerts.sh



```
#!/bin/bash
while true; do
        scp ids-pi@192.168.1.61:/var/log/suricata/alerts.json /config/suricata_logs/pre_filtered_alerts.json # Moves alerts.json to home assistant machine, renames to alerts.json
        jq -c . /config/suricata_logs/pre_filtered_alerts.json | tail -n 1 > /config/suricata_logs/alerts.json # creates a one line entry for the file sensor.
        sleep 1800 # 30 minute timer.
done
```

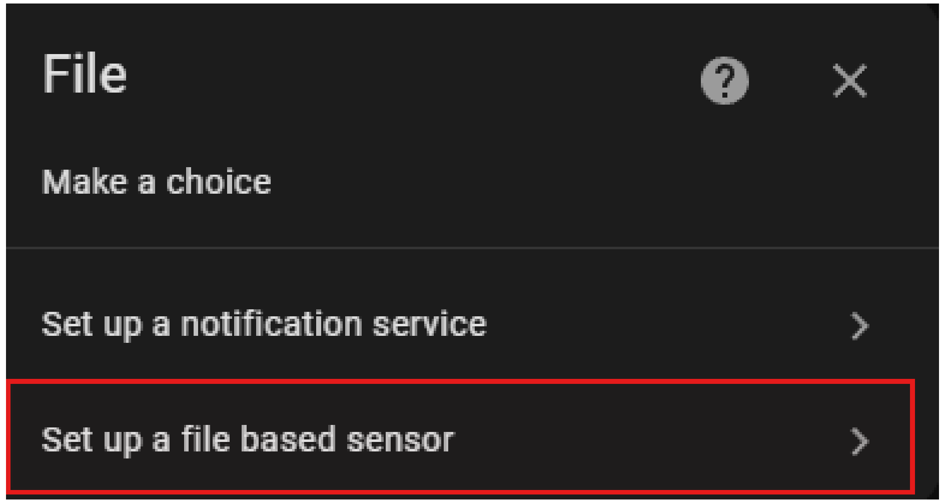
File Sensor’s… Fun!

- Sense when alert.json is updated.
- Pulls the designated fields I want.



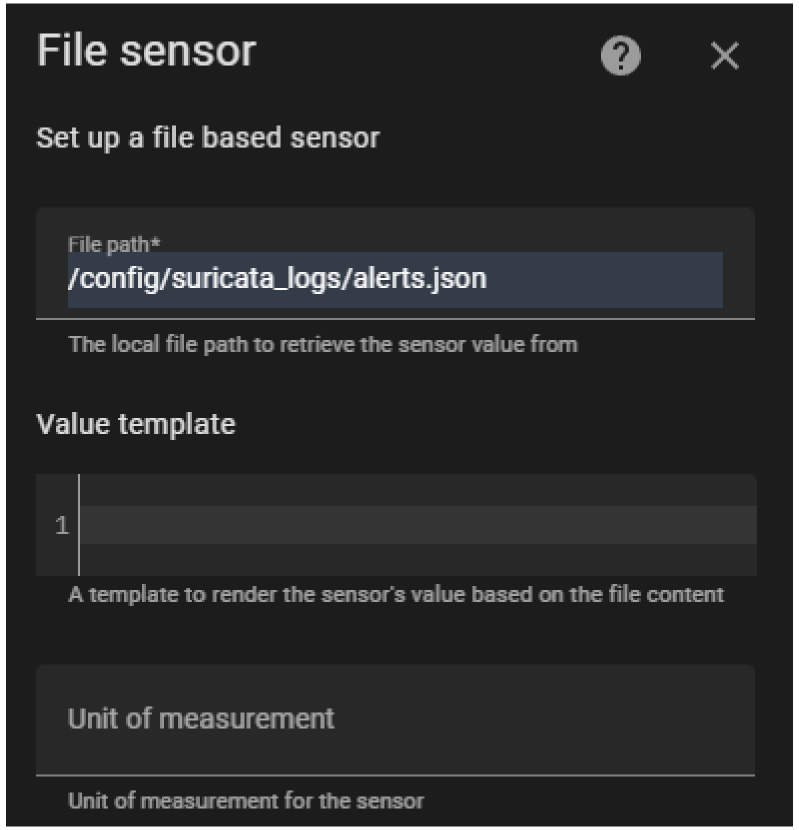
Select brand

Search for a brand name
file



File

Make a choice



File sensor

Set up a file based sensor

File path*
/config/suricata_logs/alerts.json

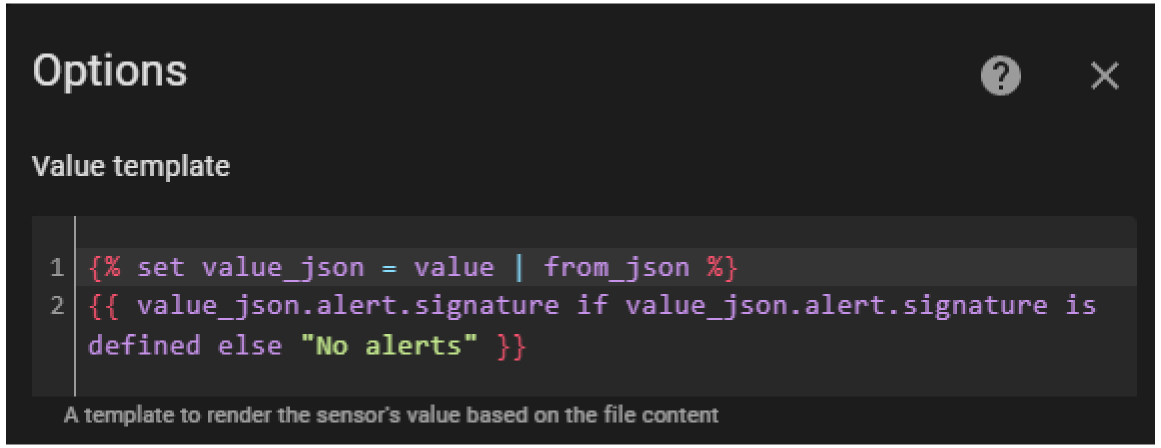
The local file path to retrieve the sensor value from

Value template

A template to render the sensor’s value based on the file content

Unit of measurement

Unit of measurement for the sensor



Options

Value template

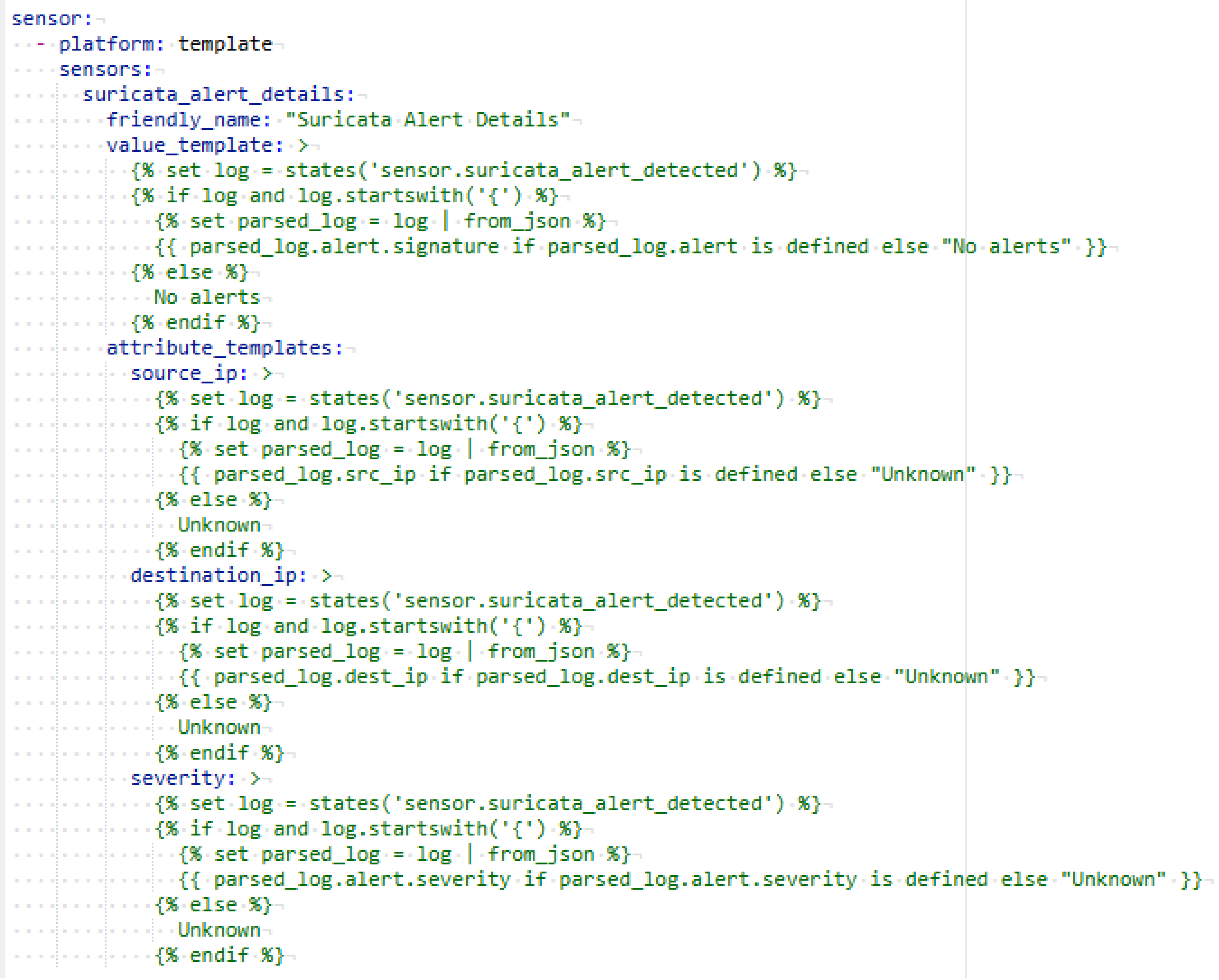
```
{% set value_json = value | from_json %}
{{ value_json.alert.signature if value_json.alert.signature is
defined else "No alerts" }}
```

A template to render the sensor’s value based on the file content

Alert Signature File Sensor

Template Sensor:

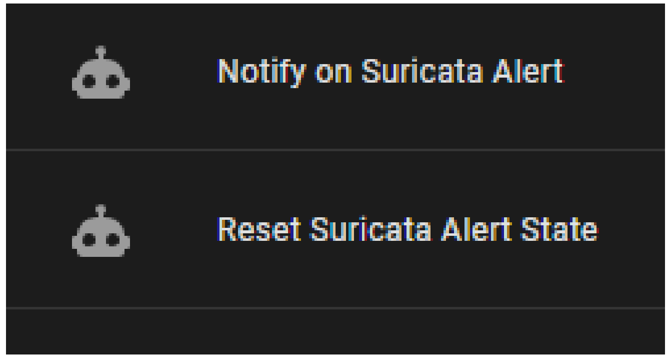
- Template extracts the field from JSON data.
- If JSON data is invalid, shows “No alerts”.
- Formats data for automation.



```
sensor:
  - platform: template
    sensors:
      suricata_alert_details:
        friendly_name: "Suricata Alert Details"
        value_template: >
          {% set log = states('sensor.suricata_alert_detected') %}
          {% if log and log.startswith('{') %}
            {% set parsed_log = log | from_json %}
            {{ parsed_log.alert.signature if parsed_log.alert is defined else "No alerts" }}
          {% else %}
            No alerts
          {% endif %}
        attribute_templates:
          source_ip: >
            {% set log = states('sensor.suricata_alert_detected') %}
            {% if log and log.startswith('{') %}
              {% set parsed_log = log | from_json %}
              {{ parsed_log.src_ip if parsed_log.src_ip is defined else "Unknown" }}
            {% else %}
              Unknown
            {% endif %}
          destination_ip: >
            {% set log = states('sensor.suricata_alert_detected') %}
            {% if log and log.startswith('{') %}
              {% set parsed_log = log | from_json %}
              {{ parsed_log.dest_ip if parsed_log.dest_ip is defined else "Unknown" }}
            {% else %}
              Unknown
            {% endif %}
          severity: >
            {% set log = states('sensor.suricata_alert_detected') %}
            {% if log and log.startswith('{') %}
              {% set parsed_log = log | from_json %}
              {{ parsed_log.alert.severity if parsed_log.alert.severity is defined else "Unknown" }}
            {% else %}
              Unknown
            {% endif %}
```

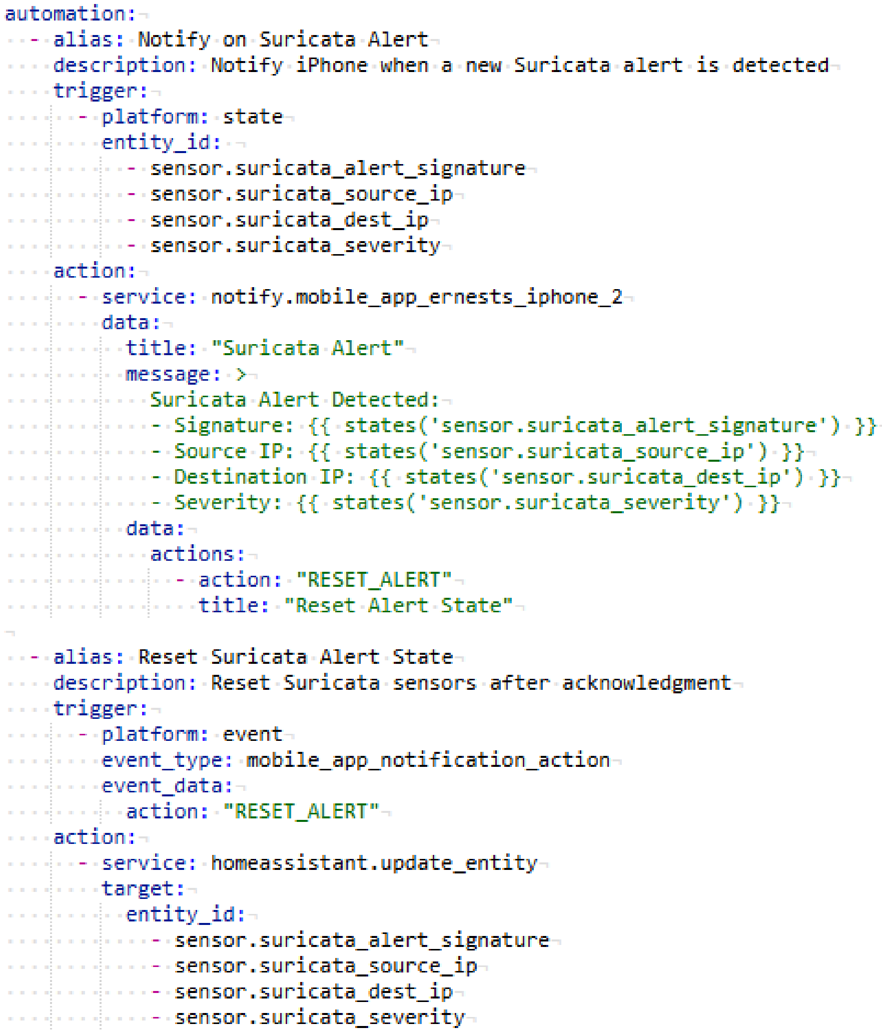
Automation, Why Not?

- Notify.mobile_app_ernest_iphone_2
- Notify on Suricata Alert
- Reset Suricata Alert State

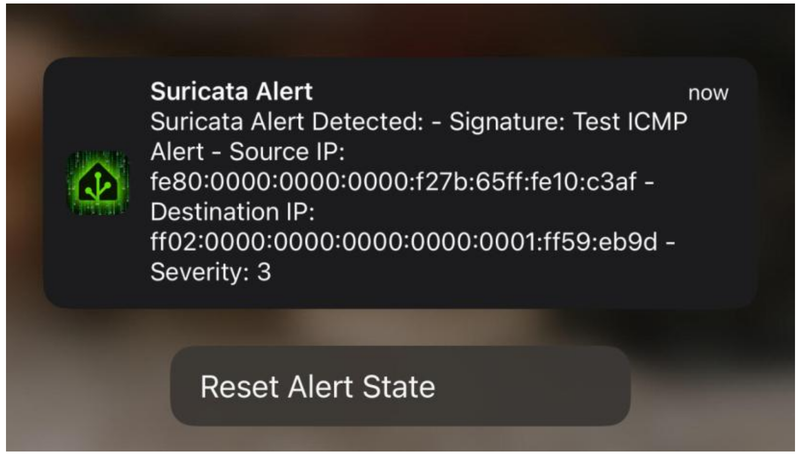


Notify on Suricata Alert

Reset Suricata Alert State



```yaml
automation:
  - alias: Notify on Suricata Alert
    description: Notify iPhone when a new Suricata alert is detected
    trigger:
      - platform: state
        entity_id: 
          - sensor.suricata_alert_signature
          - sensor.suricata_source_ip
          - sensor.suricata_dest_ip
          - sensor.suricata_severity
    action:
      - service: notify.mobile_app_ernests_iphone_2
        data:
          title: "Suricata Alert"
          message: >
            Suricata Alert Detected:
            - Signature: {{ states('sensor.suricata_alert_signature') }}
            - Source IP: {{ states('sensor.suricata_source_ip') }}
            - Destination IP: {{ states('sensor.suricata_dest_ip') }}
            - Severity: {{ states('sensor.suricata_severity') }}
          data:
            actions:
              - action: "RESET_ALERT"
                title: "Reset Alert State"

  - alias: Reset Suricata Alert State
    description: Reset Suricata sensors after acknowledgment
    trigger:
      - platform: event
        event_type: mobile_app_notification_action
        event_data:
          action: "RESET_ALERT"
    action:
      - service: homeassistant.update_entity
        target:
          entity_id:
            - sensor.suricata_alert_signature
            - sensor.suricata_source_ip
            - sensor.suricata_dest_ip
            - sensor.suricata_severity
```

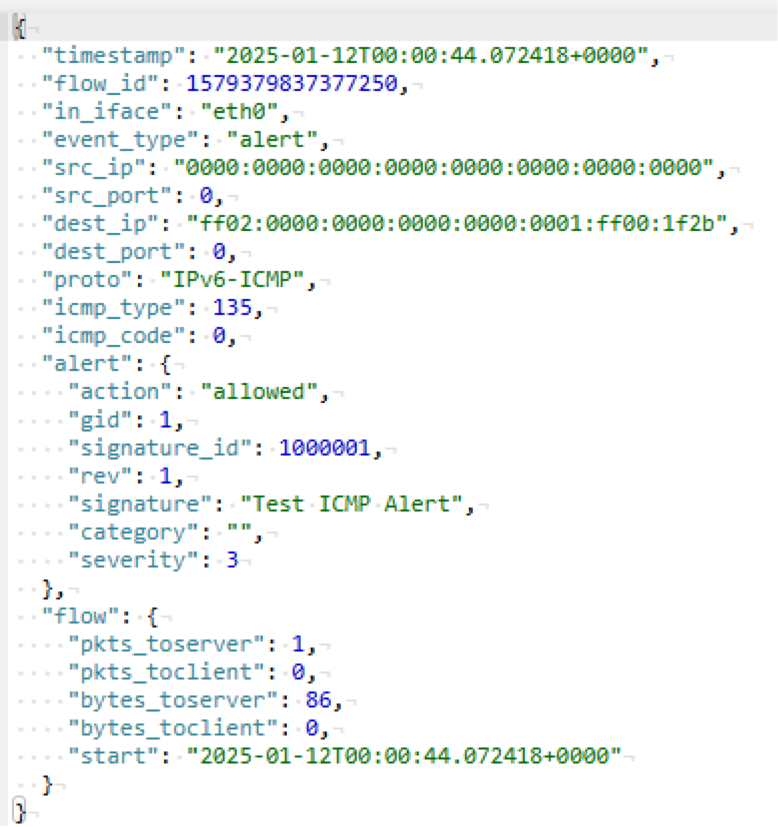


Suricata Alert now

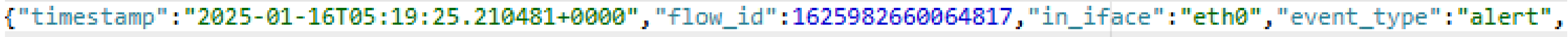
Suricata Alert Detected: - Signature: Test ICMP Alert - Source IP: fe80:0000:0000:0000:f27b:65ff:fe10:c3af - Destination IP: ff02:0000:0000:0000:0000:0001:ff59:eb9d - Severity: 3

Roadblocks?

- Storage Size – Can’t keep logs for an extended amount of time.
- Alert.json formatting.



```
{
  "timestamp": "2025-01-12T00:00:44.072418+0000",
  "flow_id": 1579379837377250,
  "in_iface": "eth0",
  "event_type": "alert",
  "src_ip": "0000:0000:0000:0000:0000:0000:0000:0000",
  "src_port": 0,
  "dest_ip": "ff02:0000:0000:0000:0000:0001:ff00:1f2b",
  "dest_port": 0,
  "proto": "IPv6-ICMP",
  "icmp_type": 135,
  "icmp_code": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 1000001,
    "rev": 1,
    "signature": "Test ICMP Alert",
    "category": "",
    "severity": 3
  },
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 0,
    "bytes_toserver": 86,
    "bytes_toclient": 0,
    "start": "2025-01-12T00:00:44.072418+0000"
  }
}
```



```
{"timestamp":"2025-01-16T05:19:25.210481+0000","flow_id":1625982660064817,"in_iface":"eth0","event_type":"alert",
```

Pacific Northwest
NATIONAL LABORATORY

Thank You!