Create your own NSM devices with Suricata using Dualcomm's ETAP-PI, network tap appliance as well as Raspbery Pi with power redundant, graceful shutdown, user defined push buttons and leds.

Dualcomm's ETAP-PI is a network tap appliance, there are two gigabit port for inline connection, and 1 monitor gigabit port that aggregate the traffic. Not only network tap, ETAP-PI has a raspberry Pi 4 inside the box. We can create our own NSM (network security monitoring), NIDS devices using Suricata, Snort and so on. This TAP appliance has dual redundant power supply and graceful shutdown button, as well as user-defined two LEDs and a push button for enterprise use.

I refer the useful websites below:

https://jufajardini.wordpress.com/2021/02/15/suricata-on-your-raspberry-pi/

https://www.reddit.com/r/raspberry_pi/comments/np1a8f/building_my_home_intrusion_detection_system/

Step1: Install Suricata for Raspberry Pi4

Install required packages

```
  apt-get install python-pip libnss3-dev liblz4-dev libnspr4-dev libcap-ng-dev git
```

Install packages for build Suricata

```
  apt install libpcre3 libpcre3-dbg libpcre3-dev build-essential libpcap-dev libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev make libmagic-dev libjansson-dev rustc cargo python-yaml python3-yaml liblua5.1-dev
```

Get Suricata source file

```
  wget https://www.openinfosecfoundation.org/download/suricata-6.0.3.tar.gz
```

Extract source file and change directory for source file

```
  tar -xvf suricata-6.0.3.tar.gz
  cd suricata-6.0.3
```

Execute configure script with some option

```
  ./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var --enable-nfqueue --enable-lua
```

Compile and install Suricata

```
  make
  sudo make install
```

Setup rules

```
  cd suricata-update
  sudo python setup.py build
  sudo python setup.py install
cd ..
sudo make install-full
```

Step2: Suricata Configuration

Update Suricata rules

```
 sudo suricata-update
```

Edit configuration file

```
 Nano /etc/suricata/suricata.yaml
```

Check #ring-size: 2048 section

And uncomment and change ring buffer size to 30000

```
 ring-size: 30000
```

Step3: Execute Suricata and Test detection

Execute suricata in background (-c config file -i interface -S rule file)

```
 sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -S /var/lib/suricata/rules/suricata.rules &
```

Check the latest log file

```
 sudo tail -f /var/log/suricata/fast.log
```

Access malware specific website

```
 wget 3wzn5p2yiumh7akj.onio
```

and you can find alert event like that

```
ET MALWARE Cryptowall .onion Proxy Domain [**] [Classification: A Network Trojan was detected] [Priority: 1]
```

ps aux | grep suricata to find process ID and kill the process after testing

Step4: Set Suricata as a service

Edit service script

```
 nano /etc/systemd/system/suricata.service
```

Copy and Paste a sample

```
  [Unit]
  Description=Suricata Intrusion Detection Service
  After=network.target syslog.target
  [Service]
  ExecStart=/usr/bin/suricata -c /etc/suricata/suricata.yaml -i eth0 -S /var/lib/suricata/rules/suricata.rules
  ExecReload=/bin/kill -HUP $MAINPID
  ExecStop=/bin/kill $MAINPID
  [Install]
  WantedBy=multi-user.target
```

Start/Stop/Restart/Check Suricata as a service

```
 sudo service suricata [start/stop/restart/status]
```

Step5: Check log and Log rotate

Suricata creates log files at /var/log/suricata

eve.json : huge json file for analysing with Erastic Search and Kibana or Sprunk, etc.

fast.log : suspicious event log (it is useful to just check event)

stats.log : network statistics log

suricata.log : Suricata's service log

Check the latest suspicious events

```
sudo tail –n 100 –f /var/log/suricata/fast.log
```

Suricata may create huge size of log file, so you may configure log rotate setting, so edit log rotate setting file

nano /etc/logrotate.d/suricata

```
   /var/log/suricata/*.log /var/log/suricata/*.json
  {
      daily
      maxsize 1G
      rotate 30
      missingok
      nocompress
      create
      sharedscripts
      postrotate
      systemctl restart suricata.service
      endscript
  }
```

It means each daily log file limit to 1GB and holds the latest 30 files (for a month)

Change logrotate configuration

```
Sudo logrotate –f /etc/logratate.conf
```

Step6: Automatically update Suricata rules at midnight

Edit crontab to update and restart suricata at 3:33 am

```
33 3 * * * sudo suricata-update && sudo service suricata restart
```

It is a typical setting of maintain Suricata by Raspberry Pi but works best with ETAP-PI

Create and customize your own stable NSM device and be ready for cyber security.

I recommend to connect other packet capturing devices at external port of ETAP-PI.

We can check actual pcap/pcapng file with Wireshark, if you find some important security event!!

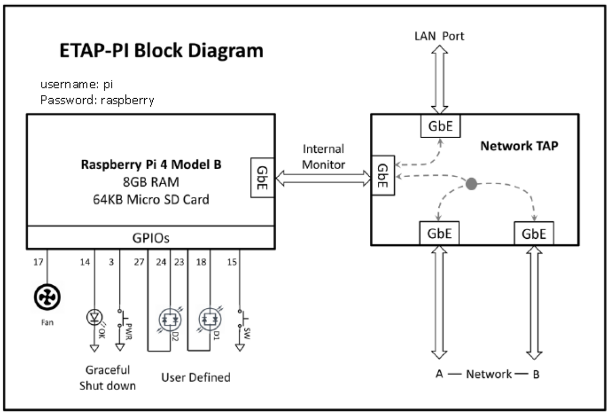
Megumi Takeshita, ikeriri network service co., ltd. (Twitter@ikeriri / megumi@ikeriri.ne.jp)

https://www.ikeriri.ne.jp/develop/Dualcomm/rapsberrypinetworkappliance.html

User’s Quick Guide

Raspberry Pi Network TAP Appliance

(Model No. ETAP-PI)



Description:

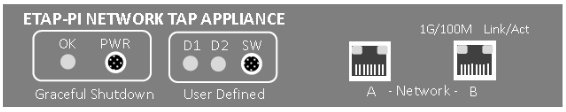
Dualcomm Raspberry Pi Network TAP Appliance (Model ETAP-PI) is a compact portable 10/100/1000Base-T Gigabit Network TAP Appliance that integrates a Raspberry Pi 4 single board computer and a Network TAP into one device. As shown in the block diagram above, ETAP-PI captures packets running through two network Ports A and B and sends them to the Raspberry Pi. An external LAN port is provided for a user to access the Raspberry Pi.

ETAP-PI offers a cost-effective solution for remotely monitoring network traffic of an Ethernet network.

Package Contents:

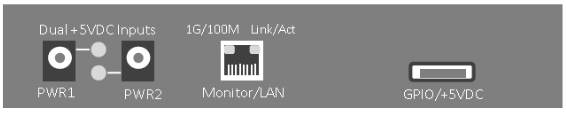
- One ETAP-PI Network Tap Appliance unit
- One AC/DC power adapter (output = +5VDC@3A)

Front Panel



Network Ports	RJ45 Ports “A” and “B”. They are used to connected two end devices of an Ethernet link being monitored. These two ports allow PoE inline power to pass-through between them.
User Defined I/F	Pushbutton “SW” and bi-color LED “D1” and “D2” that are connected to GPIO pins with GPIO pin numbers as shown in the block diagram.
Graceful Shutdown	Hold the pushbutton “PWR” for 5 seconds to gracefully shutdown the Raspberry Pi and the LED “OK” will be turn off. This is necessary before removing power input on the rear panel.

Rear Panel



Dual Power Inputs	Power jack “PWR1” and/or “PWR2” is used to connected to a +5VDC AC/DC power adapter. When ETAP-PI is powered properly, the corresponding LED will be turned on.
Monitor/LAN Port	RJ45 port. It is used to access the Raspberry Pi in ETAP-PI. The monitoring function is enabled by software that is currently not available.
GPIO/+5VDC I/F	Reserved for future uses