Snort IPS using DAQ AFPacket

In order to take full advantage of an IPS sensor, the machine used should have 3 interfaces.

Two interfaces will be used for passing live traffic through Snort, and the remaining interface will be used for management such as SSH or for sending alert data to a management server.

In general, enforcing Snort into running inline (IPS) with DAQ AFPacket, requires four major configuration changes:

a. Configuring Snort policy to run inline (config option within snort.conf).
b. Configuring DAQ AFPacket to run inline (config option within snort.conf, can be passed during runtime).
c. Forcing Snort to run in inline mode with the –Q command line runtime argument.
d. Modifying the rules to drop traffic on matches, i.e., changing "alert" to "drop" using PulledPork.

Notes:

a. Running Snort as an IPS with DAQ AFPacket does not require changing your iptables rules since Snort handles dropping the traffic.
b. When running Snort as an IPS with DAQ AFPacket, Snort itself bridges the interfaces used on the fly. No prior interface bridging/bonding is required.

Snort IPS Configurations (edit snort.conf):

1. Configure the "Inline Packet Normalization" to be enabled. If running Snort in passive mode (IDS), comment/disable "Inline Packet Normalization":

Keep these unchanged. If they are commented out, then uncomment them.

```
preprocessor normalize_ip4
preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
preprocessor normalize_icmp6
```

2. Configure Snort Policy mode to run in inline (IPS):

Under Step #2: add the following line

```
config policy_mode:inline
```

3. Configure DAQ variables to run AFPacket in inline (IPS) mode:

Configure DAQ variables for AFPacket

```
config daq: afpacket
config daq_mode: inline
config daq_var: buffer_size_mb=1024
```

The `buffer_size_mb` value depends on the hardware Snort is running on, amount traffic being inspected, and number of rules enabled.See DAQ README for more information.

4. Configuring rules to drop using PulledPork:

In order to change the behavior of a rule/category to drop, modify the PulledPork dropsid.conf file to make the necessary changes. For example, if rules sid:384 needs to be dropped, simply add the GID:SID of that rule in the dropsid.conf file 1:384.

See PulledPork documentation for more information.

5. Running Snort in Inline (IPS) mode with AFPacket:

Once all configurations are completed, a list of the available DAQ modules can be listed:

```
$ snort --daq-list
```

Output would look like (Note the below is a result of compiling DAQ with --disable-ipq-module --disable-nfq-module --disable-ipfw-module):

```
Available DAQ modules:
pcap(v3): readback live multi unpriv
dump(v2): readback live inline multi unpriv
afpacket(v5): live inline multi unpriv
```

Since DAQ is already configured in snort.conf, Snort can be run using "inline pairs" with the below command:

```
$ snort –c snort.conf –i eth1:eth2 –Q
```

If DAQ was not configured in snort.conf, then Snort can be run with the below command:

```
$ snort –c snort.conf –i eth1:eth2 –Q --daq afpacket --daq-mode inline \
  --daq-var buffer_size_mb=1024
```

In the commands above, Snort bridges the two interfaces (eth1:eth2) and acts as the bridge (sort of like br0).

If multiple interfaces are being monitored, then run snort as:

```
$ snort -c snort.conf -i eth1:eth2::eth3:eth4 -Q
```

For more info, see this: http://vrt-blog.snort.org/2010/08/snort-29-essentials-daq.html.