Intrusion Detection systems

Suricata

On your pfsense machine, navigate to system->package manager. Install the suricata package. After doing so, you should see a `suricata` option on your `Services` menu.

The video here provides a good overview as to how to install and configure suricata on pfsense. You should watch it and configure yours.

Testing your IDS

A few words of advice here... If we trigger an alert, it also might be triggered upstream if another IDS is running. Here are some ways to trigger an alert to see if suricata is correctly working. These things would have to be done from a machine that is configured to go through the pfsense machine (i.e. Kali).

- `curl testmyids.com`
- ping some site from the flagged ip list. A list of flagged hosts can be found here Not all may respond. You could easily write some script that pings a host that might look similar to this:

  ```
  for ip in $badips
  do
      echo $ip
      ping -c1 -w1 $ip
  done


  #badips would need to be a list of badips you want to ping.
  ```

- do a dns query to a black listed domain (like .tk domain)
- Download a torrent file `sudo apt install transmission-cli` then download something from this page.

You should see some alerts in your suricata machine now.

To pass off

You should show me that you are getting some alerts.