Snort!

What’s it all about?

- Intrusion Detection System
- ... and Prevention, and Wiretapping, and ...
  - We’re only interested in detection
  - We already have iptables well integrated with lcfg
  - Wireshark does a good enough job for wiretapping

Component parts

- Snort itself does the capture
  - Watches packets as they go past
  - Rule-based inspection engine
  - Writes out a log for later processing
- Rules are managed using pulledpork
  - Pulls down the latest set from snort.org
  - Enables rules based on how paranoid you configure things to be
- Logs are processed using barnyard2
  - Haven’t explored that yet!

Where do you run it?

- Basically everywhere you think you might want to detect intrusions.
- In our case that's on at least every primary edge router.
- We might run it elsewhere too, or we might decide that's too heavy. We won't know until we try it.

Rules

- Rules come in three categories:
  - Paid-for, which are available for download immediately they're released
  - Free, which are the paid-for from 30+ days before
  - Community-written
- Charging model is per-machine, so we couldn't run paid-for rules everywhere
  - Not actually clear whether we would gain by paying anyway.

Where are we at?

- Not as far as we would have hoped, unfortunately, as other things keep taking priority!
- Basic packages built, header created.
- Still to set up a prototype.
- Lcfg configuration??