COMMON PROBLEMS

- No logs!
- Doesn’t work right at all
- Works, but high Packet Loss or Capture loss
- Works, but Crashes
NO LOGS

Everything looks like it is working but...

This is almost always a firewall problem.
DOESN’T WORK RIGHT AT ALL

Generally related to capture issues
TROUBLESHOOTING CAPTURE ISSUES

# broctl stop
# tcpdump -n -i plp1 -c 1000 -s 0 -w cap.pcap
# bro -r cap.pcap
# wiresharp cap.pcap # get a 2nd opinion

If the pcap is broken, bro has no chance of working right.
WORKS, BUT HIGH PACKET LOSS OR CAPTURE LOSS

Step one: determine the difference!

High capture loss with no packet loss is not a problem Bro can fix.
WORKS, BUT … LOSS

- Underpowered hardware: Not all processors are alike
- https://www.cpubenchmark.net/singleThread.html
WORKS, BUT ... LOSS

Configuration issues:

- Too many workers
- Not using CPU Pinning
- Using CPU pinning in exactly the wrong way
WORKS, BUT CRASHES

OOM crashes on the manager are the most common problem.