SAND2016-7171C

Exceptional service in the national interest

Sandia National Laboratories

Inferring Netflow Data

Harrison Roth

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

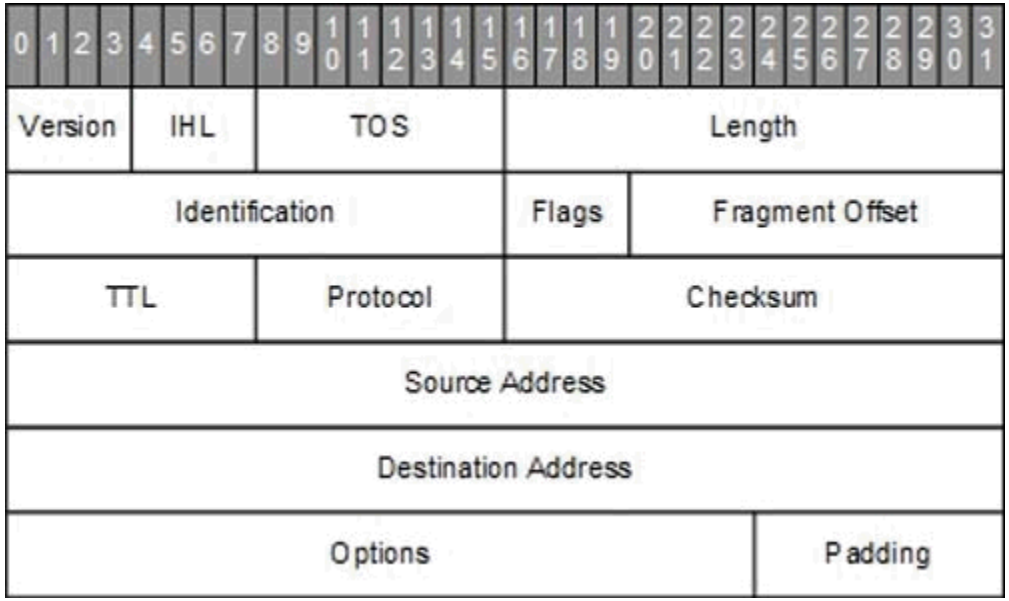
Background

Sandia National Laboratories

- Netflow Data
- Cloud Service Provider (CSP) logs
  - Box.com
  - Amazon Web Services

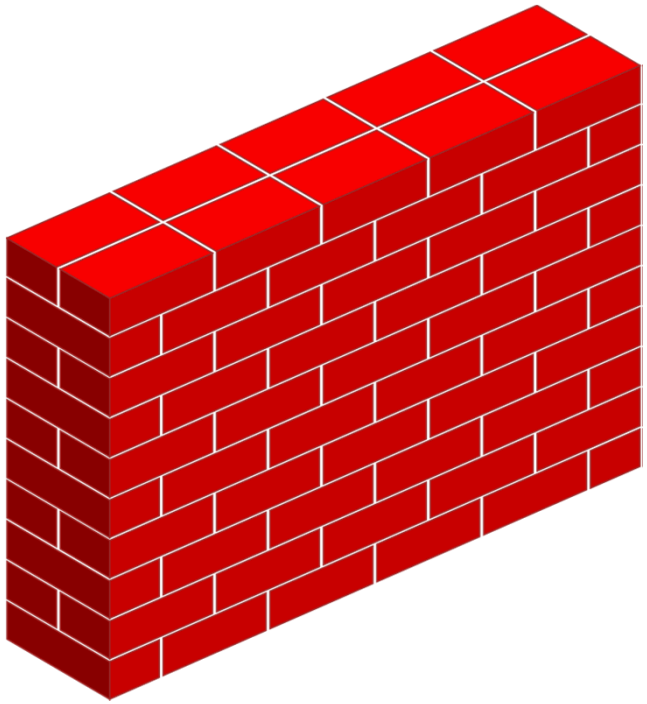
Task

- Infer missing netflow data fields from synthetic CSP logs
- Potential inferable data:
  - Destination IP
  - Source and Destination Ports
  - Sensor ID



Obstacles

- Unknown Information
- Admin Rights
- Amazon Web Services restrictions
- Computer Problems



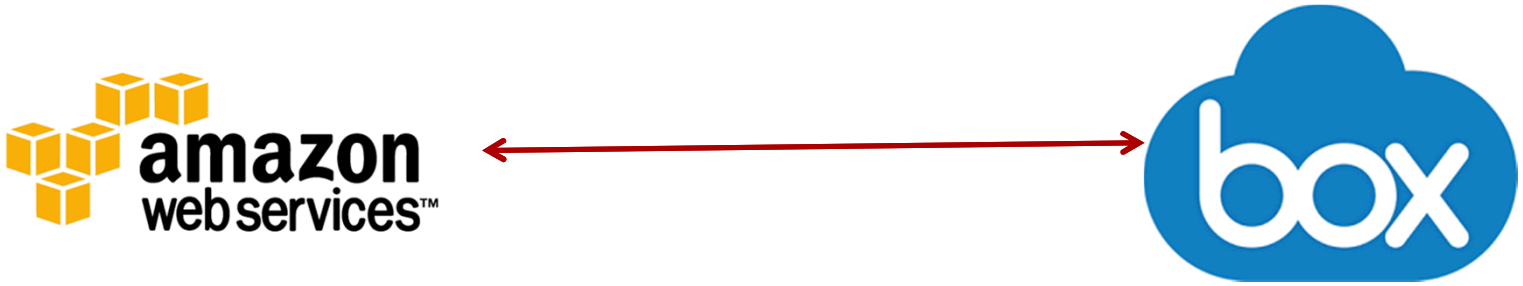
Outcomes

- Sensor ID confirmed
- Destination IP restricted for Box

Ongoing Work

Sandia National Laboratories

- Client side packet capture
- Make box calls from AWS server



Next Steps

- Confirm Destination IP spread for Box.com
- Confirm Assumed Ports