Egress Filtering

How to implement egress filtering with out becoming the most hated person in the organization

Intro

- Name: Archie Woodworth
- Employer: MaineHealth
- Position: Sr. IT Security Engineer
- Background:
  - IT audit
  - Policy and program management
  - Technical and hands-on
- Contact: awoodworth@mmc.og

Approach

- Recon & Research
- Project Planning
- Management Buy in and Support
- Phased Approach
- Implementation Process
- Conclusion
- Questions

Recon & Research

- Lots of sites and subnets spread out all over the state
- Lots of outbound traffic
- Lots of questions

Project Planning

- Project Charter
- Project Plan
- Approach

Management Buy in and Support

- Really important
  - Someone has to back you
  - Someone has to make decisions
- Technology & Infrastructure Governance Committee

Phased Approach

- Start small
- Communicate
- Build on your successes
- Then just go for it

Implementation Process

- Pick location/subnet(s)
- Monitor traffic
- Research get approvals if needed
- Add to existing rules or create new
- Schedule and communicate
- Implement block rule
- Monitor and adjust as needed

Conclusion

- So far the approach seems to be working
  - I haven't broken anything major
  - Change control meetings area a breeze
  - Yes, I do get blamed for stuff, but egress filtering is generally not the culprit
  - I have not become the most hated person in the organization
    - Well not because of egress filtering anyway