DDoS Mitigation at NORDUnet

Lars Fischer
(w/ big thanks to Martin Aldrin)
TF-MSP Meeting
Malta, 27 November 2014
DDoS is a major issue; every responsible network must be working on the best ways to counter it.

So far NORDUnet is doing blackholing.

- It works
- It kills an entire network
- Creates "Innocent bystander" problem
- Creates reluctance to deploy
Options

- Scrubbing
  - Intelligence DDoS Mitigation Systems (IDMS)
  - Commercial products available (i.e., Arbor Networks)
  - Costly
  - Unlike carriers, we cannot sell it as a service

- Enterprise-level solutions
  - IP rewrite, running traffic through filter or firewall
  - Does not scale to our needs

- Flowspec
  - Promising
  - This is our bet for a future solution
What is FlowSpec?

- Flow Specification (RFC 5575)
  - Designed for DDoS mitigation
  - Remote triggered ACLs
  - Extension to BGP
  - Can match in various events and traffic types
  - Can act to rate-limit, redirect, mark, etc
- Bleeding edge technology, working it’s way through IETF
  - Per-interface capability only came this summer
• **Objective**
  • Investigate what a FlowSpec-based solution might look like
  • Is there a good match for NREN environment?
  • DIY, since there’s nothing in the market
  • Can we create a controller to dynamically assign FlowSpec rules?

• **Student project**
  • MSc student: Martin Aldrin
  • Controller design and development
  • Full implementation and test
  • Lab exercise
Real traffic lost
Better, but still load on core
Co-operating networks reduce core load.
NORDUnet
Nordic infrastructure for Research & Education

Lab w/ FlowSpec controllers
NORDUnet
Nordic infrastructure for Research & Education

Real traffic flow

Survival rate vs. Time in minutes
- Multi weight
- Multi
- Single

50% 60% 70% 80% 90% 100%
0 0,5 1 1,5 2 2,5 3 3,5 4 4,5 5 5,5 6 6,5 7 7,5 8

Multi weight
Multi
Single
• We have done the experiment
• We have it working in the lab
  • Decision point: is this something we’re pushing towards production?
• Live network trial?
  • We have not decided
  • We need a customer / border to try it on
• Solution has network effect
  • Value go up with more deployments
  • There’s mutual benefit
• (and there’s additional technical work we’d like to do)
Joint Effort?

- Collaborative DDoS effort based on FlowSpec?
  - Are we solving a problem?
  - Is this something other networks see value in?
- Community adopting the technology?
  - GÉANT Firewall-as-a-service based on FlowSpec
- What next?
  - Is the idea liked?
  - How do we set up a collaboration?
  - What is the way forward?
Conclusions

• We must have something better than blackhole
• Right now that means FlowSpec
• We have to go DIY
• It works in the lab
• We want to work with YOU
  • Real value comes if many are doing it