CGN Log Reduction
draft-donley-behave-deterministic-cgn

Chris Donley | July 30, 2012
1) describe the problem to be solved and show that there is widespread demand for a solution

- CGN Logging Generates Huge Data Volumes
- Subscribers generate around 33,000 connections/day
  - 150-byte log messages x 33,000 connections/day = 5MB/day/sub
  - 1M-sub ISP will generate 150 TB of data/month (1.8 PB/yr)
  - Assuming 50,000 subs/CGN => 23 Mbps of logging traffic
- Conclusion: per-connection CGN logging is not scalable
- Significant interest from service providers and public safety officials in a solution
2) demonstrate that the problem can not be solved with existing Technologies

- Two existing approaches to CGN logging
  - per-connection logging
  - bulk-port logging
- Bulk-port logging reduces log volumes, but still poses search impact on ISPs/public safety
  - Logging infrastructure
  - Timestamp alignment
  - DB Search time
Proposed solution: Deterministic CGN

- Supports both v4 and v6
- Uses an algorithm to allocate ports per subscriber
  - Abuse Response reverses algorithm to identify inside address
  - Eliminates the need for most logging (except for power users)
  - Reduces privacy impact on subscribers
- Logging only required for subs that exceed predefined port ranges
  - Uses bulk port logging for overflow log
- Reduces logging volumes 100 K – 1 M x vs. per-connection logging
Will not harm/delay v6 transition

• Carrier Grade NAT/NAT444 is already occurring
• Requirements documented in draft-ietf-behave-lsn-requirements-08
• Solution optimizes port reservation/logging; does not introduce new v4-v6 transition technologies
• Supports incremental cgn approach (RFC 6264)
Changes since -02

• Reviewed in BEHAVE and v6ops
• Reviewed with public safety community
• Incorporated feedback from both working groups and public safety officials
• Updated to fit within sunset4 charter
• Minor cleanup
Next Steps

- WG draft?