RRL -- Strategies for a Successful Deployment

November 2013
Welcome!

- Presentation – 45 minutes
  - Interactive Question & Answer Format
- All attendees are on **mute**
- Q&A during the session
  - Use WebEx chat window to submit questions
  - In the interest of time, please email unanswered questions to info@isc.org
- A recording of this event will be sent to all registered attendees
Agenda

- ISC and DNSco
- RRL Question & Answer
  - Configuration
  - Utilizing Log Files
  - Gotchas
  - Additional Classifier Options
- Summary
Presenters

- Eddy Winstead, Senior Systems Engineer
- Peter Losher, Senior Operations Architect
ISC at a Glance

**Sponsored R&D**
- Open Home Gateway
- Open Source Routing

**Public Benefit**
- Hosted@
- F-Root
- Open Source Software

**Commercial Services**
- Subscription Services
- DNS Hosting
- Training

© 2013 ISC
RRL OVERVIEW
Response Rate Limiting

- **An Enhancement to the DNS**
  - A mechanism for limiting the number of unique responses returned by a DNS server
  - A mitigation tool for the problem of DNS Amplification Attacks
  - The only practical defense available for filtering in the name server
    - **BIND 9.9.4** includes RRL as a key feature
      - Available for download at [https://www.isc.org/downloads/](https://www.isc.org/downloads/)
Normal Traffic

5.6.7.8

Responds to 5.6.7.8

Source IP Address: 5.6.7.8

Internet

1.2.3.4
rDoS Attack

Source IP Address:
5.6.7.8
1.2.3.4

Responds to 1.2.3.4
ISC’S EXPERIENCE
How did RRL come about?

- ISC signed our zones in 2006
- Observed queries that were occurring too frequently from the same IP
- Defensive strategy sessions with Paul led to RRL

EDNS0 query for isc.org of type ANY is 36 bytes long. **Response is 3,576 bytes long**
Accidental? Enemies

Poor Network Hygiene

- Non-caching name servers
- Too frequent flushing
- Open recursive servers
RRL on ISC network

- Deployed on isc.org and SNS in Spring of 2012
- Deployed on F-root in Summer of 2013
ISC F-Root

f-ams1 traffic (~1 day, bits)

(as of Fri Jul 19 06:09:42 2013 GMT)

IN
Max(Max)= 11.48Mb
Avg(Max)= 4.43Mb
Max(Avg)= 11.48Mb
Cur(Avg)= 0b

OUT
Max(Max)= 56.53Mb
Avg(Max)= 9.21Mb
Max(Avg)= 56.53Mb
Cur(Avg)= 0b
ISC F-Root

f-ams1 traffic (~1 day, bits)

max input  avg input  max output  avg output
(as of Fri Jul 19 06:09:42 2013 GMT)

IN  Max(Max)= 11.48Mb  Avg(Max)= 4.43Mb  Max(Avg)= 11.48Mb  Cur(Avg)= 0b
OUT  Max(Max)= 56.53Mb  Avg(Max)= 9.21Mb  Max(Avg)= 56.53Mb  Cur(Avg)= 0b
ISC F-Root

f-ams1 traffic (~1 day, bits)

- Implemented RRL

Attackers gave up in frustration

<table>
<thead>
<tr>
<th></th>
<th>max input</th>
<th>avg input</th>
<th>max output</th>
<th>avg output</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN</td>
<td>Max(Max) = 11.48Mb</td>
<td>Avg(Max) = 4.43Mb</td>
<td>Max(Avg) = 11.48Mb</td>
<td>Cur(Avg) = 0b</td>
</tr>
<tr>
<td>OUT</td>
<td>Max(Max) = 56.53Mb</td>
<td>Avg(Max) = 9.21Mb</td>
<td>Max(Avg) = 56.53Mb</td>
<td>Cur(Avg) = 0b</td>
</tr>
</tbody>
</table>

(as of Fri Jul 19 06:09:42 2013 GMT)
CONFIGURING RRL
K.I.S.S.

- **SLIP**
  - How many UDP requests can be answered with a truncated response.
  - Setting to “2” means every other query gets a short answer

- **Window**
  - 1 to 3600 second timeframe for defining identical response threshold
  - Highly variable based on conditions

- **Responses-per-second**
  - How many responses per second for identical query from a single subnet
  - Highly variable based on conditions
RRL Config

rate-limit {
  slip 2;       // Every other response truncated
  window 15;    // Seconds to bucket
  responses-per-second 5; // # of good responses per prefix-length/sec
rate-limit {
    slip 2;       // Every other response truncated
    window 15;    // Seconds to bucket
    responses-per-second 5;   // # of good responses per prefix-length/sec
    referrals-per-second 5;  // referral responses
    nodata-per-second 5;     // nodata responses
    nxdomains-per-second 5;  // nxdomain responses
    errors-per-second 5;     // error responses
    all-per-second 20;       // When we drop all
}
rate-limit {
    slip 2; // Every other response truncated
    window 15; // Seconds to bucket
    responses-per-second 5; // # of good responses per prefix-length/sec
    referrals-per-second 5; // referral responses
    nodata-per-second 5; // nodata responses
    nxdomains-per-second 5; // nxdomain responses
    errors-per-second 5; // error responses
    all-per-second 20; // When we drop all

    log-only no; // Debugging mode
RRL Config

rate-limit {
  slip 2;       // Every other response truncated
  window 15;    // Seconds to bucket
  responses-per-second 5; // # of good responses per prefix-length/sec
  referrals-per-second 5; // referral responses
  nodata-per-second 5; // nodata responses
  nxdomains-per-second 5; // nxdomain responses
  errors-per-second 5; // error responses
  all-per-second 20; // When we drop all

  log-only no;    // Debugging mode
  qps-scale 250;  // x / 1000 * per-second
                   // = new drop limit
  exempt-clients  {127.0.0.1; 192.153.154.0/24;};
}
rate-limit {
    slip 2;       // Every other response truncated
    window 15;    // Seconds to bucket
    responses-per-second 5; // # of good responses per prefix-length/sec
    referrals-per-second 5; // referral responses
    nodata-per-second 5; // nodata responses
    nxdomains-per-second 5; // nxdomain responses
    errors-per-second 5; // error responses
    all-per-second 20;  // When we drop all

    log-only no;     // Debugging mode
    qps-scale 250;   // x / 1000 * per-second
                     // = new drop limit
    exempt-clients { 127.0.0.1; 192.153.154.0/24; 192.160.238.0/24 }

    ipv4-prefix-length 24;  // Define the IPv4 block size
    ipv6-prefix-length 56;  // Define the IPv6 block size
RRL Config

every client can hit 5 p/s of:
rate-limit {
  slip 2;  // Every other response truncated
  window 15;  // Seconds to bucket
  responses-per-second 5; // # of good responses per prefix-length/sec
  referrals-per-second 5; // referral responses
  nodata-per-second 5; // nodata responses
  nxdomains-per-second 5; // nxdomain responses
  errors-per-second 5; // error responses
  all-per-second 20; // When we drop all

  log-only no;  // Debugging mode
  qps-scale 250; // x / 1000 * per-second
    // = new drop limit
  exempt-clients { 127.0.0.1; 192.153.154.0/24; 192.160.238.0/24 }
  ipv4-prefix-length 24; // Define the IPv4 block size
  ipv6-prefix-length 56; // Define the IPv6 block size

  max-table-size 20000; // 40 bytes * this much maximum memory
  min-table-size 500;  // pre-allocate to speed startup
};
Use of Logfiles

- Initially use logging
- Use a separate logging channel to segregate data from regular logs

Log only “dry run” feature to view behavior before going live with RRL
Logging Config

```plaintext
logging {
    channel query-error_log {
        file "log/query-error.log" versions 7 size 100M;
        print-category yes;
        print-severity yes;
        print-time yes;
        severity info;
    }
    category query-errors { query-error_log; }
}
```
Things to Consider

- French Connection – SLIP issue
- Window length – interrupt self-monitoring
  - Whitelist option ‘exempt clients’
- Not responding to legitimate queries
RRL Classifier

- **Expansion of RRL Basic**
  - RRL Basic filters on Destination Address of Response (source of attack traffic is assumed to be forged, but provides address of attack target)

- **2014**
  - Name Requested (QNAME)– allows for whitelisting and supports possible expansion to recursive use case
  - Size of the Response– limits amplification potential
Additional info on RRL

- Response to SLIP issue

- Vixie Article on DNS Security
FURTHER QUESTIONS?
Webinar Special Offer

- 10% discount on Advanced BIND Training Class
  - For registrations made before March 15th
  - Coupon code will be in the email with the recording link
We want to hear from you!

- Look for follow-up email with links to webinar recordings and this presentation
- Take the user profile survey

https://www.surveymonkey.com/s/isc-downloads
Webinar Survey

- Please take a moment to complete the survey now displayed.
Thank You

For more information about RRL Basic, contact us at info@isc.org

For more information about RRL Classifier, contact us at info@dns-co.com

www.ISC.org

www.DNS-co.com