Response Policy Zones for the Domain Name System (DNS RPZ)

By Paul Vixie, ISC (et.al.)
2010 World Tour

Overview

- Motivation for DNS Response Policy Zones
- Relationship to DNS RBL (DNSBL)
- RPZ Constraints and Goals
- How RPZ Works
- Design Details
- Future Directions
- Demo
- Conclusion

Motivation for DNS RPZ

- Most new and many existing domain names are noncooperative (infospam, malevolent, etc)
- Noncooperative domain owners depend on the Global (cooperative) DNS for their success
- No method exists for withholding cooperation for these domain names or their owners
- Such a method, implemented in recursive DNS (RDNS), could prevent some uncooperative domain owners (including criminals) from reaching victims

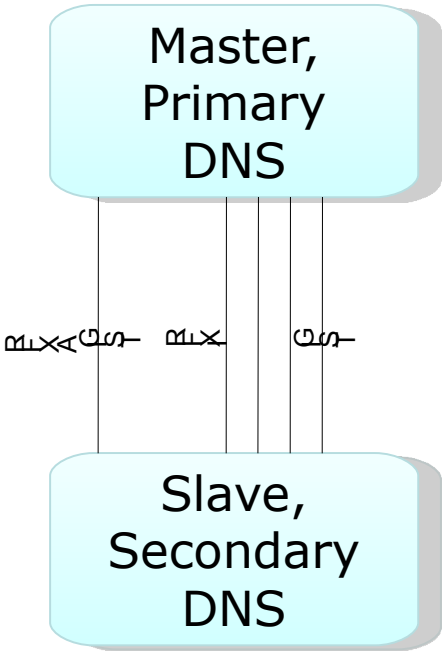
Relationship to DNS RBL (DNSBL)

- In 1998, the first DNS-based SMTP reputation system was created at Vixie Enterprises
- This was published by MAPS (Vixie and Rand) and was the first Realtime Blackhole List (RBL)
- Now 15 years later, hundreds of RBL providers protect virtually all Internet SMTP servers
- With DNS RPZ, we (ISC) intend to repeat this story, but this time protecting recursive DNS (RDNS) servers

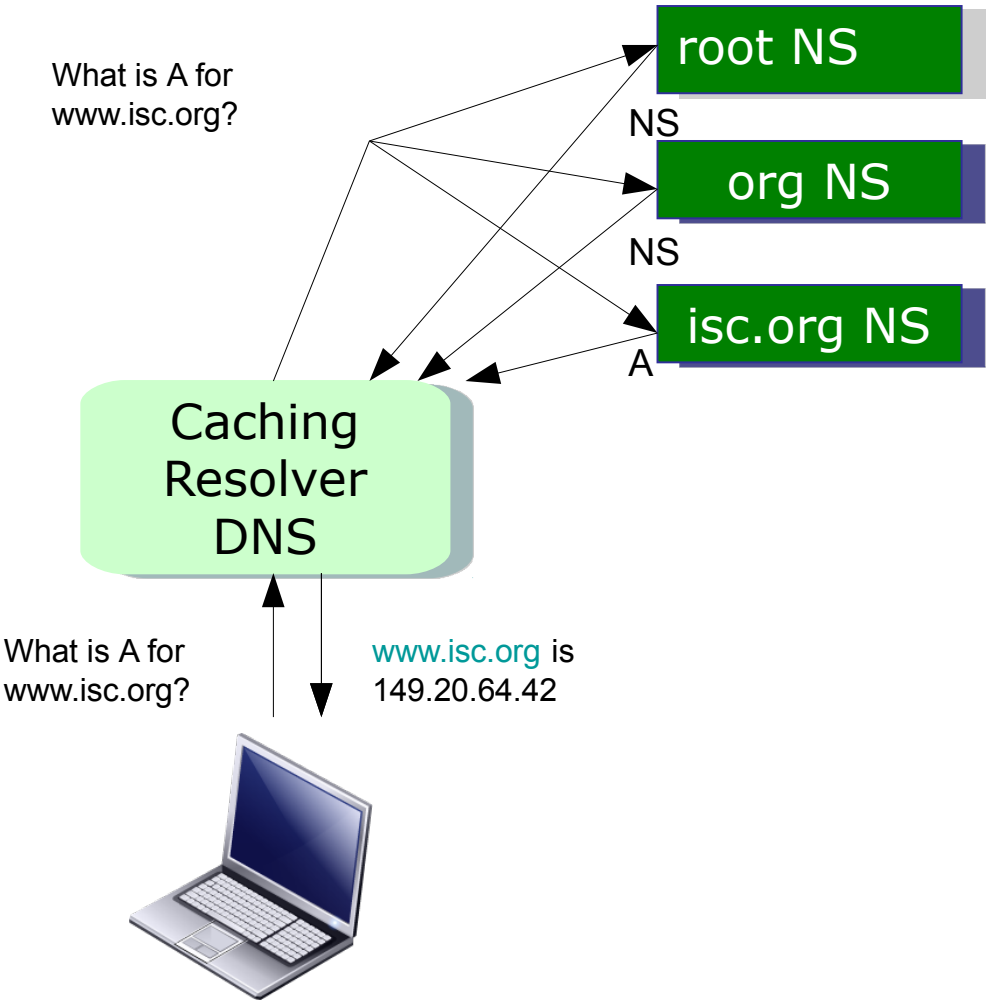
RPZ Constraints and Goals

- The goal of DNS RPZ is a global technology standard and market for publication/subscription of DNS reputation information
- Must be unencumbered by patents or licenses, and available in many RDNS implementations
- Must not generate new wide area DNS traffic or make RDNS more fragile / less robust / slower
- Must not directly facilitate NXDOMAIN remapping or any other form of DNS pollution

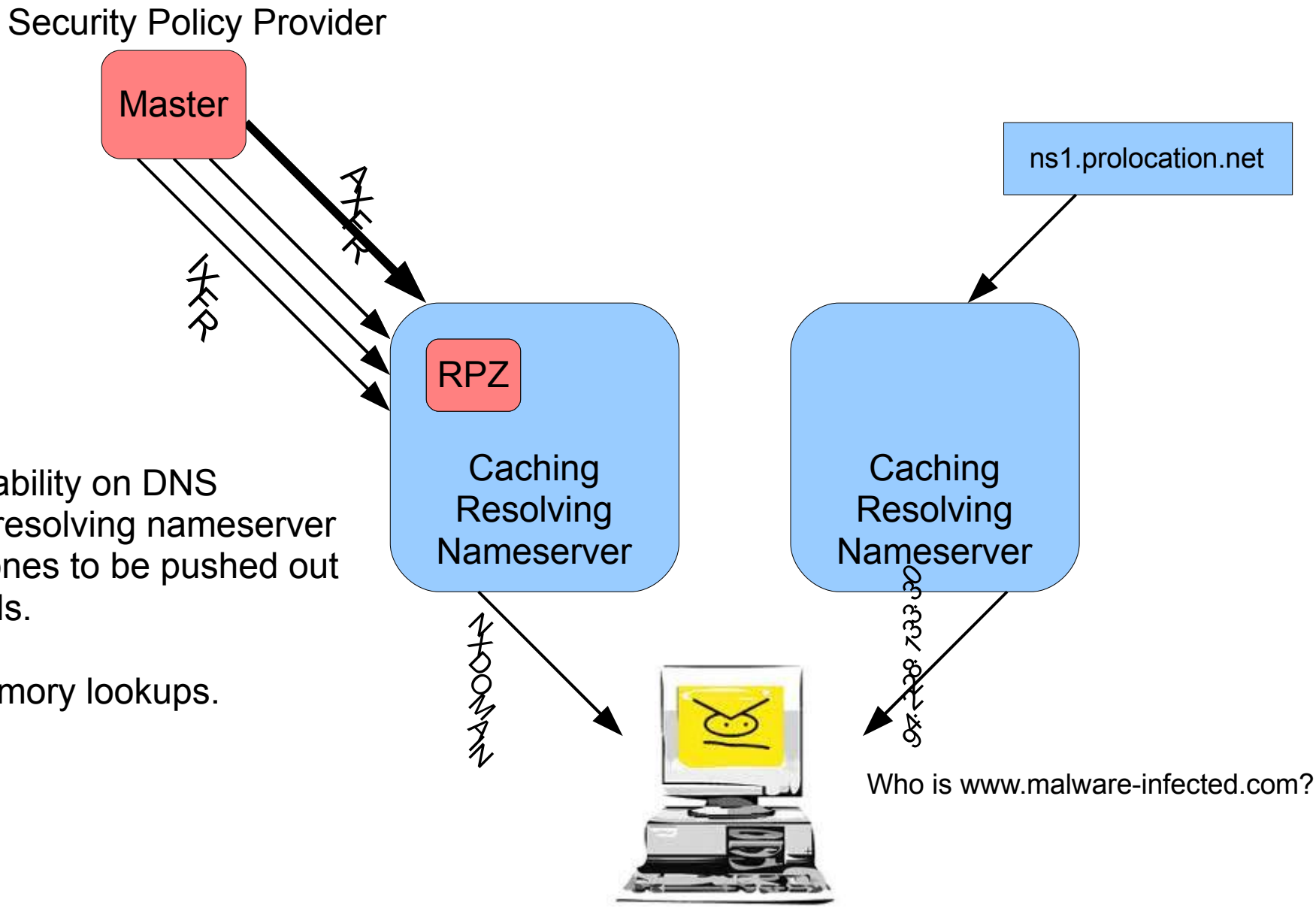
Normal DNS operation



AXFR - Full Zone Transfers
IXFR - Incremental Zone Transfers
TSIG - **Transaction SIGnature**
used to secure the AXFR/IXFR



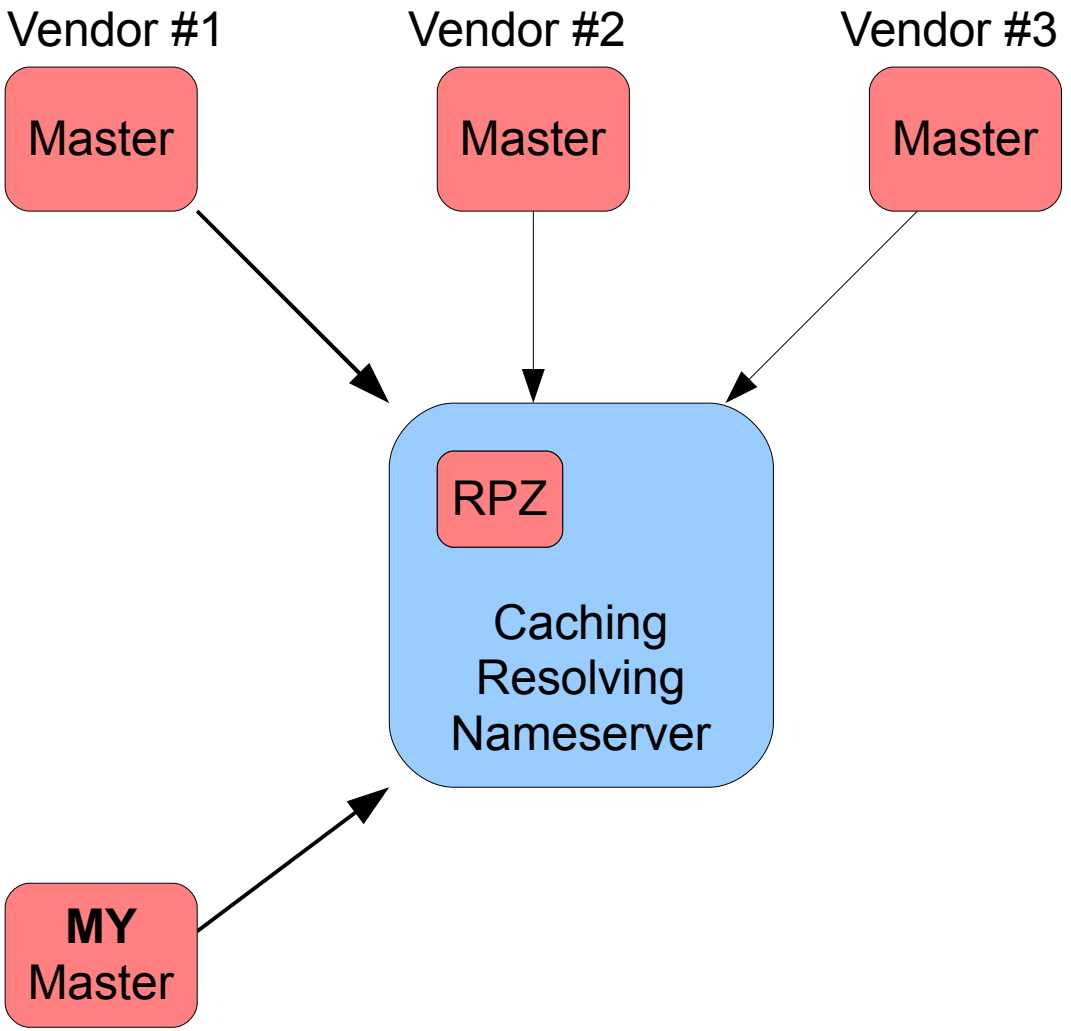
How RPZ is different



RPZ capability on DNS Caching resolving nameserver Allows zones to be pushed out in seconds.

Local memory lookups.

Multiple providers



RPZ Design Details (1)

- Subscribing RDNS servers are made a stealth secondary for response policy zone(s) (RPZs)
- TSIG is used to control access and authenticity
- NOTIFY is used to ensure timeliness of updates
- IXFR is used to compress updates into deltas
- An RDNS can subscribe to more than one RPZ and if so they are searched in order, per query
- RDNS operators can use a mix of private and public RPZs, using search order for precedence

RPZ Design Details (2)

- At an RPZ apex, there is an SOA (used to control IXFR and negative cache TTL) and an NS (which is never used)
- RPZs are never queried and so need not be delegated by their parents nor have globally unique names
- Linkage from RDNS to RPZ is by configuration
  - response-policy {

        zone "dns-policy.vix.com";

        zone "rpz.deteque.com";

    };

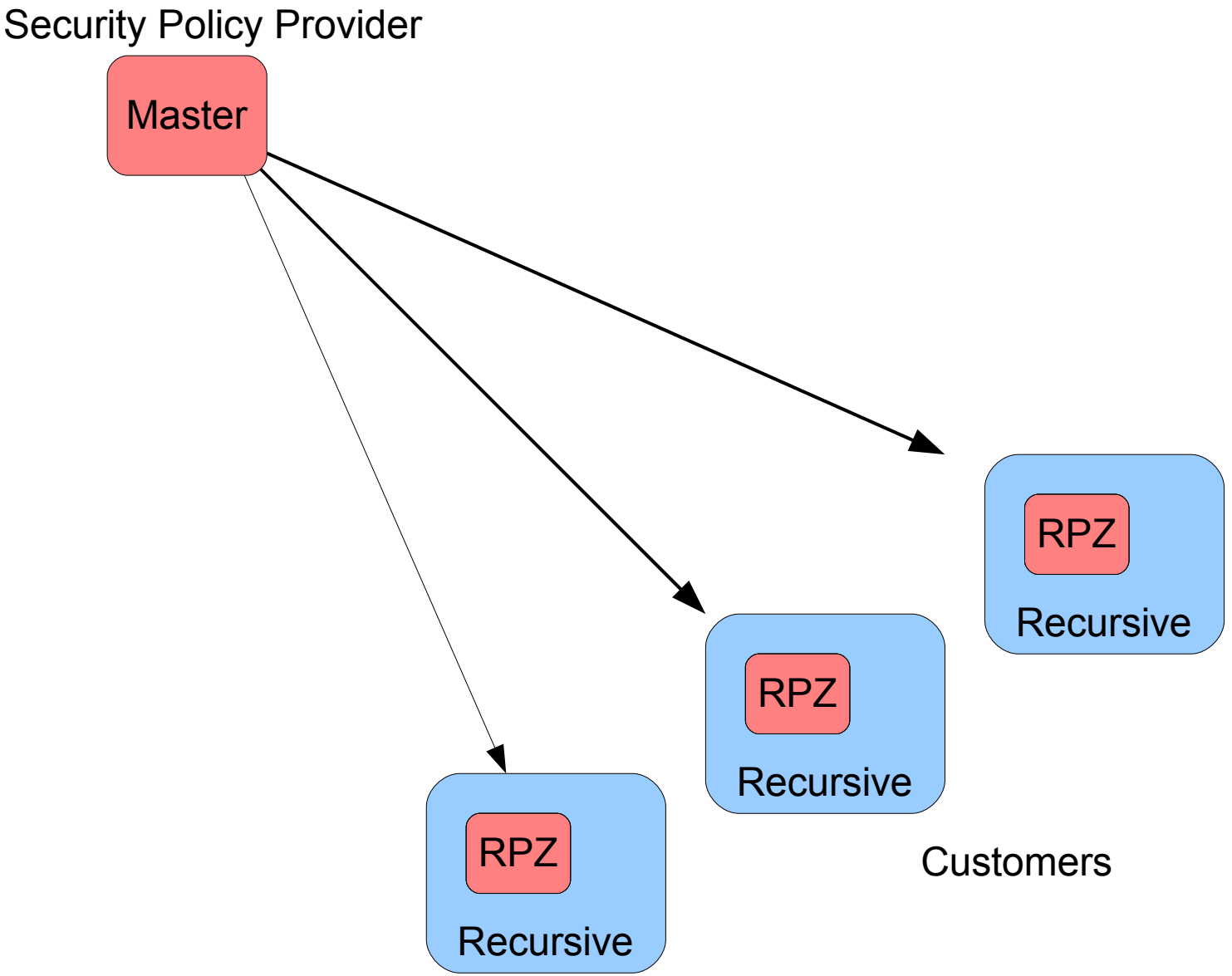
RPZ Design Details (3)

- Policy data uses rehomed global names and some special RDATA patterns for control:
  - To force an NXDOMAIN:
    - `www.malware-infected.com.@ CNAME .`
  - To force a NODATA:
    - `www.malware-infected.com.@ CNAME *.`
  - To end the search early:
    - `www.malware-infected.com.@ CNAME www.malware-infected.com.`
  - To force a specified answer:
    - Use any normal RR, including CNAME

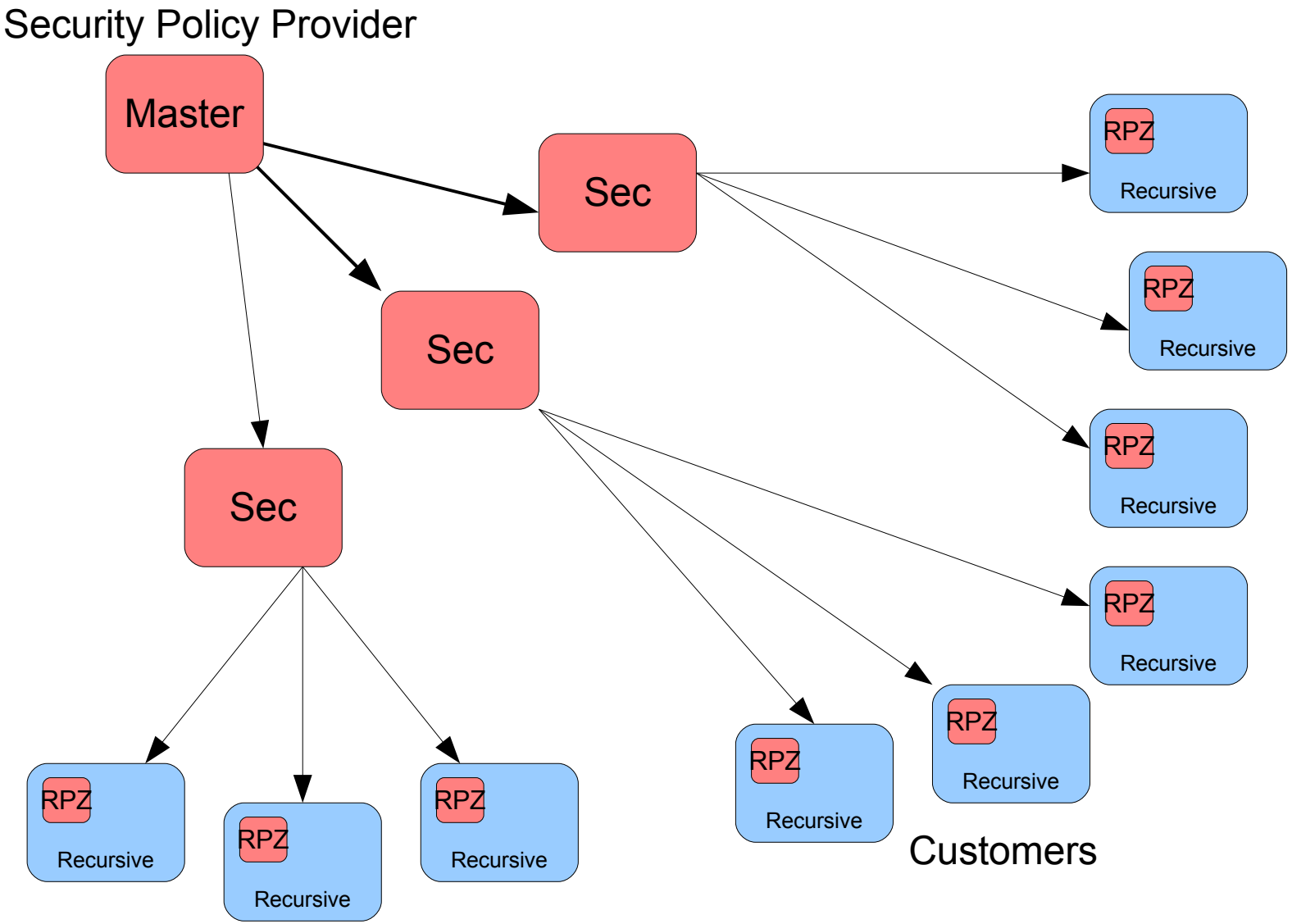
RPZ Design Details (4)

- Note that `wide.ad.jp.@` would match only `wide.ad.jp`, not subdomains – so maybe also add `*.wide.ad.jp.@`
- There is no way to do NXDOMAIN remapping with RPZ since processing happens before recursion

Distribution



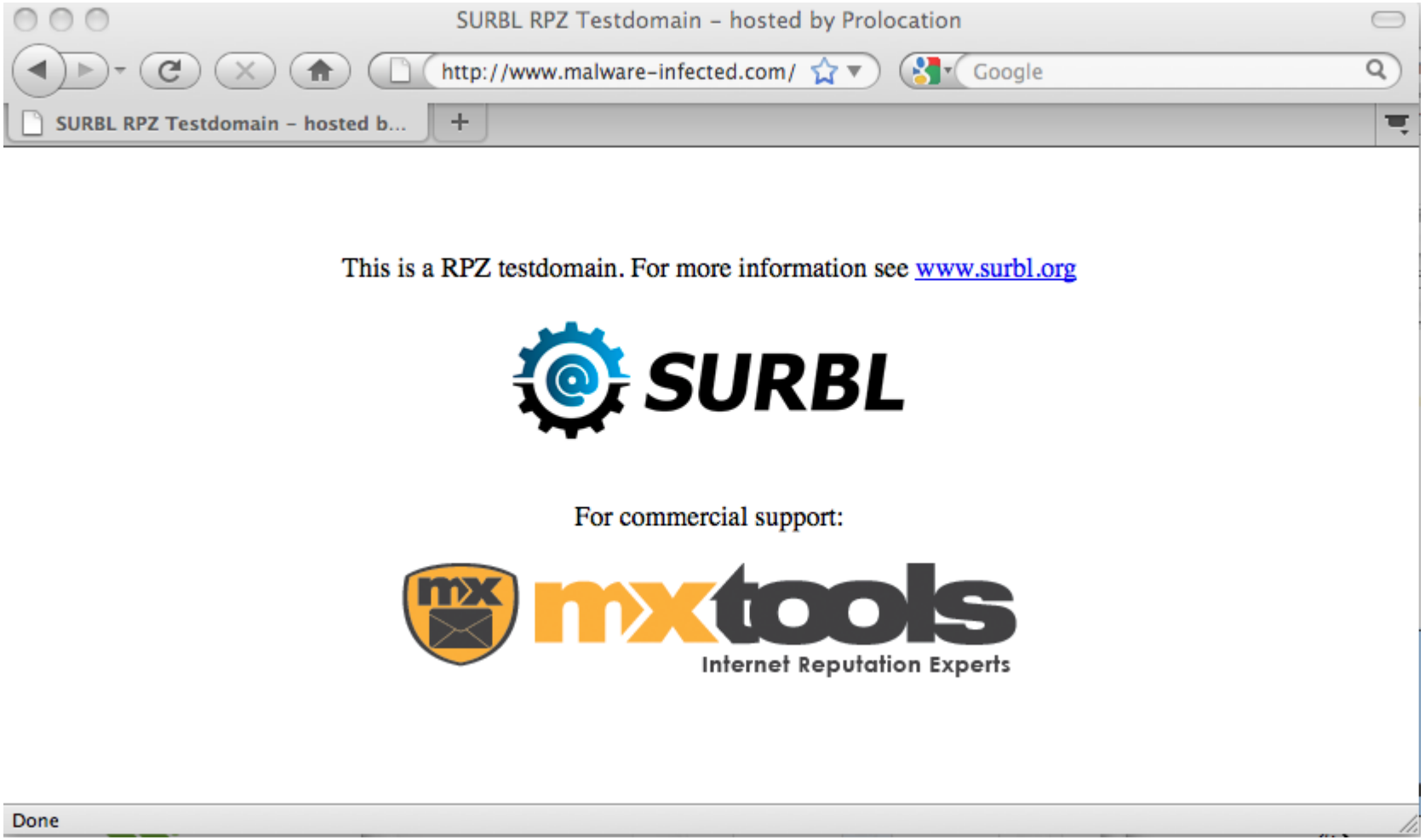
Distribution



Demo

- RPZ.SURBL.ORG

Demo


SURBL RPZ Testdomain – hosted by Prolocation
http://www.malware-infected.com/
Google
SURBL RPZ Testdomain – hosted b...
This is a RPZ testdomain. For more information see www.surbl.org
SURBL
For commercial support:
mxtools
Internet Reputation Experts
Done

Demo


Terminal — sh — 106×22
zl:~ root# cat /etc/resolv.conf
nameserver 204.152.187.111
zl:~ root# dig www.malware-infected.com a
; <<>> DiG 9.6.0-APPLE-P2 <<>> www.malware-infected.com a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 8248
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;www.malware-infected.com.   IN   A
;; AUTHORITY SECTION:
rpz.surbl.org.   180   IN   SOA   dev.null. zone.surbl.org. 1287751686 180 180 604800 180
;; Query time: 238 msec
;; SERVER: 204.152.187.111#53(204.152.187.111)
;; WHEN: Fri Oct 22 14:55:16 2010
;; MSG SIZE rcvd: 104
zl:~ root#

RPZ Future Directions

- RPZ can be revised by adding new patterns which are invisible to prior RDNS implementations
- Next feature will be IP4/IP6 reputation support:
  - Triggered by response data, not by query name
  - So, `27.0.150.104.24._ip4.@` would match any “A” RRset matching 24.104.150.0/27
  - Likewise `64.0.0.0.0.cb.8000.559.2001._ip6.@` would match any “AAAA” RRset in 2001:559:8000:cb::/64
  - Similarly `._ns4.@` and `._ns6.@` to match NS addresses
  - Finally, `._nsn.@` will match NS names
  - There is still (deliberately) no way to match NXDOMAIN

Conclusion

- ISC's role in RPZ is to create a new global capability for the information security market
- ISC's unique capability is to implement this in BIND, making it instantly real and viable
- ISC will not be producing any RPZ data; we will leave that to the security vendor community
- ISC expects our Security Information Exchange (SIE) to be useful to such security vendors
- Questions and comments always welcomed!

More Info

- Email dnsrpz@isc.org
- Look for “dnsrpz-interest” mailing list at lists.isc.org.
- For more background, look for the “Taking Back the DNS” blog article by Paul Vixie.
- Tech note:

  ftp://ftp.isc.org/isc/dnsrpz/isc-tn-2010-1.txt
- Patches
  - ftp://ftp.isc.org/isc/dnsrpz/policy-9.4-ESV-R2.patch
  - ftp://ftp.isc.org/isc/dnsrpz/policy-9.6-ESV-R1.patch
  - ftp://ftp.isc.org/isc/dnsrpz/policy-9.7.1-P2.patch