HITB SECCONF SIN-2021

KEYNOTE 2: Protective DNS – Why It Matters and How to Deploy It With No Cloud Needed

Paul Vixie

CEO, Farsight Security

TRACK 1

HITB SECCONF SIN-2021

Abstract

Many cloud DNS providers including OpenDNS, Heimdal, DNSfilter, CloudFlare, and Quad9 offer DNS filtering whereby questions or answers deemed dangerous are answered dishonestly. This constructive dishonesty is a valuable security feature, and one which the US government recommended universally in an announcement published in March 2021. These are all “cloud” solutions.

Notably, managed private networks who use DNS as a control and monitoring point for cybersecurity can’t or won’t push their DNS service into the cloud. For them, a DNS firewall called RPZ can be used to subscribe to protective DNS filtering policy, and then be deployed locally using any open source DNS server or any DNS appliance. In this presentation, we will cover the motives, methods, and context of on-premise protective DNS.

On DNS

- Since 1986, used for address lookups and a whole lot more.
- ~All Internet activities begin with one or more DNS lookups.
- Like BGP: necessary for the reachability of resources.
- Like NetFlow: sufficient for monitoring access to resources.
- Like The Spice: control DNS, and control the universe.

On Firewalls

- Early Internet was entirely trusted – no hardening needed.
- Firewalls, access control lists, traffic encryption came later.
- do { prototype(); deploy(); set_hair_afire(); } while (true);
- “Just secure your endpoints” will never be good advice.
- Until then, we will restrict and monitor whatever we still can.

On Protective DNS (1)

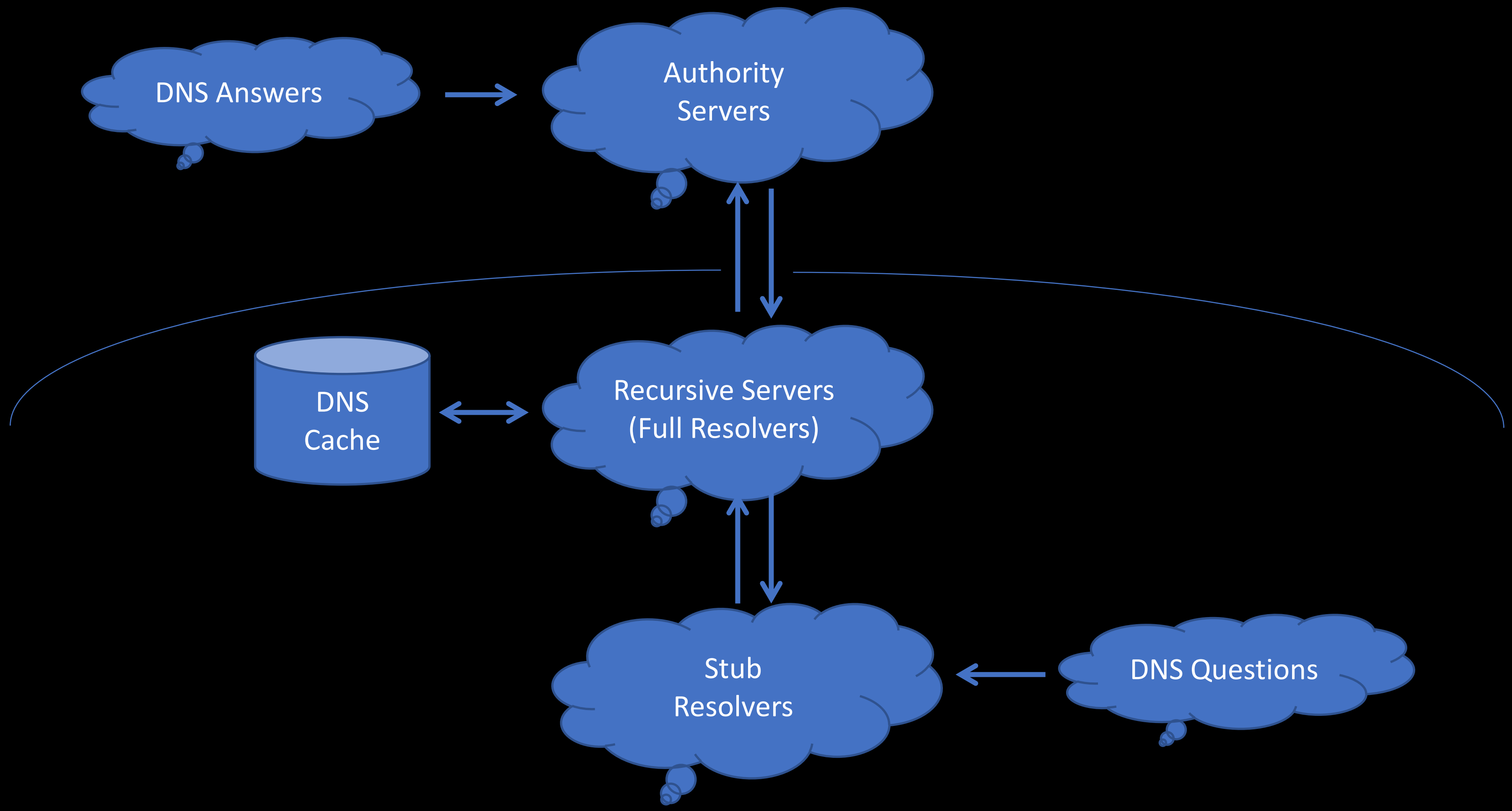
- By monitoring DNS, one can detect infections and bots.
- By filtering DNS, one can prevent (some) infections and block (some) botnet command-and-control data paths.
- Obviously the user and the application and the operating system have to want this or at least cooperate with it.
  - For details, see also 8.8.8.8, DNS over HTTPS, and VPNs.

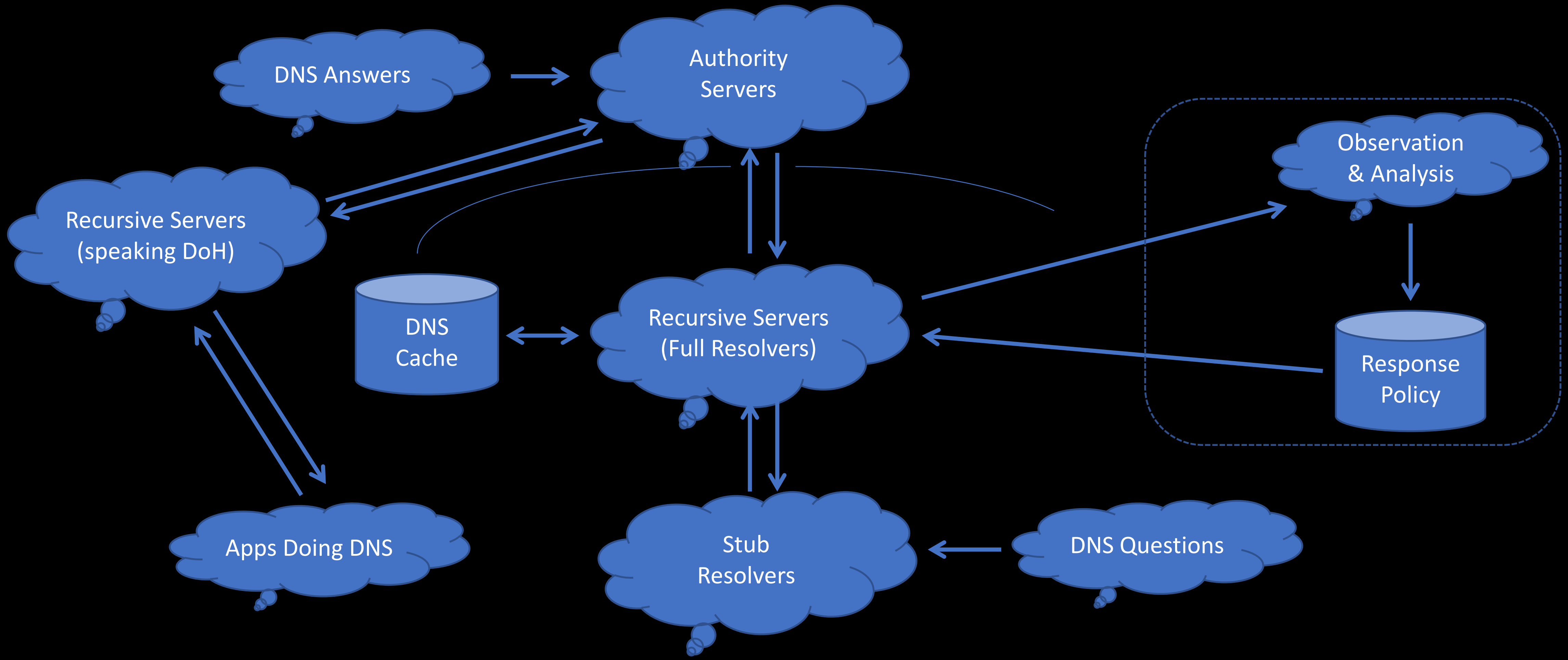
On The Post-Snowden Era

- It’s concerning to see broad bypassery of security controls:
  - DNS over HTTP, Encrypted Client Hello, QUIC (replace TCP w/ UDP)
- Endpoints, applications, kernels, libraries, users: not secure
  - In the old days, Internet = Network of Networks
  - In these new days, Web = Network of Eyeballs
- To secure a network, this new stuff will have to be blocked.

On Protective DNS (2)

- When not bypassed, Protective DNS is a powerful tool.
  - An endpoint is probably malicious by design, or compromised.
  - An application or operating system, likewise.
  - A user may be an intruder, “insider”, or untrained.
- Any monitoring or control of DNS can help security.
- Contrary to the headlines, DNS otherwise works *too well*.


DNS Answers
Authority Servers
DNS Cache
Recursive Servers (Full Resolvers)
Stub Resolvers
DNS Questions


DNS Answers
Authority Servers
Recursive Servers (speaking DoH)
DNS Cache
Recursive Servers (Full Resolvers)
Observation & Analysis
Response Policy
Apps Doing DNS
Stub Resolvers
DNS Questions

On Takedowns

- Takedown at the far end doesn’t work (no cooperation).
- Takedown at the near end doesn’t scale (cost/benefit).
- Protective DNS is “takedown in the middle.”
- The productive side of the economy must self-defend.

On Protective DNS (3)

- Most cloud-based DNS services offer “filtering”.
  - (After DHS/DOD in March 2021, we will call this “Protective DNS.”)
- Many users, families, and companies want this.
- Some, though, don’t trust “the cloud” with their DNS.
- For them, there’s DNS Firewalls, with RPZ.

On DNS Firewalls

- Back when most networks still ran their own DNS servers, it made sense to add monitoring and filtering features there.
- Benefiting from history, we did it with federation and automation, on a publish/subscribe model.
  - Not all DNS server operators can afford their own threat research.
- The DNS Firewall protocols are ‘dnstap’ and ‘dnsrpz’.

On Response Policy Zones (RPZ)

- In 2010, Schryver and Vixie (ISC) prototyped RPZ in BIND9.
- In the years since then, RPZ has grown and matured.
- Now present in Unbound, Knot, PowerDNS, and BIND9.
- Not an IETF effort; an RFC draft exists, revised periodically.
- All DNS appliances have adopted RPZ.

Implications of DNS RPZ

- Any DNS server operator can surf the available RPZ feeds.
- Subscriptions are controlled with TSIG; most aren’t free.
- Updates to an RPZ stream automatically in real time.
- Any threat research team can their publish results via RPZ.
- This should enable a services market of unconstrained size.

Example of a DNS RPZ

- At $dayjob, we publish some RPZs we call “newly observed”.
  - $new might be 10m, 30m, 60m, …, 24h.
- Breaking name resolution for too-fresh domains works.
- We have a lot more ideas to bring to this market.
- So do a lot of other security publishers.
- None of this is patented or otherwise controlled.

Current Events in DNS RPZ

- The ioc2rpz project is vastly expanding available content.
- $dayjob has announced a fork of the PiHole project for RPZ.
- ThreatSTOP has “personal DNS” (RPZ for Windows.)
- Expect massive growth among “runs their own DNS server”.
- Q&A immediately following this talk – detailed demo.

Resources

- https://dnsrpz.info/
  - RPZ specification, history, implementations, catalogue.
- https://dnstap.info/
  - DNS monitoring middleware, of which, not much said today.
- https://labs.fsi.io/
  - $dayjob’s PiHole fork for RPZ, and other free stuff.
- https://youtu.be/aF99kI5x1e8
  - video giving a tech demo of the concepts described today.

HITB SECCONF SIN-2021

Thank You for Joining Us

Join our Discord channel to discuss more or ask questions

https://discord.gg/dXE8ZMvU9J