

# Protective DNS – Why It Matters, How to Deploy It On-prem, and to Take Control and Defense back

Dr. Paul Vixie, CEO

Boris Taratine, Principal Architect

FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions

<https://www.first.org/events/symposium/africa-arab-regions2021/>

December 7-9, 2021

# Speakers



Dr. Paul Vixie is an internet pioneer, founder of award-winning Farsight Security, Inc. Dr. Vixie was inducted into the internet Hall of Fame in 2014 for work related to DNS and anti-spam technologies. He is the author of open source internet software including BIND 8, and of many internet standards documents concerning DNS and DNSSEC. In addition, he founded the first anti-spam company (MAPS, 1996), the first non-profit internet infrastructure company (ISC, 1994), and the first neutral and commercial internet exchange (PAIX, 1991). In 2018, he cofounded SIE Europe UG, a European data sharing collective to fight cybercrime. Dr. Vixie earned his Ph.D. from Keio University for work related to DNS and DNSSEC in 2010. Dr. Vixie is frequently invited to deliver keynotes at technology and business events around the world. He has presented at such events as Copenhagen Cybercrime Conference, FIRST, Palo Alto Networks IGNITE, RSA, Black Hat, DNS-OARC, SANS, Swiss Cyber Storm, and VirusBulletin.



Boris Taratine is a passionate visionary and an influential ambassador of cyber security and cyber defence. He is an active participant in various industry forums influencing global cybersecurity development. Being often at odds with the conventional wisdom he actively promotes industry collaboration to take proactive actions for improvements and collective defence. He was honoured to judge at the Atlantic Council's Cyber 9/12 UK Strategy Challenge competition since inception. As a trusted adviser to the C-suite, he has helped global businesses understand the importance of cyber disciplines and take proactive actions for improvements. Boris graduated with the highest honour at the Saint-Petersburg State University, where he also continued his Ph.D. studies in Physics. He is an author of a number of scientific publications and dozens of patents granted and pending.

# 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. However, the USG recommendation only mentioned “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.
- Designed as highly distributed system for reliability.
- Fundamental: ~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 BGP) 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 (101) - What is it?

- Protective DNS (often referred to as PDNS) is an umbrella term for security solutions that examine DNS queries by analysing destination IP addresses and domain names against a variety of pre-defined policies and implement safeguards to prevent access to malicious content.

# 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 must 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

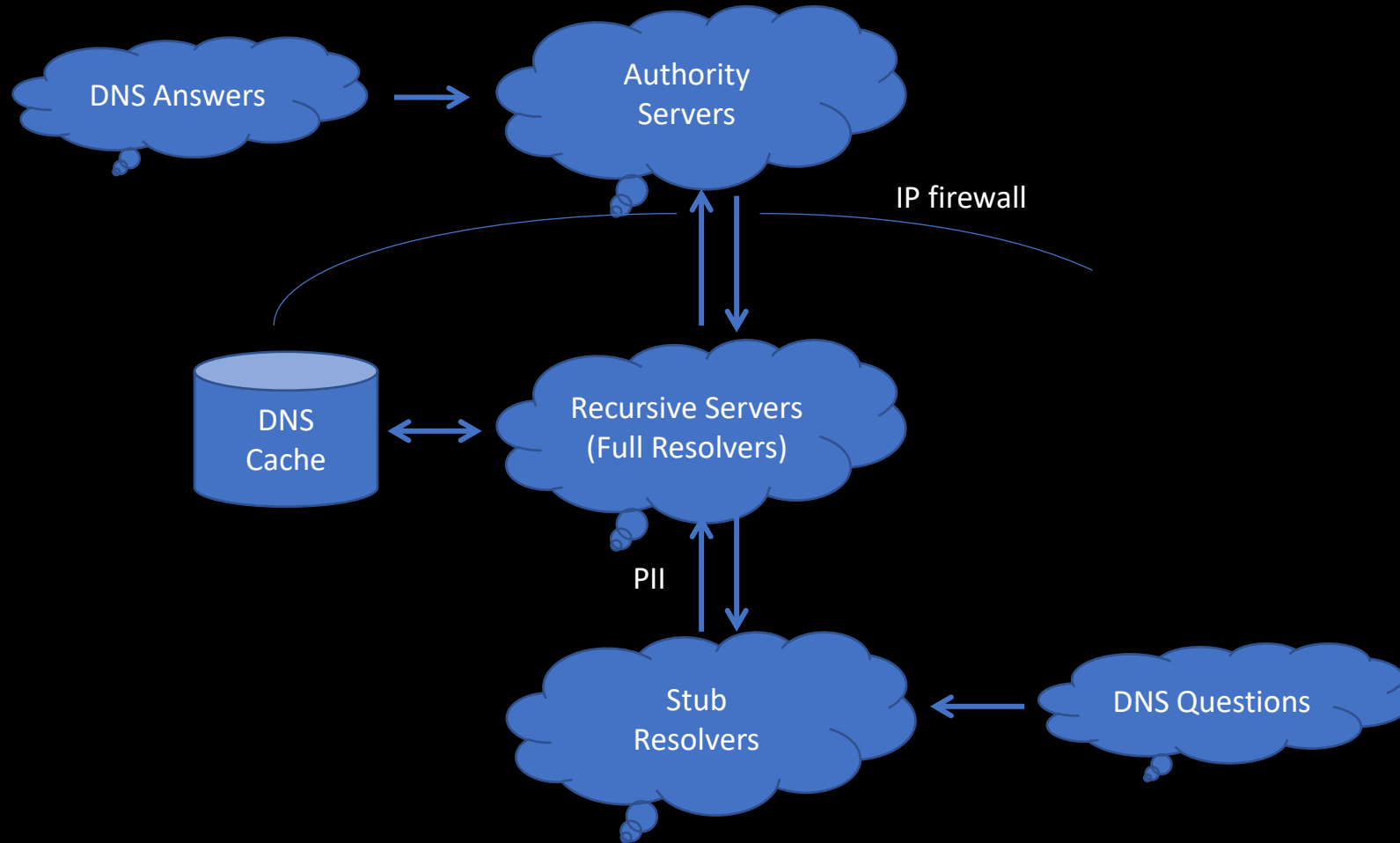
- It's concerning to see broad bypassery of security controls:
  - DNS over HTTP, Encrypted Client Hello, QUIC (replace TCP w/ UDP)
- Endpoints, applications, kernels, libraries, users: not secure.
  - In the old days, Internet = Network of Networks
  - In these new days, Web = Network of Eyeballs
-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



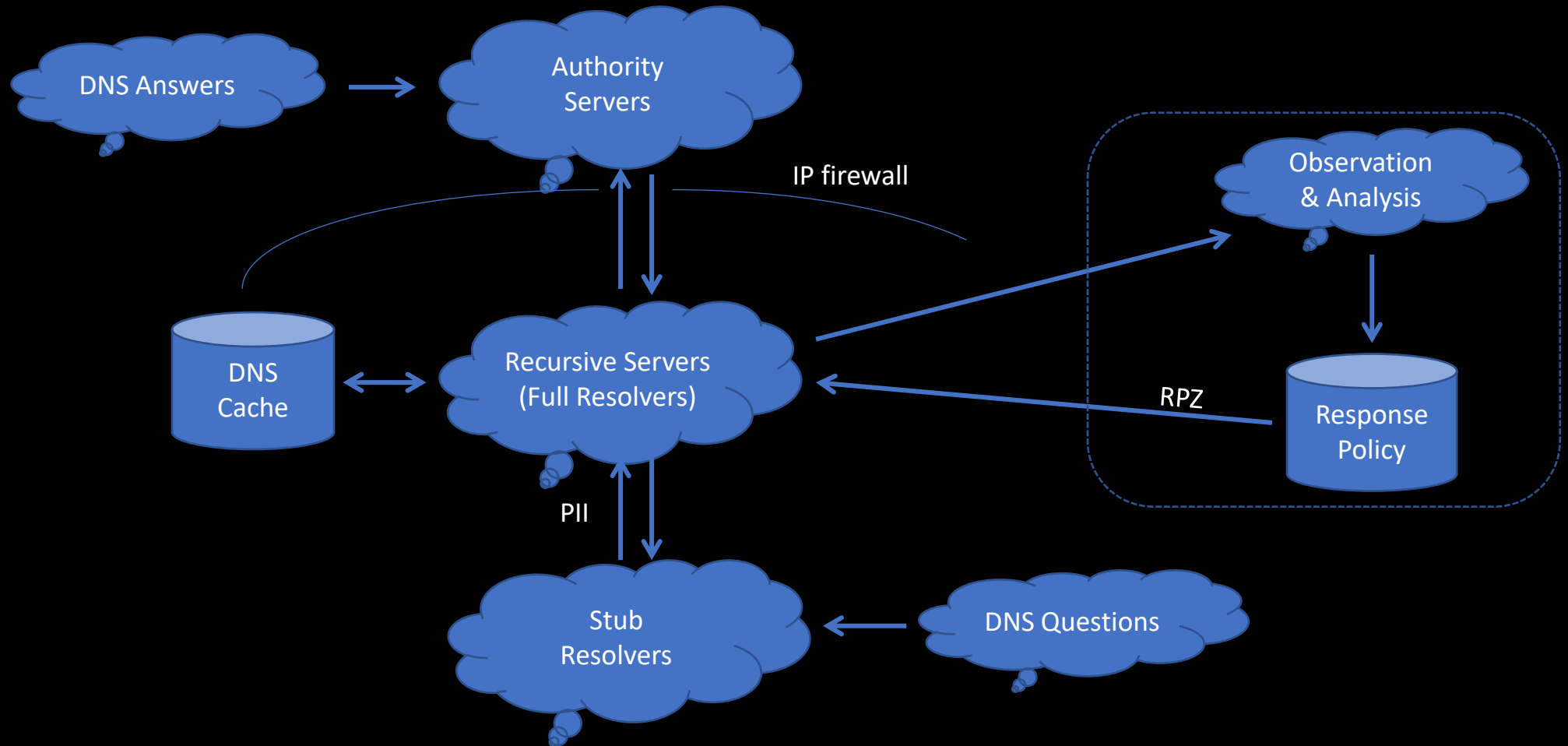
# On Protective DNS (2)

- 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 – you can not tell them apart.
- Any monitoring or control of DNS can help security.
- Contrary to the headlines, DNS otherwise works too well.

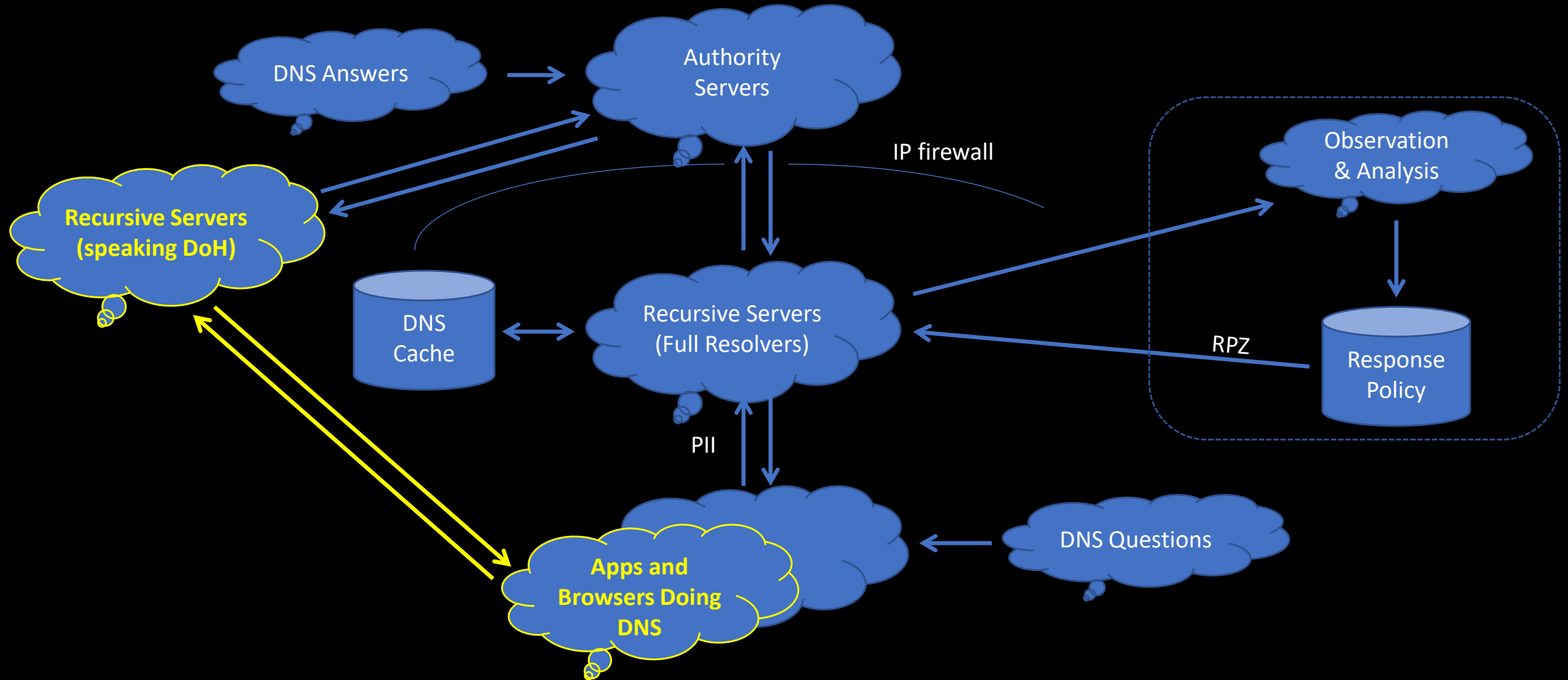
# You Have Control



# You Now Have Control and Protection



# And Now You Do Not...



# On Takedowns

- Takedown at the far end doesn't work (lack of cooperation / takes time).
- Takedown at the near end doesn't scale (unfavorable cost/benefit).
- The productive side of the economy must self-defend.
- Protective DNS is “takedown in the middle”
  - Effective real-time centralized (self)defense of cooperating parties at low cost

# On Protective DNS (3)

- Most cloud-based DNS services offer “filtering”.
  - After DHS/DOD in March 2021 in US we will call this “Protective DNS”
  - In UK “Protective DNS” is used by NCSC since August 2017 but “PDNS is not currently available to the private sector”
- Many users, families, and companies want and need this.
- Some, though, don’t trust “the cloud” with their DNS.
- For them, there’re 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 'dnssrpz'.

# 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.
- RPZ is the heart of Protective DNS – invented by us!



# 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 publish their 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 & AdGuard projects 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.

# A DNS Firewall with RPZ on... Raspberry Pi 😊

RpiDNS powered by [ioc2rpz.net](https://ioc2rpz.net)

Dashboard Query log RPZ hits Admin

Assets RPZ Feeds Block Allow Settings Tools

Feed	Feed action	Description	Actions
wl.ioc2rpz.local	PASSTHRU log no	local whitelist	🔄
wl-ip.ioc2rpz.local	PASSTHRU log no	local whitelist ip-based	🔄
bl.ioc2rpz.local	NXDOMAIN	local blacklist	🔄
bl-ip.ioc2rpz.local	NXDOMAIN	local blacklist ip-based	🔄
24h.rpz.dns-nod.net	GIVEN	FSI NOD 24h.rpz.dns-nod.net policy	🔄
blocklist-malicious.ioc2rpz	NXDOMAIN	Malicious domains powered by The Block List Project ( <a href="https://github.com/blocklistproject/Lists">https://github.com/blocklistproject/Lists</a> ).The feed is based on: fraud, malware, phishing, ransomware, scam lists. False positives can be r>	🔄
bogons-ipv4.ioc2rpz	NXDOMAIN	Bogon IPv4 prefixes by Team Cymru ( <a href="https://www.team-cymru.com/bogon-reference.html">https://www.team-cymru.com/bogon-reference.html</a> ). A bogon prefix is a route that should never appear in the Internet routing table. The RPZ feed includes IP space th>	🔄
covid19.ioc2rpz	NXDOMAIN	Covid-19 malicious domains powered by Covid-19 Cyber Threat Coalition ( <a href="https://www.cyberthreatcoalition.org">https://www.cyberthreatcoalition.org</a> ) blacklist. To report false positives currently listed in the blacklist, please send an email to>	🔄
dga-360.ioc2rpz	NXDOMAIN	DGA feed powered by Netlab 360 ( <a href="http://data.netlab.360.com/dga/">http://data.netlab.360.com/dga/</a> ). It contains domains generated by malware: bamital, banjori, blackhole, ccleaner, chinad, conficker, cryptolocker, dircrypt, dyre, emotet, >	🔄
doh.ioc2rpz	NXDOMAIN	The feed contains publicly available DNS over HTTPs (DoH) servers and canary domains ( <a href="https://raw.githubusercontent.com/DNSCrypt/dnscrypt-resolvers/master/v2/public-resolvers.md">https://raw.githubusercontent.com/DNSCrypt/dnscrypt-resolvers/master/v2/public-resolvers.md</a> ). It is very important when yo>	🔄
local.ioc2rpz	NXDOMAIN	Block local, non Internet routable networks and domains (e.g. RFE-1918) to protect against DNS rebinding attack.	🔄
malicious.ioc2rpz	NXDOMAIN	A single feed with malicious domains which superseeds the following feeds: phishing, rescure-domains, blocklist-malicious, covid19.	🔄
notracking-dead.ioc2rpz	NXDOMAIN	No more ads, tracking and other virtual garbage ( <a href="https://github.com/notracking/hosts-blocklists">https://github.com/notracking/hosts-blocklists</a> ). These domains/hosts doesn't have A, AAAA, CNAME, NS records or/and not registers and considered as dead.	🔄
notracking.ioc2rpz	NXDOMAIN	No more ads, tracking and other virtual garbage ( <a href="https://github.com/notracking/hosts-blocklists">https://github.com/notracking/hosts-blocklists</a> ).	🔄
phishtank.ioc2rpz	NXDOMAIN	PhishTank is a free community site where anyone can submit, verify, track and share phishing data. The source contains only phishing domains/hosts and IPs. ( <a href="https://www.phishtank.com">https://www.phishtank.com</a> ).	🔄
rescure-domains.ioc2rpz	NXDOMAIN	Curated list of malicious domains powered by Fruxlabs Crack Team ( <a href="https://rescure.me">https://rescure.me</a> )	🔄
urlhaus.ioc2rpz	NXDOMAIN	URLhaus is a project operated by abuse.ch ( <a href="https://urlhaus.abuse.ch">https://urlhaus.abuse.ch</a> ). The purpose of the project is to collect, track and share malware URLs, helping network administrators and security analysts to protect their network and customers from cyber threats. urlhaus.ioc2rpz feed contains only malicious domains.	🔄

Farsight Security's Newly Observed Domains real time RPZ

- Protective DNS as a “takedown in the middle” with millions of “rules” – can your corporate firewall handle that?
- Effective real-time centralized (self)defense of cooperating parties at low cost.

# ...Keeps Perpetrators at Bay

Get your Digital Coronavirus Passports (HPS) today

NC

NHS Certificate <kayleigh.dutton@conceptresourcing.com>

Tue 2021-09-14 08:25

To: You



Dear Sir/Madam,

Starting today you can apply for a Digital Passport.

The Coronavirus Digital Passport is documentation proving that you have been vaccinated against COVID-19 or you recently recovered from COVID-19. The passport will allow you to travel safely and freely around the world without having to self-isolate.

### Who is eligible?

UK citizens and their families, and legal residents.

### How do I get the certificate?

You can get your Digital Passport via NHS portal by clicking the button below:

Get Digital Passport

### How does it work?

Each issuing body has been allocated a digital signature, which is embedded in the QR code; border staff will scan the QR code to see the data, although no personal data will be seen -- nor will personal data of the holder go through the gateway which nations are using to verify signatures.

```
[21/09/14 09:08:56 BST +0100]
tarat@SPECTRE ~
$ dig nhsappcerts.co.uk @ my home recursive DNS with RPZ

;<<>> DiG 9.11.9 <<>> nhsappcerts.co.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 16644
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 4463305f970b68fe010000006140589d99bffb200df2c281 (good)
;; QUESTION SECTION:
;; nhsappcerts.co.uk.                IN      A

;; ADDITIONAL SECTION:
24h.rpz.dns-nod.net. 1 IN SOA  a.rpz-ns.dns-nod.net. nod-admin.fsi.io. 1631606927 600 300 86400 300

;; Query time: 14 msec
;; SERVER: 192.168.8.1#53(192.168.8.1)
;; WHEN: Tue Sep 14 09:09:01 BST 2021
;; MSG SIZE rcvd: 165

[21/09/14 09:09:01 BST +0100]
tarat@SPECTRE ~
$ dig nhsappcerts.co.uk @ Open Public DNS

;<<>> DiG 9.11.9 <<>> nhsappcerts.co.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51085
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;; nhsappcerts.co.uk.                IN      A

;; ANSWER SECTION:
nhsappcerts.co.uk. 13639 IN A    198.187.31.159

;; Query time: 10 msec
;; SERVER: Open Public DNS
;; WHEN: Tue Sep 14 09:09:08 BST 2021
;; MSG SIZE rcvd: 62

[21/09/14 09:09:08 BST +0100]
tarat@SPECTRE ~
$
```

- Phish email received
- But RPZ already defends providing NXDOMAIN response to DNS query
- Other DNSs provide resolution to reach the malicious site

# Resources

- <https://dnsrcpz.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/AdGuard/ioc2rpz for RPZ, and other free stuff.
- <https://youtu.be/aF99kl5x1e8>
  - video giving a tech demo of the concepts described today.