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 have control over your domain's DNS infrastructure. This includes:

- **DNS Answers**: These servers provide the final answers to DNS queries.
- **Authority Servers**: These servers are responsible for managing the DNS records of your domain.
- **Recursive Servers** (Full Resolvers): These servers handle DNS queries for other domains.
- **Stub Resolvers**: These servers are typically configured to query the recursive servers.
- **DNS Cache**: This is a temporary storage for DNS queries and responses.
- **PII**: Personal Information (usually not directly related to DNS but important in security context).
- **DNS Questions**: These are the initial requests for information from the DNS system.
You Now Have Control and Protection
And Now You **Do Not...**

- **Recursive Servers (speaking DoH)**
- **DNS Cache**
- **Authority Servers**
  - DNS Questions
  - DNS Answers
  - Recursive Servers
    - (Full Resolvers)
  - PII
  - Apps and Browsers Doing DNS

- IP firewall
- Observation & Analysis
- Response Policy
- RPZ
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 ‘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.

• 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 $\text{dayjob}$, we publish some RPZs we call “newly observed”.
  - $\text{new}$ 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.
• 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

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.

Open Public DNS

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

- [https://dnsrpz.info/](https://dnsrpz.info/)
  - RPZ specification, history, implementations, catalogue.

- [https://dnstap.info/](https://dnstap.info/)
  - DNS monitoring middleware, of which, not much said today.

- [https://labs.fsi.io/](https://labs.fsi.io/)
  - $dayjob’s PiHole/AdGuard/ioc2rpz for RPZ, and other free stuff.

- [https://youtu.be/aF99kI5x1e8](https://youtu.be/aF99kI5x1e8)
  - video giving a tech demo of the concepts described today.