Deploying Hyperlocal

Paul Muchene
Office of the CTO (OCTO)

RIPE NCC DNS Workshop

18 November 2020

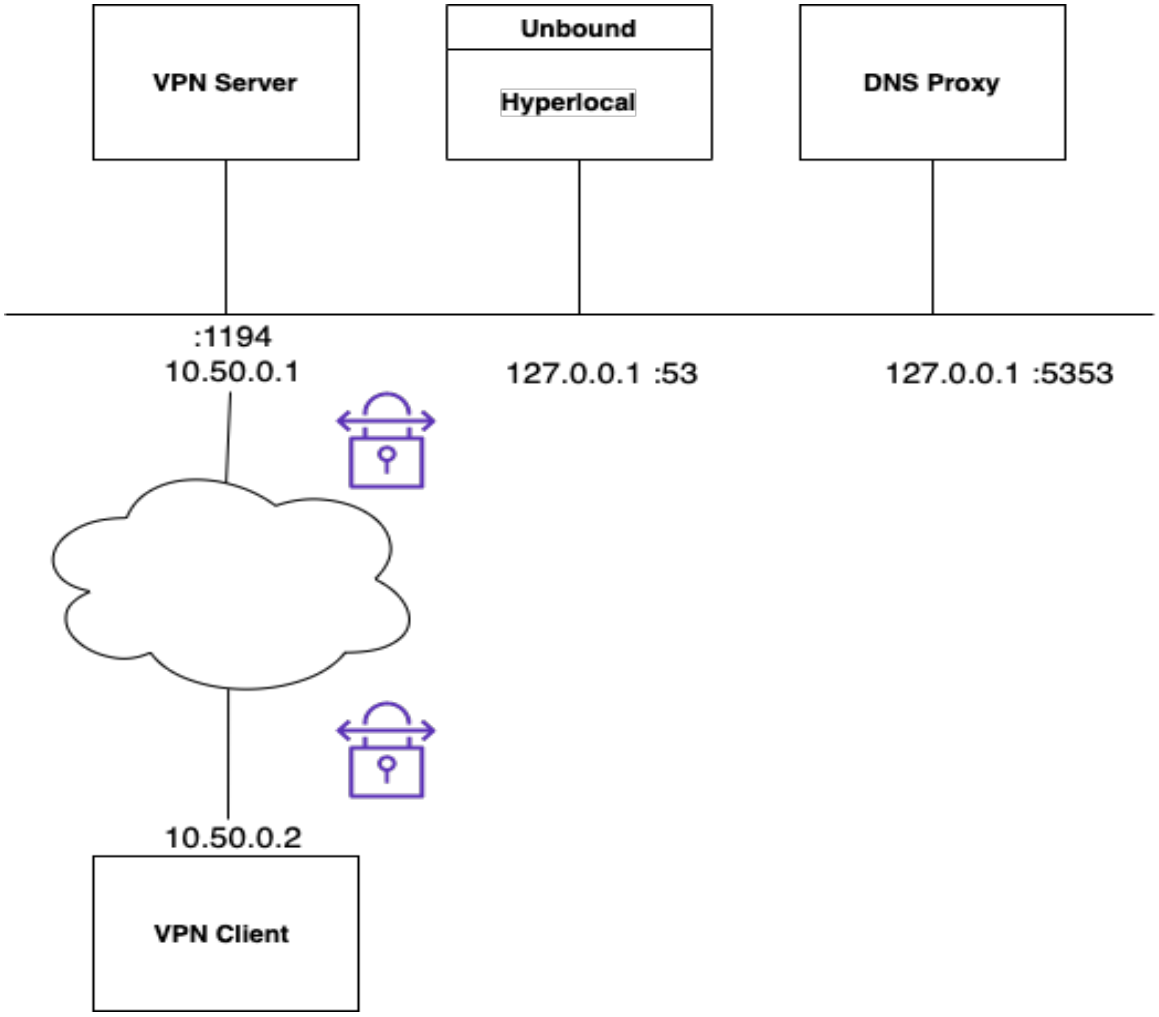
RFC 8806

- Serve a copy of the root zone locally
- Run on same server as the recursive resolver
- Respond only to queries from the same host
- Local authoritative root zone data must be identical to DNS root
- Retrieve a copy of root zone (AXFR) from root operators:
  - b.root-servers.net
  - c.root-servers.net
  - d.root-servers.net
  - f.root-servers.net
  - g.root-servers.net
  - k.root-servers.net

Practical Hyperlocal Application

- Run a custom VPN Server in the Cloud
- VPN Server – Wireguard 1.02
- Unbound >= 1.8 (Acts as both a resolver and a recursive resolver)
- DNS Proxy – Choice of either DoH or DNSCrypt
- VM Server Specs:
  - Single core processor
  - 500 mb RAM
  - 20 GB SSD
  - FreeBSD 12.1 (Comes with shipped with Unbound 1.10)

VPN Setup


VPN Server
Unbound
Hyperlocal
DNS Proxy
:1194
10.50.0.1
127.0.0.1 :53
127.0.0.1 :5353
10.50.0.2
VPN Client

Unbound Configuration Settings

- Added the following lines to unbound.conf (see RFC 8806 Appendix B2):

```
auth-zone:
        name: "."
        master: "b.root-servers.net"
        master: "c.root-servers.net"
        master: "d.root-servers.net"
        master: "f.root-servers.net"
        master: "g.root-servers.net"
        master: "k.root-servers.net"
        fallback-enabled: yes
        for-downstream: no
        for-upstream: yes
        zonefile: "root.zone"
```

- For Validation of DNSSEC data for trust-anchored zones:

```
        harden-dnssec-stripped: yes
```

Dig Test: Query Root Zone

- **dig @127.0.0.1 . NS**
  - Query time: 0 ms
  - No AA flags

```
root@free-vpn:~ # dig @127.0.0.1 . NS

; <<>> DiG 9.16.8 <<>> @127.0.0.1 . NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22303
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518078  IN      NS      a.root-servers.net.
.                       518078  IN      NS      b.root-servers.net.
.                       518078  IN      NS      c.root-servers.net.
.                       518078  IN      NS      d.root-servers.net.
.                       518078  IN      NS      e.root-servers.net.
.                       518078  IN      NS      f.root-servers.net.
.                       518078  IN      NS      g.root-servers.net.
.                       518078  IN      NS      h.root-servers.net.
.                       518078  IN      NS      i.root-servers.net.
.                       518078  IN      NS      j.root-servers.net.
.                       518078  IN      NS      k.root-servers.net.
.                       518078  IN      NS      l.root-servers.net.
.                       518078  IN      NS      m.root-servers.net.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Nov 17 13:08:46 UTC 2020
;; MSG SIZE  rcvd: 239

root@free-vpn:~ #
```

Dig Test: Query NXDOMAIN

- **dig @127.0.0.1 xyz.abcdefg NS**
  - Query time: 0 ms

```
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Nov 17 13:25:25 UTC 2020
;; MSG SIZE  rcvd: 115
```

- **dig @8.8.8.8 xyz.abcdefg NS**
  - Query time: 13 ms

```
;; Query time: 13 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Nov 17 13:25:43 UTC 2020
;; MSG SIZE  rcvd: 115
```

- **dig @9.9.9.9 xyz.abcdefg NS**
  - Query time: 9 ms

```
;; Query time: 9 msec
;; SERVER: 9.9.9.9#53(9.9.9.9)
;; WHEN: Tue Nov 17 13:27:44 UTC 2020
;; MSG SIZE  rcvd: 115
```

Dig Test: Query TLDs

- **dig @127.0.0.1 rocks NS**
  - Query time: 20 ms
- **dig @8.8.8.8 rocks NS**
  - Query time: 10 ms
- **dig @9.9.9.9 rocks NS**
  - Query time: 20 ms

```
root@free-vpn:~ # dig @127.0.0.1 rocks ns

; <<>> DiG 9.16.8 <<>> @127.0.0.1 rocks ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21050
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;rocks.                         IN      NS

;; ANSWER SECTION:
rocks.                  86400   IN      NS      demand.delta.aridns.net.au.
rocks.                  86400   IN      NS      demand.gamma.aridns.net.au.
rocks.                  86400   IN      NS      demand.beta.aridns.net.au.
rocks.                  86400   IN      NS      demand.alpha.aridns.net.au.

;; Query time: 20 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Nov 17 14:09:18 UTC 2020
;; MSG SIZE  rcvd: 154
```

Why the Marginal Performance for TLDs?

- Hyperlocal serves only the root zone and not other TLD zones
- Unbound recursively queries name servers to obtain RR

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on xn0, link-type EN10MB (Ethernet), capture size 262144 bytes
IP 172.26.6.3.56786 > 37.209.196.7.53: 55571% [1au] NS? rocks. (34)
IP 37.209.196.7.53 > 172.26.6.3.56786: 55571*- 5/0/1 NS demand.delta.aridns.net.au., NS demand.alpha.aridns.net.au., NS demand.beta.aridns.net.au
., NS demand.gamma.aridns.net.au., RRSIG (390)
IP 172.26.6.3.52351 > 37.209.198.7.53: 30670% [1au] DNSKEY? rocks. (34)
IP 37.209.198.7.53 > 172.26.6.3.52351: 30670*- 4/0/1 DNSKEY, DNSKEY, RRSIG, RRSIG (980)
IP 172.26.6.3.9415 > 37.209.198.7.53: 59608% [1au] DNSKEY? rocks. (34)
IP 37.209.198.7.53 > 172.26.6.3.9415: 59608*- 4/0/1 DNSKEY, DNSKEY, RRSIG, RRSIG (980)
```

- Popular Open recursors aggressively cache TLD DNS records

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**


@icann


linkedin/company/icann


facebook.com/icannorg


slideshare/icannpresentations

youtube.com/icannnews


soundcloud/icann


flickr.com/icann


instagram.com/icannorg