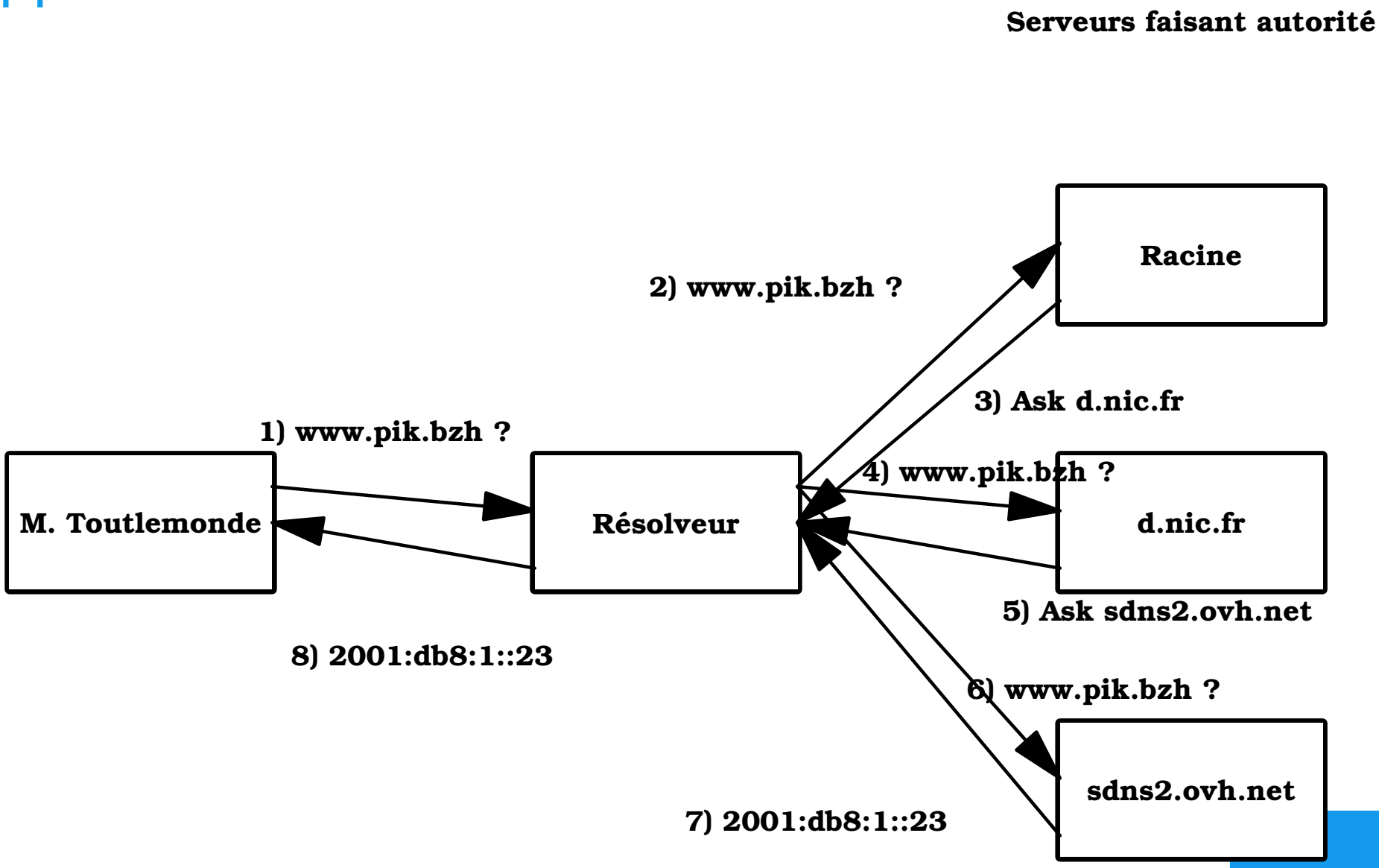
Un résolveur DoT/DoH public, leçons et expériences (1/21)

Stéphane Bortzmeyer
bortzmeyer@nic.fr

Rappel DNS


Serveurs faisant autorité
Racine
2) www.pik.bzh ?
3) Ask d.nic.fr
1) www.pik.bzh ?
4) www.pik.bzh ?
M. Toutlemonde
Résolveur
d.nic.fr
5) Ask sdns2.ovh.net
8) 2001:db8:1::23
6) www.pik.bzh ?
sdns2.ovh.net
7) 2001:db8:1::23

DNS, confiance et vie privée

DNS, confiance et vie privée

- Problème : risques de surveillance « Il a résolu `www.alcooliques-anonymes.fr` »

DNS, confiance et vie privée

- Problème : risques de surveillance
- Solution : chiffrement

DNS, confiance et vie privée

- Problème : risques de surveillance
- Solution : chiffrement
- Problème : résolveur menteur « `sci-hub.se` n'existe pas »

DNS, confiance et vie privée

- Problème : risques de surveillance
- Solution : chiffrement
- Problème : résolveur menteur
- Solution : utiliser un bon résolveur (protège aussi de la surveillance par le résolveur)

afnic

DNS, confiance et vie privée

- Problème : risques de surveillance
- Solution : chiffrement
- Problème : résolveur menteur
- Solution : utiliser un bon résolveur
- Problème : trafic DNS détourné / bloqué

DNS, confiance et vie privée

- Problème : risques de surveillance
- Solution : chiffrement
- Problème : résolveur menteur
- Solution : utiliser un bon résolveur
- Problème : trafic DNS détourné / bloqué
- Solution : authentification du résolveur

DNS, confiance et vie privée

- Problème : risques de surveillance
- Solution : chiffrement
- Problème : résolveur menteur
- Solution : utiliser un bon résolveur
- Problème : trafic DNS détourné / bloqué
- Solution : authentification du résolveur
- RFC 7626 pour l'analyse détaillée

DNS sur TLS

DNS sur TLS

- Le DNS est le seul protocole important en clair

DNS sur TLS

- Le DNS est le seul protocole important en clair
- Solution évidente : cryptographie

DNS sur TLS

- Le DNS est le seul protocole important en clair
- Solution évidente : cryptographie
- Tout le monde adore TLS

DNS sur TLS

- Le DNS est le seul protocole important en clair
- Solution évidente : cryptographie
- Tout le monde adore TLS
- RFC 7858 : DoT (*DNS over TLS*)

DNS sur TLS

- Le DNS est le seul protocole important en clair
- Solution évidente : cryptographie
- Tout le monde adore TLS
- RFC 7858 : DoT (*DNS over TLS*)
- Port 853

DNS sur HTTPS

DNS sur HTTPS

- DoT peut être bloqué trivialement (blocage explicite ou implicite « uniquement 80 et 443 »)

DNS sur HTTPS

- DoT peut être bloqué trivialement
- Comme toujours en sécurité, la lutte de l'épée et de la cuirasse est permanente

DNS sur HTTPS

- DoT peut être bloqué trivialement
- Comme toujours en sécurité, la lutte de l'épée et de la cuirasse est permanente
- Tout le monde adore HTTPS, et il passe partout

DNS sur HTTPS

- DoT peut être bloqué trivialement
- Comme toujours en sécurité, la lutte de l'épée et de la cuirasse est permanente
- Tout le monde adore HTTPS, et il passe partout
- RFC 8484 : DoH (*DNS over HTTPS*)

Applicabilité

Applicabilité

- DoT et DoH, pour l'instant, sécurisent le lien entre le client final et le résolveur

Applicabilité

- DoT et DoH, pour l'instant, sécurisent le lien entre le client final et le résolveur
- Utilisations typiques : via un relais du système d'exploitation (systemd, stubby) ou directement depuis l'application (Firefox, Chrome)

Applicabilité

- DoT et DoH, pour l'instant, sécurisent le lien entre le client final et le résolveur
- Utilisations typiques : via un relais du système d'exploitation (systemd, stubby) ou directement depuis l'application (Firefox, Chrome)
- Nombreux résolveurs publics mais surtout GAFA

Tests DoT et DoH

```
% kdig +tls @dns.shaftinc.fr AAAA www.afnic.fr
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(ECDSA-SECP384R1-SHA384)-\
                        (CHACHA20-POLY1305)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 42827
...
;; ANSWER SECTION:
www.afnic.fr.        600 IN AAAA 2a00:e00:0:5::2
...
;; Received 75 B
;; From 2001:bc8:2c86:853::853@853(TCP) in 21.4 ms

% kdig +https=/ @dns.shaftinc.fr AAAA réussir-en.fr
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(ECDSA-SECP384R1-SHA384)-\
                        (CHACHA20-POLY1305)
;; HTTP session (HTTP/2-POST)-([2001:bc8:2c86:853::853]/)-(status: 200)
...
;; ANSWER SECTION:
réussir-en.fr.      1000 IN AAAA 2001:41d0:305:2100::6cfb
...
;; Received 77 B
;; From 2001:bc8:2c86:853::853@443(TCP) in 19.8 ms
```

Le projet

Le projet

- Un résolveur DoT/DoH public (pas de DNS sur UDP)

Le projet

- Un résolveur DoT/DoH public
- Projet personnel, expérimental

Le projet

- Un résolveur DoT/DoH public
- Projet personnel, expérimental
- `dot.bortzmeyer.fr` et `https://doh.bortzmeyer.fr/`

afnic

Le projet

- Un résolveur DoT/DoH public
- Projet personnel, expérimental
- `dot.bortzmeyer.fr` et `https://doh.bortzmeyer.fr/`
- Lancement en septembre 2019

afnic

La politique

La politique

- https://doh.bortzmeyer.fr/policy

La politique

- `https://doh.bortzmeyer.fr/policy`
- Principes :
  - Pas de garantie
  - Accepte tout le monde
  - Authentifiable
  - Pas de mensonge, même pour la bonne cause
  - Pas de journalisation des requêtes
  - *QNAME minimisation*
  - Pas d'ECS

La politique

- `https://doh.bortzmeyer.fr/policy`
- Principes :
  - Pas de garantie
  - Accepte tout le monde
  - Authentifiable
  - Pas de mensonge, même pour la bonne cause
  - Pas de journalisation des requêtes
  - *QNAME minimisation*
  - Pas d'ECS
- RFC 8932, la lecture recommandée sur les politiques des résolveurs (RPS pour *Recursive operator Privacy Statement*)

Autres politiques

Autres politiques

- Mozilla TRR `https://wiki.mozilla.org/Security/DOH-resolver-policy`

Autres politiques

- Mozilla TRR `https://wiki.mozilla.org/Security/DOH-resolver-policy`
- Quad9 `https://quad9.net/service/privacy/`

Autres politiques

- Mozilla TRR `https://wiki.mozilla.org/Security/DOH-resolver-policy`
- Quad9 `https://quad9.net/service/privacy/`
- Cloudflare `https://developers.cloudflare.com/1.1.1.1/privacy/public-dns-resolver`

Autres politiques

- Mozilla TRR `https://wiki.mozilla.org/Security/DOH-resolver-policy`
- Quad9 `https://quad9.net/service/privacy/`
- Cloudflare `https://developers.cloudflare.com/1.1.1.1/privacy/public-dns-resolver`
- Shaft `https://www.shaftinc.fr/dns-shaftinc.html`

La technique

La technique

- Frontal dnsdist, pour DoT et DoH `https://dnsdist.org/`

La technique

- Frontal dnsdist, pour DoT et DoH `https://dnsdist.org/`
- Unbound en dorsal

La technique

- Frontal dnsdist, pour DoT et DoH `https://dnsdist.org/`
- Unbound en dorsal
- Authentifiable SPKI, PKIX, DANE

La technique

- Frontal dnsdist, pour DoT et DoH `https://dnsdist.org/`
- Unbound en dorsal
- Authentifiable SPKI, PKIX, DANE
- Pas d'anycast

La configuration

```
-- DoT
addTLSLocal("[2001:41d0:302:2200::180]:853",
  "/etc/dnsdist/server-dot.pem", "/etc/dnsdist/server-dot.key",
  {minTLSVersion="tls1.2", provider="Gnu TLS",
  ciphers="PFS:-VERS-TLS1.1:-VERS-TLS1.0", maxInFlight=1024})

-- Du calme, les clients
addAction(MaxQPSIPRule(100), DropAction())

-- Le dorsal
newServer({address="127.0.0.1:53", name="Local-Unbound",
          useClientSubnet=false})

-- Pas de journalisation
-- addAction(AllRule(), LogAction("/tmp/dnsdist.log", false, true, fals
-- Idem pour TeeAction et SpoofAction, inutilisés.
```

Oignons

Oignons

- Le résolveur voit l'adresse IP source du client

Oignons

- Le résolveur voit l'adresse IP source du client
- Service également accessible sous forme d'un oignon, `lani4a4fr33kqqjeiy3qubhfx2jewfd3aeaepuwzxrx6zywp2mo4cja` `onion`

Oignons

- Le résolveur voit l'adresse IP source du client
- Service également accessible sous forme d'un oignon, `lani4a4fr33kqqjeiy3qubhfx2jewfd3aeaepuwzxrx6zywp2mo4cja` `onion`
- (Travaux en cours à l'IETF sur l'*oblivious HTTP*)

Oignons

- Le résolveur voit l'adresse IP source du client
- Service également accessible sous forme d'un oignon, `lani4a4fr33kqqjeiy3qubhfx2jewfd3aeaepuwzxrx6zywp2mo4cja onion`
- (Travaux en cours à l'IETF sur l'*oblivious HTTP*)
- Curiosité : également utilisé comme dorsal dnscrypt

Console graphique

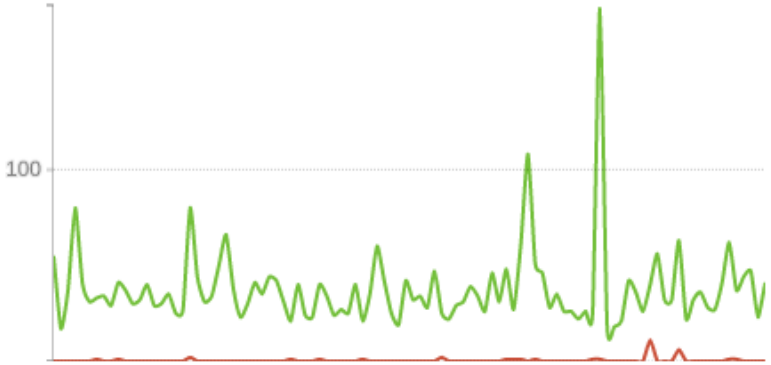
https://doh.bortzmeyer.fr:8083

POWERDNS

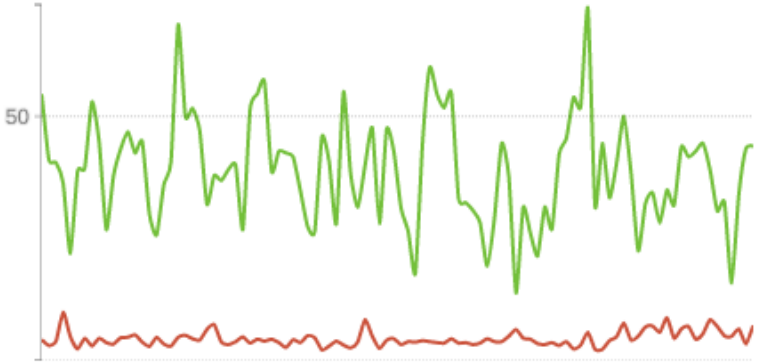
dnsdist 1.6.1
dnsdist comes with ABSOLUTELY NO WARRANTY. This is free software, and you are welcome to redistribute

Uptime: 4 hours, Number of queries: 575941 (41.00 qps), ACL drops: 0, Dynamic drops: 0, Rule drops: 30
Average response time: 64.73 ms, CPU Usage: 7.20%, Cache hitrate: 43.90%, Server selection policy: firstAvailable
Listening on: 0.0.0.0:443, 193.70.85.11:853, [2001:41d0:302:2200::180]:853, [::]:443, ACL: 10.0.0.0/8, 100.64.0.0/10, 127.0.0.0/8, 0.0.0.0/0, 169.2
fc00::/7, fe80::/10

QPS / SERVFAILPS



CACHE HITRATE / CPU %



#	Name	Address	Status	Latency
0	Local-Unbound	127.0.0.1:53	up	112.51
1	OVH	213.186.33.99:53	up	0.00

#	Rule
0	IP (/32, /64) match for QPS over 100 burst 100

#	Response Rule
	No response rul

Dyn blocked netmask	Secon
	No dynamic bloc

Kernel-based dyn blocked netmask
No eBPF block

Console texte

```
> getPool("").getCache():printStats()
Entries: 33026/100000
Hits: 254588
Misses: 322271
Deferred inserts: 13
Deferred lookups: 8
Lookup Collisions: 2
Insert Collisions: 2
TTL Too Shorts: 0

> topQueries(30)
...

> topClients(20)
...
```

API

```
% curl -s -k --header "X-API-Key: XXX" \
     https://doh.bortzmeyer.fr:8083/api/v1/servers/localhost/statistics
   jq .
[
  ...
  {
    "name": "queries",
    "type": "StatisticItem",
    "value": 242640
  },
  {
    "name": "frontend-nxdomain",
    "type": "StatisticItem",
    "value": 23911
  },
  {
    "name": "frontend-servfail",
    "type": "StatisticItem",
    "value": 1722
  },
```

Supervision

Avec Icinga

Host | Service | Services | History

UP
since Oct 13

radia
2001:41d0:302:2200::180
193.70.85.11

OK
since 08:36

Service: **doh6**

Check now | Comment | Notification | Downtime

Plugin Output

```
https://doh.bortzmeyer.fr/ OK - No error for fr.wikipedia.org/AAAA, 102 bytes re-
ceived
```

Avec les sondes RIPE Atlas

```
% blaeu-resolve --displayrtt --tls --nameserver=dot.bortzmeyer.fr \
    --requested=1000   cyberstructure.fr
[2001:4b98:dc0:41:216:3eff:fe27:3d3f] : 706 occurrences \
                Average RTT 1237 ms
[TIMEOUT] : 15 occurrences Average RTT 0 ms
Test #33113690 done at 2021-11-02T10:59:09Z

% blaeu-resolve ... --nameserver=dns.quad9.net ...
[2001:4b98:dc0:41:216:3eff:fe27:3d3f] : 656 occurrences \
               Average RTT 275 ms
[TIMEOUT] : 35 occurrences Average RTT 0 ms
```

Leçons tirées

Leçons tirées

- La fiabilité est cruciale (sans résolveur DNS, plus rien ne marche) : supervision nécessaire

Leçons tirées

- La fiabilité est cruciale : supervision nécessaire
- dnsdist (et Unbound) marche très bien

Leçons tirées

- La fiabilité est cruciale : supervision nécessaire
- dnsdist (et Unbound) marche très bien
- Relativement peu de clients (quelques dizaines de requêtes par seconde)

Leçons tirées

- La fiabilité est cruciale : supervision nécessaire
- dnsdist (et Unbound) marche très bien
- Relativement peu de clients (quelques dizaines de requêtes par seconde)
- Au début, on trouvait encore des bogues (*Query ID* à zéro dans DoH)

Leçons tirées

- La fiabilité est cruciale : supervision nécessaire
- dnsdist (et Unbound) marche très bien
- Relativement peu de clients (quelques dizaines de requêtes par seconde)
- Au début, on trouvait encore des bogues
- Attaques par déni de service (ciblées ?)

afnic

Et demain ?

Et demain ?

- Côté technique, DoQ (*DNS over QUIC*)

Et demain ?

- Côté technique, DoQ (*DNS over QUIC*)
- Mais surtout, meilleure intégration logicielle

afnic

Et demain ?

- Côté technique, DoQ (*DNS over QUIC*)
- Mais surtout, meilleure intégration logicielle
- Côté politique, le projet européen DNS4EU ?

afnic

Et demain ?

- Côté technique, DoQ (*DNS over QUIC*)
- Mais surtout, meilleure intégration logicielle
- Côté politique, le projet européen DNS4EU ?
- Mais surtout, davantage de résolveurs libres et joyeux

afnic

Merci !

www.afnic.fr
contact@afnic.fr

afnic