La politique du serveur DoH doh.bortzmeyer.fr et ce qu'il faut savoir

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 septembre 2019. Dernière mise à jour le 7 novembre 2023

`https://www.bortzmeyer.org/doh-bortzmeyer-fr-policy.html`

Ce texte est la politique suivie par le résolveur <https://www.bortzmeyer.org/resolveur-dns.html> DoH `doh.bortzmeyer.fr` et par le résolveur <https://www.bortzmeyer.org/resolveur-dns.html> DoT `dot.bortzmeyer.fr`. Il explique ce qui est garanti (ou pas), ce qui est journalisé (ou pas), etc. (Vous pouvez également accéder à ce texte par l'URL `https://doh.bortzmeyer.fr/policy` .)

[*"If you don't read French, sorry, no translation is planned. But there are many other DoH resolvers available (or DoT), sometimes with policies in English."* <https://github.com/curl/curl/wiki/DNS-over-HTTPS#publicly-available-servers> <https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Public+Resolvers#DNSPrivacyPublicResolvers-DNS-over-TLS(DoT)>]

— Nouveauté du 7 novembre 2023 : le service DNS-over-QUIC.
— Nouveauté du 28 septembre 2021 : le service `.onion`.
— Nouveauté du 25 octobre 2020 : engagement de couper ECS.
— Nouveauté du 14 août 2020 : mention des statistiques agrégées.

Les protocoles DoH (DNS sur HTTPS), normalisé dans le RFC 8484 [1], et DoT (DNS sur TLS), normalisé dans le RFC 7858, permettent d'avoir un canal sécurisé (confidentialité et intégrité) avec un résolveur DNS qu'on choisit. DoH est mis en œuvre dans plusieurs clients comme Mozilla Firefox. Ce texte n'est pas un mode d'emploi (qui dépend du client) mais une description de la politique suivie. La sécurisation du canal (par la cryptographie) vous protège contre un tiers mais évidemment pas contre le gérant du résolveur DoH ou DoT. C'est pour cela qu'il faut évaluer le résolveur DoH qu'on utilise, juger de la confiance à lui accorder, à la fois sur la base de ses déclarations, et sur la base d'une évaluation du respect effectif de ces déclarations. Cette politique suit à peu près les principes du RFC 8932.

Le résolveur DoH `doh.bortzmeyer.fr` et le résolveur DoT `dot.bortzmeyer.fr` sont gérés par moi. C'est un projet individuel, avec ce que cela implique en bien ou en mal.

Ce résolveur :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8484.txt`

— Est public (au sens du RFC 9499), ce qui veut dire que tout le monde peut l'utiliser,
— Est authentifiable par le nom dans le certificat, ou bien par DANE (RFC 6698) ou encore par l'épinglage de la clé qui vaut, pour le serveur DoT, `eHAFsxc9HJW8QlJB6kDlR0tkTwD97X/TXYc1AzFkTFY=` (en SHA-256/Base64, comme spécifié par le RFC 7858),
— Outre les noms `doh.bortzmeyer.fr` et `dot.bortzmeyer.fr`, le serveur est accessible par les adresses IP `193.70.85.11` et `2001:41d0:302:2200::180`, que j'essaierai de ne pas changer (vous pouvez de toute façon les vérifier <`https://dns.bortzmeyer.org/dot.bortzmeyer.fr/ADDR`> dans le DNS, la zone est signée avec DNSSEC) et est aussi accessible via un service `.onion` (Tor), `lani4a4fr33kqqjeiy3qubhfx2jewfd3aeaepuwzxrx6zywp2mo4cjad.onion`,
— Est également accessible avec DoQ ("*DNS over QUIC*", RFC 9250), via le nom `doq.bortzmeyer.fr`, mais c'est très expérimental et pas garanti,
— N'offre aucune garantie de bon fonctionnement. Il est supervisé mais les ressources humaines et financières disponibles ne permettent pas de s'engager sur sa stabilité. (Mais vous êtes bien sûr encouragé·e·s à signaler tous les problèmes ou limites que vous rencontreriez.)
— Accepte tous les clients gentils, mais avec une limitation de trafic (actuellement cent requêtes par seconde mais cela peut changer sans préavis). Les clients méchants pourraient se retrouver bloqués.
— N'enregistre pas du tout les requêtes DNS reçues. Elles ne sont jamais mises en mémoire stable. Notez que la liste des adresses IP des clients (sauf si vous utilisez Tor), et celle des noms de domaines demandés est gardée en mémoire temporaire, et ne survit donc pas à un redémarrage du logiciel serveur (ou a fortiori de la machine). Les deux listes sont stockées séparément donc je peux voir que `2001:db8:99:fa4::1` a fait une requête, ou que quelqu'un a demandé `toto.example`, mais je ne sais pas si c'est la même requête.
— Et les requêtes complètes ne sont pas copiées vers un autre serveur. (Certaines politiques de serveurs disent « nous ne gardons rien » mais sont muettes sur l'envoi de copies à un tiers.) Notez que, pour faire son travail, le résolveur DoH doit bien transmettre une partie de la requête aux serveurs faisant autorité, mais cette partie est aussi minimisée que possible (RFC 9156), et ECS (RFC 7871) est coupé.
— Des statistiques fortement agrégées (comme « nombre total de requêtes de la semaine » ou bien « les TLD les plus demandés ») pourront être produites et publiées. Elles seront toujours suffisamment agrégées pour qu'il ne soit pas possible de retrouver les requêtes individuelles ou leur origine.
— Le résolveur ne ment pas, il transmet telles quelles les réponses reçues des serveurs faisant autorité. Même des domaines dangereux pour la vie privée comme `google-analytics.com` sont traités de manière neutre.
— Je suis sincère (si, si, faites-moi confiance) mais ce serveur dépend d'autres acteurs. C'est une simple machine virtuelle et l'hébergeur peut techniquement interférer avec son fonctionnement. C'est d'autant plus vrai que la machine est en France et donc soumise à diverses lois liberticides comme la loi Renseignement.

Comme indiqué plus haut, il s'agit d'un projet individuel, donc sa gouvernance est simple : c'est moi qui décide (mais, en cas de changement des règles, je modifierai cet article, et en changeant la date pour que les utilisateurices de la syndication aient la nouvelle version). Si cela ne vous convient pas, je vous suggère de regarder les autres serveurs DoH disponibles <`https://github.com/curl/curl/wiki/DNS-over-HTTPS#publicly-available-servers`> (plus il y en a, mieux c'est). Voyez aussi les serveurs DoT <`https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Public+Resolvers#DNSPrivacyPublicResolvers-DNS-over-TLS(DoT)`>. En français, il existe aussi le serveur public de Shaft <`https://www.shaftinc.fr/dns-shaftinc.html`>, avec une politique et une documentation utilisateur détaillée.

Et si vous êtes technicien·ne, j'ai également publié sur la mise en œuvre de ce résolveur <`https://www.bortzmeyer.org/doh-mon-resolveur.html`>.

`https://www.bortzmeyer.org/doh-bortzmeyer-fr-policy.html`