Compas'2023 : Parallélisme/ Architecture/ Système
LISTIC/USMB - Annecy France, 4-7 juillet 2023

Effets de l'utilisation de transports sécurisés sur les performances d'un resolveur DNS

Etienne Le Louët, Antoine Blin, Julien Sopena, Ahmed Amaou, Kamel Hadadou

Résumé
Des contraintes de performances et de passage à l'échelle ont orienté les choix de conception initiaux de DNS vers l'utilisation de protocoles non chiffrés, le rendant vulnérable à certaines attaques. Des protocoles visant à sécuriser les échanges DNS ont récemment été standardisés, mais la question de leur passage à l'échelle ainsi que de leur soutenabilité reste ouverte. Les travaux présentés dans cet article ont pour but d'étudier le coût de la transition du protocole DNS historique à ceux plus récents, en étudiant le surcoût associé à chaque protocole. En comparant différents transports DNS, nous observons que le passage du protocole DNS historique à un plus sécurisé peut mener à une diminution importante des performances.

Mots-clés : DNS, chiffrement, resolver

1. Introduction

Les choix de conception initiaux de DNS ont été orientés par des problématiques de performance et de passage à l'échelle. L'utilisation du protocole de transport UDP a permis d'obtenir des temps de latence ainsi qu'une charge serveur les plus faibles possibles. Étant donné que ce protocole n'est pas chiffré, les messages DNS sont vulnérables à de l'espionnage ou à la modification de leur contenu. De nouvelles normes, DNS over TLS (DoT) [9] et DNS over HTTPS (DoH) [7], ont été proposées au sein de l'IETF afin d'y remédier.
Bien que ces nouvelles normes garantissent à la fois la confidentialité et l'intégrité des messages DNS, la question de leur coût reste ouverte : nous ne savons pas si la transition vers ces nouveaux protocoles de l'ensemble du trafic DNS est viable d'un point de vue énergétique ou environnemental. Ce travail propose une estimation des ressources serveur supplémentaires nécessaires pour passer d'un protocole DNS non chiffré et non connecté à un protocole sécurisé mais coûteux en mesurant, dans un environnement contrôlé, le coût ajouté par ces protocoles.
Nous avons effectués plusieurs mesures des performances de deux résolveurs mettant en oeuvre ces protocoles sécurisés : une première dans laquelle tous les messages sont envoyés et reçus en utilisant le protocole UDP, afin d'obtenir une base de comparaison, puis d'autres visant à isoler les différences étapes de chacun de ces nouveaux protocoles afin de déterminer leur coût.
Le passage d'UDP à DoH peut entraîner une diminution de 70% des performances (pour les connexions TCP à durée de vie relativement longue). Cette diminution est due au coût de l'échange de clés TLS, mais aussi à la mise en oeuvre du protocole HTTP.
Le reste du document est organisé comme suit : les sections 2 et 3 décrivent le contexte technique et les travaux connexes, la section 4 propose une analyse des performances côté serveur et dans la section 5, nous concluons.

2. Contexte technique

DNS peut être vu comme un registre interrogé par un client afin de trouver (entre autres) l'adresse IP correspondant à un nom de domaine. Il a été mis en œuvre sous la forme d'une base de données arborescente, dans laquelle l'information est distribuée sur plusieurs serveurs ne détenant chacun qu'une fraction de l'information : la recherche d'informations dans DNS est donc un parcours en profondeur de cet arbre, commençant par la racine. Cependant, si chaque client cherchant à traduire un nom de domaine en adresse IP réalisait un tel processus, cela occasionerait des temps de latence prohibitifs et une surcharge des serveurs les plus proches de la racine ; c'est pour cela que ce processus est délégué aux résolveurs, des serveurs qui, lorsqu'ils reçoivent une requête d'un client, effectuent la résolution, ou répondent à partir de leur cache.

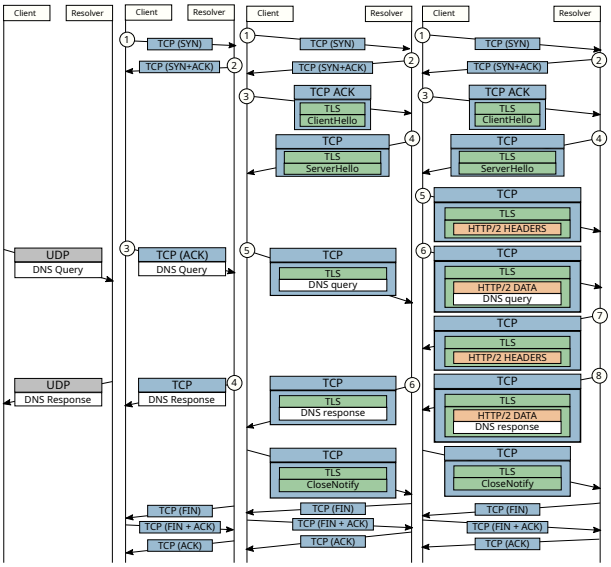

FIGURE 1 – Comparison de DNS over UDP, TCP, TLS et HTTP/2

Contrairement aux autres protocoles web, historiquement basés sur des messages contenant du texte brut, le protocole DNS a été mis en œuvre en utilisant un format de message binaire afin de viser les performances les plus élevées. Les protocoles UDP et TCP ont été choisis pour acheminer les messages DNS. Le premier protocole, UDP, ne requiert aucun établissement de connexion (figure 1 a), et fournit des performances élevées, mais n'offre aucune garantie de remise et limite la taille de la charge utile des messages. C'est donc le protocole recommandé pour transporter les requêtes DNS standard (qui représentent la majeure partie du trafic DNS). Le second, TCP, nécessite l'échange de trois messages (flèches 1 à 3 sur les figures 1 b c d) pour établir une connexion, avant de pouvoir échanger des message DNS. Il est principalement utilisé pour transporter des messages DNS dont la taille est supérieure à la charge utile maximale d'un datagramme UDP.

Ces anciens protocoles de transport n'offrent aucune garantie de sécurité. Plusieurs protocoles ont été proposés pour y remédier :

Le premier de ces protocoles sécurisé, DoT [9], utilise une connexion TLS [15] pour assurer l'authentification des pairs ainsi que la confidentialité et l'intégrité des messages. Il s'appuie sur une connexion TCP pour établir une session TLS entre le client et le serveur. Deux messages (flèches 3 et 4 de la figure) sont échangés pour dériver, à partir de leurs paires respectives de clés asymétriques, une clé symétrique utilisée pour chiffrer les messages DNS. Au cours de ce processus, le client valide également l'identité du résolveur en utilisant le certificat numérique de ce dernier.

Le protocole DoH a été proposé comme alternative pour offrir un transport DNS sécurisé. Il s'appuie sur HTTP/2 [2] pour transporter les messages DNS, contournant ainsi les blocages basés sur le port. DoH peut être considéré comme une couche supplémentaire construite audessus d'une session TLS. Une fois cette session établie, les flux multiples du protocole HTTP/2 sont utilisés pour échanger les requêtes DNS, soient en tant que corps d'une requête HTTP

POST (flèches 5, 6, 7 et 8 de la figure 1 d), soient encodées en base64url et envoyées en tant que paramètre URL d'une requête GET (étant donné que cette méthode est moins courante et donc non prise en compte dans le présent document, elle n'est pas présentée sur la figure 1).

3. Travaux connexes

Nous classons les travaux relatifs à la sécurité des DNS en trois catégories : les travaux qui se concentrent sur la description et la proposition de mesures d'atténuation pour différentes failles de sécurité, les travaux qui visent à comparer le coût côté client des protocoles DNS sécurisés, et enfin, les travaux qui se concentrent sur l'évaluation de leur adoption.
Lorsqu'on étudie la sécurité d'un système d'information, trois propriétés doivent être prises en compte : la confidentialité, l'intégrité et la disponibilité.
Confidentialité : DoUDP et DoTCP n'offrent aucune mécanisme garantissant la confidentialité des messages, ce qui signifie que tout acteur malveillant peut utiliser l'historique de messages DNS d'un utilisateur pour en déduire des informations sur sa vie privée [3]. DoT et DoH règlent ce problème par l'utilisation du protocole TLS pour le transport des messages, ce qui garantit la confidentialité. Cependant, plusieurs études ont montré que certaines caractéristiques du trafic DNS peuvent être exploitées pour, dans certains cas, désanonymiser le trafic DNS chiffré : Dans [16], Siby et al montrent que, malgré l'utilisation du chiffrement, il est toujours possible de déterminer le contenu de messages DNS chiffrés par TLS en utilisant des techniques de prise d'empreintes, et Bushart et Roshow montrent dans [5] que même les techniques de bourrage modernes ne permettent pas d'empêcher complètement ce genre d'attaques. Il convient toutefois de noter que les modèles utilisés dans ces attaques ne peuvent désanonymiser que les flux TLS sur lesquels ils ont été préalablement entraînés (généralement des sites web populaires), et que des techniques telles que l'introduction d'un délai arbitraire dans l'émission des requêtes et des réponses, ou bien l'utilisation de réseaux proxy tels que TOR, peuvent constituer de puissantes mesures d'atténuation face à ces attaques. En outre, ces dernières nécessitent à la fois une mise à jour constante du modèle utilisé pour cibler les sites web afin de faire face aux modifications qui leurs sont apportées, ainsi que la connaissance de la source du trafic, car les clients ont des comportements différents en ce qui concerne les délais entre les requêtes et la taille des messages.
Intégrité : Le protocole DNS n'offrait initialement aucun mécanisme garantissant l'intégrité des données, ce qui signifie qu'un adversaire pouvait, en modifiant une réponse DNS, rediriger un client vers des services frauduleux [11]. DNSSEC a par la suite été normalisé et garantit l'intégrité des données échangées entre le résolveur et les serveurs de noms. En revanche, les échanges de données entre le client et le résolveur utilisent toujours l'ancien protocole, ce qui les rend vulnérables aux attaques susmentionnées.
Étant donné que TLS garantit l'intégrité des messages qu'il transporte, l'utilisation de DoT ou DoH en association avec un résolveur de confiance qui valide l'intégrité des données à l'aide de DNSSEC, peut protéger contre cette catégorie d'attaques.
Disponibilité : Les deux propriétés susmentionnées sont nécessaires mais non suffisantes pour protéger totalement un client. DNS est l'un des protocoles les plus couramment filtrés (par les gouvernements ou les FAI [10]). DoT, qui utilise le port 853 par défaut, peut être facilement bloqué par des filtres basés sur les ports, alors que DoH ne l'est pas, car il repose sur un protocole largement utilisé. Il reste vulnérable aux techniques de prise d'empreinte, capables de détecter si un flux chiffré contient ou non des requêtes et des réponses DoH, comme Vekshin et al l'ont prototypé dans [17]. Cependant, comme nous l'avons dit précédemment, ces techniques nécessitent des modèles entraînés sur une variété de clients, de résolveurs et de formes de trafic qui

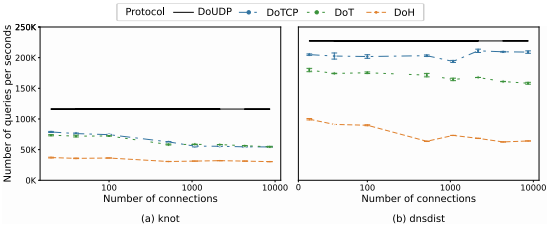

FIGURE 2 – QPS traitées par les deux résolveurs lorsque les connexions durent toute l'expérience

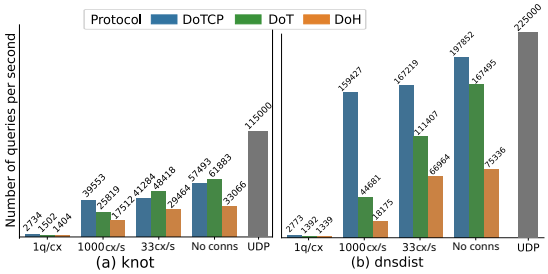

FIGURE 3 – QPS traitées par résolveur et par protocole en fonction du nombre de connexions par seconde

nécessitent une mise à jour constante. Il n'est donc pas réaliste de s'attendre à ce qu'elles soient utilisées à l'échelle mondiale.

Malgré les limitations qui subsistent en matière de sécurité, les avantages offerts par le DoT et le DoH complètent les efforts entrepris pour la première fois avec l'introduction de DNSSEC.

Diverses études se concentrent sur le coût côté client de DoT ou DoH : Hounsel et al. [8] comparent les temps de chargement des pages en utilisant différentes combinaisons de transports DNS, de types de réseaux et de résolveurs publics. Boettger et al. [4] comparent également les temps de résolution ainsi que le coût supplémentaire en matière de taille de messages induit par l'utilisation des différents transports lors de l'utilisation de connexions persistantes ou non persistantes. Ces études montrent que la réutilisation des connexions est bénéfique pour le client et que le DNS sécurisé n'ajoute aucun coût notable pour les clients, sauf sur certains réseaux cellulaires.

Dans [6] Garcìa et al analysent à la fois le nombre de résolveurs DNS sécurisés disponibles ainsi que le taux d'utilisation du DNS chiffré. Alors que le volume du trafic chiffré ne représente toujours que 1% du trafic DNS actuel, le nombre de serveurs disponibles augmente régulièrement, exposant la question de la durabilité énergétique de la généralisation de leur utilisation.

4. Performances serveur

Le passage d'UDP à des protocoles connectés plus complexes peut entraîner une augmentation de la consommation de ressources matérielles du résolveur. Alors que le traitement par le résolveur des requêtes DNS transportées dans un datagramme UDP nécessite simplement de recevoir le datagramme et d'en envoyer un autre contenant la réponse une fois la résolution terminée, l'utilisation de protocoles basés sur des sessions est plus complexe, car ils nécessitent, afin de recevoir des requêtes et d'émettre des réponses, l'établissement d'une session et la gestion de l'état qui lui est associé.

Le coût de ces étapes supplémentaires soulève des questions sur le passage à l'échelle et la consommation de ressources. Afin d'évaluer leur coût, nous avons réalisé une série de benchmarks synthétiques, en utilisant d'abord DNS over UDP (DoUDP), puis DNS over TCP (DoTCP), DNS over TLS (DoT) et enfin DNS over HTTPS (DoH). Bien qu'il n'offre aucune garantie de sécurité, la mesure des performances de DoTCP reste intéressante car, comme nous l'avons dit dans la section 2, les deux protocoles sécurisés ont été construits sur la base de TCP. Ainsi, la comparaison entre DoUDP et DoTCP est un bon indicateur du coût ajouté par la gestion des connexions TCP. De la même manière, la comparaison entre DoTCP et DoT nous permet de mesurer le coût de de l'établissement de la session TLS et du chiffrement du trafic, et la

comparaison entre DoT et DoH nous donne des indications sur le coût des couches HTTP/2.
Dans la section 4.1, nous décrivons l'environnement dans lequel ont été effectué nos expériences. La section 4.2 présente les résultats d'un benchmark du protocole UDP, tandis que les sections 4.3 et 4.4 décrivent les multiples benchmarks synthétiques que nous avons réalisés pour caractériser les coûts des différentes étapes des protocoles basés sur les connexions.

4.1. Configuration expérimentale

Nous avons déployé une architecture DNS sur la plateforme Grid5000 [1], en utilisant les machines du cluster «gros». Notre banc d'essai est composé de 22 Dell PowerEdge R640, chacun d'entre eux ayant un CPU à 18 cœurs avec une fréquence de base de 2,2 GHz et une fréquence «turbo» de 3,9 GHz, 96 GiB de RAM et une carte réseau de 25 Gbps, tous reliés ensemble par le même commutateur. Sur chacune de ces machines est installé Debian 11 «bullseye», avec un noyau Linux 5.10. De ces 22 machines, nous exécutons un résolveur sur l'une d'entre elles, en utilisons vingt comme clients et la dernière comme orchestrateur des expériences.
Nous avons sélectionné deux résolveurs à tester : knot-resolver, car il est utilisé par des acteurs influents de l'industrie (notamment Cloudflare) et dnsdist, qui n'est pas un résolveur en soi, mais agit comme un relais et un équilibreur de charge entre un client et un autre résolveur, et qui répond soit à partir de son cache, soit en transmettant la requête à un autre résolveur. Comme il est compatible avec DoH et DoT, il permet de moderniser une infrastructure DNS existante en ajoutant la prise en charge de ces protocoles sans modifier les logiciels existants. Étant donné que nous avons besoin d'un grand nombre de clients pour atteindre une charge de 100% sur un seul cœur dans notre configuration, nous configurons les deux résolveurs pour qu'ils ne fonctionnent que sur un seul cœur en utilisant les *cgroups*.
Comme nous voulons nous concentrer sur le coût induit par l'utilisation de différents protocoles de transport, nous avons décidé d'exclure de nos mesures le coût du processus de résolution, afin d'éviter le bruit de mesure qui lié à l'interrogation de serveurs de noms externes non contrôlés. Pour ce faire, nous remplissons, au début de chaque expérience, le cache de knot ou de dnsdist avec les enregistrements DNS qui seront demandés par les clients. Pour réduire autant que possible la variabilité expérimentale, tous les noms de domaine interrogés ont tous la même longueur et le même faux TLD.
Les requêtes DNS sont générées à l'aide du logiciel Flamethrower [12]. Nous avons corrigé son code pour qu'il puisse garder les connexions sous-jacentes ouvertes pendant une durée configurable, car le comportement par défaut était de les fermer une fois un lot de requêtes envoyé. Un fork de Flamethrower incluant ces changements est disponible sur github [13]. Lors des benchmarks concernant DoH, nous envoyons nos requêtes dans le corps d'une requête POST HTTP/2, car c'est cette méthode qui est utilisée par les clients que nous avons testé.

4.2. Base de comparaison

Comme il s'agit du transport le plus ancien, le plus largement utilisé et le plus efficace, la mesure des performances d'UDP nous donne une base de référence. Par conséquent, nous évaluons nos résolveurs en envoyant autant de requêtes que possible, ne nous arrêtant que lorsque nous commençons à enregistrer des pertes systématiques. Au mieux, knot a répondu à 115 000 qps (queries per second), tandis que dnsdist a répondu à 225 000 qps. Nous avons étudié la raison de ces pertes et avons observé qu'elles étaient dues à une saturation du processeur, les deux résolveurs étant incapables de traiter les requêtes à un tel rythme, causant un remplissage du tampon de réception UDP côté noyau, et donc un rejet des paquets. Nous expliquons la différence de performances de presque 50% entre knot et dnsdist par le fait que dnsdist est un proxy et un équilibreur de charge dont le but est de transmettre les requêtes à un serveur en

amont aussi efficacement que possible, n'ayant rien d'autre à faire lors de la réception d'une requête que de la transférer ou bien d'y répondre à partir de son cache, alors que knot doit, même dans le cas d'un cache hit, effectuer plus de traitements (comme la vérification et l'application de la politique de requête, le bourrage de la réponse).

4.3. Surcoût lié au traitement des requêtes

L'utilisation des protocoles sécurisés peut induire une utilisation plus importante du processeur en raison des étapes supplémentaires requises pour traiter une requête. Ces étapes supplémentaires peuvent être décomposées en deux parties. Tout d'abord, l'ouverture de la connexion, puis le traitement des requêtes individuelles, dont la complexité dépend du protocole utilisé (voir la section 2). Dans cette section, nous nous concentrons sur le coût de cette dernière étape.
Afin de mesurer le coût supplémentaire par requête, nous devons prendre en considération le nombre de connexions ouvertes simultanément sur lesquelles les requêtes sont envoyées. Pour ce faire, nous avons envoyé une quantité fixe de trafic sur un nombre variable de connexions déjà ouvertes. La quantité fixe totale de requêtes envoyées, ainsi que le nombre minimum de connexions, ont été choisis de manière à ce que l'utilisation du processeur par le résolveur, ainsi que la fréquence du cœur sur lequel il s'exécute soient aussi élevées que possible. Nous avons rencontré un problème lors de l'utilisation de Flamethrower, car nous ne pouvions pas dépasser un certain nombre de requêtes par seconde avec DoH, de sorte que le nombre de requêtes par seconde envoyées n'est pas le même entre DoH et DoT / DoTCP. Cependant, toutes les configurations testées nous ont permis d'atteindre 100% d'utilisation du CPU, ce qui signifie que ce problème n'affecte pas la validité de nos résultats.
Chaque point de la figure 2 présente, pour un protocole donné, le nombre de requêtes par seconde auxquelles le résolveur testé a répondu avec succès (obtenu en divisant le nombre total de requêtes traitées par la durée de l'expérience), en fonction du nombre de connexions sur lequel le trafic est réparti. Étant donné que chaque expérience (combinaison de resolveur, protocole et nombre de connexions) a été répétée au moins trois fois, chaque point présente la valeur minimale, maximale et médiane mesurée. Nous avons également représenté la valeur que nous avons mesuré pour UDP dans l'expérience décrite dans la section 4.2. Pour chaque protocole connecté, il y a une baisse de performance par rapport à UDP, due à la gestion de l'état associé aux connexions. Nous observons une différence notable entre DoTCP et DoT, pour dnsdist seulement alors que pour knot-resolver les performances sont les mêmes. Étant donné que knot-resolver doit exécuter plus de tâches que dnsdist lors de la réception d'une requête DNS, le coût supplémentaire du chiffrement symétrique est absorbé par le coût du traitement des requêtes DNS, et comme dnsdist a moins de travail à effectuer lors de la réception d'une requête, le coût par message ajouté par le chiffrement symétrique a un impact plus important. En comparant DoH à d'autres protocoles, nous constatons, pour les deux résolveurs, une baisse d'un facteur de deux des performances, que nous expliquons par le coût de traitement des messages HTTP/2. Pour chaque protocole, nous observons que les performances ont tendance à baisser lorsque le nombre de connexions augmente (jusqu'à une baisse de 40% lorsque l'on considère dnsdist sur DoH), à l'exception de dnsdist sur TCP.

4.4. Surcout lié à l'établissement des connexions

L'objectif de l'expérience décrite ici est la mesure du coût d'ouverture et de fermeture des connexions pour chaque protocole. Pour cela, nous utilisons les mêmes paramètres expérimentaux que ceux utilisés dans l'expérience précédente (figure 2, annexe) pour tracer le point correspondant à 1000 connexions, en tenant compte de l'établissement et de la fermeture des connexions. Ainsi, en comparant cette expérience et la précédente, nous pouvons déduire le

coût induit par l'établissement des connexions. Nous effectuons deux séries d'expériences, une au cours de laquelle les connexions durent 30 secondes et une autre au cours de laquelle ces dernières durent 1 seconde. Cela signifie que, dans la première expérience, 33 connexions sont établies toutes les secondes, tandis que dans la seconde, 1000 connexions sont établies toutes les secondes. Nous effectuons une série supplémentaire d'expériences où les connexions sont utilisées pour une seule requête, et rouvertes immédiatement, afin de mesurer les performances liées uniquement à l'ouverture de la connexion.
Les résultats de l'expérience sont présentés dans la Figure 3. Chaque barre présente le nombre de requêtes par seconde traitées par le résolveur pour chaque combinaison de résolveur, de protocole et de durée de connexion. Nous avons également représenté le nombre maximum de requêtes par seconde atteint lors des expériences précédentes (sections 4.2, 4.3) à titre de référence. En général, pour knot-resolver et dnsdist, nous observons les mêmes variations de performance entre les protocoles, mais avec des ordres de grandeur différents :
Lorsque peu de connexions sont établies (les connexions durent 30 secondes), nous observons une diminution de 20% des performances pour TCP et DoT, par rapport à une situation où aucune connexion n'est établie. Cependant, nous n'observons pas cette perte de performance pour DoH, car le coût CPU de la gestion des requêtes reste le goulot d'étranglement.
Lorsque la fréquence d'établissement des connexions augmente (les connexions durent 1 seconde), les performances de TCP ne changent pas, tandis que les deux protocoles cryptés voient leurs performances diminuer en raison du coût supplémentaire de l'échange de clés TLS.
Les performances de DoH sont très proches quel que soit le résolveur lorsque les connexions durent une seconde : dans ce cas, le coût de l'établissement des connexions TLS ainsi que le coût de gestion d'HTTP/2 sont si importants qu'ils masquent totalement la différence de performance des deux résolveurs en matière de traitement des messages.
Lorsque les connexions TCP sont utilisées pour une seule requête, le coût de leur établissement induit un effondrement des performances pour tous les protocoles.

5. Conclusion

DNS est toujours au cœur de l'internet d'aujourd'hui. Conçu à l'origine pour les performances (l'utilisation d'un transport non chiffré en témoigne), des préoccupations croissantes en matière de sécurité ont conduit à la normalisation de protocoles sécurisés. Dans cet article, nous avons étudié le coût, du côté du résolveur, de la transition vers de tels protocoles en mesurant le coût de chaque étape ajoutée par les protocoles connectés (DoTCP, DoT, DoH). Nous avons observé que le passage de l'ancien protocole à un protocole sécurisé entraînait, au minimum, une division des performances par deux, en raison du coût induit par l'établissement de la connexion TCP, de la session TLS et par le chiffrement des messages, et que la perte de performance était encore plus importante en ce qui concernait le passage à DoH en raison des couches protocolaires ajoutées par HTTP/2, ce qui, compte tenu du fait que l'utilisation de ce protocole semble être poussée par l'industrie, est contradictoire avec les objectifs initiaux d'efficacité du DNS. De plus, dans le cas où les connexions sont courtes, les performances sont encore plus affectées, ce qui peut conduire, pour absorber la charge, au déploiement d'un grand nombre de résolveurs, entraînant à son tour un coût d'exploitation et environnemental plus élevé. En l'état actuel des choses, le transfert de la totalité du trafic DNS vers DoH ne paraît pas viable. Pour réaliser cette transition il faudra veiller à la minimisation des ouvertures de connexion ainsi qu'à l'utilisation de protocoles moins coûteux que HTTP/2, tout en conservant sa capacité à traverser les pare-feux. Il pourrait donc être intéressant à l'avenir de se pencher sur le protocole HTTP/3, basé sur QUIC, qui est toujours en cours de développement.

6. Annexe 1 - Etude comportement clients

Étant donné que les nouveaux transports DNS nécessitent l'établissement de connexions, de nouvelles questions se posent : bien que le protocole définisse la manière d'interroger le service, il ne contraint aucunement la gestion des connexions sous-jacentes par le client ou le résolveur. La séquence d'ouverture des connexions et d'envoi des requêtes est principalement contrôlée par le client, mais s'intéresser uniquement à son comportement n'est pas suffisant, car le serveur a le choix d'accepter, de rejeter, de fermer ou de garder des connexions ouvertes. L'objectif de cette expérience est de caractériser la forme du trafic entre les clients existants et les résolveurs accessibles au public, afin de pouvoir générer un trafic similaire lors de la mesure des performances côté serveur. La section 6.1 décrit le dispositif expérimental utilisé pour les mesures, tandis que la section 6.2 contient une analyse des différents comportements observés chez les clients et les résolveurs.

6.1. Configuration expérimentale

Nous avons choisi comme clients deux navigateurs web : Firefox v91.5 et Chromium v101.01, car ils annoncent l'utilisation de protocoles sécurisés en proposant un résolveur interne compatible avec DoH. Nous avons également testé DNScrypt-proxy v2.0, un démon qui remplace le résolveur interne d'un système, permettant l'utilisation transparente des protocoles DNS sécurisés pour tous les logiciels présents sur le système, ainsi que le partage de la connexion TLS sous-jacente. Nous avons choisi de concentrer cette analyse sur le protocole DoH qui a gagné plus de terrain que DoT, et qui est donc intégré dans les navigateurs. Pour les résolveurs publics, nous avons choisi trois acteurs majeurs très utilisés par le public : Quad9, Google et Cloudflare. Nous rassemblons la liste des sites web utilisés pour la résolution à travers une liste publique de noms de domaines [14], filtrée pour garder ceux qui ont encore un enregistrement A correspondant à un serveur acceptant le trafic HTTP. Afin de générer le trafic approprié, nous configurons le navigateur pour qu'il utilise un des résolveurs DoH cités, puis nous chargeons un script JavaScript qui effectue des requêtes HTTP HEAD à différents rythmes (une toutes les 50 ms, 1000 ms et 60 000 ms) pendant une période de 30 minutes. Pour générer du trafic à l'aide de DNScrypt-proxy, nous utilisons un programme qui émet régulièrement des requêtes DNS, qui sont transmises à DNSCrypt-proxy. Nous caractérisons la forme du trafic en mesurant le nombre de connexions et, pour chaque connexion, sa durée, le nombre de requêtes qu'elle a transporté, ainsi que l'origine (client ou serveur) et la méthode (FIN ou RST) de fermeture de la connexion.

6.2. Résultats

La figure 2 présente, pour chaque combinaison de logiciel, de délai entre les requêtes et de résolveur public, le nombre et la durée des connexions au résolveur établies par le client (par exemple, sur la figure 4(a), la figure en haut à droite présente le nombre et la durée des connexions TCP que Chromium a établi vers le résolveur quad9). L'axe horizontal de chaque sous-figure représente le temps au cours de l'expérience et une connexion est représentée par un rectangle coloré, dont les bords gauche et droit marquent respectivement sa date de début et de fin. Les connexions de moins d'une seconde sont représentées par une croix. Par exemple, nous observons que, lorsque le délai inter-requêtes est de 50 ms, DNScrypt-proxy n'établit qu'une seule connexion avec le résolveur quad9 (figure 2(b), en haut à droite). D'autre part, nous observons que, avec le même délai inter-requêtes de 50ms, Firefox a établi un grand nombre de connexions de courte durée (moins de 1s) vers le résolveur quad9 (figure 2(a), en haut à droite). Nous avons choisi de ne présenter que le profil de Chromium, car celui de Firefox est similaire.

DNScrypt-proxy

De tous les logiciels utilisés, DNScrypt-proxy est celui qui génère la charge la moins agressive pour le serveur. En effet, son comportement principal est d'ouvrir et de maintenir ouverte une seule connexion TCP qu'il utilisera pour effectuer toutes les requêtes, quelle que soit l'intensité du trafic généré. De plus, un temporisateur interne est mis en place pour déclencher la fermeture de la connexion TCP lorsqu'elle est inutilisée, libérant ainsi les ressources du serveur (ligne inférieure de la figure 4b).

Navigateurs web

Les navigateurs utilisent les ressources DNS de manière plus agressive : au début des sessions, ils tentent de maximiser la probabilité d'une connexion réussie au serveur DNS en ouvrant plusieurs connexions en parallèle au même serveur, ce qui accélère probablement les premières résolutions que les navigateurs effectuent habituellement (figure 4a), entraînant une augmentation de l'utilisation des ressources du serveur. L'utilisation ultérieure de ces connexions ouvertes dépend de l'intensité du trafic. Lorsque celle-ci est faible, avec une fréquence de requêtes inférieure à 1 requête par seconde (voir les deux lignes inférieures de la figure 4a), une seule connexion est principalement utilisée pour gérer le trafic, les connexions restantes finissent par être fermées. Nous observons parfois des fermetures de connexion, forçant une réouverture (ligne de délai de 1000 ms sur la figure 4a), ou plusieurs connexions en même temps (lignes de délai de 1000 ms et 60 000 ms sur la figure 4a), mais ces événements n'ont pas lieu assez souvent au cours d'une expérience pour être significatifs. En cas de trafic DNS intense (plus d'une requête par seconde), le schéma de connexion des navigateurs web change radicalement. Non seulement le navigateur ne parvient pas à générer le trafic que nous demandons, mais nous observons également que les connexions sont ouvertes et fermées en séquence, chaque fermeture de connexion provenant du client (voir la ligne supérieure de la figure 4a) et chaque connexion étant utilisée pour acheminer peu ou pas de requêtes. Du point de vue du serveur, ce comportement représente le pire des cas, car chaque ouverture de connexion étant coûteuse, il en résulte une énorme consommation de ressources.

Resolvers

Cependant, les clients ne sont pas les seuls responsables des schémas de connexion. Les résolveurs ont le choix d'accepter ou de refuser les connexions et le trafic provenant des clients. Nous avons observé que Google a la configuration de résolveur la plus permissive de celles que nous avons testé, car nous n'avons observé aucune limitation en termes de nombre de connexions, de durée ou de nombre de requêtes par seconde (qps) par connexion. Cloudflare n'impose aucune restriction sur la durée de la connexion, alors que le nombre maximum de requêtes par connexion est limité à 10 000 (figure 4b, graphique en haut à gauche). Contrairement à Cloudflare, quad9 n'impose aucune limite au nombre de requêtes par connexion, mais ferme les connexions inutilisées après environ 20 secondes d'inactivité (figure 4a, graphique en bas à droite).
Le comportement voulu des clients et des résolveurs semble être de maintenir une connexion TCP/TLS en vie pendant qu'elle est en cours d'utilisation.

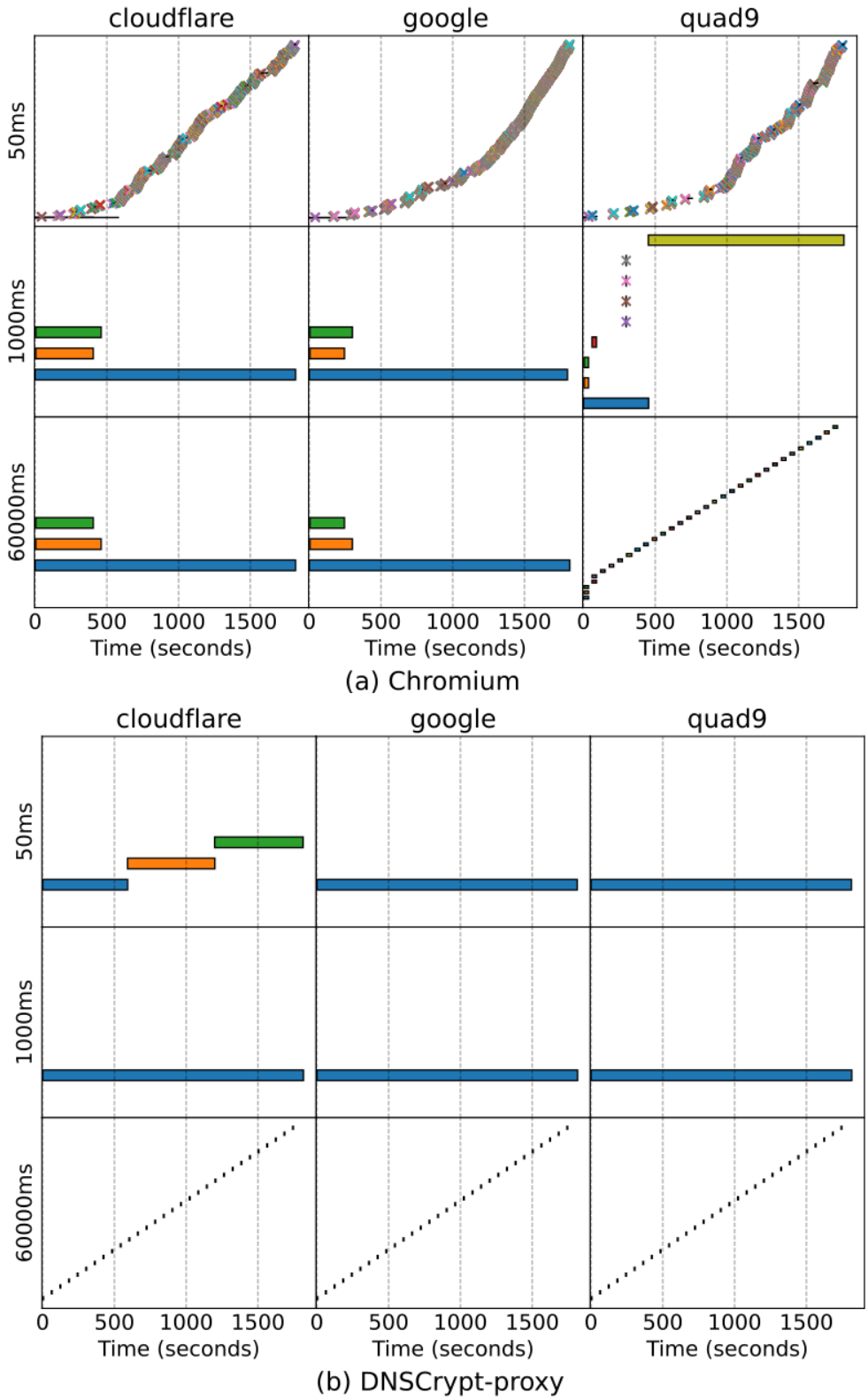

FIGURE 4 – Connexion utilisée par Chromium et DNSCrypt-proxy pour un ensemble de délais de résolution et de requête

Bibliographie

1. Balouek (D.), Carpen A. (A.), Charrier (G.), Desprez (F.), Jeannot (E.), Jeanvoine (E.), Lèbre (A.), Margery (D.), Niclausse (N.), Nussbaum (L.), Richard (O.), Pérez (C.), Quesnel (F.), Rohr (C.) et Sarzyniec (L.). – Adding virtualization capabilities to the Grid'5000 testbed. *In : Cloud Computing and Services Science*. – 2013.
2. Belshe (M.), Peon (R.) et Thomson (M.). – *Hypertext Transfer Protocol Version 2 (HTTP/2)*. – RFC n7540.
3. Bortzmeyer (S.). – *DNS Privacy Considerations*. – RFC n7626.
4. Böttger (T.), Cuadrado (F.), Antichi (G.), Fernandes (E. L. a.), Tyson (G.), Castro (I.) et Uhlig (S.). – An empirical study of the cost of dns-over-https. – In *Internet Measurement Conference (IMC '19)*, 2019.
5. Bushart et Rossow. – Padding ain't enough : Assessing the privacy guarantees of encrypted DNS. – In *10th USENIX Workshop on Free and Open Communications on the Internet, FOCI 2020*.
6. Garcia (S.), Hynek (K.), Vekshin (D.), Cejka (T.) et Wasicek (A.). – Large scale measurement on the adoption of encrypted dns. *arXiv preprint arXiv :2107.04436*, 2021.
7. Hoffman (P.) et McManus (P.). – *DNS Queries over HTTPS (DoH)*. – RFC n8484.
8. Hounsel (A.), Borgolte (K.), Schmitt (P.), Holland (J.) et Feamster (N.). – *Comparing the Effects of DNS, DoT, and DoH on Web Performance*. – 2020.
9. Hu (Z.), Zhu (L.), Heidemann (J.), Mankin (A.), Wessels (D.) et Hoffman (P.). – *Specification for DNS over Transport Layer Security (TLS)*. – RFC n7858.
10. Lowe (G.), Winters (P.) et Marcus (M.). – The great dns wall of china. *MS, New York University*, 2007.
11. M. Dissanayake (I. M.). – Dns cache poisoning : A review on its technique and countermeasures. – In *National Information Technology Conference (NITC '18)*.
12. ns1labs. – flamethrower : github.com/dns-oarc/flamethrower.
13. ns1labs et Le Louët (E.). – flamethrower : github.com/etienne-lelouet/flamethrower.
14. OARC (D.). – Dns sample queries file, 2012.
15. Rescorla (E.). – *The Transport Layer Security (TLS) Protocol Version 1.3*. – RFC n8446.
16. Siby (S.), Juarez (M.), Diaz (C.), Vallina-Rodriguez (N.) et Troncoso (C.). – Encrypted dns ==> privacy ? a traffic analysis perspective. – In *The Network and Distributed System Security Symposium (NDSS '20)*.
17. Vekshin (D.), Hynek (K.) et Cejka (T.). – Doh insight : Detecting dns over https by machine learning. – In *15th International Conference on Availability, Reliability and Security (ARES '20)*, 2020.