SGBLE

Geste de savoir

Utilisez le DNS sécurisé : DoT et DoH

17 février 2023

Table des matières

Introduction

La sécurisation des communications sur Internet tend à devenir la norme depuis quelques années. Cela est flagrant pour le Web où tout est mis en place pour encourager au maximum l'utilisation de HTTP**S** depuis quelques années: la promesse d'un meilleur référencement pour les sites sécurisés, l'UI des navigateurs qui pointe du doigt la non-utilisation de la couche sécurisée, la naissance des services de certification gratuits et automatisables comme Let's Encrypt ou ZeroSSL.

Malgré cette tendance qu'on ne peut qu'apprécier, DNS est resté un peu en marge alors même qu'il s'agit d'un service critique et précédant l'utilisation des services sécurisés. Eh oui, sans résoudre un nom de domaine, on n'accède même pas à un site Web en HTTPS en premier lieu!

Pour rappel, la sécurisation des communications permet d'assurer le respect de sa vie privée: les informations échangées ne peuvent être lues par un tiers non désiré; et sa sécurité: l'authentification des communications permet de s'assurer qu'on reçoit bien les vraies informations et que celles-ci n'ont pas été altérées, à dessein malveillant, en cours de route.

Le DNS en clair ne permet ni l'un, ni l'autre. De par sa nature sensible, il est important de le sécuriser pour éviter par exemple:

— de laisser savoir quels services nous visitons (vie privée);
— de laisser la possibilité à un tiers d'altérer une réponse DNS, en y injectant une adresse IP illégitime par exemple (sécurité).

Fort heureusement, le DNS aussi a eu le droit à sa version sécurisée, c'est même deux choix qui s'offrent à nous: **DNS over TLS** (DoT) et **DNS over HTTPS** (DoH).

On ne parlera pas de DNSSEC ici, qui n'est pas une mesure concurrente mais plutôt une mesure complémentaire.

DNS over TLS (DoT)

Le DoT consiste à faire passer DNS sur TCP sur couche TLS (port standard 853) qui sécurise le trafic. Cela fonctionne exactement de la même façon qu'avec d'autres protocoles dans leur version sécurisée: HTTP**S**, FTP**S**, SMTP**S**, etc.[1]

Le DoT bénéficie d'un support acceptable dans les appareils grand public. Les smartphones l'implémentent depuis Android 9 Pie et Apple iOS/iPadOS 14 au niveau système (via une app ou un profil). Linux avec systemd le supporte aussi nativement au niveau système.

Pour utiliser DoT, il faut utiliser un service de résolution (serveur DNS) compatible le proposant sur son port 853/tcp. Parmi les plus populaires: Google *Public DNS*, Cloudflare *1.1.1.1*, Quad9 (IBM), et un petit nouveau franco-européen: DNS0.EU.

> Attention, il est évident que le service de résolution DNS choisi doit être digne de confiance! De plus, la phase récursive assurée par le résolveur du service n'a plus à être sécurisée par la suite. Cela n'est pas forcément un problème, mais il faut le garder à l'esprit.

Pour mettre en place le vôtre, il faudra trouver un résolveur DNS compatible DoT, Unbound par exemple.[2]

DNS over HTTPS (DoH)

Avec DoH, le protocole DNS passe ici dans le contenu d'une requête HTTP**S**, ce qui revient *in fine* à faire passer DNS sur TLS, mais avec HTTP comme protocole intermédiaire[3].

Cela peut sembler manquer d'intérêt par rapport à l'utilisation de DoT évoquée plus haut, mais il y a malgré tout quelques avantages à utiliser ce «détour». Une requête DoH est une requête HTTPS comme les autres, ainsi n'y a-t-il pas de moyen simple de discriminer le trafic DoH du trafic HTTPS. Dans un réseau bloquant l'accès au port tcp/853 nécessaire au DoT, c'est donc un avantage. Le trafic HTTPS, quant à lui, n'est presque jamais bloqué puisque cela rendrait l'accès Internet quasiment inutile pour les usages courants.

En bref, utiliser DoH peut s'avérer plus résilient à travers les réseaux plus ou moins filtrés (entreprise, cellulaire, wifi public) que d'utiliser DoT pour le même niveau de sécurité.

Notons aussi que le DoH est très bien supporté par les navigateurs Web courants. Firefox ouvrait le bal, mais Chrome et Edge supportent aussi bien DoH aujourd'hui (à configurer dans les paramètres). Cette approche agit au niveau du navigateur seul, pas du système entier. Cette solution peut néanmoins être tout-à-fait acceptable sur un système ne supportant ni DoT, ni DoH au niveau système. C'est toujours mieux que rien. Heureusement, certains systèmes supportent quand même DoH aussi au niveau système, comme Apple iOS/iPadOS et Android.

Là encore, il faut trouver un service de résolution compatible offrant le service sur DoH. Ceux qui ont été évoqués plus hauts supportent aussi bien DoT que DoH: Google *Public DNS*, Cloudflare *1.1.1.1*, Quad9, DNS0.EU. Le serveur Unbound aussi, depuis les versions récentes.

Limites

Utiliser DoT ou DoH c'est bien mieux que le DNS en clair. Cependant, ce n'est pas assez pour garantir à coup sûr la protection de sa vie privée face à des personnes trop curieuses. N'oubliez pas qu'en vous connectant à un site en HTTPS, le *handshake* TLS fait potentiellement fuiter le nom de domaine que vous venez de résoudre, dans le SNI !

```
# tcpdump port 443 -v -A -n
12:26:08.645713 IP (tos 0x0, ttl 64, id 34468, offset 0, flags
    [DF], proto TCP (6), length 569)
    10.8.42.54.38008 > 92.243.7.44.https: Flags [P.], cksum 0x75f3
    (correct), seq 1:518, ack 1, win 502, options [nop,nop,TS val
    1257528485 ecr 550319964], length 517
E..9..@.@.A.
..6\..,.x........T.....u......
J.\. .7\........... v!.....x.d~.v.d...$......./z..
    .;......o..K.c..........N.."Q....".......+./.....,.0.
.   ........./.5............zestedesavoir.com.........
.............................h2.http/1.1..........3.k.i...
    fG....y...@..E..Z...E....0..K).....A.Qb....f<.
..'.^#K.....,`...e.>..v..b..P..8..f.y..".c;R.....$.!...+..........
    ......................-........@....L.........................
    ..................................................).K.&.
    ..r..N6....;.....g..".......T.6}..X..!
    .D....w.o.O....(.$.$.j....Xs./O.
```

Exemple de connexion sécurisée (HTTPS). On voit passer en clair le `zestedesavoir.com`, on peut donc deviner que je me connecte à ce site, même si les échanges entre ma machine et le site restent bien sécurisés, et même si ma requête DNS demandant l'adresse associée à ce nom de domaine a été faite de façon sécurisée juste avant.

Enfin, si une administration est déterminée à bloquer l'utilisation du DoH, elle peut aisément bloquer les adresses IP des services connus. Selon le niveau de détermination, une observation humaine très minutieuse et experte pourrait aussi deviner qu'un trafic DoH est établi avec un serveur particulier, le différenciant ainsi du reste du trafic HTTPS. Rien n'est parfait.

Cependant, vous devriez être tranquilles dans 99,999% des cas!

En milieu hostile, faites donc attention à vous.

1. Pour autant, l'apellation *DoT* a été retenue, mais pas *DNSS*.
2. À défaut d'un serveur compatible DoT, il faut au minimum un serveur compatible avec le DNS sur TCP et mettre en place une terminaison TLS devant, avec HAProxy par exemple.
3. Dans le cas de l'utilisation de HTTP/3, il s'agira bien d'une connexion UDP/QUIC avec sa couche de sécurité, mais cela ne change pas le principe.