PowerDNS

DNS over TLS, DNS over HTTPS: an exciting time for DNS

Rémi Gacogne – Senior PowerDNS Engineer

FRnOG 32, 29 mars 2019

POWERDNS
AN OX COMPANY

TL;DR

Le déploiement de DNS over TLS et DNS over HTTPS change les rapports entre utilisateurs et ISPs :

- DNS fourni par une partie tierce
- Contrôlé par le navigateur ou l'application, contourne les réglages systèmes
- Chiffré, extrêmement difficile à bloquer voire même à détecter

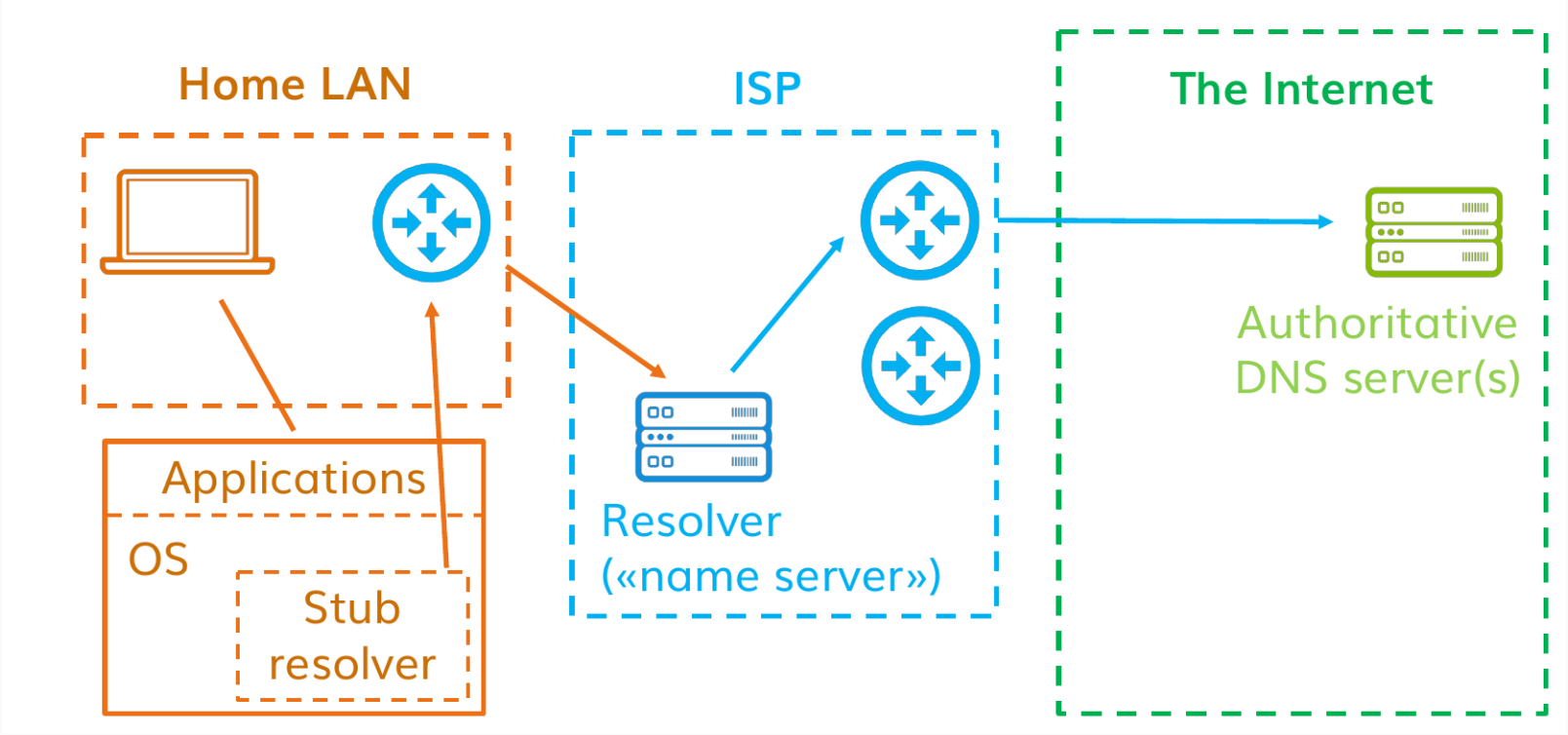
DoT, DoH ?

Encapsulation du protocole DNS existant pour les échanges entre le client et le serveur DNS récursif.

- DNS over TLS[1]: Encapsulation dans TLS
- DNS over HTTPS[2]: Encapsulation dans HTTP/2

[1] https://tools.ietf.org/html/rfc7858
[2] https://tools.ietf.org/html/rfc8484

Les serveurs quoi ?



DNS “classique”

- UDP pour l’écrasante majorité des échanges, TCP, en clair
- Serveur récursif géré par le fournisseur d’accès Internet, via DHCP
- De plus en plus d’alternatives tierces : 1.1.1.1 (Cloudflare), 8.8.8.8 (Google), 9.9.9.9 (Quad9)

Pourquoi changer ce qui fonctionne ?

- Serveur annoncé via DHCP
- En clair : confidentialité, intégrité
- Confiance : NXDOMAIN redirection, censure
- Besoin de réaliser des requêtes DNS depuis les applications Web

Et DNSSEC ?

- DNSSEC permet d'assurer l'intégrité
- Mais validation essentiellement au niveau du serveur récursif
- Et toujours en clair

DNS over TLS

- Identique à DNS sur TCP, encapsulé dans TLS
- Port dédié : TCP/853
- Déjà utilisé automatiquement depuis Android Pie
- Facile à déployer
- N'assure l'intégrité que de point à point : DNSSEC reste pertinent

DNS over HTTPS : Pourquoi ?

Par rapport à DNS over TLS :

- Quasiment impossible à distinguer du trafic HTTPS “classique”, port TCP/443
- Manque de confiance dans les ISPs (data mining, censure, monétisation)
- Par les gens du Web pour les gens du Web

DNS over HTTPS : avantages techniques sur DoT ?

- Impossible à bloquer ? Seulement lorsque déployé par des acteurs incontournables (Cloudflare, Google, ...)
- Plus rapide ? DoT fait aussi bien lorsque correctement mis en oeuvre (TFO, multiplexing, connection reuse..)
- Plus sécurisé ? Uniquement lorsque pré-configuré à la place de l'utilisateur

DNS over HTTPS : problèmes

- Pas de réels problèmes techniques
- Mais de sérieuses inquiétudes dans le déploiement
- “On ne peut pas faire confiance à l’utilisateur pour choisir un fournisseur sûr, il est nécessaire de choisir pour lui”

DNS over HTTPS : Navigateurs

- Mozilla : DoH par défaut vers un petit nombre de Trusted Recursive Resolver (Cloudflare) : “The user will be informed that we have enabled use of a TRR and have the opportunity to turn it off at that time, but will not be required to opt-in to get DoH with a TRR.” [3]
- Google : Expérimentation en cours dans Chrome, DNS “classique” rapidement reporté comme “non sûr” aux utilisateurs [4]

---

[3] https://mailarchive.ietf.org/arch/msg/doh/po6GCAJ52BAKuyL-dZiU91v6hLw

[4] https://mailarchive.ietf.org/arch/msg/doh/EVomTCdmATxr19VmRu9uloxDDVg

DNS over HTTPS : Applications

Applications mobiles et IoT utilisent de plus en plus des DNS personnalisés, difficile à inspecter et bloquer

Conséquences pour les utilisateurs

- Risque de concentration chez Cloudflare, Google, sans alternative ni relation commerciale
- Perte de services : Filtrage parental, protection et détection malware / botnet, blocage de publicités
- Interruption de service en cas de split-horizon (VPNs, ...)
- Performance (latence, CDN, ...)

Conséquences pour les fournisseurs de services

- Dépendance : si le fournisseur DoH est indisponible ou lent, l'utilisateur considère qu'Internet ne fonctionne plus
- Filtrage légal : impossible à assurer au niveau du DNS (DPI ?)
- CDN : plus de géo-localisation au niveau DNS, tout repose sur un anycast global
- Interruption de service : filtrage parental, protection et détection malware / botnet
- Perte de contrôle et de visibilité

Recommandations pour les utilisateurs

- Soyez attentif à la fenêtre vous proposant un DNS “plus sûr”
- Choisissez soigneusement votre fournisseur DoH, si vous le pouvez

Recommandations pour les fournisseurs de services

Soyez le plus neutre, rapide et fiable possible avec votre DNS :

- La latence est primordiale, la disponibilité également
- Filtrage légal plus simple, moins coûteux et intrusif
- Pas de monétisation à outrance en vendant la vie privée des utilisateurs
- Inutile de donner des raisons pour contourner votre service

Recommandations pour les fournisseurs de services

Déployez DoT sans tarder :

- Réel gain pour la vie privée et la sécurité
- Android l'utilisera s'il est présent, repassera en mode normal sinon
- Google indiquera bientôt que le DNS n'est pas "sûr" dans le cas contraire, et proposera le sien
- Déjà déployé par plusieurs fournisseurs d'accès majeurs en Europe
- Plusieurs solutions Open Source : DNSDist, Knot Resolver, Unbound [5]

[5] https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status

Recommandations pour les fournisseurs de services

Considérez le déploiement de DoH :

- Le protocole est techniquement sain
- Il est important d'avoir de nombreuses alternatives, géographiquement distribuée, soumises au droit européen
- Plusieurs solutions Open Source : DoH Proxy, DNSDist, Rust DoH
- Mais : "As noted above, we don't think secure transport to the local resolver is sufficient to ensure the privacy and security guarantees we are trying to provide." [6]

[6] https://mailarchive.ietf.org/arch/msg/doh/iZ9WHptC9Vw1eJW6tUmsuCmaYAc

Questions ?

Merci !