Inria

jres DIJON 2019

DoH/Firefox : Gestion d'horizon DNS sur un serveur DoH/DoT exposé sur internet

Pierre Bénard

Glossaire

DoT

- DNS over TLS : chiffrement des échanges DNS au travers de TLS
- Port standard : TCP 853

DoH

- DNS over HTTPS : chiffrement des échanges DNS au travers de HTTPS
- Port standard : TCP 443

Contexte et objectifs

Contexte

- Sept. 2019 : annonce de Mozilla d'activer le DoH via CloudFlare par défaut (aux USA)
- Pourquoi ne pas offrir nous même ce service ?

Objectif

- Utiliser DoH, mais pas celui de CloudFlare
- Utilisable depuis internet, intranet ou VPN
- Conserver les horizons DNS clients différents entre intranet/VPN et internet

Utilisation de DNSDIST

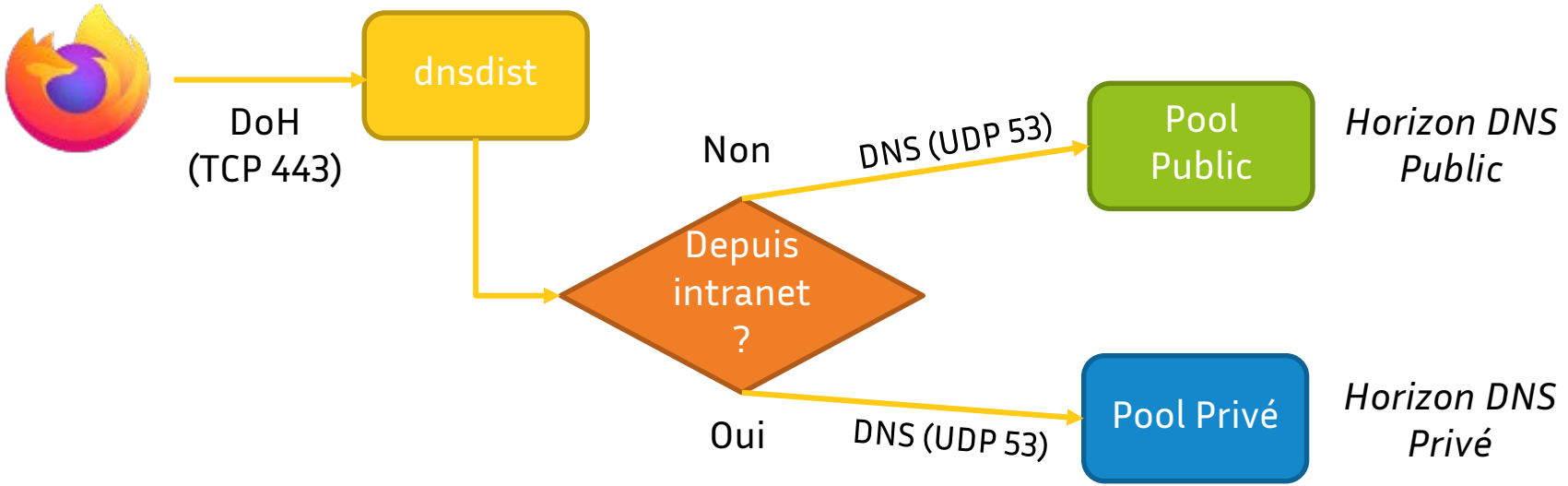
DNSDIST (https://dnsdist.org)

- Proxy DNS, répartiteur de charge DNS applicatif
- Open source
- Editer et supporter par PowerDNS (https://www.powerdns.com/)
- DoH/DoT disponible depuis la version 1.4

Fonctionnalités remarquables

- Configuration dynamique en Lua (possibilité de fonctions personnalisées)
- Gestion d'objets (*NetmaskGroup*, *Pool*, *Server*, ...)
- Gestion de *Rules* (sur les demandes) et de *ResponseRules* (sur les réponses)
- API REST

Schéma de principe



Configuration de Firefox

Paramètres avancés (About:config)

- Ajout du service DoH personnalisé

```
network.trr.resolvers = [{ "name": "Cloudflare", "url": "https://mozilla.cloudflare-dns.com/dns-query" },
{ "name": "My DoH", "url": "https://mydoh.chezmoi.fr" } ]
```

- Choix du mode TRR *(DoH prioritaire, si indisponible, rebascule sur le DNS standard de l'OS) :*

```
network.trr.mode = 2
```

Choix et activation du DoH dans les paramètres

- Préférences -> Général -> Paramètres réseau -> Activer le DNS via HTTPS -> Utiliser le fournisseur : "My DoH"

Configuration de dnsdist

Extrait de dnsdist.conf :

```
-- #### SERVERS/POOLS ####
newServer({address="10.0.0.2", name="ns1-priv", pool="private"})
newServer({address="10.0.0.3", name="ns2-priv", pool="private"})
newServer({address="192.0.2.2", name="ns1-pub", pool="public"})
newServer({address="192.0.2.3", name="ns2-pub", pool="public"})

-- #### NETMASK GROUP ####
intranet = newNMG()
intranet:addMask("10.0.0.0/8") -- intranet subnet 1
intranet:addMask("192.0.2.0/24") -- intranet subnet 2

-- #### RULES #####
addAction(NotRule(NetmaskGroupRule(intranet)), PoolAction("public"))
addAction(NetmaskGroupRule(intranet), PoolAction("private"))
```

Bilan

DoH/DoT

- Le sujet est encore frais
- Documentations et exemples encore rares
- Peu d'applications ou OS gèrent nativement DoH/DoT à ce jour

La suite

- Tester d'autre usage de dnsdist (load-balancer applicatif vs VIP classique)
- Tester la configuration Firefox/DoH à plus grande échelle
- Tester le mode opportuniste sur les DNS fournis par l'OS (le client teste la disponibilité de DoT puis DoH puis se rabat sur DNS)

Bibliographie

Dnsdist/Powerdns :

- Documentation dnsdist : https://dnsdist.org/
- Blog PowerDNS (realeases notes + article sur DoH) : https://blog.powerdns.com/

Le blog de Stéphane Bortzmeyer :

- Configuration d'un serveur DoH : https://www.bortzmeyer.org/doh-mon-resolveur.html
- Analyse du RFC 8484 (DOH) : https://www.bortzmeyer.org/8484.html
- Analyse du RFC 7858 (DOT) : https://www.bortzmeyer.org/7858.html

Mozilla :

- Annonce activation DoH par défaut (USA) : https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/