

A Proxy Use Case of DNS over HTTPS

draft-ietf-dnsop-dns-wireformat-http-03

Davey Song (speaker)/BII lab,

Paul Vixie, Shane Kerr

2018-07-17 @IETF 102 Montreal



Brief History of this document

- First drafted in February 17, 2016 intending to record an novel experiment during WIDECAMPE
- This draft was presented in IETF 95
 - with the title “DNS wire-format over HTTP”
 - including two scenarios : proxy mode and director mode
- Accepted as WG document in September 15, 2016
 - postponed by Chair later due to concerns from HTTP people
 - Waited for DOH to define a good transport protocol, draft-ietf-doh-dns-over-https
- Awake and focus on proxy scenario with DOH protocol
 - Change the title to “An Proxy Use Case of DNS over HTTPS” and still be an experimental document
 - Try several approaches of keep the transparency in DOH proxy

Wire format scenarios

- Proxy mode
 - Either client or server can run as a proxy
 - "drop-in" support
- Direct mode
 - Support in server
 - none yet... is it useful?
 - Support in applications
 - via API
 - Better in truncation case

Source : 2016-04-08 DNSOP IETF95 presented by Shane Kerr

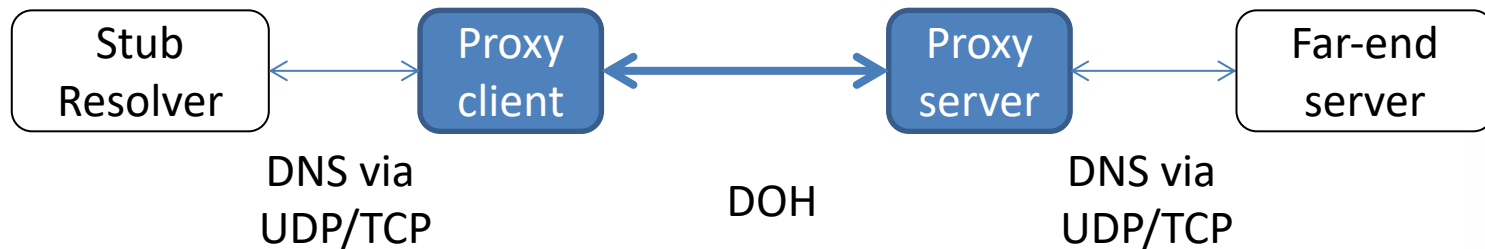


Wire format latest discussion

- POST vs. GET for HTTP message
- *Could* be used by web developers
- TCP/UDP flag required
- Clarification of 2-byte length field in TCP
- Expanded security section
 - A bit vague, since all DNS, HTTP, and TLS vulnerabilities may be applicable....
- /.well-known/dns-over-http
- Thanks to Bob Harold and Paul Hoffman for review!

DOH in Proxy scenario

- DOH proposes a approach to cure DNS's long-time suffering from on-path attack by spoofing and blocking
- Proxy use case served as an incremental adoption tool when DOH is not widely available
 - To leverage the DOH protocol as a substrate to tunnel DNS data over HTTPs which is called DOH proxy
 - DOH proxy works as a simple DNS forwarder keeping the transparency principle, as a normal DNS proxy described in [RFC5625](#)



Implementations on DOH proxy

- BII's implementations of proxy_dns in both [C version](#) and [Go version](#)
- Facebook's [doh-proxy](#) implementation
- Frank Denis' [doh-proxy](#) (server-side proxy) and [dnscrypt-proxy](#) (client proxy)
- Travis Burtrum's [jDnsProxy](#) DNS proxy and cache

Transparency principle in DOH Proxy

- DOH proxy keeps transparency principle of DNS proxy recommended in [RFC5625](#)
 - “Proxies should be as transparent as possible, such that any "hop-by-hop" mechanisms or newly introduced protocol extensions operate as if the proxy were not there.”
 - **“DNS proxies MUST therefore be prepared to receive and forward queries over TCP.”**
- Original transport indicator in DOH proxy
 - Introduce a indicator to allow the proxy server use the same transport protocol (UDP or TCP) to forward DNS query to far-end server just as the stub-client does without DOH proxy

Relation with DOH protocol

- Inherit most protocol definition from DOH
 - Can use both GET and POST
 - HTTPs is mandatory for proxy case
 - Use and process application/dns-message media type
 - Keep most HTTP context in DOH, like HTTP Cache, HTTP/2, server push and content Negotiation
- Extension of DOH for proxy use case
 - Extend the DOH URI Template with a new a new variable "proto" , "proto=tcp " or "proto=udp“
 - Two-byte length field in wireformat TCP DNS message will be omitted by proxy client

Variable "proto" examples

- `https://example.com/proxy_dns?proto=tcp` will cause the server to make a request using TCP
- `"https://example.com/proxy_dns?proto=udp"` will cause the server to make a request using UDP

Suggested Implementation

- The DOH proxy may return TC bit to the sub-resolver which will cause TCP fallback starting from the sub-resolver. An alternative advised is that the proxy has to have sufficient smarts to recognize the returned TC bit and re-issue the request over TCP to the back-end DNS server.
- Another implementation is suggested that DOH proxy server has a pool of TCP connections from the proxy to the back-end DNS server(s), over which incoming requests can be multiplexed

Next step

- Do you think DOH proxy case is useful?
- Informational or experimental?
- Adoption in DNSOP? Or move to DOH

