SUBJECT: DNS-over-HTTPS Implementation
FROM: Christof Meerwald <[redacted]
TO: [redacted]
DATE: 19/11/2020 20:50

Hi,

I want to specifically comment on "Although Firefox disables DoH when it detects that enterprise policies are in place, are there other situations in which deployment of DoH might cause technical or operational challenges (e.g., mobile networks, NAT64 and DNS64)?"

I am particularly concerned about cases where users connect via VPN into a private network, potentially with split-horizon DNS. These will be nightmare scenarios for anyone trying to figure out what is going on. Having the system use one set of DNS servers and Firefox use a different set will just cause additional confusion when trying to debug the set-up as the often used "ping" command will likely show the expected results. Using a different browser might also work, probably even restarting the browser after the VPN was connected might affect results.

Seriously, using a completely separate DNS set up compared to the rest of the system is such a bad idea (irrespective of if DNS over HTTPS would be an improvement or not). If you care about DoH, make your case and provide the tools so that users can switch to DoH on the system level if they are convinced, but don't try to make the browser an operating system on its own.

Let me add a general comment about your TRR policies: Will the end-user be told that you are in effect hijacking DNS requests and re-routing them to one of your partners? Do you consider that an open and transparent practice?

Christof

--

[redacted]