DNS-over-HTTPS: How Does It Affect User Quality of Experience?

Alan Jones
September 2019

NetForecast.com

Executive Summary

As DNS-over-HTTPS (DoH) gains traction to protect DNS users from surveillance and manipulation, it is important to know how it will affect the quality of the user experience compared to “regular” DNS. To shed light on this, NetForecast performed preliminary tests from three geographically distributed US data centers to nine popular websites for eight consecutive days. Initial results show that on average DoH adds approximately 77ms to the lookup time compared to DNS. This longer lookup time will adversely affect the user experience in cases where DNS calls are invoked many times for a web site or application. Additionally, NetForecast found that DoH as well as DNS performance varies by region as well as by destination over time.

Specifically, NetForecast’s preliminary research findings show that:

- The average DoH lookup time was 92.2ms, compared to an average DNS lookup time of 15.1ms.
- DoH lookup times vary over time.
- DNS lookup times also vary over time, although the variations are not as pronounced as for DoH.
- Because DoH and DNS lookup times vary over time, their performance should be continuously monitored.
- DoH performance varies by user location and by content destination.
- Applications requiring many lookups will be most adversely affected by DoH.

Background

The DNS over HTTPS (DoH) protocol is emerging as a more secure alternative to conventional DNS. The DoH protocol, described in Internet Engineering Task Force RFC 8484, performs DNS lookups using encrypted exchanges defined in the HTTPS protocol. Proponents of DoH see it as a tool to protect users’ private information. Several browsers currently offer DoH as an option, and it is expected to become a preferred protocol.

Detractors cite a variety of possible issues with mainstream DoH deployment, including: DoH servers as a single point of failure; loss of protection from malicious URLs; and reduced performance based on increased DNS lookup overhead.

NetForecast is uniquely positioned to measure DoH and DNS performance because we operate a large network of probes measuring latency and DNS lookup times.

Methodology

NetForecast tests initiated both DNS and DoH domain name resolution calls from computers located in Amazon Web Services (AWS) data centers in the Washington DC area, Central Ohio, and the San Francisco Bay area to a list of servers to resolve IP addresses. The AWS computer locations were selected to distribute testing across the continental US. NetForecast selected five DNS and two DoH servers for testing based on their popularity (see figure 1 below).

Each AWS instance ran a series of DNS and DoH lookups. The tests rotated through the DNS and DoH servers, performing a lookup every 10 seconds. Each test also rotated the sites used for the lookup from the domain names.

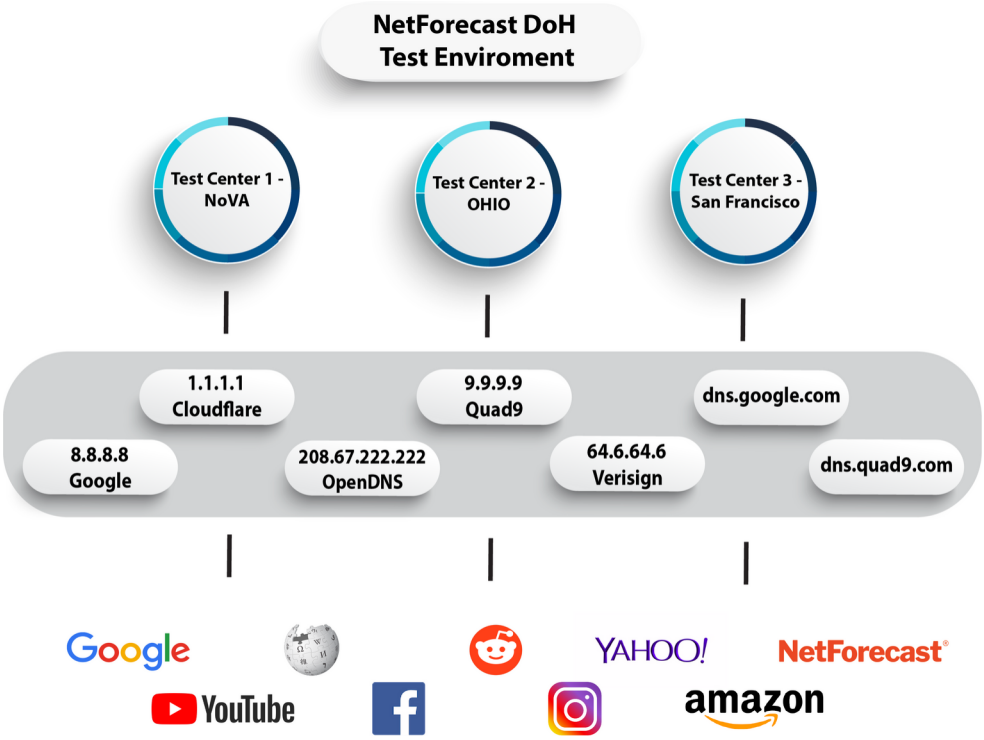

Figure 1 - DNS and DoH Servers with Domain Names Used for Lookup

The round-trip time for each test was measured and rounded to the nearest millisecond. Data from each test was then written to a database in real time and stored in a MySQL database hosted on AWS. Data reported here are based on hourly mean values of the 360 samples gathered each hour for each domain-server pair.

Results

Over the course of the eight days of testing NetForecast made over 175,000 measurements from the three AWS test instances. The primary finding is that DoH lookup times are much longer than DNS lookup times. Although longer lookup times

were expected, the actual magnitude of the difference was larger than expected. For the entire test period the average DNS resolution time was 15.1ms compared to an average DoH lookup time of 92.2ms.

Examining the resolution time by server type over the test period, two significant increases in DoH resolution times occurred on July 10th as Figure 2 shows.

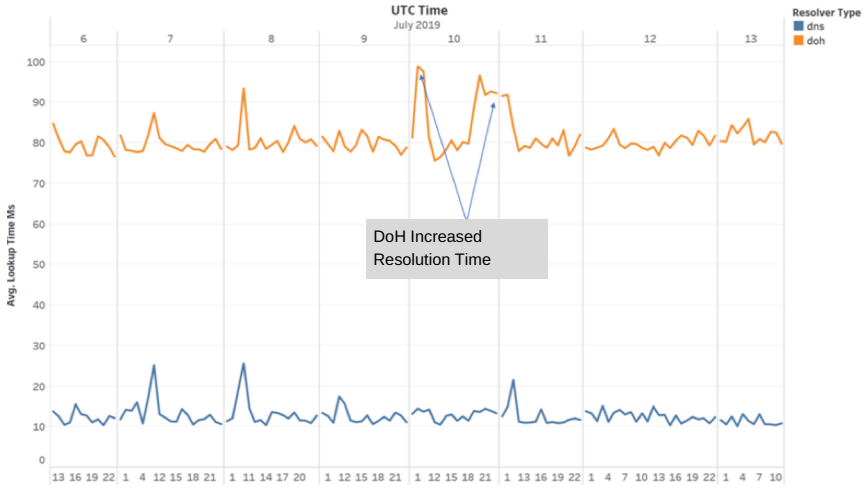

Figure 2 - Average DNS and DoH Lookup Times

Figure 3 shows the servers responsible for the DoH July 10th resolution time increases. All the resolution time increases occurred on the Google DoH server. The San Francisco Bay area event was shorter but of a greater magnitude. The Washington DC and Ohio events were time aligned and lasted longer.

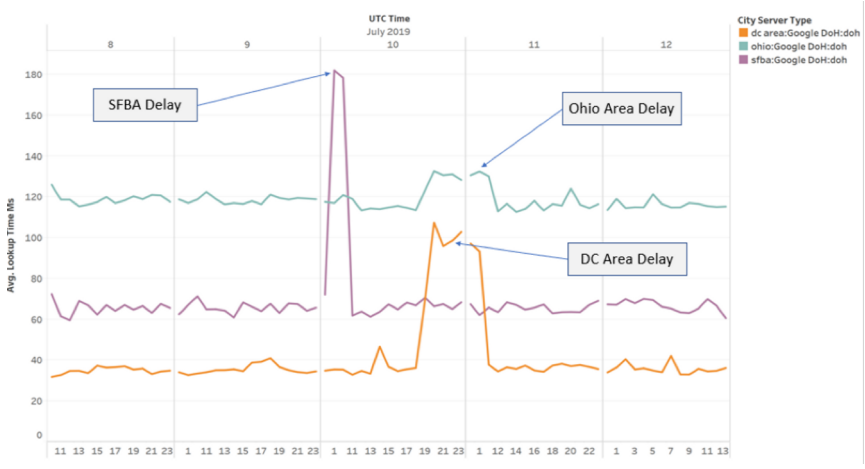

Figure 3 - DoH Lookup Times by Region

Related to the event highlighted in Figure 3 was a resolution time increase on the corresponding DNS servers for Google in the Washington DC and Ohio areas. Increases were also observed on the OpenDNS server in the Washington DC area as Figure 4 shows.

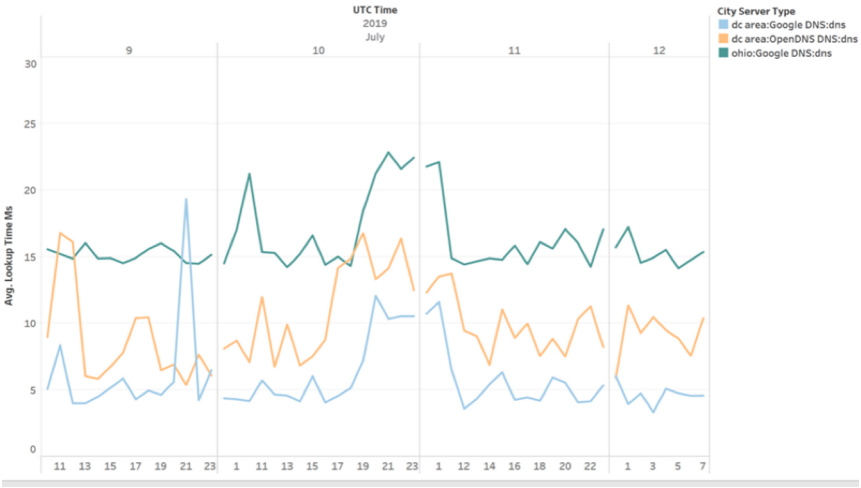

Figure 4 - DNS Lookup Times Corresponding to DoH Delays

An unexpected result was the difference in resolution time by site name (domain). Looking at the extreme case for two well-known sites, there is a remarkable difference in the resolution time of amazon.com and wikipedia.org (Figure 5). This difference appeared in both the DNS and DoH data.

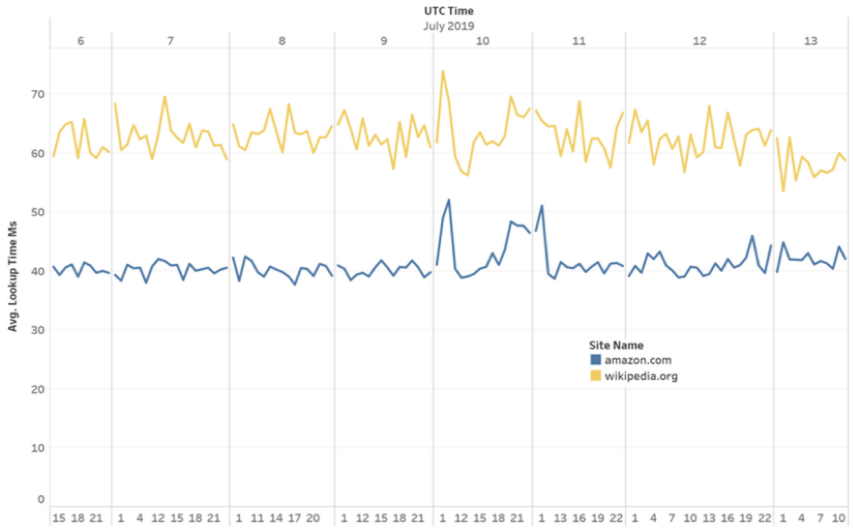

Figure 5 - Composite Resolution Time for Amazon and Wikipedia

Location played a larger than expected role in the resolution time for both DNS and DoH. For the best and worst cases, the delta in the resolution time between the Ohio region and the Washington DC region was 10.7ms for DNS (Figure 6) and 55.7ms for DoH (Figure 7).

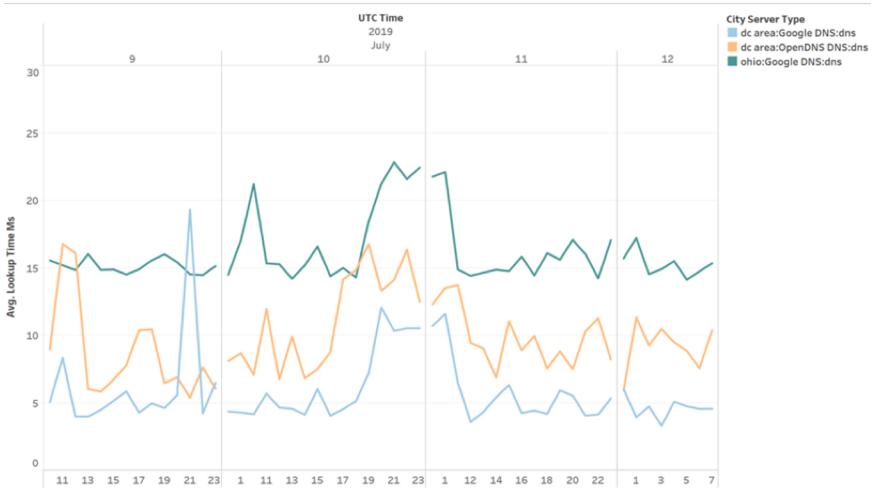

Figure 6 - DNS Resolution Times by Region

During the test period NetForecast observed a significant increase in resolution time in the CloudFlare server on July 10th as Figure 7 shows.

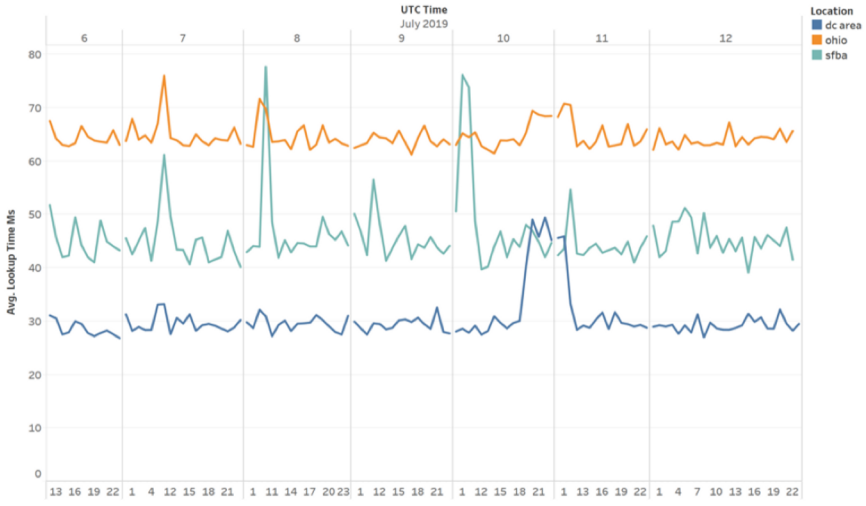

Figure 7 - DoH Resolution Time by Region

Conclusions

NetForecast's initial test results show that DoH lookup times are longer than DNS lookup times. Longer lookup times will have the most notable adverse effect on users of applications that require many lookups. Other important research findings are that DoH performance varies over time and it varies based on the region in which the user is located as well as the destination content server. Additionally, both DoH and DNS servers showed unexpected resolution time variations over the test period.

It is important to note that resolution time variations cause significant quality of experience problems for users that are impossible to detect or analyze using speed tests alone. Real-world applications that perform multiple name resolution lookups—i.e., news feeds, social media, and online shopping experiences—would experience the greatest degradation.

Other end-to-end network latency increases will exaggerate the effect of DoH over DNS name resolution. Specialized network measurements like those deployed by NetForecast are a useful tool in detecting issues affecting customer QoE over extended periods or for alarming on real time events.

Unexpected differences in resolution time by location and by site name show more tests are required to qualify the influence of these factors. Suggested new tests include new server sites and a larger sample of top domain names.

NetForecast suggests that website owners and network service providers measure user experience quality before and after deploying DoH, and that performance monitoring be continuous because lookup times are inconsistent over time.