DNS over HTTPS

DNS over HTTPS (DOH) is an implementation of DNS on an application level that bypasses the standard, distributed name resolution. While this has advantages, the disadvantages can outweigh them in many cases.

Advantages

- DNS tracking and snooping, where a DNS provider can track which web sites you visit is disabled. This is something a lot of ISP's do by default when you use their DNS server.
- DNS blocking by ISP's or government can be bypassed, so you can find sites. In many cases, ISP's will block access to certain web sites.
- DNS redirection is bypassed, where a query for “microsoft.com”, for example, would take you to a hackers web site to attempt to take over your computer.

Disadvantages

DOH breaks many things which are commonly used today to protect home and business networks.

- Many parental controls are based on DNS redirection to keep children from accessing inappropriate web sites.
- Businesses can utilize this to block inappropriate web site access on work computers, similar to parental controls used in a home.
- networks which use a DMZ network to expose one or more servers to the Internet sometimes use DNS overrides to give access these services differently when the client machine is inside of the network using something called *split dns*. DOH can make it impossible to connect to these machines from inside the network or more costly as the traffic will have to exit the LAN, then reenter it after traversing one or more public network switches/routers.
- Some anti-virus software on personal machines have firewalls that redirect network traffic for inspection to protect the workstation.

Firefox

Mozilla Firefox, as of the 25 Feb 2020 release, implements DOH by default, forcing non-technical users to use Cloudflare for their DNS resolution. While it is fairly simple for technologically adept users to turn this off, most users will begin using it with little notification and may see some of the issues above.

Disabling DOH in a network

Many routers/firewalls have the ability to create DNS overrides. Mozilla has taken advantage of this by allowing a systems administrator to create one record in the firewall/DNS server that will tell Firefox

not to use DOH. For opnSense, the instructions are as follows:

1. Log into OPNsens router as an administrator
2. Open Services | Unbound DNS | Overrides
3. Create a new *Domain Override* with the following values
    1. Domain: use-application-dns.net
    2. IP Address: 127.0.0.1
    3. Description: block DOH in Firefox
    4. Save

When you open a new session of Firefox, assuming your OPNSense router's Unbound service is your DNS, Firefox will request the IP of use-application-dns.net *from your configured DNS server*. Your firewall/Router will return a null value, which tells Firefox to not use DOH in the future.

Firefox will perform this check every time it is started.

Links

- https://www.reddit.com/r/PFSENSE/comments/djb6pi/dealing_with_dns_over_https_in_a_business_network/
- https://support.umbrella.com/hc/en-us/articles/230904088-Preventing-circumvention-of-Cisco-Umbrella-with-firewall-rules
- https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https
- https://support.mozilla.org/en-US/kb/canary-domain-use-application-dnsnet
- https://en.wikipedia.org/wiki/DNS_over_HTTPS