paloalto NETWORKS

STRATA™
BY PALO ALTO NETWORKS

Protecting Organizations in a World of DoH and DoT

Organizations invest a lot of time, money, and effort in securing their networks. However, one area that often does not receive its due attention is the Domain Name System (DNS). DNS is commonly utilized in many attacks, from malware propagation to data exfiltration. According to Palo Alto Networks Unit 42 threat research, approximately 80% of malware uses DNS to establish a command-and-control (C2) channel.

Since its inception, DNS has largely been unencrypted, but new encrypted DNS protocols that aim to improve privacy are gaining support among leading browser and other software vendors. With this increase in support, enterprise networks will begin to see more encrypted DNS traffic. While this should accomplish the goal of increasing privacy, encrypted DNS traffic that is not properly inspected or prohibited poses a security risk. This leaves many organizations needing to figure out how to protect against threats in a new world of encrypted DNS.

What Is Encrypted DNS?

DNS converts domain names that humans can read (e.g., www.paloaltonetworks.com) into Internet Protocol (IP) addresses (e.g., 34.107.151.202). When a user types a domain name into a web browser, the browser sends a DNS request to a DNS server, asking for the IP address associated with that domain name. The DNS server then responds with the IP address for that browser to use.

DNS traffic is sent over the network in plaintext, unencrypted, which leaves it vulnerable to spying or being intercepted and redirected to undesired destinations. Encryption of DNS makes it harder for anyone to snoop into DNS queries or corrupt them in transit. Specifically, encrypted DNS protocols add a layer of client privacy and protection from man-in-the-middle tampering while performing the same function as the traditional plaintext DNS Protocol.

Two methods for encrypting DNS have been introduced over the past few years: DNS over HTTPS and DNS over TLS.

DNS over HTTPS

DNS over HTTPS (DoH) Protocol uses the well-known HTTPS port 443, for which the Internet Engineering Task Force's RFC specifically states the intent is to "mix DoH traffic with other HTTPS traffic on the same connection," "make DNS traffic analysis more difficult,"[1] and thereby evade enterprise controls. The DoH Protocol simply uses the underlying TLS encryption and request syntax provided by the common HTTPS and HTTP/2 standards, adding only a method to encapsulate standard DNS queries and responses over the top of standard HTTP requests.

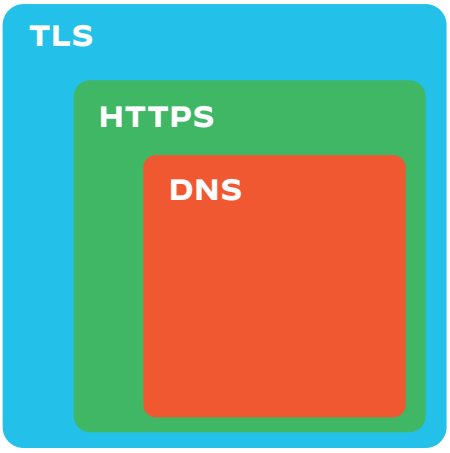

Figure 1: DNS over HTTPS

Unless HTTPS traffic is being identified as DoH queries, ideally using decryption, applications already in use within your organization can bypass the local DNS settings, routing queries out to third-party DoH resolvers and around all existing DNS logging, monitoring, inspection, and controls.

Google and Mozilla have implemented DoH capabilities in the latest versions of their browsers, with both companies working toward deployment of DoH as the enabled default for all DNS queries.[2] Microsoft also announced plans to integrate DoH in its operating systems.[3] Unfortunately, in addition to legitimate software companies, malicious parties have recently adapted to begin using DoH as a means of bypassing traditional enterprise controls.[4,5] In either case, both benign and malicious DoH traffic will go unnoticed, leaving organizations blind to malicious usage of DoH as a channel for malware, C2, and exfiltration of sensitive data.

DNS over TLS

Whereas the DoH Protocol seeks to intermingle with other traffic on the same port, the DNS over TLS (DoT) Protocol instead defaults to a port reserved for this sole purpose, even specifically excluding the use of the same port for traditional unencrypted DNS traffic.[6]

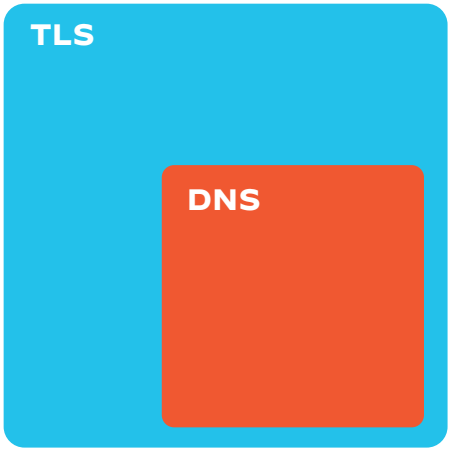

Figure 1: DNS over TLS

The DoT Protocol uses Transport Layer Security (TLS) to provide a layer of encryption encapsulating standard DNS Protocol queries, with traffic using the well-known port 853.[7] In establishing this dedicated port, the DoT Protocol was designed to make it easy for organizations to either simply block the port traffic or opt in to its usage and decryption by controlling access to the port.

1. "DNS Queries over HTTPS (DoH)," Internet Engineering Task Force, October 2018, https://tools.ietf.org/html/rfc8484#section-8.1.
2. "Firefox continues push to bring DNS over HTTPS by default for US users," Mozilla, February 25, 2020, https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users.
3. "Windows will improve user privacy with DNS over HTTPS," Microsoft, November 17, 2019, https://techcommunity.microsoft.com/t5/Networking-Blog/Windows-will-improve-user-privacy-with-DNS-over-HTTPS/ba-p/1014229.
4. "PsiXBot Now Using Google DNS over HTTPS and Possible New Sexploitation Module," Proofpoint, September 6, 2019, https://www.proofpoint.com/us/threat-insight/post/psixbot-now-using-google-dns-over-https-and-possible-new-sexploitation-module.
5. "An Analysis of Godlua Backdoor," Netlab, July 1, 2019, https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en.
6. "DNS Queries over HTTPS (DoH)," Internet Engineering Task Force, October 2018, https://tools.ietf.org/html/rfc7858#section-3.1.
7. "DNS Queries over HTTPS (DoH)," Internet Engineering Task Force, October 2018, https://tools.ietf.org/html/rfc7858#section-6.

Google has implemented DoT in Android® Pie and later clients, with the setting enabled by default to automatically use DoT if it is available.[8] However, at the organizational level, DoT's adoption is opt-in by nature since it requires that network administrators explicitly allow traffic on port 853 through their firewall for this new protocol.

How Does Encrypted DNS Affect My Organization?

Over the last 20 years, most web traffic has moved from HTTP to HTTPS to protect it from prying eyes. DNS is moving to encryption to enhance privacy in much the same way. As we live in a much faster world these days, it's reasonable to assume that the majority of DNS traffic will be encrypted much more quickly. As evident in the activities of companies like Google, Microsoft, and Mozilla, adoption of encrypted DNS is already well underway. In fact, it's highly likely that encrypted DNS traffic is already traversing your network, introducing significant risk. While encryption provides privacy for end users, the protective nature of encryption can be easily misused to hide malicious activities. Encryption creates a significant blind spot for enterprises, where attackers can infiltrate the network regardless of firewalls or other security capabilities.

How Can Palo Alto Networks Help?

With proper configuration, Palo Alto Networks Next-Generation Firewalls can prohibit the use of the DoH Protocol and are equipped to prohibit or secure usage of DoT Protocol, allowing you to retain visibility and security over all DNS traffic on your network. With DoH, you must decrypt the HTTPS traffic and block DoH to secure it. With DoT, you have the option to decrypt and secure, or simply block. Either way, decryption is critical. In addition, we recommend using our DNS Security subscription to analyze DNS traffic for threats in real time.

Securing Encrypted DNS

DoH and DoT share some traits that purposefully lower the visibility of DNS requests from a given client and the organization as a whole. The protocols foundationally use TLS to establish encrypted connections—over a port not traditionally used for DNS traffic—between the client making requests and the server resolving DNS queries.

While privacy from third-party visibility may be desirable, the methods these protocols use create additional security challenges for organizations wanting to maintain their own visibility into and control over outbound network traffic. As the protocols differ in their implementations, the methods of maintaining organizational visibility and controls will differ by protocol.

Getting Visibility and Control of DoH Traffic

As a best practice for DoH, we recommend configuring the Next-Generation Firewall to decrypt HTTPS traffic and block DoH traffic with the "dns-over-https" App-ID. First, ensure the firewall is configured to decrypt HTTPS by consulting our Decryption Best Practices. Next, create a policy to apply the action to traffic identified with the "dns-over-https" App-ID (see figure 3).

As an intermediate alternative if your organization has not fully implemented HTTPS decryption, the Next-Generation Firewall can still be configured to apply the "deny" action to the "dns-over-https" App-ID, but the effect will be limited to blocking certain well-known DoH resolvers by their domain names,[9] as DoH traffic cannot be fully inspected without HTTPS decryption.

				Source			Destination				
	Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action
1	Block DoH	none	universal	Inside	any	any	Outside	any	dns-over-https	any	Drop

Figure 3: Using App-ID to block DoH

Getting Visibility and Control of DoT Traffic

As a best practice for DoT, we recommend either of the following based on organizational considerations:

- Configure the Next-Generation Firewall to decrypt all DoT traffic through port 853. Utilizing full support for decrypted DoT traffic, the decrypted traffic will then appear as the "dns" App-ID, to which you can apply any action, Palo Alto Networks DNS Security subscription, or signatures.
- Alternatively, fully block the "dns-over-tls" App-ID over port 853. As it is implicitly blocked by default, no action is necessary unless your organization has previously allowed the "dns-over-tls" App-ID or traffic over port 853.

8. "DNS over TLS support in Android P Developer Preview," Android Developers Blog, April 13, 2018, https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html.
9. Search for "dns-over-http" in Applipedia and view the description for details.

Conclusion

DNS, much like email and the web, presents significant security challenges as an internet-facing, flexible protocol that attackers commonly use to penetrate networks, remotely control malware, and steal data through sophisticated exfiltration. Just as with email and web traffic, enterprises must secure DNS traffic with the same levels of visibility, control, and threat prevention.

The Palo Alto Networks DNS Security service, when combined with App-ID™ technology in our Next-Generation Firewalls, is uniquely positioned to provide visibility, control, and security for all DNS traffic. With the emergence of encrypted DNS, it is important to maintain visibility and control by following the best practices described in this document.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com