National Security Agency | Cybersecurity Information

Adopting Encrypted DNS in Enterprise Environments

Executive summary

Use of the Internet relies on translating domain names (like “nsa.gov”) to Internet Protocol addresses. This is the job of the Domain Name System (DNS). In the past, DNS lookups were generally unencrypted, since they have to be handled by the network to direct traffic to the right locations. DNS over Hypertext Transfer Protocol over Transport Layer Security (HTTPS), often referred to as DNS over HTTPS (DoH), encrypts DNS requests by using HTTPS to provide privacy, integrity, and “last mile” source authentication with a client’s DNS resolver. It is useful to prevent eavesdropping and manipulation of DNS traffic. While DoH can help protect the privacy of DNS requests and the integrity of responses, enterprises that use DoH will lose some of the control needed to govern DNS usage within their networks unless they allow only their chosen DoH resolver to be used. Enterprise DNS controls can prevent numerous threat techniques used by cyber threat actors for initial access, command and control, and exfiltration.

Using DoH with external resolvers can be good for home or mobile users and networks that do not use DNS security controls. For enterprise networks, however, NSA recommends using only designated enterprise DNS resolvers in order to properly leverage essential enterprise cybersecurity defenses, facilitate access to local network resources, and protect internal network information. The enterprise DNS resolver may be either an enterprise-operated DNS server or an externally hosted service. Either way, the enterprise resolver should support encrypted DNS requests, such as DoH, for local privacy and integrity protections, but all other encrypted DNS resolvers should be disabled and blocked. However, if the enterprise DNS resolver does not support DoH, the enterprise DNS resolver should still be used and all encrypted DNS should be disabled and blocked until encrypted DNS capabilities can be fully integrated into the enterprise DNS infrastructure.

This guidance explains the purpose behind the DoH design and the importance of configuring enterprise networks appropriately to add benefits to, but not hinder, their DNS security controls. The following recommendations will assist enterprise network owners and administrators to balance DNS privacy and governance.

Contact

Cybersecurity Inquiries: 410-854-4200, Cybersecurity_Requests@nsa.gov

Media Inquiries: 443-634-0721, MediaRelations@nsa.gov

What is DoH?

Domain Name System (DNS) over Hypertext Transfer Protocol over Transport Layer Security (HTTPS), often referred to as DNS over HTTPS (DoH), encrypts DNS requests to provide privacy, integrity, and “last mile” source authentication for DNS transactions with a client’s DNS resolver. It is useful to prevent eavesdropping and manipulation of DNS traffic (T1040, T1565.002).[1] While DoH can help protect the privacy of DNS requests and the integrity of responses, enterprises that use DoH will lose some of the control needed to govern DNS usage within their networks unless they allow only their designated DoH resolver to be used. These essential protective DNS controls can prevent numerous threat techniques used for initial access, command and control, and exfiltration, such as phishing links to malicious domains, connections using dynamic name resolution, and commands hidden in DNS traffic (TA0001, TA0011, TA0010, T1566.002, T1568, T1071.004). The enterprise DoH resolver may be either an enterprise-operated DNS server or an external resolver from a protective DNS provider. However, if the enterprise DNS resolver does not support DoH, the enterprise resolver should still be used and all encrypted DNS should be disabled and blocked until encrypted DNS capabilities can be fully integrated into the enterprise DNS infrastructure.

How do DNS and DoH work?

DNS translates domain names to their corresponding Internet Protocol (IP) addresses, allowing web users to more easily access websites. With traditional enterprise DNS architectures, once a client submits a DNS query, it will first go to the enterprise recursive DNS resolver, often assigned via Dynamic Host Configuration Protocol (DHCP). The enterprise DNS resolver will either return the answered query from its cache or forward the query through the enterprise gateway to the external authoritative DNS servers. The DNS response will return through the enterprise gateway, to the enterprise DNS resolver, and then finally to the client. During this exchange, both the enterprise DNS resolver and the enterprise gateway can see the plaintext query and response and log it for analysis or block it if it seems malicious or violates enterprise policies.

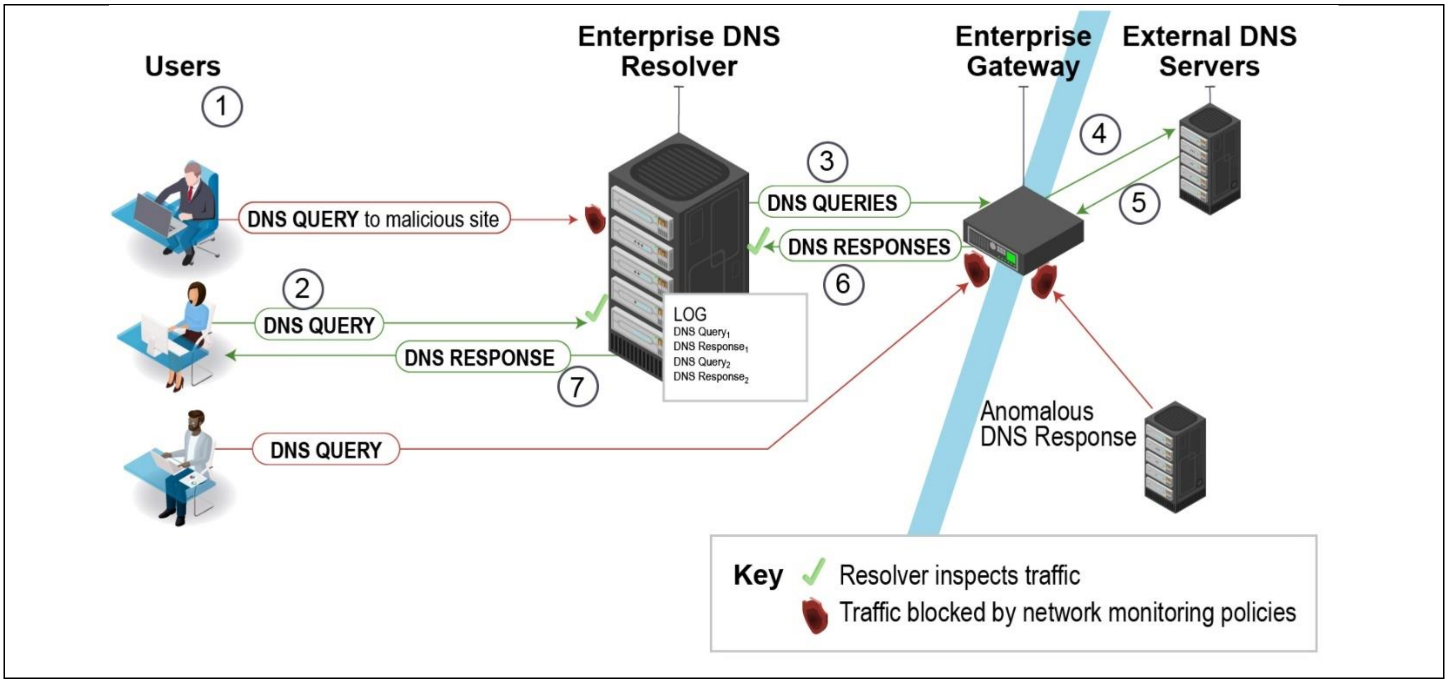

Figure 1: How common enterprise DNS architectures work

1. The user wants to visit a website they do not know is malicious and types the domain name into the web browser.
2. The request for the domain name is sent to the enterprise DNS resolver with a plaintext packet on port 53. Queries that violate DNS monitoring policies may generate alerts and/or be blocked.

[1] T1040 and similar notations identify MITRE ATT&CK® techniques and tactics. MITRE ATT&CK is a registered trademark of The MITRE Corporation.

3. If the IP address for the domain is not in the enterprise DNS resolver's cache of domains and the domain is not filtered, it will send a DNS query through the enterprise gateway.
4. The enterprise gateway forwards the plaintext DNS request to an external DNS server. It also blocks DNS requests not from the enterprise DNS resolver.
5. The response to the query with the IP address of the domain, the address of another DNS server with more information, or an error is returned in plaintext back through the enterprise gateway.
6. The enterprise gateway forwards the response back to the enterprise DNS resolver. Steps 3-6 repeat until either the IP address for the requested domain name is found or there is an error.
7. The DNS resolver returns the response back to the user's web browser, which then requests the webpage from the IP address in the response.

The DNS resolver to query can be configured in the operating system (OS) or sometimes in a specific application, such as a web browser. When a client has DoH enabled and configured to use a DoH resolver not designated by the enterprise, the DoH traffic will be sent directly to the enterprise gateway as HTTPS encrypted traffic over port 443, bypassing the enterprise DNS resolver entirely. The request will then go to the client-selected DoH resolver, which will either return the response or pass it along to the authoritative servers to resolve the request. The answered query returns from the DoH resolver through the enterprise gateway back to the client over port 443. The transaction between the client and DoH resolver is encrypted, therefore the plaintext request and response usually cannot be analyzed by the enterprise gateway. If the DoH resolver cannot answer the query, or is inaccessible, the original query may be re-sent using traditional DNS.

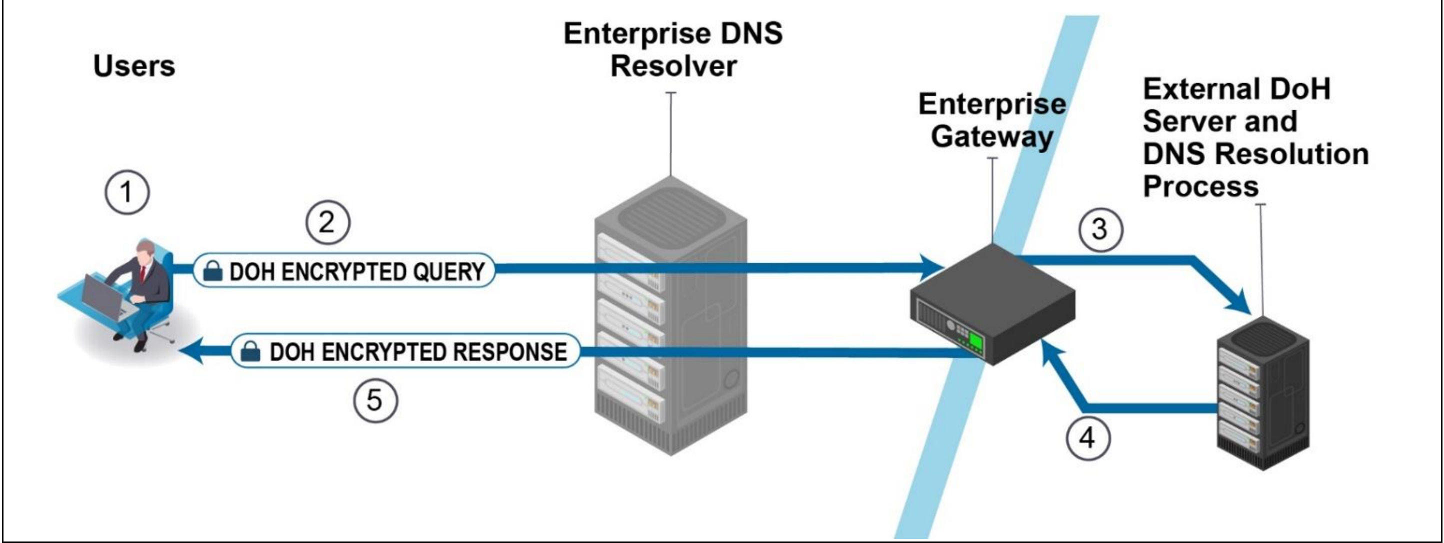

Figure 2: How DoH with an external DoH resolver works

1. The user wants to visit an unauthorized website, and types the domain into the web browser.
2. The DoH request is encrypted and sent through the enterprise gateway over port 443. The enterprise DNS resolver is bypassed, therefore circumventing its blocking and monitoring capabilities.
3. The enterprise gateway forwards the encrypted request to the external DoH resolver, just like it would forward any other HTTPS request to an external server. Logging and visibility at the enterprise gateway is usually not possible.
4. The external DoH resolver performs DNS resolution and responds to the query with the IP address of the site.
5. The enterprise gateway forwards the encrypted DoH response back to the user's web browser, which then requests the webpage from the IP address in the response.

In addition to DoH, there are other protocols that encrypt DNS communication with a DNS resolver. DNS over Transport Layer Security (DoT), is another implementation that encrypts DNS transactions. Instead of using HTTPS over port 443, DoT uses Transport Layer Security (TLS) over port 853, so it is easier to detect than DoH. Oblivious DoH (ODoH) is another protocol that adds a proxy layer to DoH requests for additional privacy protection. The majority of the issues and mitigations that apply to DoH also apply to DoT and ODoH, but are not covered in this guidance.

What are the benefits of using DoH?

DoH protects DNS traffic between a client and a DNS resolver from unauthorized access to its information by cyber threat actors. Since the traffic is encrypted and blends in with other HTTPS traffic to websites, it is difficult for cyber threat actors to determine which packets contain DNS requests or responses and see which domains and IP addresses were requested. The responses from the DNS resolver are also authenticated and protected from unauthorized modification. In contrast, traditional DNS transactions occur in plaintext on a port that is exclusively used for DNS, so cyber threat actors can easily read and modify the traditional DNS traffic.

What are the issues with using DoH?

DoH provides the benefit of encrypted DNS transactions, but it can also bring issues to enterprises, including a false sense of security, bypassing of DNS monitoring and protections, concerns for internal network configurations and information, and exploitation of upstream DNS traffic. In some cases, individual client applications may enable DoH using external resolvers, causing some of these issues automatically.

A false sense of security

DoH is not a panacea. DoH does not guarantee protection from cyber threat actors and their ability to see where a client is going on the web. DoH is specifically designed to encrypt only the DNS transaction between the client and resolver, not any other traffic that happens after the query is satisfied. While this allows clients to privately obtain an IP address based on a domain name, there are other ways cyber threat actors can determine information without reading the DNS request directly, such as monitoring the connection a client makes after the DNS request. That connection will still have the destination IP address unencrypted and may reveal the domain or server name. This and other traffic analysis techniques could identify domains [1, 2]. If there is a concern that a user's activity is being tracked and they must conceal their activity, DoH alone will not fully address the problem.

Bypassing DNS monitoring and protections

Enterprises may use network monitoring tools to inspect DNS traffic and look for indications of anomalous activity. Many tools typically inspect plaintext DNS traffic. DoH encrypts the DNS traffic, which prevents enterprises from monitoring DNS with these network-based tools unless they are breaking and inspecting TLS traffic. If DoH is used with the enterprise resolver, then inspection can still occur at the resolver or using resolver logs. However, if external DoH resolvers are not blocked and DoH is enabled on the user's browser or OS to use a different resolver, there could be issues gaining visibility into that encrypted DNS traffic.

Many organizations use enterprise DNS resolvers or specific external DNS providers as a key element in the overall network security architecture. These protective DNS services may filter domains and IP addresses based on known malicious domains, restricted content categories, reputation information, typosquatting protections, advanced analysis, DNS Security Extensions (DNSSEC) validation, or other reasons.[2] When DoH is used with external DoH resolvers and the enterprise DNS service is bypassed, the organization's devices can lose these important defenses. This also prevents local-level DNS caching and the performance improvements it can bring.

Malware can also leverage DoH to perform DNS lookups that bypass enterprise DNS resolvers and network monitoring tools, often for command and control or exfiltration purposes (T1071.001, T1071.004, T1568, T1573, and T1572) [3].

Concerns for internal network configurations and information

If a device or application is configured to use an external DoH resolver and connects to an enterprise network, it will ignore the address of the DNS resolver assigned to it through the DHCP and connect straight to its preferred DoH resolver. This is a security concern because if a client is trying to connect to an internal domain, the query will be sent to the external DoH resolver first before failing over to the enterprise DNS resolver, which can spill internal network information to a third party. In addition, if an enterprise uses a split DNS configuration where the same domain name is resolved to different addresses depending on whether the client is within the enterprise network, an internal client using an external DoH resolver will receive the address intended for external clients instead. This may cause internal enterprise services to be inaccessible, confuse the user, or cause other issues [4].

[2] Recommendations on protective DNS will be discussed in an upcoming NSA guidance document.

Exploitation of upstream DNS traffic

Typically, DoH occurs only in the “last mile” between the client system initiating the DNS request and the DoH resolver the client is configured to use. DoH requests and responses are protected from modification and other cyber threat activities between the resolver and client. DNS traffic for the rest of the DNS process, such as between the DoH resolver and the top-level root DNS servers on the internet, often do not use DoH and are not encrypted. For parts of the DNS process that are not encrypted, cyber threat actors could still passively view the plaintext DNS traffic or try to redirect the traffic to malicious DNS servers, just as with any traditional DNS traffic. Even with DoH protection, resolvers that communicate with malicious servers upstream could still be susceptible to DNS cache poisoning techniques. DNSSEC should be used to protect the upstream responses, but the DoH resolver may not validate DNSSEC. Enterprises that do not realize which parts of the DNS process are vulnerable could fall into a false sense of security [5].

Mitigating DoH issues

For home, mobile, and teleworking users without enterprise DNS controls, DoH can be a good way to protect the confidentiality and integrity of DNS traffic. There are even several reputable DNS resolvers that are free for public use that provide additional protections, such as malicious site blocking, family-oriented filters, and DNSSEC validation. For enterprises, NSA recommends that the enterprise DNS resolver supports encrypted DNS, such as DoH, and that only that resolver be used in order to have the best DNS protections and visibility. If protective DNS capabilities are provided by an external source, then encrypted DNS should be allowed for that specific resolver and all others should be blocked. However, if the enterprise DNS service provides DNS protections, but does not support encrypted DNS, then there has to be a tradeoff. In this case, the loss of enterprise security controls outweighs the protections offered by DoH, so NSA recommends that enterprises disable encrypted DNS within their network and continue to use only the enterprise DNS service.[3]

Only use the enterprise DNS resolver and disable all others

If an enterprise wants to use DoH, ensure that the DoH clients only send queries to the enterprise DNS resolver. Disable and block all other DoH resolvers. To disable all other DoH on an enterprise network, configure network security devices at the enterprise gateway to block known DoH resolvers so hosts cannot circumvent DNS security controls and cyber threat actors cannot easily use it to hide their actions. There are several public lists of known DoH resolver domain names and IP addresses. In addition, disable DoT by blocking transmission control protocol port 853 at the enterprise gateway. For web browsers, applications, and operating systems that support DoH, especially the ones that may enable it automatically, disable it in standard configurations and set canary domains so that DoH is automatically disabled. For example, Firefox®[4] and Chrome®[5] automatically disable DoH if enterprise policies are configured. Enterprise policies can also be used to configure DoH to use the enterprise DoH resolver [7–9].

Block unauthorized DoH resolvers and traffic

Enterprise administrators should understand the limitations of DHCP for devices connecting to their network. If clients use their own default DoH resolver, the clients will attempt to send DoH requests to that resolver first before the DNS resolver from the DHCP configuration is used. An enterprise that chooses to disable DoH should block known DoH resolver IP addresses and domains, so devices on the network will fail to resolve a domain name using DoH and usually revert back to traditional DNS, going through the DNS resolver assigned by DHCP.

Enterprises may monitor encrypted network traffic using TLS inspection. These enterprises should apply signatures in the devices that break and inspect the TLS traffic to block unauthorized DoH requests. Note that the TLS inspection devices must be able to properly decrypt and interpret DoH requests for this to be effective since the decrypted DNS requests would not come over port 53 like traditional DNS requests.

[3] This recommendation is consistent with the DHS requirement for federal networks to only use approved DNS resolvers [6].
[4] Firefox is a registered trademark of Mozilla Foundation.
[5] Chrome is a registered trademark of Google LLC.

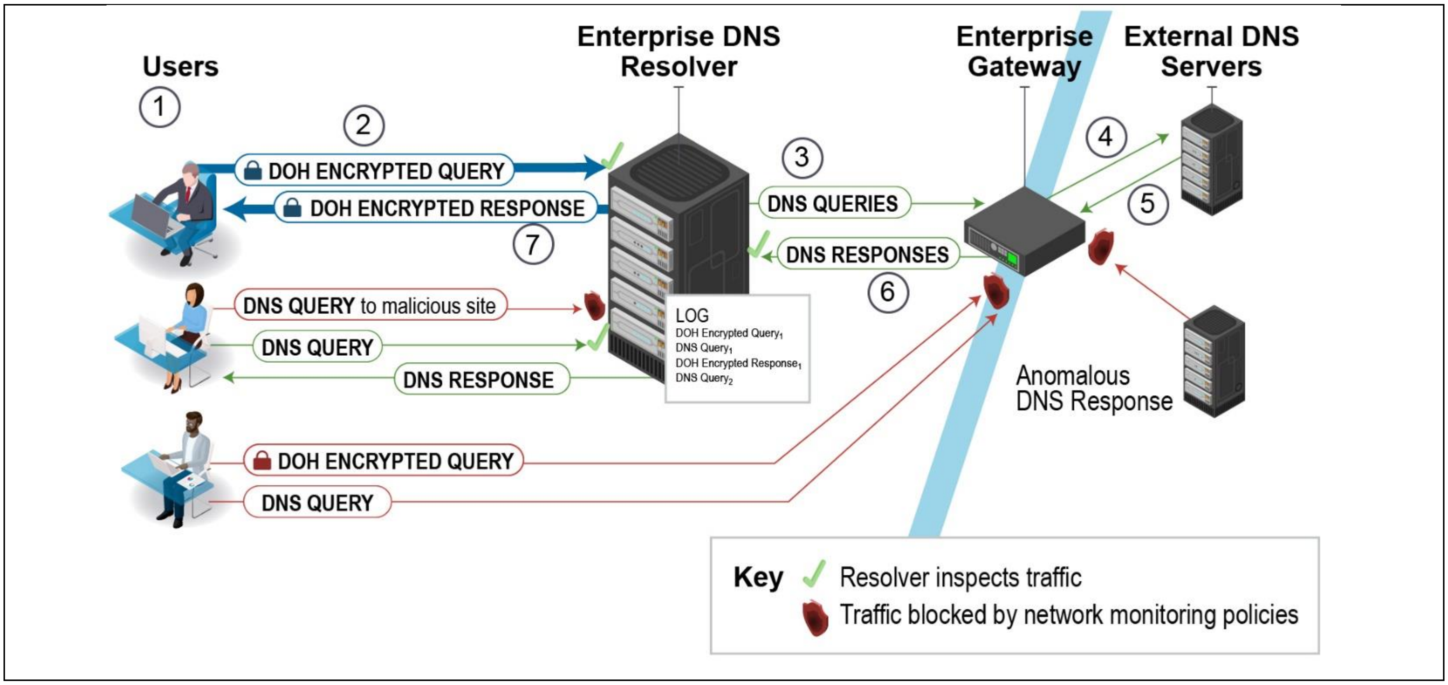

Figure 3: NSA recommended enterprise DNS architecture with DoH

1. The user wants to visit a compromised web site and types the domain into the web browser. The enterprise configuration on the client configures DoH for the enterprise DNS resolver or disables DoH.
2. The DoH request for the domain is encrypted and sent to the enterprise DNS resolver over port 443. The resolver blocks queries that violate DNS monitoring policies and known malicious domains, possibly generating alerts. It responds with an error for the canary domain, signaling to disable all other DoH that has not been properly configured by the enterprise. The resolver also logs requests and responses.
3. If the IP address for the domain is not in the enterprise DNS resolver's cache and the domain is not filtered, it will send a DNS query through the enterprise gateway.
4. The enterprise gateway forwards the plaintext DNS request to an external DNS server. It also blocks DNS, DoH, and DoT requests to external resolvers and DNS servers that are not from the enterprise resolver.
5. The response to the query with the IP address is returned over plaintext back through the enterprise gateway.
6. The enterprise gateway forwards the response back to the enterprise DNS resolver.
7. The DNS resolver validates the DNSSEC information in the response and then returns it as an encrypted DoH response back to the user's web browser, which then requests the webpage from the IP address in the response.

Utilize host and device DNS logs

Enterprises that want to enable DoH should not rely solely on network monitoring tools to inspect DNS traffic. DNS logging on all network devices and hosts can increase the network visibility that is lost with less DNS network monitoring capability. Supplement DNS protection with threat reputation services on a firewall or through an intrusion detection system to help keep up with increasing and changing malicious domains and block known bad traffic.[6]

Consider a VPN for additional privacy protection

Enterprises that are concerned with passive surveillance may use virtual private networks (VPN) or proxies to keep their traffic more private, especially in mobile and teleworking environments. Enterprises that decide to use DoH should avoid using obsolete TLS. Only use current TLS versions to protect against issues in the underlying HTTPS [11].

Validate DNSSEC and use protective DNS capabilities

Enterprises must understand which parts of the DNS process are DoH-protected and account for the unprotected parts and other vulnerabilities. DoH is independent from, but compatible with DNSSEC. Ensure that the enterprise DNS resolver validates DNSSEC to authenticate traffic from other DNS servers. Protective DNS capabilities are an essential

[6] For more information on threat reputation services, please refer to "Integrate Threat Reputation Services" on nsa.gov [10].

part of network defense. When using an external resolver, ensure that the DoH resolver chosen by the enterprise has a reputation for security and reliability.

Balance found: a better sense of security

DoH provides privacy benefits for users, but can present issues to enterprises wanting to achieve governance and DNS traffic monitoring. Enterprises can implement DoH on their DNS service to gain both the benefits of DoH and best practice DNS protections. However, enterprises that allow DoH without a strategic and thorough approach can end up interfering with network monitoring tools, preventing them from detecting malicious threat activity inside the network, and allowing cyber threat actors and malware to bypass the designated enterprise DNS resolvers.▪

Works cited

[1] Sandra Siby, Marc Juarez, Claudia Diaz, Narseo Vallina-Rodriguez, and Carmela Troncoso (2020), Encrypted DNS => Privacy? A Traffic Analysis Perspective. Available at: https://www.ndss-symposium.org/wp-content/uploads/2020/02/24301-paper.pdf

[2] Bert Hubert (2019), Centralised DoH is bad for Privacy, in 2019 and beyond. Available at: https://labs.ripe.net/Members/bert_hubert/centralised-doh-is-bad-for-privacy-in-2019-and-beyond

[3] New Jersey Cybersecurity & Communications Integration Cell (2019), Godlua – NJCCIC Threat Profile. Available at: https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/godlua

[4] The Implications of DNS over HTTPS and DNS over TLS. Available at: https://icann.org/en/system/files/files/sac-109-en.pdf

[5] National Security Agency (2019), Defending Your DNS Infrastructure. Available at: https://www.nsa.gov/cybersecurity-guidance

[6] Cybersecurity & Infrastructure Security Agency (2020), Addressing Domain Name System Resolution on Federal Networks. Available at: https://www.cisa.gov/sites/default/files/publications/Addressing_DNS_Resolution_on_Federal_Networks_Memo.pdf

[7] Mozilla Corporation (2020), Firefox DNS-over-HTTPS. Available at: https://support.mozilla.org/en-US/kb/firefox-dns-over-https

[8] Google LLC (2020), A safer and more private browsing experience with Secure DNS. Available at: https://blog.chromium.org/2020/05/a-safer-and-more-private-browsing-DoH.html

[9] Mozilla Corporation (2020), Canary domain - use-application-dns.net. Available at: https://support.mozilla.org/en-US/kb/canary-domain-use-application-dnsnet

[10] National Security Agency (2019), Integrate Threat Reputation Services. Available at: https://www.nsa.gov/cybersecurity-guidance

[11] National Security Agency (2020), Eliminating Obsolete TLS Protocol Configurations. Available at: https://www.nsa.gov/cybersecurity-guidance

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov