CARBONITE an opentext company | WEBROOT an opentext company

DNS over HTTPS (DoH): Making Sense of the NSA's Recommendation

In January 2021, the NSA released a guide that identified concerns around encrypted DNS, aka DNS over HTTPS (DoH). Although the NSA strongly recommends businesses protect their networks from rogue DNS sources to improve their network security, the question they don't really answer is: **how?**

"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."

– National Security Agency, "Adopting Encrypted DNS in Enterprise Environments"

A Brief History of DNS

In 1983, the domain name system (DNS) was designed to locate servers on the rudimentary networks that were in the process of becoming the internet. Now, it functions as the internet's address book, and is involved in almost every type of internet action. While the original design has scaled to meet the demands of today's internet, the need for addressing privacy concerns is a new challenge that requires innovation.

The Dangers of Unencrypted DNS

Standard, unencrypted DNS has become a popular attack vector for malicious actors who execute DNS hijacking attacks, in which they redirect legitimate traffic to their own malicious servers, allowing them to intercept login credentials and sensitive data (i.e., "man in the middle" attacks). By encrypting DNS traffic, you can prevent these types of attacks and others.

The Upgrade to DNS over HTTPS (DoH)

Also known as DNS 2.0 and encrypted DNS, DoH uses HTTPS to encrypt DNS requests to ensure that each request stays private and is only fielded by the intended DNS server. This, in turn, helps prevent spying, DNS hijacking and other threats.

Encrypted DNS is increasingly being used to prevent eavesdropping and manipulation of DNS traffic. DNS controls can prevent numerous threat techniques used by cyber threat actors for initial access, command and control, and exfiltration. Additionally, since DoH verifies the resolver fielding the request, you can be sure of its integrity.

What the NSA Guide Recommends

In its guide, Adopting Encrypted DNS in Enterprise Environments, the NSA recommends that while encrypted DNS such as DoH has privacy and security advantages, businesses must carefully control available DNS resolvers on their networks and that all other DNS resolvers be disabled or blocked.

The Security Drawbacks of DoH

Because DoH fully encrypts DNS requests, it doesn't just blind malicious actors. It can also hide traffic from IT administrators who manage and filter DNS requests for their organizations. The lack of administrative visibility leads to a lack of control which can pose stability and security issues.

The Path Forward

Since DoH is encrypted and runs on the same port as HTTPS traffic, it is very hard to block or control these requests as the NSA recommends. To do so, you need either need a firewall that is capable of inspecting SSL traffic, which is both expensive and problematic in itself, or the ability to block DoH providers. It's imperative that organizations begin to leverage the security of DoH while staying in control of DNS sources to help secure their network traffic, particularly as more applications support it. For example, Mozilla Firefox, Google™ Chrome and Microsoft® Edge web browsers have all begun introducing DoH for DNS resolution in different capacities.

How to Handle DoH with a DNS Filtering Solution

Although many commercial network/DNS filtering solutions are not yet capable of handling this traffic correctly, the Webroot® DNS Protection agent already secures DNS requests by using DoH for all of its communications.

Privacy and Security with Webroot® DNS Protection

Not only was Webroot® DNS Protection the first DNS security product on the market to support both privacy and security with DoH, it also leverages Webroot BrightCloud® Threat Intelligence to identify and block alternate DoH connections. And, since DoH can obfuscate DNS requests, the solution also lets you echo all DNS requests to your local resolver, providing visibility into the requests being made. That means you can still benefit from the power of DNS filtering with the privacy and security of DoH. By securing remote and on-site users, devices, and networks, Webroot DNS Protection is the simple and effective solution to fulfill the NSA's recommendations.

Next Steps

Start your free trial of Webroot® DNS Protection today at webroot.com.