SOLUTION NOTE

DoT and DoH Present New Challenges

SUMMARY

Securing your DNS infrastructure has never been more critical: More than 90 percent of malware incidents and more than half of all ransomware and data theft attacks rely on the DNS vector. The good news is that two recent and evolving technologies designed to improve DNS privacy are making significant headway. Leading browser organizations have announced go-live plans for introducing DNS privacy in their respective browsers.

The bad news? A vigorous debate over which solution works best, coupled with unintended security consequences of these new technologies. Existing enterprise DNS solutions, such as those Infoblox provides, deliver substantial security benefits to the enterprise. They protect users from malicious actors, provide fast and reliable access to local services and automatically block content that users and network operators deem objectionable or suspicious. These new DNS privacy initiatives are necessary and valuable. However, they inadvertently bypass enterprise DNS solutions to some extent. As a result, they can potentially expose enterprises to unexpected risk, break mission-critical applications, slow browser performance and adversely affect user experiences.

This solution note will help you understand what these new DNS privacy innovations mean for your organization. It also describes the best practices Infoblox recommends for maintaining enterprise control over DNS services and optimizing your users' browsing experiences moving forward.

Room for Improvement

The concept of openness has been a fundamental feature of the Internet since its inception. Although users transmit sensitive information such as credit card numbers, email and passwords between their web browsers and websites using the secure HTTPS protocol, initial requests for Internet addresses and subsequent responses for website locations are transmitted in plain text. As a result, DNS has traditionally suffered from what we describe as a "last mile" security problem. Communications between a DNS client and its local DNS server are almost always unencrypted and therefore subject to spoofing, interception, hijacking and more problems. Improvements have been made to incorporate greater end-to-end security. DNS Security Extensions added authentication and data integrity checking to DNS, but the last leg of communication to the web browser was still open to spoofing.

Introducing DoT and DoH

Industry groups such as the Internet Engineering Task Force (IETF) have proposed two mechanisms to address these issues. They work by encrypting the DNS communication between your operating system's stub resolver and your recursive DNS resolver. One is known as DNS over TLS (Transport Layer Security) or "DoT" and the other is DNS over HTTPS or "DoH." Both technologies ensure data privacy and authentication by encrypting communications between DNS clients and servers. However, in doing so, each points to external DNS resolvers, thereby allowing client devices to access DNS services outside of your control and exposing the enterprise to potential security risk.

DNS over TLS (DoT)

DoT is an IETF standard that uses the common Transmission Control Protocol (TCP) as a connection protocol to layer over TLS encryption and authentication between a DNS client and a DNS server. Functioning at the operating system level, it communicates over TCP port 853. This is a well-known port used for all encrypted DNS traffic, and network administrators are very familiar with it. DoT traffic is encrypted, but its use of a well-understood port makes it easier for network administrators to monitor and control encrypted DNS when it appears. DoT is also a mature standard backed by traditional players in the DNS industry.

DNS over HTTPS (DoH)

Backed by the Mozilla Foundation and Chromium Projects, DoH is the other IETF security protocol that addresses DNS client and DNS server communication security. It leverages the security protocol extension HTTPS to provide encryption and authentication between a DNS client and server.

A potential problem with DoH is that it uses the same TCP port (443) that all HTTPS traffic uses. As a result, it might prove difficult to troubleshoot DoH-related DNS issues because of the inability to distinguish DoH-based DNS requests from regular HTTPS requests. For example, if a network administrator is employing DNS monitoring to block DNS requests to known malicious domains, he or she would not see those particular requests in HTTPS. Hence, that malicious traffic would go undetected.

In addition, DoH operates at the application layer rather than the operating system, which introduces the potential for browser traffic to bypass enterprise DNS controls. The circumvention of DNS controls could hamper the support team's ability to maintain the levels of network performance, security, scale and reliability that enterprises demand from DNS.

DoT and DoH Enterprise Challenges

Network and security administrators rely on DNS as a significant element of the network control plane to ensure fast application access and keep users safe from malware and other Internet-borne threats. Notable challenges that networking and security teams may face as a result of the new DoT and DoH standards include:

- **Centralized DNS:** External control of DNS can allow clients to use centralized DNS resolvers controlled by third-parties and not provided by IT, introducing risk and making it potentially harder to manage and secure network resources effectively.

- **Bypassing of enterprise controls:** DoH specifically introduces the potential for hundreds of applications, each with its own unique DoH settings, to bypass DNS controls. Aside from complicating monitoring for such DNS exploits as DNS hijacking, DoH also has the potential to enable the bypassing of enterprise content filters, such as adult content, gaming, streaming and malware sites.

- **Exposure to data exfiltration and malware proliferation:** Cybercriminals use DNS as a backdoor to obtain and exfiltrate sensitive information and to spread malware through command and control (C&C) communications with devices. Security teams can stop these attacks effectively by using threat intelligence on internal DNS infrastructure combined with analytics based on artificial intelligence and machine learning. And yet, because DoH bypasses any DNS security measures in place, enterprises remain exposed to these and other pervasive DNS-based threats.

- **Increased DNS server overhead/decreased DNS server performance:** DoT and DoH increase the load each DNS query places on a DNS server and can affect a user's quality of experience. Traditional DNS is based on the User Datagram Protocol and introduces minimal overhead. Both DoT and DoH run over TCP, which is more resource-intensive for a DNS server. Also, both DoT and DoH require the DNS server to decrypt the query and encrypt the response, further adding to the overhead on the DNS server. Administrators of DNS servers should expect to find that their servers can handle only a fraction of the DoH- and DoT-based query rate they could with traditional DNS queries.

Differing Rollout Plans

Many public recursive DNS providers, such as Google DNS, Cloudflare and Quad9, include DoT and DoH as part of their offerings. Many operating system clients must opt into DoT (although many Android clients are configured to use DoT by default). In the case of DoH, however, web browsers such as Chromium and Mozilla each require their own methods for clients to attach.

Chromium

The Chromium implementation of DoH will affect all browsers based on the Chromium Project, including Google Chrome, Microsoft Edge and Opera. Chromium plans to default to an automatic mode that will probe a supported list of operating system–configured resolvers for DoH availability, and then use the configured resolver for DoH only if it's available. It also plans to observe the DoT operating system client settings in Android and behave in a controllable and predictable manner. For most Infoblox customers, Chromium's changes may not obligate you to change your resolver or network.

Mozilla

Mozilla will attempt to detect and disable the use of DoH when it deems it necessary. Unfortunately, the methods used in accomplishing this are not yet proven and may not fit all situations. Some enterprises may lack full control over the browsers installed in their organization. For example, it may prove difficult to ensure compliance with company preferences for browser settings across BYOD, work from home and other mobile scenarios. Similarly, communications service providers with their diverse end users will have even less influence over browser settings on network devices.

Conclusion

As the industry leader in Secure, Cloud-Managed Network Services, Infoblox maintains that circumventing internal DNS infrastructure is always a bad idea. These new DNS privacy options are just beginning to unfold. Accordingly, enterprises should take steps now to reduce the risks these technologies pose. A good place to start is by blocking direct DNS traffic—including DoT and DoH—between internal IP addresses and DNS servers on the Internet (Figure 1). This step will ensure that end users employ their company's internal DNS infrastructure, allowing their IT organization to comprehensively apply DNS resolution policy and troubleshoot problems.

Infoblox considers solving DNS's "last mile" problem an important and worthwhile effort and is working with our partner, the Internet Systems Consortium, toward supporting DoT and DoH in future versions of BIND and Infoblox's NIOS. Meanwhile, we encourage customers to leverage Infoblox best practices to help them maintain control of their DNS and mitigate unforeseen downstream problems from new DNS privacy initiatives. Those seeking more information are welcome to visit the Infoblox Community to learn about these evolving technologies and Infoblox solutions.

And finally, if you want to influence how these new privacy options are configured and to promote the proper adoption of encrypted DNS protocols, we encourage you to join us and others in the Encrypted DNS Deployment Initiative at encrypted-dns.org.

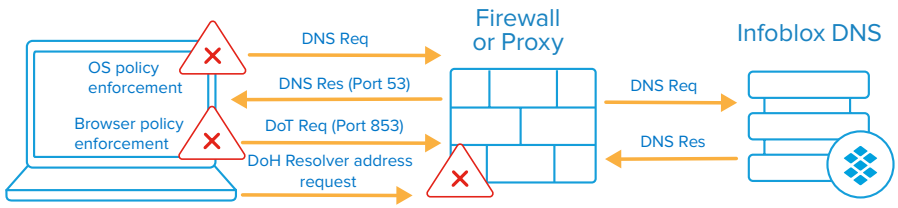

Figure 1: How to block DoT and DoH

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com