SOLUTION NOTE

# SOLVING UNINTENDED SERVICE PROVIDER CHALLENGES WITH DoT AND DoH

## SUMMARY

**Securing your DNS infrastructure has never been more critical: Over 90 percent of malware incidents and more than half of all ransomware and data theft attacks rely on the DNS vector.**

The good news? Two new and evolving technologies designed to improve DNS privacy are making significant headway.

The bad news? These technologies direct servers and applications to external DNS resolvers, allowing subscriber devices to sidestep traditional DNS mechanisms to DNS services outside of your control. And these changes are happening right now. As a result, they can expose subscribers to unexpected risks, 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 how Infoblox provides communications service providers with solutions that solve these DNS privacy challenges to maintain control over DNS services and optimize your subscribers' Internet experiences.

## OVERVIEW

Created over 30 years ago, DNS (Domain Name System) is an Internet protocol that converts human-readable names to IP addresses, changes IP addresses back to names and provides easy-to-remember names for many Internet-based services, such as email. When subscribers visit a website, they typically enter the web address into a browser, and the site is loaded. Flash forward to today: This same system is still much in use. As subscriber devices come online, they will need to connect to Internet services.

### Communications Service Provider Use of DNS Query Data

Communications service providers (CSPs) can use the information gained from DNS query data for a variety of useful purposes. For example, CSPs can determine the geographically closest instance of websites that subscribers seek to deliver content faster. Through DNS content filtering, CSPs can protect children in homes, schools and libraries from accessing harmful or objectionable content. CSPs also rely on DNS query data to comply with law enforcement requests for subscriber Internet activity records. In addition, DNS information can defend the network and subscribers from evolving cyber threats.

### Room for Improvement

The original DNS design did not take security into account, because DNS queries were sent unencrypted. Besides monitoring the IP address that users were visiting, any party between the browser and the resolver can discover which websites users are seeking–even if the website's content is encrypted. DNS queries can also be hijacked or spoofed, diverting users from intended to malicious websites.

While DNSSEC addresses many of the security shortcomings of the traditional DNS design, especially in server-to server communication, it falls short in adequately addressing the "last mile" problem, the communication between a DNS client (such as a mobile phone) and its nearest DNS server (such as the corporate or ISP DNS server).

## INTRODUCING DoT AND DoH

To fill this significant gap in the "last mile," many competing technologies have emerged. While these technologies try to bring privacy between DNS clients and servers, they have one thing in common: They are proprietary and not standardized. Industry groups working within 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 or a local application 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. While DoT and DoH were designed to address DNS privacy issues, they also introduce significant DNS behavior changes to how browsers and applications function. These changes create additional complexity and unintended network security consequences and directly affect enterprise delivery of security and content filtering services. DoT and DoH can point servers and applications to external DNS resolvers, allowing client devices to sidestep traditional DNS mechanisms to DNS services outside of your control and expose subscribers to potential security risks and negative customer experiences. Case in point: The United States National Security Agency (NSA) recently posted guidance that organizations host their own DoH resolvers and avoid sending internal DNS traffic to external third-party resolvers.

## 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. Often functioning at the operating system level, it communicates over TCP port 853. This well-known port is 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.

A potential problem with DoH is that it uses the same TCP port (443) that all HTTPS traffic uses. It might prove challenging to troubleshoot DoH-related DNS issues because of the inability to distinguish DoH-based DNS requests from regular HTTPS requests. For example, if CSPs are employing DNS monitoring to block DNS requests to known malicious domains, they would not see those requests in HTTPS. Hence, that malicious traffic would go undetected.

Also, DoH is often implemented at the application layer rather than the operating system, which introduces the potential for browser traffic to bypass 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 subscribers expect from DNS.

## DoT AND DoH SERVICE PROVIDER CHALLENGES

Service providers have invested heavily in their networks to ensure a safe, reliable and fast network experience for their subscribers. They rely on DNS as a significant element of the network control plane to ensure rapid application access and keep users safe from malware and other Internet-borne threats.

From a performance perspective, latency matters more than ever. Slow DNS resolution times lead to a bad subscriber experience through longer page load times and sluggish application responses, creating the perception that the network is slow. Many CSPs must supply Internet content filtering from the perspective of protection, such as opt-in content protection for minors and malware/security protection for enterprises and public safety organizations, and leverage DNS to furnish efficient yet comprehensive subscriber protections.

Unique challenges that CSP networking and security teams may face because of these new DNS standards include:

### The proliferation of centralized cloud DNS providers:

Service providers maintain their DNS infrastructure, and the shift of DNS to centralized, external cloud DNS providers creates numerous competitive, user experience and legal concerns. While subscribers have been free to optionally leverage alternate DNS providers other than the CSP's solution, DoH explicitly introduces the potential for a proliferation of resolvers maintained by various entities.

While implementing DoH currently relies on a handful of centralized cloud DNS services at the web browser, it is widely expected that applications will soon be developed that can bind themselves to a specific cloud DNS resolver of a developer's choosing.

### Lack of DNS traffic visibility:

Using external cloud DNS also creates numerous user safety and regulatory concerns because CSP DNS servers will no longer be in the path of subscriber DNS requests. Since DoH traffic is encrypted and indistinguishable from regular HTTPS traffic, CSPs will have no subscriber DNS traffic view. They cannot offer DNS-based network-level content filtering and protection.

- Blocking the resolution of malicious and illegal content is a significant concern. Implementing regulatory obligations is challenging or impossible when there is no business relationship or legal authority over a company outside of the CSP's network or traditional territory. And complying with law enforcement requests for DNS query information will be complicated if SPs no longer have access to DNS query data. Law enforcement agencies will need to know which DoH resolver subscriber browsers and applications are using. Even then, these resolvers may not be retaining this information or be in the same jurisdiction necessary to comply with the request.
- DoH implementations outside SPs' networks inhibit content filtering controls that many subscribers rely upon, preventing SPs from offering subscriber-facing services like parental controls, advertisement blocking, enterprise content filtering, public Wi-Fi protection and other DNSbased security services. They also introduce the potential for hundreds of applications and websites, each with its own unique DoH settings, to bypass DNS controls. Without visibility into DNS query data, households with children will need to set up and manage parental controls on a per-device, per-application basis. This challenging prospect could lead to inconsistent user experiences, especially considering the potential number of devices.

### Competitive concerns:

Cloud DNS providers create numerous competitive, user experience and performance concerns. Some of the cloud DNS providers are owned by content delivery networks and other large technology companies. Sometimes, the cloud DNS providers may be direct competitors to the service provider or each other. If problems arise, regulators may have little or no influence over commercial issues between the cloud DNS provider and their competitors or customers. For example, competitors could route each other's traffic to slower-responding sites or take other liberties with the user experience.

### Performance concerns:

DNS is the first message in most IP conversations, so low latency is critical to user experience. Routing DNS off the CSP network will always make the DNS experience slower. CSP DNS servers are closer to the subscriber because they operate within the network, and these servers employ DNS caching to ensure optimal low latency performance. Using cloud DNS may affect subscriber performance since DoT and DoH DNS requests will need to travel off-network. Customer experience will also be affected if DoT and DoH block DNS information commonly used by CSPs to route subscribers to local content.

In addition, using centralized cloud DNS resolvers may affect subscribers' Internet performance by complicating content delivery. To deliver content more quickly, content delivery networks (CDNs) host multiple web content instances on geographically dispersed servers. DNS is used to optimize connectivity to streaming video caches and other content based on the client computer's IP address. In using DoT and DoH, how CDNs localize clients (meaning, the ability to direct traffic to the most geographically optimal CDN caching node) is affected. If CSPs cannot view subscriber DNS queries, they may not be able to route subscribers to the geographically closest or most efficient CDN node.

### Customer service impacts:

DoH creates unique support problems for the service provider. Many CSPs use DNS redirects for their subscribers to enhance their service support. Minimally, CSPs commonly show redirect pages when subscribers enter invalid DNS names in web requests. Redirects may be used to kick off device self-provisioning or provide broadband account support. Because the most common implementation of DoH occurs between the browser and a cloud DNS provider (and not the OS resolver and the CSP's DNS service), support teams will need to be trained to identify if DoH clients are installed or browser-level settings have been altered. For example, how will support agents handle situations where applications running on user equipment might behave differently than when being run via a web browser or an application running on the user equipment OS? Will they route issues to the third-party DoH provider?

### Privacy concerns:

From a privacy standpoint, centralized cloud DNS resolver services are implemented worldwide rather than within a specific country or region. Instead of residing within the CSP network, subscriber DNS metadata is sent externally and sometimes out of the country to for-profit cloud service providers. DoT and DoH DNS traffic can still be subject to observation, spying or other alteration based on governments' legal orders outside of the CSP's territory. Additionally, while these cloud DNS resolver services have published privacy policies stating that DNS resolution data will not be used for commercial purposes, DNS's centralization to several large, third-party companies whose business model includes collecting and leveraging user-related data may introduce unforeseen issues for subscribers and CSPs. Consider this: DoH resolvers can identify specific users and what sites they are visiting on the Internet.

### Exposure to data exfiltration and malware proliferation:

If uncontrolled, DoH can increase exposure to data exfiltration and malware proliferation because it can open back doors to protected networks. Cybercriminals often use DNS as a back door to obtain and export trade-sensitive information and spread malware through command-and-control (C&C) communications with devices. Therefore, the DoH DNS request is encrypted and invisible to third parties, including cybersecurity software that may rely on passive DNS monitoring to block requests to known malicious domains. Typically, security teams can effectively stop these attacks by using threat intelligence on internal DNS infrastructure, combined with analytics based on artificial intelligence and machine learning. Because DoH bypasses these DNS security measures, there is new potential for enterprises to become exposed to these and other DNS-based filters.

For example, recent versions of PsiXBot malware use DoH to encrypt malicious communications, allowing it to hide in regular HTTPS traffic and install malware that can steal data or add a victim to a botnet.

## DIFFERING BROWSER AND OPERATING SYSTEM ROLLOUT PLANS

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

### Chromium

The Chromium implementation of DoH affects all browsers based on the Chromium Project, including Google Chrome, Microsoft Edge and Opera. Chromium defaults to an automatic mode that probes a supported list of the OSconfigured resolvers for DoH availability. It then uses the configured resolver for DoH only if it's available. It also plans to observe the DoT OS 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 offers Cloudflare as its default trusted recursive resolver using DoH. Mozilla will attempt to detect and disable the use of DoH when it deems it necessary. Unfortunately, the methods used in accomplishing this process 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.

### Apple

Apple's recently released versions of iOS and macOS support both DoT and DoH protocols. These settings can be applied selectively, ranging from the entire operating system through MDM profiles or a network extension to individual applications or selected network requests of applications.

According to Apple, there are three ways to enable encrypted DNS. One option can apply system-wide encrypted DNS settings. Users or administrators can choose a single encrypted DNS server as the default resolver for all OSs' applications. Developers can write network extension applications that configure the OS to use that server or MDM profiles can be pushed to clients who configure encrypted DNS settings. If this option is not used, the other two options are automatically enabled, and the device owner cannot directly disable them.

The second option is for domain owners. They can configure settings at the domain level that message the existence of an encrypted resolver for the domain. If these settings are detected and verified, the DNS traffic for that domain is rerouted to the domain-provided encrypted resolver.

The final option is encrypted DNS at the application layer. Here, developers can create applications that allow applications to use DoT and DoH directly from individual apps. With this option, developers can select a specific server for some or all of their application connections when the OS is not configured.

Apple plans to warn users with a specific message should a particular network block encrypted DNS communications on the network by policy. Particular networks will be visually marked with a privacy warning, and applications configured to use specific DoH resolvers will not communicate properly.

### Microsoft

Microsoft devised its approach under the premise that users should not require specialized knowledge to use DoH while allowing network administrators to retain control by permitting fallback to the traditional DNS protocol.

When configured, the DNS client will operate in "opportunistic mode," which means that it will attempt to use the DoH protocol instead of the traditional DNS. However, the client can be configured to fall back to conventional DNS if DoH protocols are unavailable or not responding. Initial DoH trusted resolvers would consist of Cloudflare, Google and Quad9.

## INFOBLOX SOLVES DoT AND DoH CHALLENGES

As the industry leader in Secure, Cloud-Managed Network Services, Infoblox maintains that circumventing existing DNS infrastructure increases operational complexity. These new DNS privacy options are just unfolding. Organizations should take steps now to reduce the risks these technologies pose. Minimally, an excellent place to start is by blocking direct DNS traffic—including DoT and DoH—between opt-in malware blocking or content control subscriber IP addresses and DNS servers on the Internet (Figure 1). This step will ensure that subscribers employ their CSPs' DNS infrastructure, allowing the organization to apply a DNS resolution policy on a per-subscriber basis and troubleshoot problems. Infoblox provides organizations with solutions that solve these DNS privacy challenges. Through the ability to block access to external DNS resolvers and provide internal encrypted DNS resolution, CSPs can maintain control over DNS.

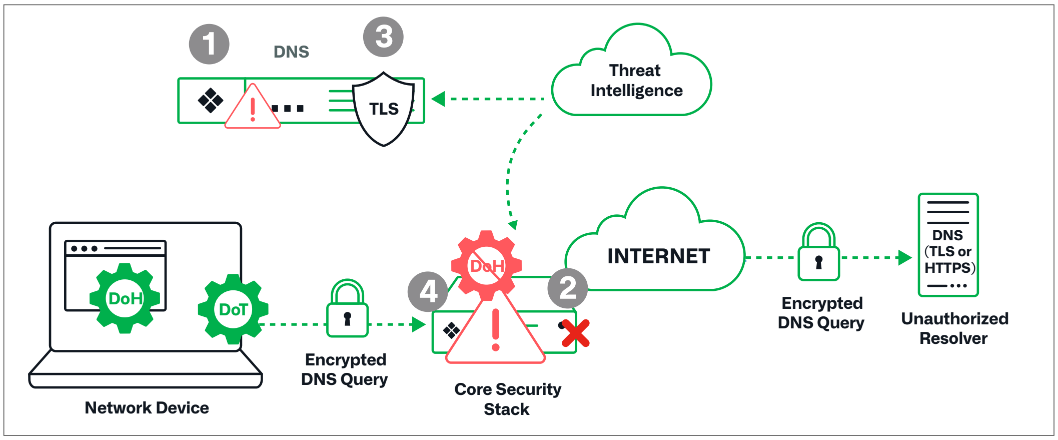

*Figure 1: DoT/DoH Best Practices protect your users and devices*

### Block Resolution to DoH Domains

BloxOne® Threat Defense, a hybrid foundational security solution from Infoblox, uses DNS as the first line of defense. It blocks resolution to DoH domains and facilitates a graceful fallback to existing internal DNS. These capabilities help prevent DoH misuse and mitigate risk.

BloxOne Threat Defense includes several features to help manage DoH:

- Policy threat intelligence feeds for DoH supply network administrators the ability to control the DNS access method used to detect and mitigate threats by disabling DoH-based security policies. Browsers will gracefully fall back to the organization's managed DNS without interrupting user activity.
- A DoH policy feed for known DoH IPs and DoH domains has been added to Threat Intelligence Data Exchange, Infoblox's threat intelligence aggregation and distribution platform. Other security tools, like NGFWs, can then use this data feed and related intelligence to block DoH traffic to external servers.
- Users can review DoH-related domains and IPs within Dossier, Infoblox's threat investigation tool.

These capabilities are available for all BloxOne Threat Defense subscription levels.

## INFOBLOX ENCRYPTED DNS FOR SERVICE PROVIDERS

Infoblox Network Identity Operating System (NIOS) is the OS that powers Infoblox core network services, ensuring the network infrastructure's continuous operation.

Infoblox Encrypted DNS for Service Providers is a NIOS feature that provides efficient encryption while delivering Infoblox best-in-class DNS and value-added subscriber services. Launch capabilities include support for DoH and DoT.

Infoblox Encrypted DNS delivers a unique approach to encrypting your DNS traffic. Unlike methods that rely on load balancers or over-provisioning, Infoblox Encrypted DNS runs as a single service for all of your DNS needs. Our standard features—including DNS Cache Acceleration, Advanced DNS protection, high-speed query logging and subscriber value-added services—are all available from the same CSP scale DNS service.

### The Infoblox Advantage: Ultra-Low Latency

Designed for CSP environments requiring scalable edge deployments and available in multiple form factors, including orchestrated VNFs and cloud-native containerized software solutions, Infoblox solutions are designed to handle the "perfect storm" of future 5G and edge-based applications. We offer ultra-low latency of 50 microseconds on average, scaling to millions of devices with ultra-high five-9s reliability.

Infoblox Encrypted DNS enables Infoblox to encrypt last-mile DNS communications between their endpoints and DNS servers regardless of which protocol the endpoint supports while solving performance concerns associated with the additional overhead related to encrypted DNS communications. From the same service, we allow CSPs to accommodate encrypted DNS with microsecond latency when the connection is already established while all other DNS features are running.

## CONCLUSION

Infoblox is committed to helping customers maintain the network performance, security, scale, and reliability that modern enterprise networks demand. These changes are happening right now as recent browser updates and operating system releases deploy these changes on networks today. While solving the "last mile" problem is essential and worthwhile, we also recognize that service providers must maintain visibility and control over their DNS traffic. Prominent security agencies, including the NSA, recommend that organizations take steps to reduce the risks these technologies pose. CSPs can leverage Infoblox solutions to maintain control of their DNS and mitigate unforeseen downstream problems from new DNS privacy initiatives. For more information, visit the Infoblox Community to learn about these evolving technologies and Infoblox solutions.

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.

infoblox

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

**Corporate Headquarters**
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

© 2024 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).

Version:20240322v1