Infoblox

SOLUTION NOTE

Solving Unintended 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 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 the enterprise to potential security risks. And these changes are happening right now.

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, organizations can maintain control over DNS.

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. While past improvements have been made to incorporate greater end-to-end security, the last leg of communication to the web browser was still open to spoofing.

Introducing DoT and DoH

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 direct servers and applications to external DNS resolvers, allowing client devices to sidestep traditional DNS mechanisms to DNS services outside of your control and expose the enterprise to potential security risks. 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.

DNS over HTTPS (DoH)

Backed by Apple, Microsoft, 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. 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 requests in HTTPS. Hence, that malicious traffic would go undetected.

In addition, DoH is often implemented 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 because 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 and websites, each with its own unique DoH settings, to bypass DNS controls. Aside from complicating monitoring for such DNS exploits as DNS hijacking, DoH could also enable the bypassing of enterprise content filters, such as adult content, gaming, streaming and malware sites.
- **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 to spread malware through command-and-control (C&C) communications with devices. The DoH DNS request is encrypted and, therefore, 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 stop these attacks effectively 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 be 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.

- **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 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 operating system clients must opt into DoT (although many Android clients are configured to use DoT by default). With DoH, however, 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 operating system–configured resolvers for DoH availability and 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 a graceful fallback to traditional DNS resolution 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 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, where users or administrators can choose a single encrypted DNS server as the default resolver for all applications on the operating system. Developers can write network extension applications that configure the OS to use that server, or MDM profiles can be pushed to clients that 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 messages 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. This option means that 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. Specific networks will be visually marked with a privacy warning, and applications configured to use specific DoH resolvers will not communicate properly.

Microsoft

Microsoft announced its intention to support DoH in 2019 and has adopted DoH in the Windows DNS client, with the option of supporting DoT in future versions. 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 internal 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 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 apply a DNS resolution policy comprehensively 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, organizations can maintain control over DNS.

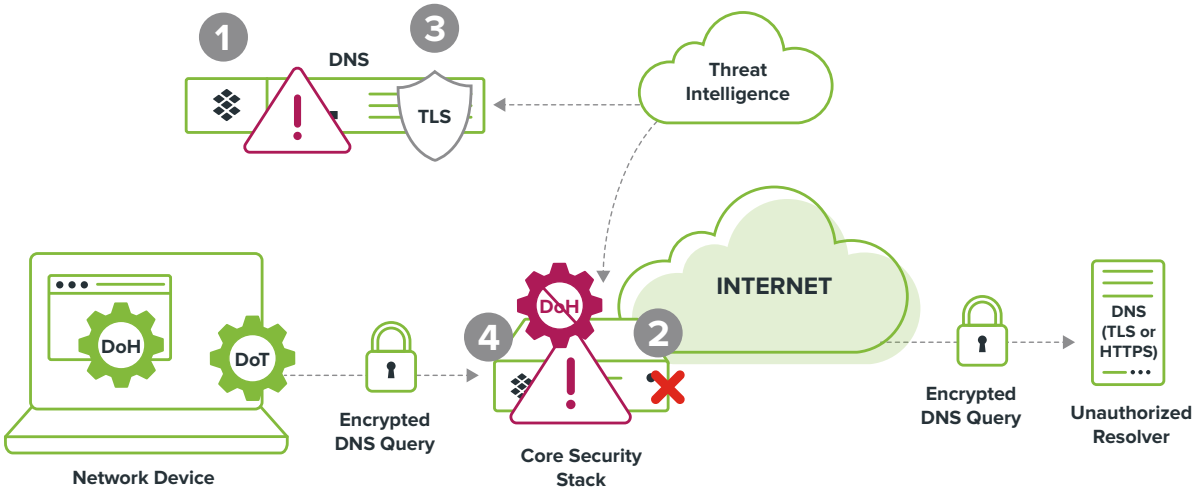

Figure 1: DoT/DoH Best Practices protects your users and device

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

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

Infoblox Encrypted DNS is a NIOS feature that provides efficient encryption while delivering Infoblox best-in-class DNS 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 Advanced DNS protection and DNS Cache Acceleration, are all available from the same highly scalable DNS service.

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 enterprises 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. Customers 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.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com