DATASHEET

Strengthening Federal Cybersecurity with Encrypted DNS

Implementing Encrypted DNS in Compliance with the White House Executive Order

OVERVIEW

In recent guidance, the White House issued a comprehensive Executive Order (EO) aimed at strengthening and promoting the Nation's cybersecurity. The EO seeks to enhance cybersecurity by improving accountability for software and cloud service providers, strengthening Federal communications and identity management systems, and promoting the use of emerging technologies across executive departments and agencies. Notably, among the key measures introduced is the requirement for encrypted DNS protocols that ensure the confidentiality and integrity of DNS traffic. This recognizes DNS as a critical frontline security control, emphasizing its significance in cybersecurity defense-in-depth strategy.

In line with recent federal cybersecurity mandates, Infoblox Advanced DNS Protection (ADP) provides strong support for encrypted DNS traffic, ensuring the confidentiality and integrity of DNS communications. This capability is essential for federal agencies that seek to improve their cybersecurity measures and comply with the latest White House Executive Order on Encrypted DNS.

Infoblox's solutions are comprehensive, scalable, and easy to implement, allowing for a smooth transition to encrypted DNS with minimal disruption. Importantly, over 15 U.S. federal civilian agencies are utilizing Infoblox DNS encryption, which is included in Advanced DNS Protection. This adoption is helping them make progress on the zero-trust security policy mandate by enabling DNS encryption in support of their Zero Trust initiatives.

AGENCY CHALLENGES

Encrypted DNS requires additional computing resources, particularly on DNS servers, because it requires performing encryption and decryption when sending and receiving DNS messages. Agencies should anticipate this and ensure that their DNS servers have sufficient resources to handle the query load before beginning any widespread deployment of encrypted DNS. Failure to adequately implement encrypted DNS could harm the entire networks, their applications and users.

Encrypted DNS may also make troubleshooting more difficult because IT staff using network troubleshooting tools won't have ready access to the contents of DNS queries or responses. The contents of DNS queries and responses will still be available to IT staff on the name servers themselves, of course, because those name servers will have performed the requisite decryption.

KEY CAPABILITIES

Supports Cybersecurity Mandates
Ensures adherence to the latest federal cybersecurity guidelines.

Encrypted DNS Traffic Support
Supports DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) for secure and authenticated DNS communications.

Advanced Threat Protection
Define and maintain address blocks and routing realms for NIOS and cloud tenants.

High-Speed Query Logging
Captures and logs DNS traffic in real-time without significant performance tradeoff.

Scalable and Reliable
Ensures efficient management of high volumes of DNS and DHCP traffic with exceptional scalability and reliability.

To overcome these challenges and ensure cyber resiliency, agencies should limit the co-existence of multiple mission-critical services on a single system. Given the increased computational requirements required, this separation of duties will provide the highest possible resilience, given the increased computational requirements. The infrastructure hosting the DNS service should be dedicated to that task and hardened for this purpose to reduce the attack surface and ensure that adequate system resources are available to the DNS service. The infrastructure should include sufficient capacity for elements of the DNS service such as logging, support of encrypted DNS protocols and Protective DNS, where applicable. This may be easier to accomplish on purpose-built DNS services, either as-a-service or via virtual or physical appliances.

INFOBLOX ADVANCED DNS PROTECTION

As a leader in secure DNS solutions, Infoblox is uniquely positioned to assist federal agencies in meeting these new requirements. Infoblox Advanced DNS Protection (ADP) is a software subscription add-on to various Infoblox Trinzic hardware and software appliances. It supports encrypted DNS protocols such as DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT), making it suitable for both on-premises and cloud environments. Additionally, ADP is a comprehensive security solution designed to protect DNS infrastructure from a wide range of threats, including DDoS attacks, malware, and data exfiltration. It enables agencies to safeguard DNS integrity and prevent both external and internal DNS DDoS attacks across on-premises, private, and public cloud environments.

Encrypted DNS Traffic Support

- DNS-over-HTTPS (DoH): ADP supports DoH, which runs DNS traffic over HTTPS, leveraging the widespread adoption and security of HTTPS to protect DNS queries and responses.
- DNS-over-TLS (DoT): ADP also supports DoT, which uses Transport Layer Security (TLS) to encrypt DNS traffic. This protocol ensures that DNS communications are secure and authenticated.

Advanced Threat Protection

ADP provides advanced threat intelligence, automated threat mitigation, and real-time visibility into DNS traffic, ensuring the integrity and availability of DNS services.

- Continuously monitors, detects and stops all types of DNS attacks—including volumetric attacks and non-volumetric attacks, such as DNS exploits and DNS hijacking—while responding to legitimate queries.
- Maintains DNS integrity, which DNS hijacking attacks can compromise.
- Infoblox ADP leverages Threat Adapt™ technology to automatically update protection against emerging threats, using independent analysis and research, while adapting to DNS configuration changes.

High-Speed Query and Response Logging

ADP includes high-speed DNS query and response logging, which is essential for capturing and analyzing DNS traffic in real time. Designed to be fast and lightweight, it provides a quick, flexible method for capturing and logging DNS traffic without significant performance tradeoffs.

- Unlike I/O-intensive query and response logging, dnstap operates asynchronously, allowing high-speed query logging with minimal performance loss.
- It uses dnstap to buffer information directly from the DNS server within a flexible binary structured log format and then streams this data to a receiving server.
- Agencies can leverage big data tools to analyze this data (and even combine this data with other sources) to build a comprehensive picture of network usage patterns.

Scalability and Reliability

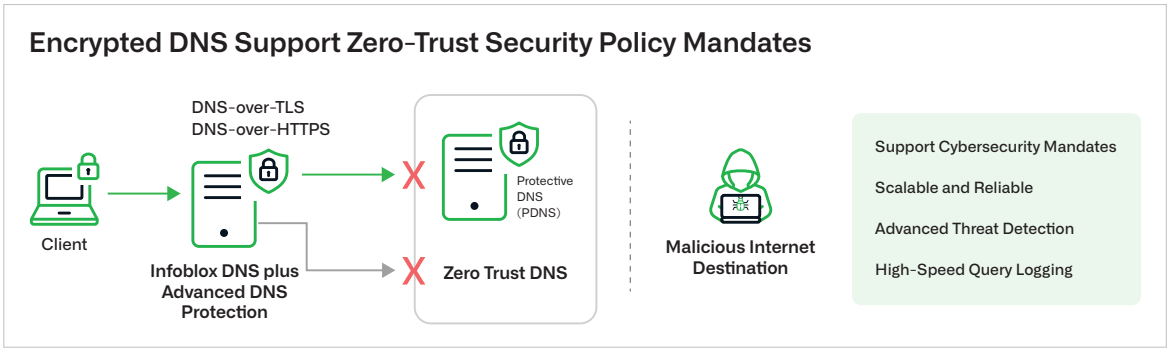
The latest Infoblox Trinzic appliances are designed to deliver exceptional scalability and reliability, making them ideal for federal agencies with demanding network requirements.

- Designed to support future network demands, leveraging Infoblox's latest innovations in networking and security advancements.
- 50% performance enhancement in DNS queries per second (QPS) and DHCP leases per second (LPS) ensure efficient management of high volumes of DNS and DHCP traffic.
- Easier to deploy and manage across distributed architectures ensures network resilience and scalability.
- Includes previously licensed functionality for Infoblox's Cloud Platform (CP) API, DNS Firewall (DFW) RPZ support, and DNS Traffic Control (DTC) integrated global server load balancing.

Deployment Options

- ADP is scalable, easy to deploy, and helps agencies enhance their cybersecurity posture by safeguarding their DNS infrastructure. Agencies can deploy Infoblox DNS servers with the ADP feature enabled to implement encrypted DNS traffic support.
- This deployment can be on-premises, in the cloud, or in a hybrid environment, providing flexibility to meet various operational needs.

For more information on how Infoblox can help your organization implement encrypted DNS, contact the Infoblox team at scsprogram@infobloxfederal.com or their account representatives directly for additional information.



CALL TO ACTION

Federal agencies are urged to prioritize DNS security by adopting Infoblox Advanced DNS Protection (ADP) in response to the recent White House Executive Order. This order mandates the use of encrypted DNS protocols, recognizing DNS as a critical frontline security control. By implementing ADP, agencies can ensure the confidentiality and integrity of their DNS traffic, protecting against potential cyber threats. Infoblox's comprehensive and scalable solutions support DNS-over-HTTPS and DNS-over-TLS, making the transition to encrypted DNS seamless and effective.

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

Version: 20250203v1