TLP:CLEAR

ENCRYPTED DNS IMPLEMENTATION GUIDANCE

Version: 1.0

Publication: April 2024

Cybersecurity and Infrastructure Security Agency

TLP:CLEAR

REVISION HISTORY

Version	Summary of revisions	Edited By	Date
1.0	Baseline version	A&E COE	02/09/2024

CONTENTS

EXECUTIVE SUMMARY

This document is intended to provide implementation guidance for federal agencies to meet federal requirements related to encryption of Domain Name System (DNS) traffic and enhance the cybersecurity posture of their IT networks, as set forth in Office of Management and Budget's (OMB) Memorandum M-22-09.[1] The Memorandum sets forth a "zero trust" cybersecurity strategy for Federal Civilian Executive Branch (FCEB) agencies. Among other requirements, the Memorandum specifically calls for agencies to use encrypted DNS traffic where technically feasible. Agencies are also required to use CISA's Protective DNS capability for all egress DNS resolution, per both M-22-09 and 6 U.S.C. § 663 Note, *Agency Responsibilities*. Broadly, this document is designed to guide agency network practitioners and assist with implementation of currently feasible technical capabilities to help ensure the following:

1. Agency DNS infrastructure uses CISA's Protective DNS service as their upstream provider.
2. Agency networks are configured to prevent endpoint devices and applications from directly communicating with third-party DNS providers, whether using traditional DNS protocols or the new encrypted DNS protocols.
3. Agency DNS infrastructure supports the use of encrypted DNS when communicating with agency endpoints, where technically supported.
4. That agency roaming or nomadic endpoints are configured to resolve endpoint DNS requests through either agency internal DNS infrastructure or Protective DNS (using Secure Access Service Edge (SASE) and/or Security Service Edge (SSE) or similar solutions). Alternatively, agencies may require roaming or nomadic endpoints to VPN into agency environments to ensure they perform appropriate DNS resolution – though this may cause performance problems for those endpoints.
5. Agency cloud deployments are, where technically supported, configured to use authorized DNS providers (i.e., agency internal DNS infrastructure or Protective DNS) with encrypted DNS protocols, and to prevent unauthorized DNS traffic to third-party DNS providers.
6. Agency on-premises endpoints have policies configured to ensure their applications and operating systems are using authorized DNS configurations (i.e., encrypted DNS with agency internal DNS infrastructure, or SASE/SSEE solutions) and policies that explicitly disable application-level DNS resolution unless using agency internal DNS infrastructure.

To help agency personnel understand the requirements and engage in the transition work, this document provides an array of resources:

- An *implementation checklist* provides a nonprioritized, high-level view of the required changes, with individual action items organized by asset category.
- Phased *implementation recommendations* to help prioritize implementation of the checklist.
- Technical guidance and references to support the implementation of the changes in the checklist.

This document offers guidance outlining possible ways to meet the requirements based on the current agency and vendor landscapes as well as the current functionality available in CISA's Protective DNS.

While this document is primarily intended for FCEB agencies, other organizations may find it a useful resource for their own zero trust efforts.

[1] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

1. BACKGROUND

On January 26, 2022, OMB released Memorandum M-22-09,[2] the Federal Zero Trust Strategy, in support of Executive Order 14028, "Improving the Nation's Cybersecurity," to align and base civilian agencies enterprise security architecture with zero trust principles.[3] The Memorandum requires FCEB agencies to ensure that "all traffic must be encrypted and authenticated as soon as practicable."[4] The strategy includes an initial focus on DNS traffic, requiring agencies to encrypt all DNS traffic, wherever technically supported, across their enterprise by FY24.

The purpose of this document is to provide FCEB agencies with guidance for implementing encrypted DNS protocols in line with M-22-09 – Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.

DNS forms a cornerstone for supporting and enabling enterprise IT. Traditionally, however, DNS has not supported methods for ensuring the confidentiality, integrity, or authenticity of requests for information or the responses. While solutions like Domain Name System Security Extensions (DNSSEC) enable verifying the authenticity and integrity of responses, the communication protocols that underly querying are still unencrypted, providing adversaries with opportunities to monitor and, in circumstances where integrity and authenticity are not strictly validated, potentially tamper with requests or responses. Various protocols[5][6][7] have been developed to support encrypting DNS request and response traffic; such protocols are increasingly integrated into products, thus easing the deployment of solutions that can increase integrity and confidentiality in DNS communications.

CISA's Protective DNS offering[8] supports encrypted DNS communication, which can help an agency align its responsibilities in 6 U.S.C. § 663 Note with the requirements laid out in M-22-09. Further, the Protective DNS offering can help protect the federal enterprise and help detect and mitigate cyber threats by preventing endpoints from resolving malicious domains.

1.1 ASSUMPTIONS AND CONSTRAINTS

- CISA's Memorandum on "Addressing DNS Resolution on Federal Networks" encourages, and OMB's Memorandum M-22-09 requires, the use of encrypted DNS protocols where technically supported.[9]
- Federal agencies are required to route all DNS traffic leaving agency networks and devices to CISA's Protective DNS capabilities.[10]
- Protective DNS and DNS encryption do not affect authoritative DNS hosting of .gov domains.

---

[2] *Id.*

[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity

[4] *Supra*, note 1.

[5] RFC 7858: Specification for DNS over Transport Layer Security (TLS).

[6] RFC 8484 (Proposed Standard): DNS Queries over HTTPS (DoH).

[7] RFC 9250 (Proposed Standard): DNS over Dedicated QUIC Connections.

[8] https://www.cisa.gov/resources-tools/services/protective-domain-name-system-resolver

[9] https://www.cisa.gov/sites/default/files/publications/Addressing_DNS_Resolution_on_Federal_Networks_Memo.pdf

[10] 6 U.S.C. §663 note, "Agency Responsibilities"

This guidance is focused on what is feasible action by agencies based on current agency and vendor landscapes as well as current functionality available from CISA's Protective DNS. With that focus, the following assumptions inform the guidance:

- Not all technologies currently deployed on FCEB networks support encrypted DNS protocols and many only support traditional unencrypted DNS protocols.
- Protective DNS is only directly accessible by agency DNS resolution infrastructure (e.g., internal DNS infrastructure, cloud resolvers, SASE/SSE resolvers) and (because of the lack of authentication mechanisms in the existing protocols) is not directly accessible from individual user endpoints.
- Agency on-premises internal DNS resolution services are not directly accessible by roaming and nomadic endpoints operating in off-premises environments.
- This guidance does not address the agency authoritative DNS infrastructure nor DNS traffic between recursive resolvers and the authoritative servers.

If these assumptions do not hold for a given agency, it may be able to meet the objectives of this guidance using different approaches than described in the guidance. If an agency selects a different approach, agencies will need to ensure that the approach meets all of the specified objectives.

2. AGENCY IMPLEMENTATION CHECKLIST

This checklist provides a high-level overview of the current requirements and best practices -- regarding encryption of DNS traffic and using CISA's Protective DNS for upstream DNS resolution -- that are applicable to federal agencies. Detailed guidance for carrying out these steps can be found in Section 3 and Appendix A.

Agency DNS Infrastructure

- Agency DNS infrastructure is configured to support agency endpoints using encrypted DNS protocols.
- Agency DNS infrastructure uses Protective DNS as their upstream provider.
- Agency DNS infrastructure uses encrypted DNS protocols when communicating with Protective DNS.
- Agency DNS infrastructure is configured to disable DNS Root Hints, DNS prioritization and any other mechanisms that might cause the infrastructure to bypass the use of Protective DNS.
- **Optional:** Agency DNS infrastructure is configured to resolve domains that force unconfigured applications to disable DNS-over-HTTPS (e.g., the canary domains for Firefox[11]).

Agency SASE/SSE Solutions

- Agency SASE/SSE solutions are configured to send all device DNS queries through the SASE/SSE solution for resolution.
- Agency SASE/SSE solutions are configured to use encrypted protocols when communicating with agency endpoints.
- Agency SASE/SSE solutions are configured to forward all DNS requests for agency endpoints through the SASE/SSE solution.

[11] See A.1.1 Firefox

- Agency SASE/SSE solutions are configured to use authorized DNS providers (i.e., agency internal DNS infrastructure or CISA's Protective DNS) when resolving DNS requests from agency endpoints.
- Agency SASE/SSE solutions are configured to disable any mechanisms that might bypass the use of authorized DNS providers (e.g., DNS Root Hints, round robin forwarding) when resolving DNS requests from agency endpoints, except for when the request is being resolved purely internally to the SASE/SSE solutions, or when Protective DNS is unavailable.

Agency On-Premises Endpoints

- Agency on-premises endpoints are configured to use internal DNS infrastructure (e.g., internal caching resolvers).
- Agency endpoints are, where technically supported, configured to use encrypted DNS protocols with agency DNS infrastructure.
- Agency endpoints that have applications that support application-level DNS resolution have appropriate configurations in place to:
    - Use the appropriately configured operating system or SASE DNS resolution mechanisms instead of application-level DNS resolution, or
    - Use application-level encrypted DNS resolution only with internal or otherwise authorized DNS infrastructure.
- Agency endpoints are configured to disable unauthorized DNS configurations, preferably using centralized mechanisms (e.g., Domain Policies, Configuration Management Systems).

Agency Roaming and Nomadic Endpoints

- Agency roaming (when off-premises) and nomadic endpoints are configured to use:
    - SASE/SSE solutions to send their DNS requests, using encrypted protocols, to authorized DNS providers (i.e., agency internal DNS infrastructure or Protective DNS), or
    - VPN solutions that allow them to use agency internal DNS infrastructure in situations where SASE/SSE solutions are not available.
- Agency endpoints are configured to disable unauthorized DNS configurations, preferably using mechanisms that can enforce that configuration even in situations where the endpoint does not have access to agency enterprise services.

Agency Networks

- Agency networks are configured to only permit communication with external third-party resolvers from authorized internal DNS servers.
- Agency networks are configured to block all unauthorized egress and ingress DNS traffic including:
    - **Traditional Unencrypted DNS:** Agencies can block traffic over port 53, and dynamic approaches may allow blocking traditional unencrypted DNS in a port independent manner.
    - **DNS-over-TLS:** Agencies can block traffic over port 853, and dynamic approaches may allow blocking DNS-over-TLS in a port independent manner.
    - **DNS-over-QUIC**: Agencies can block traffic over port 853, and dynamic approaches may allow blocking DNS-over-TLS in a port independent manner.
    - **DNS-over-HTTPS**: Agencies can block traffic over port 443 to external well-known DNS-over-HTTPS providers but should consider mechanisms that can block the traffic independent of destination (e.g., Break-and-Inspect, Zero Trust network architectures).

Agency Cloud Deployments

- Agency cloud deployments are, where technically supported, configured to use Protective DNS as their upstream provider, either directly or via a SASE/SSE solution.
- Agency cloud deployments are, where technically supported, configured to use encrypted DNS protocols for upstream resolution, either directly or via a SASE/SSE solution.
- Agency cloud deployments are, where technically supported, configured to block all unauthorized DNS traffic.
- Agency cloud deployments are configured to disable unauthorized DNS configurations, preferably using automated mechanisms (e.g., Domain Policies, Configuration Management Systems).

2.1 PHASED IMPLEMENTATION

Given the complexity of transitioning an existing agency enterprise to the use of encrypted DNS and Protective DNS, agencies may consider a phased approach, transitioning portions of their enterprise over time. While agency considerations will drive the best approach, agencies should prioritize preventing usage of unauthorized DNS providers, implementing Protective DNS protections, and encrypting DNS for roaming and nomadic endpoints.

For example, a phased approach might look like:

- **Phase 1: Use Protective DNS –** The agency configures their internal DNS infrastructure to use Protective DNS as the upstream DNS provider. The agency configures their SASE/SSE solutions to use Protective DNS or agency internal DNS infrastructure as the upstream DNS provider. The agency configures their Infrastructure-as-a-Service deployments to use Protective DNS or agency internal DNS infrastructure as their upstream DNS provider. Given existing statutory requirements, all FCEB agencies should already have implemented Phase 1 requirements.
- **Phase 2: Block Unauthorized DNS traffic –** The agency configures their networks and Secure Web Gateways to block DNS traffic for both traditional unencrypted DNS as well as for new encrypted DNS protocols to and from unauthorized endpoints. The agency uses centralized configuration management to configure on-premises agency endpoints and applications (e.g., web browsers) to only use agency internal DNS infrastructure, disabling any configurations that might use encrypted DNS with unauthorized DNS providers.
- **Phase 3: Encrypt DNS Traffic with Protective DNS –** The agency configures their internal DNS infrastructure and their SASE/SSE solutions to use encrypted DNS when communicating with Protective DNS as their upstream provider.
- **Phase 4: Encrypt DNS for Roaming and Nomadic Endpoints –** The agency configures their roaming and nomadic endpoints to use a SASE/SSE solution that resolves all DNS requests through an authorized DNS provider (i.e., Protective DNS or Agency internal DNS infrastructure). The agency uses configuration management solutions to enforce appropriate secure DNS configuration for roaming and nomadic endpoints even when those endpoints are unable to access agency enterprise services.
- **Phase 5: Encrypt DNS Traffic in Cloud Deployments –** The agency configures their cloud deployments to use encrypted DNS to resolve all DNS requests through an authorized DNS provider (i.e., Protective DNS or agency internal DNS infrastructure).
- **Phase 6: Encrypt DNS Traffic for On-Premises Endpoints –** The agency configures their internal DNS infrastructure to support receiving DNS requests using encrypted DNS protocols. The agency configures their on-premises endpoints, where technically supported, to use encrypted DNS protocols with the agency internal DNS infrastructure. Alternatively, the agency may configure their on-premises endpoints to use a SASE/SSE solution, similar to their roaming and nomadic endpoints.

3. IMPLEMENTATION GUIDANCE

The following subsections provide background on the technologies involved and the requirements under M-22-09, as well as more detailed guidance for implementing encrypted DNS and using CISA's Protective DNS service.

3.1 ENCRYPTED DNS

Encrypted DNS is intended to enable confidentiality and integrity for DNS traffic between clients and servers. The existing encrypted DNS protocols provide client-server and server-server traffic protection, but do not provide end-to-end encryption between the client and the DNS servers authoritative for a given domain. DNSSEC, a protocol extension to DNS which enables the verification of the authenticity and integrity of domain information, is distinct from Encrypted DNS and is beyond the scope of this document.

There are various methods for encrypting DNS traffic, with varying levels of support in off-the-shelf software and hardware:

- **DNS-over-HTTPS:** DNS-over-HTTPS is a broadly supported protocol that enables DNS encryption.[12] The protocol uses existing web protocols as its transport mechanism, facilitating its use in existing networks, and through proxies. However, this use of existing web protocols blends in with other web traffic, making it more difficult to monitor and block than traditional DNS and other encrypted DNS protocols.
- **DNS-over-TLS:** DNS-over-TLS is another standard protocol that encapsulates the DNS protocol within a standard TLS session using a well-defined port, 853, specifically assigned to DNS-over-TLS.[13] The use of a well-defined port can facilitate blocking the unauthorized use of external DNS providers, though clients could potentially use DNS-over-TLS over a different port. However, proxies may need to be configured to support transporting the new traffic type over the new port.
- **DNS-over-QUIC:** DNS-over-QUIC is the newest encrypted DNS protocol that uses the QUIC transport protocol. While it similarly makes use of an existing web traffic protocol, DNS-over-QUIC is currently supported by a more limited set of vendor solutions and services than DNS-over-HTTPS.

3.2 PROTECTIVE DNS

Protective DNS is a DNS resolver service provided by CISA for use by FCEB agencies, that replaced the legacy E3A DNS Sinkholing Capability. This service has protections to help prevent agency endpoints from reaching known or suspected malicious domains while providing agencies and CISA with visibility into the domains that the agencies are resolving. Agencies are required to route their egress DNS queries to this service, and have their endpoints use this service, whether mobile, roaming, nomadic, on-premises, or cloud deployed. The Protective DNS service supports DNS-over-HTTPS and DNS-over-TLS over both IPv4 and IPv6. Additionally, the service supports traditional unencrypted DNS for authorized FCEB DNS infrastructure.

Figure 1 shows various methods that agencies may use to enable endpoints to use the Protective DNS service. The methods used to access Protective DNS may differ between endpoints, even within an enterprise. Additionally, endpoints may need to use different methods as their network location changes (e.g., a roaming device is taken off-premises, an on-premises virtual machine fails over to a cloud environment).

---

[12] RFC 8484 (Proposed Standard): DNS Queries over HTTPS (DoH)

[13] RFC 7858: Specification for DNS over Transport Layer Security (TLS)

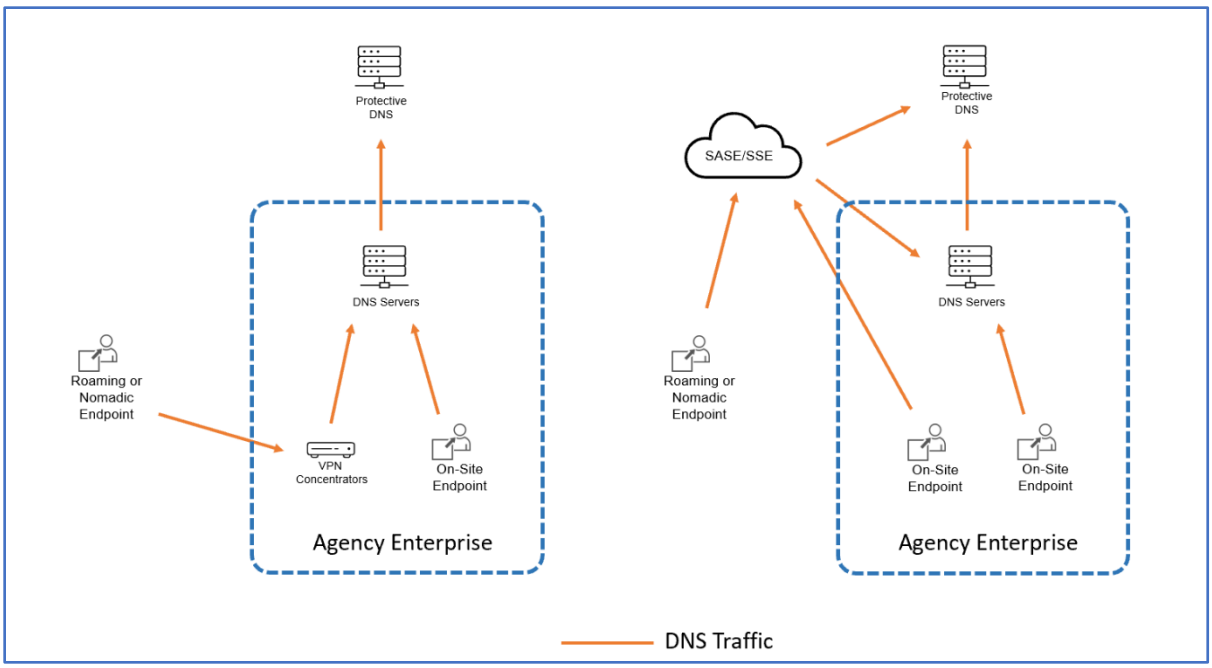

Figure 1: Methods for Using Protective DNS

- **Access via Agency DNS Infrastructure:** Agencies configure their internal DNS infrastructure (i.e., internal caching resolvers) to use Protective DNS as the upstream provider for DNS resolution, and endpoints use these internal DNS servers. Beyond supporting traditional on-premises environments, this model also supports other agency environments (e.g., cloud deployments).

While roaming or nomadic endpoints can potentially VPN into traditional agency environments and use these servers, this approach can cause performance problems for those endpoints. Agencies should consider other methods to enable roaming or nomadic endpoints to use Protective DNS without needing to connect to traditional agency on-premises environments.

- **Access via Agency SASE/SSE:** A growing number of agencies are deploying SASE/SSE services that their endpoints use for external access, including DNS resolution. The SASE/SSE service can then be configured to use either Protective DNS or agency internal DNS infrastructure to resolve domains. This model can allow for the use of Protective DNS independent of network location, facilitating use by roaming or nomadic endpoints.

Additionally, if the SASE/SSE solution uses the agency internal DNS infrastructure to resolve domains, roaming and nomadic endpoints will be able to resolve internal agency domains and other resources that are not advertised publicly. Agencies will need to work with their SASE/SSE providers to ensure that all DNS traffic from endpoints is routed to the provider, and that the provider uses appropriate DNS services and encrypted protocols for resolving those requests.

Internal Resources

Protective DNS is only able to resolve publicly available addresses. Agencies may have services or other resources that are only resolvable via internal DNS servers (e.g., internal applications, Microsoft Active Directory resources) and agency endpoints that bypass these internal DNS servers will be unable to resolve these resources.

Agencies may consider making agency internal resources publicly addressable, where technically feasible. This approach is in alignment with the Federal Zero Trust Strategy and would ensure that agency endpoints can resolve these services independent of how they resolve domain names.[14] Alternatively, agencies may consider making their internal resources accessible to endpoints using a SASE/SSE solution that does not require the resources to be publicly addressable. In these scenarios, agencies should make these resources available through the SASE/SSE solution independent of where the endpoint is deployed. While this model is better aligned with Zero Trust principles, agencies will need to understand and account for any potential legacy use that may not be compatible with the SASE/SSE solution.

Agencies may also consider having roaming or nomadic endpoints connect to an agency environment to access these internal resources (e.g., via VPN to on-premises environments). However, this method is not recommended as it can cause performance and usability issues for users as all of their network traffic will need to be routed through the agency environment.

3.3 AGENCY DNS INFRASTRUCTURE

To support M-22-09, agencies will need to ensure that, where technically feasible, their DNS infrastructure uses encrypted DNS protocols when communicating with their upstream DNS providers as well as with agency endpoints. Additionally, agency DNS infrastructure should use only Protective DNS as its upstream provider except in situations where Protective DNS is unavailable.

Encrypted DNS Support

DNS server software is beginning to include support for encrypted DNS protocols, including both when communicating with clients and when communicating with upstream providers. Where technically feasible, agency DNS servers should use encrypted DNS protocols, both for communicating with clients as well as with other servers. Where agencies deploy multiple levels of agency-managed DNS servers, they should use encrypted DNS protocols for communications between their DNS servers.

Agencies will need to determine the support for encrypted DNS available for their DNS server solutions as well as their clients. As many DNS server vendors are still in the process of integrating encrypted DNS protocols into their solutions, support for DNS encryption can vary widely. For example, many DNS server solutions in common use do not support encrypted DNS protocols or may require additional licenses to support them. Additionally, some DNS server solutions may only support encrypted DNS protocols for communicating with upstream providers or may only support encrypted DNS for communicating with clients.

Agencies should, where possible, consider updating or replacing infrastructure that does not support DNS encryption. In situations where DNS infrastructure cannot be replaced, it may be possible to use proxies to handle the encrypted DNS. Where the DNS infrastructure does not support using encrypted DNS from clients, a proxy could be used to receive queries via encrypted DNS protocols, and then forward those queries using traditional unencrypted DNS to the DNS infrastructure. Where the DNS infrastructure does not support using encrypted DNS with the upstream DNS servers, a proxy can be used to receive DNS queries from the DNS infrastructure using traditional unencrypted DNS, and then forward those queries to the upstream DNS servers using encrypted DNS. Agencies will need to work with their DNS server vendor to understand the feasibility of this model.

[14] *Supra*, note 1.

In situations where agencies need to make use of traditional, unencrypted DNS protocols for any of their DNS communication, they will need to understand and account for the lack of confidentiality or integrity in this communication.

To meet the encrypted DNS requirements of M-22-09, the use of external encryption mechanisms, such as tunneling unencrypted DNS:53 traffic through an IPsec tunnel, is not considered an acceptable substitute for the use of encrypted DNS protocols.

Protective DNS Support

Agencies will need to work with CISA's Protective DNS service to understand how to best configure their DNS Infrastructure to use Protective DNS as the upstream provider, including the use of encrypted DNS protocols when communicating with Protective DNS.

Some DNS servers may not support using encrypted DNS protocols with upstream servers. To support these servers that do not natively support encrypted DNS protocols, it may be possible to install a proxy to forward the server's DNS upstream queries via encrypted DNS protocols to Protective DNS. Agencies will need to work with their DNS server vendor to understand the feasibility of this model.

DNS servers commonly support a feature called DNS Root Hints. Under certain conditions, these may cause the DNS servers to switch to iterative resolution. In this mode of operation, the DNS server will bypass upstream recursive resolvers and communicate directly with the DNS root servers and, consequently, other DNS resolvers on the Internet. Agencies must disable Root Hints on all agency managed endpoints supporting this feature to help prevent their DNS queries from bypassing the Protective DNS service.

Agencies may configure backup DNS resolvers (e.g., well-known public resolvers) as fallback resolvers to be used only when Protective DNS resolver is unavailable (e.g., in case of a service outage). The agency DNS infrastructure must use encrypted DNS with these fallback resolvers. This configuration is commonly enabled by configuring Protective DNS as the highest priority server and configuring the fallback DNS servers at a lower priority (e.g., secondary, tertiary). However, as DNS servers commonly use prioritization as a suggestion, they may use lower priority servers even when the primary server is available. When configuring backup DNS resolvers, agencies must ensure that their configuration only permits the DNS servers to be used when Protective DNS is unavailable. Additionally, as use of these backup public resolvers bypass Protective DNS protections, agencies should ensure that they have mechanisms (e.g., alerting) in place to track when the backup DNS resolvers are being used in place of Protective DNS.

Some agencies employ a "Split DNS" configuration where their DNS infrastructure resolves the same domain, service or resource to different addresses depending on the network location of the endpoint requesting the resolution. For example, an agency might have endpoints operating within internal agency environments resolve publicly accessible agency services to internal addresses. When agency endpoints resolve domains through agency DNS infrastructure, the use of Protective DNS will not impact the operations of these configurations.

3.4 AGENCY SASE/SSE SOLUTIONS

Many SASE/SSE providers encrypt communications with endpoints and can support sending the endpoint DNS queries to Protective DNS, enabling agencies to meet the requirements of M-22-09 as well as Protective DNS. Additionally, agency endpoints may be able to take advantage of these features, independent of whether nomadic, roaming, mobile devices, on-premises, or cloud-deployed.

To ensure appropriate protections, endpoints must be configured so that all their DNS traffic is intercepted by the SASE/SSE service and resolved through authorized DNS services (i.e., Protective DNS or agency internal DNS infrastructure). A common SASE/SSE deployment can simplify the deployment and management of protections across a variety of endpoints.

Agencies will need to work with the SASE/SSE provider to ensure that traffic is only sent to authorized providers, including disabling any mechanisms that might permit routing traffic to unauthorized providers (e.g., DNS Root Hints, root servers, DNS failover, load balancing). The SASE/SSE provider may perform filtering and caching so long as all traffic that cannot be resolved is routed to Protective DNS. Where technically feasible, agencies need to ensure that the SASE/SSE provider uses encrypted DNS protocols when communicating with authorized DNS services.

In some instances, agencies may have internal resources that are not publicly addressable. To support these scenarios, the SASE/SSE provider can be configured to use the Agency internal DNS infrastructure. In such scenarios, the SASE/SSE provider can be configured to route some or all traffic back through the Agency internal DNS infrastructure. However, it may be possible to limit the load on the agency DNS infrastructure by using a configuration where the SASE/SSE provider resolves external resources using Protective DNS and internal resources using the Agency internal DNS infrastructure.

When endpoints are operating outside traditional environments, they may be able to bypass SASE/SSE protections due to intentional or unintentional misconfiguration, and without compensating controls, agencies may not be able to determine that the endpoint is bypassing the protections. Agencies should consider mechanisms that prevent changes to the endpoint's SASE/SSE configuration or that automatically revert unauthorized changes to a known-good state.

3.5 AGENCY ENDPOINTS

To meet the M-22-09 requirements, agency endpoints need to use encrypted protocols, where technical feasible, to resolve their DNS queries and only use authorized DNS providers (i.e., agency internal DNS infrastructure or Protective DNS), whether operating in on-premises environments, cloud environments, nomadic, or roaming. Additionally, applications and operating systems may, by default, enable encrypted DNS in ways that bypass agency and CISA DNS protections. Agencies will need to explicitly configure their endpoints and applications to either disable those encrypted DNS protocols or to use an authorized configuration for resolving DNS queries using encrypted protocols. Agencies will also need to maintain those configurations as updates to the applications or operating systems occur.

Encrypted DNS Support

Applications and operating systems are beginning to support the use of encrypted DNS protocols. Appendix A includes implementation guidance that discusses specific products that currently support encrypted DNS protocols. However, at a high level, the methods for configuring endpoints to use encrypted DNS protocols include:

- **Operating System Support:** Operating systems are beginning to include native support for encrypted DNS protocols. Native support can simplify configuration and decrease the chance of operating system upgrades impacting an endpoints' DNS configuration.
- **SASE/SSE Solutions:** As described in the previous section, SASE/SSE solutions can support using encrypted communications to resolve endpoint DNS queries through authorized DNS providers (i.e., authorized agency internal DNS infrastructure, Protective DNS). These solutions can support endpoints where the operating system does not include native support. Additionally, these solutions can provide more uniform support across endpoints, allowing agencies to use a single configuration, independent of the operating system version on the endpoint.
- **Web Browser/Application Support:** Web browsers and other applications may support DNS encryption. However, this method will only provide protection for DNS resolution from the specific web browsers or applications, leaving the rest of the applications on the endpoint and the underlying operating system unprotected. Additionally, since application-level DNS resolution may bypass operating system or SASE/SSE DNS resolution and associated protections, application-level encrypted DNS resolution should be explicitly disabled when other encrypted DNS options are employed.

Application and operating system support for encrypted DNS often include a default configuration to retry DNS requests using traditional unencrypted DNS protocols when encrypted DNS lookups fail. Additionally, implementations may look for certain features of the network to determine whether to downgrade to unencrypted DNS. Agencies need to ensure their endpoints are configured to explicitly disable downgrading to unencrypted DNS to ensure that malicious entities cannot force them to use insecure protocols.

Application and operating system support for encrypted DNS often comes with software configuration options, including potentially default configurations, that bypass the local DNS configuration to use external providers known to support the encrypted DNS protocols. Agencies will need to prevent endpoints from bypassing DNS protections by directly accessing unauthorized DNS providers (e.g., third-party public). Beyond directly blocking the use of encrypted DNS protocols with unauthorized providers, agencies need to configure endpoints to disable these kinds of configurations and should use enterprise-wide policies to ensure comprehensive enforcement.[15] As new and updated software may include new configurations that enable encrypted DNS protocols, agencies will need a process to track the support for encrypted DNS in their deployed software, including both operating systems and applications, to ensure appropriate configurations for their endpoints.

Protective DNS Support

Endpoints can be configured to make use of the Protective DNS protections through agency internal DNS infrastructure or through SASE/SSE solutions.

- **Through Agency DNS Infrastructure:** Endpoints can be configured to use agency internal DNS infrastructure, which in turn uses Protective DNS. By using the agency's internal DNS infrastructure, the endpoint will be able to resolve agency internal resources (e.g., internal applications, Microsoft Active Directory resources). While this configuration works effectively for endpoints permanently residing in on-premises environments, it requires roaming and nomadic endpoints to VPN into an agency environment, which can cause performance problems for those endpoints.
- **Through SASE/SSE:** Endpoints can be configured to use SASE/SSE solutions that make use of Protective DNS. SASE/SSE solutions can allow for agency endpoints to make use of Protective DNS, independent of whether nomadic, roaming, mobile devices, on-premises, or cloud-deployed. This location independence can be especially helpful for endpoints that might move between environments (e.g., roaming endpoints, mobile devices). If the agency has internal resources that the endpoint needs to be able to resolve, the agency will need to ensure that the SASE/SSE solution uses the agency internal DNS infrastructure as the upstream provider.

3.6 CLOUD DEPLOYMENTS

Cloud providers and services provide varying levels of control over how DNS resolutions are performed, and agencies will need to understand the configuration opportunities available. While specific options are going to depend on the Cloud provider and their particular service offerings, the following provides a high-level overview of commonly available options:

- **Infrastructure-as-a-Service (IaaS):** Agencies may be able to configure their IaaS deployment so that all external DNS traffic from endpoints in the deployment is sent to an authorized DNS provider (i.e., Protective DNS or agency DNS infrastructure) using encrypted DNS protocols. Alternatively, agencies may be able to configure endpoints (e.g., Virtual Machines) to directly use encrypted DNS protocols with an authorized DNS provider.

[15] CISA Memorandum on "Addressing DNS Resolution on Federal Networks"

- **Platform-as-a-Service (PaaS):** DNS for PaaS endpoints is often managed as part of the PaaS infrastructure. In such scenarios, it may be possible to configure the PaaS infrastructure to forward DNS queries for external resources to an authorized DNS provider (i.e., Protective DNS or agency DNS infrastructure) for resolution. Alternatively, PaaS endpoints (e.g., Containers) may be able to directly use encrypted DNS protocols with an authorized DNS provider.
- **Software-as-a-Service (SaaS):** Agencies may have limited control over how DNS is performed in SaaS deployments. Often, these deployments will use the cloud providers DNS solution, and agencies will need to understand, and account for, any potential differences in the protections and visibility provided by those services.

Cloud deployments may comprise a variety of Cloud services and each deployment is a unique use case. For example, an agency deployed web service might consist of an Identity-as-a-Service solution to manage identity within the deployment; a Web Application Firewall-as-a-Service solution to manage access to the web service; a mixture of PaaS and IaaS solutions for the web service; and a Database-as-a-Service solution to store the data. In these scenarios, agencies may only be able to configure DNS resolution for a portion of their overall cloud deployment. Agencies will need to understand and account for these differences to ensure a commensurate level of protection and visibility is available. For example, the web service deployment might ensure that all external domains are resolved prior to being brought into the cloud deployment, and that the deployment only communicates using internal addresses.

3.7 PREVENTING UNAUTHORIZED DNS TRAFFIC

Agencies will need to ensure that endpoints are not able to bypass DNS protections by directly using unauthorized DNS providers (e.g., third-party public DNS resolvers). This is especially important as applications and operating systems increasingly facilitate the use of encrypted DNS protocols through the inclusion of configurations, including potentially default configurations, that bypass local DNS to use external providers. As these new configurations use encrypted DNS protocols, they may bypass existing agency controls meant to limit access to unauthorized DNS services. Agencies will need to understand the controls they have in place to prevent unauthorized access to DNS services as well as assess whether said controls need to be updated or augmented with compensating controls to account for encrypted DNS protocols.

Agencies must consider mechanisms to deploy appropriate endpoint DNS configurations for supported operating systems and applications that only permit encrypted DNS with authorized DNS services (i.e., either Protective DNS or agency internal DNS infrastructure). These mechanisms should allow for the centralized management of these endpoint configurations (e.g., Group Policies, Configuration Management). While these configurations can be applied statically when endpoints are deployed or updated, agencies should consider mechanisms that prevent changes to the DNS configuration or that automatically revert unauthorized changes to a known-good state. These enforcement mechanisms can be specifically important where endpoints operate outside traditional environments, as they may be able to bypass DNS protections due to intentional or unintentional misconfiguration. Without compensating controls, agencies may not be able to determine that the endpoint is bypassing the protections. When certain features are not used (e.g., application-level DNS over TLS or DOH implementations), they must be explicitly disabled through group policies or other means.

Agencies should take advantage of weekly DNS reports sent by CISA to monitor DNS traffic leaving their on-premises networks to identify misconfigurations, rogue endpoints, and other potential anomalies.

On-Premises Environments

For on-premises environments, agencies will need to block connections between endpoints and unauthorized DNS providers to ensure that misconfigured endpoints do not bypass DNS protections. Agencies should only permit

authorized internal DNS resolvers to query authorized external DNS resolvers, and prevent all other endpoints from querying external DNS resolvers. This can be partially accomplished by blocking TCP and UDP traffic over well-known DNS ports (e.g., 53, 853) that are not destined for authorized providers. However, as DNS-over-HTTPS makes use of common ports and protocols, other methods may be needed to block this traffic. If agencies have enabled Break-and-Inspect mechanisms, whether deployed on-premises or via a SASE/SSE service, it may be possible to directly block DNS-over-HTTPS traffic to unauthorized providers. Yet, if Break-and-Inspect capabilities are not employed, agencies may need to use other mechanisms to block such traffic (e.g., blocking communication with well-known DNS-over-HTTPS providers).

For environments such as guest wireless networks that permit guest user endpoints, agencies should follow the same guidance for blocking unauthorized traffic and routing all egress DNS traffic to protective DNS. Additionally guest networks should segregate all traffic to a dedicated IP range so that the guest network traffic can easily be differentiated from agency enterprise network traffic by security devices and analysts.

3.8 VISIBILITY

DNS encryption can hinder existing network-based solutions that depend on access to unencrypted DNS traffic for visibility. With the DNS traffic being encrypted, agencies will need to obtain comparable visibility through solutions that can obtain visibility into DNS activity from client and server endpoints. This endpoint-based visibility will require the encrypted DNS traffic only be permitted between authorized clients and servers where agencies have visibility (e.g., authorized endpoints and agency internal DNS servers, agency internal DNS servers, and Protective DNS). With the diversity of endpoints, their locations, and the information available for them, agencies may need to integrate data from multiple sources to gain comprehensive visibility.

- **Protective DNS Logs:** Logs from Protective DNS can provide information on all DNS queries made by agency caching resolvers and associated responses. While these logs can provide overall insight into agency domain resolutions, agencies may need additional context to determine the specific endpoint that made the request.
- **Agency DNS Server Logs:** Agency DNS server logs can provide visibility into the DNS resolutions performed by on-premises agency endpoints as well as roaming or nomadic endpoints that have connected into an on-premises environment. However, these logs may not have comprehensive visibility as roaming, nomadic, or cloud endpoints may use methods for DNS resolution that bypass the agency DNS servers.
- **SASE/SSE Logs:** SASE/SSE logs can provide visibility into the DNS resolutions performed by endpoints that use the SASE/SSE, whether those endpoints are on-premises or remote. SASE/SSE solutions can provide a uniform visibility across agency endpoints where a common solution is used across the enterprise. However, improperly configured roaming, nomadic, or legacy endpoints may bypass the SASE/SSE solution, limiting agency visibility.
- **Device Logs:** Device logs, whether obtained through Endpoint Detection and Response (EDR), Mobile Device Management (MDM), or other solutions, may be able to provide visibility into the domain resolutions performed by the devices. While many solutions provide or have access to DNS information, the information available via these solutions can vary considerably depending on the type of device (e.g., mobile vs workstation). Additionally, as these logs are provided from the device, there is the potential for delays in receiving the information from the devices, or for misconfigured devices to not provide the information; and, if a malicious entity compromises a device, they may be able to limit or compromise the information being sent from the device.
- **Cloud Logs:** Logs from Cloud providers may be able to provide information about the DNS resolutions performed by an agency's cloud deployment. For some cloud environments, there may be direct logs of DNS resolutions performed by agency endpoints. However, for certain environments or deployments, there may not be direct logs of the DNS resolutions performed by the managed services. In these scenarios, agencies may need to reconstruct the DNS resolutions from other logs (e.g., logs of connections made by the cloud deployment that include DNS names).

APPENDIX A: VENDOR-SPECIFIC IMPLEMENTATION GUIDANCE

A.1 WEB BROWSERS

A.1.1. Firefox

An Firefox is a web browser that includes support for encrypted DNS protocols, with recent versions automatically using encrypted DNS protocols with external DNS providers. If left to default settings, these configurations bypass agency and CISA DNS protections. Agencies will need to understand how to properly configure Firefox to either use the native DNS resolution of the operating system, or, if needed, to use encrypted DNS protocols only with authorized DNS servers (i.e., agency DNS infrastructure).

Overview

To prevent Firefox from bypassing agency DNS protections or Protective DNS protections, agencies must configure all Firefox instances on agency endpoints to either:

- Use the native DNS resolution of the properly configured operating system, or
- Use encrypted DNS with agency internal DNS services

Additionally, agencies must validate appropriate DNS resolution behavior for new or updated versions of Firefox.

Firefox can only be configured to use encrypted DNS for name resolutions that it performs. Agencies will still need to configure other applications and the underlying operating system to ensure proper encryption of all DNS requests.

Deployment Considerations

- Agencies will need to configure Firefox no matter their approach to encrypted DNS, as the default and available configurations included with Firefox bypass agency and CISA DNS protections.
- Firefox will only provide protection for DNS resolution that it performs; other applications and the underlying operating system will need to be configured separately to encrypt DNS requests from the endpoint.
- Firefox only supports DNS-over-HTTPS as its encrypted DNS protocol.
- While Firefox has supported DNS-over-HTTPS since version 73, agencies should be using the most recent version of Firefox to employ up to date security protections.
- Firefox will fall back to unencrypted DNS if encrypted DNS lookups fail or if a network signals that encrypted DNS should be disabled. Agencies will need to understand this fallback mechanism to help ensure that entities cannot force endpoints to use unencrypted DNS.
- Updates to Firefox may require new or updated configurations from agencies, and agencies will need to verify that updates do not enable invalid encrypted DNS configurations that bypass authorized DNS providers before deploying the updates across the enterprise.
- When configured to use encrypted DNS protocols, Firefox will use the operating system DNS configuration to resolve the DNS server FQDN address (and for captive portals that are used as part of the initial access to a network), but will subsequently resolve addresses according to the encrypted DNS configuration.

Guidance

Configuring Firefox Policy

There are various methods that agencies can use to configure Firefox:

- **Group Policy Objects:** Agencies can use Group Policy Objects in Active Directory to centrally configure Firefox for any Windows endpoints that are joined to the Active Directory domain[16]. While these configuration options only apply to Windows machines, the user will not be able to override the settings, and the centralized configuration will ease policy updates and enforcement.
- **Policies Configuration File:** Agencies may use a custom policies configuration file (i.e., policies, json) to set default settings for endpoints that are either not running Windows or are not joined to the Active Directory domain.[17] However, these configurations only specify the default configuration, potentially allowing users to change the settings. Agencies should use centralized configuration management systems to apply and update these configurations, and to validate unauthorized changes are not made to the Firefox configuration.

Disabling DNS-over-HTTPS

- **Browser Configuration:** Firefox can be directly configured to disable DNS-over-HTTPS.[18] Additionally, agencies should consider removing the available DNS services to make it more difficult for users to re-enable DNS-over-HTTPS.
- **Network Configuration:** Agencies can configure their networks to ensure that any Firefox instances using default configurations will disable DNS-over-HTTPS.[19] This can augment the browser configuration approach to disabling DNS-over-HTTPS.

Enabling DNS-over-HTTPS

Firefox can be directly configured to use DNS-over-HTTPS[20] using either Group Policy Objects or through a policies configuration file. Agencies will need to ensure that the provider is configured to be their internal DNS infrastructure since using CISA's protective DNS as a provider will bypass the local DNS infrastructure and will fail to resolve queries for internal domains. Additionally, agencies should consider removing the preconfigured available DNS provider to make it more difficult for users to misconfigure their DNS configuration.

Beyond configuring Firefox to use DNS-over-HTTPS, agencies will also need to configure settings to help ensure that Firefox does not fall back to native OS-level DNS[21] under certain circumstances, including:

- When an endpoint is using a VPN.
- When Firefox is using a web proxy.

---

[16] https://support.mozilla.org/en-US/kb/customizing-firefox-using-group-policy-windows

[17] https://support.mozilla.org/en-US/kb/customizing-firefox-using-policiesjson

[18] https://support.mozilla.org/en-US/kb/firefox-dns-over-https

[19] https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https

[20] https://support.mozilla.org/en-US/kb/firefox-dns-over-https

[21] https://wiki.mozilla.org/Trusted_Recursive_Resolver

- When using the Name Resolution Policy Table (NRPT) to configure endpoint DNS settings.

Additionally, agencies will need to ensure that Parental Controls are disabled in both Windows and macOS installations, or Firefox will automatically disable DNS-over-HTTPS.

Resources

- https://support.mozilla.org/en-US/kb/firefox-dns-over-https
- https://support.mozilla.org/en-US/kb/dns-over-https-doh-faqs

A.1.2. Chrome

Google Chrome is a web browser that includes support for encrypted DNS protocols, with recent versions automatically choosing encrypted DNS protocols when the configured DNS server supports them. These configurations can bypass agency and CISA DNS protections, and agencies will need to understand how to properly configure Chrome to either use the native DNS resolution of the operating system, or, if needed, to use encrypted DNS protocols only with authorized DNS providers (i.e., agency DNS infrastructure).

Overview

To keep Chrome from bypassing agency DNS protections or Protective DNS protections, agencies must configure Chrome to either:

- Use the native DNS resolution of the properly configured operating system, or
- Use encrypted DNS with agency internal DNS services. (Using CISA's protective DNS as a provider will bypass the local DNS infrastructure and will fail to resolve queries for internal domains.)

Additionally, agencies must validate appropriate DNS resolution behavior for new or updated versions of Chrome.

Chrome can only be configured to use encrypted DNS for name resolutions that it performs. Agencies will still need to configure other applications and the underlying operating system to ensure proper encryption of all DNS requests.

Deployment Considerations

- Chrome will only provide protection for DNS resolution that it performs; other applications and the underlying operating system will need to be configured separately to encrypt all DNS requests from the endpoint.
- Chrome only supports the use of DNS-over-HTTPS as its encrypted DNS protocol.
- While Chrome has supported DNS-over-HTTPS since version 83, agencies should be using the most recent version of Chrome to use up to date security protections.
- Chrome will fall back to unencrypted DNS if encrypted DNS lookups fail. Agencies will need to understand this fallback mechanism to help ensure that entities cannot force endpoints to use unencrypted DNS.
- Updates to Chrome may require new or updated configurations from agencies, and agencies will need to verify that updates do not enable invalid encrypted DNS configurations that bypass authorized DNS providers before deploying the updates across the enterprise.

- When configured to use encrypted DNS protocols, Chrome will use the operating system DNS configuration to resolve the DNS server address, but will subsequently resolve addresses using DNS-over-HTTPS.

Guidance

Configuring Chrome Policy

There are various methods that agencies can use to configure Chrome:[22]

- **Group Policy Objects:** Agencies can use Group Policy Objects in Active Directory to centrally configure Chrome for any Windows endpoints that are joined to the Active Directory domain[23]. While these configuration options only apply to Windows machines, the user will not be able to override any settings that are configured in this manner. The centralized configuration makes it easy to update and enforce policies.
- **Policy Templates:** Agencies may use custom policies to set default settings for endpoints that are either not running Windows or are not joined to the Active Directory domain. The method for applying these policies differs between operating systems. Agencies should use centralized configuration management systems to apply and update these configurations.
- **Cloud Policies:** Agencies using Google Workplace may define custom policies for their users, which will be applied when the users sign into their Chrome Browser with their Google account[24]. Since these policies require the user to be signed into their Google account, users that have not signed into Chrome on the device they are using will have the default settings. When agencies make updates to these policies, they will be applied whenever the client has Internet connectivity.

Disabling DNS-over-HTTPS

Chrome can be directly configured to disable DNS-over-HTTPS.[25] [26]

Enabling DNS-over-HTTPS

Chrome can be directly configured to use DNS-over-HTTPS.[27] [28] Agencies will need to ensure that the provider is configured for their internal DNS infrastructure since using CISA's protective DNS as a provider will bypass the local DNS infrastructure and will fail to resolve queries for internal domains.[29] Agencies will need to ensure that Chrome does not revert back to performing insecure DNS requests when it receives an error while trying to resolve the domain name via encrypted DNS. Additionally, agencies will need to ensure that Parental Controls are disabled in both Windows and macOS installations, or Chrome will automatically disable DNS-over-HTTPS.

---

[22] https://storage.googleapis.com/support-kms-prod/vB6e8QUlyKUJmIVUMpOrLhTzUrzZA5G7O71t

[23] https://support.google.com/chrome/a/answer/7649838?hl=en

[24] https://support.google.com/chrome/a/topic/9025410

[25] https://support.google.com/chrome/answer/10468685

[26] https://chromeenterprise.google/policies/#DnsOverHttpsMode

[27] https://support.google.com/chrome/answer/10468685

[28] https://chromeenterprise.google/policies/#DnsOverHttpsMode

[29] https://chromeenterprise.google/policies/#DnsOverHttpsTemplates

Resources

- https://blog.chromium.org/2020/05/a-safer-and-more-private-browsing-DoH.html
- https://developers.cloudflare.com/1.1.1.1/encryption/dns-over-https/encrypted-dns-browsers/
- https://chromeenterprise.google/policies/

A.1.3. Safari

Safari is a web browser available for macOS, iOS, and iPadOS. Safari does not currently include its own DNS resolution mechanism, instead relying on the DNS resolution for the underlying operating system. To ensure appropriate DNS resolution behavior for Safari, agencies will need to properly configure the endpoint on which Safari is running. Agencies will need to validate continued appropriate DNS resolution behavior for new or updated versions of Safari.

A.2 OPERATING SYSTEMS

A.2.1. Microsoft Windows

For Microsoft Windows DNS Server, see section A.3.2.

The Windows 11 Operating System includes support for encrypted DNS protocols[30]. Additionally, there are SASE/SSE solutions that agencies can use to enable encrypting DNS traffic on Windows endpoints. Agencies will need to understand how to properly configure Windows to ensure use of encrypted protocols to perform DNS requests via authorized DNS providers (i.e., agency DNS infrastructure), and to ensure that misconfigured Windows endpoints do not bypass agency and CISA DNS protections.

Overview

To help ensure the endpoint is using encrypted DNS, and not bypassing agency DNS protections or Protective DNS protections, agencies could configure endpoints to either:

- Use Windows-native encrypted DNS with agency internal DNS services, or
- Use a SASE/SSE solution that routes DNS requests through authorized DNS providers (i.e., Protective DNS or agency DNS infrastructure).

For new or updated versions of Windows, agencies must validate them to ensure appropriate DNS resolution behavior.

Windows can be configured to use encrypted protocols for the DNS resolution that it performs as well as any applications that make use of its DNS resolution configuration. However, agencies will still need to configure applications that support their own DNS resolution (e.g., web browsers) to ensure proper encryption of all DNS requests.

[30] Windows versions prior to Windows 11 do not include native, supported options for encrypted DNS. There may be alternative solutions available to enable encrypted DNS for these older versions of Windows. However, those solutions are out of scope for this guidance.

Deployment Considerations

- There are various methods that agencies can employ to have their Windows endpoints use encrypted DNS (native support and via SASE/SSE provider). Further details about these methods are described below.
- While the Microsoft Windows 11 Operating System natively supports encrypted DNS protocols, Microsoft DNS Servers are currently not capable of using encrypted protocols neither for client to server, nor server to server communications.
- Windows will only work with Protective DNS when either:
    - Windows is using agency internal DNS infrastructure; or
    - Windows is using a SASE/SSE provider that performs the DNS resolution using authorized DNS providers (i.e., Protective DNS or agency DNS infrastructure).
- Windows will provide protection for the DNS resolution that it performs as well as any applications that make use of its DNS resolution configuration. Applications that support their own DNS resolution (e.g., web browsers) may need to be configured to ensure they use the Windows DNS resolution configuration, or that they use their own encrypted DNS implementation with an appropriate DNS provider.

Encrypted DNS Methods

There are various methods that agencies can employ to have their Windows endpoints use encrypted DNS and receive Protective DNS protections:

- **Native Support:** Agencies can have endpoints use the native Windows support for DNS-over-HTTPS when communicating with their internal DNS infrastructure[31]. By using the native support, agencies can simplify configuration and decrease the chance of operating system upgrades impacting an endpoint's DNS configuration. While this configuration can work effectively for endpoints operating in on-premises environments, it requires roaming and nomadic endpoints to VPN into an agency environment, which can cause performance problems for those endpoints. Additionally, if the agency needs to support earlier versions of Windows or other operating systems, they will need to support additional operating system-specific configurations.
- **SASE/SSE:** Many SASE/SSE providers encrypt communications with endpoints and can support sending the endpoint DNS queries to appropriate providers (i.e., Protective DNS or agency internal infrastructure). These SASE/SSE solutions can support agency endpoints independent of their location, easing the support of roaming and nomadic endpoints. A common SASE/SSE deployment can simplify the deployment and management of protections across a variety of endpoints.

There are a variety of SASE/SSE solutions available, each of which will have differing deployment guidance. The guidance included below focuses on the native Windows support for encrypted DNS.

[31] Windows includes protection support for DNS-over-HTTPS starting with Windows 11.

Encrypted DNS Methods

There are various methods that agencies can employ to have their macOS endpoints use encrypted DNS and receive Protective DNS protections:

- **Native Support:** Agencies can use the native macOS support for encrypted protocols to communicate with their internal DNS infrastructure.[34] By using the native support, agencies can simplify configuration and decrease the chance of operating system upgrades impacting an endpoint's DNS configuration. However, the native macOS support will not work for Remote and Roaming endpoints.
- **SASE/SSE:** Many SASE/SSE providers encrypt communications with endpoints and can support sending the endpoint DNS queries to appropriate providers (i.e., Protective DNS or agency internal DNS infrastructure). These SASE/SSE solutions can support agency endpoints independent of their location, easing the support of roaming and nomadic endpoints. A common SASE/SSE deployment can simplify the deployment and management of protections across a variety of endpoints.

There are a variety of SASE/SSE solutions available, each of which will have differing deployment guidance. The guidance included below focuses on the native macOS support for encrypted DNS.

Guidance

Configuring macOS

There are various methods that agencies can use to configure macOS:

- **Configuration Management Solutions:** There are a variety of centralized solutions that agencies can use to apply and enforcement configurations for their macOS endpoints (e.g., Profile Manager, MDM solutions) These solutions may include native support for deploying encrypted DNS configurations, or they may include general support for defining DNS policies that agencies can use to define the endpoint's DNS configuration. These configuration management solutions can potentially simplify deployments where agencies have a diverse set of endpoints to configure. Agencies will need to understand the support provided by their solutions, and how they can be used to enable encrypted DNS.
- **Manual Configuration:** Agencies can manually configure macOS endpoints. This method can make it easy to test out or configure ad hoc endpoints, but such can be difficult to scale and deliver updated configurations.

There are a variety of configuration management solutions available, each of which will have differing deployment guidance. The guidance in this section will focus on manual configuration, which may inform how an agency might configure their configuration management solution.

Enabling Encrypted DNS

Profile configuration files need to be created to enable encrypted DNS. Agencies will need to ensure that the provider is configured to be their internal DNS infrastructure. Agencies will need to ensure that their configuration management solutions prevent changes from being made to this configuration.

---

[34] macOS has included native support for DNS-over-HTTPS and DNS-over-TLS since macOS Big Sur (Version 11).

Resources

- https://docs.quad9.net/Setup_Guides/MacOS/Big_Sur_and_later_%28Encrypted%29/
- https://support.apple.com/guide/profile-manager/distribute-profiles-manually-pmdbd71ebc9/mac

A.2.3 iOS/iPadOS

The operating systems used in iPhones and iPads include support for encrypted DNS protocols. However, with the inherent roaming nature of these devices, agencies should employ a SASE/SSE solution to help ensure that the devices use encrypted DNS with authorized DNS providers (i.e., Protective DNS or agency DNS infrastructure) independent of the device's location. Alternatively, agencies may consider using a SASE/SSE solution when devices operate in off-site locations, and the native support for encrypted DNS when devices operate in agency environments.

Overview

To help ensure devices are using encrypted DNS, and not bypassing agency DNS protections or Protective DNS protections, agencies can configure them with an appropriate DNS configuration that accounts for where the devices operate:

- Roaming devices that can operate both within and outside of agency environments could use a SASE/SSE solution that works independent of the devices' locations. They may otherwise use solutions that specifically account for the devices' current locations as they move between environments (e.g., SASE/SSE while operating remotely, native iOS/iPadOS encrypted DNS with agency internal DNS services while operating on-site).
- On-premises devices may use a SASE/SSE solution or may use the native iOS/iPadOS encrypted DNS with agency internal DNS services.
- Nomadic devices that only operate outside agency environments may use a SASE/SSE solution.

Given the mobile nature of these devices, agencies should use mechanisms that can ensure appropriate configurations are applied, even in situations where the device does not have access to agency enterprise services.

For new or updated versions of iOS/iPadOS, agencies must validate them to ensure appropriate DNS resolution behavior.

Deployment Considerations

- There are various methods that agencies can employ to have their iOS/iPadOS endpoints use encrypted DNS (native support and via SASE/SSE provider). Further details about these methods are described below.
- iOS/iPadOS will only work with Protective DNS when:
    - the device is using an appropriately configured SASE/SSE solution, or
    - the device is using agency internal DNS infrastructure.
- Applications operating on iOS/iPadOS devices may support their own DNS resolution and need to be configured to ensure appropriate DNS resolution behavior.

Encrypted DNS Methods

There are various methods that agencies can employ to have their iPhone and iPad devices use encrypted DNS with Protective DNS:

- **SASE/SSE:** Many SASE/SSE providers encrypt communications with endpoints and can support sending the endpoint DNS queries to appropriate providers (i.e., Protective DNS or agency internal DNS infrastructure). These SASE/SSE solutions can support agency endpoints independent of their location, easing the support of roaming and nomadic endpoints. Additionally, SASE/SSE solutions can allow for appropriate use of encrypted DNS and Protective DNS for iOS and iPad devices, independent of their location.
- **Native Support:** Agencies can have iPhone and iPad devices that are operating in on-premises environments, or that have connected into agency environments via VPN, use the native iOS/iPadOS support for encrypted DNS protocols to communicate with the agency's internal DNS infrastructure[35]. However, the native support will not work for roaming or nomadic endpoints operating outside of agency environments.

There are a variety of SASE/SSE solutions available, each of which will have differing deployment guidance. The guidance included below focuses on the native iOS/iPadOS support for encrypted DNS.

Guidance

Configuring iOS/iPadOS

There are various methods that agencies can use to configure macOS:

- **Configuration Management Solutions:** There are a variety of centralized solutions that agencies can use to apply and enforcement configurations for their iPhone and iPad devices (e.g., Profile Manager, MDM solutions). These solutions may include specific support for deploying encrypted DNS configurations or may include general support for defining DNS policies. These configuration management solutions can potentially simplify deployments where agencies have a diverse set of endpoints to configure. Agencies will need to understand the support provided by their solutions, and how they can be used to enable encrypted DNS.
- **Manual Configuration:** Agencies can manually configure their iPhone and iPad devices. This method can make it easy to test out or configure ad hoc endpoints, but can be difficult to scale and deliver updated configurations.

There are a variety of configuration management solutions available, each of which will have differing deployment guidance. The guidance in this section will focus on manual configuration, which may inform how an agency might configure their configuration management solution.

[35] macOS has included native support for DNS-over-HTTPS and DNS-over-TLS since macOS Big Sur (Version 11).

Enabling Encrypted DNS

Profile configuration files need to be created to enable encrypted DNS. Agencies will need to ensure that the provider is configured to be their internal DNS infrastructure. Agencies will need to ensure that their configuration management solutions prevent changes from being made to this configuration.

A.3 DNS SERVERS

A.3.1 BIND DNS Server

BIND is an open-source DNS server solution available for Unix-like Operating Systems, including Linux, *BSD, and macOS. Agencies will need to understand how to properly configure their BIND DNS servers to accept encrypted DNS traffic from agency endpoints as well as to use encrypted DNS protocols when communicating with Protective DNS.

Overview

BIND currently supports communicating with DNS clients over both DNS-over-HTTPS and DNS-over-TLS for the server side. BIND does not currently support communicating with upstream DNS servers using encrypted DNS protocols.[36] As depicted in *Figure 2*, agencies can deploy a DNS proxy to enable encrypted communication with upstream servers (e.g., Protective DNS).

There are a variety of solutions available that can be used to implement these DNS proxies. Agencies will need to ensure that their solutions are configured in accordance with the guidance below.

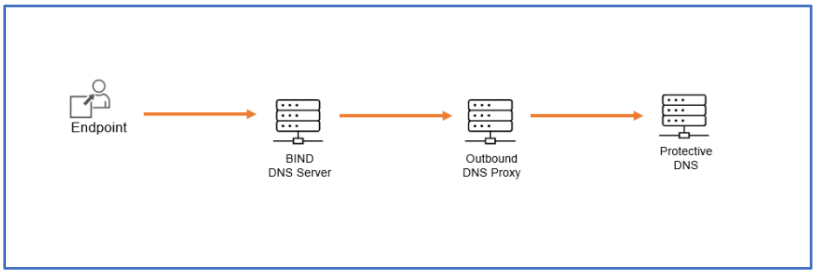

Figure 2: BIND DNS Server Encrypted DNS Proxy Setup

Where agencies employ zone transfers, they should ensure that zone transfers are performed over TLS, preferably using Mutual Authentication, and do not fall back to unauthenticated mode.

Guidance

Encrypted DNS With Agency Endpoints

The BIND DNS Server can be configured to support receiving DNS requests over DNS-over-HTTPS as well as DNS-over-TLS. Agencies should enable DNS-over-HTTPS as it is commonly the only encrypted DNS option

[36] The development version of BIND currently supports using DNS-over-TLS with upstream providers, but the stable version does not yet have that capability.

available for endpoint-based DNS solutions (e.g., operating systems, web browsers). Agencies may consider enabling DNS-over-TLS as well to support other use cases.[37]

Where agency endpoints require the use of unencrypted DNS, agencies should configure the BIND DNS Server to only accept unencrypted DNS from authorized endpoints using enforcement mechanisms like protected tunnels, microsegmentation, or IP permit lists. Agencies should, where possible, consider mechanisms to encrypt the communication between these authorized endpoints and the BIND DNS servers (e.g., encrypted tunnels).

Protective DNS

Agencies can deploy a DNS proxy to support encrypting DNS traffic between the BIND DNS server and Protective DNS. This DNS proxy may be a specialized DNS proxy. It could also take the form of a DNS server that does not perform any direct resolution, but simply proxies DNS traffic from the BIND DNS server.

As the communications between the BIND DNS server and the proxy will be unencrypted, agencies should consider either collocating the proxy with the BIND DNS server or using encrypted tunnels to limit the potential for eavesdropping or modification.

The DNS proxy must be configured to only accept DNS requests from the BIND DNS server, and to only forward those requests to the Protective DNS service.

All queries from the BIND DNS server must be configured to go through the proxy. This can be achieved by either:

- Having the DNS proxy be the only configured forwarder for BIND DNS server, or
- Using a transparent DNS proxy that can intercept and redirect all the outbound DNS traffic from the BIND DNS server.

Agencies will need to work with the Protective DNS service to ensure that the DNS proxy can send encrypted DNS requests to the Protective DNS service.

DNS Root Hints

By default, the BIND DNS server will use a set of pre-defined root server hints if it is unable to resolve a domain name. In this situation, the server might bypass agency DNS or Protective DNS protections and contact the DNS root servers directly. To disable this functionality, the BIND DNS server needs to be configured as a Forwarding DNS server instead of a Recursive Name server. This can be accomplished by setting the recursion flag to “no” in the BIND configuration.

[37] The development version of BIND supports DNS-over-TLS for communicating with upstream servers, which may make that a common encrypted DNS protocol for communicating between BIND DNS servers in the future.

Zone Transfers

Zone transfers are commonly used to allow a primary DNS server to be authoritative for a domain while other DNS servers answer queries about that domain. In these scenarios, copies of the domain DNS zone information are sent from the primary DNS server to the other DNS servers to enable them to answer queries.

These transfers need to be secured over TLS as well. Additionally, these transfers should be authenticated to ensure that only authorized servers are able to access the zone information, and to protect against potential modification while in transit.

By default, the BIND DNS server uses "opportunistic encryption" when performing zone transfers. This means that the server first checks to see if the zone transfer can happen over TLS, and if so, encrypts, but does not authenticate, the transfer. Agencies will need to enforce that all transfers must occur over TLS by specifying in the BIND configuration to use TLS for zone transfers in place of the default configuration.

Agencies should, where possible, use mutual TLS authentication so that both the server providing the zone information and the server receiving it can verify that they are talking to an authorized party. Where not possible, agencies may consider using transaction signatures (TSIG), a way of signing DNS traffic using a shared secret, to help ensure that zone information is being received unmodified from an authorized DNS server.

Resources

- https://bind9.readthedocs.io/en/stable/reference.html
- https://www.isc.org/blogs/bind-implements-doh-2021/

A.3.2 Microsoft DNS Server

Microsoft DNS Server is a DNS server software natively available for Windows servers. The Active Directory component of Windows integrates with the Microsoft DNS Server to make Active Directory resources available for resolution by clients.

Note that the Microsoft DNS server does not use the operating systems stub resolver discussed in the Microsoft Windows endpoint section. The server uses a separate dedicated DNS stack and does not inherit configuration settings from the operating system.

Overview

The Microsoft DNS Server does not currently support encrypted DNS protocols for communicating with either DNS clients or with upstream DNS servers. Agencies can deploy DNS proxies to enable encrypted communication with upstream servers.

To help ensure that the Microsoft DNS Server only routes traffic to authorized DNS providers (i.e., Protective DNS or agency internal DNS infrastructure), agencies must route upstream DNS requests from the Microsoft DNS Server through the proxy, including disabling DNS Root Hints.

There are a variety of solutions available that can be used to implement these DNS proxies. Agencies will need to ensure that their solutions are configured in accordance with the guidance below.

Guidance

Agencies can deploy DNS proxies to support encrypted DNS traffic from the Microsoft DNS Server to Protective DNS. These DNS proxies may be specialized DNS proxies, but could also take the form of DNS servers that do not perform any direct resolution, simply proxying DNS traffic to or from the Microsoft DNS server.

As the communications between these proxies and the Microsoft DNS server will be unencrypted, agencies should consider either collocating the proxies with the Microsoft DNS server or using encrypted tunnels to limit the potential for eavesdropping or modification.

Encrypted DNS With Agency Endpoints

Currently, Microsoft DNS Server does not support encrypted DNS protocols for communicating with DNS and there are no viable solutions to remediate this deficiency.

Protective DNS

Agencies should set up a DNS proxy that can receive DNS queries from the Microsoft DNS Server and sends them to Protective DNS using encrypted DNS protocols. The DNS proxy must be configured to only accept DNS requests from the Microsoft DNS Server, and to only forward those requests to the Protective DNS service.

All queries from the Microsoft DNS Server must be configured to go through the proxy. This can be achieved by:

- Having the DNS proxy be the only configured DNS Forwarder for Microsoft DNS Server; or
- Using a transparent DNS proxy that can intercept and redirect all the outbound DNS traffic from the Microsoft DNS Server.

Agencies will need to work with the Protective DNS service to ensure that the DNS proxy can send encrypted DNS requests to the Protective DNS service.

DNS Root Hints

By default, the Microsoft DNS Server includes DNS Root Hint servers. These servers will be used if the DNS server cannot resolve the domain using the configured upstream provider, which can bypass the DNS proxy and consequently the agency and Protective DNS protections. Agencies must disable usage of DNS Root Hints.[38]

Resources

- https://learn.microsoft.com/en-us/windows-server/networking/dns/quickstart-install-configure-dns-server

[38] https://learn.microsoft.com/en-us/windows-server/networking/dns/quickstart-install-configure-dns-server?tabs=powershell#configure-root-hints

A.3.3 Azure Private DNS Server

Azure DNS Private Resolver is a DNS resolver natively available on Azure for virtual networks and hybrid name resolution scenarios. This cloud native service enables customers to query Azure DNS private zones from an on-premises environment and vice versa, privately, without deploying Virtual Machine based DNS servers.

Overview

Azure DNS Private Resolver does not currently support encrypted DNS protocols for communicating with either DNS clients or with upstream DNS servers. Agencies can deploy DNS proxies to enable encrypted communication with upstream servers.

To ensure that the Azure DNS Private Resolver only routes traffic to authorized DNS providers (i.e., Protective DNS or agency internal DNS infrastructure), agencies must route all upstream DNS requests from Azure DNS Private Resolver through the proxy.

There are a variety of solutions available that can be used to implement these DNS proxies. Agencies will need to configure their solutions in accordance with the guidance below.

Guidance

Agencies would need to deploy DNS proxies to support encrypted DNS traffic from the Azure DNS Private Resolver to Protective DNS. These DNS proxies may be specialized DNS proxies, but could also take the form of DNS servers that do not perform any direct resolution, simply proxying DNS traffic to or from the Azure DNS Private Resolver endpoints.

As the communications between these proxies and the Azure DNS Private Resolver will be unencrypted, agencies should consider either collocating the proxies with the Azure DNS Private Resolver Virtual Network on Azure, or using encrypted tunnels to limit the potential for eavesdropping or modification.

Encrypted DNS With Agency Endpoints

Currently, Azure DNS Private Resolver does not support encrypted DNS protocols for communicating with either DNS clients or with upstream DNS servers. There are no viable recommendations to remediate this deficiency.

Protective DNS

Agencies could set up a DNS proxy that can receive DNS queries from the Azure DNS Private Resolver outbound endpoint and sends them to Protective DNS using encrypted DNS protocols. The DNS proxy must be configured to only accept DNS requests from the Azure DNS Private Resolver outbound endpoint subnet range, and to only forward those requests to the Protective DNS service.

All queries from the Azure DNS Private Resolver outbound endpoint must be configured to go through the proxy. This can be achieved by having the DNS proxy as the only configured DNS Forwarding target for Azure DNS Private Resolver ruleset, which is linked to the outbound endpoint with a wildcard rule mapped to the DNS proxy.

Agencies will need to work with the Protective DNS service to ensure that the DNS proxy can send encrypted DNS requests to the Protective DNS service.

Resources

- https://aka.ms/azdnsresolver
- https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-get-started-portal#configure-a-dns-forwarding-ruleset

A.3.4 Infoblox DNS Appliance

The Infoblox DNS appliance is a DNS server solution that supports encrypted DNS communications with upstream DNS providers. The Infoblox DNS appliance also supports direct encrypted DNS communications with end clients.

Overview

Infoblox DNS appliances support encrypted DNS in two contexts:

- Select Infoblox appliances can support encrypted DNS traffic (both DNS-over-TLS and DNS-over-HTTPS) from end user DNS clients to Infoblox DNS servers.
- Infoblox appliances can also support encrypted DNS traffic (DNS-over-TLS only) forwarded to the CISA Protective DNS service.

Infoblox support of encrypted DNS from end user clients to the Infoblox DNS server requires the optional Infoblox Advanced DNS Protection (ADP) product feature, available on Infoblox DNS servers deployed on-premises as either physical appliances or virtual appliances running under VMware. ADP supports DNS-over-HTTPS and DNS-over-TLS connections from end clients when deployed on mid-range and high-end Infoblox appliances (models TE-1415 and above).

Infoblox support of encrypted DNS when forwarding to the CISA Protective DNS service (sometimes referred to as “RFE-12211 support”) requires the use of the DNS Forwarding Proxy (DFP) component of Infoblox DNS servers. (Note: The DFP is a built-in component of the Infoblox appliance software, but not a separate system.)

Guidance

Encrypted DNS With Agency Endpoints

To support encrypted DNS traffic from agency endpoints to the Infoblox DNS appliance, agencies can deploy the Infoblox Advanced DNS Protection product feature as described above. If this is not possible (e.g., the agencies are deploying low-end Infoblox appliances not capable of DOT and DOH support, or are deploying Infoblox appliances in public cloud environments where ADP is not supported), then they will need to deploy a separate DNS proxy.

The DNS proxy need not be a specialized DNS proxy but could instead take the form of DNS servers that do not perform any direct resolution, simply proxying DNS traffic to or from the Infoblox DNS appliance. As the communications between the DNS proxy and the Infoblox DNS appliance will be unencrypted, agencies should consider either collocating the proxies with the Infoblox DNS appliance, or using encrypted tunnels to limit the potential for eavesdropping or modification.

If such a proxy is used, then agency endpoints should be configured using either dynamic means (e.g., Group Policy, DHCP) or manual configuration to use the proxy as their DNS provider. As the DNS proxy will be the primary method of name resolution by agency endpoints, it will need to be configured with commensurate security protections and resiliency as the Infoblox DNS appliance.

Agencies should, where possible, configure the Infoblox DNS appliance to only permit inbound DNS queries from the DNS proxy.

Where agency endpoints require the use of unencrypted DNS, agencies may either configure the proxy to support unencrypted DNS, or may have those endpoints use unencrypted DNS directly with the Infoblox DNS appliance. However, unencrypted DNS should only be accepted from authorized endpoints using enforcement mechanisms like protected tunnels, microsegmentation, or IP permit lists. Agencies should, where possible, consider mechanisms to encrypt the communication between the authorized endpoints and the unencrypted DNS servers (e.g., encrypted tunnels).

Agencies must validate appropriate DNS resolution behavior for new or updated versions of the Infoblox appliance as well as updates to the endpoints, including both the operating systems and applications.

Protective DNS

The Infoblox DNS appliance supports the use of encrypted DNS with upstream DNS servers, including the CISA Protective DNS service.

To ensure that DNS traffic forwarded from Infoblox DNS servers to the CISA Protective DNS service is protected by encryption, agencies must:

- Contact their Infoblox account teams to obtain a no-charge entitlement required for this support, if not already obtained.
- Use the Infoblox CSP portal to activate the DNS Forward proxy components on the Infoblox DNS servers that will be forwarding DNS traffic to the CISA Protective DNS service.
- Use the Infoblox CSP portal to configure the DFPs on these Infoblox DNS servers to use the CISA Protective DNS service as an external resolver, with DNS-over-TLS enabled and use of unencrypted DNS disabled.
- Agencies that have a license for the Infoblox BloxOne Threat Defense Advanced product may optionally configure the DNS Forwarding proxies on these Infoblox DNS servers to use the BloxOne Threat Defense cloud-based DNS resolver as a fallback resolver in the event that the DFPs are not able to reach the CISA Protective DNS service.

Resources

- Agencies should contact their Infoblox account teams for additional resources and to obtain a no-charge entitlement required for this support.