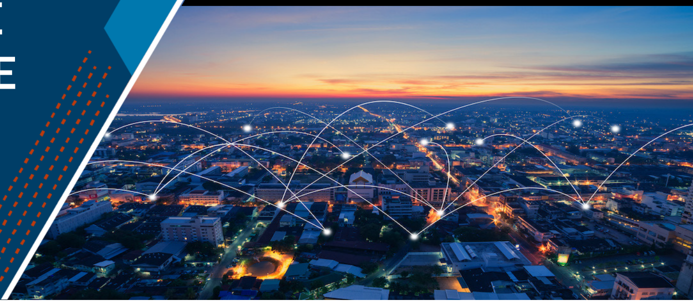
PROTECTIVE DOMAIN NAME SYSTEM RESOLVER SERVICE FREQUENTLY ASKED QUESTIONS



WHAT IS THE PROTECTIVE DOMAIN NAME SYSTEM RESOLVER SERVICE?

CISA launched the Protective Domain Name System (DNS) Resolver Service in September 2022 as part of its mission — and the national effort — to manage and reduce risk to cybersecurity and physical infrastructure. Protective DNS safeguards federal agencies by preventing network traffic from reaching malicious destinations. This creates a national enterprise IT environment that is more resilient to cyberattacks. Protective DNS fulfills the mandates set forth in The Federal Intrusion Detection and Prevention System, 6 U.S.C. § 663.

WHAT ARE THE KEY FEATURES OF PROTECTIVE DNS?

Protective DNS prevents government network traffic from reaching malicious destinations. Here are the key components:

- **Expanded Coverage.** The service is device-centric, protecting both organizational networks and standalone devices regardless of network location (e.g., on-agency premises, roaming/nomadic, or cloud). This functionality provides enhanced security and a greater range of coverage for more devices. In addition to traditional, unencrypted DNS:53, the service also supports modern protocols such as encrypted DNS [e.g., DNS-over-HTTPS (DoH), DNS-over-TLS (DoT)] over both IPv6 and IPv4.

- **Enhanced Threat Intelligence.** The service leverages a combination of unclassified commercial threat intelligence feeds and indicators sourced by CISA from government and industry partners to provide more comprehensive threat detection and prevent government internet traffic from reaching malicious destinations.

- **Real-Time Alerts.** The service leverages an application programming interface (API) to provide real-time updates to participating agencies when potential malicious DNS requests are identified, increasing early response capabilities and preventing security compromises.

- **Increased Visibility and Accessibility.** Agencies participating in the service can access their records and threat trends via a web application. This data also enables CISA to view trends and data across the federal civilian executive branch (FCEB) enterprise and can help identify common threats and potential targets for further action and threat hunting operations.

- **Zero-Trust Architecture Alignment.** In alignment with zero trust concepts, the service protects devices that were previously challenging to protect such as mobile, roaming, and nomadic devices.

HOW MUCH DOES PROTECTIVE DNS COST?

Protective DNS is offered at no cost to participating agencies. This CISA-funded service carries out its mission to protect agency network traffic from intrusions while empowering its government partners with enhanced capability.

WHEN DID PROTECTIVE DNS ENTER GENERAL AVAILABILITY?

Protective DNS became available to FCEB agencies in September 2022.

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

HOW IS PROTECTIVE DNS DEPLOYED?

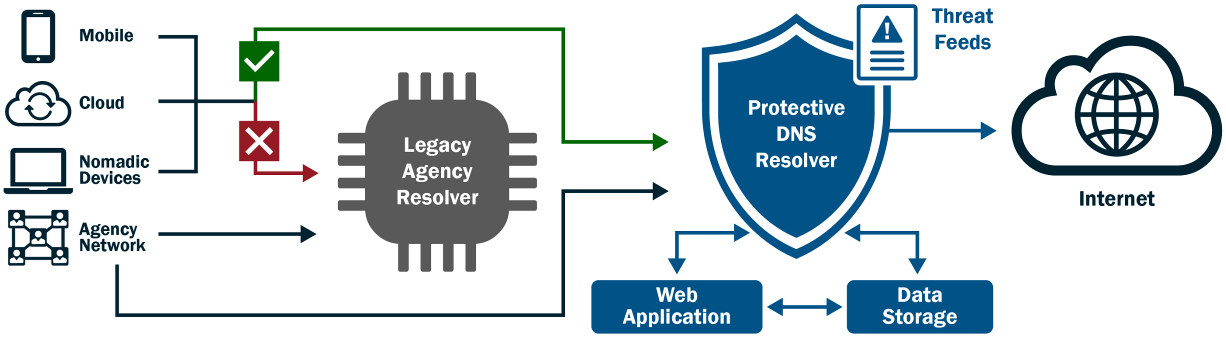
Protective DNS is a cloud-based solution that FCEB agencies manage across their networks and devices. Agencies have access to a front-end web application to update, maintain, and block DNS traffic and to view and download their log records for analysis.

WHY CHOOSE PROTECTIVE DNS?

CISA's Protective DNS enhances incident detection and response capabilities to support network resiliency to cyberattacks and threats. The service protects federal on-premises networks as well as assets that were previously challenging to protect such as mobile devices, nomadic devices, roaming devices, and cloud-based networks. It integrates with and complements DNS infrastructure protections that reside on agency networks and provides FCEB agencies with detailed insights into threat activities. This helps FCEB agencies prevent future attacks and better respond to current incidents.

HOW DOES PROTECTIVE DNS WORK?

CISA's Protective DNS service is implemented upstream from agency networks and does not interfere with internal DNS architecture (e.g., internal caching resolvers). The traffic from mobile, roaming, and cloud assets flows directly into the Protective DNS. DNS queries pass through Protective DNS resolvers for active traffic filtering against unclassified threat intelligence feeds. If Protective DNS finds a match between the DNS request and a threat intelligence indicator, the service blocks, redirects, or sinkholes the query response and sends an alert to the origin agency and to CISA.



WHAT IF I CANNOT ACCESS THE PROTECTIVE DNS WEB APPLICATION?

It is possible that an FCEB agency may be blocked by the Protective DNS web application firewall. In this case, the agency network will need to be allowlisted. Please contact the Protective DNS team for assistance. Protective DNS uses login.gov for user account authentication. If you are experiencing issues logging in to Protective DNS due to login.gov, please contact login.gov for account help.

It is possible that an FCEB agency may be blocked by the Protective DNS web application firewall. In this case, the agency network will need to be allowlisted. Please contact the Protective DNS team for assistance. After three failed login attempts, the account will be blocked for 20 minutes. Password resets should be done through login.gov.

WHAT PROTECTIONS ARE ENABLED BY PROTECTIVE DNS?

Protective DNS is designed to be a device-centric service that works to protect organizational devices regardless of network location (e.g., on-premises, off-premises, roaming, nomadic, mobile). The service requires minimal effort from agencies because it integrates into existing security and IT operations to provide real-time and historical visibility of all outbound DNS traffic to support incident response and analysis.

HOW DO USERS INTEGRATE WITH PROTECTIVE DNS?

Protective DNS is designed to fulfill agency obligations under The Federal Intrusion Detection and Prevention System, 6 U.S.C. § 663 note, "Agency Responsibilities." Protective DNS replaced the E3A service that was fully decommissioned in December 2023. Unlike E3A, Protective DNS supports roaming and on-premises devices, including those directed to a network through a virtual private network (VPN). To ensure a coordinated and seamless process, Protective DNS empowers users to go beyond the CISA global baseline of protections to configure, manage, and add their own organization-specific policies within the management application. Users can monitor their organization-specific traffic through interactive dashboards, customizable reports, and actionable email alerts triggered by malicious events. The Protective DNS resolver is implemented upstream from organization networks to complement an organization's DNS infrastructure protections. Traffic can be routed directly from on-premises assets or from an organization's existing DNS resolver service. The diagram on the previous page illustrates the high-level integration architecture for on-premises devices to Protective DNS.

Protective DNS users can also now integrate with security service edge (SSE) technology. This integration allows Protective DNS to work seamlessly with Zscaler and Cisco, regardless of whether the network uses IPv4/IPv6 protocols or if it is a secure access service edge (SASE) product. This compatibility ensures that Protective DNS functions efficiently within these platforms. To set up authorized sources and integrate with Protective DNS, reference the user guide and training video.

WHAT INDICATORS ARE BEING USED WITHIN PROTECTIVE DNS?

The service consistently reacts and responds to evolving threats by utilizing integrated CISA-proprietary indicators and commercial intelligence feeds. Protective DNS uses this blend of proactive commercial threat intelligence and unclassified indicators sourced from government and industry partners to provide threat detection and prevention. Threat intelligence feeds include various cybersecurity indicators such as spyware, malware, and phishing, along with other unclassified indicators that cover DNS-specific threats such as command and control botnets.

WILL A PERSONAL MOBILE DEVICE ON THE NETWORK RESOLVE THROUGH PROTECTIVE DNS?

Absent an agency supporting a Bring Your Own Device (BYOD) program or routing bannered Guest Network traffic through protective DNS, personal mobile devices should not resolve through Protective DNS. However, any government-distributed phone likely will resolve through the Protective DNS service.

DOES PROTECTIVE DNS SUPPORT IPV6?

Yes, CISA's Protective DNS service supports both traditional IPv4 and IPv6, as well as emerging encrypted protocols such as DNS over HTTPS (DoH) and DNS over TLS (DoT).

HOW WILL PROTECTIVE DNS HELP USERS COMPLY WITH ZERO TRUST REQUIREMENTS?

CISA's Protective DNS helps fulfill the requirement set forth by Network Pillar, Action 1 in OMB M-22-09, which states: "Agencies must resolve DNS queries using encrypted DNS wherever it is technically supported. CISA's Protective DNS program will support encrypted DNS requests."

However, it is important to note that not every DNS query's point of origin can currently transmit data in an encrypted format. This is entirely agency dependent. In addition, some vendors do not support protocols for forwarding queries to CISA's resolver service. Agencies should seek out and implement technology that will allow them to send encrypted data.

In short, Protective DNS will resolve encrypted protocols if the agency itself has the correct infrastructure in place for transmittal.

HOW DO AGENCIES SIGN UP FOR PROTECTIVE DNS?

Agencies can reach out to CyberSharedServices@cisa.dhs.gov and request to begin onboarding.

IS THERE A PROTECTIVE DNS HELP DESK?

Yes, a help desk is available to support users 24/7 via phone at 833-507-1894 or email at cisadnssupport@afs.com.

HAVE ADDITIONAL QUESTIONS?

Onboarded federal users can find additional information in the following documents:

- User Guide: Complete step-by-step guide to all Protective DNS features and functionality.
- Transition Guidance: Guide for DNS resolver transition to Protective DNS.
- Log Push Guide: Instructions to set up DNS log push to a local environment.

For more information, email CyberSharedServices@cisa.dhs.gov.