Selecting a Protective DNS Service

Why Protective DNS?

The Domain Name System (DNS) is central to the operation of modern networks, translating human-readable domain names into machine-usable Internet Protocol (IP) addresses. DNS makes navigating to a website, sending an email, or making a secure shell connection easier, and is a key component of the Internet's resilience. As with many Internet protocols, DNS was not built to withstand abuse from bad actors intent on causing harm. “Protective DNS” (PDNS) is different from earlier security-related changes to DNS in that it is envisioned as a security service – *not a protocol* – that analyzes DNS queries and takes action to mitigate threats, leveraging the existing DNS protocol and architecture.

Protecting users’ DNS queries is a key defense because cyber threat actors use domain names across the network exploitation lifecycle: users frequently mistype domain names while attempting to navigate to a known-good website and unintentionally go to a malicious one instead (T1583.001); threat actors lace phishing emails with malicious links (T1566.002); a compromised device may seek commands from a remote command and control server (TA0011); a threat actor may exfiltrate data from a compromised device to a remote host (TA0010).[1] The domain names associated with malicious content are often known or knowable, and preventing their resolution protects individual users and the enterprise.

Due to the centrality of DNS for cybersecurity, the Department of Defense (DoD) included DNS filtering as a requirement in its Cybersecurity Maturity Model Certification (CMMC) standard (SC.3.192). The Cybersecurity and Infrastructure Security Agency issued a memo and directive requiring U.S. government organizations to take steps to mitigate related DNS issues. Additionally, the National Security Agency has published guidance documents on defending DNS [1, 2, 3].

This guidance outlines the benefits and risks of using a protective DNS service and assesses several commercial PDNS providers based on reported capabilities. The assessment is meant to serve as information for organizations, not as recommendations for provider selection. Users of these services must evaluate their architectures and specific needs when choosing a service for PDNS and then validate that a provider meets those needs.

How does it work?

Widely implemented DNS security enhancements – that address the integrity and authenticity of DNS records (e.g., DNS Security Extensions, or DNSSEC) or that support the privacy and integrity of client DNS queries and responses (e.g., DNS over Transport Layer Security [DoT], and DNS over HTTPS [DoH]) – do not address the trustworthiness of upstream DNS infrastructure that may be compromised or DNS registrations that may be maliciously provisioned.

To address this shortcoming, PDNS uses a policy-implementing DNS resolver that returns answers based on policy criteria. This is often called Response Policy Zone (RPZ) functionality in DNS documentation. The resolver usually checks both the domain name queries and the returned IP addresses against threat intelligence, and then prevents connections to known or suspected malicious sites. PDNS can also protect a user by redirecting the requesting application to a non-malicious site or returning a response that indicates no IP address was found for the domain queried. In addition, many enterprise DNS resolvers still do not validate DNSSEC or support DoH/DoT, but many PDNS providers add these DNS security enhancements as well [4].

It should be noted that one inherent constraint of PDNS is that it is bypassed by any traffic using IP addresses directly without doing DNS lookups. For this reason, customers should not rely on it alone to detect and prevent malicious traffic. Some PDNS services may provide additional non-DNS related capabilities or integration with other security capabilities. Some network device equipment, such as firewalls, may have DNS protection capabilities as well. These devices and their functions or integrations with other capabilities are not covered in this guidance.

[1] T1583, TA0010, and similar notations identify MITRE® ATT&CK® techniques and tactics.

Service setup

The setup costs for a new security service is an important decision point for many organizations. A key benefit of PDNS is that it can be set up in a simple deployment just by changing an organization's recursive resolver to use the PDNS provider's DNS server.

More complex and secure deployments of PDNS may involve software changes on hosts. This may include lightweight DNS clients or virtualized applications that can keep the protections working in a variety of environments and enable a faster response to incidents. Additionally, enterprises should take measures to limit the use of alternative DNS resolvers, e.g., by configuring firewalls to block unauthorized DNS ports or DoH servers. PDNS systems may also support multiple policies for different groups, users, and/or devices.

Domain classification

A core capability of PDNS is the ability to categorize domain names based on threat intelligence. PDNS services typically leverage open source, commercial, and governmental information feeds of known malicious domains. These feeds enable coverage of domain names found at numerous points of the network exploitation lifecycle. Some solutions may also detect novel malicious domains based on pattern recognition. The types of domains typically addressed by a PDNS system include the following:

- **Phishing**: *Sites known to host applications that maliciously collect personal or organizational information, including credential harvesting scams.* These domains may include typosquats – or close lookalikes of common domains. PDNS can protect users from accidentally connecting to a potentially malicious link.

- **Malware distribution and command and control**: *Sites known to serve malicious content or used by threat actors to command and control malware.* For example, these may include sites hosting malicious JavaScript® files or domains that host advertisements that collect information for undesired profiling. PDNS can block and alert on known malicious connection attempts.

- **Domain generation algorithms**: *Sites with programmatically generated domain names that are used by malware to circumvent static blocking.* Advanced malware – including some botnets – depend on the ability to communicate with command and control (C2) infrastructure. Cyber threat actors use domain generation algorithms (DGAs) for malware to circumvent static blocking – either by domain name or IP – through programmatically generating domain names according to a pre-set seed. PDNS can offer protection from malware DGAs by analyzing every domain's textual attributes and tagging those associated with known DGA attributes, such as high entropy.

- **Content filtering**: *Sites whose content is in certain categories that are against an organization's access policies.* Although an ancillary benefit to malware protection, PDNS can use a categorization of various domains' use cases (e.g., "gambling") and warn or block on those that are deemed a risk for a given environment.

Response to identified domain names

A PDNS service may take several actions to respond to a malicious or suspicious domain name query. Of the protective actions, PDNS may restrict communication with a domain by returning an NXDOMAIN response, which means that there is no IP address answer for the domain name query. PDNS may also prevent the connection by redirecting to a block page, possibly offering a reason for the block to the user. It may also "sinkhole" the domain and provide a custom response. These responses delay or prevent further malicious actions – such as cryptolocking by ransomware or the use of command and control protocols – enabling an organization to conduct an investigation into a domain's provenance or initiate follow-on infection hunting.

Interactions with the PDNS platform

Typical administrative interactions with PDNS systems are through a web interface, an application programming interface (API), or a Security Information and Event Management (SIEM) integration. Cybersecurity leaders and administrators will

need to consider the increased workload of responding to PDNS alerts and integrating evolving network knowledge into their PDNS deployment plans.

Additionally, PDNS providers should collect and store the logs of DNS queries or provide them to the organization for it to keep. In either scenario, historical DNS logs can prove useful for retroactively searching for indications of earlier intrusions using indicators that only become known later on.

Cybersecurity best practices and PDNS

The following best practices address only the use of DNS resolver services. They do not address the management of an organization's own authoritative DNS zone(s) and related attributes – including availability, reliability, security, and performance.

Use a PDNS provider

Select and use a PDNS system as part of a layered defense-in-depth strategy. See below for some options for enterprise PDNS services. Other reputable PDNS services that are available and free for public use may be appropriate for personal use cases, but enterprise PDNS services that provide malicious activity alerts, enterprise dashboard views, historical logging and analysis, and other enterprise-focused features are recommended for enterprise networks. Additionally, due to DNS being foundational to most online activity, ensure that PDNS is provided as a high availability service.

Because an organization's PDNS provider can view their DNS queries, selecting a provider has privacy and security impacts. Obtain an understanding of how the service provider may use the organization's generated PDNS data – especially whether the provider will use the data for any non-security purposes.

Block unauthorized DNS queries

Unless required for operations, take measures to harden internal DNS resolution to prevent bypass. These measures should include blocking outbound port 53 (DNS) and port 853 (DoT) to thwart malware's potential use of DNS services, circumventing PDNS. In addition, block traffic to unauthorized DoH servers. Also, configure client applications – especially web browsers – with enterprise policies that configure DoH solely for designated resolvers, or disable DoH entirely. See NSA's *Adopting Encrypted DNS in Enterprise Environments* for more information [5].

Account for hybrid enterprise architectures

Classes of users may require different PDNS policies depending on their environments, and the prevalence of mobile and home network use can create additional challenges to PDNS implementations. One PDNS policy will not often fit the entire enterprise. Ensure that the chosen PDNS solution is flexible enough to adapt to your architectural and mission requirements. Deployment flexibility is typically achieved through the provider's implementation of a lightweight or "roaming" DNS client.

PDNS provider analysis

This document uses public information to provide an assessment of how some commercial providers may satisfy the above criteria as of February 2021. The selection of services for this initial assessment was based on publicly available information about enterprise PDNS services, as defined by this document, offered by vendors that are registered for federal contracts; this is not a comprehensive list of services or all possible criteria. NSA and CISA welcome providers to submit additional information that can be included in this guide to Cybersecurity_Requests@nsa.gov. Analysts gathered material from published company literature and product specifications, supplemented by other openly published analyses. No formal testing was performed on products or services for this analysis. NSA and CISA do not affirm the recency or accuracy of the data provided. This assessment is meant to serve as information for organizations, not as recommendations for provider selection. Users of these services must evaluate their architectures and specific needs when choosing a service for PDNS and then validate that a provider meets those needs.

Table 1: PDNS performance attributes comparison based on reported capabilities (note disclaimer below)

Capability	Akamai® ETP	BlueCat® Networks DNS Edge®	Cisco® Umbrella DNS SE	Cloudflare® Gateway	EfficientIP™ DNS Guardian	HYAS™ Protect	Infoblox® BloxOne® Threat Defense Cloud	Neustar® UltraDNS	Nominet® Protective DNS
Blocks malware domains	X	X	X	X	X	X	X	X	X
Blocks phishing domains	X	X	X	X	X	X	X	X	X
Malware Domain Generation Algorithm (DGA) protection	X	X	X	X	X	X	X	X	X
Leverages machine learning or other heuristics to augment threat feeds	X	X	X	X	X	X	X	X	X
Content filtering	X	X	X	X	X	X	X	X	X
Supports API access for SIEM integration or custom analytics	X	X	X	X	X	X	X	X	X
Web interface dashboard	X	X	X	X	X	X	X	X	X
Validates DNSSEC	X		X	X	X	X	X	X	X
DoH/DoT capable	X		X	X	X	X	X	X	X
Enables customizable policies by group, device, or network	X	X	X	X	X	X	X	X	X
Deploys across hybrid architectures	X	X	X	X	X	X	X	X	X

Disclaimer of Endorsement

This document does not constitute a Qualified Products List, within the meaning of the definition of Federal Acquisition Regulation (FAR) 2.101 or a Qualified Manufacturers List under FAR subpart 9.2–Qualification Requirements. The government has not undertaken any testing or evaluation of the products listed under this analysis, but has only reviewed the published attributes of the products. The list is not all-inclusive. This list may be amended and supplemented from time to time as market research discloses other items or as new products become available.

The information and opinions contained in this document are provided “as is” and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Works Cited

[1] Cybersecurity and Infrastructure Security Agency (2020), Addressing Domain Name System Resolution on Federal Networks. Available at: https://www.cisa.gov/sites/default/files/publications/Addressing_DNS_Resolution_on_Federal_Networks_Memo.pdf
[2] Cybersecurity and Infrastructure Security Agency, (2019) Emergency Directive 19-01: Mitigate DNS Infrastructure Tampering. Available at: https://cyber.dhs.gov/ed/19-01/
[3] Office of the Undersecretary of Defense for Acquisition & Sustainment (2020), Cybersecurity Maturity Model Certification. Available at: https://www.acq.osd.mil/cmmc/draft.html
[4] UK National Cyber Security Centre (2017), Protective DNS (PDNS). Available at: https://www.ncsc.gov.uk/information/pdns
[5] National Security Agency (2020), Adopting Encrypted DNS in Enterprise Environments. Available at: https://www.nsa.gov/cybersecurity-guidance

Purpose

This document was developed in furtherance of the NSA and CISA cybersecurity missions, including their responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, Defense Industrial Base, U.S. government, and critical infrastructure information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Trademarks

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov