Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

PROTECTIVE DOMAIN NAME SYSTEM (DNS)

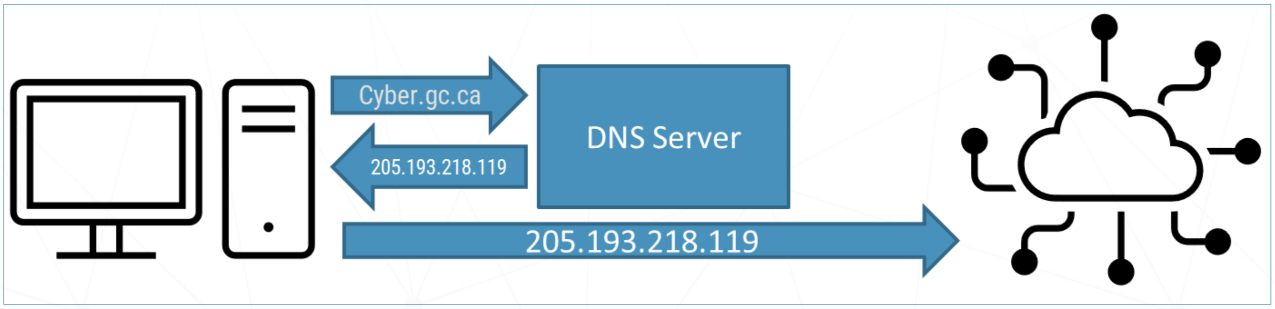
MARCH 2022

ITSAP.40.019

Threat actors frequently use connections to malicious web domains to further compromise victim's systems and data. Industry reports estimate that between 80 to 90 percent of cyber attacks leverage the DNS system. If a threat actor can persuade you or a member of your organization to connect to a malicious website, they can infect your network and devices with malware or steal your data.

WHAT IS DNS?

DNS is a protocol that translates user-friendly web addresses, such as "cyber.gc.ca", into machine-readable IP addresses. It is often referred to as the address book for the Internet. DNS is used for both human-initiated actions (e.g. visiting a website) and machine-initiated actions (e.g. running an update). This translation process is called DNS resolution. DNS queries are required for almost everything your organization does with network applications and online activity. Protective DNS can benefit you as an individual public user or as an organization.



WHAT IS PROTECTIVE DNS?

Protective DNS (PDNS) or DNS firewall is a tool that can be implemented by your organization to protect employees from inadvertently visiting potentially malicious domains on the internet. Malicious domains identified in PDNS blocklists are derived from a variety of cyber threat intelligence sources. These blocklists contain all of the domains that users are prevented from visiting when using corporate IT assets or while on your organization's networks. PDNS typically addresses the following four types of domains: phishing, malware command and control, domain generation algorithms, and content filtering.

DNS ENCRYPTION STANDARDS

There are two options within the DNS protocol to encrypt DNS queries and traffic: DNS over HTTPS (DoH) and DNS over Transport Layer Security (DoT). The intent of both is to increase user privacy and prevent observation and manipulation of DNS. DoT or DoH can provide protections against certain cyber attacks, such as person in the middle (PITM). When determining if your organization will implement DoT or DoH you should consider the risks and benefits of both.

DoT

A protocol for encrypting Domain Name System (DNS) resolution via the Transport Layer Security (TLS) protocol.

DoH

A protocol for performing remote Domain Name System (DNS) resolution via the HTTPS protocol.

For more information on DNS encryption standards, see the National Cyber Security Centre's *Protective DNS for the private sector*

AWARENESS SERIES

Cat. No. D97-1/40-019-2022E-PDF
ISBN 978-0-660-42360-9

BENEFITS OF PROTECTIVE DNS?

By implementing PDNS in your organization, you are adding a layer of defence to protect against malicious domains and potential cyber attacks, like phishing or ransomware. PDNS will also benefit your organization by:

- Informing users of potentially malicious links so they know what to look for and aim to avoid them in the future.
- Detecting potential threats to your networks, systems, and devices and allowing you more time to ensure mitigation measures are in place.
- Protecting mobile devices where traditional anti-virus and anti-malware protection may not apply.
- Offering increased protection if your organization has a bring your own devices (BYOD) policy.
- Protecting users' from malicious sites when a typo is made in entering a URL in a browser.
- Protecting users from websites that have been compromised by a threat actor without the domain owner's knowledge, provided the domain has been flagged as malicious.

FREE VS. PAID PROTECTED DNS SERVICES

There are both free and paid protected DNS services available in Canada. Free DNS services are typically marketed for personal and home use. The Canadian Internet Registration Authority (CIRA) provides a free publicly available protected DNS service called Canadian Shield to ensure personal devices always use a trusted DNS and filter out malicious web domains. Canadian Shield can be set-up on your home router or gateway to better protect your network.

Paid DNS services are usually designed and marketed for organizations. Small and medium sized organizations can procure protected DNS services from vendors within Canada.

HOW DO I SELECT A VENDOR?

Consider the following items when selecting a vendor to supply protective DNS for your home or organizational network:

- Research providers and ensure they have a solid reputation and can demonstrate their experience in cyber security.
- Procure protected DNS services from vendors who allow your organization to have visibility into what is being blocked across your organization.
- Ask vendors for case studies or examples in which their services protected an organization from a potential cyber threat.
- Confirm whether the vendor or a third party performs regular security testing on their own infrastructure.
- Confirm if the vendor provides API access to your DNS query data, including security integration with products like Security Information and Event Management (SIEM).
- Ensure the vendor's service will work across multiple systems and devices, in particular mobile and BYOD devices (if required).
- Determine whether the vendor releases their own security testing and certification results and reports.
- Enquire about your vendor's DNS service analytics and the source of their threat intelligence feeds.

For more information on selecting a protected DNS provider, see *Selecting a Protective DNS Service* from the National Security Agency (NSA) and the Cybersecurity & Infrastructure Security Agency (CISA).

LEARN MORE

- *Protecting Your Organization Against Denial of Service Attacks (ITSAP.80.100)*
- *Secure Your Accounts and Devices With Multi-Factor Authentication (ITSAP.30.030)*
- *Don't Take the Bait: Recognize and Avoid Phishing Attacks (ITSAP.00.101)*
- *Spotting Malicious Email Messages (ITSAP.00.100)*
- *Have you been a victim of cybercrime? (ITSAP.00.037)*
- *Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)*

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**