IT NATION™ SECURE

hosted by CONNECTWISE

opentext™ | Cybersecurity

Regain Control with DNS Leak Prevention

- Jonathan Barnett – Senior Product Manager
- Craig Papke – Senior Manager, Solutions Consulting

IT NATION™ SECURE

Agenda

1 **Background of DNS**

2 **Encryption**

DNS over HTTPS

3 **Why now?**

DNS Exposure

4 **Protective DNS**

The NSA and DNS

5 **Webroot**

DNS Protection

6 **Demo**

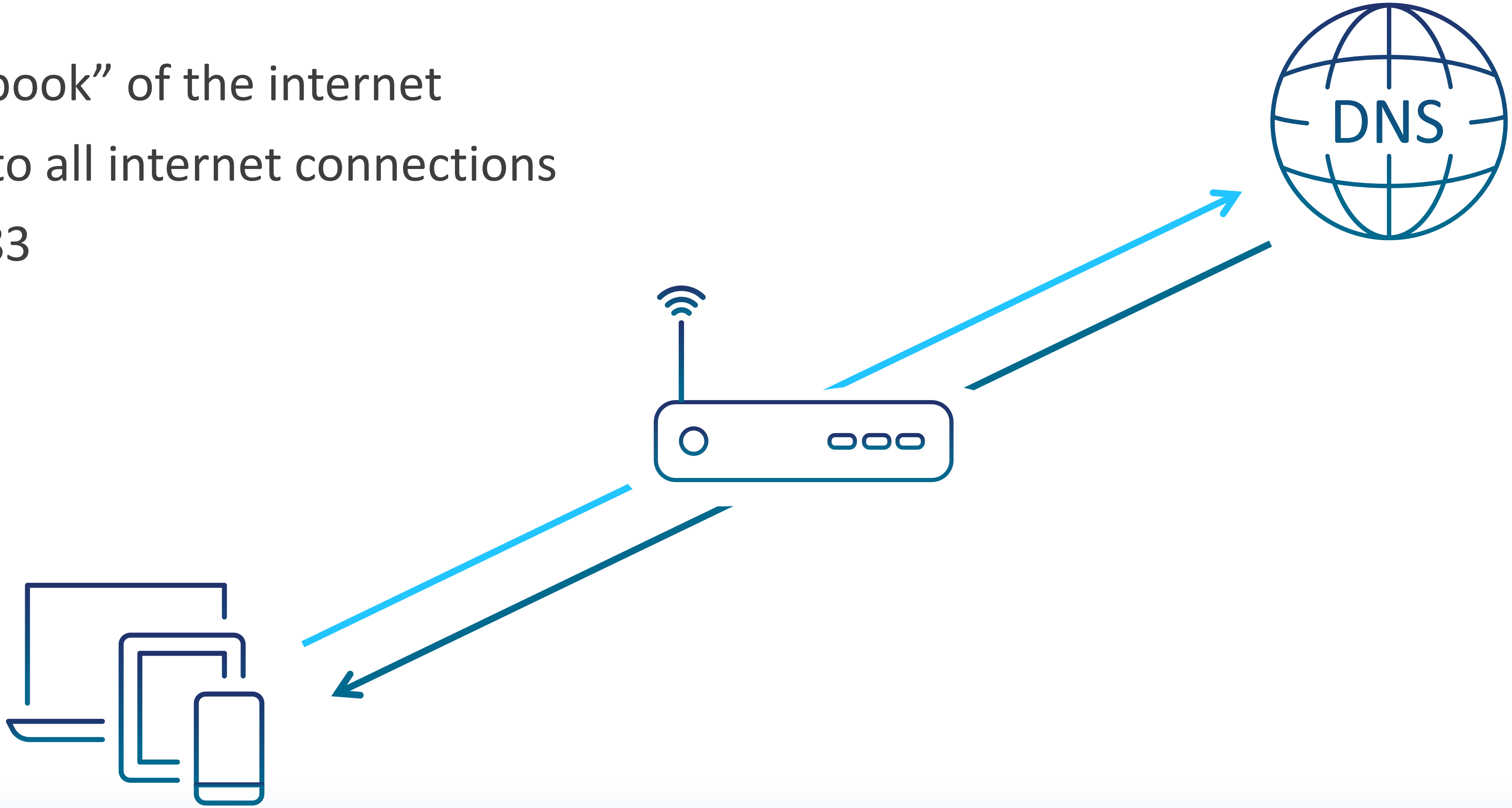
DNS Leak Prevention in action

Today’s DNS

The “address book” of the internet

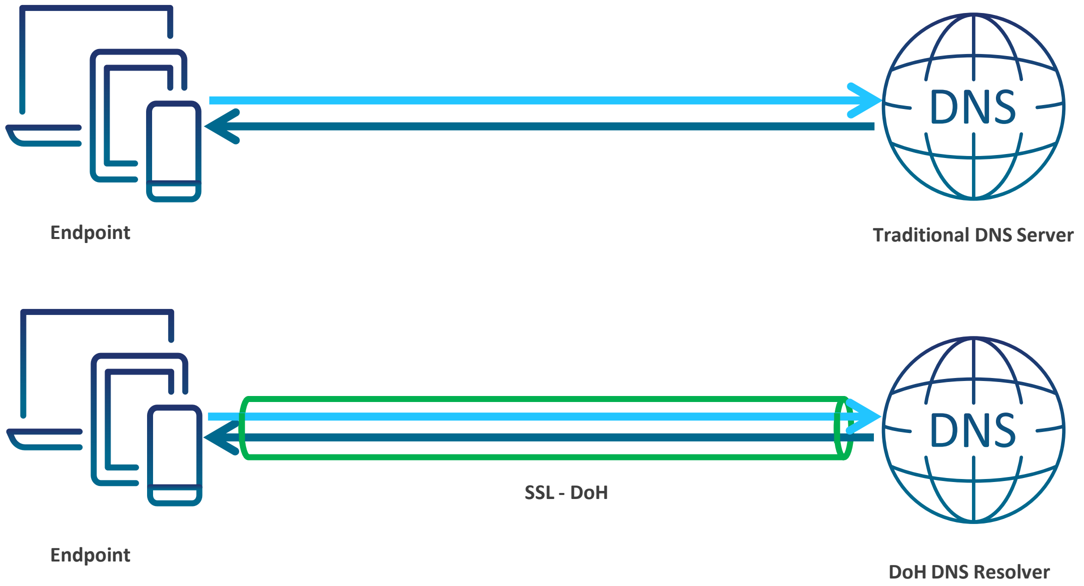
Fundamental to all internet connections

Created in 1983



Adding Encryption with DoH (DNS over HTTPS)

- Mozilla Firefox
- Chromium
- Apple
- Microsoft
  - Windows 11
  - Server 2022



DNS Weaknesses

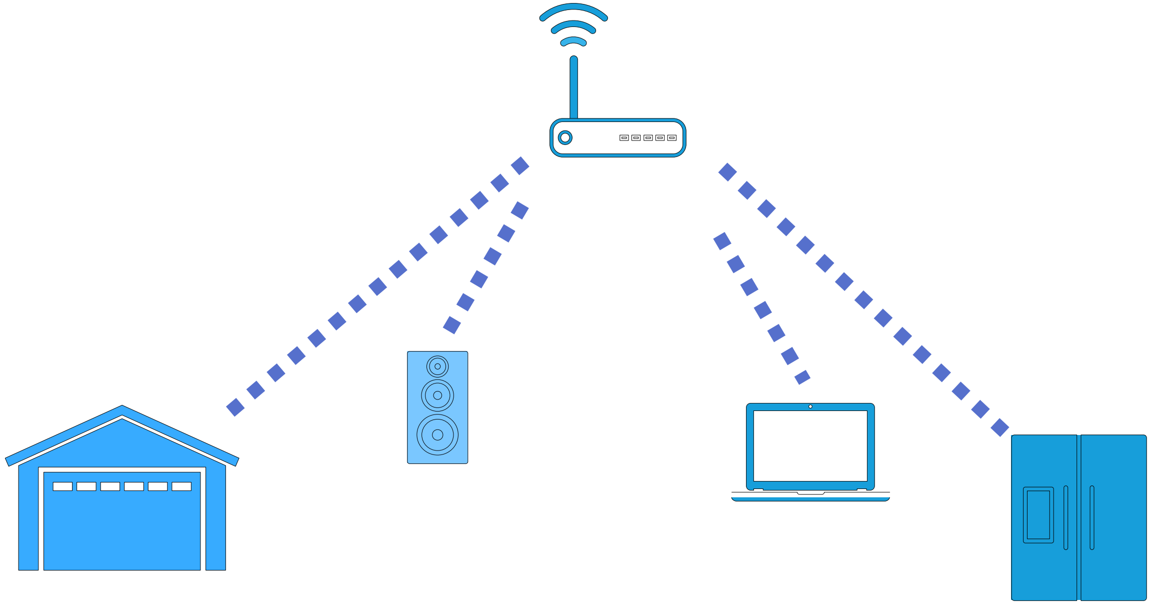
Created in 1983

Security and privacy missing

All communication in clear text

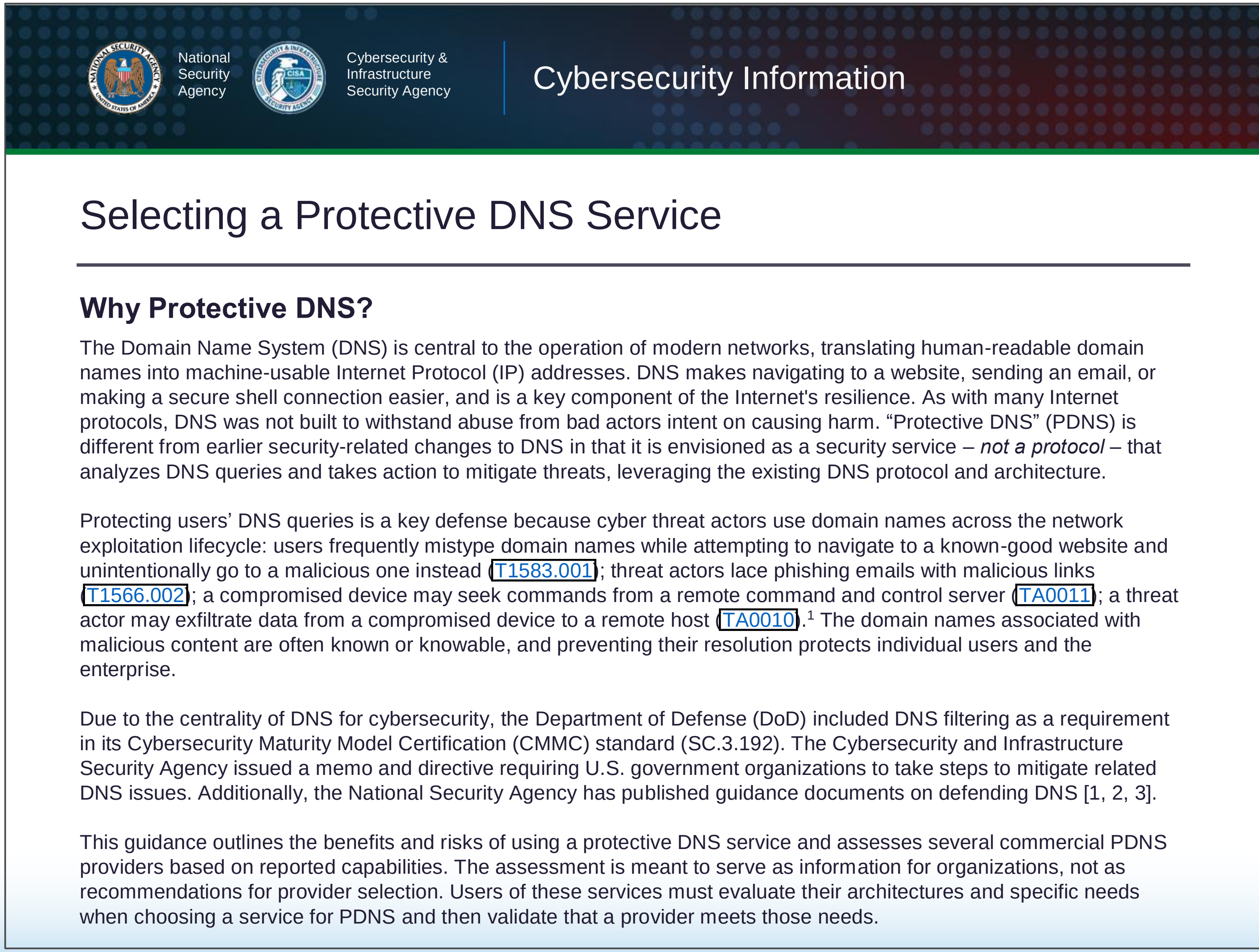
No verification or visibility of resolver

Lacks intelligence



Protective DNS

- Encrypted DNS
- Filtered DNS requests
- Block unauthorized DNS queries
- Reporting – both blocked and allowed



National Security Agency

Cybersecurity & Infrastructure Security Agency

Cybersecurity Information

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.

Possible Solutions

- Block Port 53 and 853 on the Firewall (DNS and DoT)
- Shut off DoH on Browsers
- Block port 443…
- Subscribe to a DNS Filtering Solution

Webroot® DNS Protection

Control and filter DNS requests with the power of BrightCloud Threat Intelligence

Control of DNS

Filter all DNS requests on devices and networks by leveraging Webroot BrightCloud® Threat Intelligence

Remote Agents

Protect devices when not on the corporate network with granular policies, DoH control, and comprehensive logging and reporting.

Easy to Use

- Management through the Webroot® Business Management Console
- Designed for MSPs and SMBs

Standalone DNS Protection Agent

Separate Installer (MSI)

- The DNS Protection agent can now be installed directly on a system or managed through Webroot Endpoint Protection

Standalone DNS in the Webroot Management Console

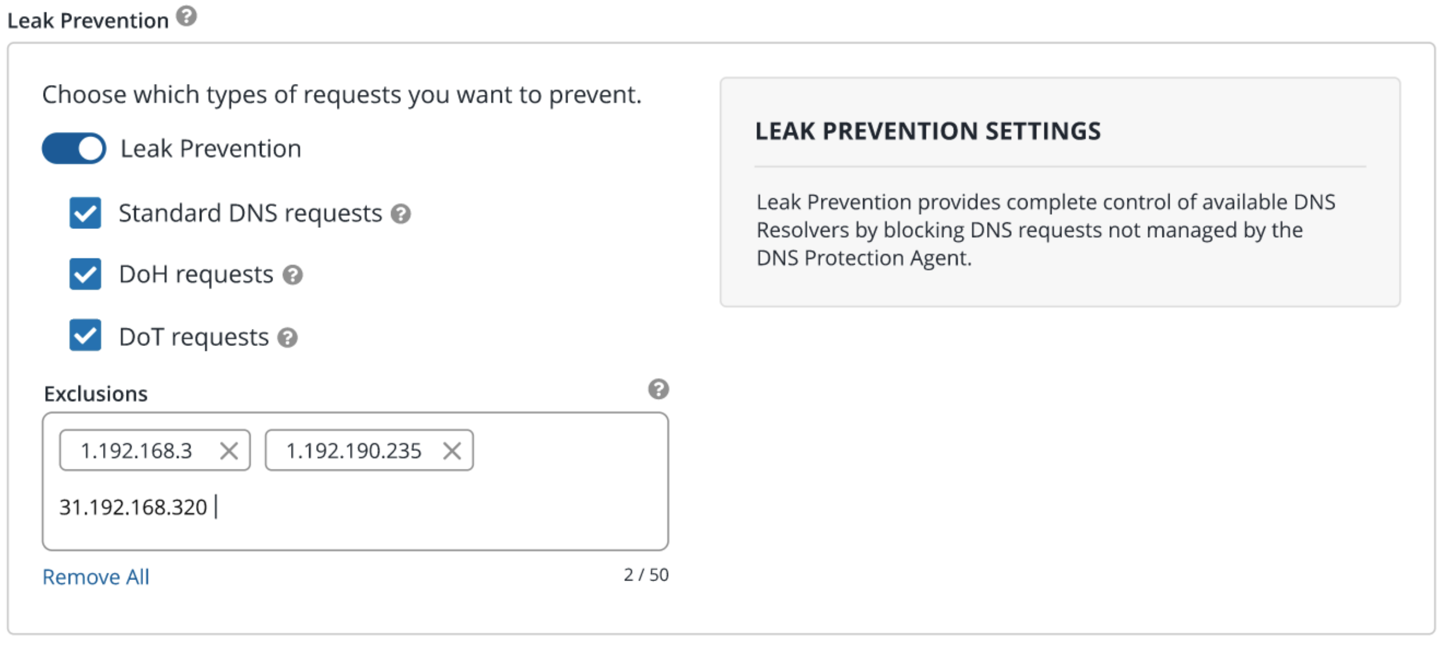
- Devices can be managed in the console with just the DNS Protection settings and reporting.

No changes required

- Current functionality will be maintained, and existing deployments do not require changes.

DNS Leak Prevention

- Industry first, agent-based comprehensive solution
- Blocks port 53, 853, and 443 to known DoH providers (BrightCloud)
- DNS exclusively managed by the DNS Protection Agent
- Log of blocked requests



Leak Prevention

Choose which types of requests you want to prevent.

● Leak Prevention

☑ Standard DNS requests

☑ DoH requests

☑ DoT requests

Exclusions

1.192.168.3 ✕ 1.192.190.235 ✕

31.192.168.320

Remove All

2 / 50

LEAK PREVENTION SETTINGS

Leak Prevention provides complete control of available DNS Resolvers by blocking DNS requests not managed by the DNS Protection Agent.

#ITNation

IT NATION

Demo

DNS Leak Prevention

- Installation
- Configuration
- Blocking
- Exceptions
- Logging

Scan for free trial!

opentext™
Cybersecurity

FLOWCODE

PRIVACY.FLOWCODE.COM

- For more info: cpapke@opentext.com

IT NATION™ SECURE

Questions?

IT NATION™ SECURE

Don't forget to fill out your

SESSION SURVEY