



AFRL-RI-RS-TR-2022-106

MOBILE NETWORK TRAFFIC VISIBILITY FOR THE ENTERPRISE

GUIDEPOINT SECURITY, LLC.

JULY 2022

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

**AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (<http://www.dtic.mil>).

AFRL-RI-RS-TR-2022-106 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /

JAMES L. SIDORAN
Work Unit Manager

/ S /

JAMES S. PERRETTA
Deputy Chief
Information Warfare Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE JULY 2022	2. REPORT TYPE FINAL TECHNICAL REPORT	3. DATES COVERED START DATE AUGUST 2020 END DATE MARCH 2022	
4. TITLE AND SUBTITLE MOBILE NETWORK TRAFFIC VISIBILITY FOR THE ENTERPRISE			
5a. CONTRACT NUMBER FA8750-20-C-1029	5b. GRANT NUMBER N/A	5c. PROGRAM ELEMENT NUMBER	
5d. PROJECT NUMBER	5e. TASK NUMBER	5f. WORK UNIT NUMBER R32Q	
6. AUTHOR(S) Matthew Devers			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Guidepoint Security Government Solutions 2201 Cooperative Way, Suite 225 Herndon VA 20171			8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/RIGA 525 Brooks Road Rome NY 13441-4505		10. SPONSOR/MONITOR'S ACRONYM(S) AFRL/RI	11. SPONSOR/MONITOR'S REPORT NUMBER(S) AFRL-RI-RS-TR-2022-106
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited. PA# AFRL-2022-1942 Date Cleared: 26 Apr 2022			
13. SUPPLEMENTARY NOTES			
14. ABSTRACT This report details methods to improve government visibility of network traffic from mobile devices to identify potential malware, attacks, or attempts to exfiltrate data from or through the device.			
15. SUBJECT TERMS Mobile network security, 4G/5G security, mobile network management			
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT U	b. ABSTRACT U	C. THIS PAGE U	SAR 59
19a. NAME OF RESPONSIBLE PERSON JAMES S. SIDORAN			19b. PHONE NUMBER (Include area code) N/A

TABLE OF CONTENTS

LIST OF FIGURES.....	II
LIST OF TABLES.....	III
1.0 SUMMARY.....	1
2.0 INTRODUCTION	2
3.0 METHODS, ASSUMPTIONS, AND PROCEDURES.....	5
3.1 ASSUMPTIONS	5
3.2 METHODS	5
3.2.1 PDNS provider and host agent evaluation was conducted as follow:.....	5
3.2.2 Mobile Device Management evaluation.....	6
3.3 PROCEDURES	7
3.3.1 PDNS provider and host agent evaluation	7
3.3.2 Mobile Device Management evaluation.....	12
4.0 RESULTS AND DISCUSSION.....	13
4.1 PDNS SERVICE PROVIDER AND ENDPOINT AGENT - CLOUDFLARE	13
4.1.1 Cloudflare Results Summary	13
4.1.2 Project Scope and Objectives Results.....	14
4.1.3 Test Methodology	16
4.1.4 Detailed test results	18
4.2 MOBILE DEVICE MANAGEMENT PROVIDER.....	25
5.0 CONCLUSIONS	28
6.0 REFERENCES	30
APPENDIX A: PUBLICATIONS AND PRESENTATIONS	31
APPENDIX B: CLOUDFLARE EVALUATION PROCEDURE SCREENSHOTS	32
LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS	53

LIST OF FIGURES

Figure 1. Traditional Network Architecture	3
Figure 2. Target Network Architecture (Desired Solution)	4
Figure 3. Protective DNS sequence in a Wi-Fi environment.....	7
Figure 4. Protective DNS sequence in a cellular environment	8

LIST OF TABLES

Table 1. Hardware device test list.....	9
Table 2. Cloudflare Results.....	19
Table 3. MDM Requirements Evaluation.....	27

1.0 SUMMARY

According to the 2016 Cisco Annual Security Report (p. 19), over 90% of malware uses the Domain Name System (DNS) in a cyber-attacks. Protecting mobile endpoints by securing the DNS layer of mobile network traffic is an “essential” part of an enterprise’s cyber security maturity model (NSA/CISA “Selecting a Protective DNS Service). GuidePoint Security was selected as part of the Department of Homeland Security’s (DHS) Science and Technology’s Secure Resilient Mobile Network Infrastructure (SRMNI) project to research the capabilities, requirements, and limitations of a Protective DNS solution for agencies.

Protective DNS is the process of “sink holing” domain name queries that are identified as malicious, potentially malicious, or violate corporate policy by refusing to respond to a query with the proper IP address of the requested resource, effectively terminating a connection. DHS supports this technology with its Einstein 3 Accelerated DNS service for agency networks, but does not support mobile endpoints (CISA, Addressing Domain Name System Resolution on Federal Networks).

GuidePoint Security’s work in the SRMNI is to identify how using Protective DNS enables DHS and its subagencies to **track, filter, and identify** different types of mobile traffic, while implanting controls that **attribute** queries and **authenticate** devices and users to the Protective DNS provider.

GuidePoint Security evaluated various Protective DNS providers, including Cisco Umbrella and DNS Filter for their efficacy in protecting mobile endpoints, before conducting a more thorough evaluation of Cloudflare’s Protective DNS service.

GuidePoint Security evaluated the capability of Cloudflare’s Protective DNS service on iOS and Android mobile endpoints by deploying their Cloudflare WARP app (also known as the 1.1.1.1 app), and complemented the deployment with various Mobile Device Management (MDM) vendors to enforce required mobile configurations and policy.

By deploying the Cloudflare WARP app on mobile endpoints, GuidePoint Security has demonstrated that it is possible to implement a Protective DNS posture against mobile devices which supports the authentication and attribution requirements necessary for incident response. Additionally, the solution demonstrated the capability to track mobile traffic by domain name, and subsequently filter mobile traffic by enforcing a Protective DNS policy. The Cloudflare WARP application utilizes DNS over Hyper Text Transfer Protocol Secure (HTTPS) as its transport mechanism, which supports CISA’s goal of enforcing encrypting DNS traffic to improve security and reduce manipulation of DNS data.

However, Protective DNS has limitations on mobile endpoints, and should be integrated with other technical solutions that complement mobile policy enforcement. GuidePoint Security has various recommendations for those technical controls throughout this report.

2.0 INTRODUCTION

The objective of this project, Mobile Network Traffic Visibility for the Enterprise, is to develop and implement a virtual Trusted Internet Connection (vTIC) for the Government, specifically the Department of Homeland Security, that will track mobile users' traffic, filter that traffic (specifically the DNS protocol), and categorize that mobile traffic to filter and identify malicious threats and actors.

As the workforce has become more mobile with Android and Apple devices, the traditional network perimeter security model has become inadequate to protect those devices. Backhauling traffic from mobile devices to a Trusted Internet Connection can be cumbersome and inefficient, with bandwidth limitations at the TIC impeding the ability for mobile users to do their work. When users find alternatives to routing their traffic through a TIC, this negatively impacts the security posture of the device, and can introduce security threats to an agency's network. Oftentimes, users simply won't be able to conduct their work.

The DNS protocol was specifically chosen for this project based on its ubiquity across the internet, and more specifically, because its use in the network exploitation lifecycle makes protecting the protocol from abuse key in a comprehensive cyber defense strategy (NSA/CISA "Selecting a Protective DNS Service).

Presently, the Cybersecurity and Infrastructure Security Agency requires U.S. government organizations to mitigate DNS issues by using a CISA provided DNS resolver. This DNS resolver falls under the Einstein 3 Accelerated (E3A) program (CISA DNS memorandum), which works to identify and block cyberattacks¹.

One of the limitations of this program is that its ability to identify and mitigate cyberattacks that are abusing the DNS protocol only applies to Federal Civilian Executive Branch (FCEB) agencies' static networks. Users utilizing mobile devices do not experience the intrusion protection capabilities that E3A provides.

The aim of this project is to research the technologies and capabilities that can improve CISA's ability to provide a comparable level of protection as E3A provides to sub-agencies mobile devices, by deploying the same capabilities to mobile devices. This capability is specific to "Protective DNS," or DNS sink-holing.

DNS sink-holing blocks access to malicious infrastructure by overriding public DNS records that have been identified as harmful.

The three problems that GuidePoint Security is attempting to solve are these²:

1. **Route** mobile DNS traffic to a centralized PDNS service. This applies to Wi-Fi and cellular connections, plain text DNS (TCP/UDP port 53), DNS over HTTPS (DoH), and DNS over TLS (DoT), for both IPv4 and IPv6 space.

¹ E3A program: <https://www.cisa.gov/einstein>

² Mobile Network Traffic Visibility for the Enterprise Target Capabilities Definition v2 (28 October 2021)

2. **Authenticate** the mobile device to protective DNS provider to prevent unauthorized access.
3. **Attribute** DNS queries to organizations that are using the protective DNS service, to prevent unauthorized access. If able, attribute those queries to the end device, not just the organization.

The traditional network architecture is easily able to provide a protective DNS service to static endpoints by intercepting and redirecting all DNS queries to a PDNS provider.

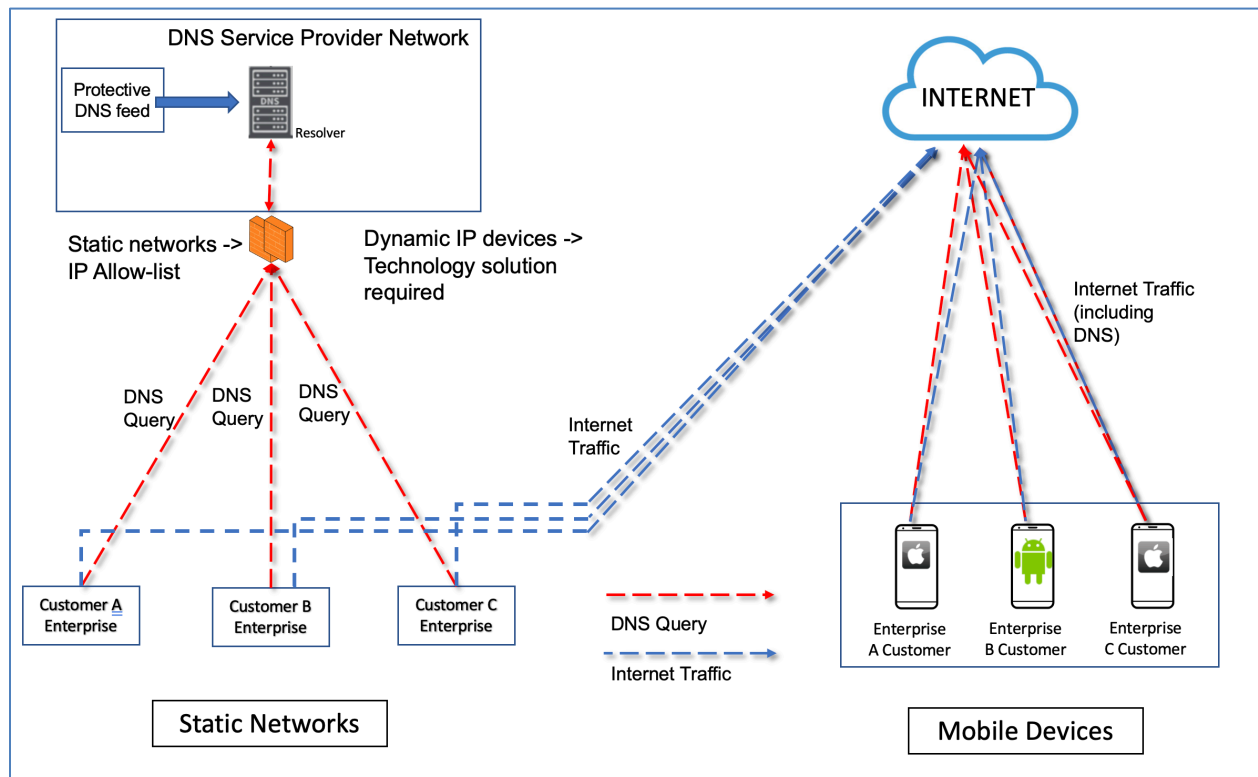


Figure 1. Traditional Network Architecture

To intercept network traffic from mobile devices requires a different approach, as they do not remain stationary on an enterprise's static network. Traditionally, enterprises would deploy Virtual Private Network (VPN) software on an endpoint, but this violates one of the central requirements of the project: do not backhaul all endpoint traffic to an enterprise's trusted internet connection.

Certain vendor solutions provide "virtual" Trusted Internet Connection (or vTIC) services, which route endpoint traffic through their cloud-based filtering solutions before routing it to the internet, and are specifically designed for the mobile workforce. To be most specific, this Protective DNS solution is designed to route only the DNS traffic that a mobile endpoint produces, regardless of its transport mechanism (DNS over port 53, DNS over TLS, or DNS over HTTPS).

Figure 2 depicts the logical design of DNS data from mobile endpoints over a network.

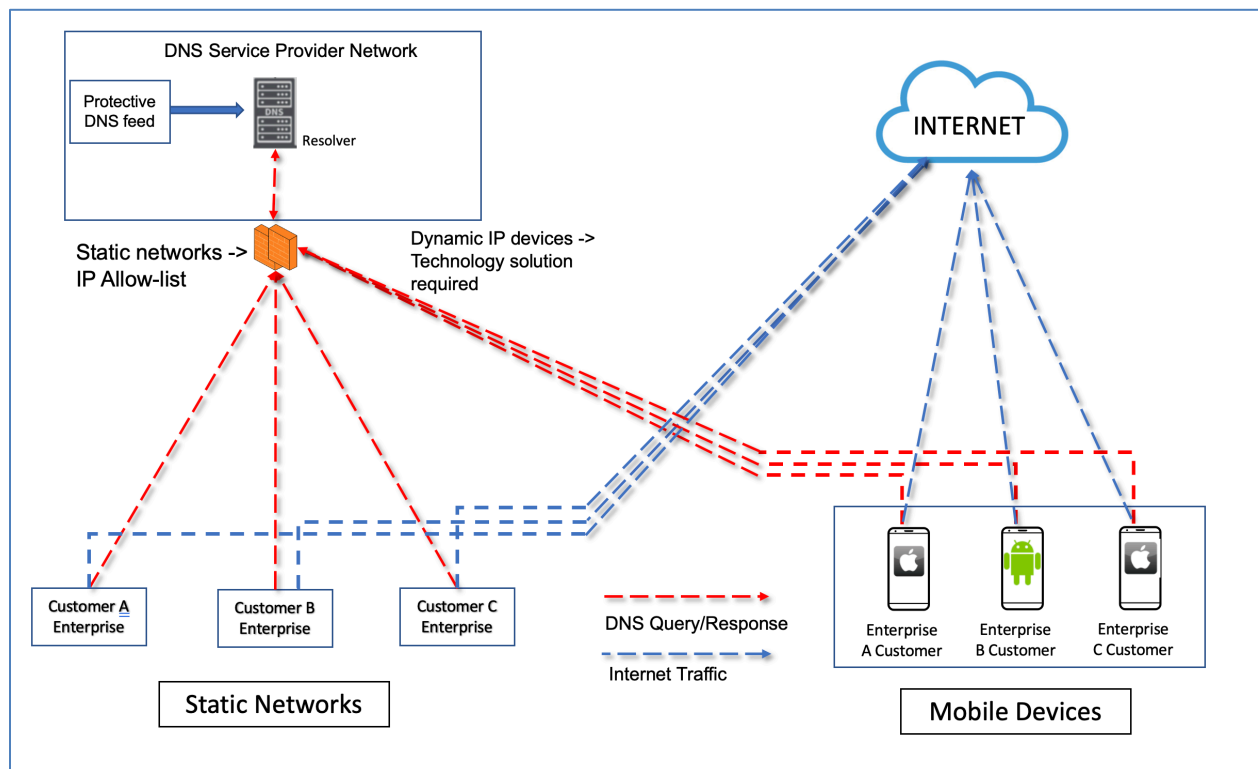


Figure 2. Target Network Architecture (Desired Solution)

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1 Assumptions

1. While logging is a core requirement of a Protective DNS solution, GPS is not required to implement it in this proof of concept.
2. Up to date, modern cellular devices are sufficient for testing. FCEB agencies might utilize older models of devices, but the Android devices: Samsung S21, Samsung Galaxy Tablet S7+, Samsung Z Fold 3 (all running Android version 12), and Apple devices: iPhone 12 pro, iPad Pro, and iPad Air (all running iOS/iPadOS version 14.7+) are sufficiently representative of the technologies being tested.
3. Some vendors provide solutions that are commercially available before going through the FedRAMP process. GPS assumes that the capabilities available in commercial vendor offerings will be the same available in the government version of a solution.

3.2 Methods

To meet the scoping requirements of the original project, as well as wholistically evaluate what this deployment would entail at the scale of thousands of endpoints, the deployment methodology was divided into two categories:

1. Evaluation of a protective DNS provider and host agent.
2. Evaluation of mobile device managers.

As part of the Mobile Network Traffic Visibility for the Enterprise, the PDNS evaluation focuses on the technical requirements of the PDNS as established in *Target Capabilities Definition version 1*, *Target Capabilities Definition version 2*, as well as the *Go No Go Evaluation Plan version 2*, while the Mobile Device Management (MDM) evaluation pulls its requirements from *Target Capabilities Definition Document version 2*.

3.2.1. PDNS provider and host agent evaluation was conducted as follow:

1. Install a protective DNS host agent on the test devices, in this case fully updated iOS/iPadOS and Android endpoints.
2. Verify that the DNS endpoint agent “intercepts” network packets at the operating system level to prevent circumvention or leakage.
 - a. This interception should be for all DNS packets, regardless of transport mechanism (DNS over 53, DoT, or DoH).
 - b. If the mobile device is using a “work profile” verify that work profile applications have their DNS traffic intercepted.
3. Validate that the PDNS service provider authenticates endpoints before authorizing DNS queries.
4. Verify that the PDNS service provider enforces DNS policy by rejecting queries to unauthorized/malicious domain names by forcing the devices to query test domain names.
5. Validate that the PDNS service provider attributes DNS queries to mobile endpoints.

6. Verify the PDNS service provider is authenticating devices and/or user.

3.2.2. Mobile Device Management evaluation

Utilizing a mobile device management solution ensures that the PDNS endpoint agent is deployed correctly to endpoints. The MDM evaluation method was not factored into the design of the original solution, but added later to ensure a wholistic deployment methodology. To ensure increased endpoint security posture, an evaluation was conducted across multiple MDM providers. The following criteria was used to evaluate the MDM:

1. The MDM should integrate with the same IDAM solution used to authorize client devices to the PDNS service provider.
2. Verify that the MDM restricts application removal.
3. Verify that operating system DNS settings, such as DoH or DoT, are restricted.
4. Verify that browser-based DNS settings are restricted.
5. Verify that mobile application configurations are deployable “over the air.”

3.3 Procedures

3.3.1. PDNS provider and host agent evaluation

To test the protective DNS agent against the requirements of this project, a target network architecture is developed, and host agents are deployed on mobile clients to intercept and redirect DNS traffic. A test environment is required for both Wi-Fi network interception and cellular testing

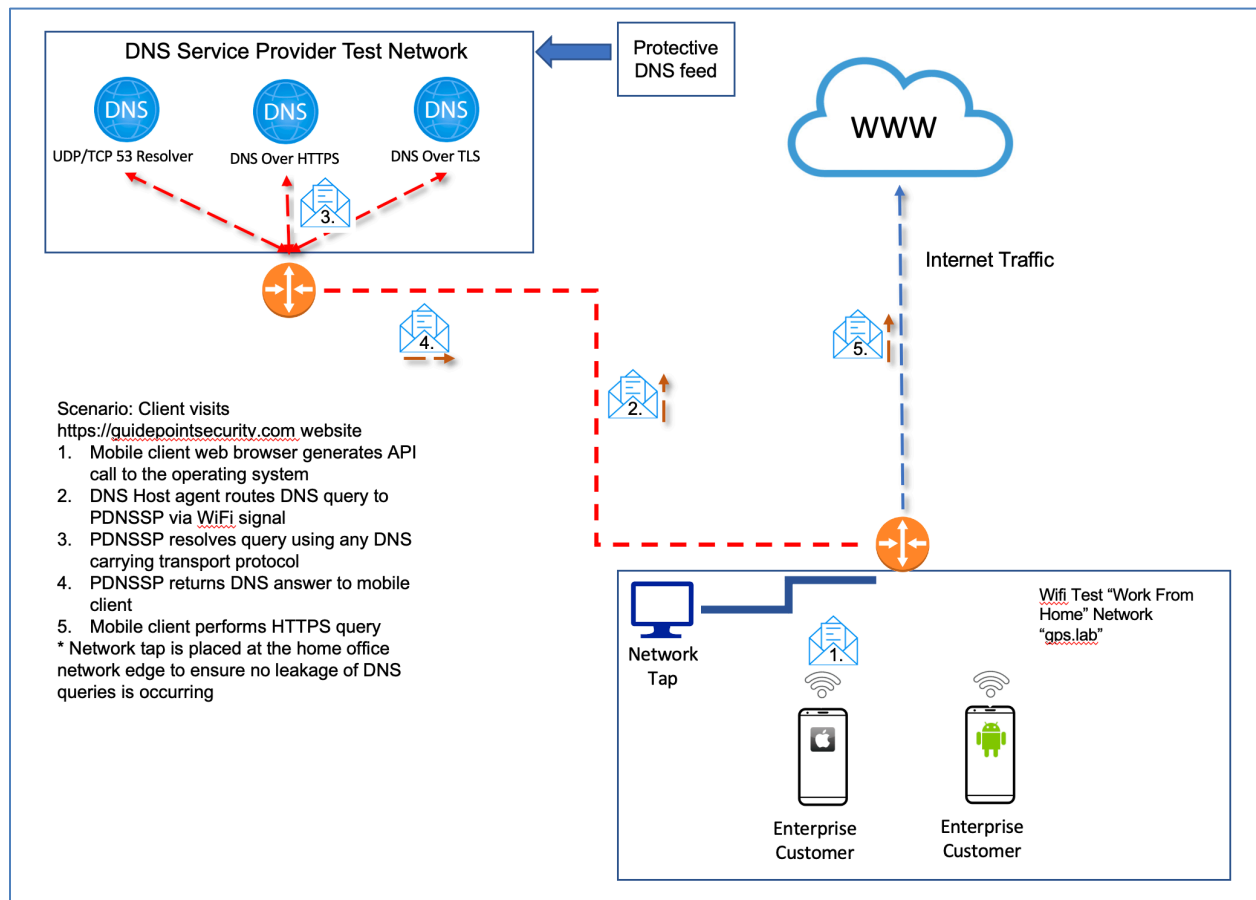


Figure 3. Protective DNS sequence in a Wi-Fi environment

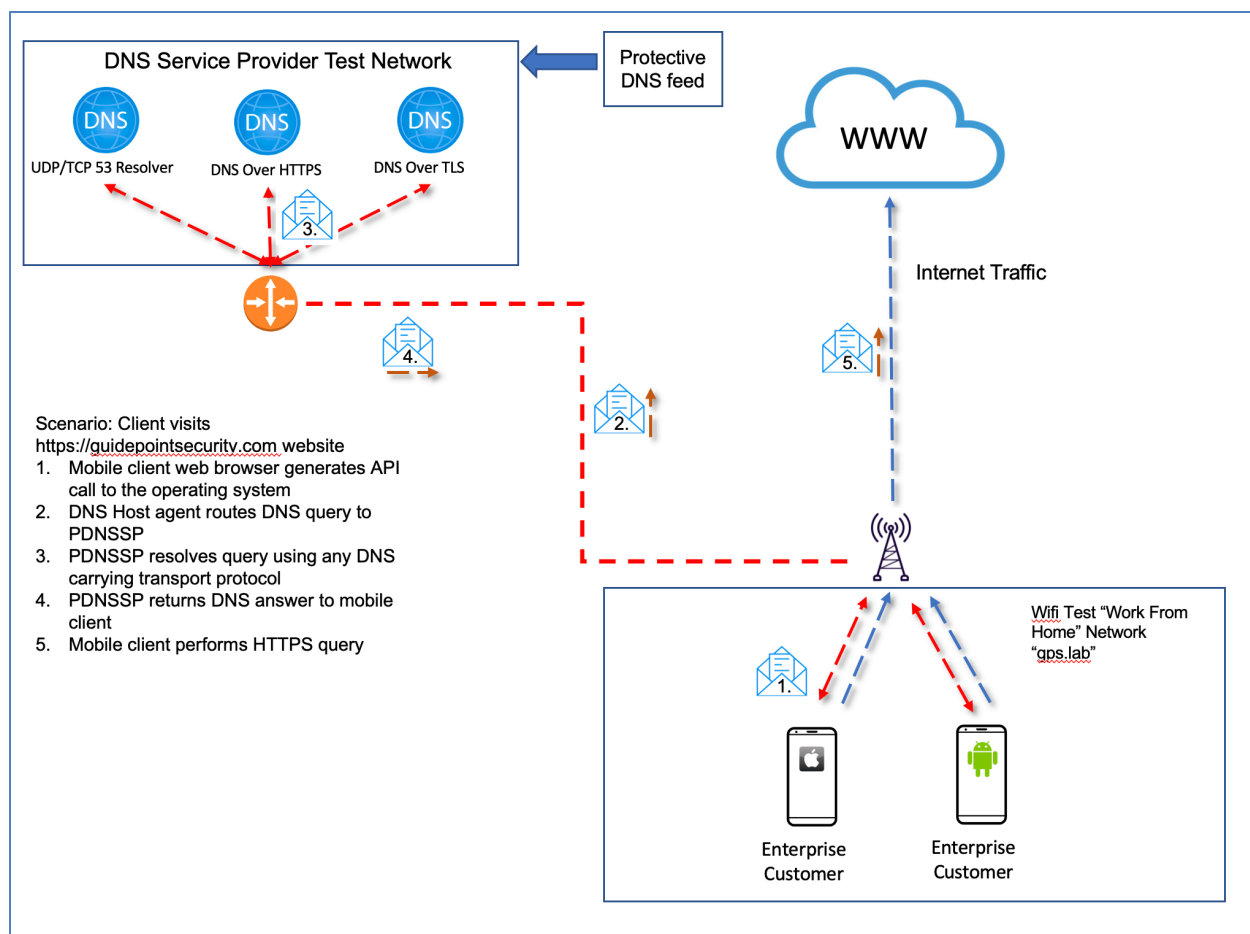


Figure 4. Protective DNS sequence in a cellular environment

Evaluation criteria for the testing procedure is specified in the Go No Go Evaluation Plan.

3.3.1.1. Hardware devices

The following devices will be used as a representative test.

Table 1. Hardware device test list

Hardware	Operating System	Cellular Test	Wi-Fi Test
Samsung Galaxy Tablet S7+ (model SM-T978U)	Android (version 11 or greater)	X	X
Samsung Galaxy Z Fold3	Android (version 11 or greater)	X	X
Samsung Galaxy S21	Android (version 11 or greater)	X	X
iPad Air (4 th Gen, model #A2324)	iPadOS, version 14.7 or greater	X	X
iPad Pro (2 nd Gen, model #A2068)	iPadOS, version 14.7 or greater	X	X
iPhone12 (model #A2172)	iOS version 14.7 or greater	X	X

3.3.1.2. Network packet capture

To validate the DNS traffic under the Wi-Fi configuration, access to the edge firewall with a packet capture capability (i.e., secure shell and tcpdump) should be used.

For conducting network capture of cellular iOS devices, an up-to-date MacBook Pro or MacBook Air with developer tools: <https://developer.apple.com/documentation/network/recording-a-packet-trace>.

For conducting a simulated cellular network capture of Android devices: Android Studio and the official Android Emulator (<https://developer.android.com/studio>).

3.3.1.3. Software

For testing, a small website is necessary to generate an appropriate level of DNS traffic, without extraneous, undesired DNS queries. For this evaluation, the following website/domain names will be used:

- *.guidepointsecuritydemo2.dom
- *.blockdns.guidepointsecuritydemo2.com
- *.ipv6.guidepointsecuritydemo2.com
- *.blockdns.ipv6.guidepointsecuritydemo2.com

3.3.1.4. Expected results

1. All the DNS traffic from the testing device is routed to the protective DNS provider using an observable³ network protocol (plaintext DNS, DNS over TLS),
OR (1 or 2)
2. Regardless of the DNS transport mechanism used, no DNS traffic is visibly going to an alternate DNS provider (i.e., a rogue application is attempting to make DNS queries using a hard programmed DNS resolver).
(1 OR 2) AND 3
3. The protective DNS providers logs that each domain lookup performed by the mobile client is present in the dashboard. If the queries are not present, this indicative of an alternate DNS provider being used.

3.3.1.5. Wi-Fi Test

Web Browser Test

Perform against all major browsers on the endpoint:

1. Start a network packet capture on the network exit point (see target architecture)
2. Verify the DNS agent is operational on the endpoint
3. Disconnect and reconnect to WI-FI. This should clear the devices DNS cache.
4. Clear any browser history, and start desired browser in “InPrivate” or “Incognito” mode to prevent web caching
5. From a web browser on the mobile device, browser to the following web addresses:
 - a. <https://home.guidepointsecuritydemo2.com>
 - b. <https://site1.guidepointsecuritydemo2.com>
 - c. <https://site2.guidepointsecuritydemo2.com>
 - d. <https://site3.guidepointsecuritydemo2.com>
 - e. <https://site4.guidepointsecuritydemo2.com>
 - f. <https://blockdns.guidepointsecuritydemo2.com>
6. For Android devices, repeat this lookup on Chrome, Firefox, and Microsoft Edge browsers from the **WORK** profile of the device (if it is not a fully managed device). Android work profiles separate managed applications from personal applications, and the network stacks associated should be different.
7. For iOS devices, utilize Safari, Chrome, Firefox, and Microsoft Edge
8. Verify that the domains resolved, and that the appropriate blocked domains did not resolve, or presented a block page.

³ Observable meaning that plaintext DNS over port 53, or DNS over TLS is observable because it is characterized by TLS traffic on TCP port 853. DNS over HTTPS is difficult to observe as network traffic independent over of typical HTTPS web traffic.

Non-Web Protocol Test

1. Install various applications that do not use Web ports (TCP 80, TCP 443), to ensure that the DNS host agent is not only proxying web traffic. i.e. install a terminal client on the endpoint.
2. Start a network packet capture on the network exit point (see target architecture)
3. Attempt to SSH to a cloud based server from that application
 - a. `ssh username@home.guidepointsecuritydemo2.com`
 - b. `ssh username@blockdns.guidepointsecuritydemo2.com`

IPv6

1. Reconfigure the Wi-Fi network to only issue IPv6 addresses.
2. Validate proper IPv6 configuration by visiting an IPv6 address checker. i.e. <https://ifconfig.io>, <https://ifconfig.me>
3. Repeat the Web Browser Test and Non-Web Protocol Test

3.3.1.6. Cellular Test

Web Browser Test

Repeat the same tests as the Wi-Fi tests, use the procedures from the Android Developer network for capturing emulated cellular traffic (<https://developer.android.com/studio/run/emulator-networking>), and the iOS tools for cellular traffic capture (https://developer.apple.com/documentation/network/recording_a_packet_trace) to test the iOS devices.

Non-Web Protocol Test

Repeat the same tests as the Wi-Fi tests, use the procedures from the Android Developer network for capturing emulated cellular traffic (<https://developer.android.com/studio/run/emulator-networking>), and the iOS tools for cellular traffic capture (https://developer.apple.com/documentation/network/recording_a_packet_trace) to test the iOS devices.

See Appendix B for visual depiction of the procedure used during testing. Appendix B contains a representative sampling of all the conditions that should be tested.

3.3.2. Mobile Device Management evaluation

Procedures for the evaluation of MDM solutions followed a more specific “configure and validate” methodology than the PDNS agent test. This is because various vendors implement their MDM solutions differently, but they all utilize the underlying mobile operating system enterprise management API. The evaluation is not simply against the MDM, but also the MDM’s implementation of features available in the operating system’s enterprise management.

Some of the most prominent MDMs were evaluated against the requirements listed in Target Capabilities Definition Documentation v2, for their ability to deploy the PDNS solution at scale, as well as improve mobile security posture by eliminating misconfiguration and preventing circumvention.

For the procedure used to deploy and evaluate VMware Workspace ONE, please see Pilot Test Group 1 Report.

For the procedure used to deploy and evaluate Microsoft Intune/Endpoint Manager, please see Pilot Test Group 2 Report.

For the procedure used to deploy and evaluate MobileIron Cloud, see Pilot Test Group 3 Report.

4.0 RESULTS AND DISCUSSION

4.1 PDNS Service Provider and Endpoint Agent - Cloudflare

Multiple Protective DNS vendor solutions were tested for their wholistic approach to DNS protection. However, to support DHS and CISA's long term goals and integration with the Secure Resilient Mobile Network Infrastructure (SRMNI) project, Cloudflare was selected as the Protective DNS vendor of choice for final, extensive testing.

Documentation: <https://developers.cloudflare.com/cloudflare-one/>

Overall Results:

Tests: 130

Passed: 113

Not tested: 17

4.1.1. Cloudflare Results Summary

The Cloudflare WARP agent⁴, when deployed via a mobile device manager and integrated with the Cloudflare Zero Trust platform, was effective at enforcing DNS policy across all mobile web browsers on both up to date⁵ Android and iOS devices. Contrary to the test results generated in September for the original evaluation in September of 2021, the Cloudflare WARP client, when operating in DNS over HTTPS mode, provides attribution in the Cloudflare console logs for both users and devices.

The testing methodology was to test all devices under all types of transport conditions: IPv4, IPv6, Wi-Fi, and cellular, verifying that DNS queries were intercepted/redirect to the Cloudflare resolver service. The results demonstrated that the transport mechanism for DNS is decoupled from the Cloudflare agent's DNS policy, so long as the Cloudflare agent is supported on the device, protection is available. If additional tests were conducted using other transport mechanisms to send DNS queries, the results would likely be the same. The Cloudflare agent for Protective DNS, deployed with a threat intelligence feed into its protective DNS policy, will improve any agency's mobile security posture.

See section 4.1.4.1 - Android over IPv6 – Wi-Fi and section 4.1.4.2 - Android over IPv6 - Cellular for information about the limitations in testing Android on IPv6.

⁴ These test results were initially published in the Go/No Go Evaluation v2 (Revision 2, 7 September 2021). They have been updated to reflect the current state of Cloudflare's deployment. The Go/No Go evaluation test was evaluated at 65/129 tests, with Cloudflare not providing attribution at that time.

⁵ *Up to date* for this test case indicates Android devices (Samsung Galaxy S7+ tablet, Samsung S21, or Samsung Fold Z3 5G with Android 11 or above, and the iPhone 12 with iOS version 14.7 or above, or the iPad Air (4th Gen, model #A2324) or the iPad Pro (2nd generation, model #A2068) with iPadOS version 14.7 or above.

While the Protective DNS capability provided by the Cloudflare solution will improve any agencies security posture, it should not be the only technical control implemented to provide endpoint security or network traffic filtering. The Cloudflare agent intercepts DNS queries generated by applications on mobile devices, so those queries must be in plaintext or generated using a cipher that the Cloudflare agent can intercept and decrypt. Malicious applications could generate their own DNS queries and submit them to any DNS over HTTPS or DNS over TLS resolver, without the Cloudflare agent being able to decrypt the traffic (especially if technologies such as PKI certificate pinning are used). Mobile device management policies that can restrict unwanted applications, or only install applications from an allow-list, and limit the potential DNS configurations of the mobile operating systems are an essential part of a wholistic security program.

Additionally, Protective DNS (not specifically Cloudflare) does not provide DNS based protection to connections made which do not use DNS, such as direct IP connections (National Security Agency and Cybersecurity Infrastructure & Security Agency, *Selecting a Protective DNS Service*). The Cloudflare WARP agent provides alternative controls that can still provide protections (such as operating Cloudflare in full proxy mode), but this method does not fall under the category of Protective DNS.

4.1.2. Project Scope and Objectives Results

Project Scope

- Scope Question 1: Can agencies identify suspicious DNS network traffic?

YES. The Cloudflare Zero Trust service intercepts DNS queries on mobile devices and directs them to Cloudflare's DNS resolver. This enables Cloudflare to log DNS queries. Those queries can be analyzed for suspicious behavior via the Cloudflare Zero Trust console, or via a SIEM (Security Information and Event Management) when the Cloudflare solution is configured with log aggregation and offsite log forwarding.

- Scope Question 2: Can agencies filter DNS traffic?

YES. The Cloudflare Zero Trust service (Cloudflare Gateway) intercepts DNS queries on mobile devices and directs them to the Cloudflare resolver. If a DNS query violates a configuration policy, that query is returned to the client with a DNS redirect to a customizable block page. The Cloudflare Zero trust console enable administrators to filter DNS traffic with multiple methods, including filtering by category (social media, malware, adult material, etc.)

- Scope Question 3: Can agencies categorize traffic based on DNS lookups?

YES. The Cloudflare WARP client intercepts DNS queries on mobile devices and directs them to the Cloudflare DNS resolver service based on the configured Cloudflare tenant.

Those queries are logged in the Cloudflare Zero Trust console. Those logs can be categorized based on available agency threat intelligence. Additionally, Cloudflare categorizes domain names internally based on various behaviors and purposes (domain age, reputation, social media, malware, adult material, etc.). The Cloudflare categories can be used to deploy domain blocking policy.

Project Objectives

- **Problem 1:** Force routing mobile DNS traffic to a centralized PDNS service of CISA's choice. This applies to both Wi-Fi and mobile DNS (i.e., standard DNS) traffic over IPv4 and IPv6 Port 53. DHS is also interested in learning if this is applicable to DNS over HTTPs (DoH), and DNS over TLS (DoT) traffic and possible solutions.

YES. The Cloudflare test results demonstrated that the Cloudflare agent intercepts most DNS queries (excluding operating system DNS queries), regardless of the transport mechanism (Wi-Fi or cellular, IPv4 or IPv6), by intercepting all application generated DNS queries and directing them to a DNS resolver owned and operated by Cloudflare. All DNS queries directed towards the Cloudflare DNS resolver are transported over HTTPS when using the mobile agent on Android or iOS.

- **Problem 2:** Authenticate device to protective DNS provider to prevent unauthorized access.

Mixed Results. Users are authenticated to the service through the Cloudflare agent deployed on the device. However, at this time, unauthenticated users can use the Cloudflare resolver service if they know the DNS sub-domain associated with a team's Cloudflare tenant (without using the Cloudflare agent). For example, a DNS over HTTPS uniform resource locator (URL) could look like this:

<https://oi6eykxg3f.cloudflare-gateway.com/dns-query>.

Only the "oi6eykxg3f" subdomain is specific to this example test tenant, so a malicious actor or benign user could configure their mobile device for DNS over HTTPS or DNS over TLS with that tenant URL and perform DNS queries against it by configuring DNS over TLS in the base operating system (Android version 9+ specifically), or DNS over HTTPS in their mobile browser. Those DNS queries are logged in the Cloudflare Zero Trust console associated with the tenant which owns the DNS sub-domain, but no user attribution would be possible without authentication.

While users are unlikely to be able to guess the sub-domain associated with a specific tenant, due to the nature of how DNS over HTTPS lookups are conducted with a plaintext query first⁶, it is highly improbable to maintain secrecy of these subdomains.

Problem 3: Attribute DNS queries to organization that owns device.

YES. When users authenticate to their Cloudflare tenant through the Cloudflare WARP application, DNS queries generated by the mobile device are sent to Cloudflare’s resolver service. Those queries are attributed to both the user and the device via user ID and device ID. Administrators can view DNS logs in the Cloudflare Zero trust console, or in a SIEM if Cloudflare Gateway logs were pushed to another logging service.

4.1.3. Test Methodology

A Cloudflare for Teams demo tenant on the commercial sector was established (Cloudflare does not have separate government/FedRAMP tenants at this time).

Apple iOS devices (iPad Air, 4th generation, iOS version 14.7), was placed into supervised mode. Both Android (Samsung Galaxy Tablet S7+, Android version 11) and iOS devices were enrolled in VMware’s Unified Endpoint Manager (UEM). The Cloudflare WARP agent (also called ‘1.1.1.1’) was pushed to the devices with policy, and the Cloudflare configuration was published which enrolled the devices into the provisioned tenant.

“1dot1” was the configured tunnel method for the Cloudflare agents (Cloudflare also provides **WARP** tunneling, which tunnels all network traffic through the app). This method configures DNS over HTTPS as its DNS protocol.

DNS policy was configured in the Cloudflare Zero Trust console⁷, with the policy set to block anything destined for *.blockdns.guidedpointsecuritydemo2.com or *.blockdns.ipv6.guidedpointsecuritydemo2.com. This allows testing a specific website to validate that the DNS queries are intercepted on those domain names, without extraneous caching of DNS results or an excessive number of queries (visits to sites like yahoo.com can generate hundreds of queries).

The guidedpointsecuritydemo2.com apex domain was hosted by Amazon Web Services (AWS). As AWS supports wildcard domains like *.guidedpointsecuritydemo2.com as a catchall for DNS queries, it was possible to distinguish which test device was originating queries by sending requests like ‘android.chrome.wifi.guidedpointsecuritydemo2.com.’

⁶ When a client uses DoH for encrypted DNS queries, it first must resolve the subdomain to know where to send that query, so a client would send a plaintext query for “oi6eykxg3f.cloudflare-gateway.com,” resolving its IP address to W.X.Y.Z, and subsequently sending the encrypted query. This initial traffic reveals the subdomain in use over the network.

⁷ See Pilot Test Group 1 (VMware Workspace ONE), Pilot Test Group 2 (Microsoft Endpoint Manager), or Pilot Test Group 3 (MobileIron Cloud) for specifics on these implementations.

For both Android and iOS devices, all common browsers were utilized in “InPrivate” or “Incognito” mode. The devices were reset between browser tests to clear any DNS or browser caching.

For Android devices, Firefox, Google Chrome, and Microsoft Edge were used to browse to the guidepointsecuritydemo2.com domain

For iOS devices, Apple Safari, Firefox, Google Chrome, and Microsoft Edge were used to browse to the guidepointsecuritydemo2.com domain

The testing was conducted on both IPv4 networks and IPv6 networks. Separate web servers were built to distinguish between IPv4 and IPv6. iOS devices were tested on Wi-Fi and cellular, both IPv4 and IPv6. Android was tested on Wi-Fi and cellular, IPv4 but only IPv6 on cellular. Android version 11 has limited support for IPv6 over Wi-Fi, so testing was limited for this condition.

A Wi-Fi enclave with IPv4 and IPv6 was setup using a pfSense v.2.5.2 firewall for routing and traffic interception during the Wi-Fi test. Traffic was filtered by device to UDP/TCP port 53 (plain text DNS) on the firewall using tcpdump. DNS over TLS was not monitored for interception, as no devices were configured to transmit in this way. DNS over HTTPS could not be monitored without establishing a proxy on the device or the firewall, which could interfere with the Cloudflare agent. This procedure was performed to validate that there was no DNS leakage to other resolvers, in addition to sending DNS queries to Cloudflare (some devices will conduct queries to multiple resolvers simultaneously, and use whichever answer is returned first).

Monitoring of cellular traffic would not be possible without placing a tap on the cellular tower that the device connects to, or by setting up a separate cellular radio for interception. However, capturing packets on iOS devices before they leave the device is possible using Apple development tools (XCode⁸) with a physical connection to the iOS device. This creates a remote virtual interface where tcpdump can be used to monitor cellular packets as they leave the device. This was used to capture cellular iOS traffic for the IPv4 and IPv6 tests. This methodology is not available on Android devices without root access, so it was not tested.

For the non-web protocol test, on Android devices the “Termius” app⁹ was installed from the Google Play store. This app allows the user to access the local Android terminal without root access. From the terminal, ping connectivity tests were conducted via domain name to check connectivity and domain resolution.

⁸ <https://developer.apple.com/xcode/>

⁹ <https://termius.com/>, available as of 22 March 2022

For iOS devices, the “iSH” app¹⁰ was used to generate a Linux shell and perform commands, such as ping, netcat (over various TCP ports (22, 80, 4444, and 8080), and wget.

4.1.4. Detailed test results

The Cloudflare agent did not intercept all DNS queries on every device. During the reboot process, the Cloudflare agent is not authenticated to the Cloudflare resolver service. Additionally, system level queries (specific to iOS), did not go through the Cloudflare agent even when the agent was connected. Certain apex level domains, such as apple.com, microsoft.com, and akadns.net were observed in plaintext over port 53 during the wireless packet capture. This behavior was also observed when testing the Cisco security connector/Cisco Umbrella solution, so it is likely a result of the iOS implementation of permissions for traffic interception.

Additionally, observed throughout the testing was that the Cloudflare Zero Trust agent (WARP app) would get stuck “Updating connection information.” Resetting the agent or the network connection was required to clear the error. It was not observed if the protective capability was not available during this time, as testing was paused until the error was resolved.

However, when the Cloudflare WARP client was in full operational mode, and general user browsing was conducted, plaintext DNS traffic was not generated by the devices. See in **Error! Reference source not found.** and **Error! Reference source not found.** that the firewall did not observe plaintext DNS traffic, except to resolve the IP address of Cloudflare’s sub-domain associated with the user’s Cloudflare tenant.

4.1.4.1. Android over IPv6 – Wi-Fi

Android version 11 supports Stateless Address Auto Configuration (SLAAC) for Wi-Fi on IPv6, but not DHCPv6. This prevented Android devices from connecting to any internet resource until after the Cloudflare agent was connected. IPv6 is an unlikely configuration for Android devices over Wi-Fi based on its lack of DHCPv6 support, therefore testing in this condition was not conducted.

4.1.4.2. Android over IPv6 - Cellular

During the first iterations of testing on Android with the Cloudflare WARP app version 6.10 (see Go/No Go Evaluation report #2, revision #2), IPv6 over cellular for Android was functional. After Cloudflare upgraded to version 6.11 of the WARP app, the Cloudflare agent interfered with connections to IPv6 only endpoints. Testing for this configuration could be conducted with the Cloudflare app in Cloudflare WARP mode (full VPN, not just DNS queries routed through Cloudflare network). This violates the tenants of the TIC 3.0 construct this project is working towards and is not testing in the specified configurations desired for mobile endpoints. Therefore, the Android over cellular/IPv6 configuration was removed from testing.

¹⁰ <https://ish.app/>, available as of 22 March 2022

4.1.4.3. Results Table

Table 2. Cloudflare Results

Test	Expected Result	Pass	Failed	Other
	Host Endpoint			
1.1 Host agent is operational	Agent is running, user is logged in with credentials or agent is registered with protective DNS provider	X		
	iOS - Network Test			
IPv4 WI-FI – iOS				
Safari browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Chrome browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Firefox test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Microsoft Edge browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
iSH app (ping/nc/wget)	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
IPv6 WI-FI – iOS				

Safari browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Chrome browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Firefox test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Microsoft Edge browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
iSH app (ping/nc/wget)	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
IPv4 Cellular – iOS				
Safari browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Chrome browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		

	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Firefox test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Microsoft Edge browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
iSH app (ping/nc/wget)	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
IPv6 Cellular – iOS				
Safari browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Chrome browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Firefox test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		

Microsoft Edge browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
iSH app (ping/nc/wget)	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
	Android – Network Test			
IPv4 Wi-Fi - Android				
Chrome browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Firefox test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Microsoft Edge browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Termius app (ping/ssh)	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
IPv6 Wi-Fi – Android				n/t
	Limited support for IPv6 over Wi-Fi			

IPv4 Cellular - Android				
Chrome browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Firefox test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Microsoft Edge browser test	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
Termius app (ping/ssh)	DNS queries directed to protective DNS resolver for permitted addresses	X		
	DNS queries directed to protective DNS resolver for unauthorized addresses	X		
	DNS Resolver attributes permitted query to unique endpoint	X		
	DNS Resolver attributes denied query to unique endpoint	X		
IPv6 Cellular - Android				
Chrome browser test	DNS queries directed to protective DNS resolver for permitted addresses			n/t
	DNS queries directed to protective DNS resolver for unauthorized addresses			n/t
	DNS Resolver attributes permitted query to unique endpoint			n/t
	DNS Resolver attributes denied query to unique endpoint			n/t
Firefox test	DNS queries directed to protective DNS resolver for permitted addresses			n/t
	DNS queries directed to protective DNS resolver for unauthorized addresses			n/t
	DNS Resolver attributes permitted query to unique endpoint			n/t
	DNS Resolver attributes denied query to unique endpoint			n/t
Microsoft Edge browser test	DNS queries directed to protective DNS resolver for permitted addresses			n/t
	DNS queries directed to protective DNS resolver for unauthorized addresses			n/t

	DNS Resolver attributes permitted query to unique endpoint			n/t
	DNS Resolver attributes denied query to unique endpoint			n/t
Termius app (ping/ssh)	DNS queries directed to protective DNS resolver for permitted addresses			n/t
	DNS queries directed to protective DNS resolver for unauthorized addresses			n/t
	DNS Resolver attributes permitted query to unique endpoint			n/t
	DNS Resolver attributes denied query to unique endpoint			n/t

4.2 Mobile Device Management Provider

The purpose of integrating the Mobile Device Management (MDM) solutions into the test were to facilitate enterprise integration at scale, reducing misconfiguration of the Protective DNS endpoint agent, and preventing Protective DNS agent circumvention. The criteria for the MDM provider, developed in Target Capabilities Definition documents version 1 and 2, support these efforts. Pilot Test Group 1: VMware Workspace ONE, Pilot Test Group 2: Microsoft Endpoint Manager, and Pilot Test Group 3: MobileIron Cloud, represent best practice technical controls to support the Protective DNS solution by preventing general misconfiguration or users from deliberately or unintentionally bypassing the Cloudflare WARP client protections. Testing the criteria against these MDM's should be relatively representative of the mobile device management space. However, using an MDM to deploy the Cloudflare WARP protective DNS agent is not required to achieve the protections offered by protective DNS. Using MDM complements the holistic solution.

Of the three MDM's, MobileIron Cloud was the only MDM to successfully implement OS level VPN restrictions on Android devices. Though not implemented by Microsoft or VMware, this requirement may be addressed by these vendors in the future, as more customers require the feature.

1. None of the MDM providers provide a profile restriction for Android devices to prevent configuration of Private DNS¹¹. Users can bypass DNS protective measures entirely by setting the system level Private DNS configuration to a service other than Cloudflare on Android version 10 or above. The Enterprise Android device management API might allow MDMs to restrict the use of private DNS, however, it was not implemented in any MDM.
2. Versions of the Cloudflare WARP application (6.10) and below allowed users to exclude applications from the WARP application's VPN tunnel, negating the protections provided by protective DNS. This was addressed by the Cloudflare team in WARP version 6.11, and no longer allows circumvention.
3. iOS browsers did not have a mechanism for configuring DNS over HTTPS, and so was not tested.
4. User interaction is required to authenticate endpoints to Cloudflare. Touchless deployment of the WARP app is in Cloudflare's roadmap. Configuration via MDM will be required for this feature.
5. Microsoft Endpoint Manager and MobileIron Cloud did not use device unique attributes (like serial number or IMEI) for asset management. The same Android device could be registered in MobileIron Cloud or Microsoft Endpoint Manager multiple times after a factory reset.
6. Deploying multiple VPN solutions (Cloudflare + Zscaler, Cloudflare + system VPN) interfered with the protections provided by the Cloudflare WARP app. Operating multiple

¹¹ <https://developers.google.com/speed/public-dns/docs/using#android>, last accessed 22 March 2022

VPN's simultaneously on Android and iOS devices is not supported and enabling one VPN disconnects the currently operating VPN application.

- a. For agencies that deploy internal resources that are historically accessed over a VPN connection, access via multiple VPN solutions (Cloudflare + agency VPN) may prove cumbersome for users. Integration with other Cloudflare services, such as Cloudflare Access may be beneficial for accessing internal resources.

Table 3. MDM Requirements Evaluation

Requirement	Operating System	VMWare Workspace ONE		Microsoft Endpoint Manager		MobileIron Cloud	
		Pass	Fail	Pass	Fail	Pass	Fail
Restricting application removal	iOS	X		X		X	
Restricting operating system level DNS settings	iOS	X		X		X	
Restricting browser-based DNS settings, such as DNS over HTTPS	iOS	n/a		n/a		n/a	
Over the air application configuration	iOS	X		X		X	
Restrict operating system level VPN settings*	iOS	X		X		X	
Restricting application removal	Android	X		X		X	
Restricting operating system level DNS settings	Android		X		X		X
Restricting browser-based DNS settings, such as DNS over HTTPS	Android	X		X		X	
Over the air application configuration	Android	X		X		X	
Restrict operating system level VPN settings*	Android		X ¹²		X	X	
Integration with local/on-premises Microsoft Active Directory environment	n/a	X		X		X	

¹² VMWare Workspace ONE is capable of restricting OS level VPN settings, but doing so interferes with creating the VPN profile for Cloudflare. The MDM must also be able to create a VPN profile for the Cloudflare app, which Workspace ONE did not support.

5.0 CONCLUSIONS

GuidePoint Security's **Mobile Network Traffic Visibility for the Enterprise** was designed to meet several scoping requirements and project objectives, evaluated against a specific Protective DNS provider (Cloudflare), and limited in evaluation to modern iOS and Android devices.

Through thorough testing of the various use cases GuidePoint Security expects users to operate these devices in, GuidePoint Security concludes that Cloudflare's Protective DNS solution, deployed via a Mobile Device Management solution, does meet the scoping requirements and project objectives.

Scoping

1. Can agencies identify suspicious DNS network traffic? **Yes.**
2. Can agencies filter DNS traffic? **Yes.**
3. Can agencies categorize traffic based on DNS lookups? **Yes.**

Project Objectives

1. Force routing mobile DNS traffic to a centralized PDNS service of CISA's choice. **Yes.**
2. Authenticate mobile devices. **Mixed Results**
3. Attribute DNS queries. **Yes**

DHS/CISA adoption of a Protective DNS vendor provider, coupled with complimenting data aggregation tools (such as a SIEM), can improve an agency's cyber security posture and resilience to cyber-attack. A quality threat feed used to deny malicious domains can stop endpoints from initiating connections to malicious domains across the internet. This can all be accomplished without backhauling traffic across a VPN to an agency's local trusted internet connection.

However, a Protective DNS product is not without limitation. Thorough testing of various conditions for mobile devices (IPv4, IPv6, Wi-Fi, cellular, various applications), demonstrated that Cloudflare's WARP application performs its function independent of the transport mechanism used to get data from a mobile endpoint to Cloudflare's DNS resolvers.

1. The protection provided to the endpoint is dependent on the quality of the intelligence threat feed used to generate DNS blocklist policies.
2. While the Cloudflare WARP agent intercepts most system DNS queries and application queries, any application that is using a non-plaintext transport for DNS queries cannot be intercepted by Cloudflare, unless the Cloudflare app is operating in proxy mode. Applications mitigate this with certificate trust pinning. Administrators must understand and trust the applications they allow to be deployed to endpoints. MDM policy can provide technical controls that prevent unauthorized applications.

3. Protective DNS technology does not protect against connections directly to IP addresses. Most web applications do not use direct IP connections over the public internet, though it is possible. While not a Protective DNS function, the Cloudflare gateway app, when operating in full proxy mode, would have visibility into this traffic connection.
4. The tested MDMs were unable to restrict users from disabling Private DNS mode on Android operating systems. This mode uses DNS over TLS and bypasses the Cloudflare WARP client entirely.

6.0 REFERENCES

1. Cisco, *Cisco 2016 Annual Security Report*, URL: <http://mkto.cisco.com/rs/564-whv-323/images/cisco-asr-2016.pdf>, last modified 2016. Accessed 22 March 2022
2. National Security Agency and Cybersecurity Infrastructure & Security Agency, *Selecting a Protective DNS Service*, URL: https://media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_Selecting-Protective-DNS_UOO11765221.PDF, last modified May 2021. Accessed 22 March 2022
3. Cybersecurity Infrastructure & Security Agency, Memorandum: *Addressing Domain Name System Resolution on Federal Networks*, URL: https://www.cisa.gov/sites/default/files/publications/Addressing_DNS_Resolution_on_Federal_Networks_Memo.pdf, last modified 21 April 2020. Accessed 22 March 2022.
4. GuidePoint Security, *Mobile Network Traffic Visibility for the Enterprise, Target Capabilities Definition*, version 2, FA8750-20-C-1029, October 2021

APPENDIX A: PUBLICATIONS AND PRESENTATIONS

1. GuidePoint Security, Mobile Network Traffic Visibility for the Enterprise, Target Capabilities Definition, (version 1), FA8750-20-C-1029, February 2021
2. GuidePoint Security, Mobile Network Traffic Visibility for the Enterprise, Target Capabilities Definition (version 2), FA8750-20-C-1029, October 2021
3. GuidePoint Security, Mobile Network Traffic Visibility for the Enterprise, Go No Go Evaluation Plan (version 2), FA8750-20-C-1029, June 2021
4. GuidePoint Security, Mobile Network Traffic Visibility for the Enterprise, Go No Go Evaluation Report (version 2, revision 2), FA8750-20-C-1029, September 2021
5. GuidePoint Security, Mobile Network Traffic Visibility for the Enterprise, Pilot Test Group 1 Evaluation Report (VMware Workspace ONE), FA8750-20-C-1029, September 2021
6. GuidePoint Security, Mobile Network Traffic Visibility for the Enterprise, Pilot Test Group 2 Evaluation Report (Microsoft Intune/Endpoint Manager), FA8750-20-C-1029, December 2021
7. GuidePoint Security, Mobile Network Traffic Visibility for the Enterprise, Pilot Test Group 3 Evaluation Report (MobileIron Cloud), FA8750-20-C-1029, February 2021

APPENDIX B: CLOUDFLARE EVALUATION PROCEDURE SCREENSHOTS

APPENDIX B - TABLE OF CONTENTS

B.1	DEVICE SETUP	33
B.2	iOS DEVICE TESTING	36
B.2.1	iOS, IPv4, Wi-Fi, Safari Browser.....	36
B.2.2	iOS, IPv4, Wi-Fi, Chrome Browser	40
B.2.3	iOS, IPv4, Wi-Fi, Firefox Browser	44
B.2.4	iOS, IPv4, Wi-Fi, Edge Browser	47
B.2.5	Other results	51

LIST OF FIGURES

Figure B- 1. Cloudflare for Teams verified host endpoint registration	33
Figure B-2. Cloudflare for Teams, host endpoint registration ID.....	34
Figure B-3. Cloudflare for Teams console, same registration ID as the endpoint.....	35
Figure B-4. iOS, IPv4, Wi-Fi, Safari web browsing.....	36
Figure B-5. iOS, IPv4, Wi-Fi, Safari, Web browsing filtered by DNS query	37
Figure B-6. iOS, IPv4, Wi-Fi, Safari – Cloudflare console DNS logs	38
Figure B-7. iOS, IPv4, Wi-Fi, Safari – Edge firewall port 53 packet capture.....	39
Figure B-8. iOS, IPv4, Wi-Fi, Chrome web browsing	40
Figure B-9. iOS, IPv4, Wi-Fi, Safari, Web browsing filtered by DNS query	41
Figure B-10. iOS, IPv4, Wi-Fi, Chrome – Cloudflare console DNS logs.....	42
Figure B-11. iOS, IPv4, Wi-Fi, Firefox – Network firewall port 53 packet capture.....	43
Figure B-12. iOS, IPv4, Wi-Fi, Firefox, Normal web browsing	44
Figure B-13. iOS, IPv4, Wi-Fi, Firefox, Web browsing filtered by DNS query	45
Figure B-14. iOS, IPv4, Wi-Fi, Firefox, Cloudflare DNS console logs.....	46
Figure B-15. iOS, IPv4, Wi-Fi, Firefox, Edge firewall port 53 packet capture.....	46
Figure B-16. iOS, IPv4, Wi-Fi, Edge, Normal web browsing.....	47
Figure B-17. iOS, IPv4, Wi-Fi, Edge, Web browsing filtered by DNS query	48
Figure B-18. iOS, IPv4, Wi-Fi, Edge, Cloudflare console DNS logs.....	49
Figure B-19. iOS, IPv4, Wi-Fi, Edge, Network edge firewall port 53 packet capture.....	50
Figure B-20. iOS, IPv4, Wi-Fi, device reboot	51
Figure B-21. Teams stuck connection	52

Screenshots of network packet captures, and mobile devices were taken throughout the process of evaluating the Cloudflare WARP app and the Cloudflare Zero Trust console to visually depict the results of the procedure. As the process became redundant across the various evaluation conditions (IPv4 vs IPv6, Wi-Fi vs cellular), these figures do not include every test conducted.

B.1 Device Setup

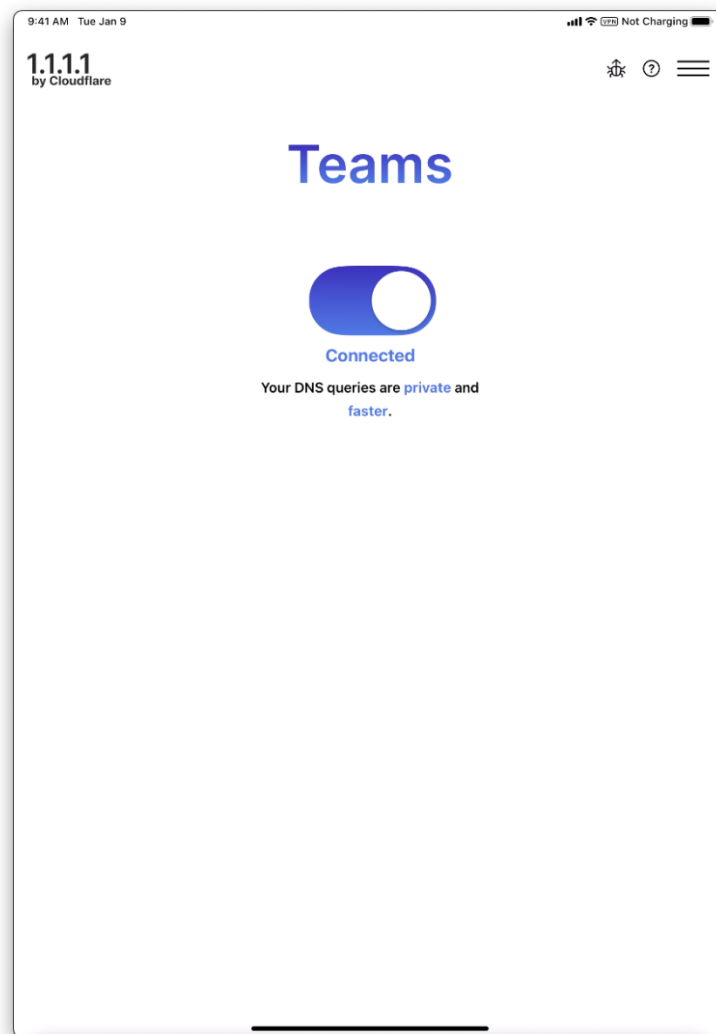


Figure B- 1. Cloudflare for Teams verified host endpoint registration

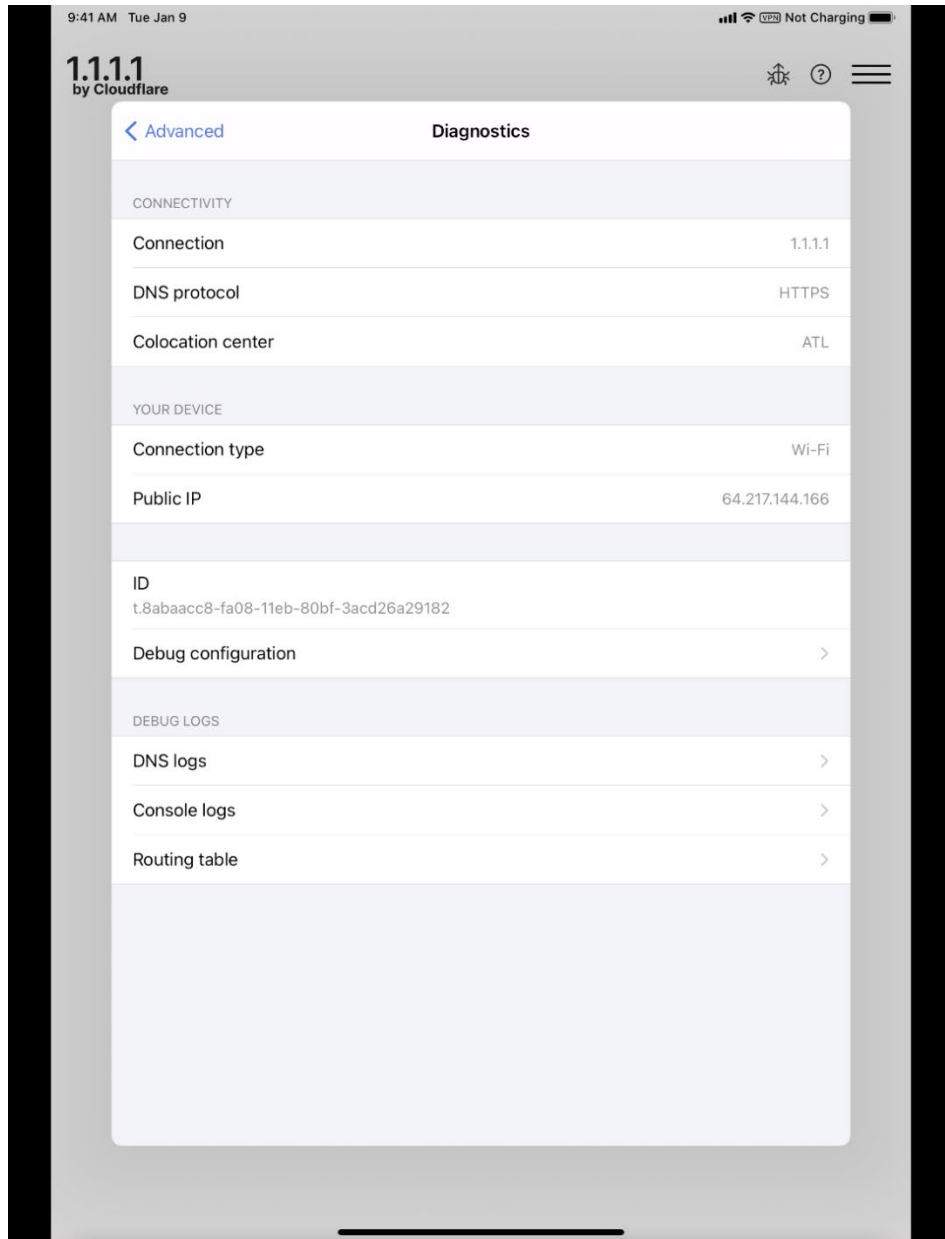


Figure B-2. Cloudflare for Teams, host endpoint registration ID

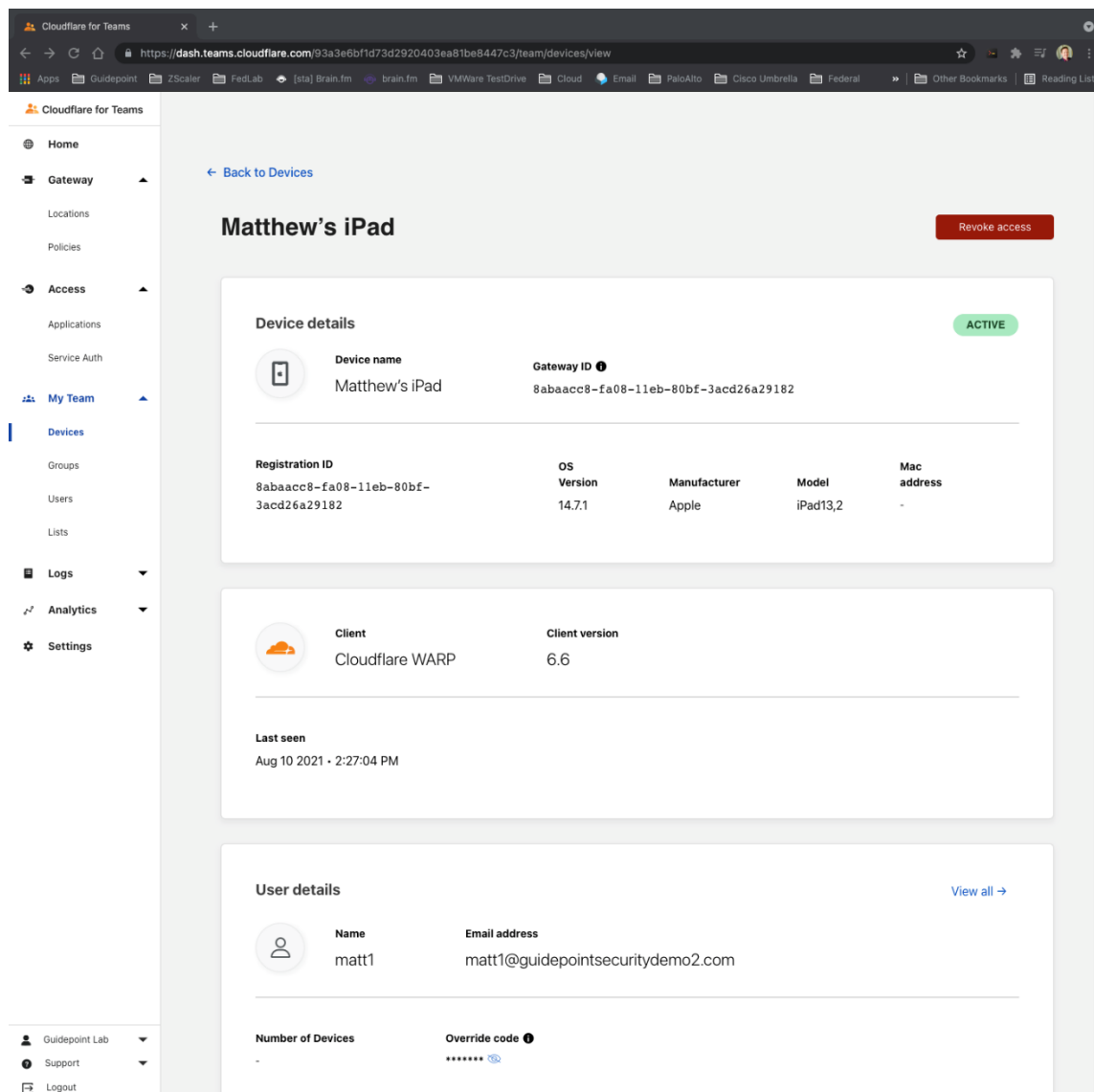


Figure B-3. Cloudflare for Teams console, same registration ID as the endpoint

B.2 iOS Device testing

B.2.1 iOS, IPv4, Wi-Fi, Safari Browser

iPad, Wi-Fi enabled, Cellular disabled. IPv4. Browser InPrivate mode

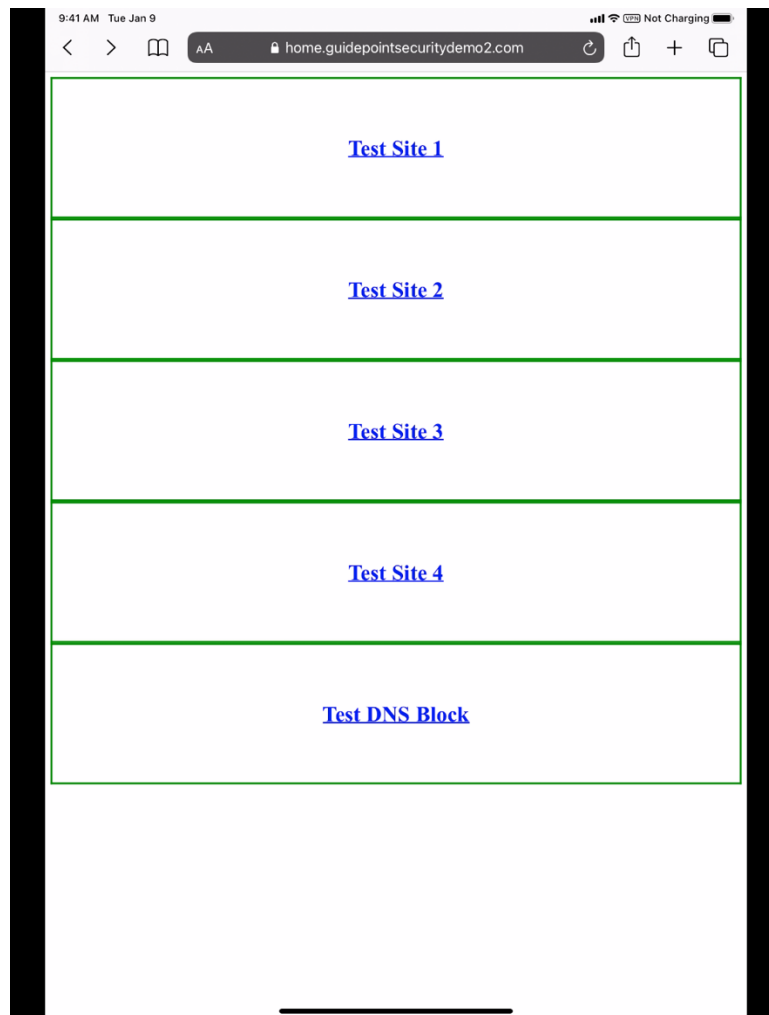


Figure B-4. iOS, IPv4, Wi-Fi, Safari web browsing

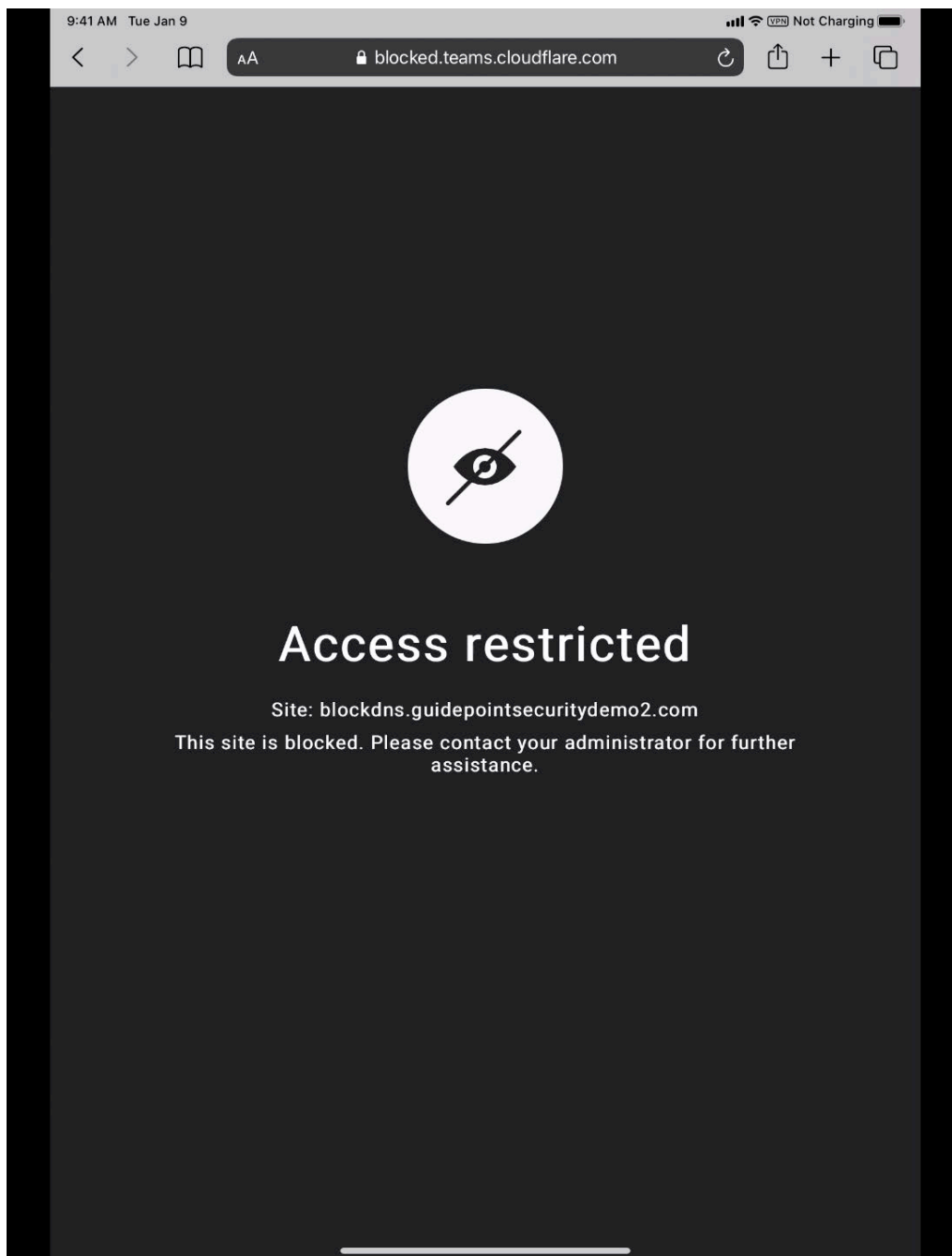


Figure B-5. iOS, IPv4, Wi-Fi, Safari, Web browsing filtered by DNS query

The screenshot shows the Cloudflare console interface. On the left is a sidebar with navigation options: Home, Gateway, Access, My Team, Logs, Analytics, and Settings. The main content area is titled 'Gateway Activity Log' and has tabs for DNS, Network, and HTTP. A search bar contains the text 'idepointsecuritydemo2'. Below the search bar is a table of log entries.

Query	Email	Action	Time
> blockdns.guidedpointsecuritydemo2.com	---	BLOCK	Aug 10 2021 • 3:29:55 PM
> blockdns.guidedpointsecuritydemo2.com	---	BLOCK	Aug 10 2021 • 3:29:55 PM
> site4.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:53 PM
> site4.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:53 PM
> site3.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:52 PM
> site3.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:51 PM
> site2.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:49 PM
> site2.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:49 PM
> site1.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:20 PM
> site1.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:20 PM
> home.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:17 PM
> home.guidedpointsecuritydemo2.com	---	ALLOW	Aug 10 2021 • 3:29:17 PM

Figure B-6. iOS, IPv4, Wi-Fi, Safari – Cloudflare console DNS logs

Packet capture from the pfSense firewall acting as the network gateway for the iPad, filtered for UDP port 53 (DNS plaintext traffic).

```
[2.5.2-RELEASE][admin@lan1.local]:/root: tcpdump -i vmx3.140 -n 'udp port 53'  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on vmx3.140, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Figure B-7. iOS, IPv4, Wi-Fi, Safari – Edge firewall port 53 packet capture

B.2.2 iOS, IPv4, Wi-Fi, Chrome Browser

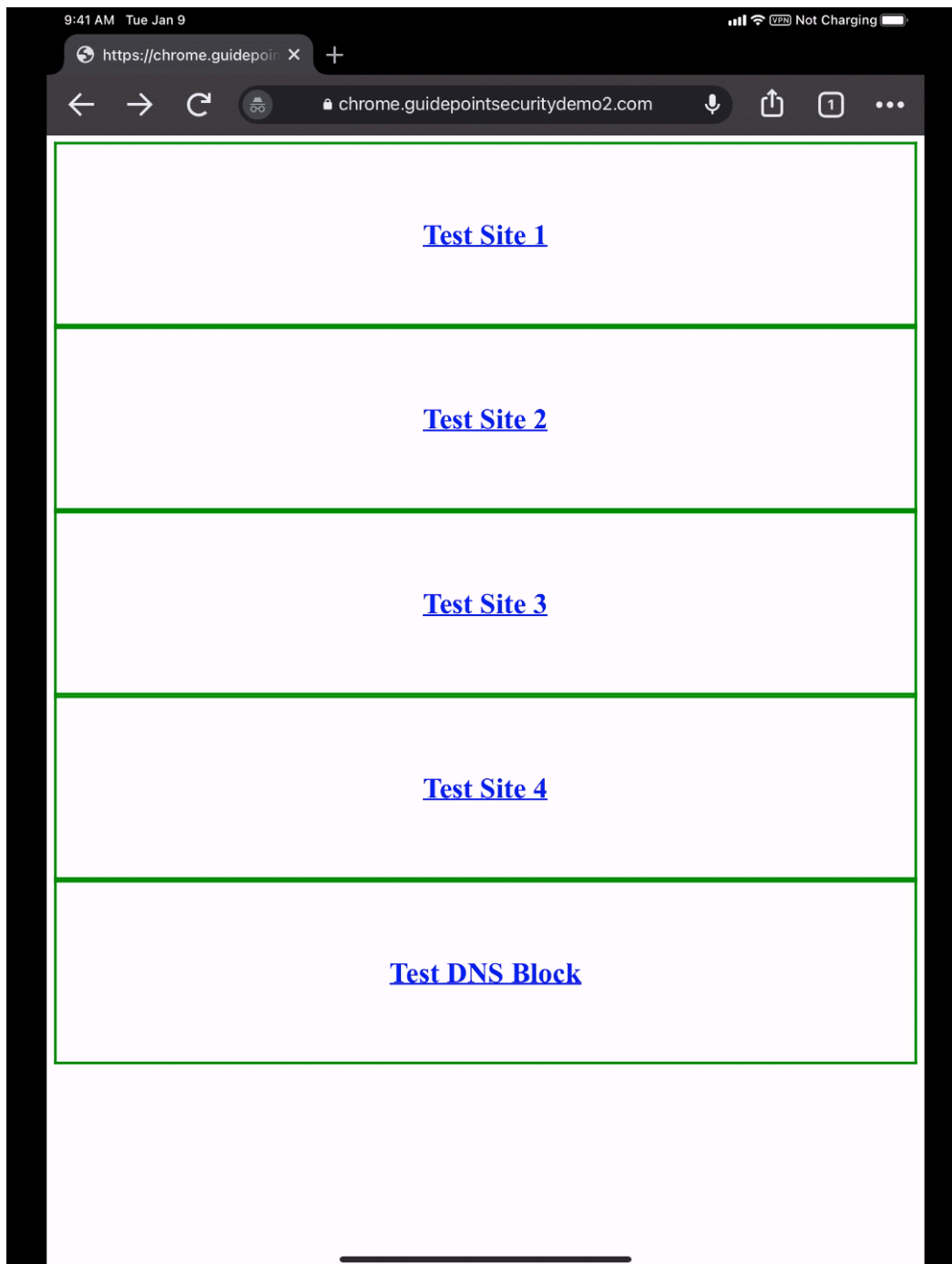


Figure B-8. iOS, IPv4, Wi-Fi, Chrome web browsing

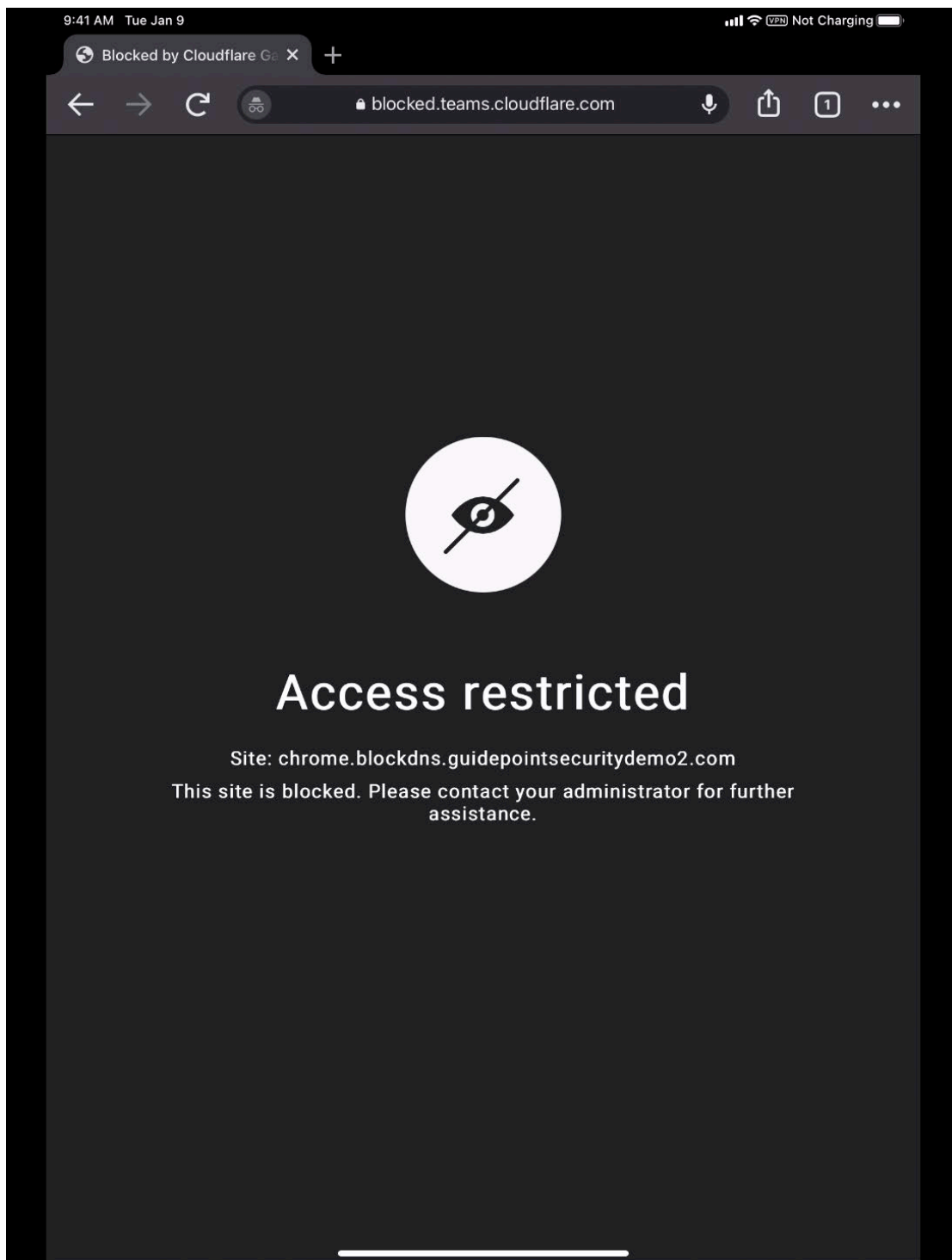


Figure B-9. iOS, IPv4, Wi-Fi, Safari, Web browsing filtered by DNS query

Query	Email	Action	Time
> clients1.google.com	irondev1@guidepointsecuritydemo2.com	ALLOW	Mar 22 2022 · 11:16:33 PM
chrome.blockdns.guidepointsecuritydemo2.com	irondev1@guidepointsecuritydemo2.com	BLOCK	Mar 22 2022 · 11:16:27 PM
Policy ID 3a27949ed0cf4798b9f1aef227dfd1a6 Source IP 64.217.144.166 Request type A Port --- Protocol type https User email irondev1@guidepointsecuritydemo2.com User ID 34913721-d0bf-49e9-8f8c-117a5a38f857 Device ID cbe93875-8aae-11ec-a48c-7a3370576a91 Location mobile v2 Resolver decision Blocked Rule View domain details in Radar →			
> chrome.blockdns.guidepointsecuritydemo2.com	irondev1@guidepointsecuritydemo2.com	BLOCK	Mar 22 2022 · 11:16:27 PM
> growth-pa.googleapis.com	irondev1@guidepointsecuritydemo2.com	ALLOW	Mar 22 2022 · 11:16:19 PM

Figure B-10. iOS, IPv4, Wi-Fi, Chrome – Cloudflare console DNS logs

DNS over port 53 – note that the only DNS query is the Cloudflare app re-resolving its domain to access Cloudflare’s resolver

```
[2.5.2-RELEASE][admin@lan1.local]/root: tcpdump -i vmx3.140 -n 'port 53'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmx3.140, link-type EN10MB (Ethernet), capture size 262144 bytes

01:26:30.687296 IP 10.0.140.24.51702 > 9.9.9.9.53: 60514+ A? oi6xykug6h.cloudflare-gateway.com. (51)
01:26:30.714729 IP 9.9.9.9.53 > 10.0.140.24.51702: 60514 2/0/0 A 162.159.36.20, A 162.159.36.5 (83)
```

Figure B-11. iOS, IPv4, Wi-Fi, Firefox – Network firewall port 53 packet capture

B.2.3 iOS, IPv4, Wi-Fi, Firefox Browser

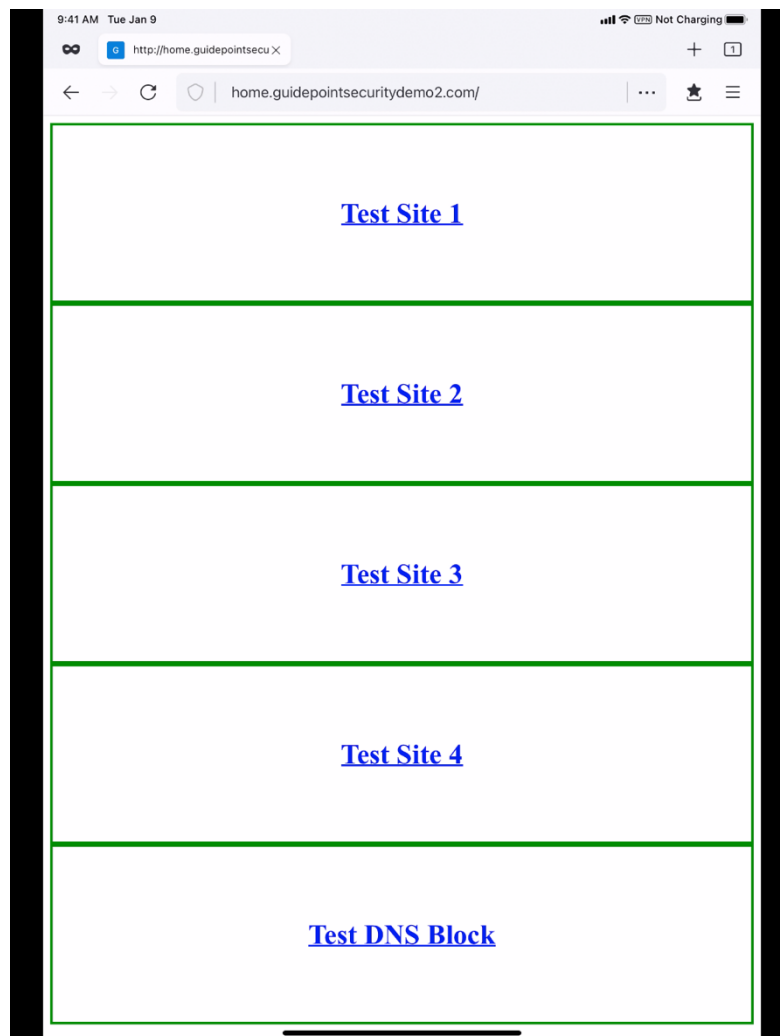


Figure B-12. iOS, IPv4, Wi-Fi, Firefox, Normal web browsing

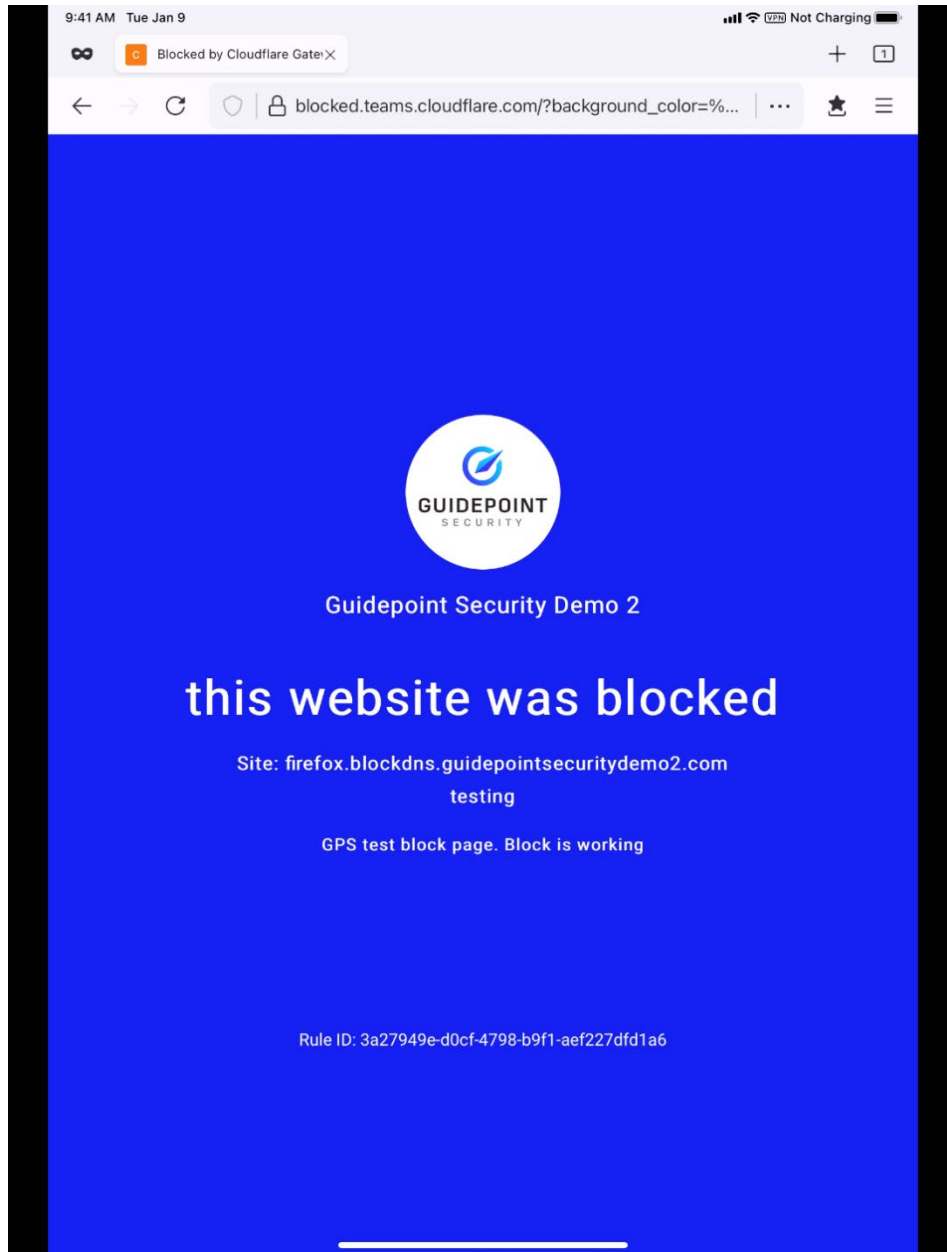


Figure B-13. iOS, IPv4, Wi-Fi, Firefox, Web browsing filtered by DNS query

Query	Email	Action	Time
▼ firefox.blockdns.guidedpointsecuritydemo2.com	irondev1@guidedpointsecuritydemo2.com	BLOCK	Mar 22 2022 • 11:18:42 PM
Policy ID 3a27949ed0cf4798b9f1aef227dfd1a6			
Source IP 64.217.144.166	Request type HTTPS	Port ---	Protocol type https
User email irondev1@guidedpointsecuritydemo2.com	User ID 34913721-d0bf-49e9-8f8c-117a5a38f857	Device ID cbe93875-8aae-11ec-a48c-7a3370576a91	Location mobile v2
Resolver decision Blocked Rule			
View domain details in Radar →			
> firefox.blockdns.guidedpointsecuritydemo2.com	irondev1@guidedpointsecuritydemo2.com	BLOCK	Mar 22 2022 • 11:18:42 PM
> accounts.firefox.com	irondev1@guidedpointsecuritydemo2.com	ALLOW	Mar 22 2022 • 11:18:18 PM

Figure B-14. iOS, IPv4, Wi-Fi, Firefox, Cloudflare DNS console logs

iPad, IPv4, Wi-Fi Firefox test, no plaintext queries were observed

```
[2.5.2-RELEASE][admin@lan1.local]/root: tcpdump -i vmx3.140 -n 'port 53'
\tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmx3.140, link-type EN10MB (Ethernet), capture size 262144 bytes
>
```

Figure B-15. iOS, IPv4, Wi-Fi, Firefox, Edge firewall port 53 packet capture

B.2.4 iOS, IPv4, Wi-Fi, Edge Browser

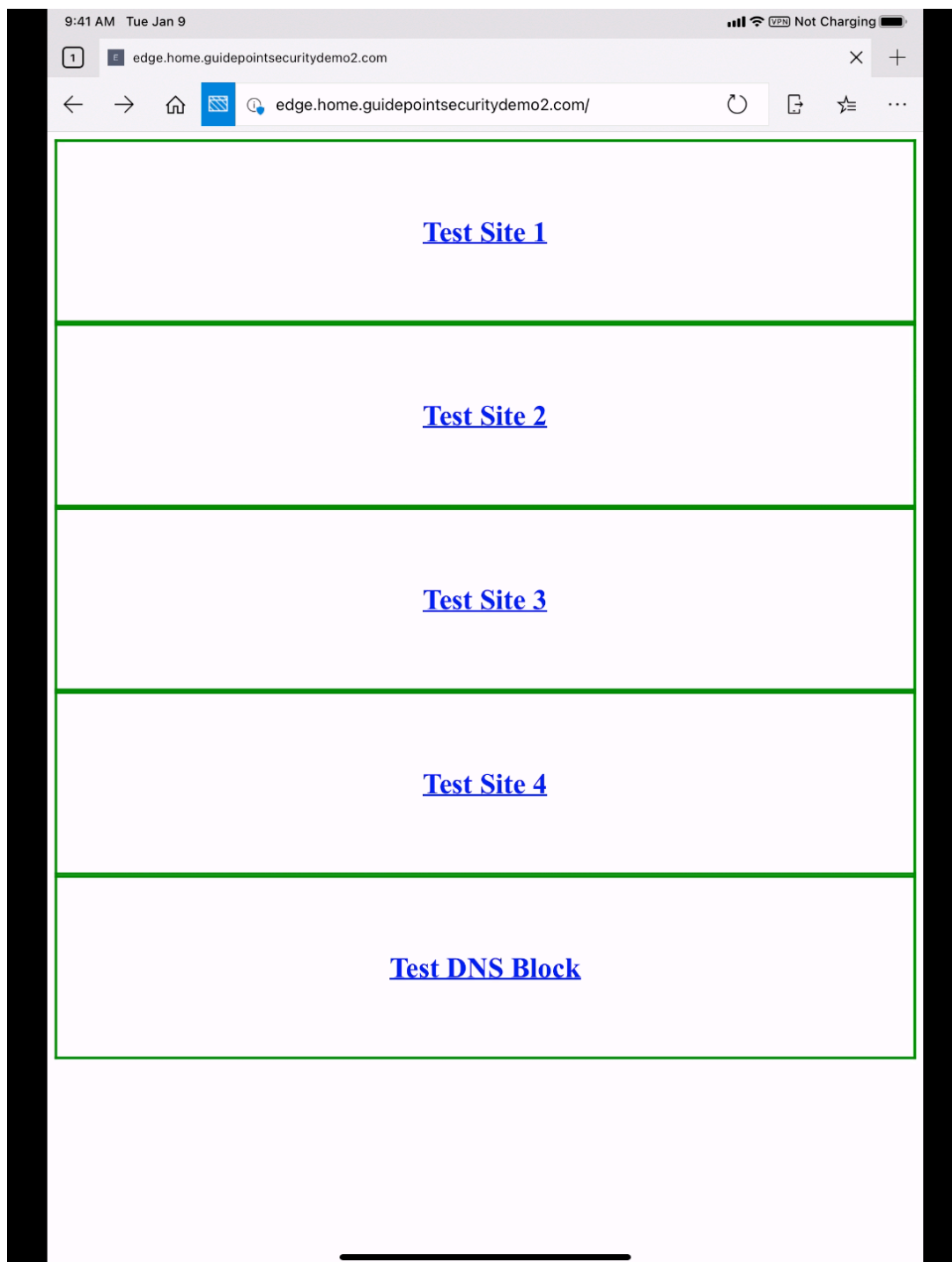


Figure B-16. iOS, IPv4, Wi-Fi, Edge, Normal web browsing

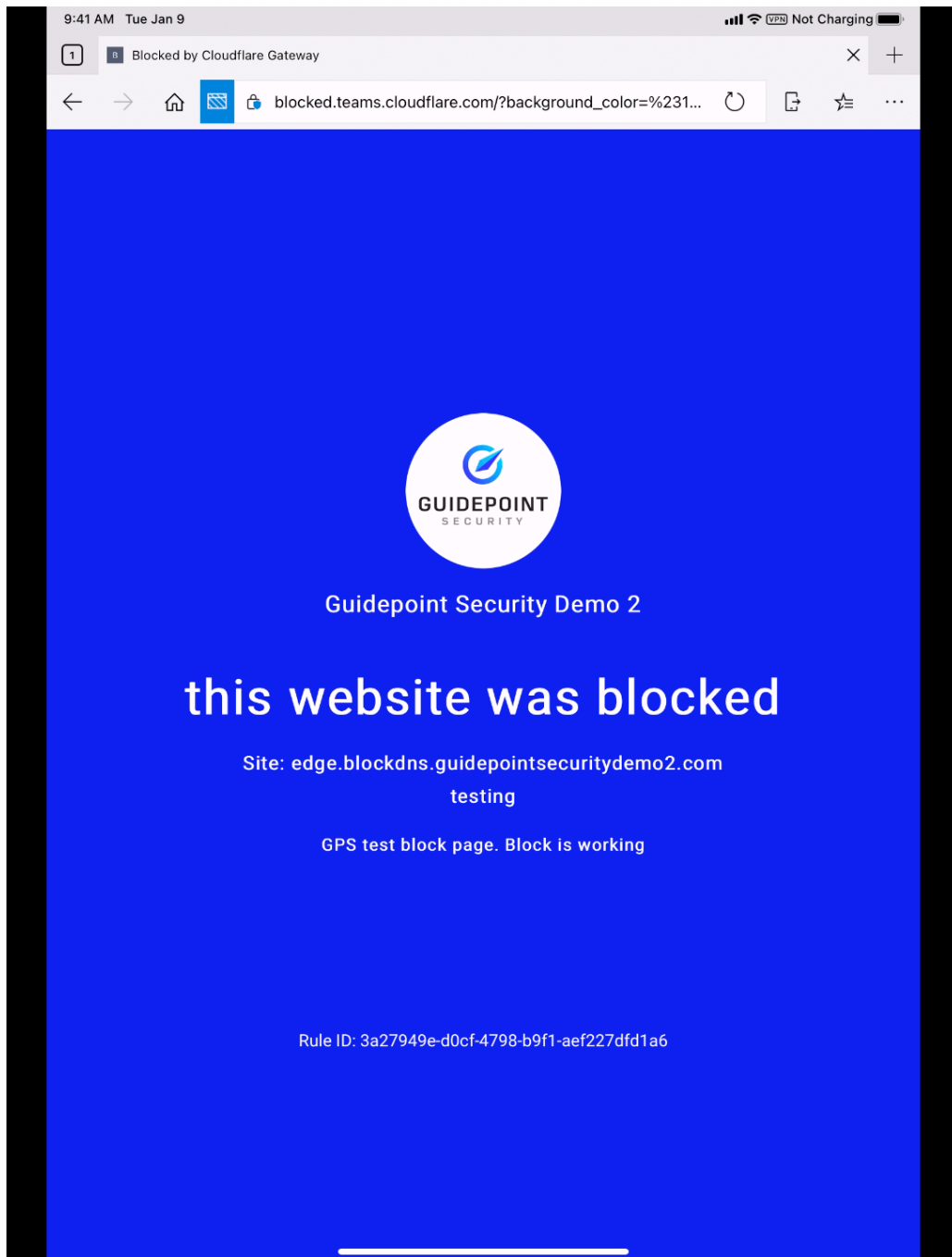


Figure B-17. iOS, IPv4, Wi-Fi, Edge, Web browsing filtered by DNS query

>	ipv4wifiedge.block.guidepointsecuritydemo2.com	irondev1@guidepointsecuritydemo2.com	BLOCK	Mar 22 2022 • 11:20:49 PM								
>	ipv4wifiedge.block.guidepointsecuritydemo2.com	irondev1@guidepointsecuritydemo2.com	BLOCK	Mar 22 2022 • 11:20:49 PM								
✓	edge.guidepointsecuritydemo2.com	irondev1@guidepointsecuritydemo2.com	ALLOW	Mar 22 2022 • 11:20:34 PM								
<table><tr><th>Source IP</th><th>Request type</th><th>Port</th><th>Protocol type</th></tr><tr><td>64.217.144.166</td><td>HTTPS</td><td>---</td><td>https</td></tr></table>					Source IP	Request type	Port	Protocol type	64.217.144.166	HTTPS	---	https
Source IP	Request type	Port	Protocol type									
64.217.144.166	HTTPS	---	https									
<table><tr><th>User email</th><th>User ID</th><th>Device ID</th><th>Location</th></tr><tr><td>irondev1@guidepointsecuritydemo2.com</td><td>34913721-d0bf-49e9-8f8c-117a5a38f857</td><td>cbe93875-8aae-11ec-a48c-7a3370576a91</td><td>mobile v2</td></tr></table>					User email	User ID	Device ID	Location	irondev1@guidepointsecuritydemo2.com	34913721-d0bf-49e9-8f8c-117a5a38f857	cbe93875-8aae-11ec-a48c-7a3370576a91	mobile v2
User email	User ID	Device ID	Location									
irondev1@guidepointsecuritydemo2.com	34913721-d0bf-49e9-8f8c-117a5a38f857	cbe93875-8aae-11ec-a48c-7a3370576a91	mobile v2									
Resolver decision Allowed On No Policy Match												
View domain details in Radar →												

Figure B-18. iOS, IPv4, Wi-Fi, Edge, Cloudflare console DNS logs

iPad IPv4 Wi-Fi Microsoft Edge browsing – Network firewall DNS packet capture

```
[2.5.2-RELEASE][admin@lan1.local]/root: tcpdump -i vmx3.140 -n 'port 53'  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on vmx3.140, link-type EN10MB (Ethernet), capture size 262144 bytes
```



Figure B-19. iOS, IPv4, Wi-Fi, Edge, Network edge firewall port 53 packet capture

B.2.5 Other results

This packet capture was taken during a device reboot. Notice a significant number of queries, but mostly directed at Apple, Cloudflare, and Akamaiedge domains. After Cloudflare authentication takes place, the DNS queries over port 53 are reduced to only a few specific top level domains.

```
01:36:15.114271 IP 9.9.9.9.53 > 10.0.140.24.61258: 44173 1/1/0 CNAME gsp85-ssl.ls2-apple.com.akadns.net. (151)
01:36:15.114365 IP 9.9.9.9.53 > 10.0.140.24.56744: 35273 3/0/0 CNAME gsp85-ssl.ls2-apple.com.akadns.net. , A 17.142.171.10, A 17.142.171.4 (120)
01:36:15.118315 IP 10.0.140.24.56138 > 9.9.9.9.53: 7474+ Type65? gsp85-ssl.ls2-apple.com.akadns.net. (52)
01:36:15.118379 IP 10.0.140.24.62067 > 9.9.9.9.53: 45715+ Type65? e10499.dsce9.akamaiedge.net. (45)
01:36:15.119461 IP 10.0.140.24.65167 > 9.9.9.9.53: 4846+ Type65? e6987.dsce9.akamaiedge.net. (44)
01:36:15.119526 IP 10.0.140.24.55072 > 9.9.9.9.53: 32750+ Type65? e1329.g.akamaiedge.net. (40)
01:36:15.131715 IP 9.9.9.9.53 > 10.0.140.24.62499: 43612 9/0/0 CNAME fmf.fe.apple-dns.net., A 17.248.137.170, A 17.248.137.211, A 17.248.137.74, A 17.248.184.113, A 17.248.184.10, A 17.248.184.74, A 17.248.184.17, A 17.248.137.138 (198)
01:36:15.131939 IP 9.9.9.9.53 > 10.0.140.24.51896: 29101 1/1/0 CNAME fmf.fe.apple-dns.net. (140)
01:36:15.133946 IP 10.0.140.24.52501 > 9.9.9.9.53: 18800+ Type65? fmf.fe.apple-dns.net. (38)
01:36:15.141840 IP 9.9.9.9.53 > 10.0.140.24.65167: 4846 0/1/0 (109)
01:36:15.142157 IP 9.9.9.9.53 > 10.0.140.24.56138: 7474 0/1/0 (118)
01:36:15.143112 IP 9.9.9.9.53 > 10.0.140.24.55072: 32750 0/1/0 (101)
01:36:15.143773 IP 9.9.9.9.53 > 10.0.140.24.62067: 45715 0/1/0 (110)
01:36:15.156451 IP 9.9.9.9.53 > 10.0.140.24.52501: 18800 0/1/0 (111)
01:36:15.219596 IP 10.0.140.24.56379 > 9.9.9.9.53: 58357+ Type65? basejumper.apple.com. (38)
01:36:15.219656 IP 10.0.140.24.61929 > 9.9.9.9.53: 18590+ A? basejumper.apple.com. (38)
01:36:15.243233 IP 9.9.9.9.53 > 10.0.140.24.56379: 58357 0/1/0 (107)
01:36:15.243334 IP 9.9.9.9.53 > 10.0.140.24.61929: 18590 0/1/0 (107)
01:36:15.308446 IP 10.0.140.24.56160 > 9.9.9.9.53: 45708+ Type65? captive.apple.com. (35)
01:36:15.308515 IP 10.0.140.24.60291 > 9.9.9.9.53: 20854+ A? captive.apple.com. (35)
01:36:15.331263 IP 9.9.9.9.53 > 10.0.140.24.56160: 45708 3/1/0 CNAME captive-cidr.origin-apple.com.akadns.net., CNAME captive-cdn.origin-apple.com.akadns.net., CNAME captive.g.aaplimg.com. (201)
01:36:15.331773 IP 9.9.9.9.53 > 10.0.140.24.60291: 20854 4/0/0 CNAME captive-cidr.origin-apple.com.akadns.net., CNAME captive-cdn.origin-apple.com.akadns.net., CNAME captive.g.aaplimg.com., A 17.253.13.205 (163)
01:36:15.333312 IP 10.0.140.24.52807 > 9.9.9.9.53: 8188+ Type65? captive.g.aaplimg.com. (39)
01:36:15.333372 IP 10.0.140.24.51822 > 9.9.9.9.53: 18095+ A? captive.g.aaplimg.com. (39)
01:36:15.355672 IP 9.9.9.9.53 > 10.0.140.24.51822: 18095 2/0/0 A 17.253.13.203, A 17.253.13.201 (71)
01:36:15.355934 IP 9.9.9.9.53 > 10.0.140.24.52807: 8188 0/1/0 (99)
01:36:15.653247 IP 10.0.140.24.58436 > 9.9.9.9.53: 25429+ A? www.icloud.com. (32)
01:36:15.683992 IP 9.9.9.9.53 > 10.0.140.24.58436: 25429 4/0/0 CNAME www-cdn.icloud.com.akadns.net., CNAME www.icloud.com.edgekey.net., CNAME e4478.a.akamaiedge.net., A 23.79.31.71 (161)
01:36:17.920343 IP 10.0.140.24.52448 > 9.9.9.9.53: 2054+ A? p50-keyvalueservice.icloud.com. (48)
01:36:17.950921 IP 9.9.9.9.53 > 10.0.140.24.52448: 2054 9/0/0 CNAME keyvalueservice.fe.apple-dns.net., A 17.248.184.143, A 17.248.137.86, A 17.248.184.201, A 17.248.137.196, A 17.248.137.208, A 17.248.137.89, A 17.248.184.101, A 17.248.137.177 (222)
01:36:18.070901 IP 10.0.140.24.55844 > 9.9.9.9.53: 34739+ Type65? cloudflareportal.com. (38)
01:36:18.070989 IP 10.0.140.24.52668 > 9.9.9.9.53: 18410+ A? cloudflareportal.com. (38)
01:36:18.096686 IP 9.9.9.9.53 > 10.0.140.24.52668: 18410 2/0/0 A 104.19.153.125, A 104.19.154.125 (70)
01:36:18.101275 IP 9.9.9.9.53 > 10.0.140.24.55844: 34739 1/0/0 Type65 (108)
01:36:18.197428 IP 10.0.140.24.60671 > 9.9.9.9.53: 60405+ A? ipv4only.arpa. (31)
01:36:18.219676 IP 9.9.9.9.53 > 10.0.140.24.60671: 60405 2/0/0 A 192.0.0.171, A 192.0.0.170 (63)
01:36:18.439424 IP 10.0.140.24.61845 > 9.9.9.9.53: 2003+ Type65? oi6xykug6h.cloudflare-gateway.com. (51)
01:36:18.439510 IP 10.0.140.24.54636 > 9.9.9.9.53: 37747+ A? oi6xykug6h.cloudflare-gateway.com. (51)
01:36:18.469668 IP 9.9.9.9.53 > 10.0.140.24.54636: 37747 2/0/0 A 162.159.36.20, A 162.159.36.5 (83)
01:36:18.474684 IP 9.9.9.9.53 > 10.0.140.24.61845: 2003 0/1/0 (110)
01:36:19.488501 IP 10.0.140.24.52317 > 9.9.9.9.53: 32274+ TXT? _aaplcache2._tcp.gps.lab. (42)
01:36:19.488571 IP 10.0.140.24.52317 > 9.9.9.9.53: 34845+ TXT? _aaplcache._tcp.gps.lab. (41)
01:36:19.488581 IP 10.0.140.24.52317 > 9.9.9.9.53: 25423+ TXT? _aaplcache1._tcp.gps.lab. (42)
01:36:19.497071 IP 10.0.140.24.52317 > 9.9.9.9.53: 9620+ TXT? _aaplcache3._tcp.gps.lab. (42)
01:36:19.497098 IP 10.0.140.24.52317 > 9.9.9.9.53: 10783+ TXT? _aaplcache4._tcp.gps.lab. (42)
01:36:19.510992 IP 9.9.9.9.53 > 10.0.140.24.52317: 32274 NXDomain 0/1/0 (117)
01:36:19.511529 IP 9.9.9.9.53 > 10.0.140.24.52317: 25423 NXDomain 0/1/0 (117)
01:36:19.511608 IP 9.9.9.9.53 > 10.0.140.24.52317: 34845 NXDomain 0/1/0 (116)
01:36:19.518822 IP 9.9.9.9.53 > 10.0.140.24.52317: 9620 NXDomain 0/1/0 (117)
01:36:19.519059 IP 9.9.9.9.53 > 10.0.140.24.52317: 10783 NXDomain 0/1/0 (117)
```

Figure B-20. iOS, IPv4, Wi-Fi, device reboot

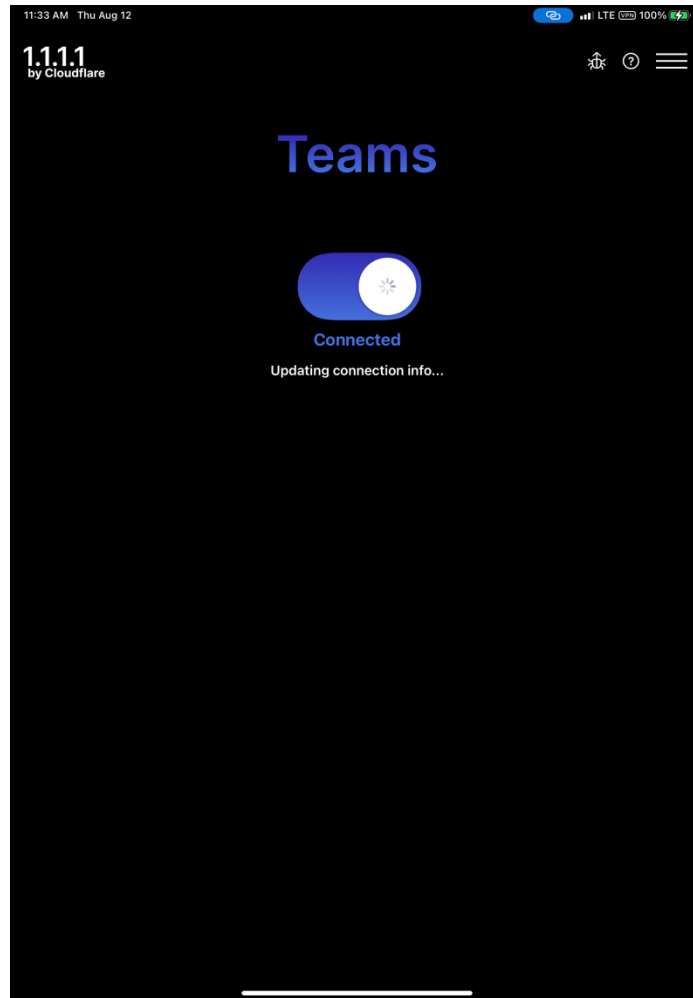


Figure B-21. Teams stuck connection

The Cloudflare WARP agent would often get stuck “Updating connection info”. It was not determined if this would have affected any of the test results, as a full connection was re-established before resuming the network tests. Resetting the agent was often required during testing.

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

BYOD	Bring Your Own Device
CISA	Cyber Security & Infrastructure Agency
DHS	Department of Homeland Security
DNS	Domain Name System
DNS over HTTPS	Domain Name System over Hyper Text Transfer Protocol Secure
DNS over TLS	Domain Name System over Transport Layer Security
FCEB	Federal Civilian Executive Branch
FedRAMP	Federal Risk and Authorization Management Program
GPS	GuidePoint Security
IdAM	Identity and Access Management
IMEI	International Mobile Equipment Identity
IdP	Identity Provider
IP	Internet Protocol
MAM	Mobile Application Management
MDM	Mobile Device Management
NSA	National Security Agency
PDNS	Protective Domain Name System
PDNSSP	Protective Domain Name System Service Provider
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SRMNI	Secure Resilient Mobile Network Infrastructure
TCP	Transmission Control Protocol
TIC	Trusted Internet Connection
TLS	Transport Layer Security
UDP	User Data Protocol
VPN	Virtual Private Network