DHS Science and Technology Directorate

Homeland Security
Science and Technology

PROVIDING MOBILE DNS SECURITY

As agencies have become mobile and their employees are working all over the country with devices such as mobile phones and tablets, there is a need to provide Domain Name System (DNS) security to those users and mobile traffic without backhauling traffic through a Virtual Private Network (VPN) back to agency networks and to a static Trusted Internet Connection (TIC).

Backhauling traffic to on-premises infrastructure impedes the ability of mobile users to effectively complete their work, which can have a negative impact on the agency's mission because of network performance issues resulting from high latency and low throughput of VPN implementations.

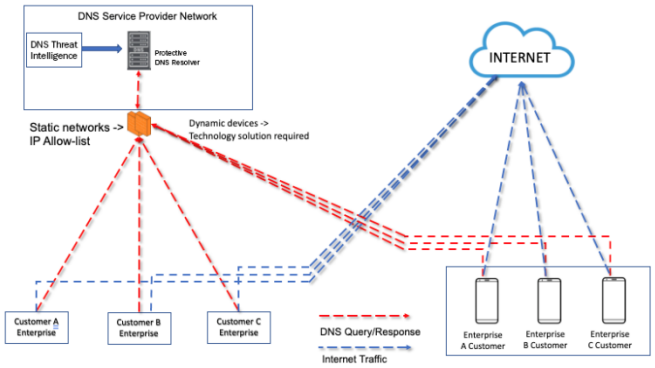
DEVELOPING PROTECTIVE DNS CAPABILITIES

This GuidePoint Security Secure and Resilient Mobile Network Infrastructure (SRMNI) research-and-development project is seeking to improve protection and monitoring of mobile devices accessing systems and services on mobile networks by building DNS capabilities and service offerings, while adhering to all privacy laws and regulations.

The developed protective DNS solution will provide a guideline to Federal Civilian Executive Branch agencies describing implementation. The development process will be used to acquire knowledge regarding tradeoffs in approach, identify issues with scalability, enterprise management and security considerations.

This effort will architect, build, and evaluate a mobile traffic filtering architecture using DNS routing as the underlying flows to be evaluated. In addition, determining performance at a user-level will be accomplished using Android and iOS devices including both smartphones and tablets.

The pilot will focus on the scaling of the user traffic to test the identified/required use-cases, including enabling the use of protective DNS on mobile devices.



Target Network Architecture Diagram

MANAGING MOBILE DNS TRAFFIC

The benefits of this work will be the creation of techniques to protect mobile DNS traffic and protect mobile device users from resolving malicious domains that host malware, disrupting malware command and control, and defending against the spread of viruses.

The diagram above shows how the protective DNS architecture will shift protection onto mobile devices via a host agent, which is capable of intercepting mobile device DNS queries before they leave the operating system and then redirecting that DNS traffic to the desired protective DNS service provider network.

This design negates the requirement to backhaul all mobile traffic to a corporate data center for filtering; only DNS traffic is redirected to a cloud based entity. Additionally, it can provide protection from malware and enforce corporate policy by shaping mobile traffic at the DNS layer.

UPCOMING MILESTONES

- Prototype Demonstration—July 2021
- Pilot Deployment—October 2021

SRMNI R&D PERFORMER

GuidePoint Security, Herndon, VA