efficient iP™

DoH For Remote Users

With more users working outside the protected walls, all organizations want to increase the security of their activities and resources, including those of IT. Improving control over the traffic between each remote worker and the organization's applications is key for smooth business operations and reducing potential of security issues that may cause severe damage.

Some web browsers are already relying on DoH (DNS over HTTPS) for their own IP resolution. But using DoH with an untrusted public DNS service risks misuse of browsing data and reveals applications being utilized. In order to better protect their remote workers, organizations should therefore instead consider extending their private DNS recursive service and manage the DoH themselves.

Use of standard protocols and available industry solutions may help increase overall security. DNS solutions which combine encryption and intelligent filtering bring a first line of defense for any IT user of the organization, whether working from the corporate buildings, from a remote facility, from home or even from an internet cafe.

This document shares how DoH and DNS security can protect the users and devices located outside the perimeter of the organization network with solutions and technologies able to encrypt traffic, control access and filter application access by leveraging cloud infrastructure, standard tools, open source solutions, commodity networks and EfficientIP SOLIDserver.

Solution Benefits

INTERNALLY MANAGED	trusted solution for the DNS service
STRENGTHENED SECURITY	secure and controlled DNS transactions
SIMPLIFIED NETWORK MANAGEMENT	same protection level for resident and remote users
ADVANCED SECURITY	optimal app protection with user behavior analysis

Why use DNS for security?

The DNS service is one of the first essential steps required to establish communication between a client and an application. As the intent of these communications, it can have a very accurate understanding of the traffic that occurs on a network and therefore what device (and by extension its user) connects to which server (and by extension which application). The central position of the DNS raises both excitement and fear with regards to security and privacy.

Privacy is directly linked to the ability to obtain data and the right to use it for a destination which is not the original one. It relies mainly on the trust a user can have in all providers starting by the one providing the application, and can be influenced through regulation and contractual documentation. On the other hand, security is a vast and complex topic. Security rules can be enforced by many solutions like encryption, digital signature, access control or observability. Security is used to protect the clients and applications, but also the infrastructure in a mutual interest.

DNS data collected along with that obtained from the real interest in the service provided can also be protected. Since its initial design, DNS still mainly uses UDP for its transport with data transferred in clear, easy to intercept, modify and use for various purposes including the bad ones. In order to improve the security associated with the DNS protocols, several proposals and implementations are available: cookie, port randomization, DNSSEC, DNS over TLS and more recently DNS over HTTPS.

DoH for Internet travel protection

DoH (DNS over HTTPS) is now gaining popularity and traction with a majority of business applications running directly from browsers which ease the implementation of such evolution on how IP addresses are resolved. The messaging around DoH adoption has surfed on the security and data protection waves, spreading fears with Internet users who suspect all providers spy on their usages, including their own ISP.

This is why the first offensives came from internet browser solutions such as Google Chrome and Mozilla Firefox with direct and automatic installation of DoH encryption using a few service providers like Cloudflare and Google. However, when it comes to private Internet usage, enterprise users and business apps, it remains debatable whether on or not DoH should be used, and with which provider.

Organizations should provide a comfortable and secure working environment to their employees - those sitting in the office and now also the vast amount working from Small Office/Home Office (SOHO) or coworking spaces. Relying on DoH with a random and trustless provider brings neither value nor ability to protect the user efficiently. A different approach is therefore required, leveraging the same technologies but relying on a private infrastructure. This can ensure that any DNS traffic from users and devices use the organization's infrastructure, which allows the company to provide additional services like security, filtering and observability in a highly performant and controlled environment.

Building a private DoH infrastructure

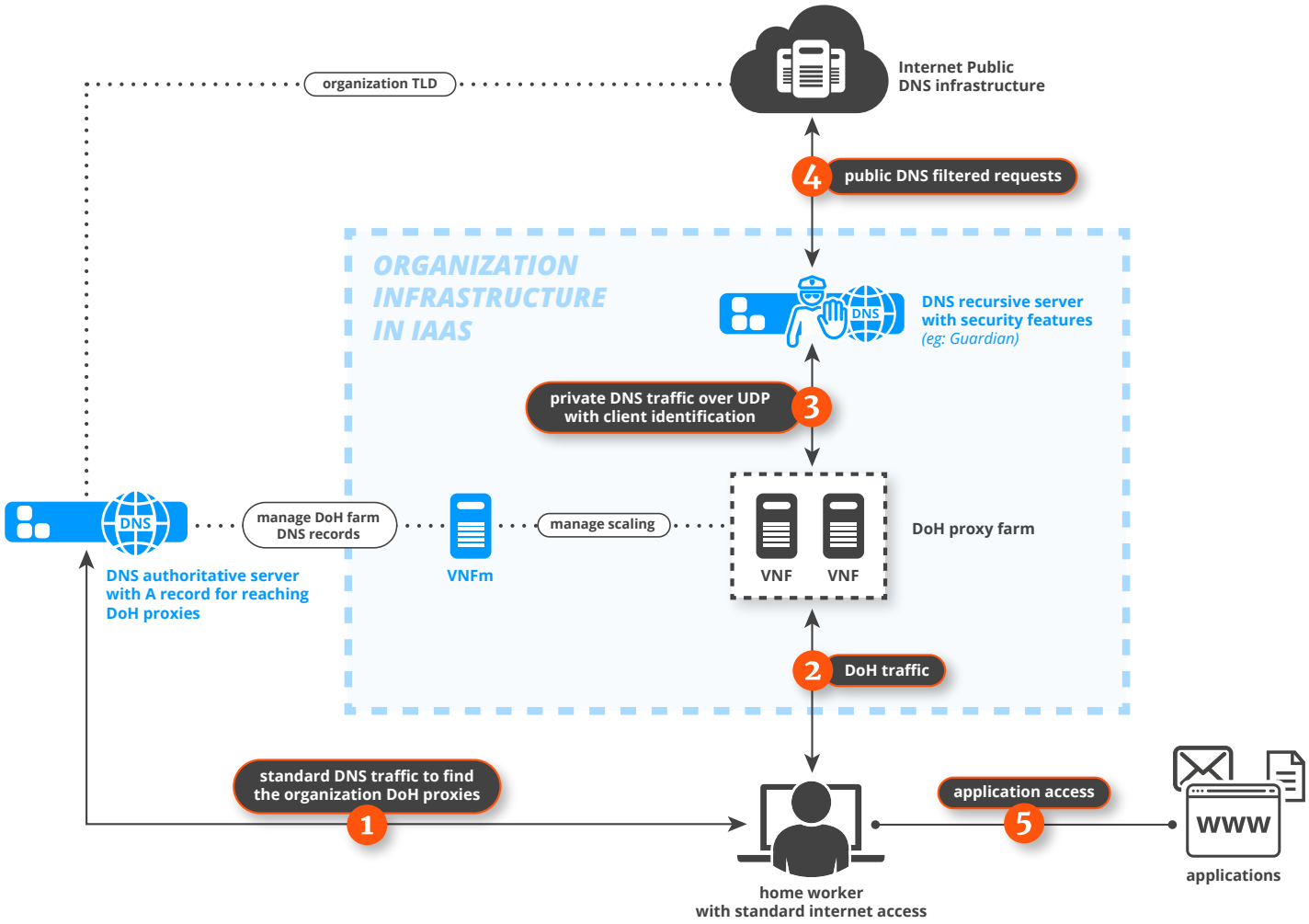
Deploying their own managed DoH infrastructure is neither complex nor costly to a business. It can be a very beneficial project involving network automation, cloud infrastructure, automatic scaling and other nice concepts.

The main 2 blocks to design and implement are:

- a backend infrastructure consisting of a robust recursive DNS service, redundant and regionalized for performances and limited localization impact. This layer can bring DNS security, user behavior analysis and domain reputation filtering if required.
- a frontend consisting of a DoH proxy service that converts a request arriving from a user internet browser into a standard DNS request pushed to the backend. This service should be available directly from the internet network and be scalable, since performance impact of HTTPS is far more important than when using UDP for the DNS traffic.

All these components can be hosted in any kind of cloud-proposing infrastructure services like VM, exposed and private networking and eventually some automatic scaling options that can also be performed with a more autonomous approach with VNF (Virtual Network Functions) and VNFm (its Manager) components. The point of presence of the cloud provider should match the main location (countries, states, towns) where the users are working from.

Since finding a DoH server is still an issue with no automatic process available on the IP network, we can easily rely on a corporate DNS record pointing to all the IP addresses of the DoH proxies in each region. For sure an anycast address would be ideal but not all companies can afford such a setup and it is not really the purpose of this internal service to be widely available.



The communication process with such an infrastructure is the following:

1. The home worker device looks for the DoH proxy address based on its name (eg: doh-emea.efficientip.com), this record is hosted in the corporate public DNS infrastructure
2. The DoH traffic is established for any subsequent request with one of the DoH proxy using HTTPS as a transport protocol and eventually mutual digital certificate authentication (client and DoH proxy)
3. The DoH proxy extracts the DNS request from the request payload, add the client identification in the EDNS fields and forward the request to the local Guardian DNS engine
4. The Guardian DNS performs analysis, filtering, cache control and if necessary recurses the request to the public DNS service
5. The home worker can access the application based on the DNS answer

On this service architecture high level design we see that the whole infrastructure is hosted for the region in a IaaS that could be proposed by internal IT or an external cloud provider. The role of the VNFm (Virtual Network Function Manager) is to evaluate the usage and load of the DoH proxies and scale the service up and down accordingly. It manages the DoH proxy service DNS record in order to allow client connection and load balancing between proxies with a very simple approach. The Guardian service represented here by a single appliance performs all the value added security that is proposed to the remote workers with its broad capacities and features from user behavioral analysis to advanced filtering and countermeasures.

Key Takeaways

DNS over HTTPS is a new opportunity and a new challenge for organizations for which remote workers bring complexity in managing application access and overall security. A controlled DNS infrastructure guarantees that security measures can match organization expectations. Managing a DoH service for remote users brings value and coherence in the DNS security approach the organization is pursuing.

SOLIDserver DNS security solution can easily manage DoH natively but also be integrated in a wider ecosystem where DoH is managed by software edge solutions closest to the users. By being able to apply the same security policies for resident and remote workers, the I&O teams enhance the overall security of the IT systems and protect first their users and the data of the organization. In a context of increased attacks through malware, backdoors, denial of service and supply chain code modification this controlled infrastructure approach brings a lot of value with minimum effort.

efficient iP™

REV: C-201229

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752