

ADD
Internet-Draft
Intended status: Informational
Expires: December 25, 2020

T. Reddy
McAfee
D. Wing
Citrix
June 23, 2020

DNS-over-HTTPS and DNS-over-TLS Server Deployment Considerations for
Enterprise Networks
draft-reddy-add-enterprise-00

Abstract

This document discusses DoH/DoT deployment considerations for Enterprise networks. It particularly sketches the required steps to use DNS-over-TLS (DoT) and/or DNS-over-HTTPS (DoH) server provided by the Enterprise network.

One of the goals of the document is to assess to what extent existing tools can be used to provide such service.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 25, 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	4
3.	IT-owned devices	4
4.	IoT Devices	4
5.	BYOD	6
6.	Roaming Enterprise Users	7
6.1.	VPN tunnel	7
6.2.	Client Authentication	7
7.	Upstream Encryption	8
8.	Security Considerations	8
9.	IANA Considerations	8
10.	Acknowledgements	8
11.	References	9
11.1.	Normative References	9
11.2.	Informative References	9
	Authors' Addresses	13

[1.](#) Introduction

[RFC7626] discusses DNS privacy considerations in both "on the wire" ([Section 2.4 of \[RFC7626\]](#)) and "in the server" ([Section 2.5 of \[RFC7626\]](#)) contexts. In recent years there has also been an increase in the availability of "public resolvers" [[RFC8499](#)] which DNS clients may be pre-configured to use instead of the default network resolver for a variety of reasons (e.g., offer a good reachability, support an encrypted transport, provide a strong privacy policy, (lack of) filtering).

If public (DoT) [[RFC7858](#)] or DNS-over-HTTPS (DoH) [[RFC8484](#)] servers are used instead of using local DNS servers, it can adversely impact Enterprise network-based security. Various network security services are provided by Enterprise networks to protect endpoints (e.g., laptops, printers, IoT devices), and to enforce enterprise policies. These policies may be necessary to protect employees, customers, or citizens. They are not the subject of this memo.

Enterprise DNS servers in place for these purpose act on DNS requests originating from endpoints. However, if an endpoint uses public DoT or DoH servers, the desired enterprise protection and enforcement can be bypassed.

In order to act on DNS requests from endpoints, network security services can block DoT traffic by dropping outgoing packets to destination port 853. Identifying DoH traffic is far more challenging than DoT traffic. Network security services may try to identify the well-known DoH resolvers by their domain name, and DNS-over-HTTPS traffic can be blocked by dropping outgoing packets to these domains. However, DoH traffic can not be fully identified without acting as a TLS proxy.

If a network security service blocks access to the public DoH/DoT server, there are incompatibilities with the privacy profiles discussed in [[RFC8310](#)]:

- o If an endpoint has enabled strict privacy profile ([Section 5 of \[\[RFC8310\]\(#\)\]](#)), the endpoint cannot resolve DNS names.
- o If an endpoint has enabled opportunistic privacy profile ([Section 5 of \[\[RFC8310\]\(#\)\]](#)), the endpoint will either fallback to an encrypted connection without authenticating the DNS server provided by the local network or fallback to clear text DNS, and cannot exchange encrypted DNS messages. The fallback adversely impacts security and privacy as internal attacks are possible in Enterprise networks. For example, an internal attacker can modify the DNS responses to re-direct the client to malicious servers or pervasively monitor the DNS traffic. The reader may refer to Section 3.2.1 of [[I-D.arkko-farrell-arch-model-t](#)] for a discussion on the need for more awareness about attacks from within closed domains.

To overcome the above threats, this document specifies mechanisms to configure endpoints to use Enterprise provided DoT and DoH servers, and bootstrap IoT devices and unmanaged endpoints to discover and authenticate the DoT and DoH servers provided by the Enterprise network.

A common usage pattern for an IoT device is for it to "call home" to

a service that resides on the public Internet, where that service is referenced through a domain name (A or AAAA record). As discussed in Manufacturer Usage Description Specification [[RFC8520](#)], because these devices tend to require access to very few sites, all other access should be considered suspect. However, if the query is not accessible for inspection, it becomes quite difficult for the infrastructure to suspect anything.

This document focuses on DoH/DoT deployment considerations for Enterprise networks, DoH/DoT sever discovery and deployment considerations for home networks are discussed in [[I-D.btw-add-home](#)].

[2.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)][[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

This document makes use of the terms defined in [[RFC8499](#)] and [[I-D.ietf-dnsop-terminology-ter](#)].

'DoH/DoT' refers to DNS-over-HTTPS and/or DNS-over-TLS.

[3.](#) IT-owned devices

If a device is managed by an enterprise's IT department, the device can be configured to use Enterprise-provided DoH/DoT servers. This configuration might be manual or rely upon whatever deployed device management tool in an Enterprise. For example, customizing Firefox using Group Policy to use the Enterprise DoH server is discussed in [[Firefox-Policy](#)] for Windows and MacOS, and setting Chrome policies is discussed in [[Chrome-Policy](#)] and [[Chrome-DoH](#)].

[4.](#) IoT Devices

The solution described in this document is aimed in general at non-constrained IoT devices (i.e., class 2+ [[RFC7228](#)]) operating on a Enterprise network without a device management tool and require agentless or standardized approaches. The basis for trust,

therefore, is quite different from that of a laptop, tablet, or smart phone. The following bootstrapping mechanisms can be used to securely provision IoT devices to use Enterprise provided DoT and DoH servers:

- o IoT devices supporting Bootstrapping Remote Secure Key Infrastructures (BRSKI) discussed in [\[I-D.ietf-anima-bootstrapping-keyinfra\]](#) can be bootstrapped with the Enterprise-provided DoH/DoT servers using the mechanism discussed in Section 5 of [\[I-D.reddy-add-iot-byod-bootstrap\]](#).
- o [\[RFC8572\]](#) defines a bootstrapping strategy for enabling devices to securely obtain the required configuration information with no installer input. DHCP/RA [\[I-D.btw-add-home\]](#) can be used to discover the DoH/DoT information. If the insecurely discovered DoH/DoT information is not pre-configured in the IoT device, the client can validate the Policy Assertion Token signature ([Section 7 \[I-D.reddy-add-server-policy-selection\]](#)) using the owner certificate ([Section 3.2 of \[RFC8572\]](#)).

- o When IoT devices connect to a network via EAP methods such as Tunnel Extensible Authentication Protocol (TEAP) [\[RFC7170\]](#), it would be possible to extend these methods to return additional configuration elements as part of completion of the authentication transaction. One simple approach would be after successful completion of the EAP method in Phase 2 for a TEAP server to return a new TLV that indicates the local DoH/DoT information.
- o Not all of IoT devices support 802.1x supplicant and need an alternate mechanism to connect to the Enterprise network. To address this limitation, unique pre-shared keys are created for each IoT device and WPA-PSK is used [\[PSK\]](#). In other words, WPA-PSK is used with unique pre-shared keys for different IoT devices to deal security issues.
- * The IoT device needs to be provisioned with a Pre-Shared Key (PSK) for mutual authentication. The PSK is only known to the IoT device and the WPA server. In this case, the bootstrapping mechanism discussed in Section 4 of [\[I-D.reddy-add-iot-byod-bootstrap\]](#) may be used to securely bootstrap IoT device with the authentication domain name (ADN) and DNS server certificate of the local network's DoH/ DoT

server. It uses password-based authenticated key exchange (PAKE) scheme to authenticate the EST server and fetch the DoH/DoT server certificate. Note that provisioning massive number of IoT devices with PSK is not a scalable onboarding mechanism but will work in Small Office/Home Office (SOHO) and Small/Medium Enterprise (SME).

- o If Device Provisioning Protocol (DPP) [[dpp](#)] is used, the configurator can securely configure IoT devices with the local DoH/DoT server by extending the content of the configuration elements provided by the configurator. Because DPP can provide a private shared key for use with WPA-PSK, it can be combined with the above methods.
- o The OMA LWM2M specification [[oma](#)] defines an architecture where a new device (LWM2M client) contacts a Bootstrap-server which is responsible for "provisioning" essential bootstrap information. The current standard defines the following four bootstrapping modes (1) Factory Bootstrap (2) Bootstrap from Smartcard (3) Client Initiated Bootstrap (4) Server Initiated Bootstrap. The bootstrap information can be extended to include the local DoH/DoT server details.
- o The Open Connectivity Foundation [[ocf](#)] defines the onboarding process before a device is operational. Once the onboarding tool and the new device have authenticated and established secure

communication, the onboarding tool can provision the IoT device with the local DoH/DoT server.

This document does not discuss opportunistic or leap-of-faith bootstrapping methods, they are susceptible to security issues (e.g., IoT device can be configured with the attacker's DoH/DoT server or disable the use of DoH/DoT).

[5.](#) BYOD

The following mechanisms can be used to bootstrap BYOD (bring your own device) with the DoH/DoT server used by the Enterprise network:

- o If mobile device management (MDM) [[MDM-Apple](#)] is used to secure BYOD, MDM can be used to configure OS/browser with the Enterprise

provided DoH/DoT server.

- o If an endpoint is on-boarded, for example, using Over-The-Air (OTA) enrollment [[OTA](#)] to provision the device with a certificate and configuration profile, the configuration profile can include the authentication domain name (ADN) of the DoH/DoT server. The OS/Browser can use the configuration profile to use the Enterprise provided DoH/DoT server. In this case, MDM is not installed on the device.
- o If an endpoint uses the credentials (username and password) provided by the IT admin to mutually authenticate to the Enterprise WiFi Access Point (e.g., PEAP-MSCHAPv2 [[PEAP](#)], EAP-pwd [[RFC8146](#)], EAP-PSK [[RFC4764](#)]), the bootstrapping mechanism discussed in Section 4 of [[I-D.reddy-add-iot-byod-bootstrap](#)] can be used to securely bootstrap the endpoint with the ADN and DNS server certificate of the local network's DoH/DoT server.

The DNS client uses PAKE scheme to authenticate the EST server using the credentials to authenticate to the network. In this case, the endpoint is neither provisioned with a configuration profile or MDM is installed on the device. Many users have privacy and personal data sovereignty concerns with employers installing MDM on their personal devices; they are concerned that admin can glean personal information and could control how they use their devices. Yet when users do not install MDM on their devices, IT admins do not get visibility into the security posture of those devices.

To overcome this problem, a host agent can cryptographically attest the security status associated with device, such as minimum passcode length, biometric login enabled, OS version etc. This approach is fast gaining traction especially with the advent of

closed OS like Windows 10 in S mode [[win10s](#)] or Chromebook [[Chromebook](#)], where applications are sandboxed (e.g., ransomware attack is not possible) and applications can only be installed via the OS store.

When attached to the enterprise network yet needing to use the enterprise's DoH server only to access the internal-only DNS names, the client device can learn about domains for which the local

network's resolver is authoritative via `dnsZones` key defined in Section 4.3 of [[I-D.ietf-intarea-provisioning-domains](#)] (as other DoH/DoT servers will be unaware of the internal-only DNS names).

[6.](#) Roaming Enterprise Users

[6.1.](#) VPN tunnel

In this Enterprise scenario ([Section 1.1.3 of \[RFC7296\]](#)), a roaming user connects to the Enterprise network through an VPN tunnel (e.g., IPsec, SSL, Wireguard). The split-tunnel Virtual Private Network (VPN) configuration allows the endpoint to access hosts that reside in the Enterprise network [[RFC8598](#)] using that tunnel; other traffic not destined to the Enterprise does not traverse the tunnel. In contrast, a non-split- tunnel VPN configuration causes all traffic to traverse the tunnel into the enterprise.

When the VPN tunnel is IPsec, The DoH/DoT server hosted by the Enterprise network can be securely discovered by the endpoint using the `INTERNAL_ENC_DNS IKEv2 Configuration Payload Attribute Type` defined in [[I-D.btw-add-ipsecme-ike](#)]. For split-tunnel VPN configurations, the endpoint uses the Enterprise-provided DoT/DoH server to resolve internal-only domain names. For non-split-tunnel VPN configurations, the endpoint uses the Enterprise-provided DoT/DoH server to resolve both internal and external domain names.

Other VPN tunnel types have similar configuration capabilities, not detailed here.

[6.2.](#) Client Authentication

When not on the local enterprise network (e.g., at home or coffee shop) yet needing to access the enterprise DoH/DoT server but not through a tunnel, roaming users can use client authentication to access the Enterprise provided DoH/DoT server. For example, Firefox DoH setting accepts user credentials [[Firefox-TRR](#)] to authenticate the client to access the DoH server. The exact client authentication mechanism to authenticate to the DoH/DoT server is outside the scope of this specification.

[7.](#) Upstream Encryption

If the Enterprise network is using the local DoH/DoT server configured as a Forwarding DNS server [[RFC8499](#)] relying on the upstream resolver (e.g., at an ISP) to perform recursive DNS lookups, DNS messages exchanged between the local DoH/DoT server and recursive resolver MUST be encrypted. If the Enterprise network is using the local DoH/DoT server configured as a recursive DNS server, DNS messages exchanges between the recursive resolver and authoritative servers SHOULD be encrypted to conform to the requirements discussed in [[I-D.ietf-dprive-phase2-requirements](#)].

[8.](#) Security Considerations

Security and privacy considerations in [[I-D.reddy-add-iot-byod-bootstrap](#)] need to be taken into consideration.

The mechanism defined in [[I-D.reddy-add-server-policy-selection](#)] can be used by the DNS server to communicate its privacy statement URL and filtering policy to a DNS client. This communication is cryptographically signed to attest to its authenticity.

The DNS client can validate the signatory (i.e., cryptographically attested by the Organization hosting the DoH/DoT server) and the user can review human-readable privacy policy information of the DNS server and assess whether the DNS server performs DNS-based content filtering.

If the discovered DoH/DoT server does not meet the privacy preserving data policy and filtering requirements of the user, the user can instruct the DNS client to take appropriate actions. For example, the action can be to use the local DNS server only to access internal-only DNS names and use another DNS server (adhering with his/her expectations) for public domains.

[9.](#) IANA Considerations

This document has no actions for IANA.

[10.](#) Acknowledgements

Thanks to Mohamed Boucadair, Sandeep Rao, Vinny Parla, Nancy Cam-Winget and Eliot Lear for the discussion and comments.

11. References

11.1. Normative References

- [I-D.reddy-add-iot-byod-bootstrap]
Reddy.K, T., Wing, D., Richardson, M., and M. Boucadair,
"A Bootstrapping Procedure to Discover and Authenticate
DNS-over-TLS and DNS-over-HTTPS Servers for IoT and BYOD
Devices", [draft-reddy-add-iot-byod-bootstrap-00](#) (work in
progress), May 2020.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", [BCP 14](#), [RFC 2119](#),
DOI 10.17487/RFC2119, March 1997,
<<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D.,
and P. Hoffman, "Specification for DNS over Transport
Layer Security (TLS)", [RFC 7858](#), DOI 10.17487/RFC7858, May
2016, <<https://www.rfc-editor.org/info/rfc7858>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC
2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174,
May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles
for DNS over TLS and DNS over DTLS", [RFC 8310](#),
DOI 10.17487/RFC8310, March 2018,
<<https://www.rfc-editor.org/info/rfc8310>>.
- [RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS
(DoH)", [RFC 8484](#), DOI 10.17487/RFC8484, October 2018,
<<https://www.rfc-editor.org/info/rfc8484>>.

11.2. Informative References

- [Chrome-DoH]
The Unicode Consortium, "Chrome DNS over HTTPS (aka DoH)",
<<https://www.chromium.org/developers/dns-over-https>>.
- [Chrome-Policy]
The Unicode Consortium, "Chrome policies for users or
browsers", <[https://support.google.com/chrome/a/
answer/2657289?hl=en](https://support.google.com/chrome/a/answer/2657289?hl=en)>.

[Chromebook]

Microsoft, "Chromebook security",
<<https://support.google.com/chromebook/answer/3438631?hl=en>>.

[dpp]

Wi-Fi Alliance, "Wi-Fi Device Provisioning Protocol (DPP)", Wi-Fi Alliance, 2018, <https://www.wi-fi.org/download.php?file=/sites/default/files/private/Device_Provisioning_Protocol_Specification_v1.1_1.pdf>.

[Firefox-Policy]

"Policy templates for Firefox",
<<https://github.com/mozilla/policy-templates/blob/master/README.md#dnsoverhttps>>.

[Firefox-TRR]

"Trusted Recursive Resolver",
<https://wiki.mozilla.org/Trusted_Recursive_Resolver>.

[I-D.arkko-farrell-arch-model-t]

Arkko, J. and S. Farrell, "Challenges and Changes in the Internet Threat Model", [draft-arkko-farrell-arch-model-t-03](#) (work in progress), March 2020.

[I-D.btw-add-home]

Boucadair, M., Reddy, K. T., Wing, D., and N. Cook, "Encrypted DNS Discovery and Deployment Considerations for Home Networks", [draft-btw-add-home-06](#) (work in progress), May 2020.

[I-D.btw-add-ipsecme-ike]

Boucadair, M., Reddy, K. T., Wing, D., and V. Smyslov, "Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS", [draft-btw-add-ipsecme-ike-00](#) (work in progress), April 2020.

[I-D.ietf-anima-bootstrapping-keyinfra]

Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key

Infrastructures (BRSKI)", [draft-ietf-anima-bootstrapping-keyinfra-41](#) (work in progress), April 2020.

[I-D.ietf-dnsop-terminology-ter]

Hoffman, P., "Terminology for DNS Transports and Location", [draft-ietf-dnsop-terminology-ter-01](#) (work in progress), February 2020.

Reddy & Wing

Expires December 25, 2020

[Page 10]

Internet-Draft

DoH/DoT in Enterprise Networks

June 2020

[I-D.ietf-dprive-phase2-requirements]

Livingood, J., Mayrhofer, A., and B. Overeinder, "DNS Privacy Requirements for Exchanges between Recursive Resolvers and Authoritative Servers", [draft-ietf-dprive-phase2-requirements-01](#) (work in progress), June 2020.

[I-D.ietf-intarea-provisioning-domains]

Pfister, P., Vyncke, E., Pauly, T., Schinazi, D., and W. Shao, "Discovering Provisioning Domain Names and Data", [draft-ietf-intarea-provisioning-domains-11](#) (work in progress), January 2020.

[I-D.reddy-add-server-policy-selection]

Reddy, K. T., Wing, D., Richardson, M., and M. Boucadair, "DNS Server Selection: DNS Server Information with Assertion Token", [draft-reddy-add-server-policy-selection-03](#) (work in progress), June 2020.

[MDM-Apple]

Apple, "Mobile Device Management",
<<https://developer.apple.com/documentation/devicemanagement>>.

[ocf]

Open Connectivity Foundation, "OCF Security Specification", Open Connectivity Foundation, June 2017,
<https://openconnectivity.org/specs/OCF_Security_Specification_v1.0.0.pdf>.

[oma]

Open Mobile Alliance, "Lightweight Machine to Machine Technical Specification: Core", Open Mobile Alliance, June 2019,
<<http://www.openmobilealliance.org/release/LightweightM2M/>>.

[V1_1_1-20190617-A/OMA-TS-LightweightM2M_Core-V1_1_1-20190617-A.pdf](#)>.

- [OTA] Apple, "Over-the-Air Profile Delivery Concepts", <<https://developer.apple.com/library/archive/documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/OTASecurity/OTASecurity.html>>.
- [PEAP] Microsoft, "[MS-PEAP]: Protected Extensible Authentication Protocol (PEAP)", <https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-peap/5308642b-90c9-4cc4-beec-fb367325c0f9>.

Reddy & Wing

Expires December 25, 2020

[Page 11]

Internet-Draft

DoH/DoT in Enterprise Networks

June 2020

- [PSK] Cisco, "Identity PSK Feature Deployment Guide", <https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html>.
- [RFC4764] Bersani, F. and H. Tschofenig, "The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method", [RFC 4764](#), DOI 10.17487/RFC4764, January 2007, <<https://www.rfc-editor.org/info/rfc4764>>.
- [RFC7170] Zhou, H., Cam-Winget, N., Salowey, J., and S. Hanna, "Tunnel Extensible Authentication Protocol (TEAP) Version 1", [RFC 7170](#), DOI 10.17487/RFC7170, May 2014, <<https://www.rfc-editor.org/info/rfc7170>>.
- [RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", [RFC 7228](#), DOI 10.17487/RFC7228, May 2014, <<https://www.rfc-editor.org/info/rfc7228>>.
- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, [RFC 7296](#), DOI 10.17487/RFC7296, October 2014, <<https://www.rfc-editor.org/info/rfc7296>>.

- [RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", [RFC 7626](#), DOI 10.17487/RFC7626, August 2015, <<https://www.rfc-editor.org/info/rfc7626>>.
- [RFC8146] Harkins, D., "Adding Support for Salted Password Databases to EAP-pwd", [RFC 8146](#), DOI 10.17487/RFC8146, April 2017, <<https://www.rfc-editor.org/info/rfc8146>>.
- [RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", [BCP 219](#), [RFC 8499](#), DOI 10.17487/RFC8499, January 2019, <<https://www.rfc-editor.org/info/rfc8499>>.
- [RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", [RFC 8520](#), DOI 10.17487/RFC8520, March 2019, <<https://www.rfc-editor.org/info/rfc8520>>.
- [RFC8572] Watsen, K., Farrer, I., and M. Abrahamsson, "Secure Zero Touch Provisioning (SZTP)", [RFC 8572](#), DOI 10.17487/RFC8572, April 2019, <<https://www.rfc-editor.org/info/rfc8572>>.

Reddy & Wing

Expires December 25, 2020

[Page 12]

Internet-Draft

DoH/DoT in Enterprise Networks

June 2020

- [RFC8598] Pauly, T. and P. Wouters, "Split DNS Configuration for the Internet Key Exchange Protocol Version 2 (IKEv2)", [RFC 8598](#), DOI 10.17487/RFC8598, May 2019, <<https://www.rfc-editor.org/info/rfc8598>>.
- [win10s] Microsoft, "Windows 10 in S mode", <<https://www.microsoft.com/en-us/windows/s-mode>>.

Authors' Addresses

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: kondtir@gmail.com

Dan Wing
Citrix Systems, Inc.
USA

Email: dwing-ietf@fuggles.com