Workgroup: ADD
Internet-Draft:
draft-reddy-add-enterprise-policy-00
Published: 21 September 2021
Intended Status: Standards Track
Expires: 25 March 2022
Authors: T. Reddy D. Wing K. Smith
Akamai Citrix Vodafone

Network policy to use Network-designated DNS Resolvers

Abstract

This document specifies a mechanism to inform endpoints about any network policy mandating the use of network-designated DNS resolvers.

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 25 March 2022.

Table of Contents

1. Introduction

Historically, an endpoint would utilize network-designated DNS servers upon joining a network (e.g., DHCP OFFER, IPv6 Router Advertisement). While it has long been possible to configure endpoints to ignore the network's suggestions and use a (public) DNS server on the Internet, this was seldom used because some networks block UDP/53 (in order to enforce their own DNS policies). Also, there has 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 claimed privacy policy, (lack of) filtering). With the advent of DoT and DoH, such network blocking is more difficult. The network is unable to express its policy to use network-designated resolvers to the endpoints and the endpoint is unable to identify the reason why the public DNS server is not reachable.

If DNS resolvers not signaled by the network (e.g., DNS-over-TLS (DoT) [RFC7858] or DNS-over-HTTPS (DoH) [RFC8484]) are used instead of using network-designated DNS servers, it can adversely impact Enterprise network-based security features. Indeed, various network security services are provided by Enterprise networks to protect endpoints (e.g., laptops, printers, IoT devices) and to enforce enterprise-specific policies. These policies may be necessary to protect employees, customers, or enterprise network. It is out of the scope of this memo to characterize such policies nor assess that they achieve the claimed intent. Nevertheless, network-designated DNS servers in place for these purposes act on DNS messages involving endpoints connected to the Enterprise network to enforce these policies. Therefore, if an endpoint uses a DNS resolver not signaled by the network, the desired enterprise protection level and enforcement will be bypassed and thus nullified.

In order to act on DNS messages involving endpoints connected to an Enterprise network, network security services can be configured to block DoT traffic by dropping outgoing packets to destination port number 853. Identifying DoH traffic is far more challenging than identifying DoT traffic. Network security services may try to identify the well-known DoH resolvers by their domain name and DoH 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.

With the advent of DoT and DoH, the network is unable to express any such policy to the endpoints, and if the network is blocking alternative resolvers, endpoints are unable to identify the reason why their choice of public DNS resolver is not reachable. This results in incompatibilities with the privacy profiles discussed in [RFC8310]:

* If an endpoint has enabled strict privacy profile (Section 5 of [RFC8310]), the endpoint cannot resolve DNS names.

* 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 signaled 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 within Enterprise networks. For example, an internal attacker can modify the DNS responses to re-direct a client to malicious servers or pervasively monitor the DNS traffic.

This document describes a mechanism for informing endpoints of network policy related to network-designated DNS servers, such as those DNS servers signaled using [I-D.ietf-add-dnr] and [I-D.ietf-add-ddr].

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]. The terms "Private DNS", "Global DNS" and "Split DNS" are defined in [RFC8499].

'Encrypted DNS' refers to a DNS protocol that provides an encrypted channel between a DNS client and server (e.g., DoT, DoH, or DoQ).

The term "enterprise network" in this document extends to a wide variety of deployment scenarios. For example, an "enterprise" can be a Small Office, Home Office or Corporation. The clients that connect to a enterprise network can securely authenticate that network and the client is sure that it has connected to the network it was expecting.

3. PvD NetworkDNSOnly and ErrorNetworkDNSOnly Keys

Provisioning Domains (PvDs) are defined in [RFC7556] as sets of network configuration information that clients can use to access networks, including rules for DNS resolution and proxy configuration. [RFC8801] defines a mechanism for discovering multiple Explicit PvDs on a single network and their Additional Information by means of an HTTP-over-TLS query using a URI derived from the PvD ID. This set of additional configuration information is referred to as a Web Provisioning Domain (Web PvD).

This document defines two PvD Key:

The NetworkDNSOnly PvD Key: which determines if network will block, or attempt to block, DNS queries sent to DNS servers that were not signaled by the network. This key has the value True or False (case insensitive).

The ErrorNetworkDNSOnly PvD Key: which contains a human-friendly description of the reason for the NetworkDNSOnly block. This key is only present if NetworkDNSOnly is True.

Some enterprise networks require clients to query the network-designated DNS servers, it sets the PvD NetworkDNSOnly key to True, otherwise sets NetworkDNSOnly to False. If NetworkDNSOnly is set to True, it implies the network will block, or attempt to block, DNS queries sent to DNS servers that were not signaled by the network. If NetworkDNSOnly is True, the ErrorNetworkDNSOnly key MUST contain a human-friendly description for this block. This information is intended for human consumption (not automated parsing). The ErrorNetworkDNSOnly key is useful when the client does not use DNS resolution by the network-designated DNS server to reach the DNS servers not signaled by the network. For example, the client can be pre-configured with both the domain name and IP addresses of the DNS server not signaled by the network (Section 7.1 in [RFC8310]) or the client can be pre-configured with the IP address of the resolver, and it uses IP address in the certificate as identifier (see [RFC8738]). In this case, the extended error code "Blocked" defined in [RFC8914] cannot be returned to the client to provide additional

information about the cause for the block. Further, the ErrorNetworkDNSOnly key is useful when the network security service fails to block access to the DNS server not signaled by the network but successfully filters traffic from the endpoint to IP addresses not conveyed to the endpoint as part of DNS resolution by the network-designated DNS server.

The NetworkDNSOnly set to True is an internal security policy expression by the operator of the network but is not a policy prescription to the endpoints to disable its use of its other configured DNS servers; that is, the endpoint can ignore NetworkDNSOnly set to True. If joining an un-trusted network (e.g., coffeeshop, hotel, airport network), a True value of NetworkDNSOnly MUST be ignored. The mechanism the client uses to determine 'trusted network' to assist the user MUST involve authenticated identity of the network (not merely matching SSID in the case of WiFi), such as 802.1X or confirming the network-designated encrypted resolver name is pre-configured in the Operating System and TLS handshake with it succeeds. For example, the client can determine "Open" (unencrypted) wireless networks are untrusted networks, notify the user that using a shared and public Pre-Shared Key (PSK) for wireless authentication is a untrusted network. If the pre-shared-key is the same for all clients that connect to the same WLAN, the shared key will be available to all nodes, including attackers, so it is possible to mount an active on-path attack (e.g., [Evil-Twin], [Krack], [Dragonblood]). For example, coffee shops and air ports use PSK and are unwilling to perform complex configuration on their networks. In addition, customers are generally unwilling to do complicated provisioning on their devices just to obtain free Wi-Fi. This type of networks can be tagged as "untrusted networks" with minimal human intervention. In such cases the endpoint MAY choose to use an alternate network (e.g., cellular) to resolve the global domain names.

4. Scope of NetworkDNSOnly Key

If a device is managed by an enterprise's IT department, the device can be configured to use a specific encrypted DNS server. This configuration may be manual or rely upon whatever deployed device management tool in an enterprise network. 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].

If mobile device management (MDM) (e.g., [MDM-Apple]) secures a device, MDM can configure OS/browser with a specific encrypted DNS server. 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 encrypted DNS server. The OS/Browser can use the configuration profile to use a specific encrypted DNS server. In this case, MDM is not installed on the device.

Provisioning IT-managed devices, BYOD devices with MDM or configuration profile with network-designated DNS server is outside the scope of this document.

Typically, Enterprise networks do not assume that all devices in their network are managed by the IT team or MDM, especially in the quite common BYOD scenario. The endpoint can use the discovered network-designated DNS server to only access DNS names for which the Enterprise network claims authority and use another public DNS server for global domains or use the discovered network-designated DNS server to access both private domains and global domains.

The scope of NetworkDNSOnly key is restricted to unmanaged BYOD devices without a configuration profile on explicitly trusted networks. In this use case, the user has authorized the client to override local DNS settings for a specific network. It is similar to the way users explicitly disable VPN connection in specific networks and VPN connection is enabled by default in other networks for privacy. The unmanaged BYOD devices use mutual authentication of the client and the enterprise network. The client is typically authenticated with their user credentials (e.g., username and password). The network is typically authenticated with a certificate (e.g., PEAP-MSCHAPv2 [PEAP]) or a mutually-authenticated key exchange which is well-defended from offline attacks (e.g., EAP-pwd [RFC8146], EAP-PSK [RFC4764]). Importantly, WPA-PSK and WPA2-PSK are not well-defended from offline attacks and MUST NOT be used in conjunction with NetworkDNSOnly set to True.

Note: 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. 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 pass code 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.

5. An Example

The following example shows how the JSON keys defined in this document can be used:

```
{
  "identifier": "cafe.example.com.",
  "expires": "2020-05-23T06:00:00Z",
  "prefixes": ["2001:db8:1::/48", "2001:db8:4::/48"],
  "NetworkDNSOnly": True,
  "ErrorNetworkDNSOnly": "example.com malware blocking service"
}
```

The JSON keys "identifier", "expires", and "prefixes" are defined in [RFC8801].

6. Security Considerations

The content of NetworkDNSOnly and ErrorSplitDNSBlocked may be passed to another (DNS) program for processing. As with any network input, the content SHOULD be considered untrusted and handled accordingly. The security considerations discussed in Section 3 and Section 4 need to be considered to restrict the scope of NetworkDNSOnly and ErrorSplitDNSBlocked PvD Keys to explicitly trusted networks. The NetworkDNSOnly and ErrorSplitDNSBlocked PvD Keys assigned by an anonymous or unknown network (e.g., coffee shops) MUST be ignored by the client.

7. IANA Considerations

IANA is requested to add NetworkDNSOnly and ErrorSplitDNSBlocked PvD Keys to the Additional Information PvD Keys registry (https://www.iana.org/assignments/pvds/pvds.xhtml).

8. Acknowledgements

Thanks to Mohamed Boucadair, Jim Reid, Ben Schwartz, Tommy Pauly, Paul Vixie, Ben Schwartz, and Vinny Parla for the discussion and comments.

9. References

9.1. Normative References

[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>.

[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>.

[RFC8801] Pfister, P., Vyncke, É., Pauly, T., Schinazi, D., and W. Shao, "Discovering Provisioning Domain Names and Data", RFC 8801, DOI 10.17487/RFC8801, July 2020, <https://www.rfc-editor.org/info/rfc8801>.

9.2. 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>.

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

[Dragonblood] The Unicode Consortium, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd", <https://papers.mathyvanhoef.com/dragonblood.pdf>.

[Evil-Twin] The Unicode Consortium, "Evil twin (wireless networks)", <https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)>.

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

[I-D.ietf-add-ddr] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-ddr-02, 8

July 2021, <https://www.ietf.org/archive/id/draft-ietf-add-ddr-02.txt>.

[I-D.ietf-add-dnr] Boucadair, M., Reddy, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", Work in Progress, Internet-Draft, draft-ietf-add-dnr-02, 17 May 2021, <https://www.ietf.org/archive/id/draft-ietf-add-dnr-02.txt>.

[Krack] The Unicode Consortium, "Key Reinstallation Attacks", 2017, <https://www.krackattacks.com/>.

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

[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>.

[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>.

[RFC7556] Anipko, D., Ed., "Multiple Provisioning Domain Architecture", RFC 7556, DOI 10.17487/RFC7556, June 2015, <https://www.rfc-editor.org/info/rfc7556>.

[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>.

[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>.

[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>.

[RFC8738] Shoemaker, R.B., "Automated Certificate Management Environment (ACME) IP Identifier Validation Extension", RFC 8738, DOI 10.17487/RFC8738, February 2020, <https://www.rfc-editor.org/info/rfc8738>.

[RFC8914] Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D. Lawrence, "Extended DNS Errors", RFC 8914, DOI 10.17487/RFC8914, October 2020, <https://www.rfc-editor.org/info/rfc8914>.

[win10s] Microsoft, "Windows 10 in S mode", <https://www.microsoft.com/en-us/windows/s-mode>.

Authors' Addresses

Tirumaleswar Reddy
Akamai
Embassy Golf Link Business Park
Bangalore 560071
Karnataka
India

Email: kondtir@gmail.com

Dan Wing
Citrix Systems, Inc.
4988 Great America Pkwy
Santa Clara, CA 95054
United States of America

Email: danwing@gmail.com

Kevin Smith
Vodafone Group
One Kingdom Street
London
United Kingdom

Email: kevin.smith@vodafone.com