ADD
Internet-Draft
Intended status: Standards Track
Expires: September 29, 2021

T. Reddy
McAfee
D. Wing
Citrix

March 28, 2021

Split-Horizon DNS Configuration in Enterprise Networks
draft-reddy-add-enterprise-split-dns-02

Abstract

When split-horizon DNS is deployed by an enterprise, certain enterprise domains are only resolvable by querying the network-designated DNS server. DNS clients which use DNS servers not provided by the network need to route those DNS domain queries to the network-designated DNS server. This document informs DNS clients of split-horizon DNS, their DNS domains, and is compatible with encrypted DNS.

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). With the advent of DoT and DoH, such network blocking is more difficult, but the endpoint is unable to (properly) resolve split-horizon DNS domains which must query the network-designated DNS server.

[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. 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).

This document specifies a mechanism to indicate which DNS zones are used for split-horizon DNS. DNS clients can discover and authenticate encrypted DNS servers provided by the Enterprise network, for example using the techniques proposed in [I-D.ietf-add-

dnr] and [I-D.ietf-add-ddr]. Discovery of encrypted DNS server for roaming enterprise endpoints is discussed in [I-D.btw-add-ipsecme-ike] (see Section 8).

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 one PvD Key:

The SplitDNSAllowed PvD Key: which determines if the Enterprise network allows split-horizon DNS.

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. Scope of the Document

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 the Split DNS configuration 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 this document is restricted to unmanaged BYOD devices without a configuration profile and split DNS configuration 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 typically use the credentials (user name and password) provided by the IT admin to mutually authenticate to the Enterprise WLAN Access Point (e.g., PEAP-MSCHAPv2 [PEAP], EAP-pwd [RFC8146], EAP-PSK [RFC4764]).

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.

4. Split DNS

[RFC2826] "does not preclude private networks from operating their own private name spaces" but notes that if private networks "wish to make use of names uniquely defined for the global Internet, they have to fetch that information from the global DNS naming hierarchy".

There are various DNS deployments outside of the global DNS, including "split horizon" deployments and DNS usages on private (or virtual private) networks. In a split horizon, an authoritative server gives different responses to queries from the Internet than they do to network-designated DNS servers; while some deployments differentiate internal queries from public queries by the source IP address, the concerns in Section 3.1.1 of [RFC6950] relating to trusting source IP addresses apply to such deployments.

When the internal address space range is private [RFC1918], this makes it both easier for the server to discriminate public from private and harder for public entities to impersonate nodes in the private network. The use cases that motivate split-horizon DNS typically involve restricting access to some network services -- intranet resources such as internal web sites, development servers, or directories, for example -- while preserving the ease of use offered by domain names for internal users.

An Enterprise can require one or more DNS domains to be resolved via network-designated DNS servers. This can be a special domain, such as "corp.example.com" for an enterprise that is publicly known to use "example.com". In this case, the endpoint needs to be informed what the private domain names are and what the IP addresses of the network-designated DNS servers are. An Enterprise can also run a different version of its global domain on its internal network. In that case, the client is instructed to send DNS queries for the enterprise public domain (e.g., "example.com") to the network-designated DNS servers. A configuration for this deployment scenario is referred to as a Split DNS configuration.

The PvD RA option defined in [RFC8801] SHOULD set the H-flag to indicate that Additional Information is available. This Additional Information JSON object SHOULD include both the "dnsZones" and "SplitDNSAllowed" keys to define the DNS domains for which the Enterprise network claims authority and to indicate if the Enterprise network allows split-horizon DNS.

5. PvD dnsZones

As discussed in Section 4, the Enterprise internal resources tend to have private DNS names. An enterprise can also run a different version of its global domain on its internal network, and require the use of network-designated DNS servers to get resolved.

The PvD Key dnsZones is defined in [RFC8801]. The PvD Key dnsZones adds support for DNS domains for which the Enterprise network claims authority. The private domains specified in the dnsZones key are intended to be resolved using network-designated DNS servers. The private domains in dnsZones are only reachable by devices authenticated or attached to the Enterprise network. The global domains specified in the dnsZones key have a different version in the internal network. DNS resolution for other domains remains unchanged.

The dnsZones PvD Key conveys the specified DNS domains that need to be resolved using an network-designated DNS server. The DNS root zone (".") MUST be ignored if it appears in dnsZones. Other generic or global domains, such as Top-Level Domains (TLDs), similarly MUST be ignored if they appear in dnsZones.

For each dnsZones entry, the client can use the network-designated DNS servers to resolve the listed domains and its subdomains. Other domain names may be resolved using some other DNS servers that are configured independently. For example, if the dnsZones key specifies "example.test", then "example.test", "www.example.test", and "mail.eng.example.test" can be resolved using the network-designated DNS resolver(s), but "otherexample.test" and "ple.test" can be resolved using the system's public resolver(s).

6. PvD SplitDNSAllowed and ErrorSplitDNSBlocked Keys

If an Enterprise network restricts all the DNS queries to be sent to the network-designated DNS server, SplitDNSAllowed will be set to false. If SplitDNSAllowed is set to false, it implies the network will try to block DNS queries to DNS servers not provided by the network and the ErrorSplitDNSBlocked key MUST contain a human-friendly description for this block. This information is intended for human consumption (not automated parsing).

Split DNS configurations may be preferable to sending all DNS queries to an network-designated DNS server in some deployments. This allows an endpoint to only send DNS queries for the enterprise to the network-designated DNS servers. The Enterprise remains unaware of all non-enterprise (DNS) activity of the user. It also allows the network-designated DNS servers to only be configured for the

enterprise DNS domains, which removes the legal and technical responsibility of the enterprise to resolve every DNS domain potentially asked for by the endpoints.

The SplitDNSAllowed key value set to false is a internal security policy expression by the operator of the network but is not a policy prescription to the endpoints to disable use of DNS servers not provided by the network. If SplitDNSAllowed is set to false, the client MUST NOT trust the SplitDNSAllowed key in case of connecting to unknown or untrusted networks (e.g., coffee shops or hotel networks). Most importantly, the endpoint can choose to use a alternate network to resolve the global domain names.

7. 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"],
  "SplitDNSAllowed": True,
   "dnsZones:": ["city.other.test", "example.com"]
}
```

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

8. Roaming Enterprise Users

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 encrypted server hosted by the Enterprise network can be securely discovered by the endpoint using the ENCDNS_IP*_* IKEv2 Configuration Payload Attribute Types defined in [I-D.btw-add-ipsecme-ike]. For split-tunnel VPN configurations, the endpoint uses the discovered encrypted DNS server to resolve domain names for which the Enterprise network claims authority. For non-split-tunnel VPN configurations, the endpoint uses the discovered encrypted DNS server to resolve both global and private domain names.

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

9. Upstream Encryption

If an Enterprise network is using a local encrypted DNS server configured as a Forwarding DNS server [RFC8499] relying upon the upstream resolver (e.g., at an ISP) to perform recursive DNS lookups, DNS messages exchanged between the local encrypted DNS server and the recursive resolver MUST be encrypted.

If the Enterprise network is using the local encrypted DNS 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].

10. Security Considerations

Clients may want to preconfigure global domains for TLDs and Second-Level Domains (SLDs) to prevent malicious DNS redirections for well-known domains. This prevents users from unknowingly giving DNS queries to third parties. This is even more important if those well-known domains are not deploying DNSSEC, as the Enterprise network could then even modify the DNS answers without detection. It is similar to the mechanism discussed in Section 8 of [RFC8598].

The content of dnsZones and SplitDNSAllowed may be passed to another (DNS) program for processing. As with any network input, the content SHOULD be considered untrusted and handled accordingly. The split DNS configuration assigned by an anonymous or unknown network (e.g., coffee shops) MUST be ignored by the client.

To comply with [RFC2826] the split-horizon DNS zone must either not exist in the global DNS hierarchy or must be authoritatively delegated to the split-horizon DNS server to answer. The client can use the mechanism described in [I-D.ietf-add-dnr] to discover the network-designated resolvers. To determine if the network-designated encrypted resolvers are authoritative over the domains in DnsZones, the client performs the following steps for each domain in DnsZones:

1. The client sends an NS query for the domain in DnsZones. This query MUST only be sent over encrypted DNS session to a public resolver that is configured independently or to a network-designated resolver whose response will be validated using DNSSEC as described in [RFC6698].

2. The client checks that the NS RRset matches, or is a subdomain of, any one of the ADN of the discovered network-designated encrypted DNS resolvers.

   A. If the match fails, the client determines the network is not authoritative for the indicated domain. It might log an error, reject the network entirely (because the network lied about its authority over a domain) or other action.

   B. If the match succeeds, the client can then establish a secure connection to that network-designated resolver and validate its certificate.

      + If the server certificate does not validate and a secure connection cannot be established to the network designated resolver, the client can action as discussed in step 3 (A).

      + If the server certificate validation is successful and a secure connection is established, the client can subsequently resolve the domains in that subtree using the network-designated resolver.

3. As an exception to this rule, the client need not perform the above validation for domains reserved for special use [RFC6761] or [RFC6762] such as ".home.arpa" or ".local".

For example, if in an network the private domain names are defined under "internal.corp1.example.com". The DnsZones PvD Key would indicate that "*.internal.corp1.example.com" are private domain names. The client can trigger a NS query of ""internal.corp1.example.com" and the NS RRset returns that the nameserver is "ns1.corp2.example.com". The client would then connect to the network-designated encrypted resolver whose name is "ns1.corp2.example.com", authenticate it using server certificate validation in TLS handshake, and use it for resolving the domains in the subtree of "*.internal.corp1.example.com".

11. IANA Considerations

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

12. Acknowledgements

Thanks to Mohamed Boucadair, Jim Reid, Ben Schwartz, Tommy Pauly, Paul Vixie and Vinny Parla for the discussion and comments. The authors would like to give special thanks to Ben Schwartz for his help.

13. References

13.1. Normative References

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[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>.

[RFC2826] Internet Architecture Board, "IAB Technical Comment on the Unique DNS Root", RFC 2826, DOI 10.17487/RFC2826, May 2000, <https://www.rfc-editor.org/info/rfc2826>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/info/rfc6761>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[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>.

[RFC8801] Pfister, P., Vyncke, E., 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>.

13.2. 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>.

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

[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-01 (work in progress), September 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-02 (work in progress), November 2020.

[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>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[RFC6950] Peterson, J., Kolkman, O., Tschofenig, H., and B. Aboba, "Architectural Considerations on Application Features in the DNS", RFC 6950, DOI 10.17487/RFC6950, October 2013, <https://www.rfc-editor.org/info/rfc6950>.

[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>.

[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>.

[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>.

[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.
4988 Great America Pkwy
Santa Clara, CA 95054
USA

Email: danwing@gmail.com