HTTPBIS
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2015

W. Chow
Mobolize
S. Mishra
Verizon Communications
J. McEachern, Ed.
ATIS

October 27, 2014

Web Proxy Description (WPD) Proxy Discovery
draft-chow-httpbis-proxy-discovery-00

Abstract

This document proposes mechanisms for applications to discover web proxy description files across different network configurations that are complementary to but not reliant upon an external network service or function, such as DHCP or DNS.

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 http://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 April 30, 2015.

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

2.1. Scope of the document

[I-D.nottingham-web-proxy-desc] proposes a web proxy description ("WPD") format and use of well-known URI to download it, but it does not specify a mechanism to identify the authority for the URL of the WPD.

This document proposes a process to bootstrap the WPD process, and outlines mechanisms to locate the authority for the WPD file, and how to validate that authority.

The mechanisms specified in this document leverage HTTP to enable a wide variety of user agents to discover a WPD without reliance on extensions being implemented in another protocol or external network service, such as DNS or DHCP. This approach also allows the WPD to be automatically discovered for a zero configuration setup.

2.2. Use cases

The mechanisms in this document were designed to enable the following use cases:

1. Support secure and private access to a proxy on a public WiFi hotspot.

2. Support a mobile device accessing multiple networks with different proxies. The mobile device must be able to access the correct network proxy, and to change proxies as it switches between WiFi and cellular, or between operator networks.

3. Support proxies operating in different locations, possibly in a cooperative manner. The proxies could be in a private network, in a service provider network, or in the cloud, and could be limited to a specific service domain or a specific access technology.

4. Support proxies deployed on a corporate or home network.

5. Allow an app or content provider to have its own proxy.

The mechanisms proposed in this document are designed to meet the following goals:

1. Enable wide scale support across many network types, including, but not limited to, wireless, satellite, enterprise and private networks.

2. Enable applications to discover a proxy without relying on support from lower software layers or external network services, such as DNS or DHCP.

3. Simplify the process for a user (or user agent) to use a proxy, while still providing robust security.

4. Enable both automatic and manual configuration, depending on the user and network requirements.

5. Enable dynamic WPDs (i.e., different WPDs for different networks).

3. Proxy locations

The location of a proxy will influence the characteristics of a proxy and how it is used. This document considers the following proxy locations:

Internet/Cloud: Proxies that are based in the cloud can be owned and managed by 3rd parties, independent of the service provider or end user. Although these proxies are owned by 3rd parties, they can be invoked by the user, the network operator, or by application providers. Over time, the party accessing the proxy can change, depending on the configuration. This makes cloud based proxies useful for 3rd party optimization services that can be used for a range of applications, or for application specific optimization. Examples include browser-specific compression services, and Content Distribution Networks (CDN).

Service provider: Proxies can also be owned and operated by the network service provider, and can be used to manage and/or optimize traffic carried over the specific network. The proxy can be physically located in the service provider core network, the access network, or even on the customer premise. These proxies can be used to provide services such as privacy, content filtering or security services such as malware detection. Service provider proxies are also used to enhance capacity through network optimization or to increase effective network speed and improve page load times. These proxies can also be used to apply network policy and track billing, including zero rating for selected applications. Examples of service provider proxies include those deployed in the MNO packet core, ISP central office, public hotspots, or inflight WiFi.

Private: Proxies can be owned or controlled by the device owner, and deployed in a controlled network environment. These proxies can be used to provide content filtering and security services. They can also provide various services to enhance the effective speed or decrease bandwidth usage. Examples of private proxies include corporate proxies and firewalls, MiFi devices, home routers and localhost.

4. WPD Authorities

A proxy's location determines the authority that is used to discover the WPD that describes it. The WPD authority may be distinct from the proxies described in the WPD, so the WPD Server is considered a logically distinct entity from the proxy. This document describes several possible WPD authorities, and provides a mechanism to identify and authenticate each one in the following sections.

4.1. Pre-defined authority

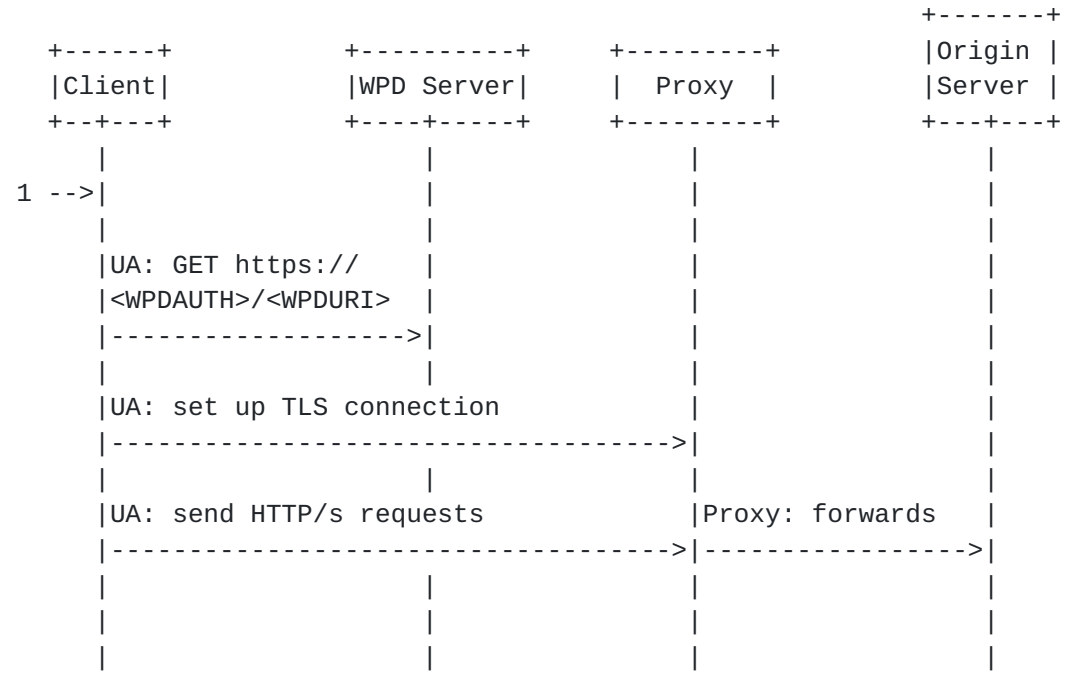
In this case, the authority is pre-configured into the device or application, and is used by the UA to probe for the appropriate proxy. This mechanism would be limited to instances where the proxy

provider is explicitly authorized to control the configuration of the device or application. Examples would include "locked" mobile phones, PCs owned by the enterprise/school, or a browser associated with a cloud-based compression service.

Mechanism: The pre-configured authority is seeded into the device or an app beforehand through an out-of-band (OOB) mechanism, so that it is available at the time that the WPD is requested. The OOB mechanism can often be static, such as being hard-coded into the UA, but this approach is complementary to dynamic mechanisms, such as those leveraging an external network service, such as a PDP context for mobile devices or LDAP for PCs.

Proxy scope: The scope of the UA determines the scope of traffic affected by the WPD. If the UA has device wide administrative privileges, it can apply the WPD configuration to all traffic on the device. If the UA is an application without administrative privileges, it can only apply the WPD configuration to the traffic for that application.

Sequence diagram:



1: OOB-defined WPD authority

4.2. Network authority

In this case, the UA probes the network for the WPD, allowing the current network to advertise its web proxies, such as a privacy proxy on a public WiFi hotspot, optimization proxy on a MiFi device, or a content filtering proxy on a corporate network. This approach allows the proxy configuration to be customized for the current network, and is dynamically updated when the user device attaches to a different network.

Mechanism: The network authority for the WPD request is identified by the UA sending a request to the WPD URI with the "http" scheme to any authority, so that the network can respond with a redirect to the authority where its WPD can be found. The redirect MUST specify a URL with the "https" scheme, to ensure that the network authority can be securely authenticated by the UA.

Proxy scope: The scope of the WPD is limited to the current network. Proxy information can be cached, but a change in the network MUST clear the proxies it configured. The scope of the UA determines the scope of traffic affected by the WPD. If the UA has device wide administrative privileges, it can apply the WPD configuration to all traffic on the device. If the UA is an application without administrative privileges, it can only apply the WPD configuration to the traffic for that application.

Sequence diagram:

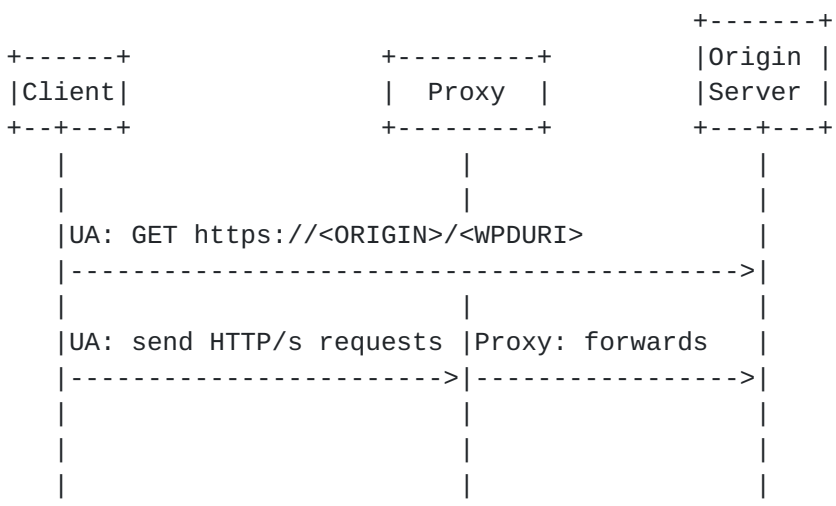
4.3. Origin authority

In this case, the UA probes for the WPD using the origin server as the authority for the WPD URI. This allows the content provider to specify a proxy for its content. The scope of the WPD from the origin server is inherently limited to the traffic to/from that origin and the UA MUST enforce this.

Mechanism: The WPD from the origin server MUST be requested using the "https" scheme, to ensure that it is coming from that origin authority. This ensures it bypasses all intermediaries and avoids overlapping with the other network authority mechanism.

Proxy scope: The scope of the WPD from the origin server MUST be limited to the traffic to that origin server.

Sequence diagram:



5. IANA Considerations

This document does not contain any considerations for IANA.

6. Security Considerations

This document specifies mechanisms to locate the authority for the WPD across different applications and network types, so it is important that these mechanisms allow the user agent to securely authenticate the WPD. Therefore, this document proposes that WPD requests SHOULD use the "https" scheme whenever possible to ensure strong authentication for the WPD server for each of the mechanisms. However, certain network scenarios may provide strong authentication of the WPD authority through other means, such as through operational security on a private network, so this document does not preclude those alternatives.

The proxy can observe unencryped traffic that traverses it, but it MUST NOT alter the end-to-end encryption for "https" requests. Also, the scope of the WPD and the traffic it affects is enforced by the user agent. In the case where the WPD is advertised by the content provider, the user agent MUST ensure that the scope of the network traffic is limited to the authority specified when requesting that WPD. This ensures that an origin server can only direct requests to proxies for its own traffic and it cannot reroute traffic for other origins.

7. Acknowledgments

The editor and authors thank Dan Druta, Vijay K. Gurbani, David Lerner, Peter Lepska, John Border and Chi-Jiun Su for feedback and suggestions.

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[I-D.nottingham-web-proxy-desc] Nottingham, M., "The Web Proxy Description Format", draft-nottingham-web-proxy-desc-01 (work in progress), October 2014.

[I-D.ietf-httpbis-http2] Belshe, M., Peon, R., and M. Thomson, "Hypertext Transfer Protocol version 2", draft-ietf-httpbis-http2-14 (work in progress), July 2014.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, April 2010.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, July 2014.

Authors' Addresses

William Chow
Mobolize

Email: wchow@mobolize.com

Sanjay Mishra
Verizon Communications

Email: sanjay.mishra@verizon.com

James McEachern (editor)
ATIS

Email: jmceachern@atis.org