Communicating Proxy Configurations in Provisioning Domains

draft-ietf-intarea-proxy-config-pvd-02

Tommy Pauly & Dragana Damjanovic
INTAREA
IETF 121, November 2024, Dublin

Protocol Recap

Use the PvD (Provisioning Domain) JSON format from RFC 8801 to add support for proxies:

- Ask a known proxy about other proxy protocols it supports — upgrade to secure MASQUE protocols, etc.
- Ask a known proxy about the configuration it has (which domains are allowed, etc)
- Learn about proxies offered by a network PvD

Updates in -02

- Editorial fixes
  - Describe upgrading from insecure to secure proxies
  - Make JSON key names more consistent
- Improve split routing
  - Add match/exclude IP subnets
  - Allow for exact vs suffix matching for domains
  - Allow port matching
  - Allow for exclusions without specific match domains

Feature parity

PvD configs vs PAC files

Many of the recent changes and open PRs are related to replacing PAC

In order to replace WPAD/PAC, we need to analyze which features of PAC have parity in PvDs

Not every feature needs to be supported, but we should make a conscious decision about which ones will be carried over

Feature parity

PvD configs vs PAC files

	PAC files	PvD configs
Proxy types	👍 SOCKS/HTTP/HTTPS	👍👍 More new protocols!
Split routing based on hosts[1]	👍 DIRECT/PROXY, based on URL input	👍 Match and exclude domains / IP subnets
Split routing based on ports[1]	👍 DIRECT/PROXY, based on URL input	👍 Match ports
Split routing based on URL scheme[1]	👍 DIRECT/PROXY, based on URL input	👎 Is this relevant for secure proxies?
Time-specific configurations	👍 Date / time JavaScript functions	👍 Expiry time on PvD config
Fallback proxies	👍 Returns list of proxies in order	👍👎 ? Can have multiple matching proxies, but no strict ordering. Less prescriptive than PAC.

1. Note that matching based on URL paths/query strings is generally no longer supported

Authentication

PR #261

Some proxies require authentication. Clients might find it useful to know authentication info ahead of time.

- One option is to include a hint about the HTTP auth schemes that the proxy will challenge for, if relevant
  - Could also include authentication hints about SOCKS, TLS, etc

What should we do with auth?

1. Nothing; we shouldn't be trying to specify that with proxy configs.
2. Something somewhere else; write another document for authentication keys.
3. Something here; this is part of the proxy configuration, and it belongs here.

ECH (TLS Encrypted Client Hello)

PR #257

We added ALPN info to the config (which can go in SVCB records), partly because this helps for connecting to proxies by IP address

This PR suggests adding ECH keys to the config too

Is there a use case for this? Generally ECH will protect the SNI, which wouldn't be present in an IP-only proxy connection

ECH could contain other information besides SNI

This could be useful even when connecting to proxies by name if the client cannot or will not make DNS SVCB queries for the proxy name

Very long lists

PR #266

Lists of match/exclude domains and IPs could get very long

- Enterprise configurations often can include hundreds or thousands of entries

Should the document provide any guidance or commentary on how to handle this?

- Should there be limits on size?
- Do we need guidance to clients on how to process the configuration?
- If this is less prescriptive than PAC, do we need to say anything about processing here?