Communicating Proxy Configurations in Provisioning Domains

draft-pauly-intarea-proxy-config-pvd-02

Tommy Pauly & Dragana Damjanovic
INTAREA
IETF 119, March 2024, Brisbane
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
Related proxy discovery

Allows "upgrade" from legacy proxy types to template-based proxies (CONNECT-UDP, etc)

I also have URLs for UDP and IP proxying
Proxy applicability discovery (split DNS, etc)

A proxy only allows access to certain hosts, or from certain users (not an "open" proxy)

Client → HTTP Proxy → Private Origin

```json
{
    "identifier": "proxy.example.org",
    "expires": "2023-06-24T06:00:00Z",
    "prefixes": [],
    "dnsZones": ["corp.example.com"]
}
```

I only allow access to corp.example.com
Network-provided proxy discovery

Network (ISP, carrier) provides a proxy that can assist in mobility (AT-SSS) or privacy (act as a first-hop Private Relay proxy)
Updated proxy details format
New in -02!

Instead of a flat list of proxies URLs, provide a structured sub-dictionary

Proxy information object contains two keys:

- `protocol`, the name of the proxy protocol
- `proxy`, the location of the proxy; a URL template, or a host:port
Proxy protocol types

Current values in the draft:

- socks5
- http-connect
- https-connect
- connect-udp
- connect-ip
- connect-tcp
Open issues:

- Handling extensibility for new keys — differentiating mandatory vs optional new keys
- Provide hints about which proxies are supported on which HTTP version
  - A server might only support connect-udp over HTTP/3, but not HTTP/2 or HTTP/1.1
- Adding support for exclusion domains for split DNS configurations
  - Should these be moved into the proxy sub-dictionaries?
Relationship with legacy proxy discovery

PAC files and WPAD are common existing techniques
  No support for modern / secure types
  Insecure provisioning
PvD allows taking any proxy that is known (manual configuration, WPAD, etc), and "upgrading" it
Do we need to do anything else here?
Next steps

Please review!

Adopt in INTAREA?

Implementation testing