

Communicating Proxy Configurations in Provisioning Domains

draft-ietf-intarea-proxy-config-pvd-01

Tommy Pauly & Dragana Damjanovic
INTAREA
IETF 120, July 2024, Vancouver

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

Status

Adopted in INTAREA since IETF 119

Published a -01 to proposed changes to main design issues

Let's review

Updates in -01

Communicate supported HTTP versions

Support excluded domains

Explicitly identify mandatory vs optional keys

HTTP versions / ALPNs

Issue #242

Avoid needing to attempt/race different HTTP versions to HTTP-based proxies

Could learn from SVCB DNS records; but this doesn't work for connect-by-address

Could learn from Alt-Svc; but this takes a round trip

Add an `alpn` key

```
"proxies": [  
  {  
    "protocol": "connect-udp",  
    "proxy": "https://p.example.org/masque{?target_host,target_port}",  
    "alpn": ["h3", "h2"]  
  }  
]
```

Exclusion domains

Issue #248

Previously used `dnsZones` to define split DNS configs

This didn't work for excluding domains

Now defines a `matchDomains` list and an `excludedDomains` list

```
"proxies": [  
  {  
    "protocol": "http-connect",  
    "proxy": "proxy.example.org:1234",  
    "matchDomains": ["example.org"],  
    "excludedDomains": ["public.example.org"]  
  }  
]
```

Mandatory vs Optional Keys

Issue #245

Previously, proxy keys were not marked mandatory or optional, to allow different use cases to define ways to use keys

However, new keys for a1pn, etc, need to be called out as optional

Updated IANA registry has a column for "mandatory"

Is this sufficient as a long-term solution? Essentially all new keys will be "optional"

Remaining issues

#249: Should we add information about client authentication to proxies?

#246: Formalize JSON character sets

Should we discuss more about constraints for safely discovering proxies from a network?