Communicating Proxy Configurations in Provisioning Domains

draft-pauly-intarea-proxy-config-pvd-01

Tommy Pauly & Dragana Damjanovic
INTAREA
IETF 118, November 2023, Prague

Updates in -01

Always use the `.well-known/pvd` resource location

> This has a side effect that all proxies on the same host share the same PvD Additional Information

Focus on the use cases for discovering related proxies, and details about proxies

> Network-provided proxies is still possible, but needs further security analysis

Related proxy discovery

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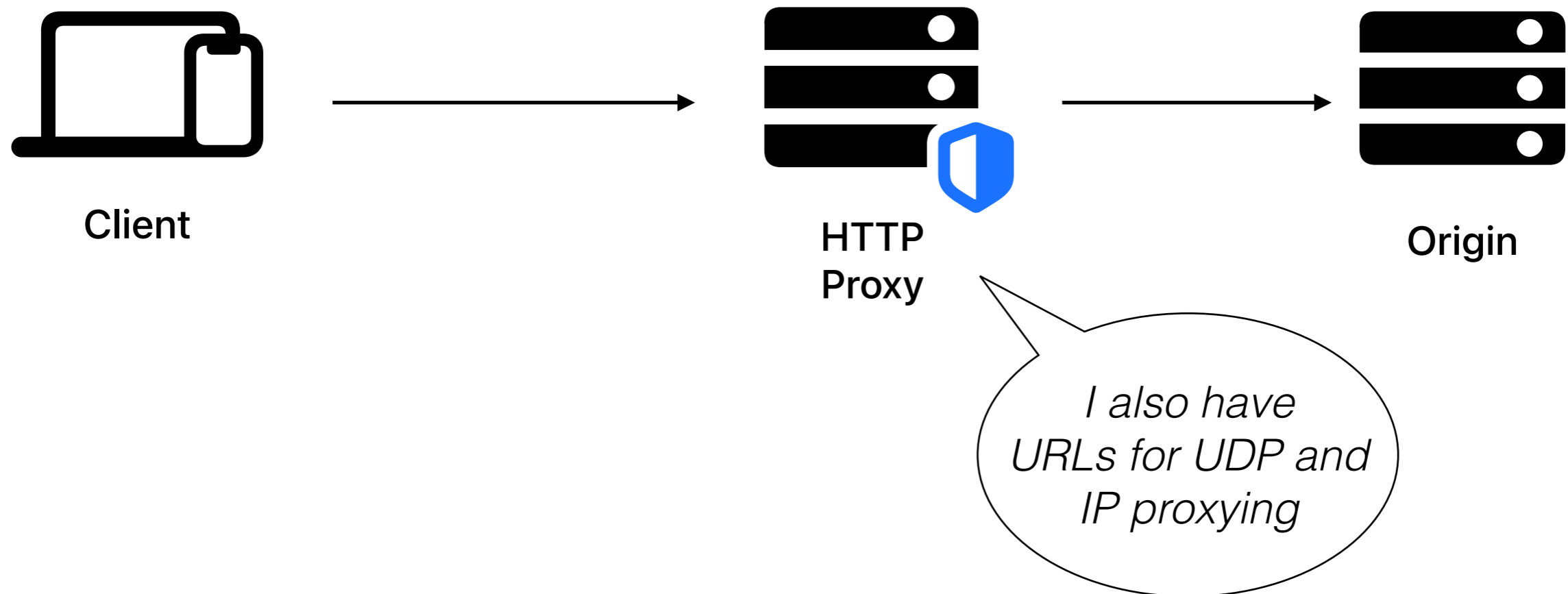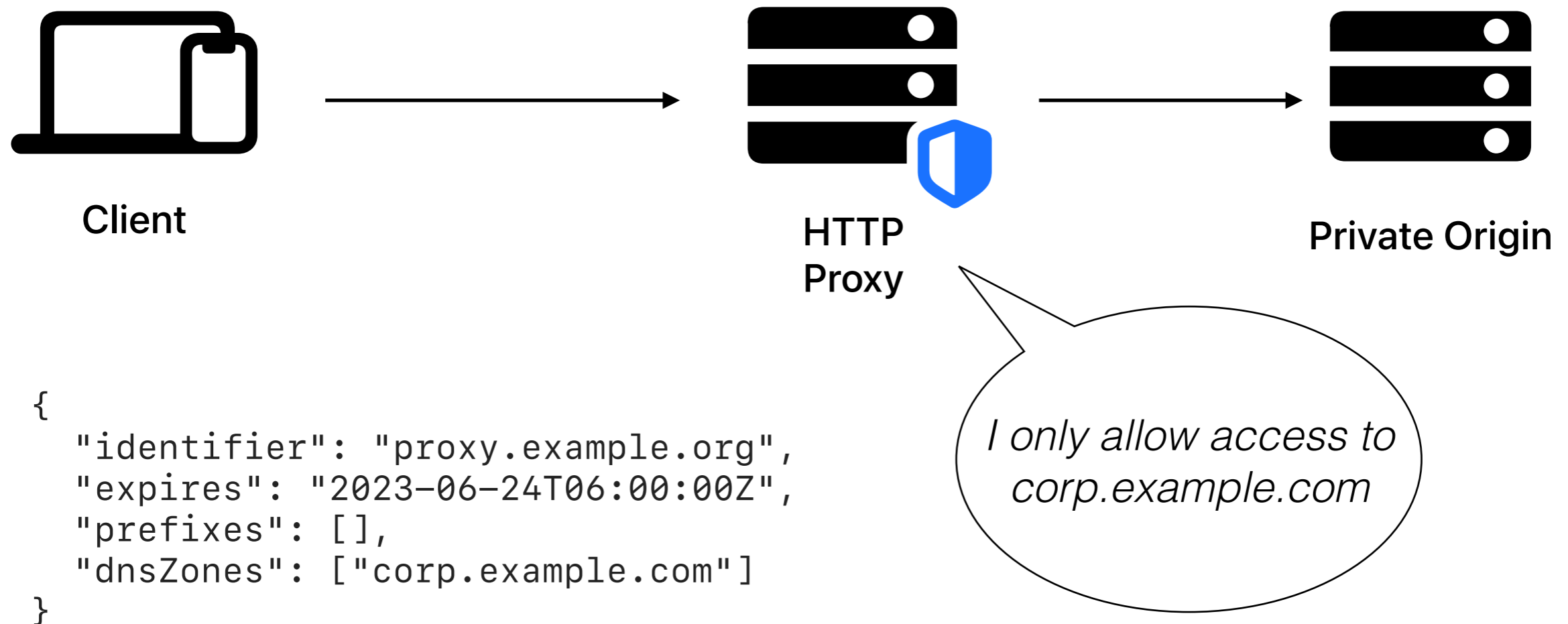
Related proxy discovery

1. Client is configured with a simple proxy name (for HTTP or SOCKS)

2. Client queries the `.well-known/pvd` URL for that name

3. Client parses the JSON to look for a `proxies` array of related proxy URLs

```
{
  "identifier": "proxy.example.org",
  "expires": "2023-06-24T06:00:00Z",
  "prefixes": [],
  "proxies": ["https://proxy.example.org","https://proxy.example.org/
masque{?target_host,target_port}"]
}
```

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**

```
{
  "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)

Client

Origin

MASQUE
Proxy
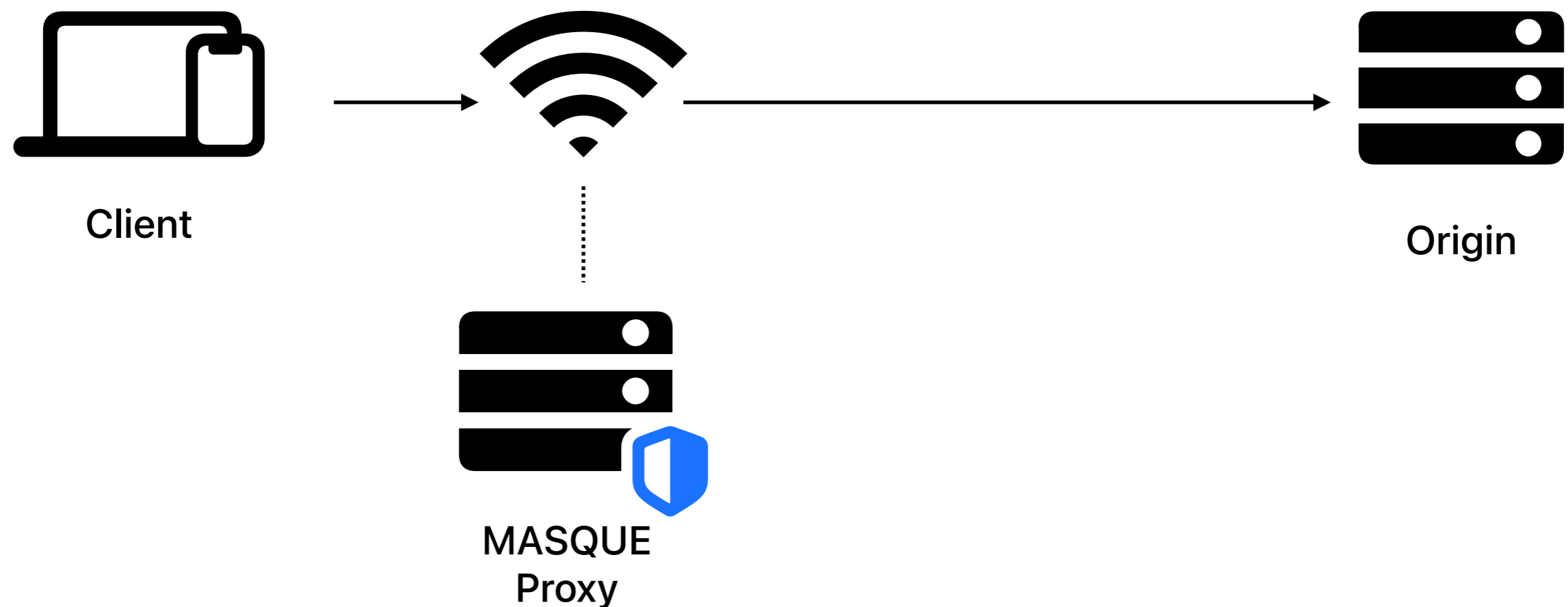
Network-provided proxy discovery

Provides a standard alternative to WPAD and PAC

    We don't want to repeat their problems, though

It might be OK to use a discovered proxy when:

- The client is already going to use a proxy for a particular set of traffic

- This proxy is already on an approved/trusted list

- The proxy is being used in a multi-hop chain of proxies

It might be *not* be OK to use a discovered proxy otherwise...

Open questions

Do we need more formal ways to identify proxy protocols?

Currently relies on URL scheme and template parameters to infer protocols

How should we define behavior for network-discovered proxies?

Should that be a separate document, or part of this one?

Next steps

Please review!

Adopt in INTAREA?

Implementation testing