DNS Configuration for Proxying IP in HTTP

draft-ietf-masque-connect-ip-dns

IETF 121 – Dublin – 2024-11-06

David Schinazi – dschinazi.ietf@gmail.com

This is not DNS-over-MASQUE

We have enough ways to send DNS

This is about configuration – which DNS *resolver* to use

`/etc/resolv.conf`

now with cryptography ✨

Most VPN protocols allow exchanging DNS configuration info

IKEv2 has INTERNAL_IP4_DNS / INTERNAL_IP6_DNS

OpenVPN can also send DNS in-band

Enterprises interested in this to use connect-ip as a drop-in replacement for IPsec

CONNECT-IP Capsules

ADDRESS_ASSIGN / ADDRESS_REQUEST

ROUTE_ADVERTISEMENT

Intentionally punted DNS from RFC 9484 to a future extension

Moar capsules: DNS_ASSIGN / DNS_REQUEST

Each DNS name server has an IP address and a list of internal domains

Also exchange DNS search domains

Also carries request IDs similar to ADDRESS_ASSIGN / ADDRESS_REQUEST

Inspired by IKEv2 (RFC 7296 & RFC 8598 & RFC 9464)

Changed since adoption last month: SVCB

Support DNSo53, DoT, DoQ, DoH, etc

Previous draft had a custom way to exchange these with its own registry

Instead, we now use SVCB alpn parameter, similar to:

RFC 9463 – DHCP and RA Options for the Discovery of Network-designated Resolvers (DNR)

RFC 9464 – IKEv2 Configuration for Encrypted DNS

Bonus: if DoH available, client SHOULD query on the same HTTP connection

Did I get it right?

Example: Full-Tunnel Consumer VPN

```
DNS Configuration = {
  Nameservers = [{
    Service Priority = 1,
    IPv4 Address = [],
    IPv6 Address = [],
    Nameserver Domain = "masque.example",
    Service Parameters = {
      alpn=h2,h3
      dohpath=/dns-query{?dns}
    },
  }],
  Internal Domains = [""],
  Search Domains = [],
}
```

Example: Split-Tunnel Enterprise VPN

```
DNS Configuration = {
  Nameservers = [{
    Service Priority = 1,
    IPv4 Address = [192.0.2.33],
    IPv6 Address = [2001:db8::1],
    Nameserver Domain = "",
    Service Parameters = {},
  }],
  Internal Domains = ["internal.corp.example"],
  Search Domains = [
    "internal.corp.example",
    "corp.example",
  ],
}
```

Next Steps

Plan on implementing soon

Are we missing any features?

Are there DNS sharp edges we should warn against?