DNS Configuration for Proxying IP in HTTP

draft-schinazi-masque-connect-ip-dns

IETF 120 – Vancouver – 2024-07-23

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`

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

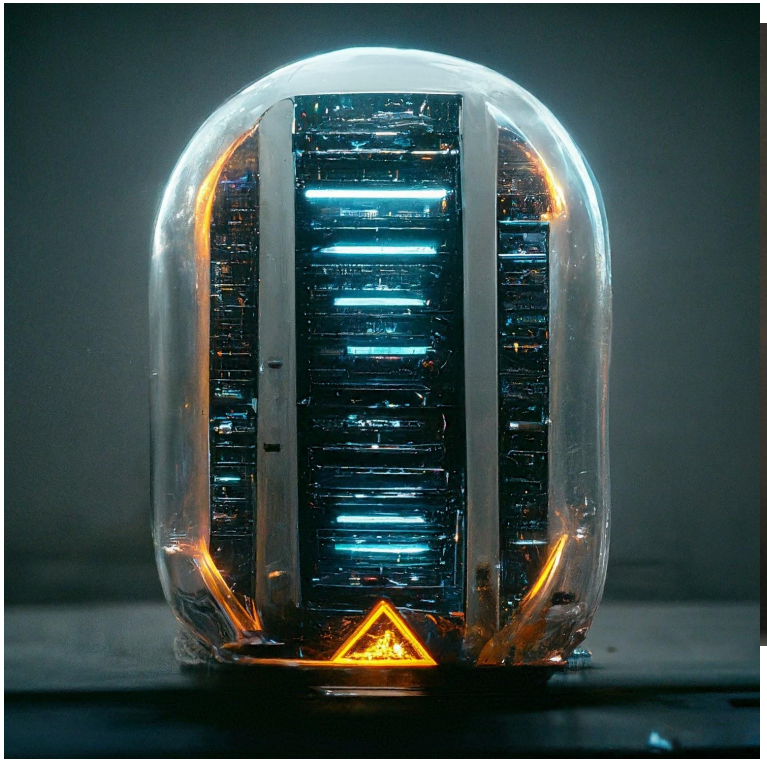
ADDRESS_ASSIGN / ADDRESS_REQUEST

ROUTE_ADVERTISEMENT

Intentionally punted DNS from RFC 9484 to a future extension

Having to exchange DNS out of band makes us sad

Solution: put DNS configuration in a capsule



Rough idea: 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)

It's 2024: we also need to configure which DNS protocol to use

DNSo53, DoT, DoQ, etc

In draft -01, added a "type" varint

Feedback from list: be consistent with ADD / SVCB RR

RFC 9463 – DHCP and RA Options for the Discovery of Network-designated Resolvers (DNR)
RFC 9464 – IKEv2 Configuration for Encrypted DNS

TLDR: use SVCB alpn parameter to convey what DNS protocols a resolver supports

Thoughts?