Network Policy to use Network-designated resolvers

draft-reddy-add-enterprise-policy-01

T. Reddy (Akamai) D.Wing (Citrix) K.Smith (Vodafone)

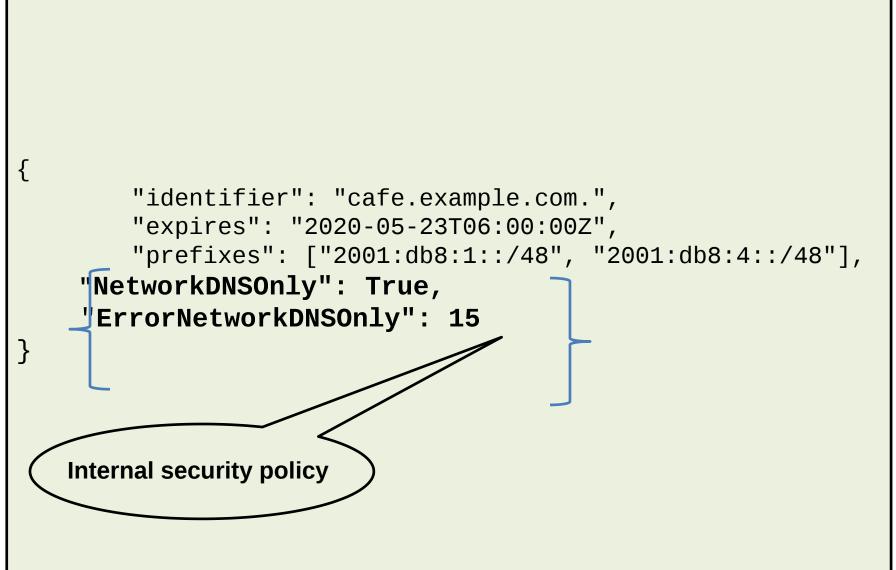
Problem

- Network policy requires using network-signaled resolvers
- Need to inform endpoints of network policy
- Avoids user confusion when accessing non-networksignaled resolvers cause security alerts, client quarantining, or block client entirely

Mechanism

- RFC8801: Discovery of explicit PvD and additional information using Web PvD (HTTP-over-TLS).
 - NetworkDNSOnly: PvD Key indicates network policy allows only using network-signaled DNS servers
 - ErrorNetworkDNSOnly: Extended DNS error code as defined by [RFC8914].

Web PVD example



Scope

- Internal security policy expression by the operator of the network <u>but is not a policy prescription</u> to the endpoints.
- Endpoints can ignore NetworkDNSOnly PvD Key.
- Explicitly trusted networks.
- BYOD without MDM
 - BYOD with a lite-weight host agent only for posture assessment.

draft-reddy-add-enterprise-policy-01

• Comments and suggestions are welcome