RETURN

IETF 93

Ben Schwartz
Justin Uberti

Changes since last time

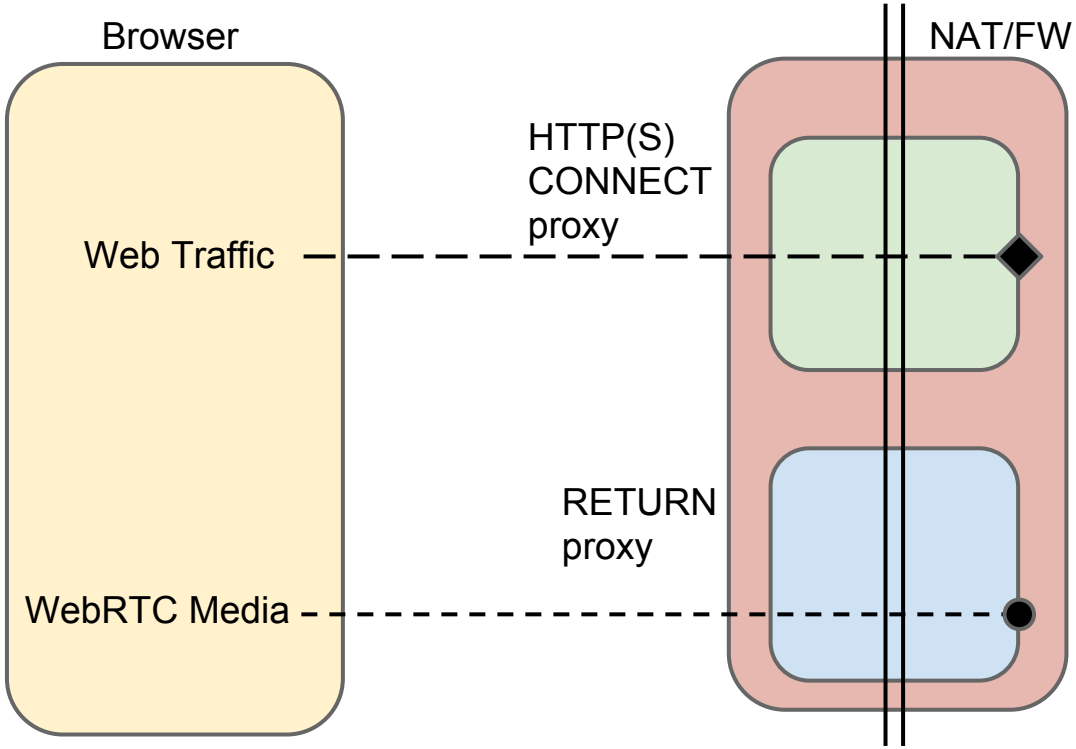
- Adopted as WG draft
- Autodiscovery security considerations

Reminder: Why

RFC 7478, Section 2.3.5.1:

An enterprise ... deploy[s] a TURN server that straddles the boundary between the internal and the external network. … The WebRTC functionality will need to utilize both network specific STUN and TURN resources and STUN and TURN servers provisioned by the web application.

Reminder: How



HTTP proxy port

Candidate | Network edge | HTTP(S) web traffic | TURN encapsulated

Security Considerations (1)

A RETURN proxy can capture, block, and otherwise interfere with all of its clients' WebRTC network activity. ***Therefore, browsers and other WebRTC endpoints MUST NOT use RETURN proxies that are provided by untrusted sources.***

For example, endpoints MUST NOT implement a configuration based on unauthenticated network multicast (e.g. mDNS) unless the endpoint will only be used on networks where all other users are fully trusted to intercept all WebRTC traffic. In contrast, endpoints MAY implement mechanisms to configure RETURN proxies by system-wide policy, which can only be modified by trusted system administrators.

Security Considerations (2)

- Ergo, the autodiscovery mechanisms (mDNS, anycast) defined in draft-ietf-tram-turn-server-discovery-03
  are not appropriate for RETURN
- Perhaps we need to revisit WPAD/.pac