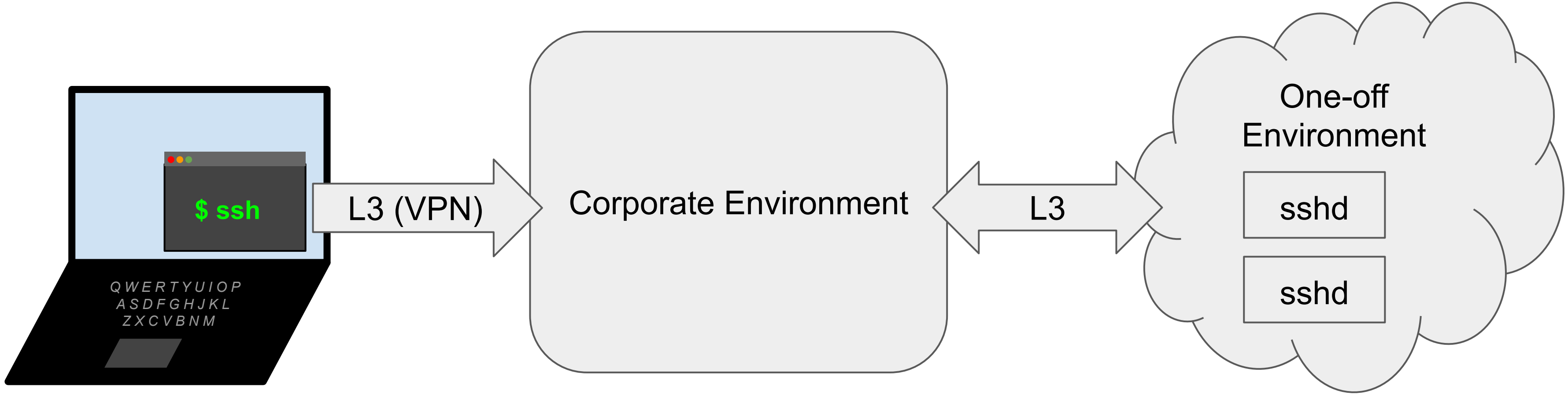
Reverse HTTP: Use Cases and Missing Functionality

Hrant Novikov, Meta

PTTH BoF, IETF 123

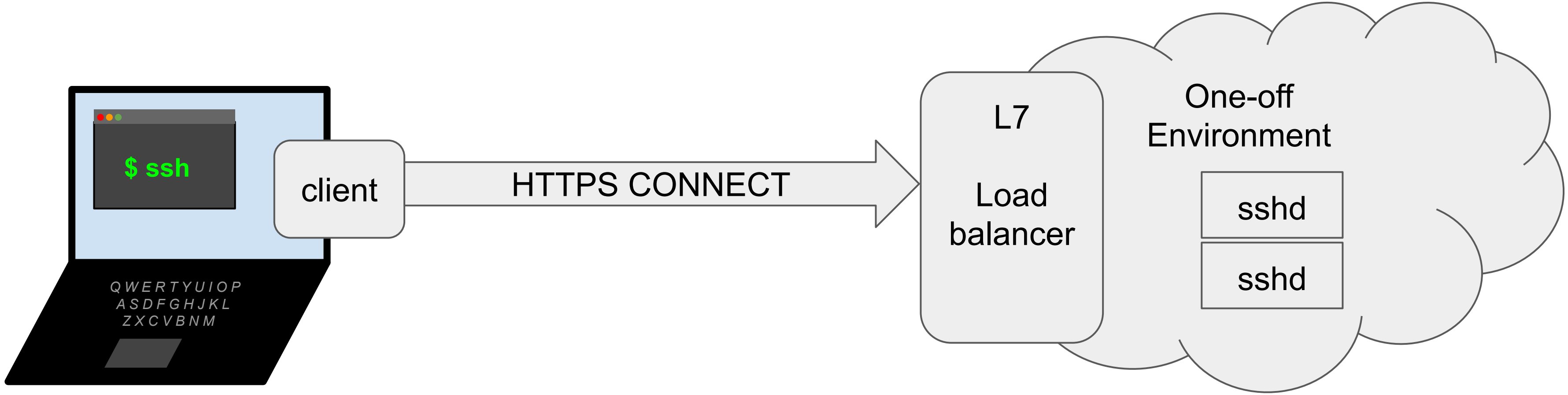
Background

L3 connectivity



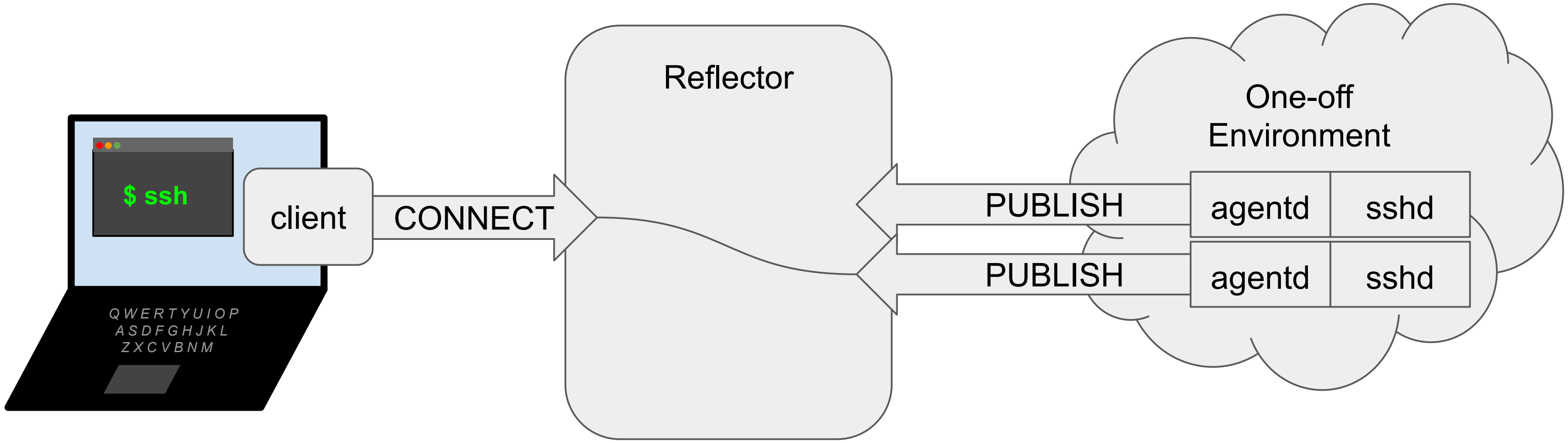
For a variety of reasons we have to have maintain a number of deployments that don't fit into our corporate environment. One typical approach is to allow L3 access into the environment from our corporate environment. This forces remote employees onto VPN.

A layer 7 alternative



A way to remove the burden of having to VPN in is to have an L7 tunnel from a device directly into the target environment. This would force us into maintaining an L7 identity-aware proxy that is open to the internet for each environment.

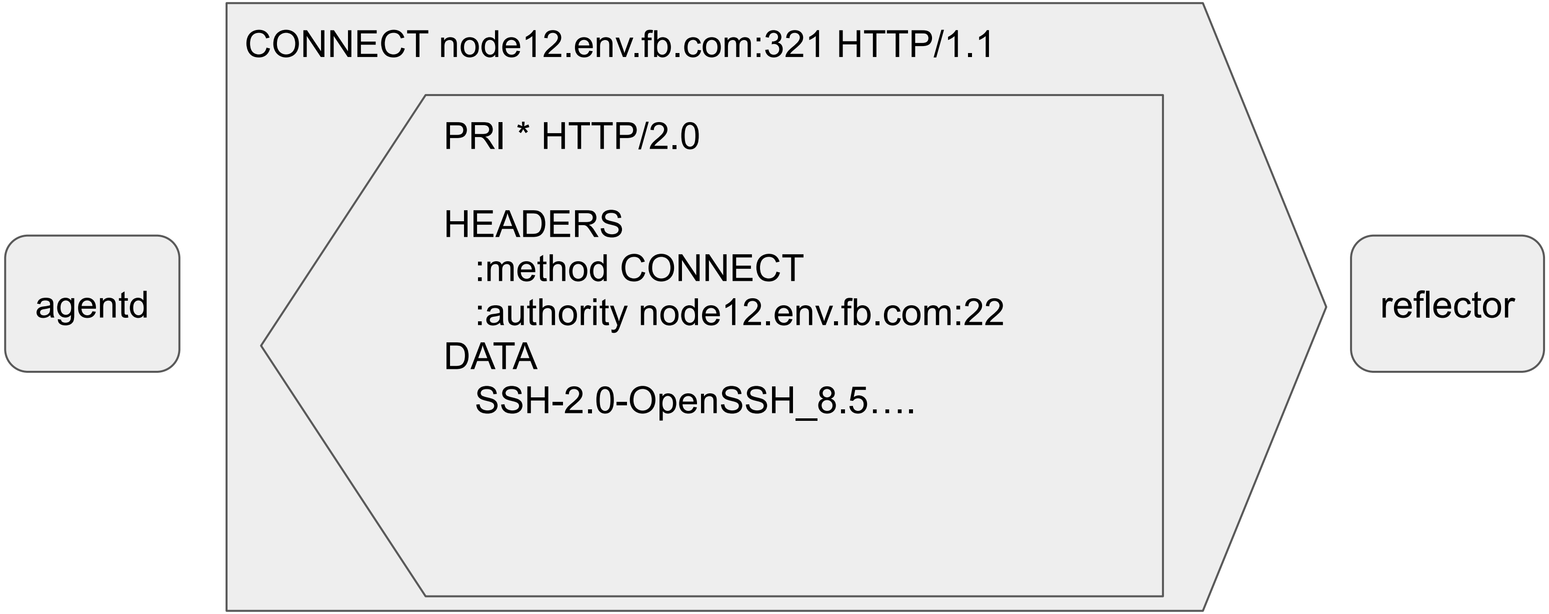
A better layer 7 alternative



An easier to scale (from a management point of view) approach would be to have hidden origins that use an on-node agent to publish resources from behind the NAT.

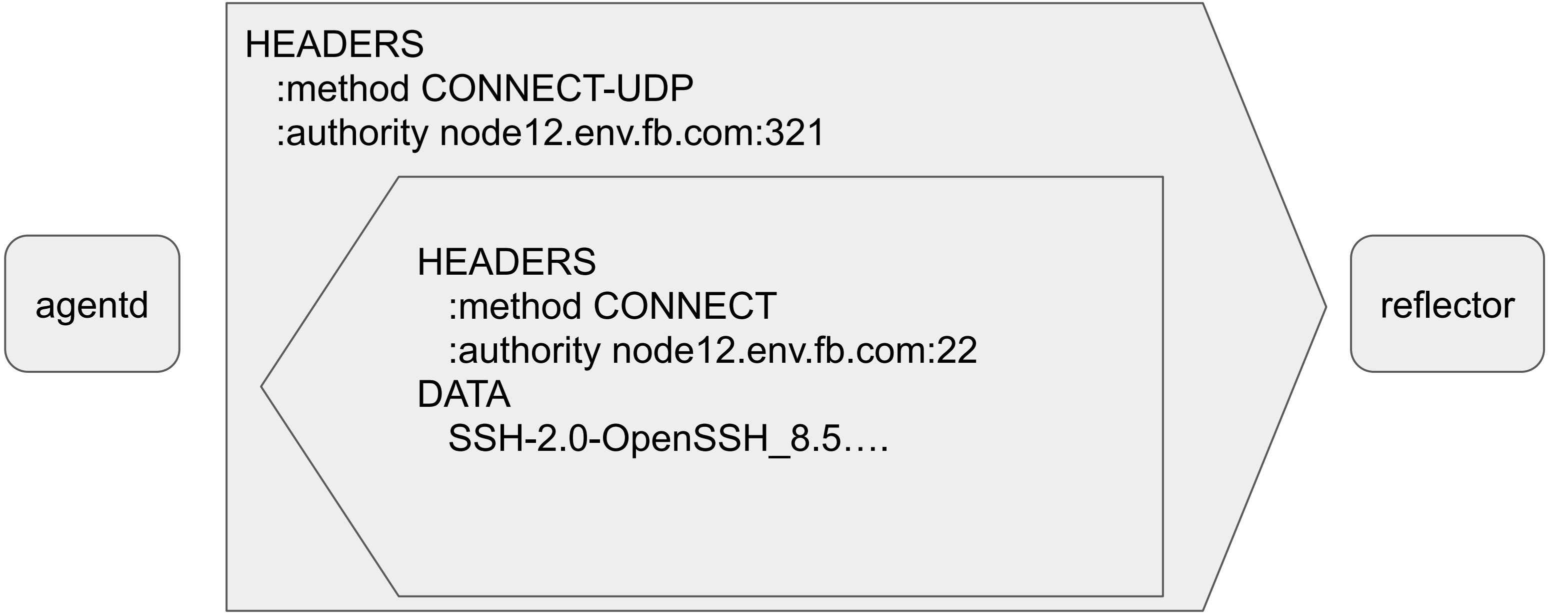
Off-the-shelf approach

What about just H2C in HTTP/*?



Gets us stream connectivity. Multiple layers of flow control and framing to deal with (TCP, inner H/2, outer H/2-3 if not using H/1.1). No native datagram connectivity.

What about HTTP/3 over HTTP/3?



Layering QUIC over QUIC-datagram gets rid of the flow control problem and gives us datagram semantics. Connectivity in non-UDP permitting environments suffers. MTUs suffer from double HTTP/3 headers.

Desired properties for publishing hidden origins

- Minimizes the number of RTTs. Should be possible to establish a stream in 1 RTT once the substrate is set up.
- Allows datagram semantics and maximizes MTU.
- Allows TCP fallback with degradation only for datagram-oriented applications.
- Semantics for the reflector or intermediate proxies to let the agent know that the substrate connection is going away.
- Possible to incorporate into existing HTTP load balancers for proxying. Ideally, the protocol should allow us to run L7 load balancers in front of the reflector.