MASQUE

Multiplexed Application Substrate over QUIC Encryption

IETF 107 Virtual Meeting Tips

This session is being recorded

- **WebEx Link**
- **Make sure your video is off**
- **Mute your microphone unless you are speaking**
- **Use headphones if you plan to speak to avoid echo/Larsen**
- **Use Webex chat only to join the mic queue**
  - "+q" adds you to the queue
  - "-q" removes you from the queue
- **Add your name and affiliation to the virtual blue sheet in the session Etherpad via IETF Datatracker Meeting agenda**
- **Join the session Jabber room via IETF Datatracker Meeting agenda <xmpp:masque@jabber.ietf.org?join>**

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a reminder:

- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process),
- BCP 25 (Working Group processes),
- BCP 25 (Anti-Harassment Procedures),
- BCP 54 (Code of Conduct),
- BCP 78 (Copyright),
- BCP 79 (Patents, Participation),
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

MASQUE

Overview & Rules of Engagement

Chairs

Agenda

Introduction and rules of engagement (5 minutes)

Problem statement and MASQUE framework (20 minutes)

Use-Cases (15 minutes)

Requirements (10 minutes)

Charter text discussion (45 minutes)

BoF questions (30 minutes)

Rules of Engagement

Please hold questions until the end of each presentation

Only clarifying questions until we get to charter discussion

Be polite and concise “at the mic”

MASQUE

Problem Statement & Framework

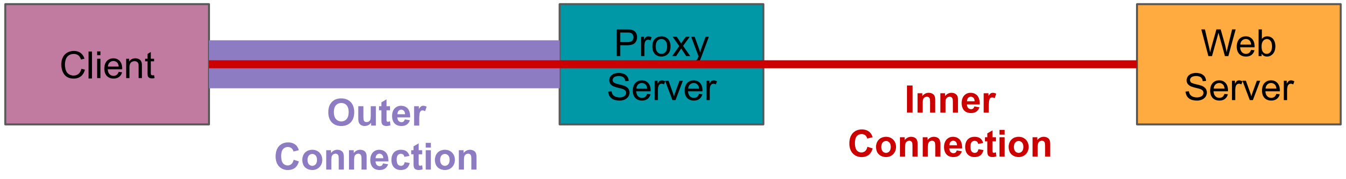
David Schinazi – Google – dschinazi.ietf@gmail.com

Proxies Can Help

Connect disjoint networks

Apply additional encryption; e.g., VPN

Assist congestion controllers



The Proxy Landscape

Native HTTP Proxying (GET, POST, etc.) – Only HTTP, cleartext

HTTP Connect Proxy – Only TCP

SOCKS – Cleartext, Requires multiple round-trips per flow

Tunnel-Mode IPsec – Requires admin privileges

Transparent TCP Proxies – Must be on path

QUIC & HTTP/3 Complicate Things

As the Web moves to HTTP/3, Web traffic now uses QUIC

TLS encryption is mandatory

Transport information, e.g., acknowledgements, are encrypted

Not built on TCP

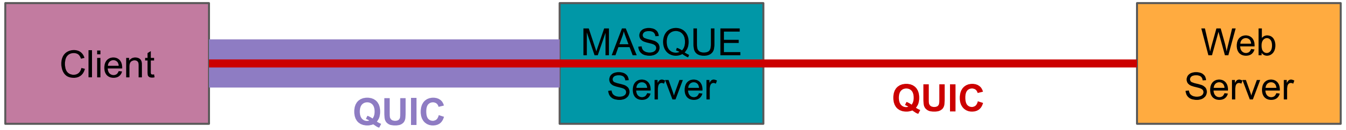
QUIC & HTTP/3 Simplify Things

What if we built a new proxy protocol, using QUIC and HTTP/3?

QUIC provides streams for multiplexing

QUIC has datagrams for unreliable transmission

HTTP/3 provides request/response mechanism, caching, auth mechanisms



The MASQUE Framework

Run multiple networking applications inside an HTTP/3 connection concurrently

Not all traffic needs the same proxy protocol

- Proxied TCP can use HTTP CONNECT to minimize overhead
- Proxied QUIC can benefit from compression of connection IDs
- IP Proxying allows proxying all IP traffic but adds significant overhead

All inside the QUIC encryption boundary, attackers can't see which type of proxy

The MASQUE Protocol

Individual proposal as basis for discussion: draft-schinazi-masque-protocol

Starts with negotiation step using HTTP POST

- Client sends its list of supported MASQUE Applications with config options
- Server replies with the same

Negotiation allows individual applications to bootstrap stream and datagram identifiers for demultiplexing

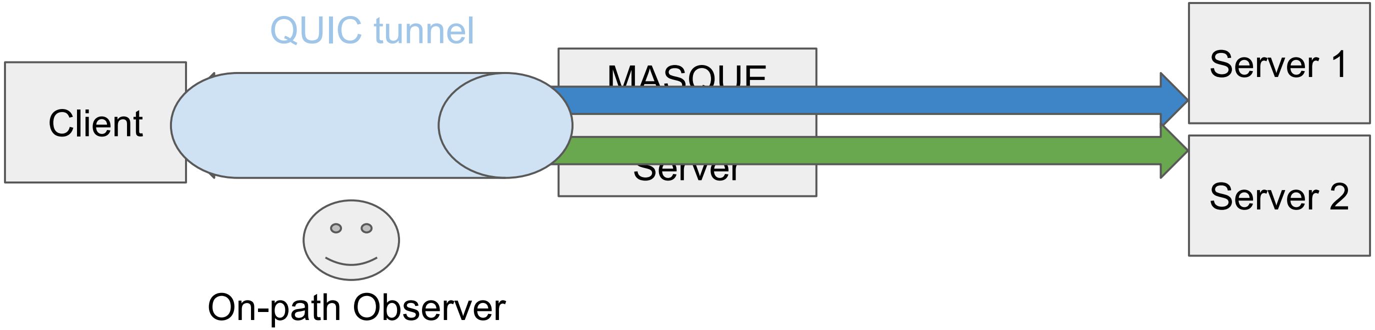
Questions?

MASQUE

Use Cases & Requirements

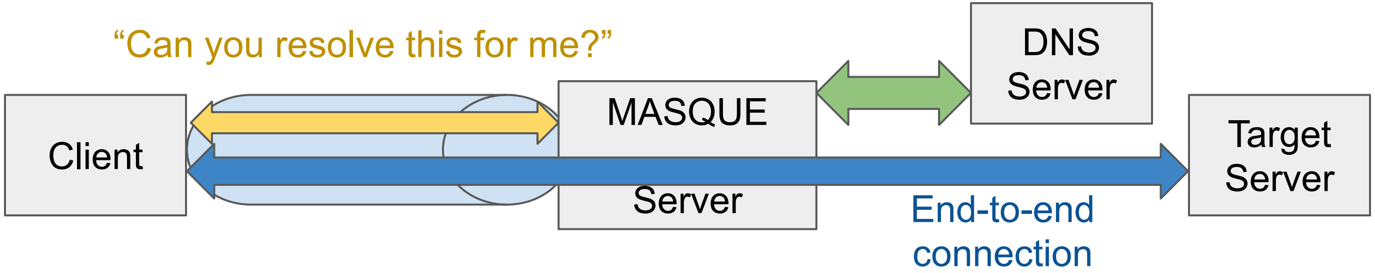
Mirja & Chairs

QUIC-Based Tunneling



- Tunneling provides additional encryption and can “hide” traffic from an on-path observer
- Use of MASQUE should not “stick out” on the path between client and MASQUE server
- Client and MASQUE server have a trust relationship and can optionally authenticate each other
- In addition, address translation at MASQUE server can increase client privacy towards the target server

Service Variety



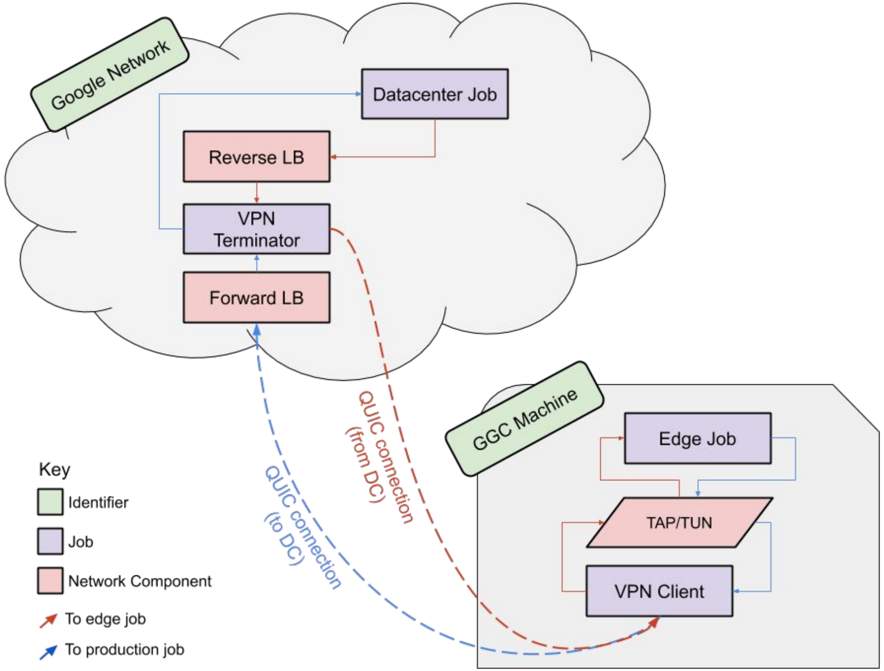
- MASQUE server can provide additional functionality (when located "close" to the client e.g. in the access network)
- Client requests functionality and may provide information to the MASQUE server
- Request DNS resolution as an example

Related: draft-piraux-quic-tunnel

```
            +----------+
       .----| Access   |----.
       |    | network  |    |
       |    |    A     |    |
       v    +----------+    v                            +--------------+
+---------+             +----------------+               | Final        |
| Client  |             | Concentrator   |<===\ ... \===>| destination  |
+---------+             +----------------+               | server       |
       ^    +----------+    ^                            +--------------+
       |    | Access   |    |           Legend:
       |    | network  |    |             --- QUIC tunnel connection A
       .----|    B     |----.             --- QUIC tunnel connection B
            +----------+                  === TCP/UDP flow
```

- Client is often multihomed, e.g. Wi-Fi and 5G
- Client would like to leverage both access networks, e.g. for load-sharing or fail-over
- MASQUE server can act as concentrator

Related: QBONE



QBONE Details – What We Built

- Why QUIC?
  - Pluggable congestion control (turn it off for tunneled packets)
  - Pluggable reliable delivery (turn it off too)
  - Pluggable authentication (we use ALTS)
  - Already part of Google's security stance
- Result
  - Internet-scale VPN deployed across ISP backbones connected back to Google
  - Handling 100+ Gbps of traffic today
  - In production for the last ~2 years
  - Connecting Google Global Cache nodes in 170+ countries

Overview of Proposed Use-Cases

- QUIC-based transport for HTTP Connect
- VPN-like forwarding service using QUIC for encryption
- DNS resolution by proxy
- Tunneling stream-based and congestion-controlled transports like QUIC
- In-network bandwidth aggregation of multiple access links
- IP address translation to improve user privacy towards the server
- Link-specific congestion control

Requirements

1. Proxy negotiation is not easily identifiable on the wire.
2. Proxy use is controlled by clients, i.e., clients cannot be transparently opted into use of a proxy.
3. Each proxy use of MASQUE will have its own semantics. MASQUE should allow clients and servers to exchange arbitrary parameters that control proxy use.
4. Proxies should support arbitrary datagram- and stream-based services.
5. End-to-middle security context between the client and the proxy should be independent from end-to-end client-server security context.

Non-Requirements (Out of Scope)

1. Proxy use can be bootstrapped by arbitrary discovery mechanisms, such as static configuration, unauthenticated DHCP options, or something else. However, building a discovery/bootstrapping mechanism is not in scope.

Questions?

MASQUE

Charter Discussion

https://github.com/chris-wood/ietf-masque/blob/master/README.md

Charter (why is this a problem?)

Many network topologies lead to situations where transport protocol proxying is beneficial. For example, proxying enables endpoints to communicate when end-to-end connectivity is not possible and can apply additional encryption where desirable (such as a VPN). **Proxying technologies such as SOCKS and HTTP(s) Connect exist, albeit with their own shortcomings. For example, SOCKS signalling is not encrypted and HTTP Connect is limited to TCP.**

Charter (why QUIC?)

In contrast, QUIC is a viable candidate protocol for proxying arbitrary traffic, as it provides secure connectivity, multiplexed streams, and connection migration. Further, HTTP/3 supports an established request/response semantic that can be used to set up and configure services.

Using QUIC as a proxying technology allows for proxying of both reliable stream (TCP) and unreliable datagram (UDP) flows. For stream flows, QUIC streams provide reliable in-order delivery across the client-proxy link. QUIC datagrams provide for unreliable data transmission, which allows for transporting UDP and other unreliable flows via a proxy without introducing potentially redundant or unnecessary recovery mechanisms. In addition, QUIC can carry both types of flows over the same connection while taking advantage of a unified congestion controller.

Charter (what will we do?)

The primary goal of this working group is to develop MASQUE (Multiplexed Application Substrate over QUIC Encryption), a framework that allows configuring and concurrently running multiple proxied stream- and datagram-based flows inside a QUIC connection. The MASQUE framework will specify a signaling protocol between client endpoints and MASQUE servers for negotiating proxy services and corresponding parameters. **The group will also specify support for an initial set of client-initiated services such as HTTP, QUIC, and IP proxying**. The group may subsequently recharter to consider additional services or applications.

Proxy services that extend the signaling of the base MASQUE protocol can be adopted by the group by creating a new milestone with AD review. **Specifying MASQUE server discovery mechanisms is out of scope for the group.**

If MASQUE requires any extensions to existing protocols, the group will coordinate closely with the respective group responsible for maintaining that protocol, such as the HTTPBIS, QUIC, or TLS working groups.

BoF Questions

Problem statement

1. Is the scope of the problem well-defined and well-understood?

Community participation

2. Who is willing to review documents or comment on the mailing list?
3. Who is willing to serve as an editor for the proposed deliverables?

Charter and WG formation

~~4. Should the WG be formed with this charter?~~

5. Does anyone feel that a WG should not be formed? If so, why not?

MASQUE

Multiplexed Application Substrate over QUIC Encryption