QUIC-Aware Proxying

draft-ietf-masque-quic-proxy-03

Tommy Pauly, Eric Rosenberg, David Schinazi
MASQUE
IETF 120, July 2024, Vancouver
Status

Version -02 (design team output)

   Packet transforms (scramble) for forwarded mode

   Security considerations

Version -03

   Loop prevention via new ACK_VCID capsule

   Major editorial pass
Protocol terminology

Client

Proxy

Target

Client-to-proxy 4-tuple

Proxy-to-target 4-tuple

Client-to-target connection
Preferred address migration

Issue #113 and Issue #86

How should target preferred addresses be handled?

The client learns the preferred address, not the proxy; but the proxy has the connection to the target

Applies to tunneled and forwarded modes equally

Possible options

1. Client opens a new CONNECT-UDP request with the target address

2. Client sends a new capsule to the proxy to inform it of the preferred target address

3. Something else?
Limiting CID registrations

Issue #109

A client can send many bogus REGISTER_TARGET_CID/REGISTER_CLIENT_CID capsules.

A proxy has to maintain the forwarding / port demultiplexing rules for each of the registered CIDs it acknowledges.

Should proxies signal some limit? Or should they merely send CLOSE_CLIENT_CID/CLOSE_TARGET_CID when the limit is exceeded?
Client VCID length

Issue #112

For loop prevention, the proxy now selects the client virtual CID

“To reduce the likelihood of connection ID conflicts, the proxy SHOULD choose a Virtual Client Connection ID that is at least as long as the Client Connection”

Should this be a MUST?

Helps avoid CID conflicts, etc.
Next steps

Please review latest updates and provide feedback in issues!