



QUIC-Aware Proxying

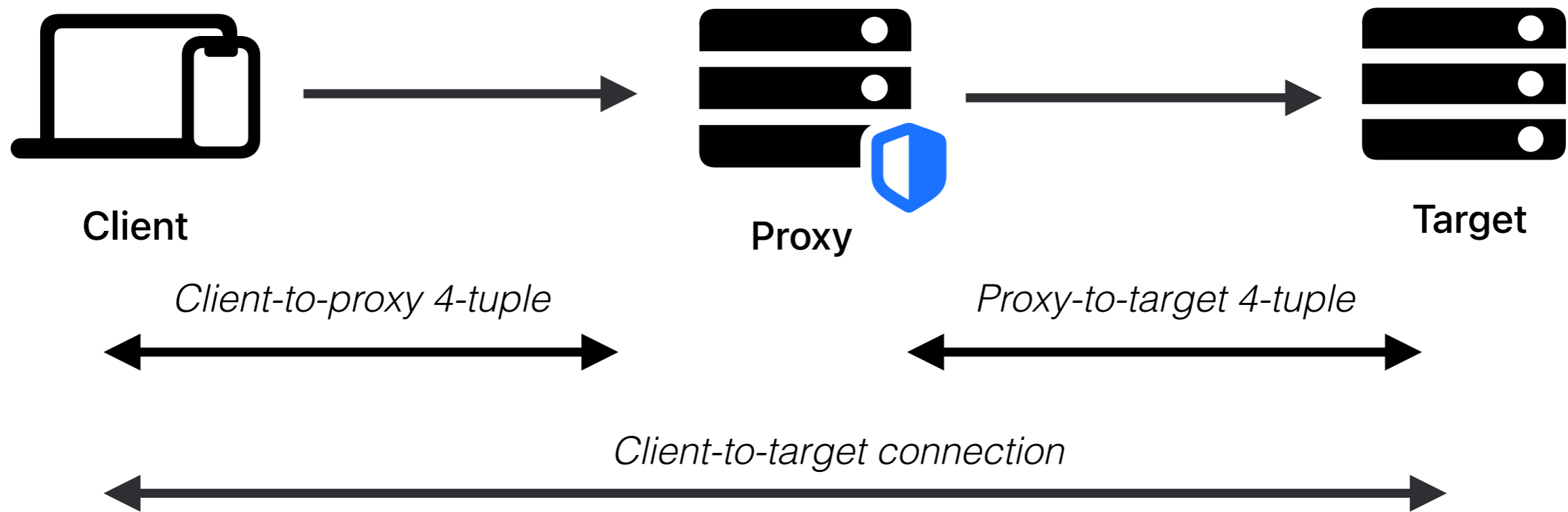
draft-ietf-masque-quic-proxy-05

Tommy Pauly, Eric Rosenberg, David Schinazi

MASQUE

IETF 122, March 2025, Bangkok

Recap



Clients register CIDs for client-to-target connections with the proxy

Proxy can use this information to manage its proxy-to-target 4-tuple, and enable "forwarding mode"

Forwarding mode supports transforms to prevent passive correlation, specifically a "scramble" transform

Updates in -05

Clarify “disabling” of forwarding mode (*Issue #91*)

Proxy-Target port sharing now opt-in (*Issue #38*)

Guidance for port sharing and failed registrations (*Issue #84*)

“Disabling” Forwarded Mode

Issue #91

A client or proxy may wish to stop using forwarding mode.

Proxies have no signaling for this other than closing the stream.

Clients wishing to stop forwarding mode may consider migrating the connection with a new connect-udp request.

Opt-in Port Sharing

Issue #38

Clients may not want connections to particular target servers to share a 4-tuple with other QUIC connections.

Target-facing port reuse is now opt-in via the *Proxy-QUIC-Port-Sharing* header field.

Port Sharing and Registration Ordering

Issue #84

When port sharing is supported, CIDs must be registered before used. What about the first flight?

- Don't want to wait a round trip before sending QUIC Initial
- CID registration is fallible - what happens if we send CID registration with first flight and it fails?

Port Sharing and Registration Ordering

Issue #84

Solution:

- REGISTER_CLIENT_CID and first flight sent at the same time
- Proxy SHOULD buffer packets until receiving REGISTER_CLIENT_CID in case there's been reordering
- On failed CID registration:
 - Client MUST stop sending packets and wait for a successful registration
 - Proxy MUST discard all incoming packets until a successful registration has been made

Next steps

More interop testing needed on scramble

Anything else after this?