



QUIC-Aware Proxying

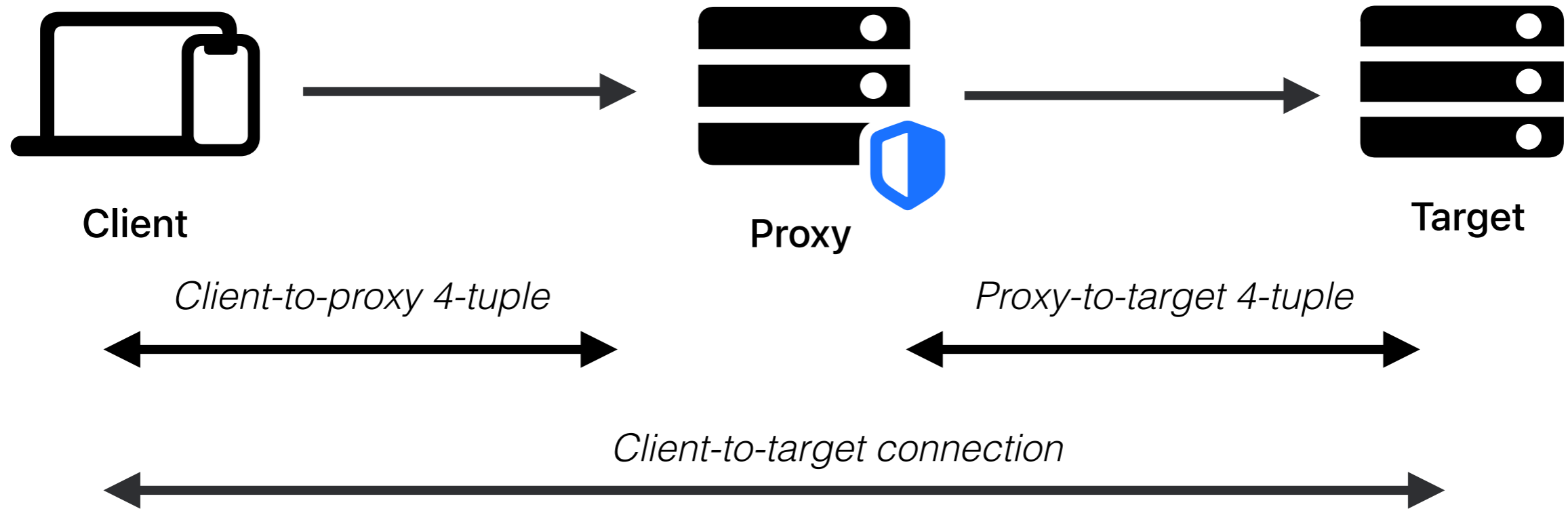
draft-ietf-masque-quic-proxy-06

Tommy Pauly, Eric Rosenberg, David Schinazi

MASQUE

IETF 123, July 2025, Madrid

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 -06

Server Preferred Address guidance ([#113](#), [#86](#))

Example active attack on scramble ([#115](#))

Proxy-QUIC-Forwarding parameters clean up ([#123](#))

Server Preferred Address guidance

Issues #113, #86

Clients can migrate to Server Preferred Address by sending a new CONNECT-UDP request.

Proxies SHOULD send Proxy-Status with next-hop parameter so clients can avoid unnecessary migrations.

Example active attack on scramble

Issue #115

We already mentioned scramble does not protect against active attacks.

Include specific example of active attack on scramble transform IV.

Proxy-QUIC-Forwarding parameters

Issue #123

Change sf-string to String

Stop quoting Booleans

Consistency around Tokens vs. Strings

Remaining Issues

Don't use the term ECB 😱 (#116)

Consider security issues of ECN forwarding (#85)

Don't use the term ECB 😱

Issue #116

Scramble uses AES-ECB in pseudocode

ECB often discouraged as vulnerable

QUIC-TLS Header Protection uses ECB too

Leave as-is? Change?

Consider security issues of ECN forwarding

Issue #85

Embed signals over a series of packets by clearing+setting ECN bits

Observe signal on output side

We have existing text for active attacks. Add ECN as another example.

Next steps

Successful scramble transform interop at
hackathon!

WGLC?