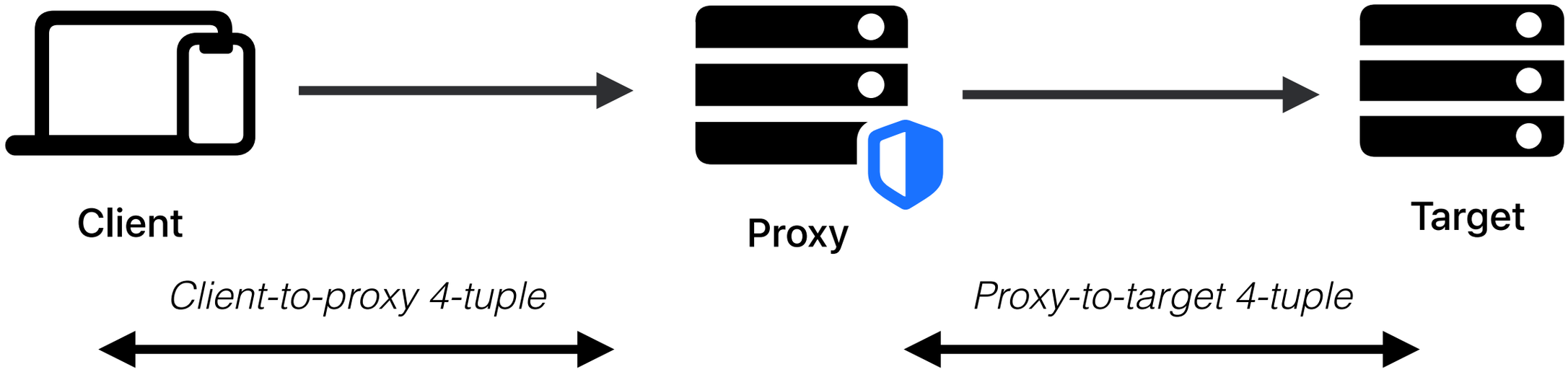
QUIC-Aware Proxying

draft-ietf-masque-quic-proxy-04

Tommy Pauly, Eric Rosenberg, David Schinazi
MASQUE
IETF 121, November 2024, Dublin

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

Updates in -04

Proxies MUST (not SHOULD) pick Virtual CIDs as long as the original CIDs *(Issue #112)*

Added MAX_CONNECTION_IDS to limit concurrently registered connection IDs at the proxy *(Issue #109)*

MAX_CONNECTION_IDS

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.

MAX_CONNECTION_IDS

Issue #109

MAX_CONNECTION_IDS capsule

- Contains a "Maximum Sequence Number" value, must ≥1
- Sent by proxy to client

Connection ID sequence indices start at 0

- 0 and 1 are implicitly always allowed
- Shared between REGISTER_CLIENT_CID and REGISTER_TARGET_CID

Register capsules did not add explicit sequence number values

- Since capsules are reliable and in-order, no ambiguity

Clients can reset the request stream if they are blocked for too long a time and require sending CIDs

Open Issues

Issue #113: Preferred address migration

- Previously discussed at 120
- "Just do another connect-udp request"
- Need to document that and considerations

Issue #115: Active attack on scramble transform

Active attack on scramble transform

Issue #115

Active attacker can modify bytes that will be used for IV generation to be common across multiple packets

- Packets will be invalid / dropped, but scrambled packets will now contain some matching bytes that allow correlating the flows across both sides of the proxy

Scramble was not intended to prevent correlation from active attacks; in our analysis, active attackers can also correlate traffic in tunneled mode

- Do we need to do anything other than document the attack?

Next steps

More interop testing needed on scramble

Anything else after this?