QUIC-Aware Proxying

draft-ietf-masque-quic-proxy-01

Tommy Pauly, Eric Rosenberg, David Schinazi
MASQUE
IETF 119, March 2024, Brisbane

Agenda

Protocol recap

Design Team encryption proposal

Loop issue

Protocol recap

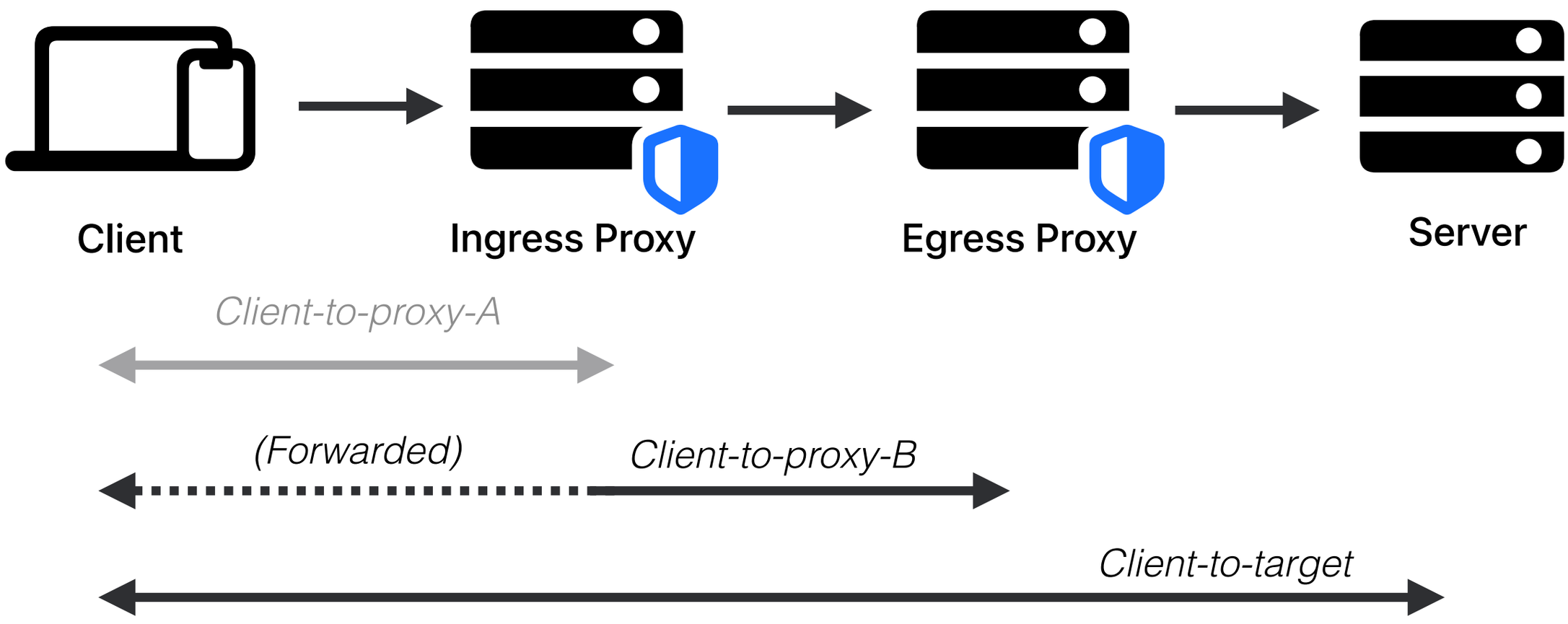
Client tells proxy about inner QUIC connection's CIDs (using capsules!)

Proxy may reuse target-facing ports

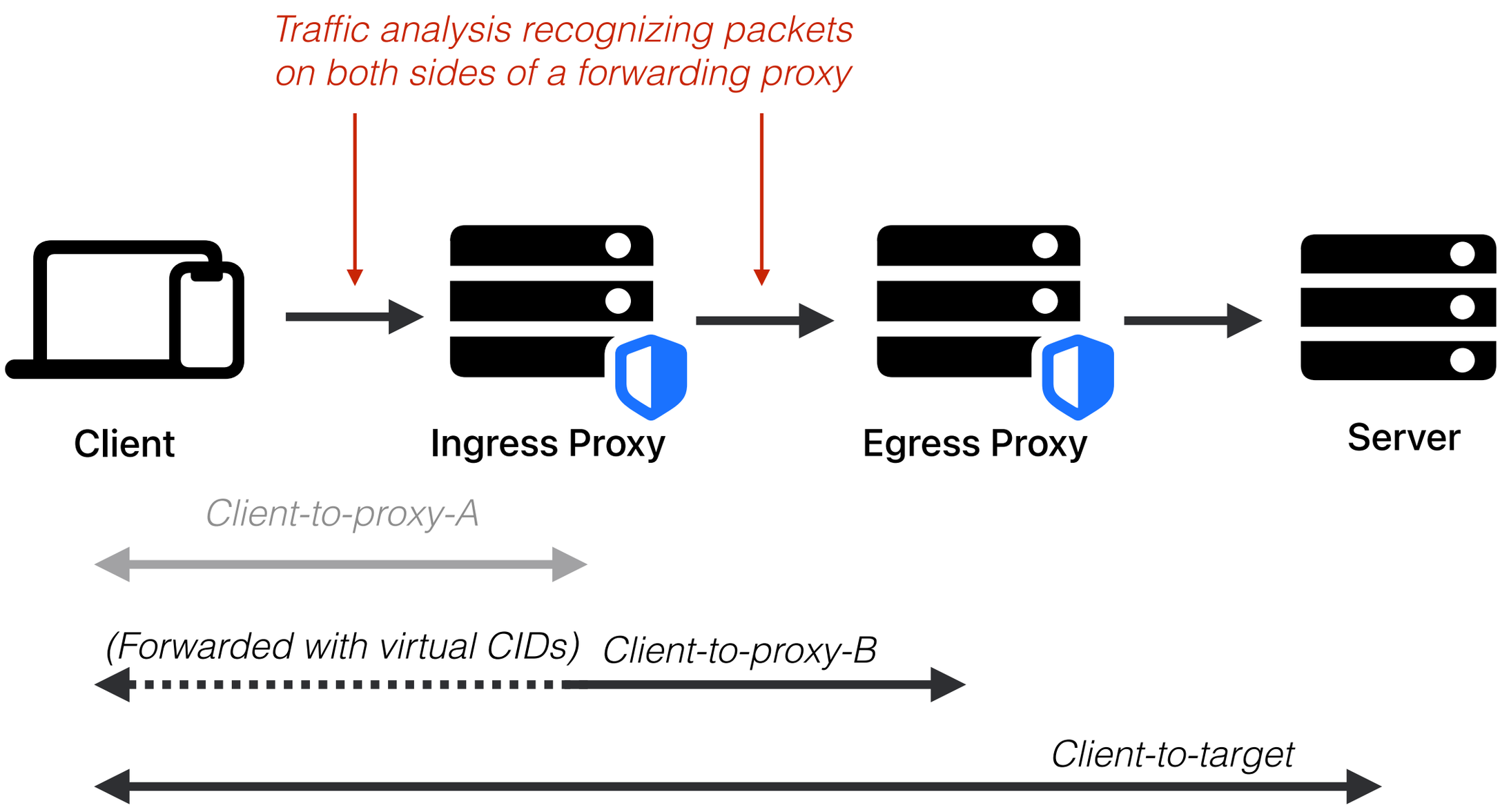
Client and proxy may skip encapsulation and encryption for proxied SH packets — avoiding cumulative MTU overhead issues

Forwarded mode packets on the wire use virtual CIDs instead of the inner connection's real CIDs

Protocol recap



Need for encryption



Design team proposal

PR #99

Goal: **analyze the threat of traffic analysis** on forwarded mode, and **propose a mechanism for adding encryption** to forwarded mode

Design team proposal

PR #99

Proposed solution:

- Add "packet transforms" for forwarded mode
- Define the "scramble" transform, using AES-128 block ciphers
- Prevents passive byte recognition attacks; like tunneling, does not prevent passive timing attacks or active injection/corruption attacks

Design team proposal

PR #99

```
STREAM(44): HEADERS                  --------->
  :method = CONNECT
  :protocol = connect-udp
  :scheme = https
  :path = /target.example.com/443/
  :authority = proxy.example.org
  proxy-quic-forwarding = ?1; accept-transform=scramble,null; \
      scramble-key=:abc...789=:
  capsule-protocol = ?1

                                ...

                     <---------  STREAM(44): HEADERS
                                   :status = 200
                                   proxy-quic-forwarding = ?1; \
                                       transform=scramble; \
                                       scramble-key=:ABC...321=:
                                   capsule-protocol = ?1
```

Design team proposal

PR #99

The base proposal does not cover transforms to add padding or chaff packets to avoid timing attacks

- Techniques to prevent timing attacks would need to be analyzed and designed even for tunneled mode

- New transforms can be defined to handle work in this area

Design team proposal

PR #99

Next steps

- Renaming "null" transform to "identity"
- Are we ready to merge the PR and close the design team?

Open issue: CID loops

Issue #88

Clients can create forwarding loops if:

- Proxy shares a client-facing IP (VIP) with other proxies; and
- Proxy reuses target-facing sockets for multiple tunnels; and
- Client picks Virtual Client Connection ID

Open issue: CID loops

Issue #88

- Prohibiting VIP sharing is incompatible with some deployments
- Eliminating target-facing port sharing may necessitate additional target-facing IPs for sufficient port space
- Proxy-chosen Virtual Client CIDs require clients to receive QUIC packets with CIDs it doesn't generate. May affect ability to demultiplex. Complicates capsule exchange. (PR#104)

Proxy-chosen Virtual Client CIDs

PR #104

Client		Proxy
REGISTER_CLIENT_CID ->		
		<- ACK_CLIENT_CID (Virtual Client CID)
ACK_CLIENT_VCID ->		
REGISTER_TARGET_CID ->		
		<- ACK_TARGET_CID (Virtual Target CID)