MASQUE CONNECT-UDP Bind

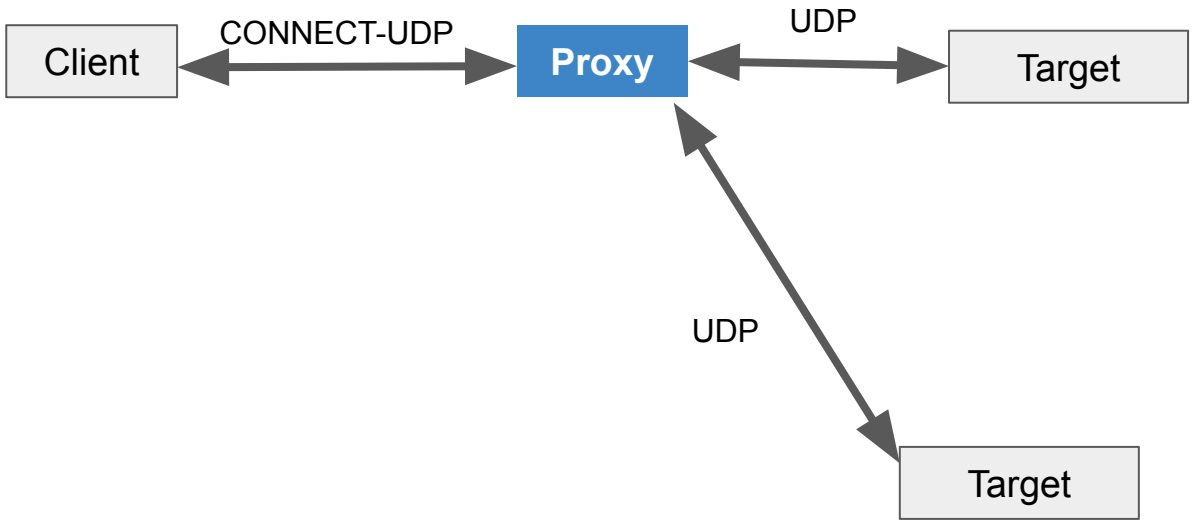
draft-ietf-masque-connect-udp-listen

IETF 123 – Madrid– 2025-07-22

David Schinazi – dschinazi.ietf@gmail.com
Abhi Singh - abhisinghietf@gmail.com

CONNECT-UDP - with Binding support

The client can open UDP port(s) on the proxy to receive traffic from multiple targets



REQUEST:

```
HEADERS
  :method = CONNECT
  :protocol = connect-udp
  :scheme = https
  :path = /masque/udp/ %2A/%2A/
  :authority = proxy.org
  capsule-protocol = ?1
  connect-udp-bind = ?1
```

RESPONSE:

```
HEADERS
  :status = 200
  capsule-protocol = ?1
  connect-udp-bind = ?1
  proxy-public-address = 192.188.0.2:8211,\
                         [2001:db8::1234]:54321
```

Opening and Closing Contexts

Exchange Capsules to create or release Contexts.

COMPRESSION_ASSIGN IP Version = 4/6:

Use that context only for the specified IP address. Omit IP:Port in datagrams

COMPRESSION_ASSIGN IP Version = 0:

Proxy forwards all packets on that context and keeps IP:Port per datagram

```
CAPSULE COMPRESSION_ASSIGN {
  Context ID (i),
  IP Version (8),
  IP Address (32..128),
  UDP Port (16),
}
```

```
CAPSULE COMPRESSION_CLOSE {
  Context ID (i),
}
```

Interop Update!

Marius Kleidl's go-quic and Google QUICHE implementations were interoped

	Google Client	Marius' Client
Marius' Server	✅	✅
Google Server	✅	✅

Changes since last time

State that only one uncompressed Context can be active at a time #29

Percent-encoding the asterisk for target_host and target_port in the URI #30

Pre-WGLC editorial pass #33

Percent-encoding the asterisk for target_host and target_port in the URI #30

Thanks to Marius Kleidl on the mailing list

- Percent encoding * to comply with RFC 6570 URI Template Section 3.2.2 on Simple String Expansion.
- `:path = /masque/udp/%2A/%2A/` instead of `/masque/udp/*/*/`

Open Issues - from Last call

- Require that proxies MUST NOT allocate new compressed contexts to represent incoming packets that don't match an existing context #34
- Allow Mixed Mode Requests #35
- Add MTU considerations #36
- echoing COMPRESSION_ASSIGN is wasteful and error-prone #40

Must not allocate new contexts that match existing contexts #34

Ben Schwartz on the mailing list:

- There must be a requirement that proxies MUST NOT allocate new compressed contexts to represent incoming packets that don't match an existing context.

Proposed changes: PR #37

- Proxy must not open contexts when no uncompressed context exists to preserve the firewall-like property of closing the uncompressed context

Add MTU considerations #36

Ben Schwartz on the mailing list:

- Switching from uncompressed to compressed contexts changes MTU and can mess with E2E DPLPMTUD

Proposed changes: PR #38

Added Operational consideration:

- if an endpoint intends to use compression, it SHOULD request it as early as possible to avoid this issue

Allow Mixed Mode Requests #35

Ben Schwartz on the mailing list:

- Headers:
  CONNECT /udp?target_host=2001:db8::1&port=443 HTTP/3
  connect-udp-bind = ?1
- Fallback on unextended CONNECT-UDP when bind isn't available. If Bind is available, then context ID 0 is 2001:db8::1:443
- Additional destinations added via compression assign

- Removes need for verifying CONNECT-UDP bind and then CONNECT-UDP in separate requests.

Facilitates WebRTC/ICE

- ICE can be performed optimistically by sending datagrams before bind is confirmed, checking peer connectivity.
- When bind is confirmed, a new ICE candidate is generated using the proxy-public-address for a direct connection.
- Peer connects directly and migrates an existing relay connection to it.

Proposed changes: PR #39

- Target Host and the Target Port are the same as unextended CONNECT-UDP
- *connect-udp-bind* request header indicates Bind preferred
- Proxy sets the response *connect-udp-bind* value to true if bind is accepted.
- Context ID 0 in Bind has the same semantics as in unextended CONNECT
- If client cannot accept bind as fallback, target host and port are set to asterisks (%2A). In this case, Context ID 0 is never used
- COMPRESSION_ASSIGN and COMPRESSION_CLOSE capsules can never have context ID 0

echoing COMPRESSION_ASSIGN is wasteful and error-prone #40

Marten Seemann on the draft git repo

- The receiver echoes the capsule with IP:Port to signal that a compression context for a certain context ID was established
- Instead have a COMPRESSION_ACK with just context ID

MASQUE CONNECT-UDP Bind

draft-ietf-masque-connect-udp-listen

IETF 123 – Madrid– 2025-07-22

David Schinazi – dschinazi.ietf@gmail.com
Abhi Singh - abhisinghietf@gmail.com