MASQUE CONNECT-UDP Listener

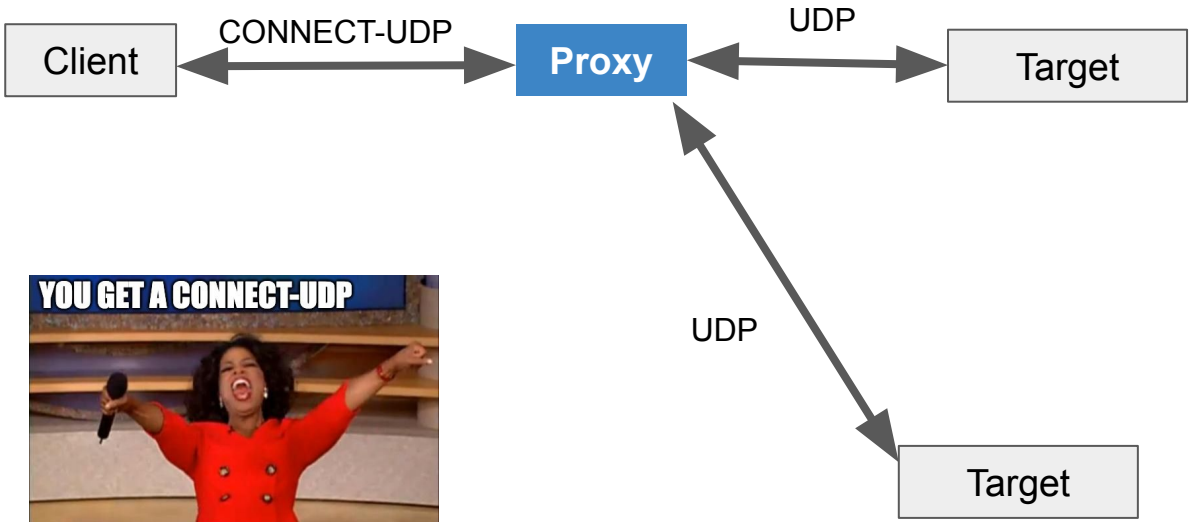
draft-ietf-masque-connect-udp-listen

IETF 118 – Prague– 2022-11-10

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

CONNECT-UDP - with Listener support

Infinite 5-tuples using just one CONNECT-UDP connection.



How does it work?

```
HEADERS
  :method = CONNECT
  :protocol = connect-udp
  :scheme = https
  :path = /masque/udp/*/*/
  :authority = proxy.org
  capsule-protocol = ?1
  connect-udp-listen = 42
```

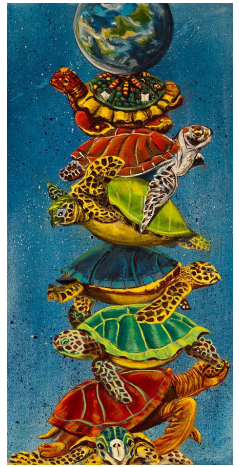
```
DATAGRAM QUIC Frame {
  Type (i) = 0x30..0x31,
  [Length (i)],
  Quarter Stream ID (i),
  Context ID (i) = 42,
  IP Version (8),
  IP Address (32..128),
  UDP Port (16),
  UDP Payload (..),
}
```

QUIC

HTTP/3

CONNECT-UDP

CONNECT-UDP-Listen



Context ID registered by header – payload then contains IP & port

More about the IP fields

IP Version (8),
IP Address (32..128),
UDP Port (16),

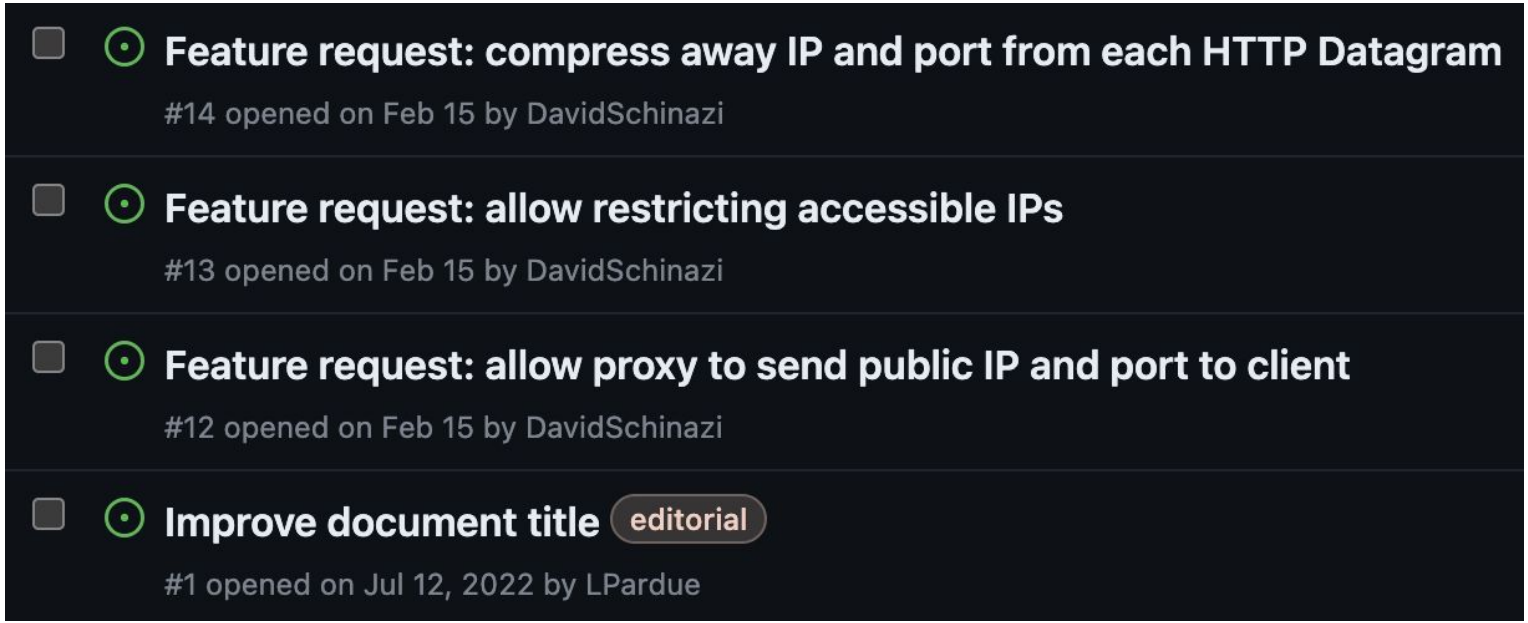
These Fields reflect:
client -> proxy
Target IP/Port PER PAYLOAD

proxy -> client
Source IP/Port PER PAYLOAD

Shall we validate source packets?

Open Issues

https://github.com/ietf-wg-masque/draft-ietf-masque-connect-udp-listen/issues



Improve Document Title (#1)

- https://github.com/ietf-wg-masque/draft-ietf-masque-connect-udp-listen/issues/1
- Name it to better reflect what it does
- From the mailing list
  - bind-udp
  - connect-udp binding extension
  - connect-udp-stable
  - mirroring-proxy

Feature request: allow proxy to send public IP and port to client #12

https://github.com/ietf-wg-masque/draft-ietf-masque-connect-udp-listen/issues/12

- Useful for a client to have this information
- Embed it in the response of the client's CONNECT-UDP request?
- Add response header

  proxy-public-address= List of [IP:port]s
- Allow midstream changes? Server sends newly allocated public IP info via capsule

  PR:

https://github.com/ietf-wg-masque/draft-ietf-masque-connect-udp-listen/pull/18

Feature request: allow restricting accessible IPs #13

https://github.com/ietf-wg-masque/draft-ietf-masque-connect-udp-listen/issues/13

- Proposition: Allow all target traffic. Add a security consideration for it.
  - Unlike non binding CONNECT-UDP, since the proxies tunnel datagrams from any target to clients bound to their respective public IP and ports, the clients SHOULD be ready to handle potential unwanted traffic from unknown destinations.
- If WG deems it necessary:
  - Allow client to specify allowed IP addresses and ranges via capsules.
  - Does it need deletion functionality?

PR:https://github.com/ietf-wg-masque/draft-ietf-masque-connect-udp-listen/pull/17

Feature request: compress away IP and port from each HTTP Datagram #14

https://github.com/ietf-wg-masque/draft-ietf-masque-connect-udp-listen/issues/14

- Our proposed header adds 19 bytes of overhead per packet
- For compressed audio formats, it may represent >50% of net bandwidth.

- Proposition: Header compression using Context IDs

PR: https://github.com/ietf-wg-masque/draft-ietf-masque-connect-udp-listen/pull/19

1.) Client registers a unique Context ID per 2 tuple using a COMPRESSION_REQUEST capsule

2.) Proxy confirms via COMPRESSION_ASSIGN capsule

3.) Omit IP/Port information for future frames to/from the same target.

4.) Reserve context ID = 0 for uncompressed frames

```
Capsule {
  Type = COMPRESSION_REQUEST,
  Quarter Stream ID = 11
  Context ID (i) = 2,
  IP Version = 4,
  IP Address = 192.0.42.1,
  UDP Port = 3939,
}
Capsule {
  Type = COMPESSION_ASSIGN,
  Quarter Stream ID = 11
  Context ID (i) = 2,
}

DATAGRAM {
  Quarter Stream ID = 11,
  Context ID (i) = 2,
  UDP Payload = …,
}
```

MASQUE CONNECT-UDP Listener

draft-ietf-masque-connect-udp-listen

IETF 118 – Prague– 2022-11-10

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