The CONNECT-IP HTTP method for proxying IP traffic

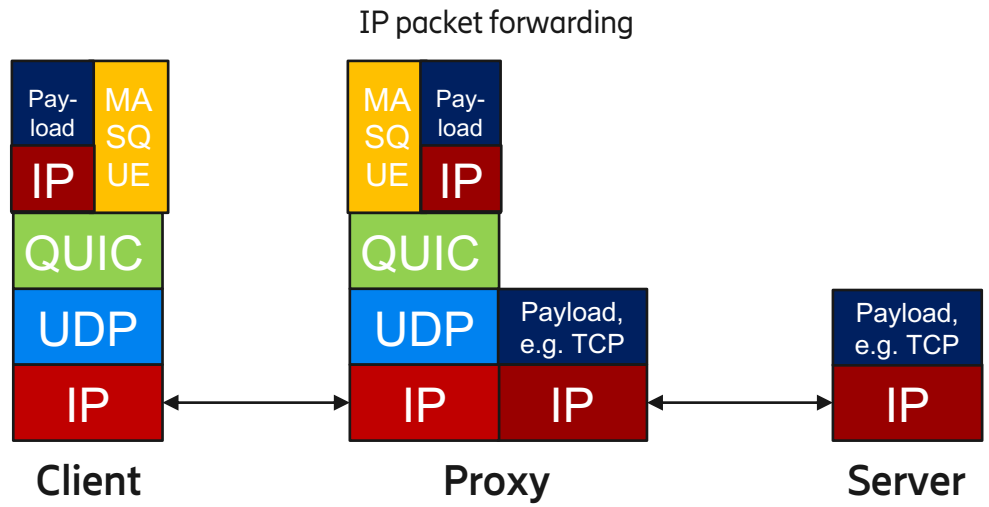
draft-kuehlewind-masque-connect-ip-01

Mirja Kühlewind
Magnus Westerlund
Marcus Ihlar
Zaheduzzaman Sarker

Tunnel mode and Flow Forwarding mode

Tunnel mode

- Client requests to tunnel IP packets to and from one or more servers via the proxy.
- Client MUST be authenticated.
- Proxy inspects IP header and forwards or drops packets based on source or destination IP address.



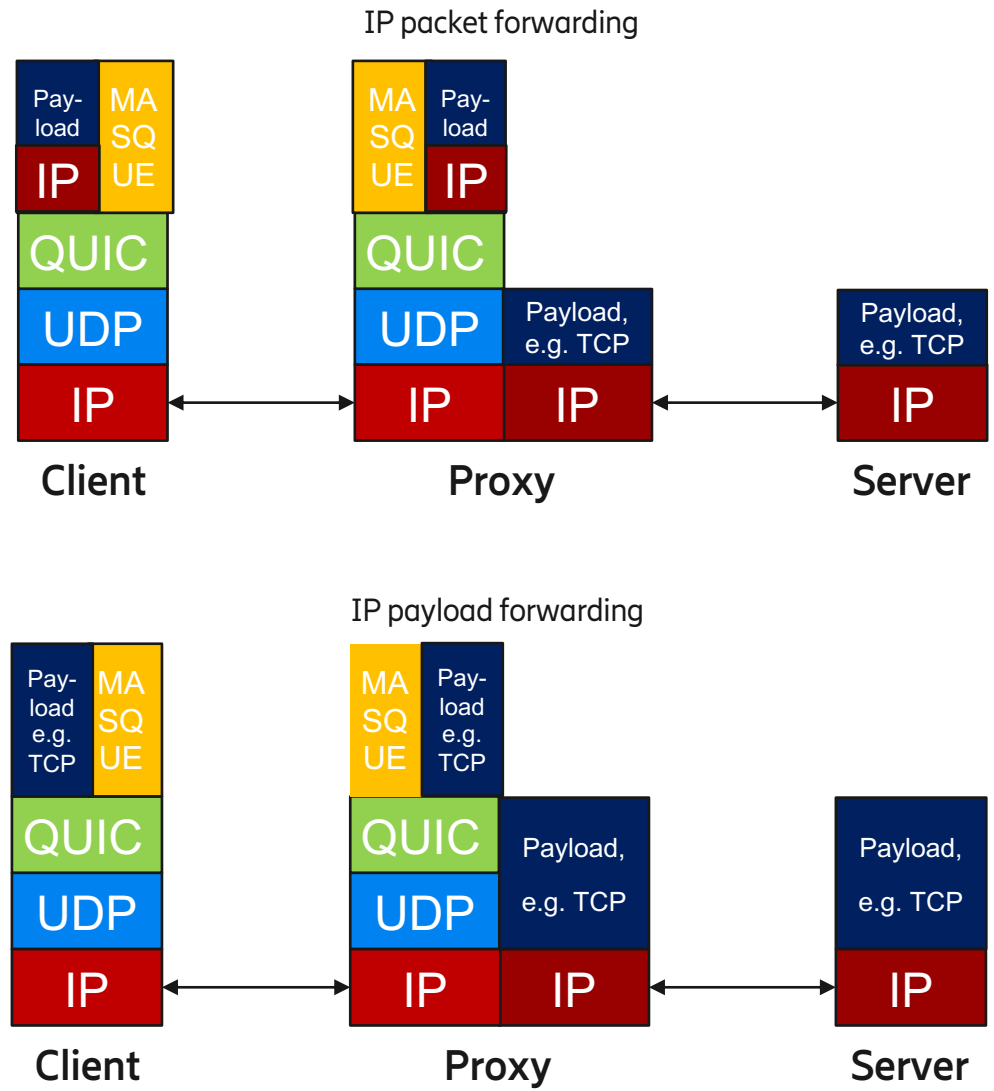
Tunnel mode and Flow Forwarding mode

Tunnel mode

- Client requests to tunnel IP packets to and from one or more servers via the proxy.
- Client MUST be authenticated.
- Proxy inspects IP header and forwards or drops packets based on source or destination IP address.

Flow Forwarding mode

- Client establishes an outgoing IP flow from the MASQUE server's external address to the target server's address for a particular upper layer protocol.
  - This mode does not support flow establishment by an external peer.
- The payload does not contain the IP header in order to reduce overhead.



CONNECT-IP in Tunnel Mode

Proxy IP address

```
CONNECT-IP 198.51.100.0:443
IP-Version: 4
```

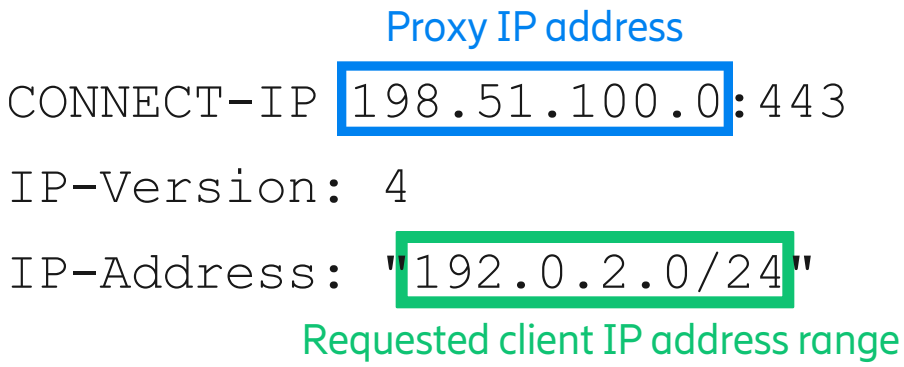
- `IP-Version` header: to check if the requested IP version is supported by the network and if the destination or source IP address for compliance

```
HTTP/3 200
IP-Address: "192.0.2.2"
```

Out-facing proxy IP address

- `IP-Address` header: out-facing IP address or IP address range assigned to the client for this association

CONNECT-IP in Tunnel Mode (network-2-network)



- `IP-Version` header: to check if the requested IP version is supported by the network and if the destination or source IP address for compliance
- *Optional:* `IP-Address` header: to request the use of a certain IP address or IP address range by the client to be used as source IP address in tunnel mode;
  - Also used in both modes in the response from the proxy to confirm IP address used, either by the client directly or as outfacing IP address by the proxy

CONNECT-IP in Flow Forwarding Mode

Target server IP address or URL

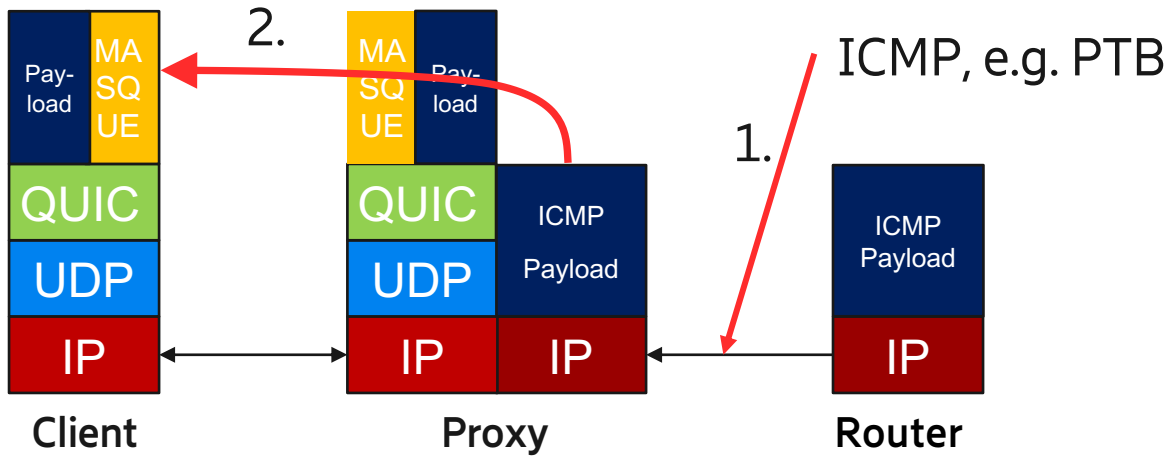
```
CONNECT-IP target.example.com:443
IP-Protocol: 6
```

- `IP-Protocol` header: For the proxy to fill the "Protocol" field in the IPv4 header or "Next header" field in the IPv6 header
- *Optional:* `IP-Address-Handling` header: to request the use of a stable address for multiple active flow forwarding associations
- *Optional:* `Conn-ID` header: indicates the `value`, `offset`, and `length` of a field in the IP payload that can be used by the proxy as a connection identifier in addition to the IP address and protocol tuple when multiple connections are proxied to the same target server

ICMP Handling in Flow Forwarding Mode

1. ICMP Message Reach Proxy
2. Proxy matches ICMP to IP Flow and verifies

- Use of separate Context ID to provide flow-based ICMP messages
  - Server to Client Message
  - Based on regular ICMP format
    - Carries payload, such as ICMPv6 PTB MTU
    - Future Proof
- ICPMP handling as a test of using Context ID
  - But lacking Context Extension to negotiate
- Next: Similarly, Context IDs for ECN support



Summary

- CONNECT-IP can easily support tunnel mode **and** flow forwarding mode
  - Tunnel mode requires a more trusted relationship to client
    - Client can provide IP address or IP address range but any other route negotiations can either happen outside of the MASQUE framework (e.g. restrict set of destination addresses) or added as an extension later
    - Updates on the client address or address range can be realized by a new CONNECT-IP request
    - Support of 0-RTT data during tunnel setup is optional
  - Flow forwarding mode is very similar to CONNECT-UDP and reduces per-packet overhead
    - Only signalling of the upper layer protocol number is required to construct IP header at proxy
    - Use of Context IDs for ICPM handling and ECN support