TURN Server Networking options
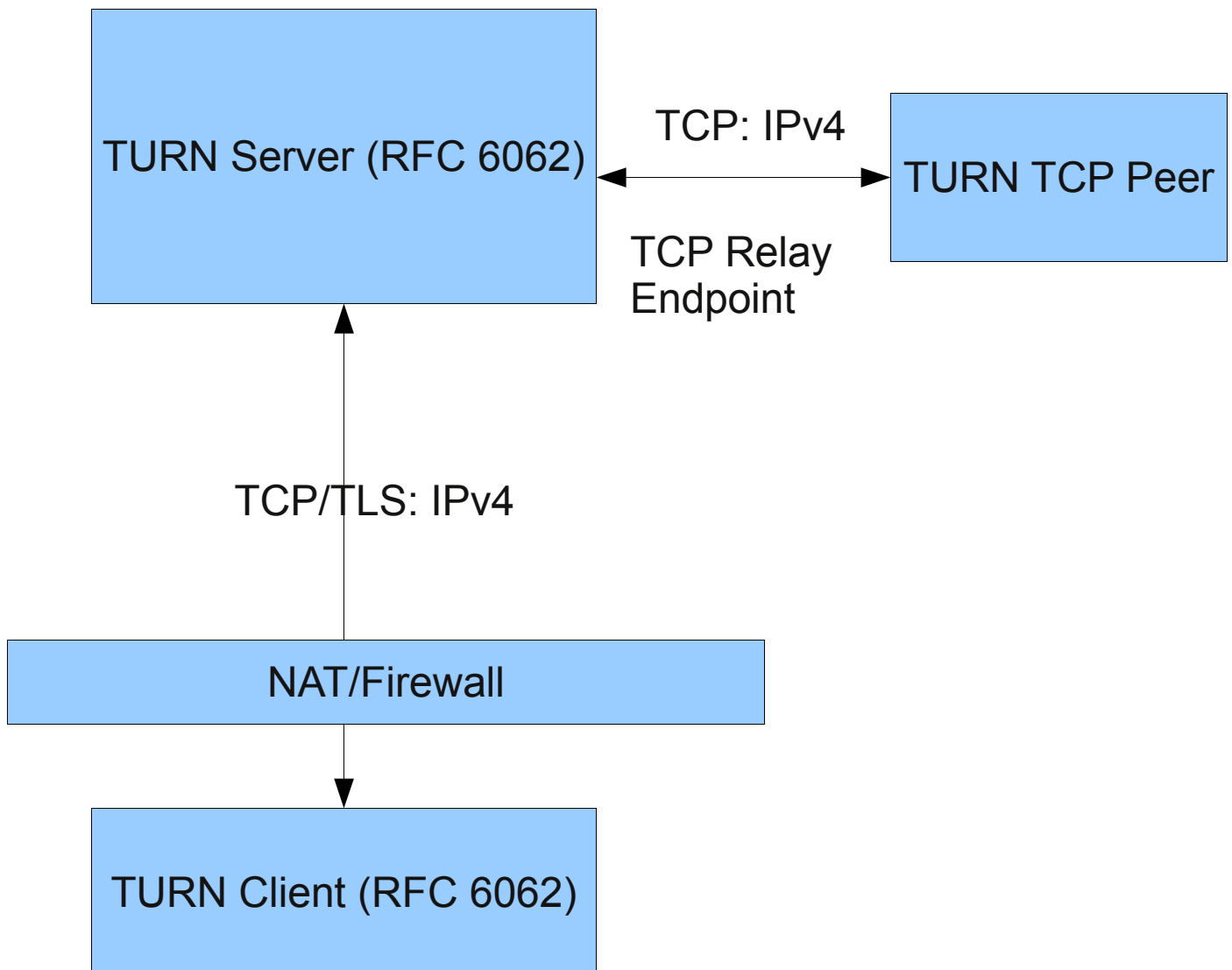# Use cases supported by the TURN Server

1. RFC 5766 classic use case

TURN Server (RFC 5766)	UDP: IPv4	TURN UDP Peer

UDP Relay
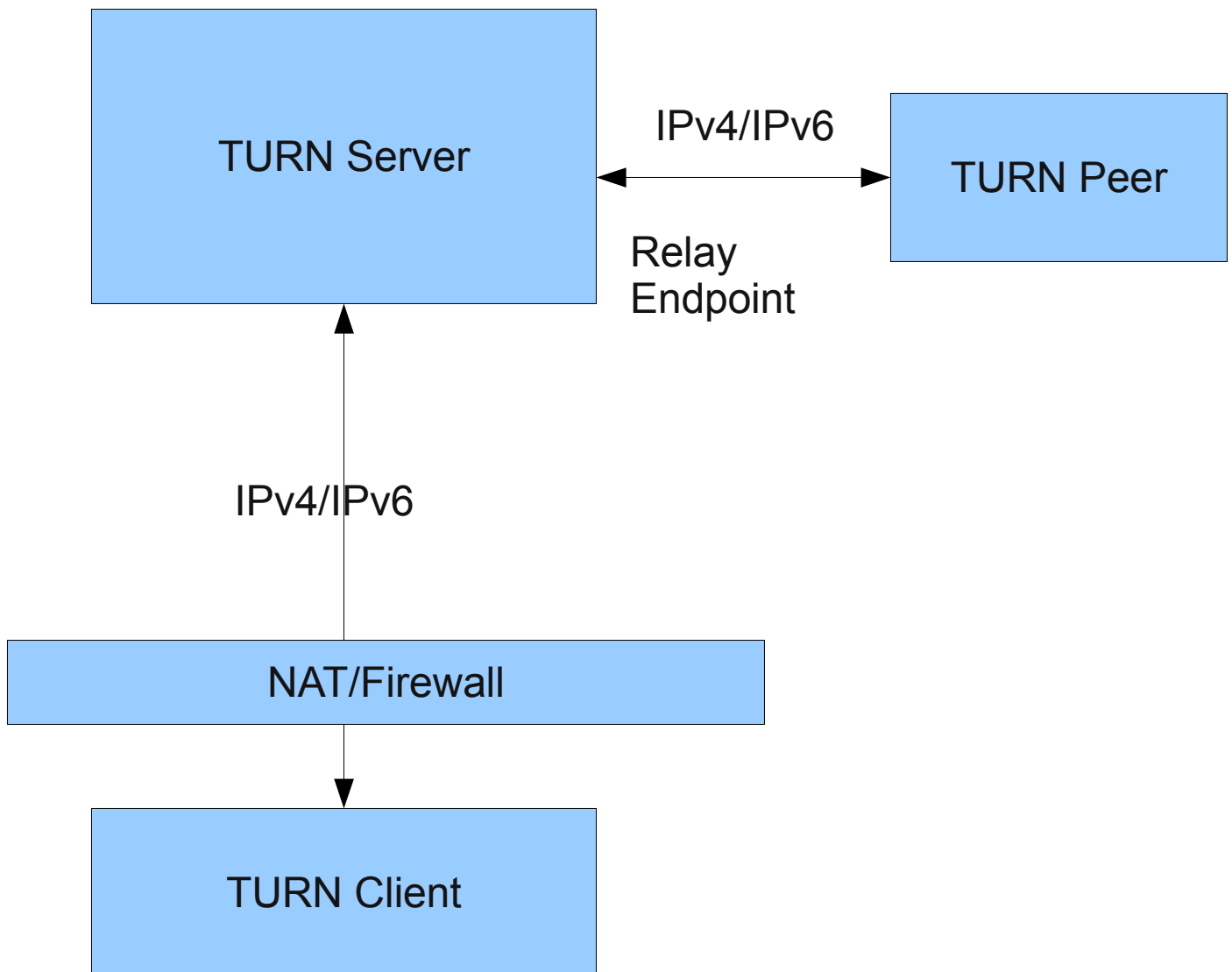Endpoint

UDP/TCP/DTLS/TLS: IPv4

NAT/Firewall

TURN Client
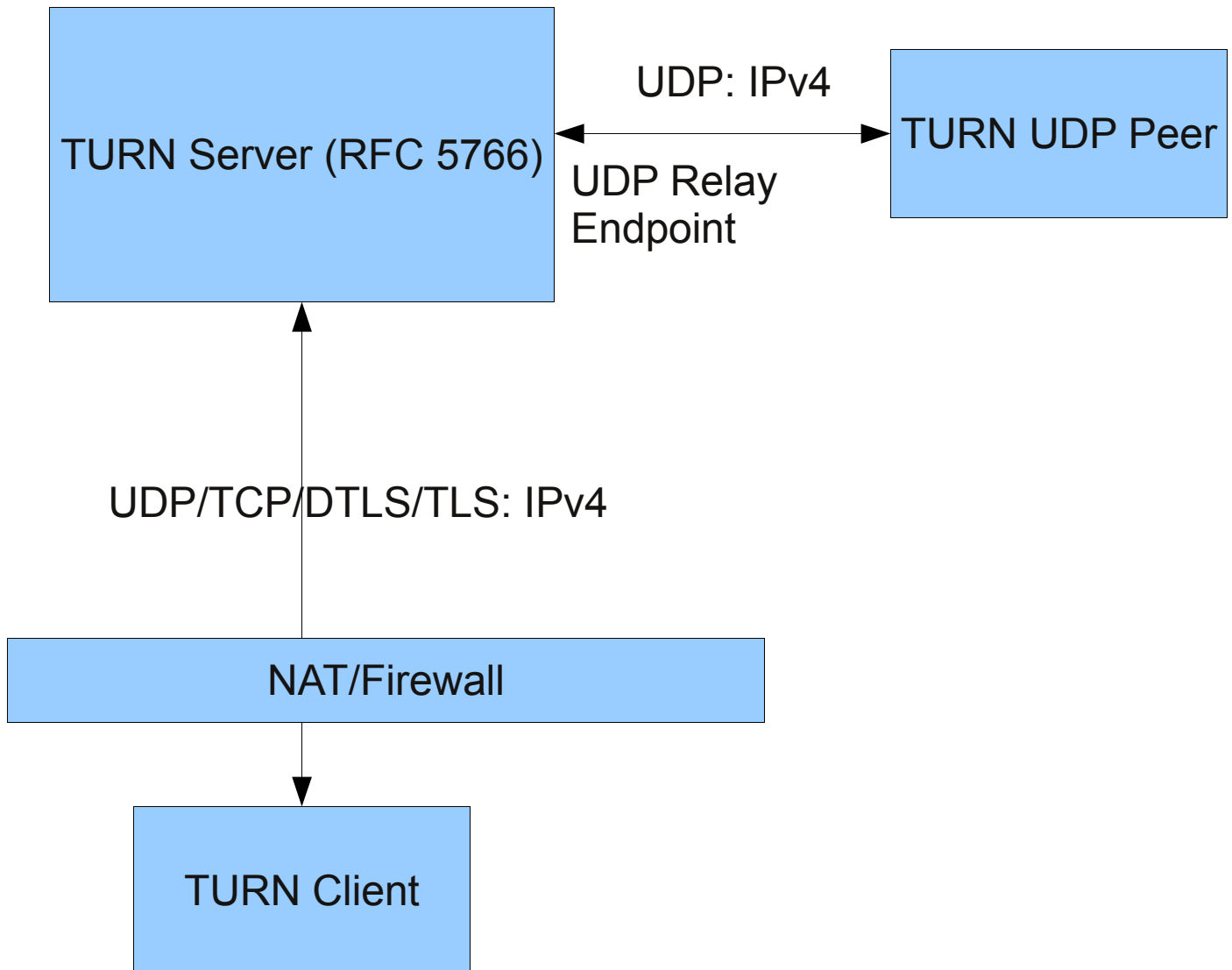
Note: DTLS is this picture is an "experimental" extension, not defined by any RFC

2. TCP relaying use case: RFC 6062

TURN Server (RFC 6062)
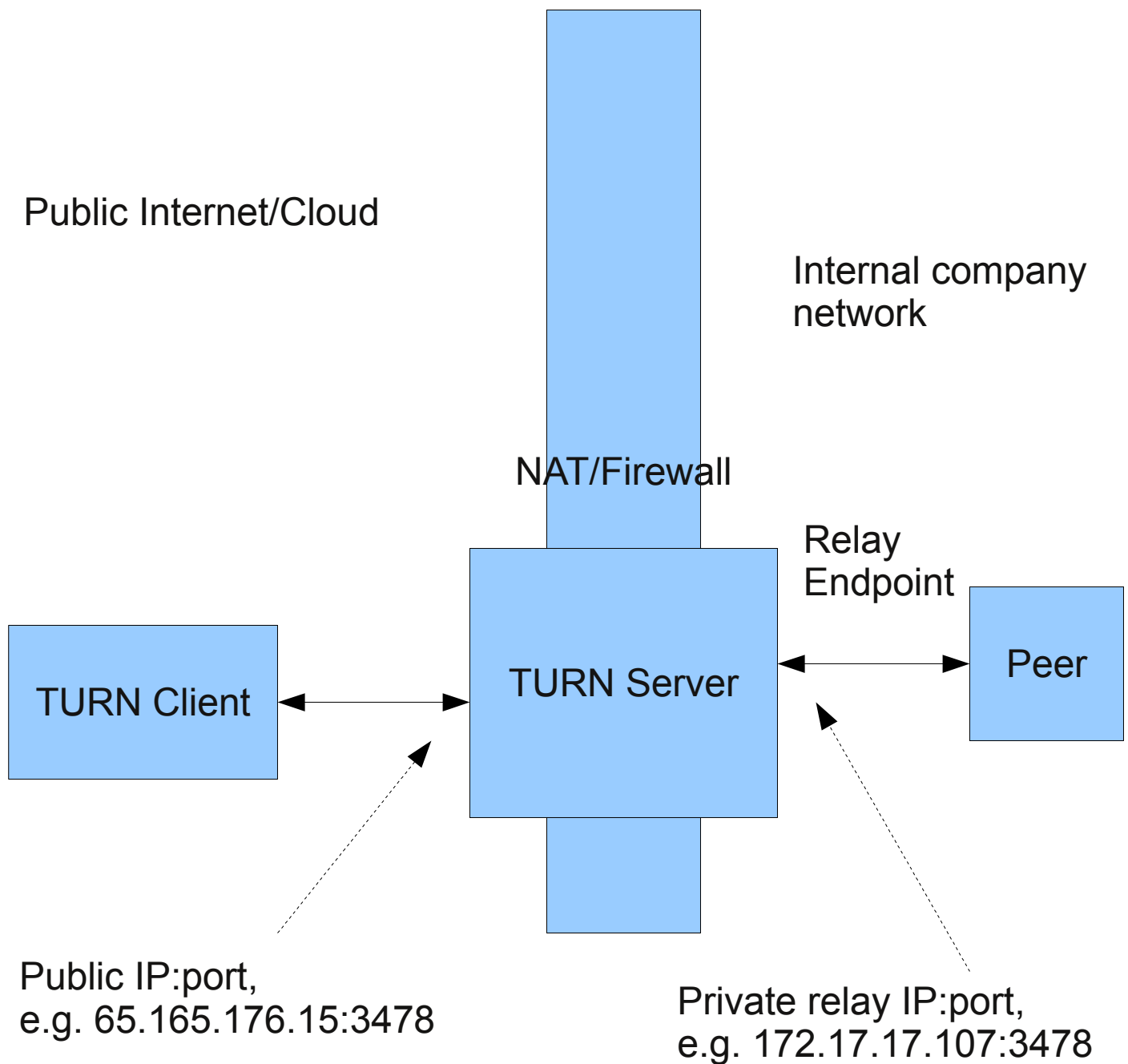
TCP: IPv4

TURN TCP Peer

TCP Relay
Endpoint

TCP/TLS: IPv4

NAT/Firewall

TURN Client (RFC 6062)

3. IPv6 extension: RFC 6156

```
                                       IPv4/IPv6
   ┌─────────────────────────┐                    ┌──────────────────┐
   │                         │ ◄────────────────► │                  │
   │       TURN Server       │                    │    TURN Peer     │
   │                         │   Relay            │                  │
   │                         │   Endpoint         └──────────────────┘
   └─────────────────────────┘
              ▲
              │ IPv4/IPv6
              │
   ┌─────────────────────────────────────┐
   │            NAT/Firewall              │
   └─────────────────────────────────────┘
              │
              ▼
   ┌─────────────────────────┐
   │       TURN Client       │
   └─────────────────────────┘
```

4. Client-to-client connectivity

Relay
Endpoint 1

Relay
Endpoint 2

TURN Server

May use separate
IP(s) for relaying,
e.g. 137.254.16.113

Public IP and port, e.g. 66.165.176..15:3478

IPv4/IPv6
UDP/TCP/DTLS/TLS

IPv4/IPv6
UDP/TCP/DTLS/TLS

NAT/Firewall 1

NAT/Firewall 2

TURN Client 1

TURN Client 2
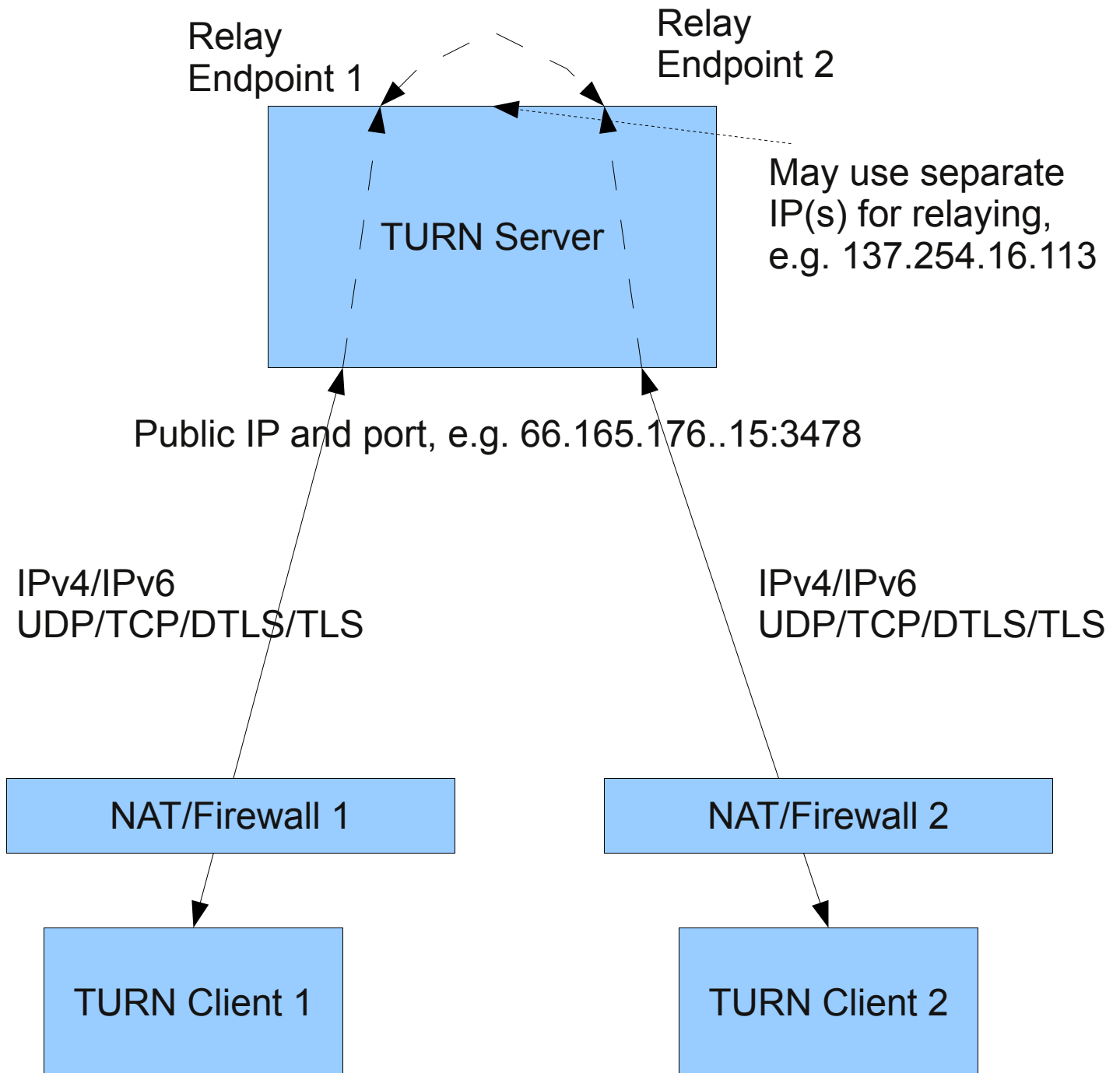
5. TURN as an UDP/TCP traffic Gateway

Public Internet/Cloud

Internal company network

NAT/Firewall

Relay Endpoint

TURN Client ←→ TURN Server ←→ Peer

Public IP:port,
e.g. 65.165.176.15:3478

Private relay IP:port,
e.g. 172.17.17.107:3478

6. TURN Server behind NAT

Public Internet/Cloud

TURN Client 1

Private IP:port, e.g.
172.17.17.107:3478
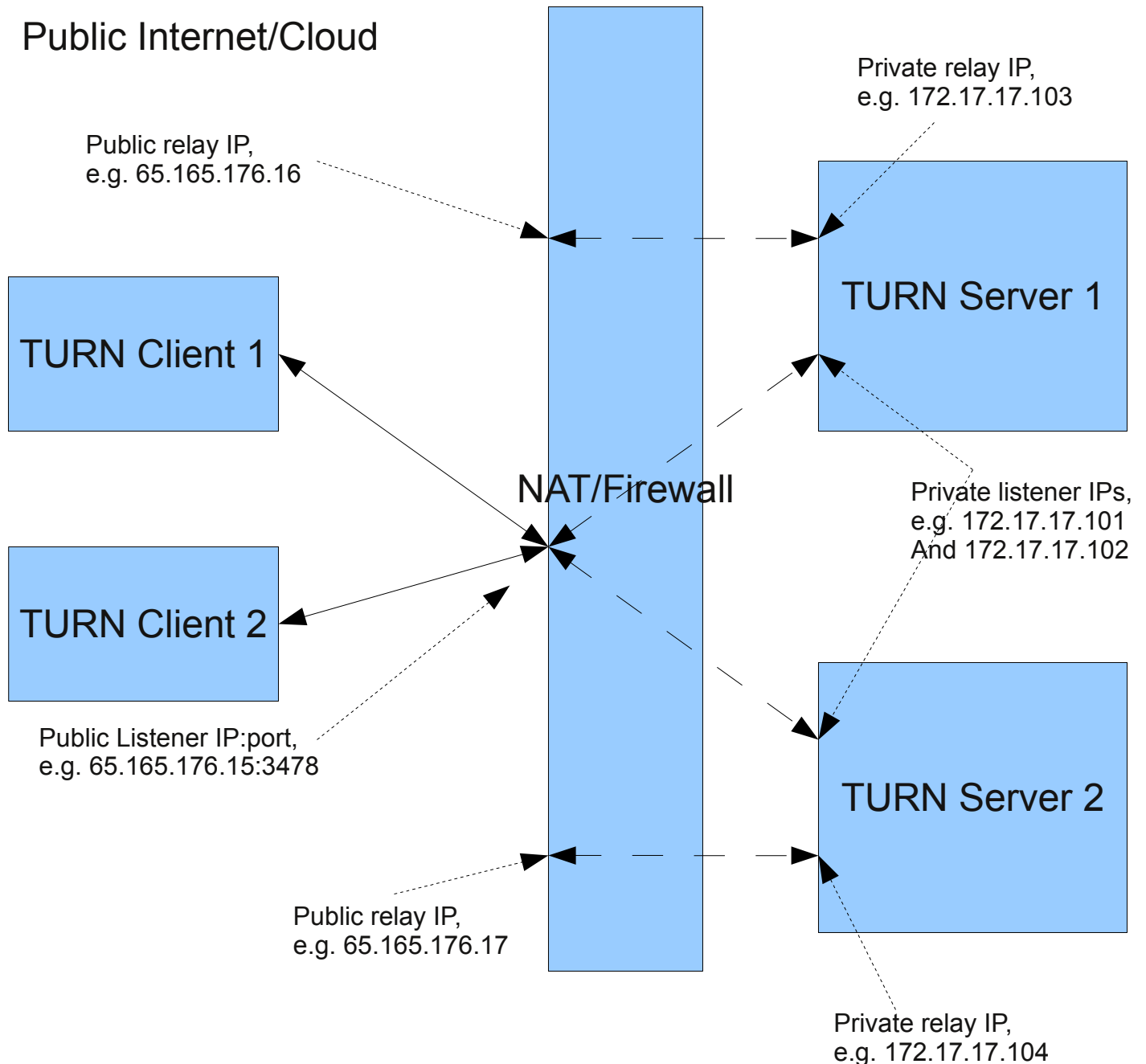
NAT/Firewall

TURN Server

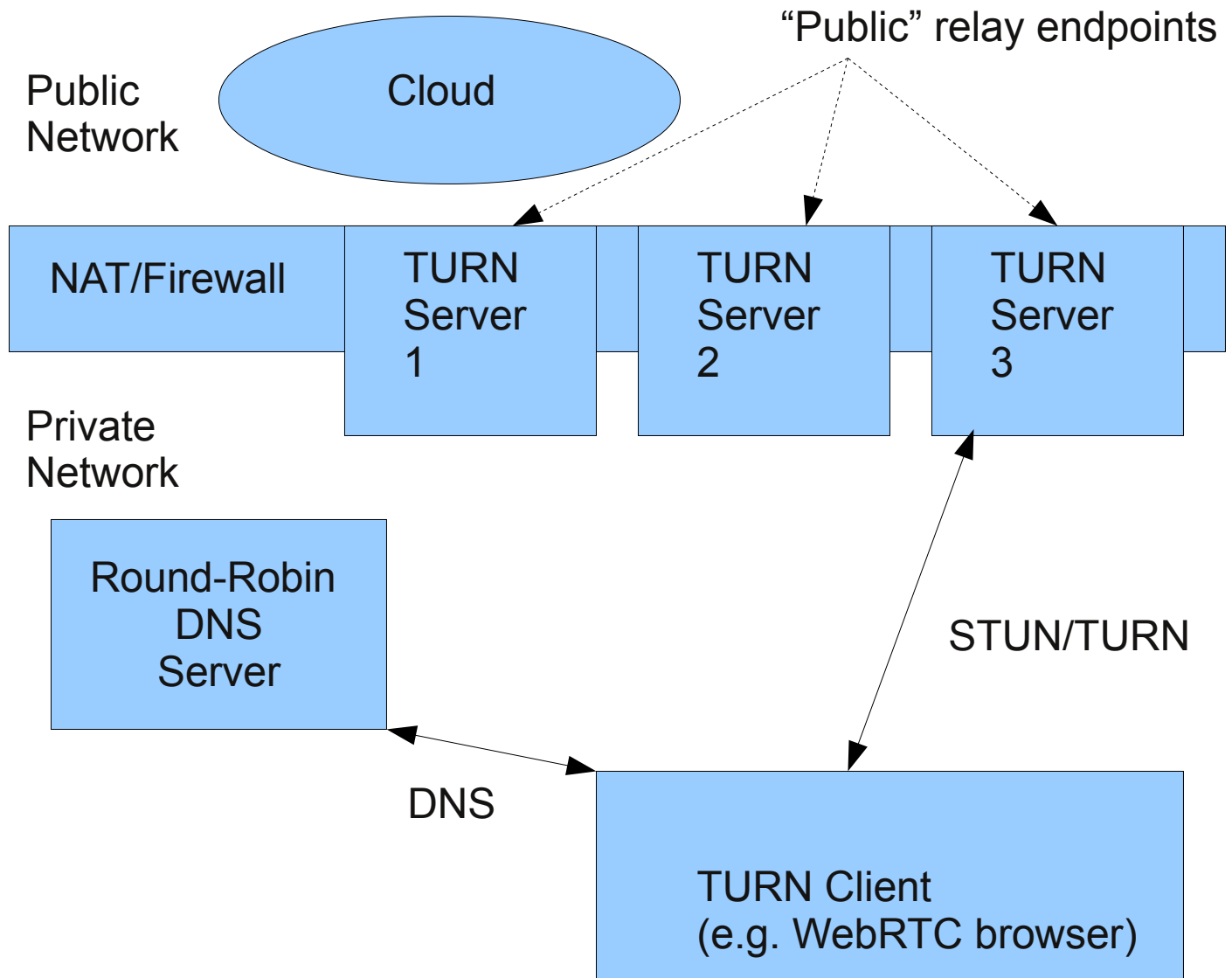TURN Client 2

Public IP:port,
e.g. 65.165.176.15:443
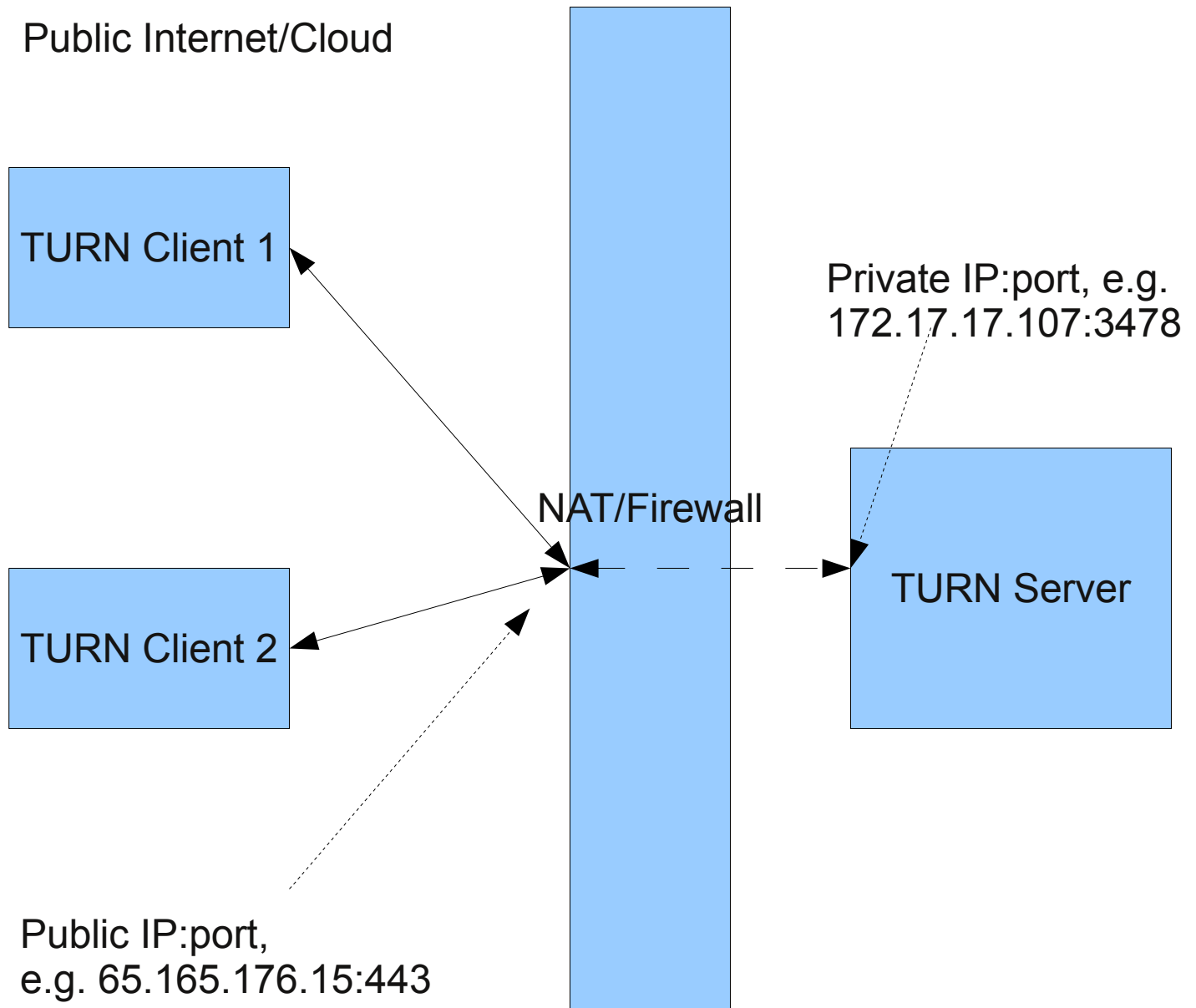
Note: -X TURN Server option can be used to set the public
TURN IP. In this case, a single private IP must be used as
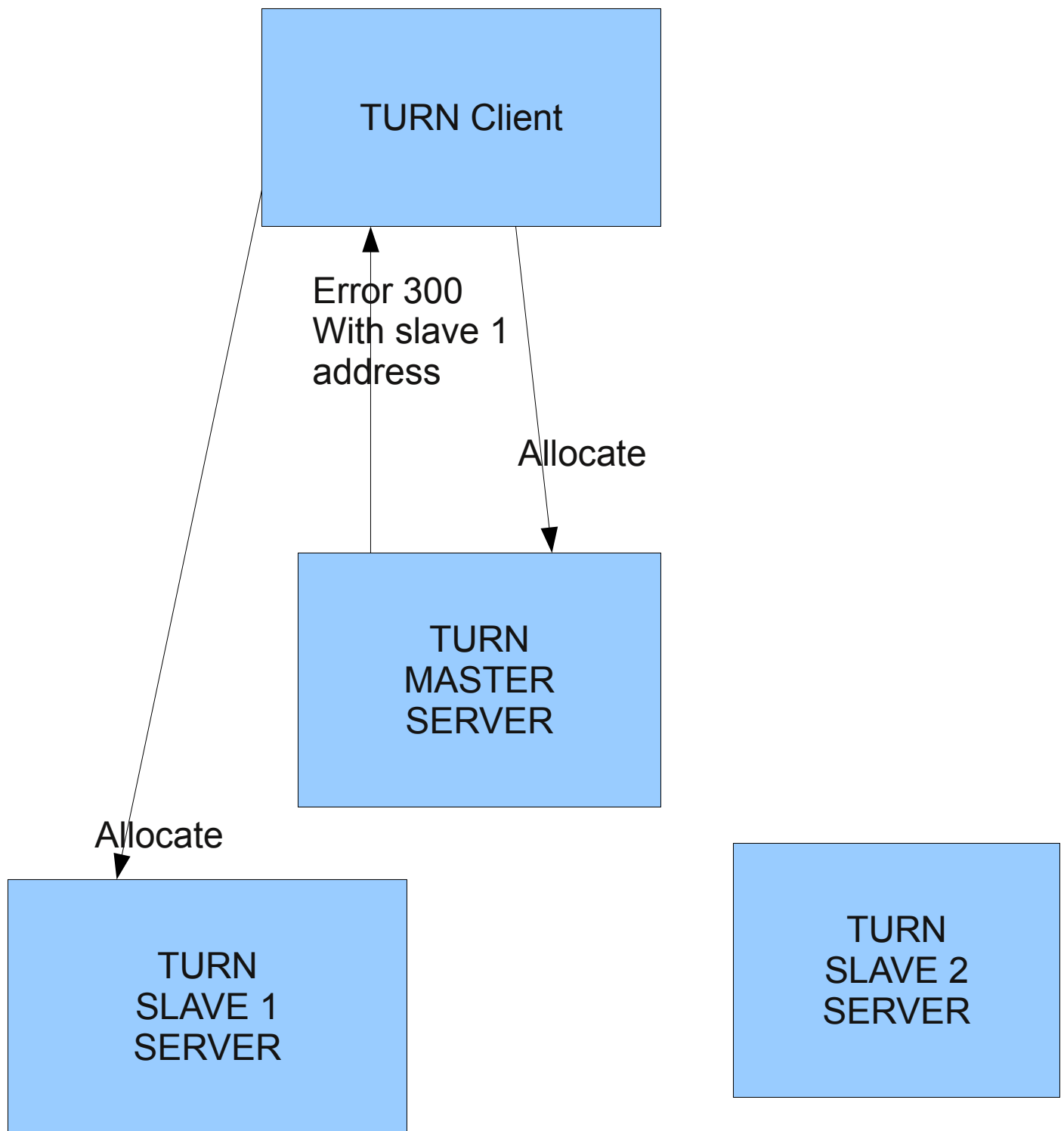the relay IP.

7. TURN Server behind NAT with load balancing

Public Internet/Cloud

Public relay IP,
e.g. 65.165.176.16

Private relay IP,
e.g. 172.17.17.103

TURN Client 1

TURN Server 1

NAT/Firewall

Private listener IPs,
e.g. 172.17.17.101
And 172.17.17.102

TURN Client 2

Public Listener IP:port,
e.g. 65.165.176.15:3478

TURN Server 2

Public relay IP,
e.g. 65.165.176.17

Private relay IP,
e.g. 172.17.17.104

Note: -X TURN Server option can be used to set the public IP.
In this case, a single private IP must be used as a relay IP
on each TURN server.

8. "Enterprise" TURN Server with load balancing

"Public" relay endpoints

Public Network

Cloud

Private Network

NAT/Firewall

TURN Server 1

TURN Server 2

TURN Server 3

Round-Robin DNS Server

STUN/TURN

DNS

TURN Client (e.g. WebRTC browser)

A TURN client obtains A TURN Server IP address that will be used for all TURN sessions of this client. Different clients May use different TURN servers for load balancing. A smart DNS server is responsible for load balancing and for TURN servers status monitoring (for failover).

9. Load balancing based upon ALTERNATE-SERVER machanism

TURN Client

Error 300
With slave 1
address

Allocate

TURN
MASTER
SERVER

Allocate

TURN
SLAVE 1
SERVER

TURN
SLAVE 2
SERVER

For latest stable TURN Server version, see the project page
http://code.google.com/p/rfc5766-turn-server/

Oleg Moskalenko, Citrix Systems,
mom040267@yahoo.com
Version 0.93
Apr 19, 2013