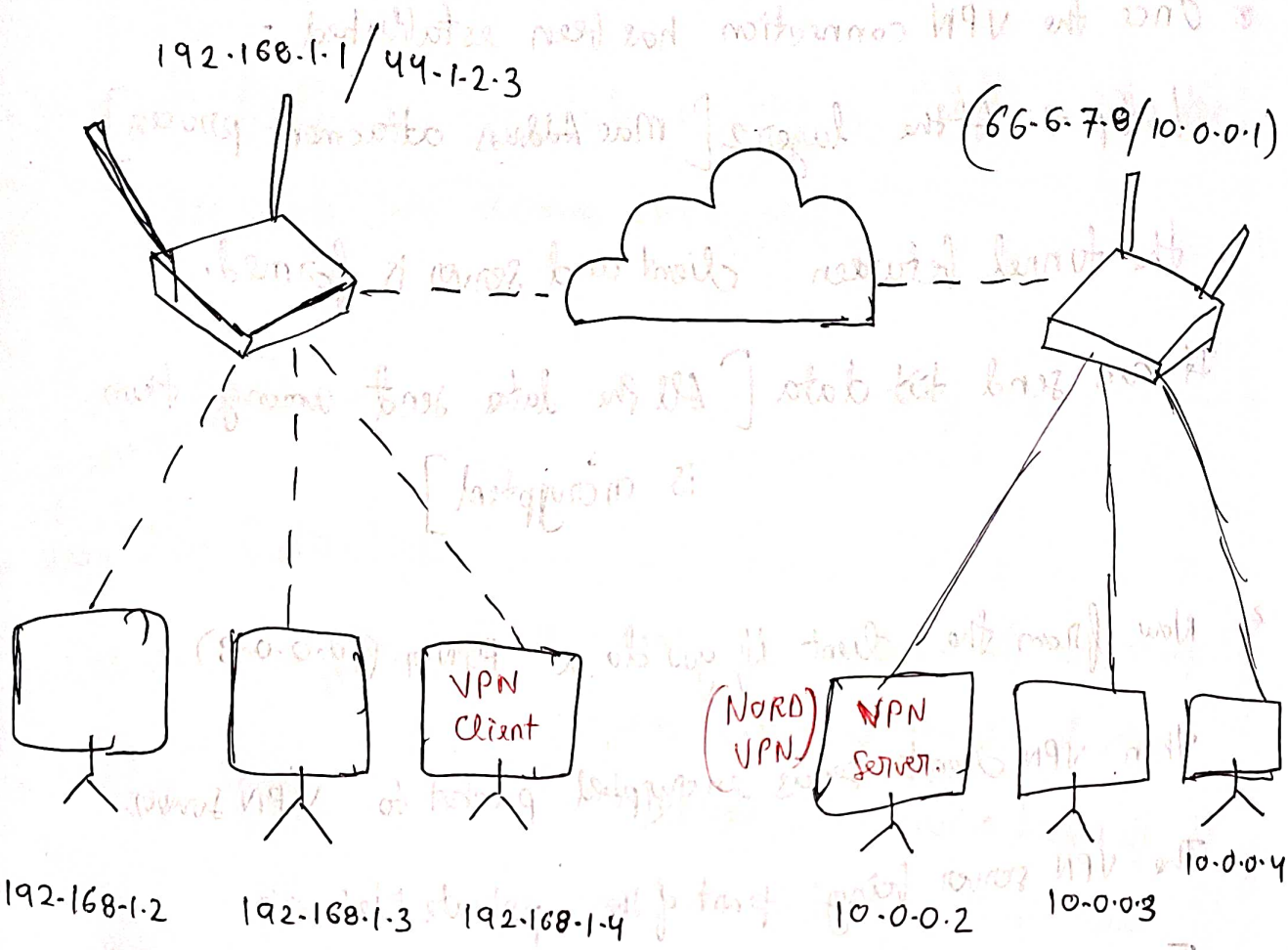
3. (VPN vs Proxy Explained Pros and Cons)



[VPN → Virtual Private Network] : It makes you part of a private Network. Using VPN client, you can ping (10.0.0.3) which is a private ip

Client tries to connect to VPN server using some protocols →

L2tp → Layer2 tunnelling protocol [Data Link layer]

Ipsec

IKEV2 → Key Exchange protocol

* Once the VPN connection has been established:

Letp → At the layer 2 [Mac Address attachment process]

the tunnel between client and server is formed.

It can send ~~test~~ data [All the data sent among them is encrypted]

* Now from the client if you do a PING (10-0-0-3)

Then VPN client sends encrypted packet to VPN server.

The VPN server being part of the private Network:

Fetches the data and sends it back to client.

This connection and midway having VPN server doing the communicatn will take time hence VPN makes avery slow.

In most VPN, the VPN server (concentrator) allocates the IP from an internal Pool and assigns it to the client via the VPN protocol itself with various info like routes, DNS resolver. etc

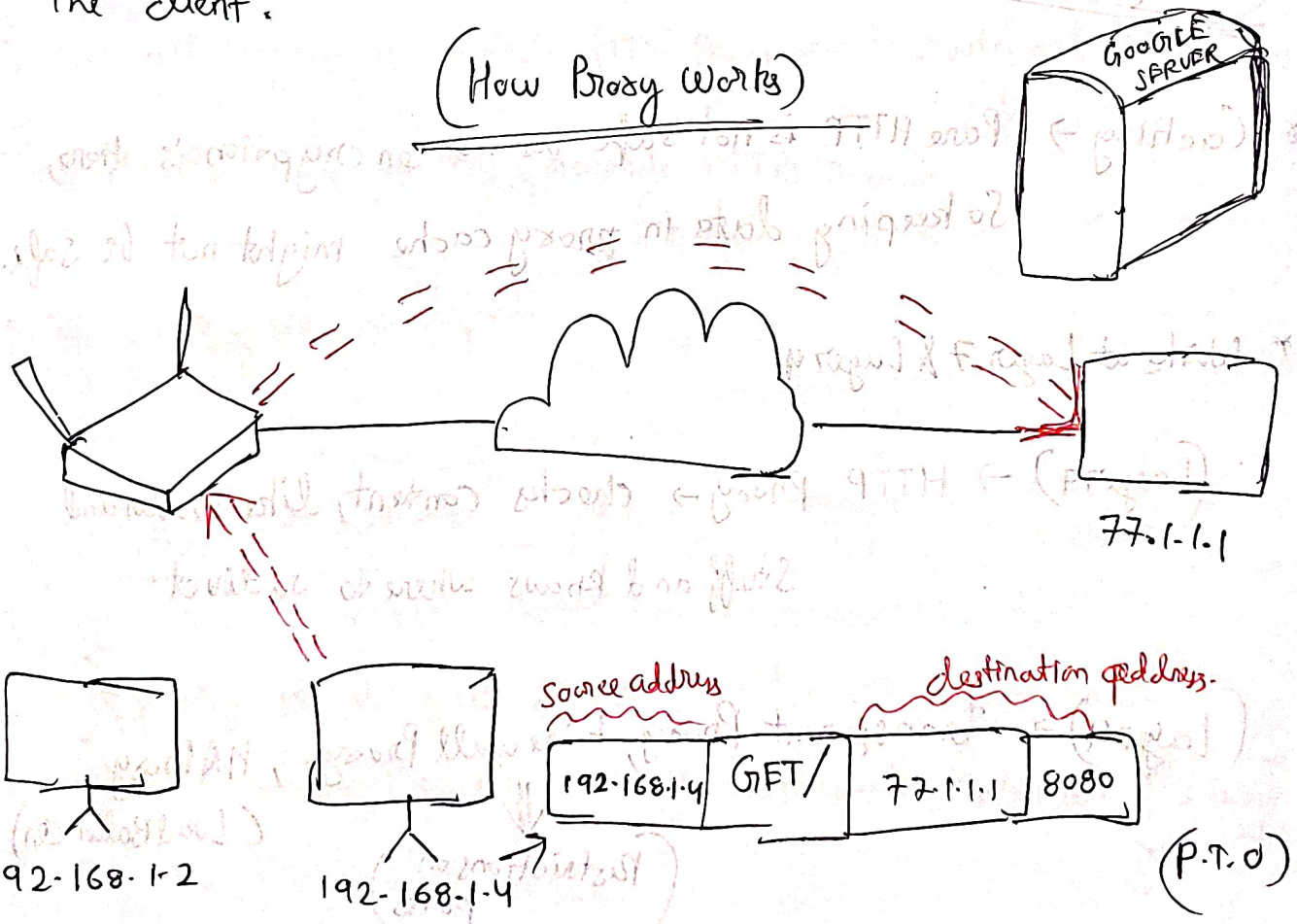
(VPN Pros)

- Encrypts traffic → So while making a tunnel with the VPN server data becomes encrypted.

(VPN Cons)

- Very Slow Extra hops
- Double Encryption → TLS/HTTPS encryption already there between client and the actual server, the VPN adds another layer of encryption and slows things down.
- No caching
- VPN can access and log your data. The client.

(How Proxy Works)



(P.T.O)

Q) But the question arises, how does the proxy know what is the destination?

A) In HTTP V 1.1, they added a header called

HOST: http:// google-com . This is what is seen by the proxy and from here it knows where to redirect.

In HTTP, earlier this control was not there and hence, HTTP was not able to support proxy.

[HTTP 1.0 → No Proxy]

(Proxy Pros)

* Caching → Pure HTTP is not safe as no encryption is there, So keeping data in proxy cache might not be safe

* Works at Layer 7 & Layer 4.

(Layer 7) → HTTP Proxy → checks content, like header and Stuff and knows where to redirect

(Layer 4) → Transparent Proxy, Firewall Proxy, HA Proxy (Load Balancer)

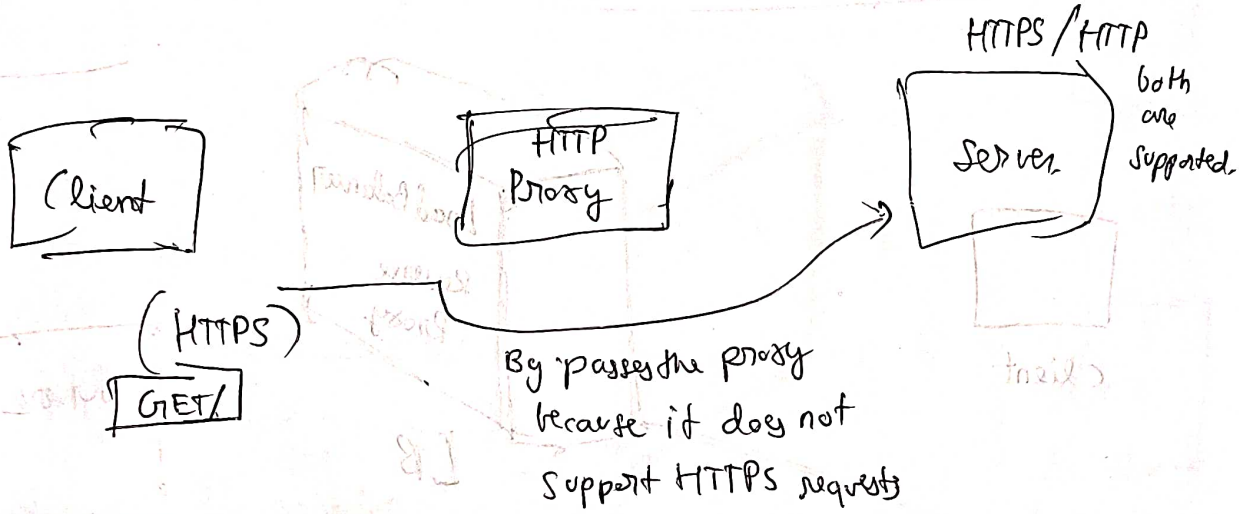
⇓

(Restrictions on ports)

- Used for many applications (Load Balancing, Service mesh, firewall proxy security → Check the port it wants to access and check if its a Restricted Port or not).

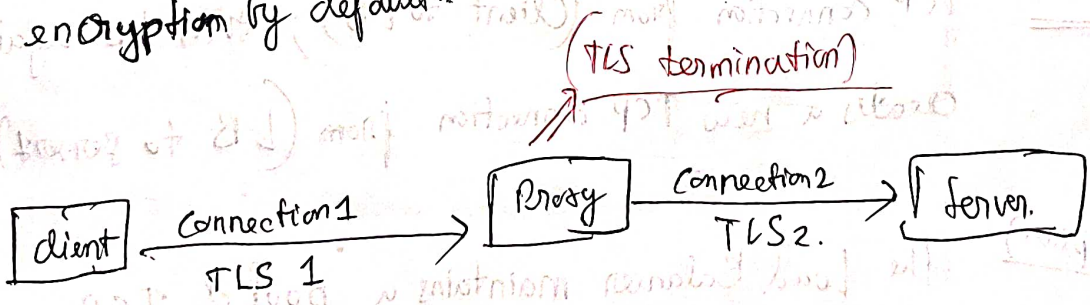
Proxy (Cons)

- Applications can bypass proxy.



- Not all traffic is routed. HTTP Proxy ⟹ routes only HTTP requests
  HTTPS Proxy ⇒ only forwards HTTPS requests

- No encryption by default:



So proxy is using its separate certifications and creating a new connection. Check who is issuing the certificate {🔒 → Lock sign}