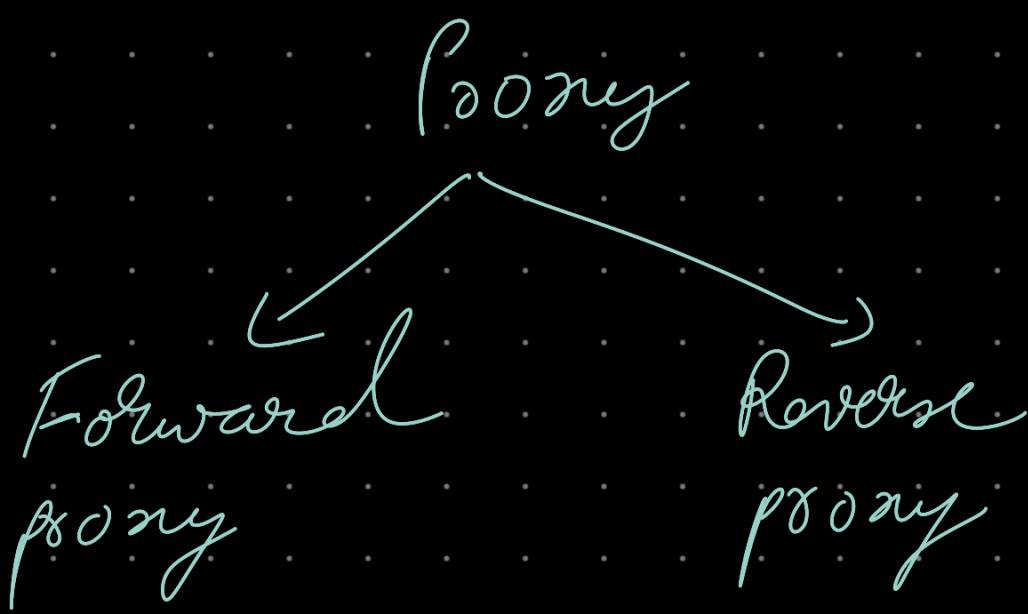
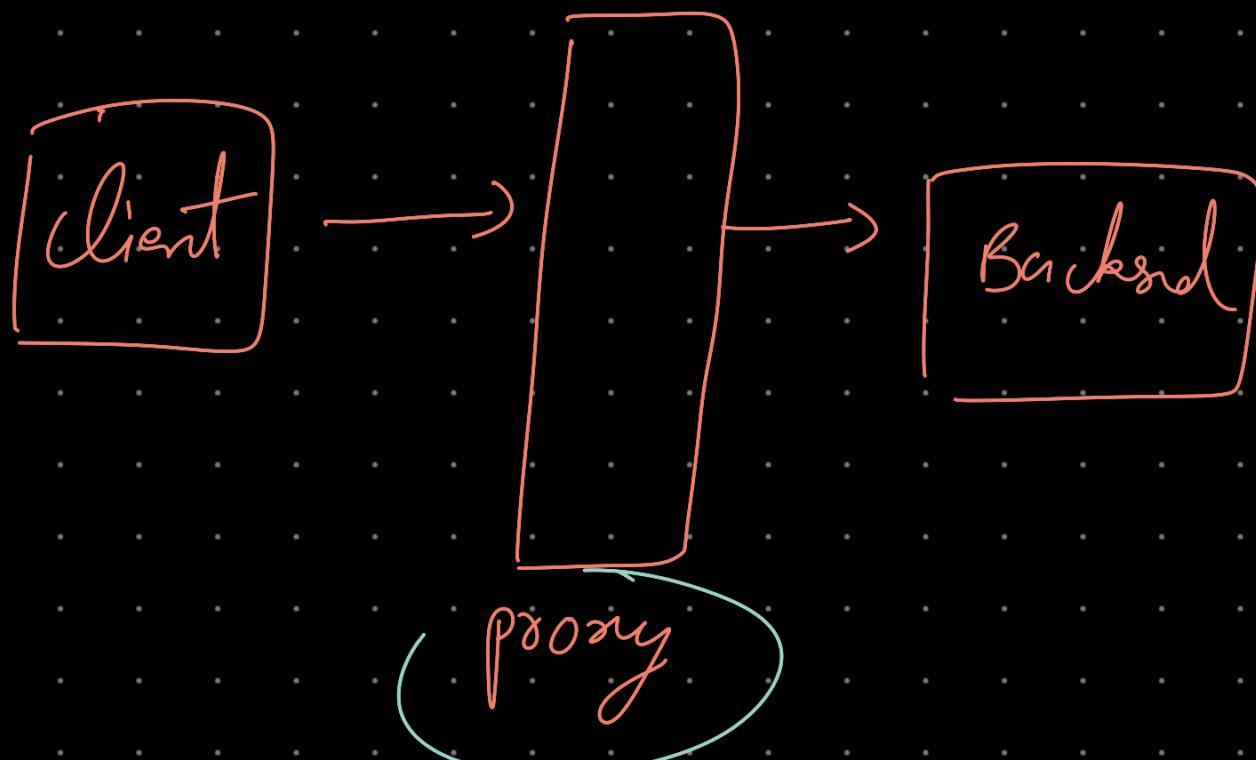


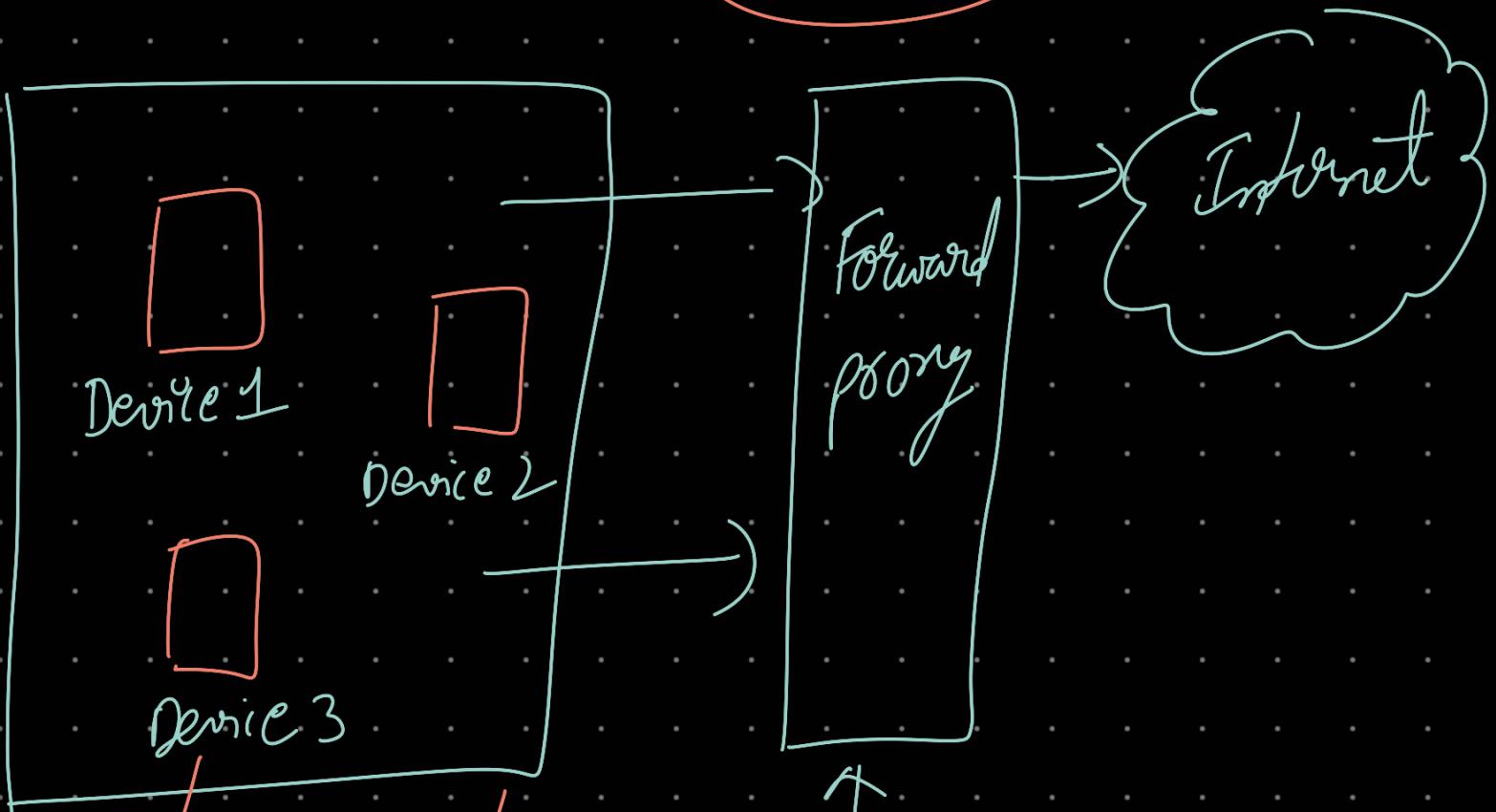
[Bony]

\* It's a machine / set of machines  
that sits b/w two systems

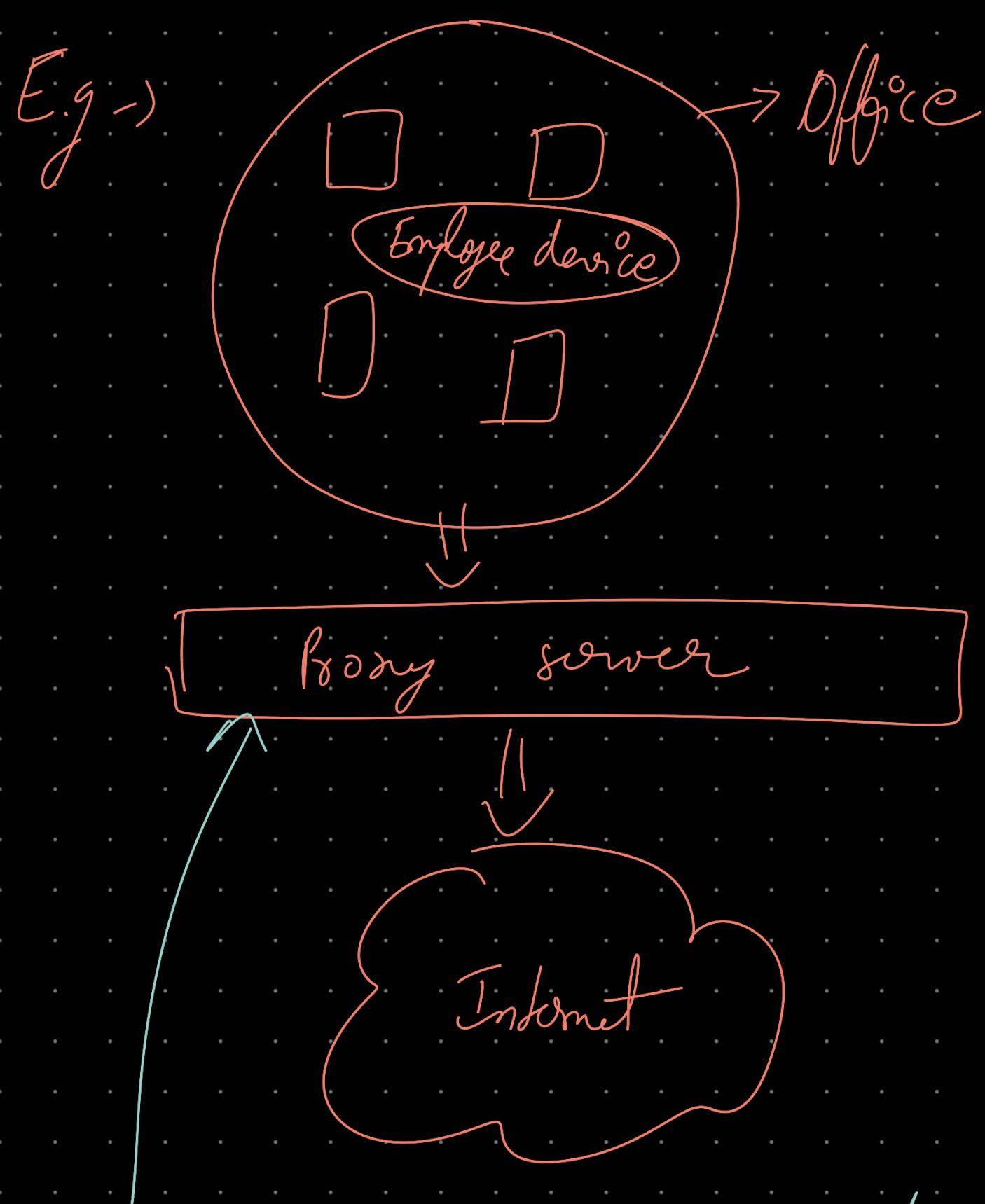


# Forward proxy

L, Abstract the clients



client identity  
is abstracted when https e.g  
is forwarded to internet  
Source IP in each packet  
is of proxy server

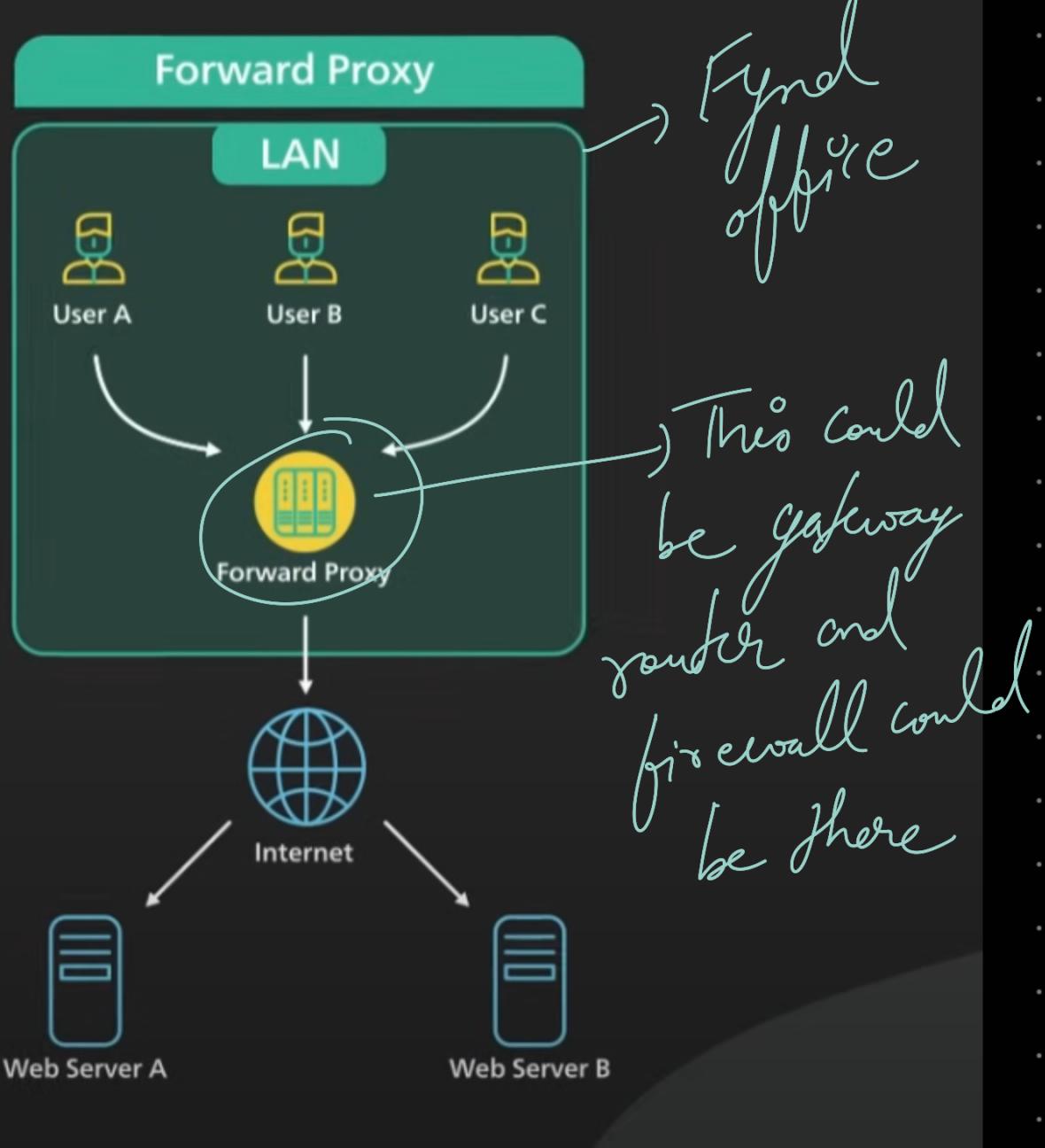


Office can block some websites  
to be accessed through office  
network

## Use Cases

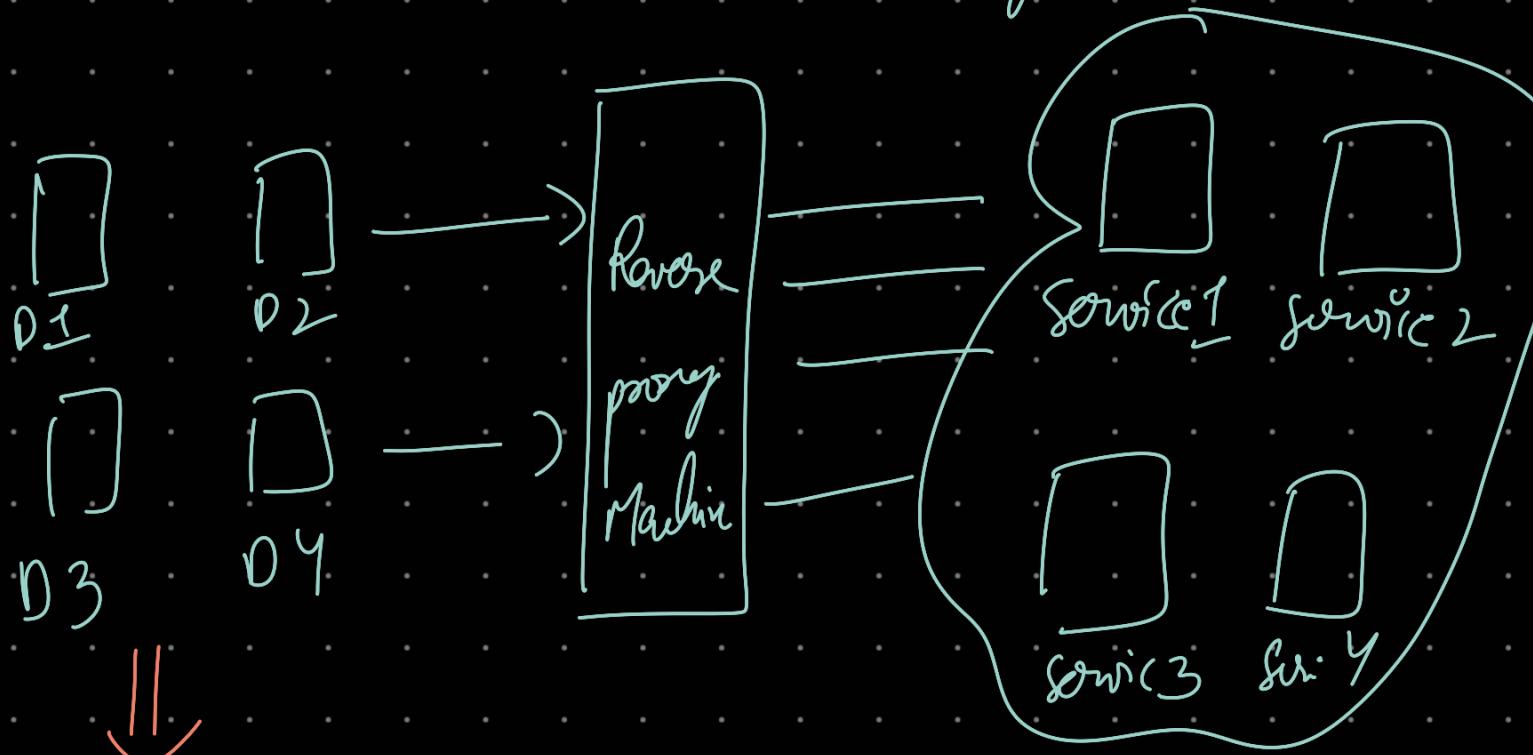
- ① Security → External network  
see proxy's IP
- ② Policies → Restrict access to  
some website
- ③ Caching → Cache some frequently  
accessed content on  
proxy server Machine





## [Reverse proxy]

↳ Abstracts downstream system

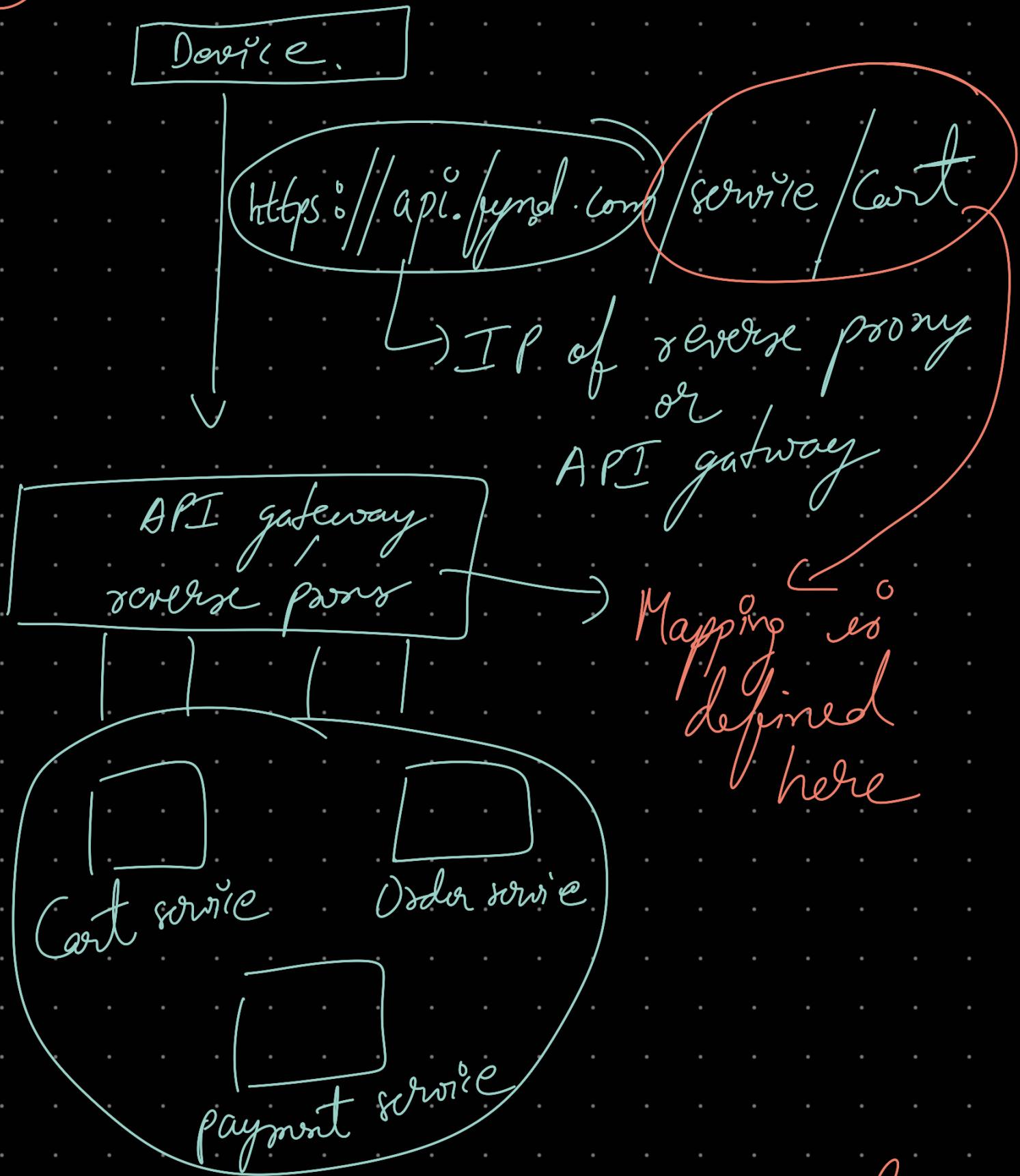


Client doesn't know complexity  
of downstream system

### Use Case

- ① Load balancing
- ② Routing
- ③ Caching

## ④ Abstraction



\* For client there is only one server which is actually

proxy server

https://api.fynd.com/service/cart

https://api.fynd.com/service/order

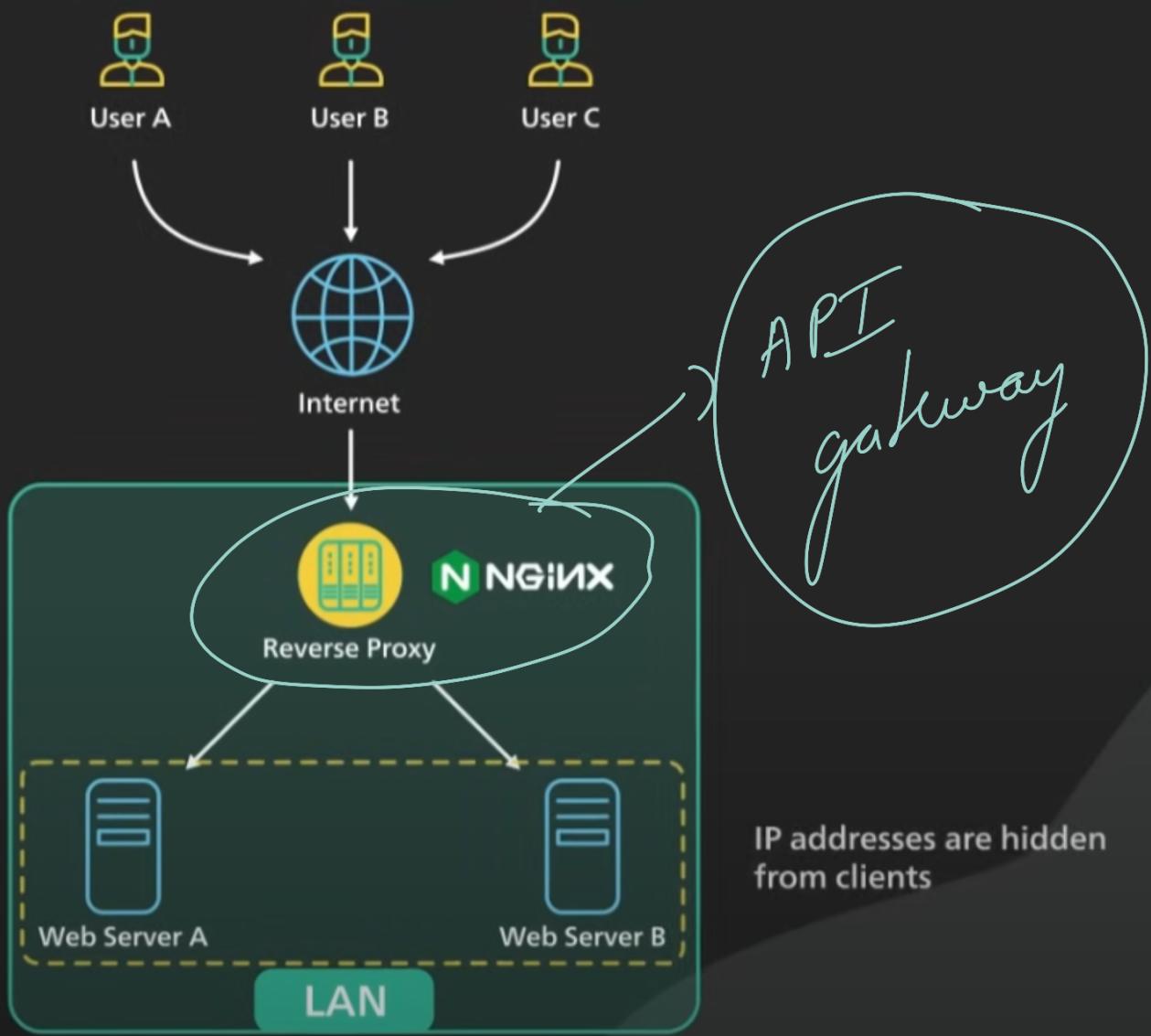
- ↳ Both seems like same server with two different routes
- ↳ seems like a monolithic server but actually could be

 Microservice → will go deep dive later

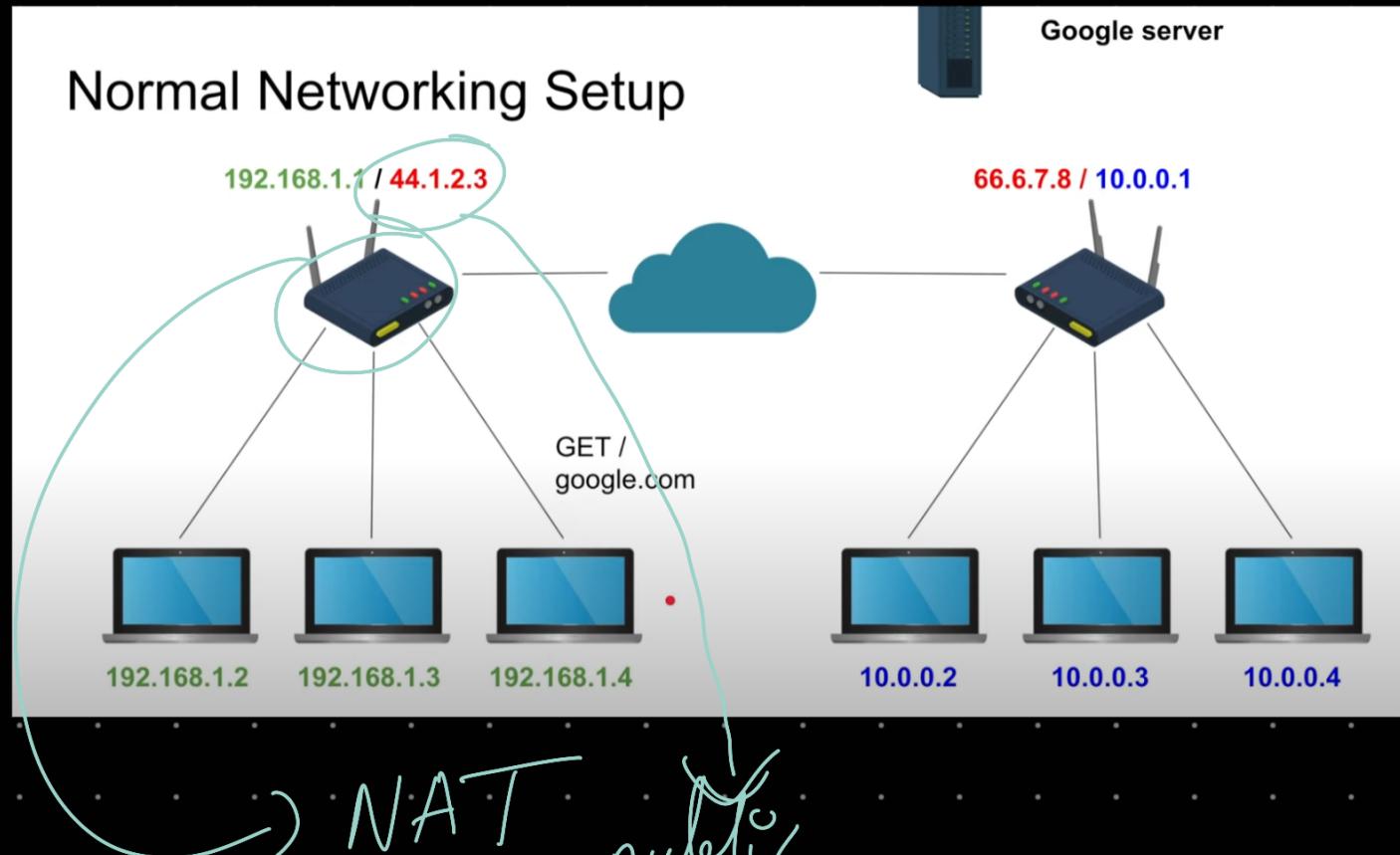
Eg → Nginx, API gateways.

## Reverse Proxy

- protects a web site



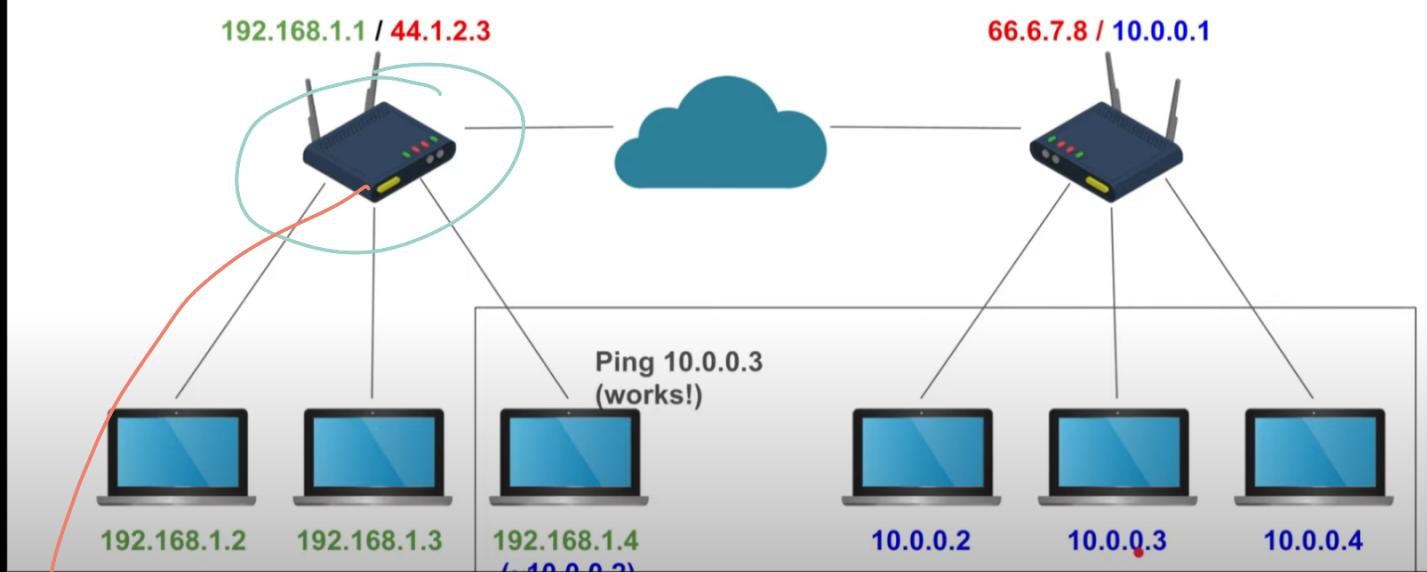
\* Is VPN same as Forward proxy?  
↳ short answer **No**.



→ NAT  
public IP of router

How VPN works

## How VPN works?



- ⇒ VPN use some protocol
- ⇒ our client connects to VPN server Machine
- ⇒ Any packet b/w our client and VPN is encrypted
- ) This server doesn't know we want to connect to 10.0.0.2  
    It connects to 66.6.7.8

II

Encryption of VPN packet is happening at client side, decryption is done at VPN server.

VPN server makes req to internet

So, client IP is anonymous

- ① Encrypts traffic
- ② Redirect all traffic at the lowest level
- ③ Access restricted content
- ④ Access private network
- ⑤ Very slow, too much hops

- \* VPN encrypts all your internet traffic, making it more secure
- \* Proxy only forwards specific requests without necessarily encrypting them.

## 1. Core Differences

Feature	VPN	Proxy
Purpose	Encrypts all internet traffic and provides privacy and security.	Routes specific traffic for anonymity or access control.
Scope	Operates at the <b>network layer</b> (system-wide).	Operates at the <b>application layer</b> (per app/browser).
Encryption	Encrypts all data between your device and the VPN server.	May not encrypt data (depends on proxy type).
IP Address Masking	Hides your IP address completely.	Hides your IP address for specific apps or traffic.
Performance	Slightly slower due to encryption overhead.	Generally faster (no encryption in most cases).
Device Coverage	Covers the entire device's internet traffic.	Typically configured for specific applications.
Security	Secures data from eavesdropping and hackers.	Limited security; primarily for IP masking.