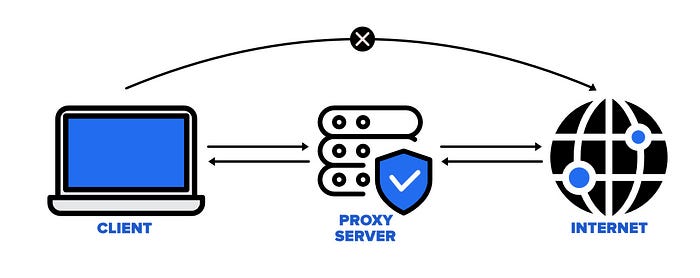
**FORWARD PROXY V/S REVERSE PROXY**

**What is a proxy?**

* A proxy plays a crucial role in enhancing security, managing traffic, and providing access to restricted content. *Proxies act as intermediaries between clients and servers.*

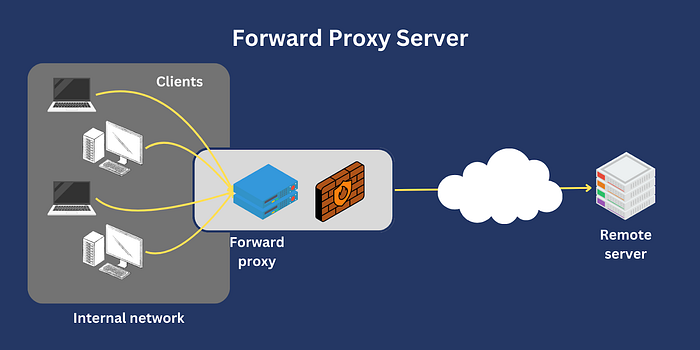
****

* There are two main types:  
  1. Forward proxy  
  2. Reverse proxy

***Let’s dive into each type and understand their functionalities.***

**1.*Forward Proxy***

* A *forward proxy* is a client-side proxy; it means only the client is aware of its existence. It acts on behalf of the client, making requests to the server. A common example of a forward proxy is a VPN (Virtual Private Network).

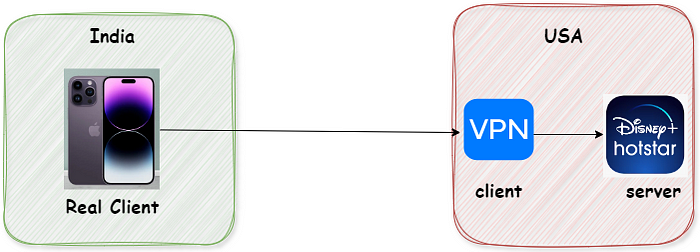
****

***Example:***

Imagine you want to watch content on Hotstar, but it’s only accessible from the United States. By using a VPN (Virtual Private Network), you can access the content from anywhere in the world. Here’s how it works:

* Client (Your Mobile Device): You download and install a VPN app.
* VPN: Your mobile sends the request to the VPN server, which then forwards it to Hotstar.
* Server (Hotstar): Hotstar sees the request coming from the VPN server, not your actual location.

In this scenario, your mobile is the real client, but for Hotstar, the VPN is the client. The VPN hides your identity and location, allowing you to access the restricted content.

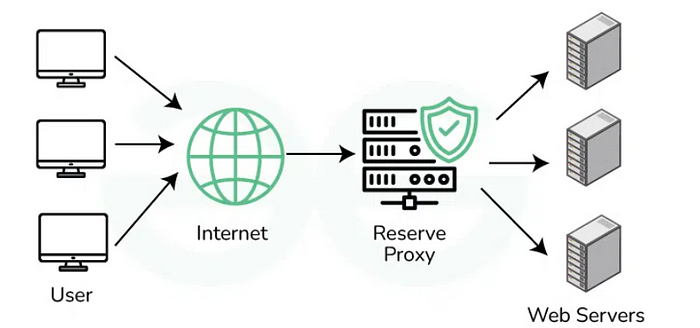
****

***Advantages of Forward Proxy:***

**1. *Access Restricted Content*:** Forward proxies allow users to bypass geo-restrictions and access content that may be restricted in their region. **2. *Change Geo-Location*:** Users can change their apparent location by routing their traffic through different proxy servers.  
**3. *Client-side Proxy*:** Only the client is aware of the proxy’s existence, which helps in maintaining user privacy.  
**4. *Hiding Client Identity*:** Forward proxies can mask the client’s identity, adding a layer of anonymity. **5. *Traffic Monitoring*:** Companies often use VPNs like Cisco VPN to monitor traffic and ensure secure connections.  
**6. *Secure Connections*:** VPNs establish secure connections, making it safer to access corporate resources remotely.  
**7. *Content Access Restriction*:** Companies can use VPNs to restrict access to certain websites on company devices.  
**8. *Caching*:** Forward proxies can be used to cache content, reducing load times and improving performance.

**2. Reverse Proxy**

* A *reverse proxy* is a server-side proxy; it means only the server is aware of its existence. It acts on behalf of the server, managing incoming requests from clients. Reverse proxies are powerful tools for load balancing, security, and SSL termination.

****

**Advantages of Reverse Proxy:**

**1. *Server-side Proxy*:** Only the server knows about the reverse proxy, which helps in managing traffic efficiently.  
**2. *Security*:** Reverse proxies add a layer of security between the client and the server, protecting sensitive data.  
**3. *Load Balancing*:** Reverse proxies distribute incoming traffic across multiple servers, preventing any single server from becoming overwhelmed. **4. *SSL Termination*:** Reverse proxy can handle SSL encryption, reducing the load on backend servers.

**Example:**

* *Nginx*is a popular reverse proxy server and load balancer. In AWS, the Application Load Balancer (ALB) is backed by Nginx, illustrating the power of reverse proxy servers.

**Understanding Load Balancers**

* A load balancer distributes incoming traffic among multiple servers, ensuring no single server is overwhelmed. This helps in maintaining performance and reliability.

**Nginx Configuration Essentials:**

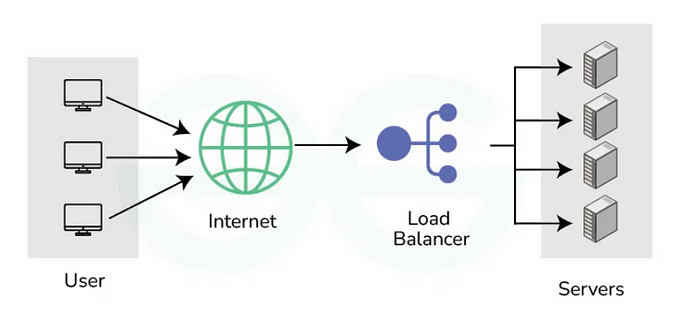
* When configuring Nginx as a reverse proxy, the default configuration file is located at **/etc/nginx/nginx.conf**
* For custom configurations, include additional settings, include **/usr/share/nginx/modules/\*.conf**

**Load Balancer Configuration Example: *→***To inform Nginx about multiple backend servers:

http {  
 upstream myproject {  
 server 127.0.0.1:8000 weight=3;  
 server 127.0.0.1:8001;  
 server 127.0.0.1:8002;   
 server 127.0.0.1:8003;  
 }  
  
 server {  
 listen 80;  
 server\_name www.domain.com;  
 location / {  
 proxy\_pass http://myproject;  
 }  
 }  
}

**Why Use a Load Balancer?**

A load balancer like Nginx distributes traffic across multiple servers, ensuring no single server is overwhelmed, which improves performance and reliability.

****

**Conclusion:**

Both forward and reverse proxies are essential in network management. A forward proxy serves the client by providing privacy, control, and access management. In contrast, a reverse proxy focuses on the server, offering load balancing, security, and performance optimization.