Forward Proxy And Reverse Proxy(正向代理和反向代理)

***正向代理（forward proxy）：***是一个位于客户端和目标服务器之间的服务器（代理服务器），为了从目标服务器取得内容，客户端向代理服务器发送一个请求并指定目标，代理服务器向目标服务器转交请求并将获得的内容返给客户端。

**例子**：如vpn科学上网、转发和重定向

**过程**：用户对国外网站的访问需要通过代理服务器来转发请求，并且该代理服务器也会将请求的响应返回给用户。

1. 客户端无法直接访问WEB服务器，但是代理服务器可以访问。
2. 代理server帮助client请求数据并缓存到本地，并将数据返回给client。

**注释**：client只需浏览器设置代理服务器ip和port即可，client知道代理服务器和WEB服务器的存在。

所以，正向代理其实是“代理服务器”代理了“客户端”，去和“目标服务器”进行交互。目标服务器并不知道正真的client是谁。

**用途**：

* 突破访问权限，如访问外网。
* 提高访问速度：代理服务器设置了较大的硬盘缓冲区，将部分请求的结果保存到缓冲区。
* 隐藏客户端的真实ip：client可通过这种方式隐藏自己的ip。

***反向代理（reverse proxy）：***指以代理服务器来接受Internet上的连接请求，然后将请求转发给内部网络上的服务器，并将返回结果返回给internet上请求连接的客户端，此时，作为客户端一方，代理服务器就像是替服务器端做代理服务，因此称为反向代理。

关键字：客户端、负载均衡服务器、服务器

1. client访问WEB服务器，并不知道访问的服务器是代理服务器，client以为代理服务器就是WEB服务器。
2. 代理服务器将WEB服务器的页面缓存到本地，当client访问时直接返回给client。

注释：client浏览器不需要做任何设置，client访问代理server就等同于访问WEB server，client不知道真实WEB server的存在。

**反向代理的用途：**

1. 隐藏服务器的真实ip：可对client隐藏服务器的ip地址
2. 负载均衡：根据所有真实服务器的负载情况，将请求分发到不同的服务器上
3. 提高访问速度：反向代理服务器能够将部分静态资源和短时间大量访问的资源缓存到本地，以提高访问速度。
4. 代理server可作为应用层防火墙，为网站提供对基于WEB的攻击行为的防护，还可以为后端服务器同意提供加密ssl加速，提供http访问认证等。

**总结：正向代理和反向代理的区别：**

1. 正向代理是客户端的代理（帮助客户端访问无法访问的资源），而反向代理则是服务器的代理（帮助服务器端做负载均衡，安全防护）。
2. 正向代理一般是客户端架设的，反向代理一般是服务器架设的。
3. 正向代理中，服务器不知道正真的客户端到底是谁；而反向代理中，客户端不知道真正的服务器是谁。
4. 正向代理用以解决访问限制问题；而反向代理用以提供负载均衡、安全防护等作用；二者均能提高访问速度。