## 正向代理的概念

正向代理,也就是传说中的代理,他的工作原理就像一个跳板,  
简单的说,  
我是一个用户,我访问不了某网站,但是我能访问一个代理服务器  
这个代理服务器呢,他能访问那个我不能访问的网站  
于是我先连上代理服务器,告诉他我需要那个无法访问网站的内容  
代理服务器去取回来,然后返回给我

从网站的角度,只在代理服务器来取内容的时候有一次记录  
有时候并不知道是用户的请求,也隐藏了用户的资料,这取决于代理告不告诉网站

结论就是 正向代理 是一个位于客户端和原始服务器(origin server)之间的服务器，为了从原始服务器取得内容，客户端向代理发送一个请求并指定目标(原始服务器)，然后代理向原始服务器转交请求并将获得的内容返回给客户端。客户端必须要进行一些特别的设置才能使用正向代理。

## 反向代理的概念

继续举例:  
例用户访问 http://ooxx.me/readme  
但ooxx.me上并不存在readme页面  
他是偷偷从另外一台服务器上取回来,然后作为自己的内容吐给用户

但用户并不知情  
这很正常,用户一般都很笨

这里所提到的 ooxx.me 这个域名对应的服务器就设置了反向代理功能

结论就是 反向代理正好相反，对于客户端而言它就像是原始服务器，并且客户端不需要进行任何特别的设置。客户端向反向代理 的命名空间(name-space)中的内容发送普通请求，接着反向代理将判断向何处(原始服务器)转交请求，并将获得的内容返回给客户端，就像这些内容 原本就是它自己的一样。

## 两者区别

从**用途** 上来讲：

正向代理的典型用途是为在防火墙内的局域网客户端提供访问Internet的途径。正向代理还可以使用缓冲特性减少网络使用率。反向代理的典型用途是将 防火墙后面的服务器提供给Internet用户访问。反向代理还可以为后端的多台服务器提供负载平衡，或为后端较慢的服务器提供缓冲服务。

另外，反向代理还可以启用高级URL策略和管理技术，从而使处于不同web服务器系统的web页面同时存在于同一个URL空间下。

从**安全性** 来讲：

正向代理允许客户端通过它访问任意网站并且隐藏客户端自身，因此你必须采取安全措施以确保仅为经过授权的客户端提供服务。

反向代理对外都是透明的，访问者并不知道自己访问的是一个代理。