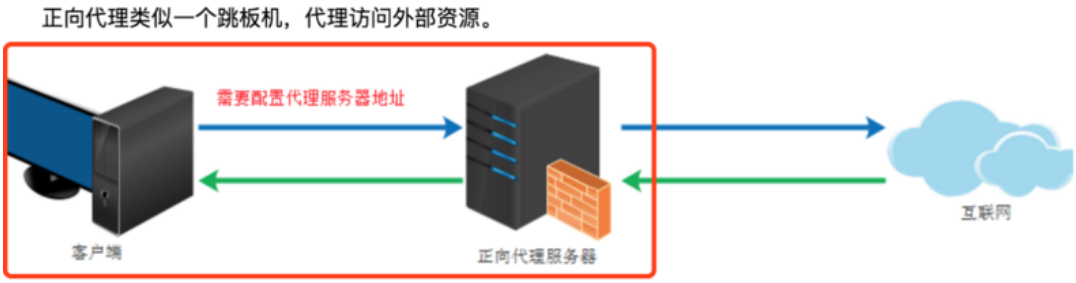
正向代理与反向代理

正向代理的基本概念

正向代理是一个位于客户端和原始服务器之间的服务器，为了从原始服务取得内容，客户端想代理发送一个请求并指定目标（原始服务器），然后代理服务器将这个请求转发给原始服务器（目标地址），然后从目标地址获得返回的数据，再转发会客户端，这样对于原始服务器来说，访问自己的就是代理服务器，客户端可以隐藏自己的身份，提高安全性。

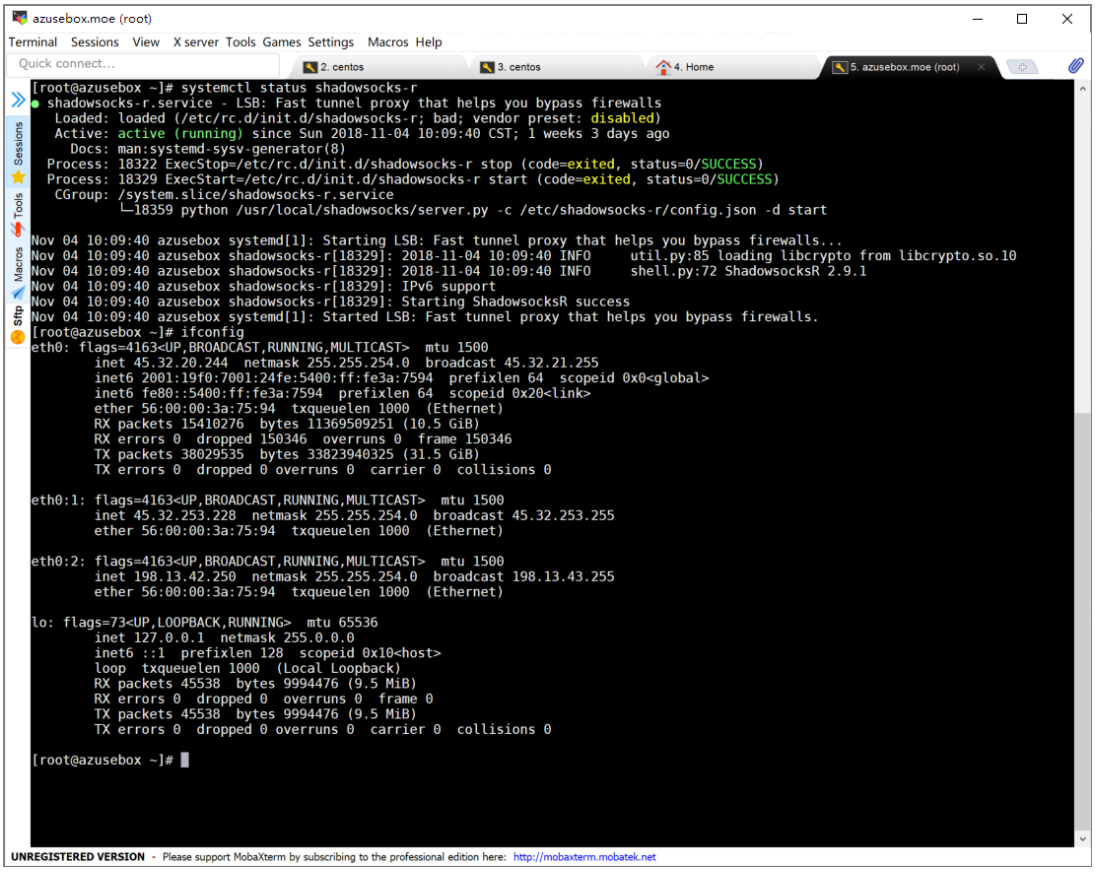
正向代理的工作原理



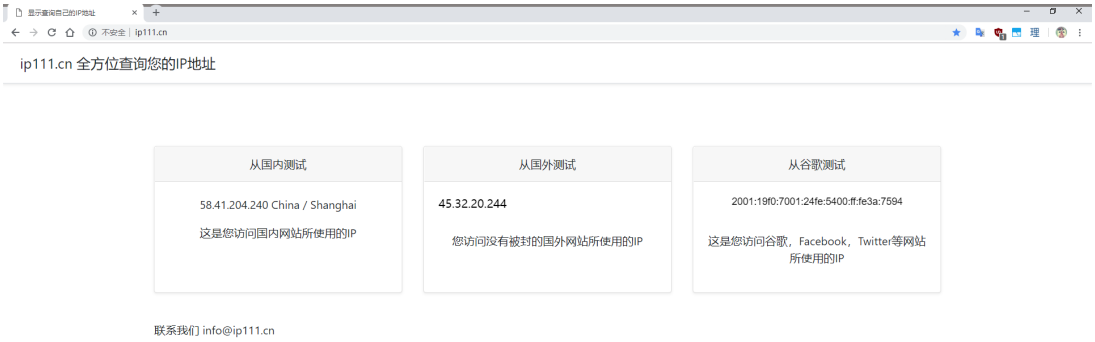
正向代理服务器代替客户端和目标服务器建立连接，相当于客户端把数据包发给正向代理服务器，正向代理服务器再根据包的目标地址发给互联网上的各个服务器

分析一个正向代理工作的实例

这是在我的远端服务器上的一个socks5代理：

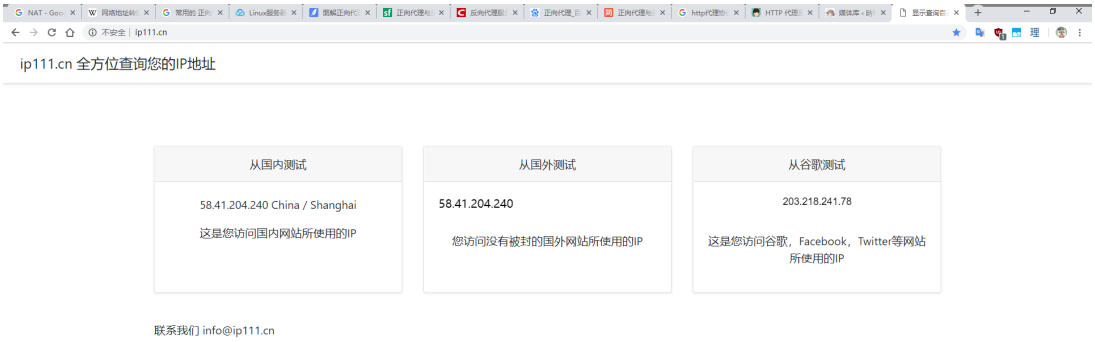


可以看到我的服务器的ipv4地址是45.32.253.255，还有一个ipv6地址是2001:19f0:7001:24fe:5400:ff:fe3a:7594
当我在电脑上设置使用这个代理时，远端服务器就会看到我的ip地址变成我的服务器的ip地址



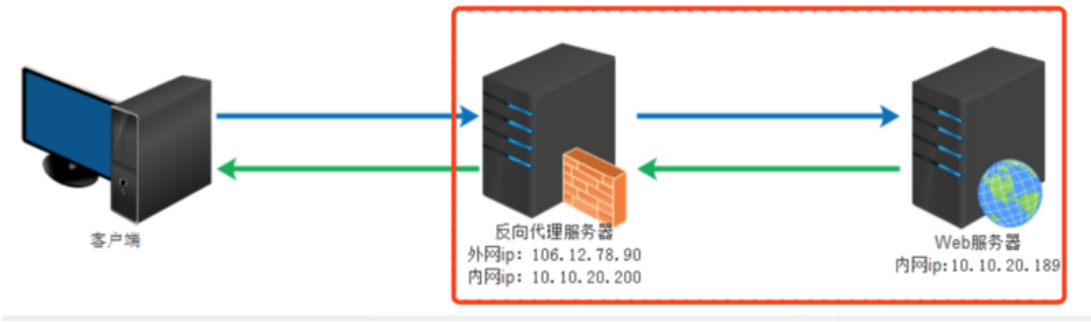
并且我现在可以使用代理服务器的ipv6地址访问ipv6网站了。

正常情况下我的ip地址：



这个socks5正向代理的原理就是把我电脑上所有的http和https链接都转发到了我的服务器上，再从我的服务器上和目标服务器建立链接，当然代理的过程肯定不是直接发送的，中间还有很多加密、混淆等等算法来保证代理的运行速度和安全性。

反向代理的基本概念



正向代理需要客户端的浏览器设置代理服务器之后才能正常使用，但是反向代理不同，反向代理对于客户端来说是透明的。
正向代理可以为在防火墙内的局域网提供访问Internet的途径，而反向代理可以把防火墙后面的服务器提供给Internet访问同时还可以完成诸如负载均衡等功能

反向代理的工作原理

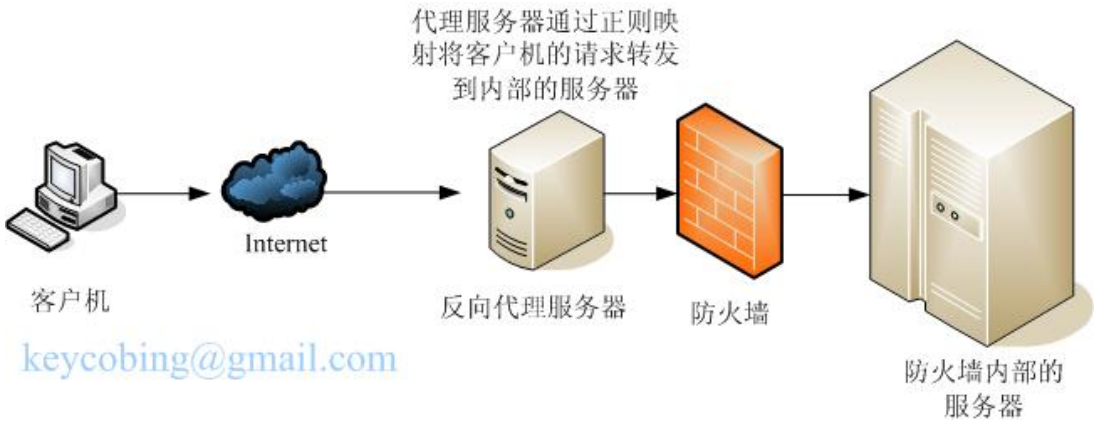
反向代理服务器通常有两种模型，它可以作为内容服务器的替身，也可以作为内容服务器集群的负载均衡器。

1，作内容服务器的替身

如果您的内容服务器具有必须保持安全的敏感信息，如信用卡号数据库，可在防火墙外部设置一个代理服务器作为内容服务器的替身。当外部客户机尝试访问内容服务器时，会将其送到代理服务器。实际内容位于内容服务器上，在防火墙内部受到安全保护。代理服务器位于防火墙外部，在客户机看来就像是内容服务器。

当客户机向站点提出请求时，请求将转到代理服务器。然后，代理服务器通过防火墙中的特定通路，将客户机的请求发送到内容服务器。内容服务器再通过该通道将结果回传给代理服务器。代理服务器将检索到的信息发送给客户机，好像代理服务器就是实际的内容服务器（参见图 2）。如果内容服务器返回错误消息，代理服务器会先行截取该消息并更改标头中列出的任何 URL，然后再将消息发送给客户机。如此可防止外部客户机获取内部内容服务器的重定向 URL。

这样，代理服务器就在安全数据库和可能的恶意攻击之间提供了又一道屏障。与有权访问整个数据库的情况相对比，就算是侥幸攻击成功，作恶者充其量也仅限于访问单个事务中所涉及的信息。未经授权的用户无法访问到真正的内容服务器，因为防火墙通路只允许代理服务器有权进行访问。

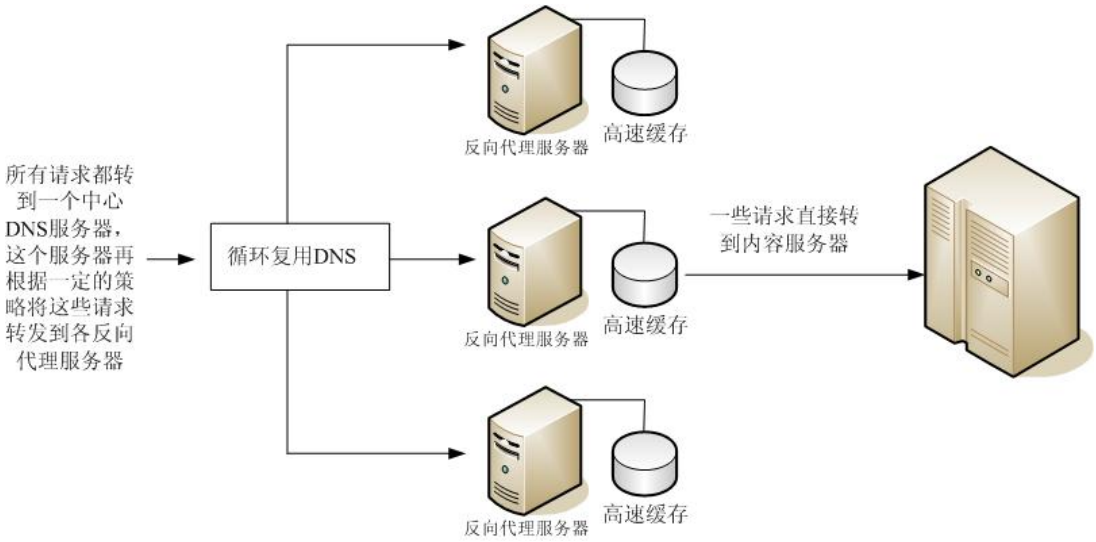


2，作为内容服务器的负载均衡器

可以在一个组织内使用多个代理服务器来平衡各 Web 服务器间的网络负载。在此模型中，可以利用代理服务器的高速缓存特性，创建一个用于负载平衡的服务器池。此时，代理服务器可以位于防火墙的任意一侧。如果 Web 服务器每天都会接收大量的请求，则可以使用代理服务器分担 Web 服务器的负载并提高网络访问效率。

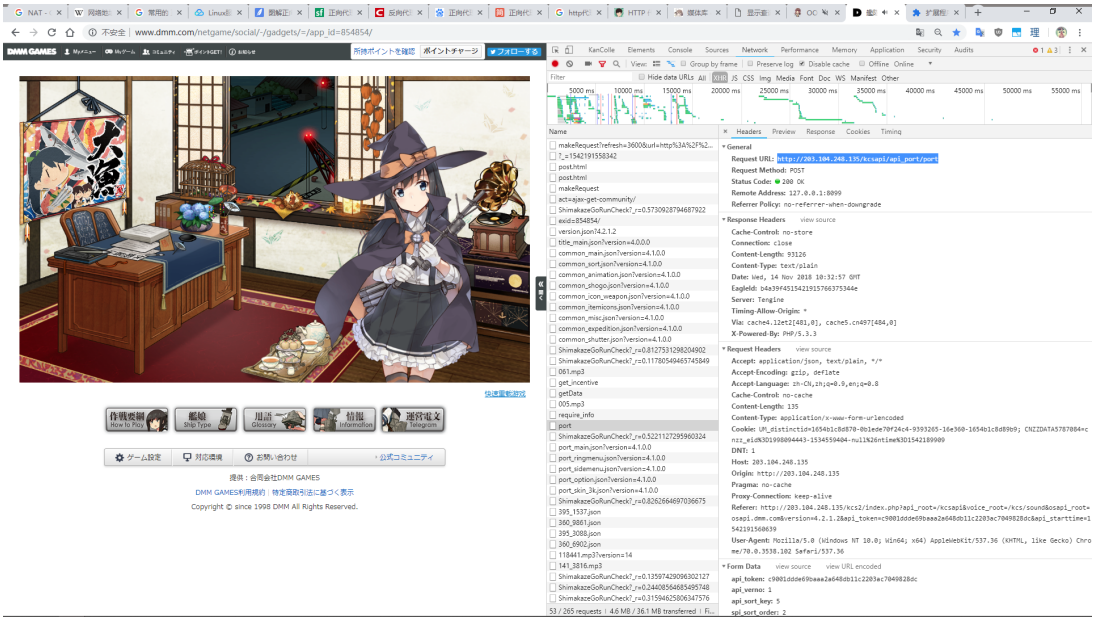
对于客户机发往真正服务器的请求，代理服务器起着中间调停者的作用。代理服务器会将所请求的文档存入高速缓存。如果有不止一个代理服务器，DNS 可以采用“循环复用法”选择其 IP 地址，随机地为请求选择路由。客户机每次都使用同一个 URL，但请求所采取的路由每次都可能经过不同的代理服务器。

可以使用多个代理服务器来处理对一个高用量内容服务器的请求，这样做的好处是内容服务器可以处理更高的负载，并且比其独自工作时更有效率。在初始启动期间，代理服务器首次从内容服务器检索文档，此后，对内容服务器的请求数会大大下降。



分析一个反向代理的实例

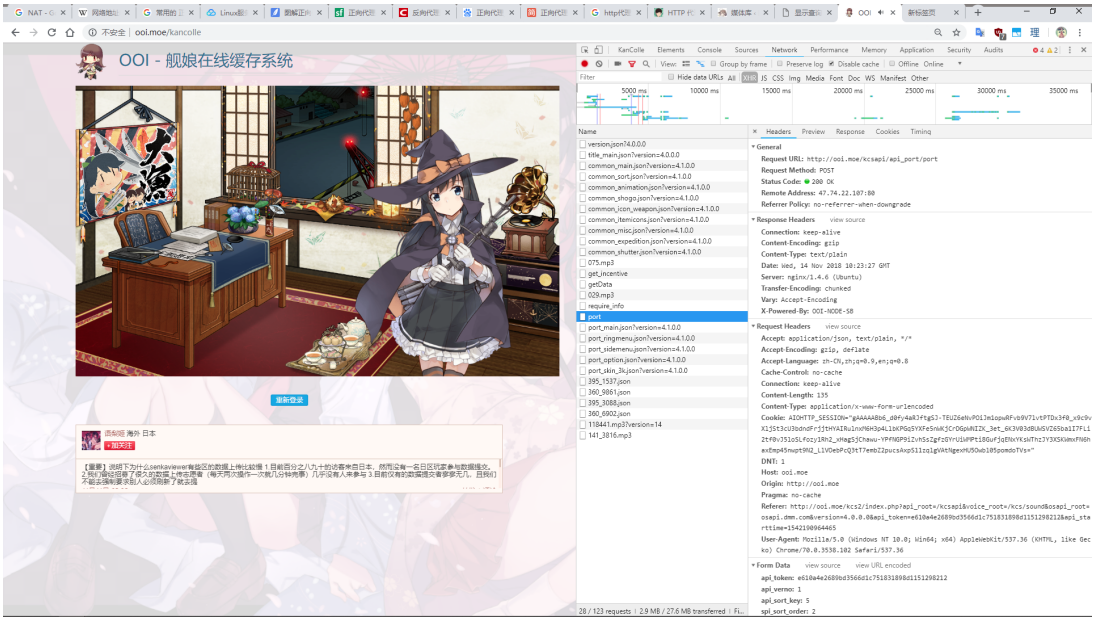
舰队收藏是一个因为某些原因只能使用日本ip访问的网页游戏，为了正常访问这个游戏，身在中国大陆的玩家开发出了许多正向代理、反向代理方法。



使用正向代理访问dmm.com的游戏页面，这是游戏的官方页面，可以看到后台中发送的api地址也是官方的一个后端地址203.104.248.135

这是使用正向代理访问的dmm.com，对于客户端也就是我来说，我访问的还是dmm.com，只不过是从我的正向代理服务器绕了一圈；而对于dmm.com的服务器来说，链接到dmm.com的客户端并不是我，而是我的有日本ip的代理服务器，所以他也不会ban掉我的代理服务器，这样我就可以正常访问了。

但是使用正向代理需要设置客户端，比较麻烦，维护成本也较高。于是有人开发了针对舰队收藏的反向代理服务器：http://ooi.moe/kancolle



从截图上可以看出，在使用反向代理链接dmm.com时，我并不是直接在浏览器输入dmm.com的地址，而是需要访问ooi的反向代理服务器ooi.moe，然后ooi.moe的网站后台会帮我转发我的http包，从一个拥有日本ip的服务器发出，与dmm.com建立链接。从开发者工具中可以看出此处网页向后端发送post请求的地址也不再是官方的203.104.248.135，而是ooi.moe，这样ooi也可以帮我转发游戏过程中发送的所有post和get请求了。将不同目标地址的post和get分别转发到dmm，或是203.104.248.135，或是别的官方后端接口；再将他们的回复转发回来给我，这样我就可以通过ooi正常访问dmm了。

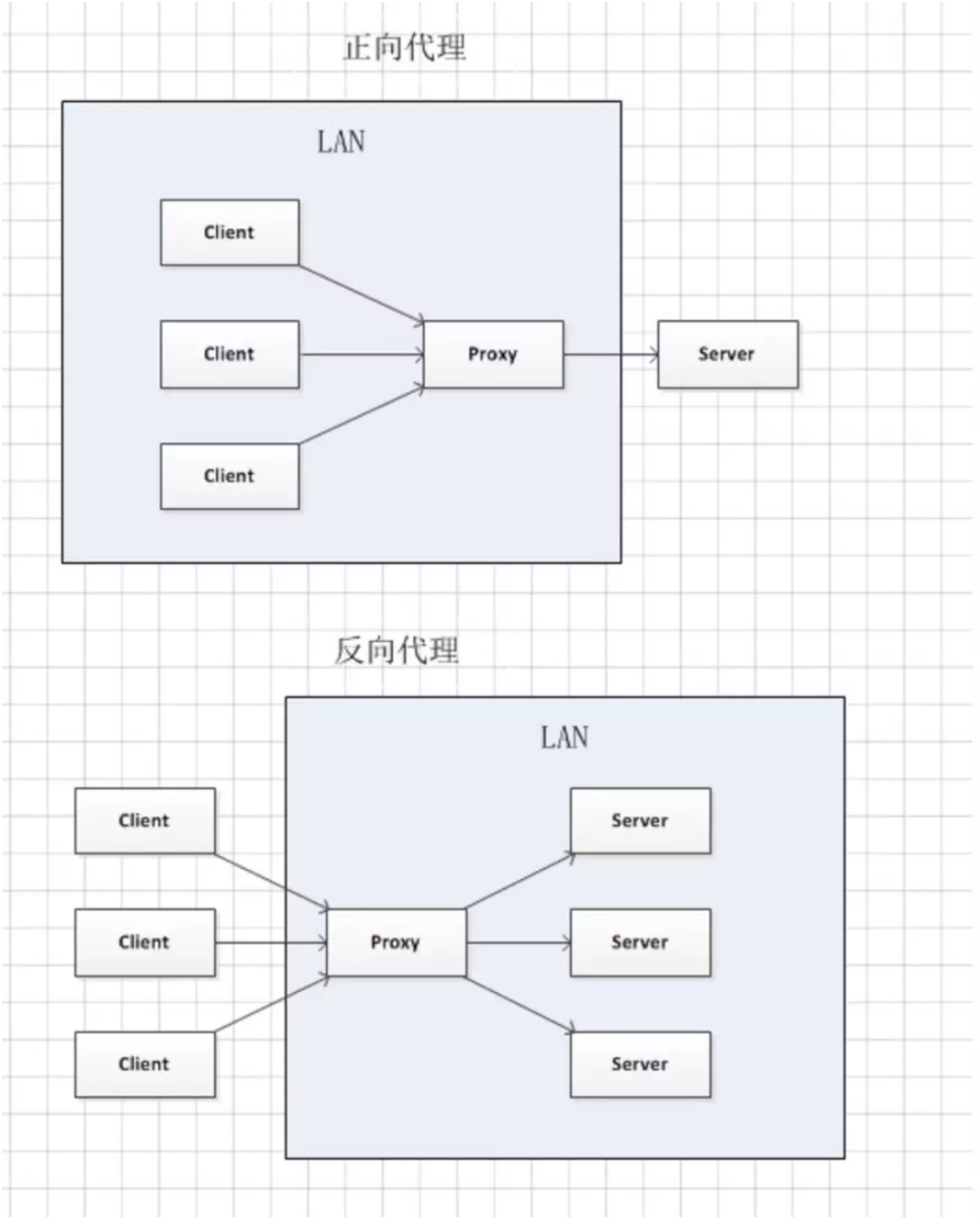
正向代理和反向代理的区别

正向代理需要你主动设置代理服务器ip或者域名进行访问，由设置的服务器ip或者域名去获取访问内容并返回；而反向代理不需要你做任何设置，直接访问服务器真实ip或者域名，但是服务器内部会自动根据访问内容进行跳转及内容返回，你不知道它最终访问的是哪些机器。

正向代理是代理客户端，为客户端收发请求，使真实客户端对服务器不可见；而反向代理是代理服务器端，为服务器收发请求，使真实服务器对客户端不可见。

从上面的描述也能看得出来正向代理和反向代理最关键的两点区别：

- 是否指定目标服务器
- 客户端是否要做设置



正向代理中，proxy和client同属一个LAN，对server透明； 反向代理中，proxy和server同属一个LAN，对client透明。 实际上proxy在两种代理中做的事都是代为收发请求和响应，不过从结构上来看正好左右互换了下，所以把前者那种代理方式叫做正向代理，后者叫做反向代理。

从用途上来区分：

- 正向代理：正向代理用途是为了在防火墙内的局域网提供访问internet的途径。另外还可以使用缓冲特性减少网络使用率。
- 反向代理：反向代理的用途是将防火墙后面的服务器提供给internet用户访问。同时还可以完成诸如负载均衡等功能。

从安全性来讲：

- 正向代理：正向代理允许客户端通过它访问任意网站并且隐蔽客户端自身，因此你必须采取安全措施来确保仅为经过授权的客户端提供服务。
- 反向代理：对外是透明的，访问者并不知道自己访问的是代理。对访问者而言，他以为访问的就是原始服务器。