



































需要说明的是

1. 前置代理服务器和后置代理服务器的区别

前置代理服务器就是将你的ip更换,使得你所用的访问请求都是通过前置代理服务器进行转发,前置代理服务器目前主要支持的代理有http和socket5,前置代理服务器的主要应用是更改请求目标网站的ip.

后置代理服务器的作用是将所有的请求都发送到后置代理服务器上,后置代理服务器将请求的结果返回给你,,但是不必考虑后置代理服务器的访问逻辑.后置代理服务器的主要应用是负载均衡器和cdn(内容转发网络).

前置代理服务器和后置代理服务器的区别是

前置代理服务器是更换ip,突破ip封锁,

后置代理是访问固定ip,隐藏内在逻辑.

值得说明的是 http,socket5,shadowsocket都是通过前置代理功能实现的网络访问.

1. 网络结构的说明.
2. 笔记本电脑处于10局域网段,局域网中开启了IP隔离,也就是局域网中不同的ip不能相互访问,
3. 局域网限制了对公网ip的访问,访问公网ip只能通过代理服务器,
4. Dns服务器是 10.88.1.1 这个应该边界的根dns服务器,没有进行dns污染.
5. 国外的vps主机在国内的公网环境下,可以正常通信.
6. 二级代理模式下Pac模式代理失效,也就是说baidu使用pac模式无法登陆,但是使用全局模式baidu可以登录,但是显示的是国外服务器ip

由于网络结构的原因,局域网ip不能直接访问公网,如果访问公网只能通过代理服务器进行访问,所以当开启shadowsocket的时候,shadowsocket修改的就是电脑的代理设置,也就是说将原先设置的公司代理服务器地址覆盖,所以当采用pac模式的时候,访问本机的1080端口,就相当于局域网直接访问公网地址,虽然可以得到dns解析,但是由于公网ip的显示,所以pac模式失效.

但是,如果采用全局模式,一切访问都是通过公司代理->国外代理,所以可以访问pac列表内的网站,但是由于是全局代理,所以ssl通信将所有的流量都是通过国外的服务器访问,所以访问百度的时候会显示国外的ip

1. 本机的网络连接的说明

由于使用了两个前置代理服务器的组合使用,第一个使用http代理,之后使用ssl 加密通道,

1. 在本机的监听端口上和直接使用ssl加密通道的端口情况没有任何区别,本机还是监听1080端口
2. 但是本机和ssl通过的tcp连接,就转接到http服务器上,导致了本机和公司代理服务器建立了很多tcp连接,推想可知,公司http代理服务器也一定和国外的vps服务器奖励了大量的tcp连接,再推想,如果很多人同时使用这个代理服务器翻墙,那么正常国内上网的人应该会很卡,因为端口有限,需要等待空闲的端口被释放,国内上网 的人才能获得连接.
3. 本机中其他使用集成http代理软件的说明.

本机中比如其他使用http上网的qq,微信,网易云,由于已经手动设置了http代理,那么他们的通过将不再经过国外的服务器,而是由公司的代理服务器直接一级代理直接上网,不需要二级代理翻墙.

1. Http前置代理和ssh可靠性连接的通信过程是怎么的

在进行二级代理,翻墙的时候,先使用http 一级代理获得访问公网的权限,再使用ssh二级代理获得访问外网的权限,

连接具体建立的过程是

1. 使用http向国外的vps服务器发送 http connect请求,然后国外vps服务器 返回 http establish 结果.

此时国内的代理服务器和国外的vps服务器之间已经建立了一条http

1. 国内的电脑使用 ssl格式,经过http代理服务器的转发,和国外服务器使用ssl进行通过,

此时的通信内容是加密的,但是dns请求是收到监控的

QA1 HTTP代理服务器可能监控的到ssl的内容?

由于http代理服务器的转发作用,也就是说http代理服务器的请求所有的通信方式都是通过http进行访问的,也就是说他们是可以监控的到http请求的报文体的,但是由于报文体里面的内容是通过ssl加密传输的,所以即使监控的到,但是也不是明文传输.