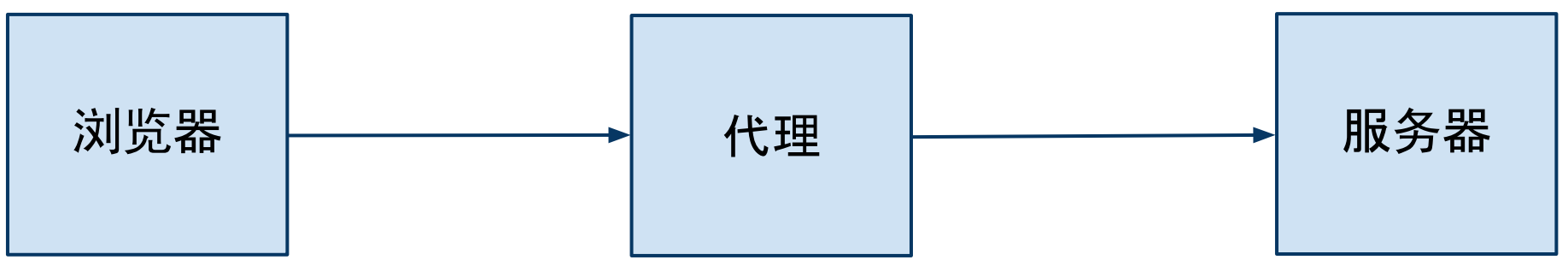
一种翻墙方法

http over http

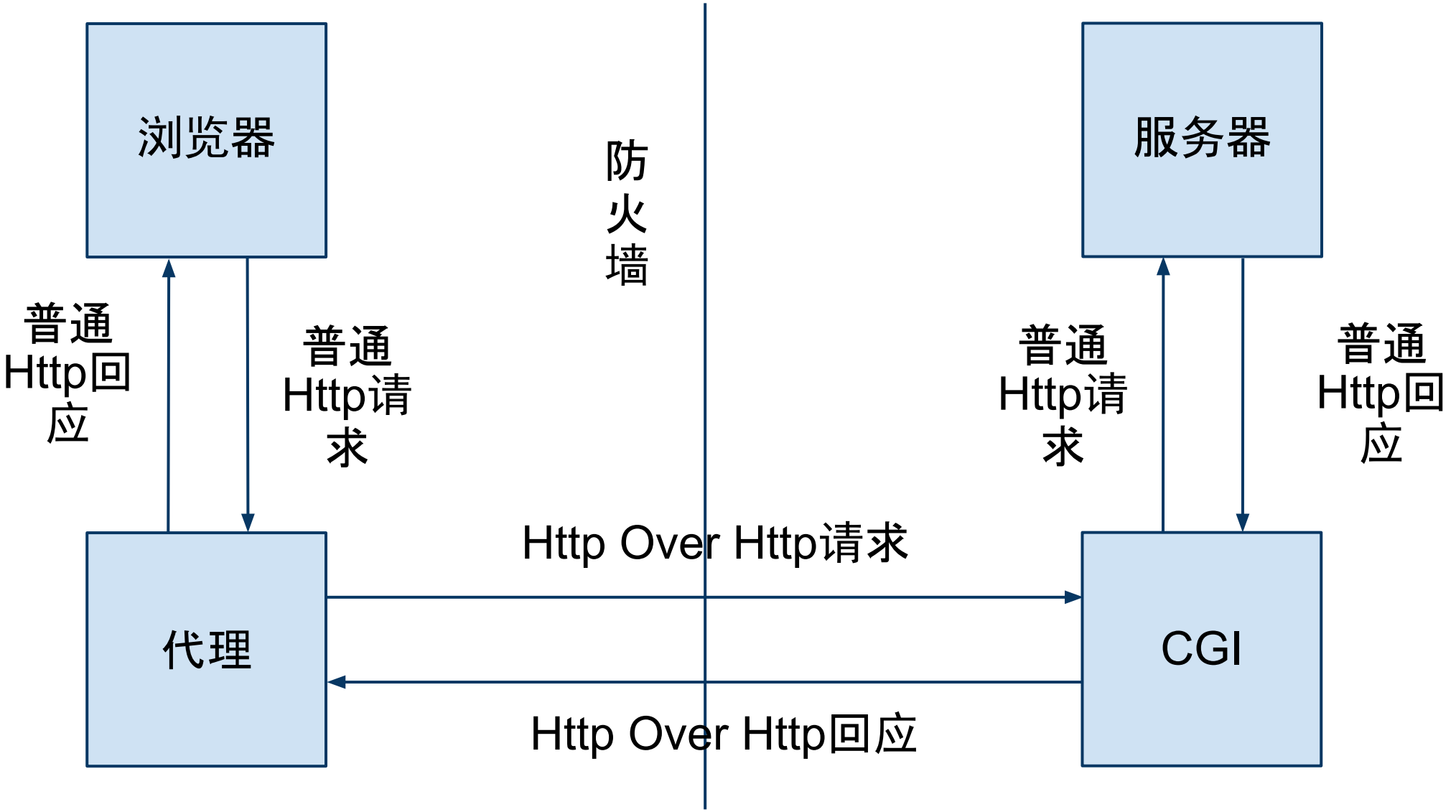
简述

Http Over Http是一种由墙外cgi代理请求的双重代理转发模式，一般由墙外有cgi服务器者向无cgi服务器者分发服务。推荐一个站点支持不超过10人的翻墙业务，对支持站点不构成太大影响。为了支持此点，需要支持请求/回应级别的身份验证。

普通Http请求过程



Http Over Http请求过程



特性

由于协议的源端和目标端均为标准的http，因此预期兼容性很好。而中间请求使用标准http，变化其请求特征，使防火墙难于和上千万普通请求区别。

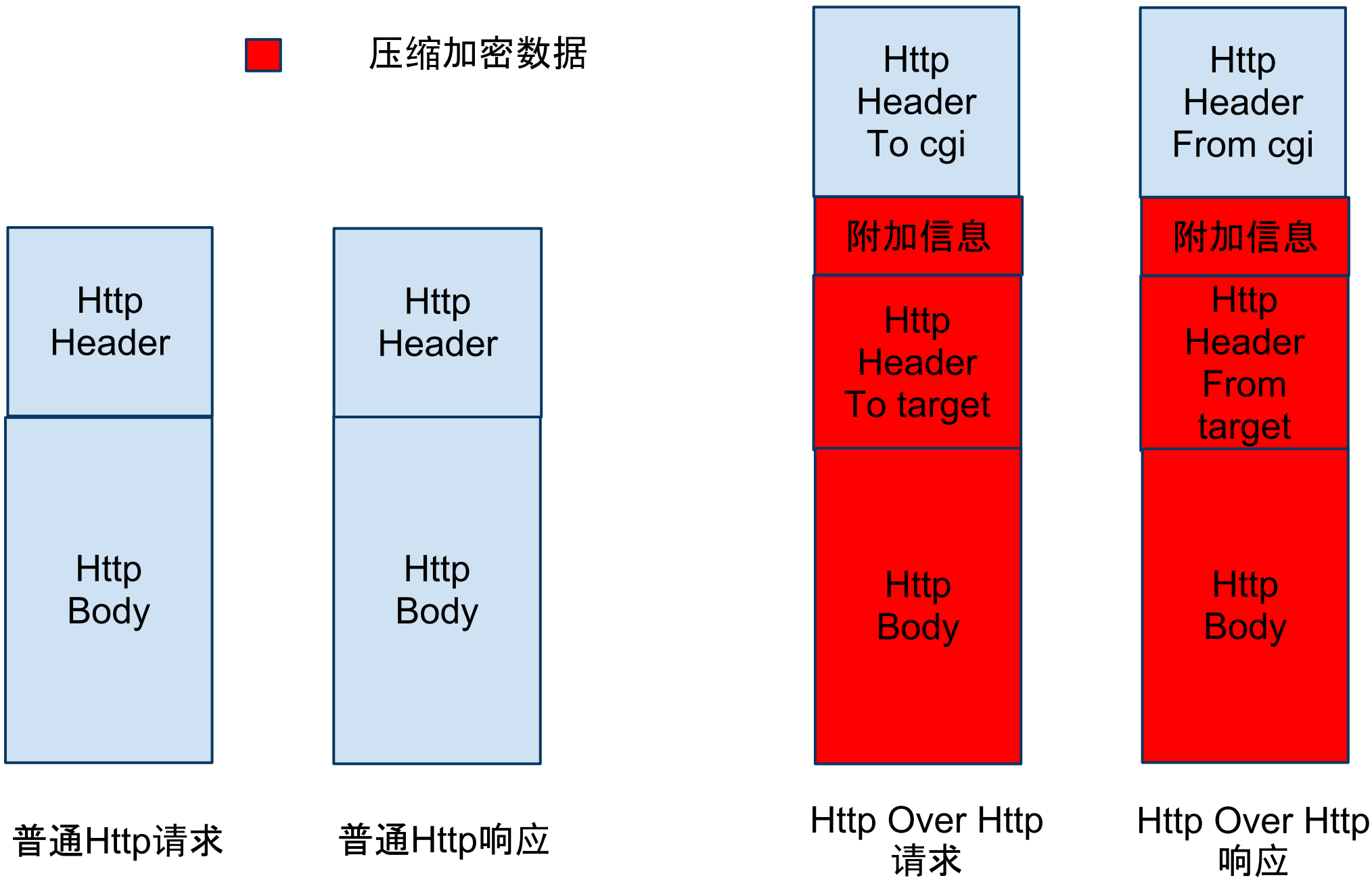
加密和压缩模式由提供者和使用端双方约定，因此即使要深度检测也需要付出许多的额外资源。

Http Over Http不提供对内容的深度加密，也无法保证内容不被截获嗅探。

对比

	成本	机密性	匿名性	稳定性	封锁难度
VPN	100-200/年	高(支持Https协议)	弱	好	容易 等同于封锁所有VPN类业务
SSH等加密代理	10-100/年 多人共享账户有安全问题 滥用SSH容易引发服务商不满	高(支持Https协议)	弱	好	中 等同于封锁所有SSH类业务
Http Over Http	0-20/年	低(不支持Https协议)	弱	中 随着cgi服务器压力而变化	难 等同于封锁所有网页业务
Tor	0	高(支持Https协议)	强	差 随着网桥数和封锁情况而变化	容易 默认网桥目录已经被封锁

Http Over Http封包



分析

Http Over Http的真正意义是允许国外的上万站长，以他们的网站，向可信的人提供翻墙服务。减小翻墙开销，从而增大翻墙用户，或者迫使防火墙被迫提高判断难度。包括增加资源做深度包解析，或者封锁上万小站点。

性能瓶颈和增强分析

Http协议本来就不快，Http Over Http更慢。所以需要使用一些方法增强性能。经过分析，hoh的性能瓶颈主要来自每次执行开销和并发限额。

每次执行开销指hoh过程中，每次必须独立创建连接，无法使用长连接技术。而且在正常http过程外还多了cgi服务器连接/进程创建/关闭的开销。

并发限额指，webhosting业者往往会限制同时可以执行的cgi数额。例如目前用于测试的服务器只支持20个进程的限额，还有部分要用于ssh转发，因此实际只有10个可用。

要解决上述问题，关键就是减少cgi请求数，在一次请求内附加多个http请求/回应。这一问题非常类似于tcp的nagle算法。

经过修改的Http情况见下页。

Http Over Http请求合并