说说这次出现的原因，一开始接收到客户反馈不能上传文件和图片等问题，一开始以为是jq插件编辑器的问题，但经过不断的调试和修改里面的相应上传文件选项都没有效果，进一步怀疑是服务器上传大小的限制，因为之前也遇到过相应的问题，但随着更改设置的同时，也发现并不是上传大小的问题。以前也未曾出现过这类的问题，发现在本地服务器测试是可以上传，没有问题的。

那么，进一步想到会不会是没有服务器上操作访问权限的问题，但是在服务器上相应的文件设置下，也没有得到解决，通过对IIS上目录等设置权限，也无法解决。后发现，因为是使用学校的服务器，在另一服务器上，也是出现不能上传文件的问题，后来咨询老师，发现是学校的网络安全策略正在发生改变。

网络访问控制策略是网络安全防范和保护的主要策略，其任务是保证网络资源不被非法使用和非法访问。各种网络安全策略必须相互配合才能真正起到保护作用，而访问控制是保证网络安全最重要的核心策略之一。访问控制策略包括入网访问控制策略、操作权限控制策略、目录安全控制策略、属性安全控制策略、网络[服务器](http://product.yesky.com/service/)安全控制策略、网络监测、锁定控制策略和[防火墙](http://product.yesky.com/hardwarefirewall/)控制策略等7个方面的内容。

因为上传文档的时候editor反馈回来的信息也是非法访问或者url攻击的信息，也验证确实是学校的网络策略发生了变化。但其具体设置了哪方面的策略，不是很清楚，似乎对html的标记也进行了过滤，提交信息中若存在html标签的信息，也是被禁止上传和提交。

大概是对防火墙的策略做了更改吧，向学校那边反馈过后，上传的问题得到解决，但是html标签的问题还是存在，那么我们团队制作的网站还是无法使用，无奈的情况下，也只能迁移，或者对输入的信息先进行一遍过滤。

但从这次的故障排查中，也发现了一些知识要点，比如是可以通过设置相应的网络访问控制策略对客户机做出一些限制，以前未曾想过这些问题，只是简单的知道防火墙防止一些带有攻击性的包进行过滤，未曾想过可以对客户端访问服务器的操作权限，以及服务器上的目录文件客户端是否有访问权限进行设置，对客户端上传文件也能做出限制，也粗略的了解了一下关于网络服务器策略和网络策略的知识。