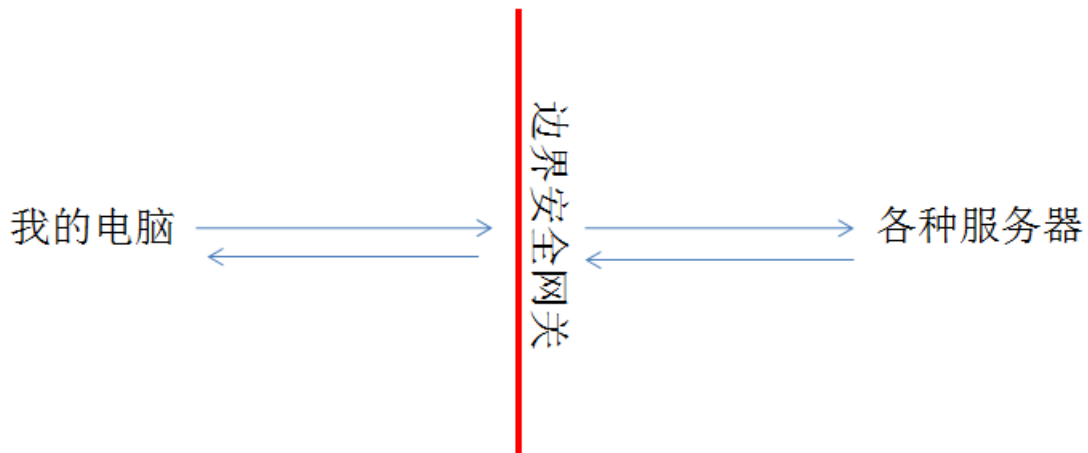


现在公司内部有很多同事反应电脑经常出现异常的断网行为,而且断网频率较高很影响工作情绪。现在我基于对此类问题的总结把这个问题跟大家剖析分享一下,希望帮助有问题的同学尽快摆脱阴影,没有问题的同学防患于未然。

起因:

1. 在了解这个问题前给大家看一张上网过程的简图



2. 从上面的图上看我们的电脑在上网访问互联网各种服务器的时候都要经过一个叫边界安全网关的东西,这个东西呢其实就是我们常说的防火墙,他的作用是我们内外部网络的桥梁也是一道内外部之间的一道安全屏障,出于不同的安全防护目的上面有很多安全策略,当然让我们产生断网现象的策略也在上面
3. 让我们产生断网的策略应用在我们一个叫做内网防护的安全模块上面,这个策略依据特定的协议去匹配我们设定的安全阈值然后智能的、动态的去识别威胁,然后出于防护目的进行临时性的惩罚性的短暂断网(原则上是永久性直到威胁被确认解决)
4. 哪些情况容易被惩罚性的断网呢? 下面一些行为习惯会造成如此
 - a. 安装流氓软件、访问流氓网站
 - a. 使用 P2P 下载工具
 - b. 安全防护工具使用不当,比如使用 360 安全管家、腾讯安全管家、百度安全管家等(公司要求每一台公司机器均需要安装公司指定的 ESET)
 - c. 浏览器中有恶意插件

5. 该怎么解决或者规避这样被封网的困扰
- b. 在管理员侧应该为用户提供纯净的没有污染的操作系统
 - c. 在管理员侧应该为用户安装纯净的没有第三方插件的办公软件和其他软件
 - d. 在管理员侧应该为用户安装公司安全部门指定的防毒软体
 - e. 在用户使用侧应该注重甄别不良的软件下载和安装(重点是非技术部门), 安装需要应该第一时间联系支持工程师协助甄别
 - f. 在用户使用侧在上网过程中应该甄别恶意网站、邮件附件等如有网络上的下载需求应该尽量在大型的、具有权威性的网站下载
 - g. 在用户使用侧在使用办公机器进行高频的网络压力测试时应该提前报备或者尽量使用非办公网络环境的测试服务器进行