简易CC攻击防御方法

1. 利用Session做访问计数器：

利用Session针对每个IP做页面访问计数器或文件下载计数器，防止用户对某个页面频繁刷新导致数据库频繁读取或频繁下载某个文件而产生大额流量。（文件下载不要直接使用下载地址，才能在服务端代码中做CC攻击的过滤处理）

2. 把网站做成静态页面：

大量事实证明，把网站尽可能做成静态页面，不仅能大大提高抗攻击能力，而且还给骇客入侵带来不少麻烦，至少到现在为止关于HTML的溢出还没出现，看看吧！新浪、搜狐、网易等门户网站主要都是静态页面，若你非需要动态脚本调用，那就把它弄到另外一台单独主机去，免的遭受攻击时连累主服务器。

3. 增强操作系统的TCP/IP栈

Win2000和Win2003作为服务器操作系统，本身就具备一定的抵抗DDOS攻击的能力，只是默认状态下没有开启而已，若开启的话可抵挡约10000个SYN攻击包，若没有开启则仅能抵御数百个，具体怎么开启，自己去看微软的文章吧！《强化 TCP/IP 堆栈安全》。也许有的人会问，那我用的是Linux和FreeBSD怎么办？很简单，按照这篇文章去做吧！《SYN Cookies》。

4. 在存在多站的服务器上，严格限制每一个站允许的IP连接数和CPU使用时间

这是一个很有效的方法。CC的防御要从代码做起，其实一个好的页面代码都应该注意这些东西，还有SQL注入，不光是一个入侵工具，更是一个DDOS缺口，大家都应该在代码中注意。举个例子吧，某服务器，开动了5000线的CC攻击，没有一点反应，因为它所有的访问数据库请求都必须一个随机参数在Session里面，全是静态页面，没有效果。突然发现它有一个请求会和外面的服务器联系获得，需要较长的时间，而且没有什么认证，开800线攻击，服务器马上满负荷了。代码层的防御需要从点点滴滴做起，一个脚本代码的错误，可能带来的是整个站的影响，甚至是整个服务器的影响!

5. 服务器前端加CDN中转

(免费的有百度云加速、360网站卫士、加速乐、安全宝等)，如果资金充裕的话，可以购买高防的盾机，用于隐藏服务器真实IP，域名解析使用CDN的IP，所有解析的子域名都使用CDN的IP地址。此外，服务器上部署的其他域名也不能使用真实IP解析，全部都使用CDN来解析。

另外，防止服务器对外传送信息泄漏IP地址，最常见的情况是，服务器不要使用发送邮件功能，因为邮件头会泄漏服务器的IP地址。如果非要发送邮件，可以通过第三方代理(例如sendcloud)发送，这样对外显示的IP是代理的IP地址。

总之，只要服务器的真实IP不泄露，1OG以下小流量DDOS的预防花不了多少钱，免费的CDN就可以应付得了。如果攻击流量超过20G，那么免费的CDN可能就顶不住了，需要购买一个高防的盾机来应付了，而服务器的真实IP同样需要隐藏

简易CC攻击防御策略

确定Web服务器正在或者曾经遭受CC攻击，那如何进行有效的防范呢?

(1).取消域名绑定

一般cc攻击都是针对网站的域名进行攻击，比如我们的网站域名是“www.abc.com”，那么攻击者就在攻击工具中设定攻击对象为该域名然后实施攻击。对于这样的攻击我们的措施是取消这个域名的绑定，让CC攻击失去目标。

(2).域名欺骗解析

如果发现针对域名的CC攻击，我们可以把被攻击的域名解析到127.0.0.1这个地址上。我们知道127.0.0.1是本地回环IP是用来进行网络测试的，如果把被攻击的域名解析到这个IP上，就可以实现攻击者自己攻击自己的目的，这样他再多的肉鸡或者代理也会宕机，让其自作自受。

(3).更改Web端口

一般情况下Web服务器通过80端口对外提供服务，因此攻击者实施攻击就以默认的80端口进行攻击，所以，我们可以修改Web端口达到防CC攻击的目的。运行IIS管理器，定位到相应站点，打开站点“属性”面板，在“网站标识”下有个TCP端口默认为80，我们修改为其他的端口就可以了。

(4).屏蔽IP

我们通过命令或在查看日志发现了CC攻击的源IP，就可以在防火墙中设置屏蔽该IP对Web站点的访问，从而达到防范攻击的目的。

————————————————————

https://blog.csdn.net/qq_34777600/article/details/81978262