DDOS 攻击防御策略

一、攻击原理

CC 攻击的原理就是攻击者控制某些主机不停地发大量数据包给对方服务器造成服务器资源耗尽，一直到宕机崩溃。CC 主要 是用来攻击页面的，每个人都有这样的体 验：当一个网页访问的人数特别多的时候，打开网页就慢了，CC 就是模拟多个用户(多少线程就是多少用户)不停地进行 访问那些需要大量数据操作(就是需要 大量 CPU 时间)的页面，造成服务器资源的浪费，CPU 长时间处于 100%，永远都有处理不完的连接直至就网络拥塞， 正常的访问被中止。

二、攻击症状

CC 攻击有一定的隐蔽性，那如何确定服务器正在遭受或者曾经遭受 CC 攻击呢?我们可以通过以下方法来确定。

进入控制面板节点信息界面，点击连接信息的详情，这里我们能一目了然的看到当前的网站连接状态，若网站正在遭受 CC 攻击，这里的连接数特别是同一个 URL 的链接超出正常数量。

CC 攻击是 DDOS(分布式拒绝服务)的一种，相比其它的 DDOS 攻击 CC 似乎更有技术含量一些。这种攻击你见不到虚假 IP，见不到特别大的异常流 量，但造 成服务器无法进行正常连接，听说一条 ADSL 足以搞掂一台高性能的 Web 服务器。由此可见其危害性，称其为“Web 杀手”也毫不为过。最让站长们 忧虑的 是这种攻击技术含量低，利用工具和一些 IP 代理一个初、中级的电脑水平的用户就能够实施攻击。因此，大家有必要了解 CC 攻击的原理及如果发现 CC 攻 击和 对其的防范措施。

demo.yundun.cn节点[115.238.236.237]的连接信息

当前连接数: 10921

源地址	时间	状态	Method	网址
110.11.94.82:1601	5	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
112.165.106.177:4862	6	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
211.107.45.146:3963	5	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
183.96.53.94:1818	6	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
118.40.131.130:3717	5	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
121.133.4.200:1306	5	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
175.215.41.113:2736	6	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
58.102.135.209:4784	6	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
14.47.167.36:3503	6	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
175.203.240.68:2790	6	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
110.11.94.82:1525	6	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
211.107.45.146:3970	5	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1
59.13.183.101:4881	6	idle	GET	http://demo.yundun.cn/index.php?c=article&a=type&tid=1

如上图所示，针对上图连接的请求数量达到了上万，这明显是不正常连接。另外还可以观察网站的源服务器 CPU 状态，w3wp/mssql /mysql 进程是否占用 CPU 超高，IIS 一停止，服务器状态就恢复正常。这些都是 CC 攻击的症状。

三、CC 攻击防御策略

确定了网站正在或者曾经遭受 CC 攻击，那如何进行有效的防范呢?云盾简单几步操作轻松解决 CC 攻击。

进入用户控制面板——安全——安全配置——防 CC 攻击配置。勾选防 CC，勾选放行搜索引擎，我这里的配置是请求数 90，秒数 20，点击保存后立即生效，如下图：

开启了防 CC 后，当有访客访问网站的时候，云盾会自动检测访客的行为，如果访客的访问有可能是 CC 攻击时（比如短时间 内重复刷新页面），就会生成一个 JavaScript 页面，自动跳转到当前页面加一个随机参数的地址，如：demo.yundun.cn/?ydkey=x4g1a；如果该访客（有可能 是肉鸡）的确是正在 CC 攻击我们的网站，将不会跳转到对应的加了参数的页面（因为一般 CC 攻击时，攻击者 只发送访问这个页面的请求，而不管页面返回的是 什么，所以不会跳转），于是就可以判断是被攻击从而屏蔽该访客的 IP 一段时间。而上图中所示的 20 秒 90 次 的意思是，当网站的某个 URL 在 20 秒内被访 问了 90 次，则会自动针对这个 URL 开启防护，假如这里的 2 个参数都设置为 0，那就是全站无条件开启防护。传 统的防火墙他只能针对全站开启防护，并且通 过限制单一 IP 的访问频率来达到防护的目的。而云盾的下一代云防火墙通过云端的智能策略，真正做到 0 误封，动态 防御。

过滤后的连接数：

说到这里，如果对 SEO 有一定了解的朋友一定会问，这样的防御方式，不就会阻碍搜索引擎蜘蛛访问我们网站？当然是不会 的啦，云盾内部默认自动放行所有蜘 蛛。在防御 CC 攻击的同时不影响搜索引擎蜘蛛正常访问我们的网站。并且云盾的高级套餐有针对指纹码过滤方式防御更高级的 CC 攻击，云端自动抓取攻击特征 码，自动过滤含有特征的报文，采用更复杂的机制来判断是否正被攻击。