* **CC攻击与ddos攻击**

1. **安域抗DDOS原理，以及与其他公司流量清洗服务的优势**

安域的流量清洗服务覆盖4层以下及7层流量清洗。通过云端LVS负载集群实现TCP\UDP\ICMP等流量清洗，通过云端CDN节点实现HTTP的7层流量清洗，比传统运营商覆盖面更全。并且安域和运营商之间也可以进行流量清洗的联动，通过安域识别攻击IP，调用运营商能力在骨干网封锁攻击IP，已经有过多次和运营商联动的成功案例。

安域是基于云端防护节点，数千台防护设备、分布式流量调度，全国最大的防护带宽储备（1T），绿盟等的设备是布在网络入口，而网络入口是有限的，当攻击超过网络入口流量时设备就会成为性能瓶颈，严重影响业务正常访问。

1. **CC攻击原理**

CC = Challenge Collapsar，意为“挑战黑洞”，其前身名为Fatboy攻击，是利用不断对网站发送连接请求致使形成拒绝服务的目的。业界赋予这种攻击名称为CC（Challenge Collapsar，挑战黑洞），是由于在DDOS攻击发展前期，绝大部分都能被业界知名的“黑洞”（Collapsar）抗拒绝服务攻击系统所防护，于是在黑客们研究出一种新型的针对http的DDOS攻击后，即命名ChallengeCollapsar，声称黑洞设备无法防御，后来大家就延用CC这个名称至今。

CC攻击是DDOS（分布式拒绝服务）的一种，其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。

1. **CC攻击处置方式**

1、开启拦截策略情况下，自动判断攻击行为，自动进行拦截ip，cc攻击时系统需要3秒钟进行一次检测，检测为cc攻击的ip，系统会根据攻击情况分等级封禁ip 5分钟—6小时左右。

2、系统自主判断目前的攻击情况，动态调整策略，根据多维度判断，自动开启HTTP验证，JS防御或者图片验证码防御，无固定阈值。

3、也支持手动自定义固定流量阈值和请求阈值，自动触发JS防御或者图片验证码防御。

4、支持手动配置并发策略。