不同套餐对应的测试节点

检测工具

http://jk.anquan.io/check\_cdn\_health.html 免费版

http://jk.anquan.io/check\_cdn\_health.html?1 专业版

http://jk.anquan.io/check\_cdn\_health.html?2 商务版

<http://jk.anquan.io/check_cdn_health.html?3> 企业版

kibana 日志查询

domain: 域名 AND 状态 AND request:”url”

domain:www.81.cn AND status:503 AND request:” /gjzx/2016-08/23/content\_7219669.htm” (按查看某个子域名指定url 访问503的情况)

domain:\*.81.cn AND status:503(查看该域名下所有子域名访问503的情况)

host：主机名 And 状态

host:cnc-tj-125-039-005-045 AND status:503 (查看节点访问503的情况)

1.免费节点的分布位置

天津联通

山东联通

重庆联通

河南联通

河南电信

湖北电信

广东电信

浙江电信

免费套餐只支持联通电信，不支持移动以及其他

2.牛盾为什么不接入未备案的域名

因为国内工信部对域名有需要备案的要求，若网站无备案，会封IP，同时会封掉牛盾节点的IP。

3.牛盾免费账户下，最多支持加速10个域名。

专业版20个

商务版40个

企业版100个

未接入域名添加有限制，当未接入域名过多时无法添加新的域名，需要清除部分域名后才能添加。

### 4.对于正常访问的ip被当做CC攻击拦截了，怎么办?

添加确认是被误拦截的ip到牛盾后台的白名单中

### 5.HTTP Response Headers关于牛盾字段的含义。

HIT-缓存 MISS-没缓存 BYPASS-不缓存回源 EXPIRE-缓存过期

### 6.安全设置“标准模式”与“高级模式”的区别

区别在于“高级模式”审查的更为严格

普通模式：对http请求的get、post、header等数据包都做检测

高级模式：增加了对post模式的BOUNDARY内容也做检测

### 7.网站监控里“报警敏感度”是什么？

源站监控报警级别：

'0.05' => '低', '0.5'=>'中', '0.95'=>'高'  
检测网站的存活率  
级别越高，检测越频繁

存活率

越高，报警越频繁

•多个监测点的检测结果，五次历史对比。有问题就会报警

是所有的监测点检测一次，存活率跟配置的存活率比对，如果存活率低于你设置的值就会记为一次，测试五次之后就会报警

30秒 检测一次

累计告警五次是这样，比如第一次已经报警了，第二次的时候就有参照了，这时候才会累计

第5次的时候 主挂了 那么 继续监测 如果第六次 发现又好了 那么不做任何处理

除非 接下来的几次监测还是宕机 满足5次 就切

8.如果用户反应访问网站异常或者节点异常，先将对应用户版本的测试链接发给用户测试，获取基本信息



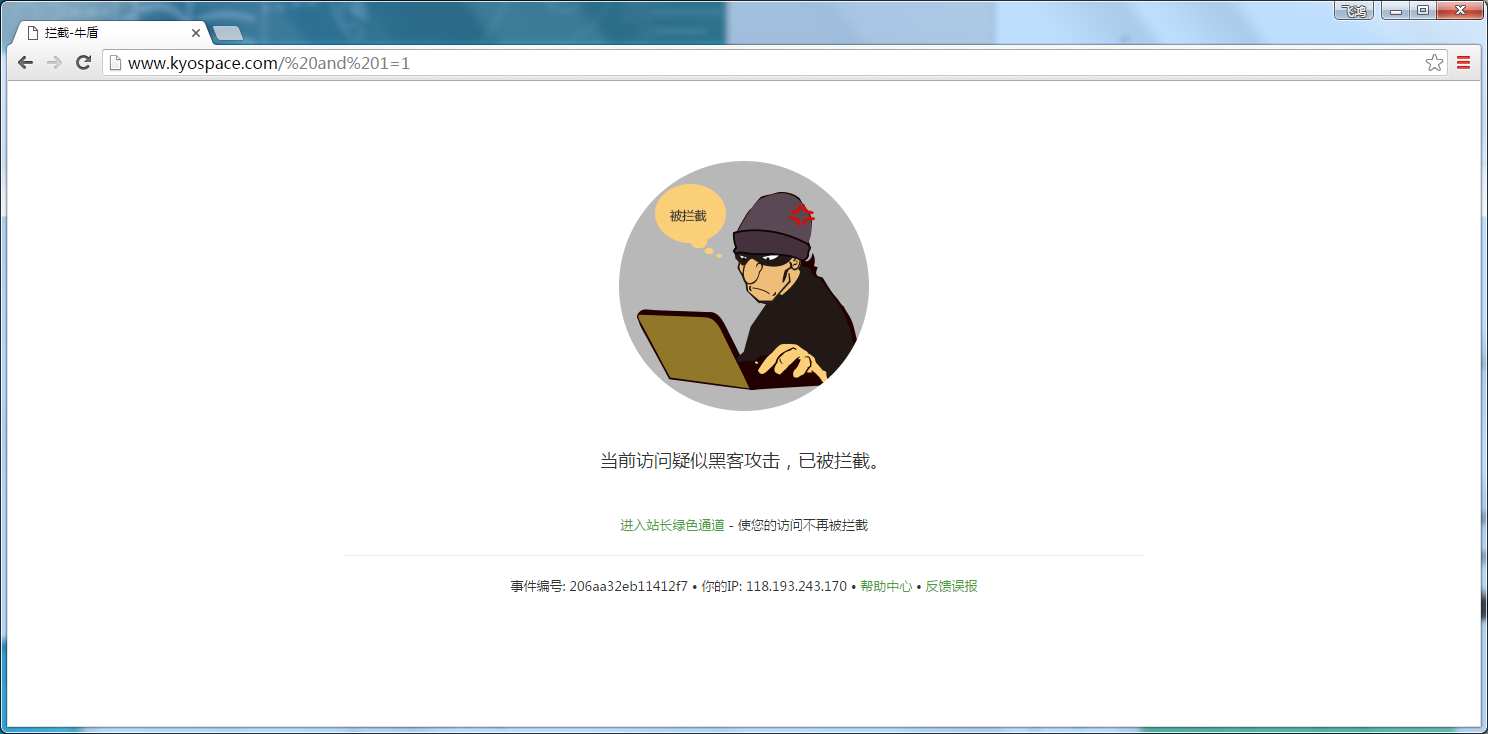
若用户急需解决问题可先切换节点，根据客户端ip找出地区和运营商，切换对应版本的线路



若用户不急，可以本地测试节点业务是否正常，节点到用户之间的链路是否正常，或者远程到用户端，查看具体情况，配合用户查找问题。

### 9.为什么会出现攻击拦截页面？

如图所示：



出现这种情况请参考以下：

提交的数据存在攻击字段。例如：SQL注入，在URL后面加上 and 1=1 等

如果是正常操作出现该页面的解决办法：

在用户后台“我的网站”——>“控制面板”——>”安全设置”——>”网站防火墙”——>”高级设置”找到URL白名单，添加白名单即可。

10.

安全设置“标准模式”与“高级模式”的区别

区别在于“高级模式”审查的更为严格

普通模式：对http请求的get、post、header等数据包都做检测

高级模式：增加了对post模式的BOUNDARY内容也做检测

11.cc规则

（1） 默认策略

用户请求--------CC策略(单个url,单IP阈值 15次/10秒)--------超过阈值,尝试植入Cookies------------校验Cookies--------校验通过---------放行

校验失败--------302跳转

（2）高级模式

高级模式优先级高于默认策略

用户请求--------高级CC策略(用户自定义限速策略)--------超过阈值,禁止访问(返回403)

用户自定义限速策略(不植入cookies, 策略覆盖默认策略)

(1）全站限速,对所有url生效

(2） 指定url限速(uri正则匹配,不用写url参数),如短信接口,支付接口被恶意攻击,可把接口加入url限速中,不用加参数(参数是忽略的)

(3) 黑名单功能(响应303)

默认策略和高级模式都有黑名单功能,10分钟内触发阈值超过200次,IP会自动拉入黑名单禁止访问,10分钟后自动解封

12. 访问日志字段说明（常用）：

clientip 客户端ip

domain 域名

hit\_status 缓存状态（HIT-缓存 MISS-没缓存 BYPASS-不缓存回源 EXPIRE-缓存过期）

host waf节点主机名

method 请求方法

p\_response\_time 父层/源站 响应时间

p\_server 父层/源站 ip地址:端口

p\_status 父层/源站 响应状态码

protocol HTTP协议

referer 从哪个页面链接过来的

request 请求uri

size 请求body大小

ss waf节点响应时间

status waf节点响应状态码

time 请求发起时间