1. 为什么推荐用户使用NS接入

更快速，推广cloudxns

1. NS接入和CNAME接入的区别

ME接入优点：生效时间更快，且操作简单，适合正在遭受攻击的网站使用。不便之处：部分网站使用的dns服务器不支持顶级域名@做cname解析，如果需要防御顶级域名@CNA，相对比较麻烦。

NS接入优点：方便网站管理，且可免费使用小量dns防查询攻击。不便之处：生效时间较慢。

牛盾的实际生效时间都会很快。Ns存在localdns刷新问题

对于NS方式，需要您到您的域名服务商（通常是您注册该域名的网站）修改NS服务器地址(NameServer)，修改成牛盾云安全的高防智能DNS服务器：lv3ns1.ffdns.net, lv3ns2.ffdns.net。

对于CNAME方式，需要您到您的域名解析管理（可能是注册域名的网站，也可能是您设置的其他域名解析服务商）设置CNAME解析记录，将您需要接入的子域名设置CNAME指向牛盾云安全为您生成的域名即可。

1. DDOS防御峰值，然后防御的ddos流量在哪看

用户界面暂时没有，可以通过ES查看

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

1. 客户在询问ddos防御的值的时候可以回答最多防御多少ddos攻击量。针对真正需要ddos防御的用户

企业版需要联系技术人员详谈，其他的按照官网上的说

1. 用户接入牛盾官方回答的需要的生效时间是多少

由于存在各级DNS缓存，每个服务商DNS切换时间不同，各地DNS刷新时间都是未知的，有的快，有的慢，所以请参考相应域名服务商的说明。

1. 大型视频网站需要接入咨询时应该怎么处理

不接入

1. 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。

1. 使用牛盾不会导致百度降权，有反应使用牛盾会导致百度降权，可以使用搜索引擎线路设置回源，就不会影响

怎么设置搜索引擎回源

10、针对部分无法直接判定网站业务内容的域名，先不要审核通过，等待客户联系或者通过其他渠道核实网站业务之后在进行审核

免费套餐只支持联通电信，不支持移动以及其他

牛盾付费套餐（商务版，企业版）拥有海外节点，免费套餐不拥有

1、部分用户会直接试用免费版（自身网站服务器配置以及带宽都较高的客户），但是在试用时反应使用CDN后加速效果没有之前的好，该怎么处理，直接推荐试用专业版？

（4）DNS切换多久后生效

由于存在各级DNS缓存，每个服务商DNS切换时间不同，各地DNS刷新时间都是未知的，有的快，有的慢，所以请参考相应域名服务商的说明。

（5）对于正常访问的ip被当做CC攻击拦截了，怎么办

在用户后台添加ip白名单即可

blockid字段：

1\*\*=>"SQL注入攻击",

2\*\*=>"跨站脚本攻击",

3\*\*=>"代码执行漏洞",

4\*\*=>"命令注入",

5\*\*=>"扫描探测",

6\*\*=>"目录遍历",

7\*\*=>"IP黑名单",

8=>"CC攻击",

9\*\*=>"其它"}   
发现客户的请求数大多数都是目录遍历。   
hackerid字段： 0代表没攻击。

sqli => 'SQL注入攻击',

xss => '跨站脚本攻击',

rce => '代码执行漏洞',

cmd => '命令注入',

scan => '扫描探测',

brutedir => '目录遍历',

blackip => 'IP黑名单',

cc => 'CC攻击',

other => other

cc 上线新策略 ip+user-agent 3次/15秒 超过该阀值 将会拦截 状态码555 blockid：8

CC 新功能 cc自定义策略 添加 url 策略 cc默认防御引擎将不会作用与 该url

默认的 同一个 clientip+同一个url+植入cookie  15s 30次

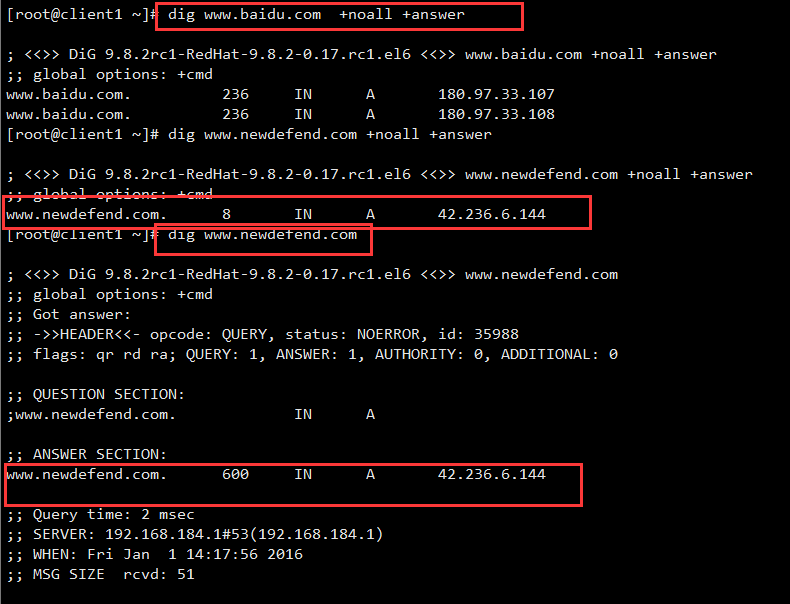
CC拦截 部分新增功能 自动拉黑 10分钟内 超过1500次cc阀值的请求 请求ip 将被拉入黑名单（响应状态码303） 黑名单中的 ip 10分钟解禁

常用检测命令

Ping

Dig 查看域名解析状况，

Dig NS 域名 （查询域名NS记录）



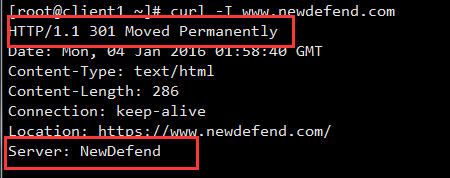
telnet 查看端口连接状况

telnet ip/域名 端口

curl

是一个利用URL规则在命令行下工作的文件传输工具。它支持文件的上传和下载，所以是综合传输工具，但按传统，习惯称url为下载工具。**下载单个文件，默认将输出打印到标准输出中(STDOUT)中**

-I参数 用于直接获取网站head信息，状态码



X-cache 为牛盾特有参数，数据缓存状态。设置缓存后会有，不同参数代表不同缓存状态

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



-x 选项可以为CURL添加代理功能

Curl –x IP:端口 目标网址

1 # 指定代理主机和端口

2 curl -x proxysever.test.com:3128 www.newdefend.com

用于检测代理IP到目标网站的连接状况。

当机器有受到攻击时可用来检测受攻击机器是否可以正常使用

curl -x vip:80 C:\Users\fast168\AppData\Local\Temp\8LDO48C$8@[GWU0353$FOVS.pngwww.huitouzi.com -Is

curl --resolve jk.anquan.io:443:14.136.136.55 C:\Users\fast168\AppData\Roaming\Tencent\QQ\Temp\%W@GJ$ACOF(TYDYECOKVDYB.pnghttps://jk.anquan.io/ -Is

Nslookup

ipconfig/flushdns 即可清空DNS缓存。

不同套餐对应的测试节点

检测工具

http://www.newdefend.com/check\_cdn\_health.html 免费版

http://www.newdefend.com/check\_cdn\_health.html?1 专业版

http://www.newdefend.com/check\_cdn\_health.html?2 商务版

<http://www.newdefend.com/check_cdn_health.html?3> 企业版

用户需要看单个域名ddos流量时需要联系运维，cacti可以看大致流量。

用户需要添加部分暂时没有的功能时可以先问清楚需求，然后回复向工程师反馈。

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

我们新版本对这个登录信息有设置时间限制么？

有过期时间。20分钟左右

出现504错误有可能是源站到节点之间端口连接有问题，需要将所有节点IP全部添加进白名单

源站监控主备切换



源站监控报警级别：

'0.05' => '低', '0.5'=>'中', '0.95'=>'高'  
  
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

如遇到用户联系营销QQ有视频或直播加速网站需要审核，无法通过时可以给用户推荐cloudcdn等公司其他加速产品。

Ns接入会遇到的问题

牛盾后台手动添加备案信息后用户后台依然显示未备案，无法开启牛盾

原因是ns接入xns那边未检测到域名的备案信息，xns的域名检测一般是晚上执行，白天直接联系xns处理。

部分域名后缀接入牛盾提示无法接入

1. 让用户提供报错或者无法接入的提示的截图
2. 自己验证重现用户的问题确定无误
3. 询问接入方式，NS接入时确定是dns没有收录或者其他dns相关问题直接转交给xns，转接时说明原因。一种是xns没有收录部分域名后缀，一种是域名管理商后台添加我们的dns服务器报错。
4. cname接入提示域名后缀不合法时将需要接入的域名后缀提交

https监控原理

一台服务器 没5分钟 向线上的所有机器 发任务 （任务是 访问咱们所有waf入口 [vip：80/443]），然后上报结果 超过30台机器没有得到正确响应 判定 vip:80/443 故障

当某个用户已接入域名达到上限，同时有域名需要通过审核接入牛盾，推荐付费。

如果用户提出停用其他域名空出名额来接入新域名，可以驳回用户关闭牛盾的域名。不建议用户删除域名，驳回操作只是关闭了域名在牛盾这边的功能，并不影响用户在clouxns的解析，删除域名会同时删除cloudxns的解析记录。

从cloudxns同步过来的未接入的域名超过用户限制，导致用户无法在牛盾添加新的域名的问题已反馈，以解决

PROBLEM: 222.186.19.143 network drop on eth0 [in] drop服务器网卡丢包, error是错误

lvs\_status\_synproxy\_rs\_error lvs服务器到后端relserver之间

PROBLEM: 42.236.6.29 redis replicate down 6379 redis复制进程down掉会影响用户后台修改后的配置的下法时间,超过10分钟通知

PROBLEM: Check\_Keepalived\_Status 119.97.146.43

PROBLEM: check nginx log 123.149.54.15 检查nginxbug日志,需要及时通知

PROBLEM: purge tid:18897 failed nodes:1

502 我们节点连接的dns解析错误导致502,其他大部分为用户源站导致

PROBLEM: check supervisord 111.7.163.48 监控自启动down掉的服务的程序长时间需要及时通知

[alert] https 103.55.236.165 北京\_铁通 failed

PROBLEM: 124.193.166.140 is unavailable by ICMP

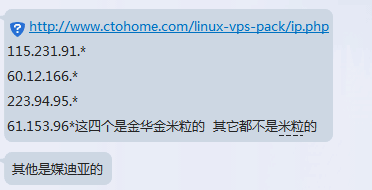
Cc攻击的判定标准

同一个url 同一个ip 30次请求/15秒

同时还有状态机制

Ns接入域名不合法时先检查域名备案，有的域名无法备案，确认备案没有问题之后再转接xns

金华电信机房联系方式



115.231.91.122-61.130.28.122  修改下 所有监控

115.231.91.126-61.130.28.126 修改所有监控

给机房发邮件需要机器的信息，机器ip、机柜位置、机器sn号、设备型号、合同编号，需要对机器有什么操作，用快网的邮箱发。

军网安全邮件联系人

王小瑾：184328514@qq.com

杨文博：56165656@qq.com

戴斌：335860828@qq.com

涉及到白名单添加的，发送给这三个人，然后抄送给李处和陈处。

李处：

jfjbmail@163.com

陈处：jfjbctw@163.com

注：标明是是牛盾云安全

邮箱

server@newdefend.com   6SeEa0hMlq1W  
  
service@newdefend.com Jf3c2cI0zdio  
C:\Users\fast168\AppData\Local\Temp\%W@GJ$ACOF(TYDYECOKVDYB.pnghttps://mail.newdefend.com

https证书上传nginx证书

怎样获取用户真实IP

直接获取HTTP\_CLIENT\_IP是用户的真实IP

海外测试工具

C:\Users\fast168\AppData\Local\Temp\%W@GJ$ACOF(TYDYECOKVDYB.pnghttps://tools.keycdn.com/performance  
C:\Users\fast168\AppData\Local\Temp\%W@GJ$ACOF(TYDYECOKVDYB.pnghttps://tools.keycdn.com/speed  
C:\Users\fast168\AppData\Local\Temp\%W@GJ$ACOF(TYDYECOKVDYB.pnghttp://www.maplatency.com/

