

自建CDN应对 大流量DDOS攻击思路

- 来自 海洋之心#hzlug@googlegroups.com
 - 来自 张磊
- #gdg-hangzhou@googlegroups.com

DDoS主要攻击类型

- 延缓性的CC攻击
- 致命的流量攻击

自建CDN 的考量

- 硬件成本
- 带宽成本
- 架构设计
- 配置要点
- 智能脚本

架构设计



为什么这里没有提LVS，因为LVS是个重量级，高效稳定的四层转发，但它不能作七层http协议的识别，但完全可以架设在七层之前，所以，LVS的使用并不会影响网络结构，后续想上就上。

Haproxy/Varnish: 防御型反向代理缓存方案

- 反向代理 (负载均衡、信息透明、支持 haproxy > squid > varnish > nginx > mysql)
- 缓存加速 (静态加速、节省带宽、连续推送) (squid > varnish > squid > nginx > haproxy)
- 防御功能 (快速解析、连接匹配) (haproxy > nginx > squid > varnish)

支持文件读取匹配

支持热加载生效

可插拔式的缓存组件灵活组合

配置要点 - Options

option forwardfor

option httplog

option dontlognull

option accept-invalid-http-request

option nolinger # reduce FIN_WAIT1

timeout client 15s

timeout connect 15s

timeout server 15s

timeout http-keep-alive 15s

timeout http-request 15s

配置要点-ACL

```
acl bad_referer hdr_sub(referer) -i -f /etc/bad_ref  
acl bad_url url_reg -i -f /etc/bad_url  
acl bad_methods method -i -f /etc/bad_method  
block if invalid_referer || invalid_url || invalid_meth
```

```
acl dyn_host hdr(host) -i -f /etc/notcache_host  
acl static_req path_end -i -f /etc/cache_file  
use_backend img_srv if static_req !dyn_host
```

智能脚本

```
config() {  
    if [ ! -z "$PROXY_HOST" ];then  
        for LINE in $PROXY_HOST;do  
            echo "$LINE" |grep -q ^#  
            [ $? = 0 ] && continue  
  
            DOMAIN=`echo "$LINE"|awk -F@ '{print $1}'`  
            HOST=`echo "h_"$DOMAIN|sed -r -e 's#\.#_#g' -e 's#\|#_#g'`  
            IPADDR=`echo "$LINE"|awk -F@ '{print $2}'|sed -r 's#&# #g'`  
            NAME=`echo "$LINE"|awk -F@ '{print $3}'`  
            PREFIX=`echo "$LINE"|awk -F@ '{print $4}'`  
            [ -z $PREFIX ] && PREFIX="www"  
            j=0  
  
            STRING3="director $NAME client {\t\t\t# ProxyList\n"  
            for SRV in $IPADDR;do  
                IP=`echo $SRV|awk -F: '{print $1}'`  
                PORT=`echo $SRV|awk -F: '{print $2}'`  
                WEIGHT=`echo $SRV|awk -F: '{print $3}'`  
                [ -z $WEIGHT ] && WEIGHT=3  
  
                ((j++))  
                STRING="backend ${HOST}_${j} {\t\t\t# ProxyList\n  
                \t.host=\"$IP\";\t\t\t# ProxyList\n  
                \t.port=\"$PORT\";\t\t\t# ProxyList\n  
                \t.connect_timeout=300s;\t\t\t# ProxyList\n  
                \t.first_byte_timeout=300s;\t\t\t# ProxyList\n  
                \t.between_bytes_timeout=300s;\t\t\t# ProxyList\n  
                }\t\t\t# ProxyList\n"  
                echo -en $STRING >> $TMP  
            done  
        done  
    fi  
}
```

如何提升

- 智能DNS区域化
- 大规模日志分析
- 后端管理不直观

OpenCDN是什么？

•做什么？ → 提供多节点CDN管理平台！

•开源

OpenCdn

Home

zenland.cn

二级域名



默认



添加

域名	线路	ip地址	切换状态	操作
node	联通	42.121.78.183	智能切换	自定义故障处理
node	教育网	42.121.79.42	智能切换	自定义故障处理
node	移动	42.121.79.43	智能切换	自定义故障处理
node	电信	42.121.125.78	智能切换	自定义故障处理

我们解决什么问题？

代维费用高

多节点管理复杂

商业软件贵

CDN部署繁琐

节点状态监测难

缓存规则门槛高

多节点授权收费价格列表如下：

版本	节点数	初次试用	终身费用
个人版	2	付费提供	3000元
标准版	5	付费提供	5000元
企业版	10	不提供	9000元
高级版	20	不提供	12000元
无限版	9999	不提供	16000元

终极无限制版（无节点无时间限制）16000元（一次性）

项目名称：LMCDN
项目性质：默认配置
价格明晰：
(不含另议)

☒ 蓝芒智能CDN管理系统 50,000 元

确认订单

修改订单

WDCDN系统架设收费标准 [下载软件文档](#)

为了方面客户自行搭建CDN系统，我们推出了组合套餐，具体收费标准

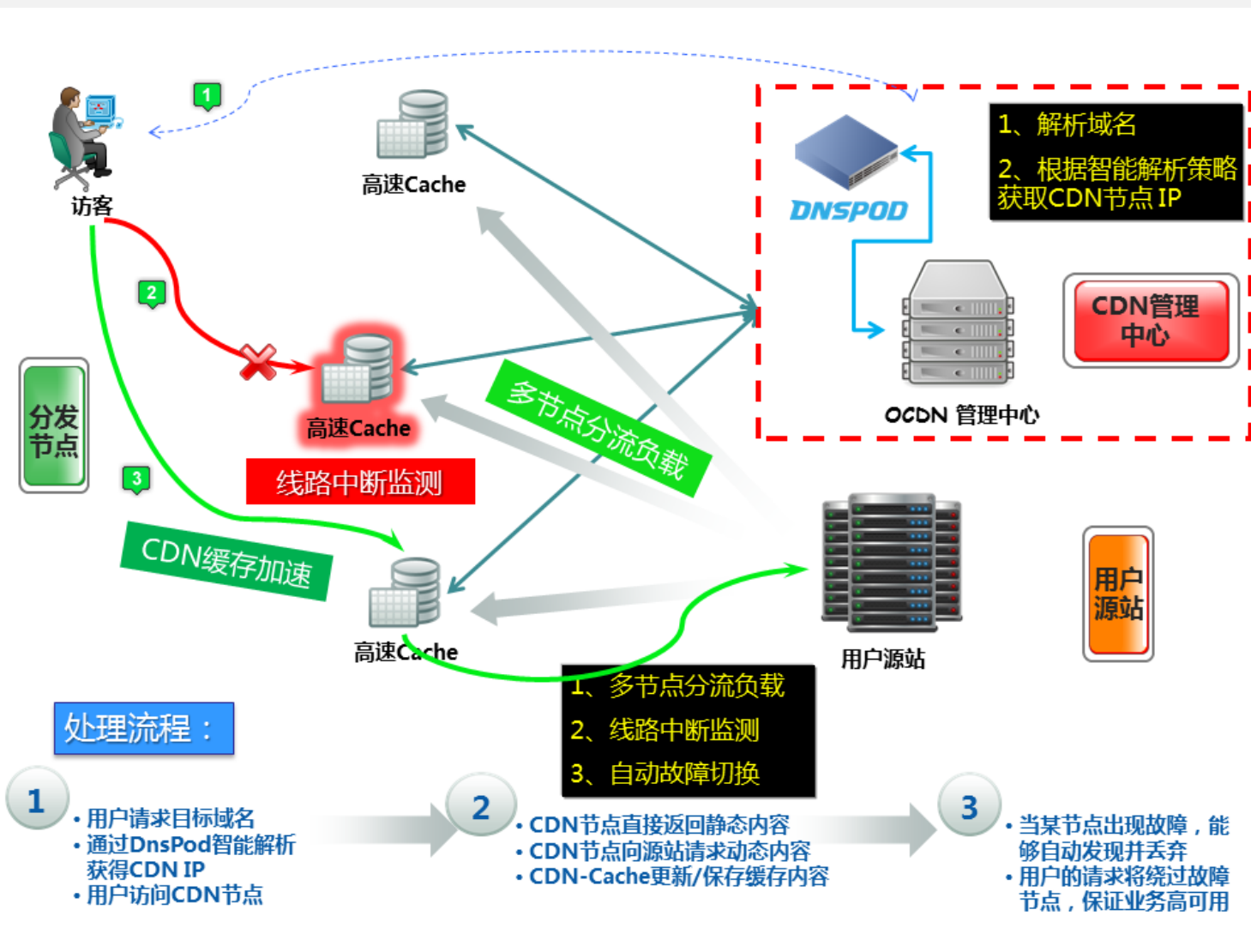
1800元 = 两台WDCDN单节点 环境配置，外加3小时QQ技术支持（性能

3600元 = 3节点授权一年+ 3节点环境配置 外加3小时QQ技术支持（性能

6800元 = 5节点授权一年+ 5节点环境配置 外加3小时QQ技术支持（性能

备注：

OpenCDN 平台技术架构



使用以下技术融合

- 基于Linux+nginx构建
- Ngx_proxy_cache 高速缓存模块
- 自主统一监测/管控平台
- DNSPod智能解析
- D监控自动故障切换
- VPS作为缓存节点

OpenCDN 的特点

- ✓ 提供给用户实时自助开设
- ✓ 5分钟开通一个CDN节点
- ✓ 管控端不限制节点数量

特点：**简单、快速、开源** → OpenCDN !

CDN加速效果对比 - Ping延迟

原始状态

Ping的地点	响应IP	响应时间	TTL	赞助商
上海[电信]	173.254.28.83	222毫秒	49	上海龙联[上海高防]
四川绵阳[电信]	173.254.28.83	274毫秒	50	西部数码 云主机
云南昆明[电信]	173.254.28.83	268毫秒	50	云南数据港
安徽淮北[电信]	173.254.28.83	238毫秒	49	安徽拓普(双线)
江苏无锡[电信]	173.254.28.83	333毫秒	47	优易互联 云主机
四川德阳[电信]	173.254.28.83	278毫秒	48	加速乐防黑客
江苏扬州[电信]	173.254.28.83	164毫秒	49	DiyVM高端云VPS
深圳[电信]	173.254.28.83	291毫秒	48	香港纵横网连
广东东莞[电信]	173.254.28.83	242毫秒	48	迅美云主机
陕西西安[电信]	173.254.28.83	295毫秒	49	中光电信云vps
四川遂宁[电信]	173.254.28.83	284毫秒	50	双线租用450元月
江苏镇江[电信]	173.254.28.83	265毫秒	48	雅科诺商务 [高防]
香港[电信]	173.254.28.83	超时	--	香港纵横网连
上海[多线]	173.254.28.83	307毫秒	45	浦东数据中心(BGP)
河南郑州[多线]	173.254.28.83	355毫秒	46	37互联 云VPS
上海[联通]	173.254.28.83	355毫秒	46	上海络安数据中心
辽宁[联通]	173.254.28.83	355毫秒	50	【70G高防】服务器
安徽滁州[联通]	173.254.28.83	384毫秒	46	(海外高防专家)
深圳[联通]	173.254.28.83	351毫秒	46	香港纵横网连
宁波[联通]	173.254.28.83	226毫秒	43	高防双线-360集群

使用OCDN后的状态

四川绵阳[电信]	42.121.125.78	49毫秒	55	西部数码 云主机
陕西西安[电信]	42.121.125.78	39毫秒	54	中光电信云vps
四川遂宁[电信]	42.121.125.78	47毫秒	55	双线租用450元月
云南昆明[电信]	42.121.125.78	44毫秒	55	云南数据港
江苏镇江[电信]	42.121.125.78	15毫秒	53	雅科诺商务 [高防]
江苏无锡[电信]	42.121.125.78	57毫秒	52	优易互联 云主机
四川德阳[电信]	42.121.125.78	46毫秒	53	加速乐防黑客
安徽淮北[电信]	42.121.125.78	20毫秒	54	安徽拓普(双线)
广东东莞[电信]	42.121.125.78	33毫秒	52	迅美云主机
上海[多线]	42.121.78.183	5毫秒	50	浦东数据中心(BGP)
河南郑州[多线]	42.121.78.183	47毫秒	52	37互联 云VPS
深圳[联通]	42.121.78.183	44毫秒	51	香港纵横网连
宁波[联通]	42.121.78.183	42毫秒	47	高防双线-360集群
北京[联通]	42.121.78.183	25毫秒	47	北京双线云主机
河南[联通]	42.121.78.183	49毫秒	53	腾佑-云计算主机
安徽滁州[联通]	42.121.78.183	61毫秒	53	(海外高防专家)
辽宁[联通]	42.121.78.183	53毫秒	54	【70G高防】服务器
上海[联通]	42.121.78.183	64毫秒	53	上海络安数据中心
天津[联通]	42.121.78.183	25毫秒	42	限时促39元.COM
河北[移动]	42.121.79.43	52毫秒	49	【免备案】360集群
上海[移动]	42.121.79.43	5毫秒	53	而邦互联 双线主机

界面长啥样？

penCdn

缓存高级配置

状态

匹配方式

目录

缓存方式

缓存

Home

zenland.cn

二级域名

默认

添加

域名	线路	ip地址	切换状态	操作
node	联通	42.121.78.183	智能切换	自定义故障处理
node	教育网	42.121.79.42	智能切换	自定义故障处理
node	移动	42.121.79.43	智能切换	自定义故障处理
node	电信	42.121.125.78	智能切换	自定义故障处理

扩展名

js|css

CSS,JS

缓存

删除

Thank You !



`http://ocdn.me`

- 来自 海洋之心#hzlug@googlegroups.com
 - 来自 张磊
- #gdg-hangzhou@googlegroups.com