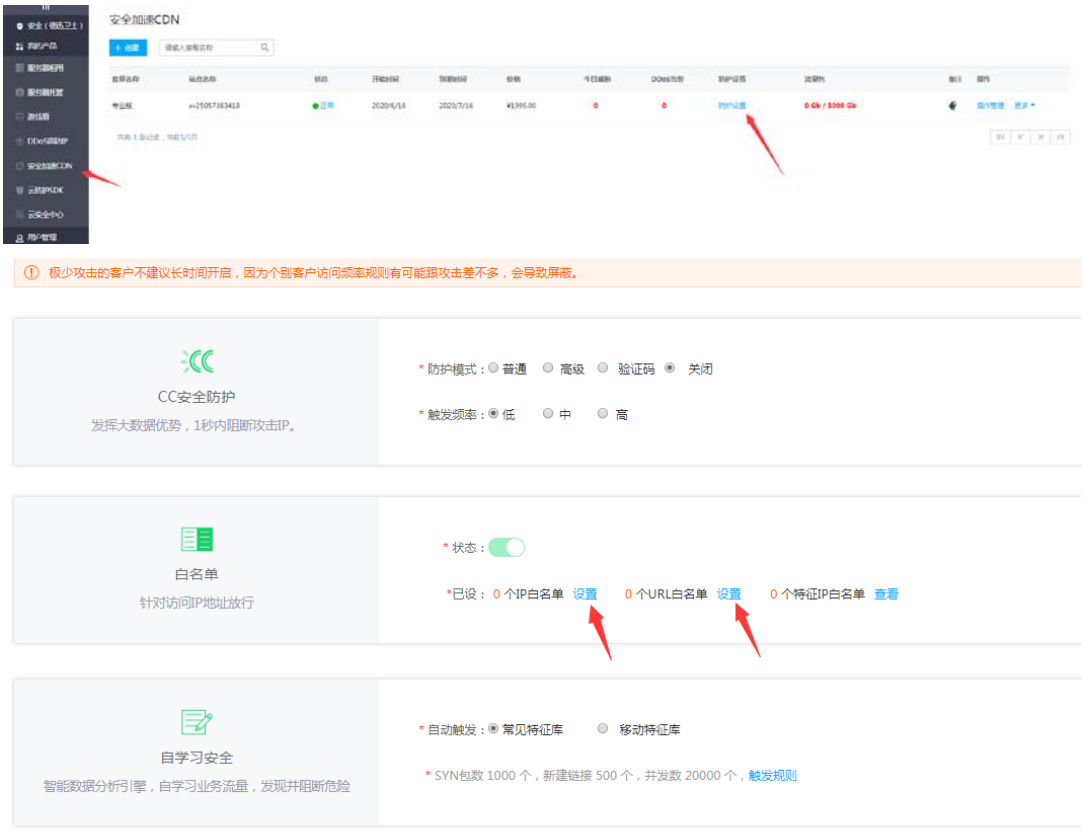
安全加速 CDN 添加 IP 白名单与 URL 白名单教程

在使用 CDN 加速的情况下，源机跟 CDN 节点之间直接会存在大量的数据包交互，最好是把所有的源机 IP 都加到白名单已防止出现 CC 攻击开启防护策略之后导致拦截的情况。

这个是这个是 IP 加白的具体步骤。



注：这边只能添加 10 个白名单 IP，如果有超出 10 个源机的情况下可以联系我们售后加白。源机也加下我们节点白名单。

一些网站 URL 地址不会被攻击并且需要跳转到我们 CDN 的也需要加白。
这个是 URL 加白的具体步骤。


极少攻击的客户不建议长时间开启，因为个别客户访问频率规则有可能跟攻击差不多，会导致屏蔽。
CC安全防护
发挥大数据优势，1秒内阻断攻击IP。
* 防护模式：普通 高级 验证码 关闭
* 触发频率：低 中 高
白名单
针对访问IP地址放行
* 状态：
*已设： 0 个IP白名单 设置 0 个URL白名单 设置 0 个特征IP白名单 查看
自学习安全
智能数据分析引擎，自学习业务流量，发现并阻断危险
* 自动触发：常见特征库 移动特征库
* SYN包数 1000 个，新建链接 500 个，并发数 20000 个，触发规则


URL白名单-创建
* 站点名称： xv25057383418
* URL地址：
描述：
确定保存
取消

安全加速 CDN 配置 SSL 证书教程

如果用户源机本身就是有 ssl 证书的情况下，可以直接在后台加上自己的公钥和私钥。

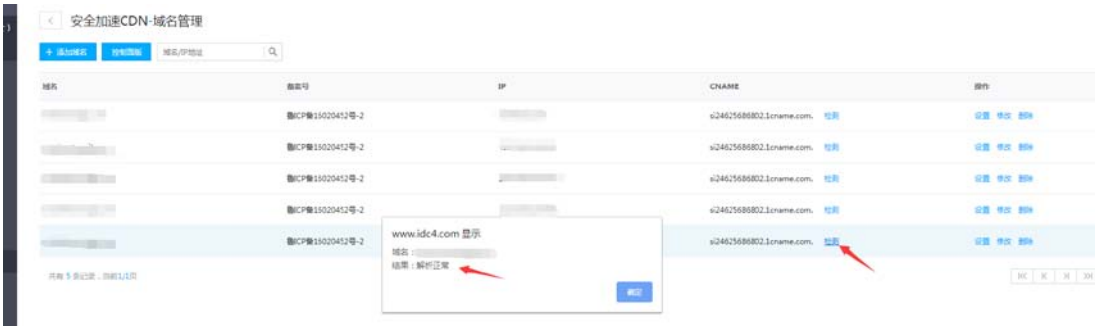
上面添加（.PEM 后缀的是公钥），下面添加私钥（.key 后缀的是私钥）。添加好之后直接点确定就可以了。

安全加速 CDN 申请免费证书教程

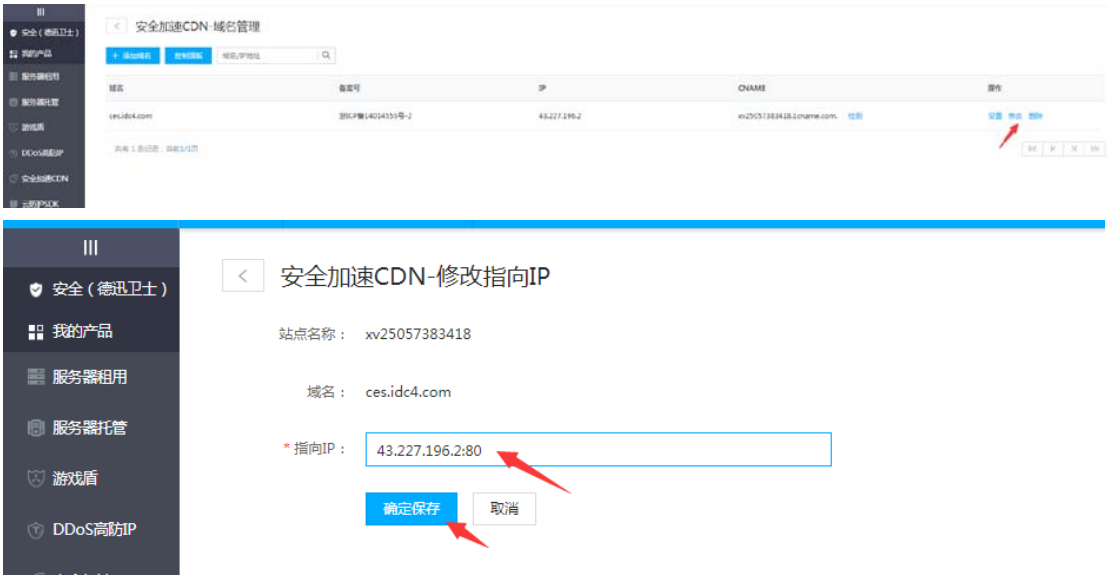
如果没有证书的情况下想要 SSL 证书，可以在我们的 CDN 后台直接申请，先点设置-自动获取，等待 10 来分钟，证书就申请下来了。

注：一定要先把域名 CNAME 解析到 CDN 先，不然的话证书申请会失败的。

这是验证是否解析成功的方法，如果生效了他会提示解析正常。



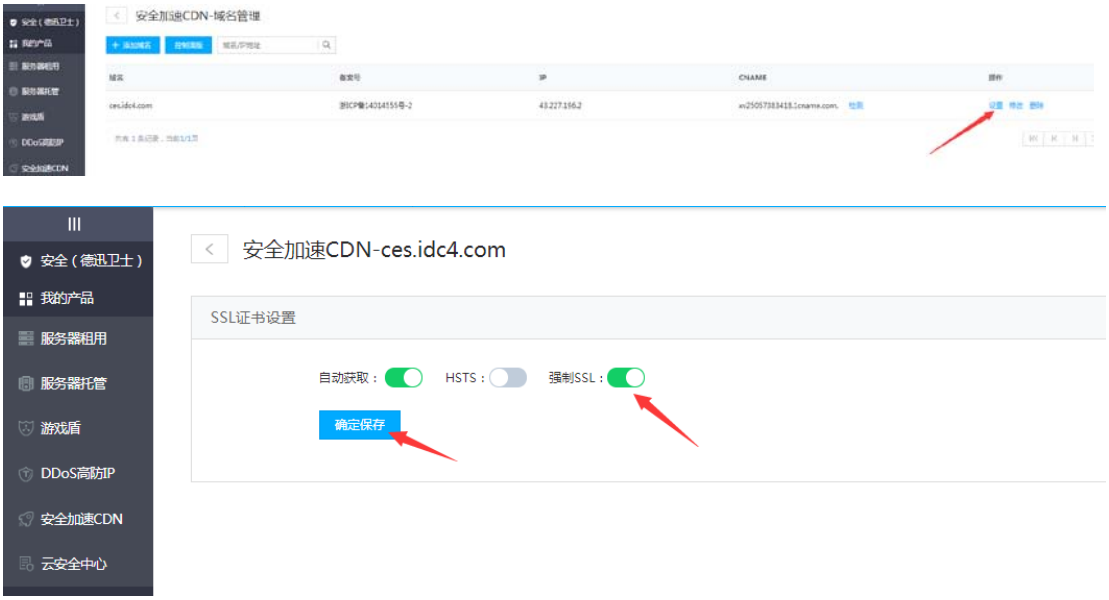
证书申请好之后，因为业务是由 CDN 443 转发到源机的 80 端口的，所以需要在 IP 后面添加下 80 端口。



这个证书配置只适合单域名的 ，多域名证书不合适。建议直接在添加记录那里设置，里面带 SSL 添加和一键跳转 https 配置。

安全加速 CDN 强制调转 HTTPS 教程

无论是用户自己添加的证书还是我们免费申请的证书都是不会自动跳转的，如果需要自动跳转，需要把强制 https 勾选上。

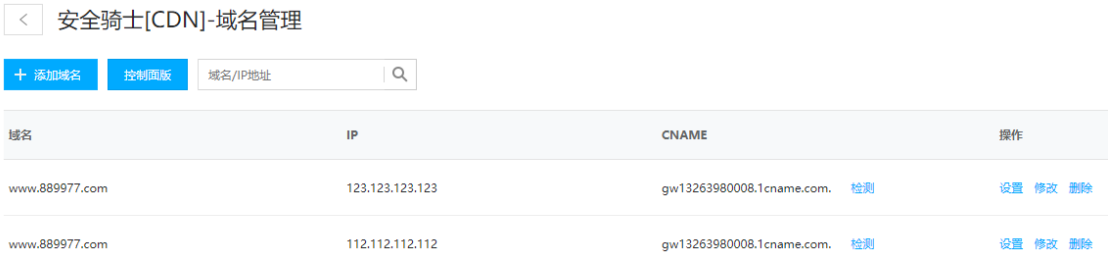


HSTS 的作用是强制客户端（如浏览器）使用 HTTPS 与服务器创建连接。服务器开启 HSTS 的方法是，当客户端通过 HTTPS 发出请求时，
在服务器返回的超文本传输协议响应头中包含 Strict-Transport-Security 字段。

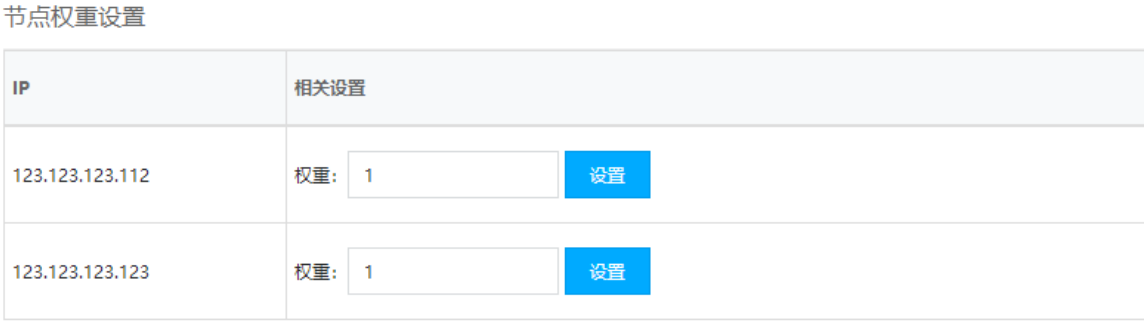
非加密传输时设置的 HSTS 字段无效。

CDN 如何设置负载均衡并设置优先级权重

当一个域名有多个源服务器时，需要做负载均衡，如下图，假如是两个源，添加如下



点设置 可以给源 IP 配置权重，比如设置权重 1，意思占百分之 10，哪个数字越大，哪个优先级越高。



策略默认选择：随机，如下图设置

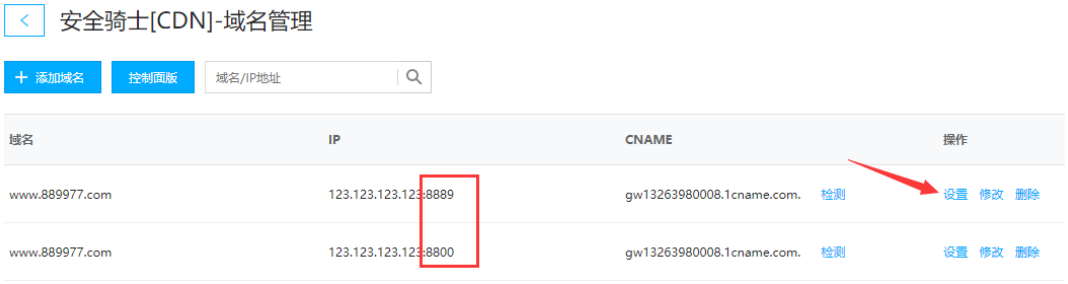
IP 哈希:
基于 ip 的稳定连接。使得来源机器的会话是持续的。
即：每个请求按访问 ip 的 hash 结果分配，这样每个访客固定访问一个后端服务器，可以解决 session 的问题
对于一个特定的请求，如果所申请的服务器不能进行处理的话，其他的服务器可以马上取代它的位置，
对所申请的请求进行处理，而且这一过程对用户感觉来说，服务是稳定的！
url_hash: url_hash 和 ip_hash 的意思差不多，只是这个是基于 url。还有如果用户访问的源是挂掉的，同样会去自动访问第二个源。

错误重试时间（秒）：
如果某个节点服务器连不上，自动会从其它节点服务器上连接。每隔设定的错误重试时间，又会尝试去连接该节点服务器。

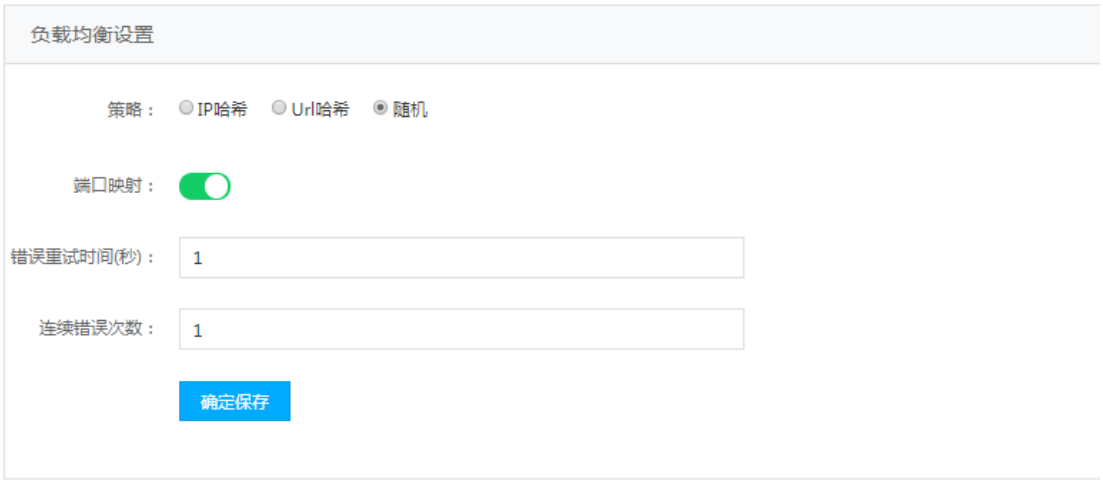
连接错误次数
当某个节点服务器没连通，系统会把分配给该节点服务的请求转给其它节点服务，
同时每隔设定的错误重试时间会自动去连接该节点。
发现能连通，作上线处理。反之，没连通并且连续连接错误次数达到“连接错误次数设定值”后，
CDN 安全骑士会认为这台节点有故障，并作下线处理。节点作下线处理后，CDN 安全骑士不会再把请求发送到该节点。

一个域名匹配多端口设置（端口映射）

添加的域名需要用到不同的端口时候，而且端口各自有对应的业务功能情况下在 CDN 的站点设置里面 IP 后面加上端口，源机自身开放好对应的端口，如果是 https 的情况下 ，端口后面要带 S



添加好后 ， 点设置，拉到下面，勾选端口映射，
错误重试时间：1
次数：1
权重默认：1
默认策略选择：随机（随机策略比较均衡实用）

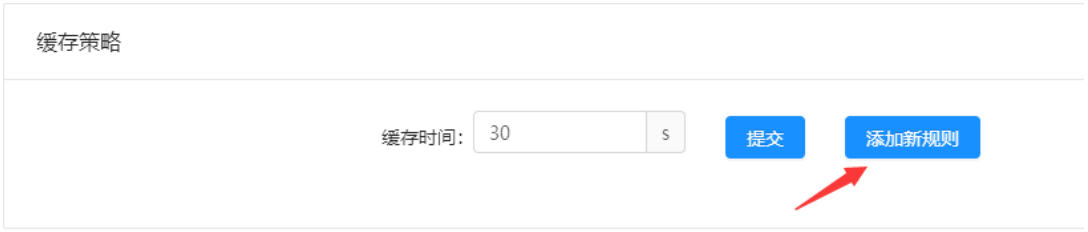


开启强制缓存

强制缓存有两种方式，一种是文件类型，一种是 url 方式
下图是以文件类型为例，输入需要强制缓存的文件扩展名，多个以竖线隔开

设置缓存时间，单位是秒，然后要记得勾选强制缓存

post 方法的不能缓存，因为 post 需要上传数据，只能缓存 get 方法的



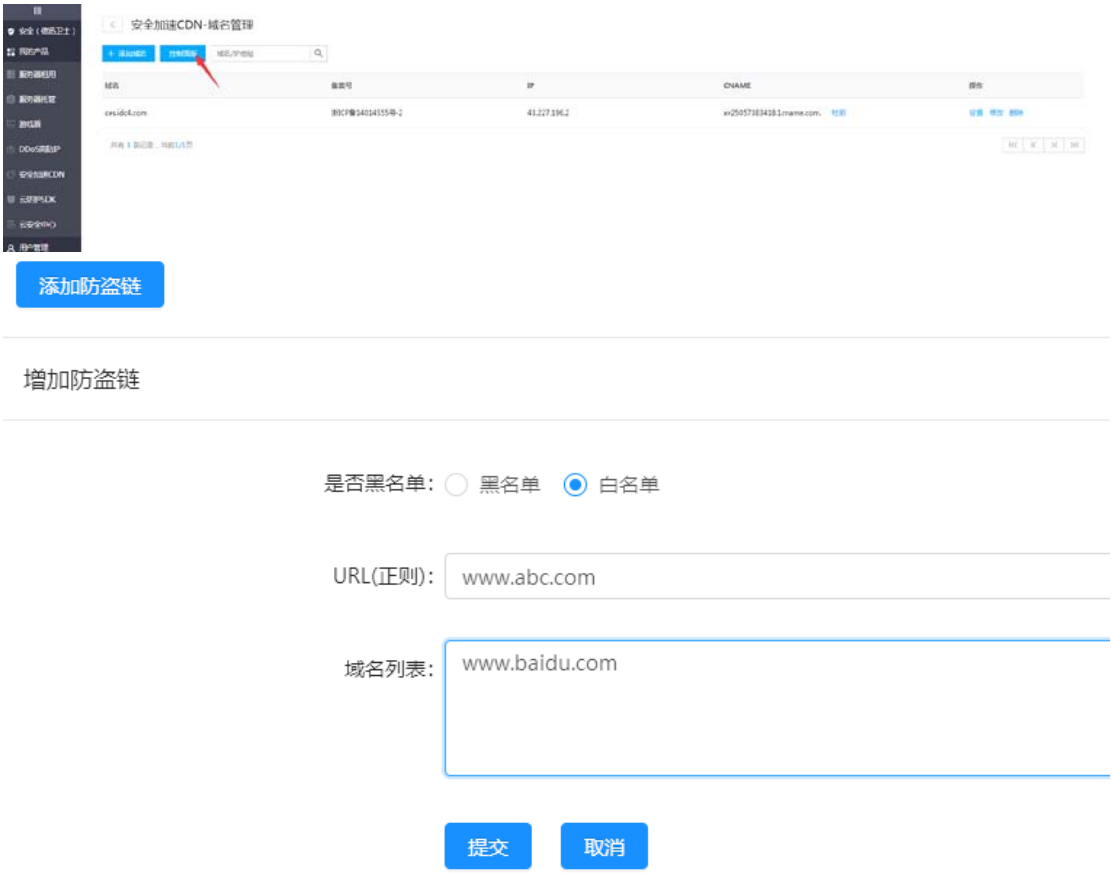
注：如果网站有所更新，后台又添加了缓存，可以在后台强制清理下 CDN 缓存。

安全加速 CDN 防盗链设置教程

示例 ：

1.白名单设置：

需求：www.abc.com 域名需要防盗链，仅允许来源于 www.baidu.com 的网址可以访问，其他网站链接全部拒绝。如下图：



安全加速 CDN 用户 IP 或 URL 限速教程

限速分为每连接、每节点、每 IP 限速
1.每连接
每连接限速只针对当前连接
点设置，在 url 输入框中输入要限速的 url 网址(支持正则表达式)和速度

2.每节点
每节点限速针对来源于此 url 的所有连接
点设置，在 url 输入框中输入要限速的 url 网址(支持正则表达式)和速度

3.每 IP
每 ip 限速：每 ip 限速针对于访问此 url 的 ip
点设置，在 url 正则输入框输入要限速的 ip 和速度

安全加速 CDN 域名带端口设置教程

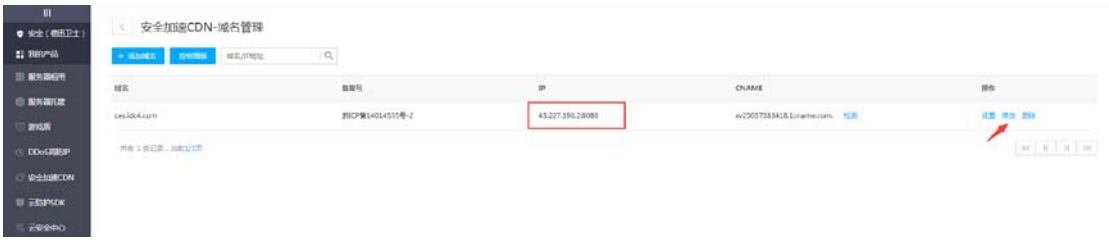
站点端口一般默认 80 443s ，用户如果需要用到其他的端口，比如：http://ces.idc4.com:8080 ,可以如下图设置端口
每个端口中间要用逗号隔开

注：下图加了两个端口 8080 这是 http 端口

要用 https 端口就要像下图中一样，在端口后面加上 s ,并且站点设置中要添加好 ssl 证书，例如：90s

一个域名用到多个端口映射的时候，或者源机上使用非 80 端口，443 等默认端口的时候，要在这添加上对应的端口。

这边添加好所有使用到的端口之后，IP 后面也需要添加对应的端口，例如 8080。



访问频率设置

IP 和 URL 组合：指的是针对某个 IP+访问某特定 URL 超过设定的次数就加入黑名单

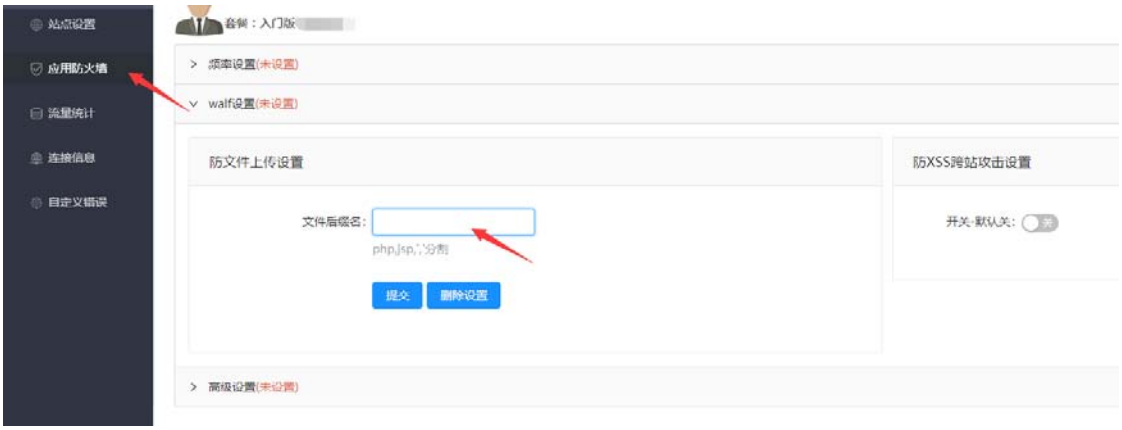
注：这个策略不建议乱开，因为可能会导致业务访问出现偶尔很慢的情况。

安全加速 CDN 限制上传文件格式

一般情况下用户搭建的网站可能存在各种漏洞，黑客可能可以利用这些网站漏洞上传文件、修改网站代码等等。

这是 CDN 防上传文件格式的方法


安全加速CDN-域名管理
添加域名
IP
CNAME


站点设置
应用防火墙
流量统计
连接信息
自定义错误
套餐：入门版
频率设置(未设置)
waf设置(未设置)
防文件上传设置
文件后缀名：
php,jsp,';'分割
提交
删除设置
防XSS跨站攻击设置
开关-默认关：
关
高级设置(未设置)