内容分发网络

安全加速

产品文档

腾讯云

安全加速

最近更新时间：2019-05-27 10:27:51

安全加速（Security Content Delivery Network，SCDN）在保证您加速服务的基础上，为您提供超强的安全防护能力。已使用腾讯云加速服务的域名，可一键开启 SCDN 安全加速，进行 DDoS（暂未上线）、CC（暂未上线）、WAF 全方位防护及攻击监控，为您的业务保驾护航。

⚠ 注意：

- 安全加速产品部分能力已开放申请，内测期间 免费试用。
- 内测功能尚未全量对外开放，DDoS、CC 防护暂不支持。

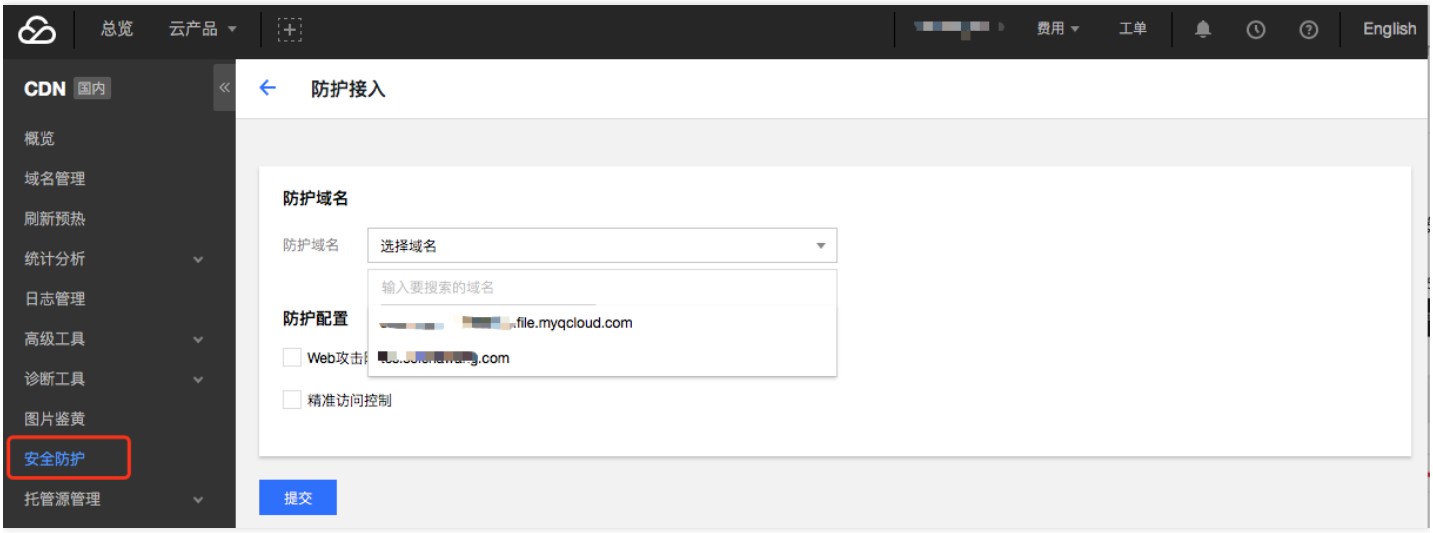
精准访问控制（申请内测）

支持精确至 IP、URI、Referer、User-Agent、Params 等字段的复杂访问规则配置，可根据业务场景进行多条件组合过滤。

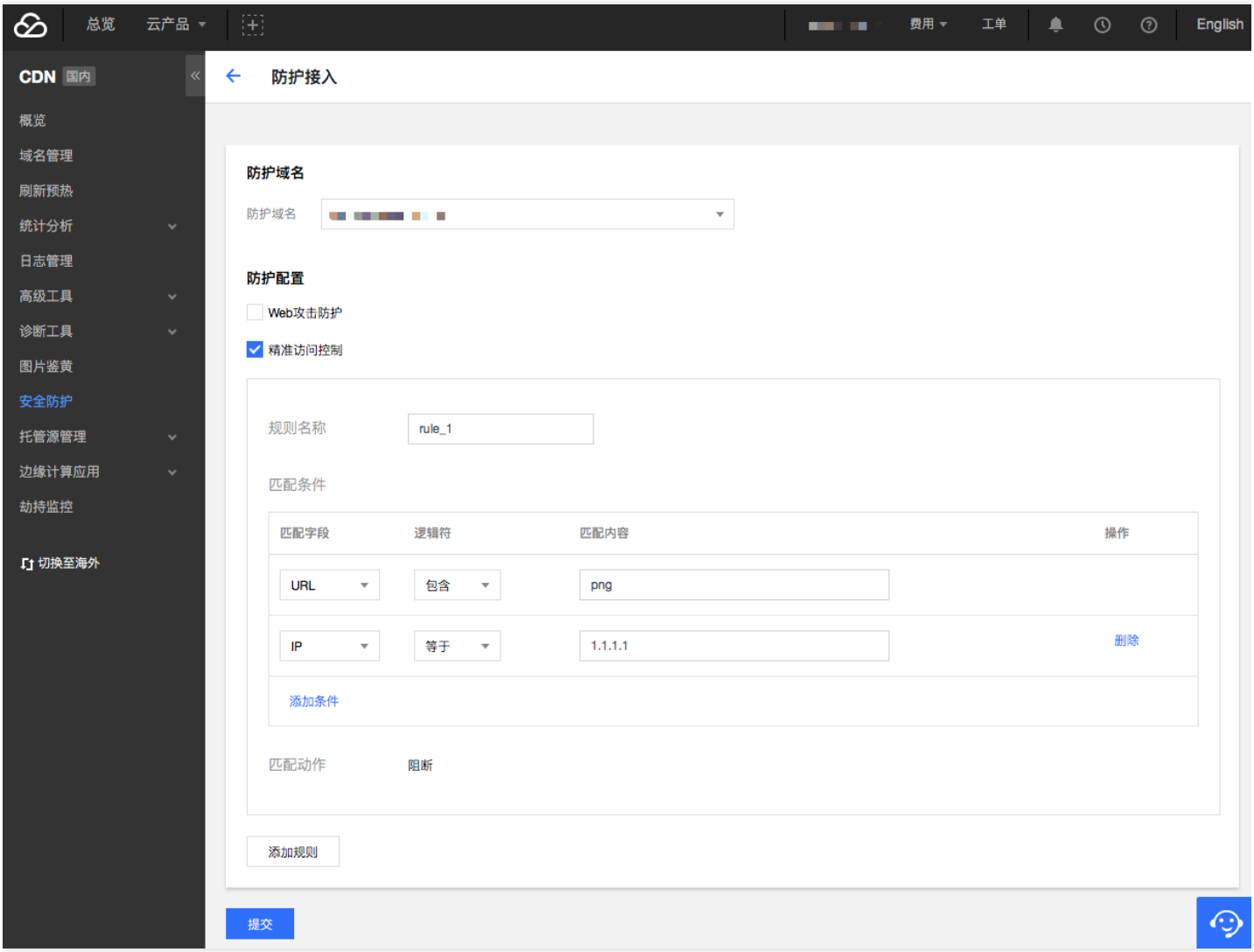
关联规则

1. 登录 CDN 控制台，选择左侧菜单栏的【安全防护】，可以看到配置过安全防护的域名列表，目前仅支持**静态加速**、**下载加速**业务类型的加速域名：

2. 单击【添加域名】，下拉列表选择域名添加安全配置：
3. 选择域名前需要先接入 CDN 加速服务；
4. 域名状态需要为【部署中】或【已启动】，关闭状态的域名无法进行安全配置；
5. 域名业务类型需要为【静态加速】或【下载加速】。



3. 勾选【精准访问控制】创建访问控制规则。
4. 共支持创建五条自定义规则，规则之间为【或】关系，执行顺序按照创建顺序由上至下，**满足所有规则中的任意一条，即会产生阻断**；
5. 每一条规则中可定义五个匹配条件，匹配条件之间为【与】关系，**必须同时匹配所有条件**，才可执行后续的阻断动作；
6. 匹配字段支持：Params、URL（仅 path 部分，如 `/test/1.jpg` ，不包含？之后参数部分）、IP（客户端 IP）、Referer、User-Agent；
7. 匹配条件支持：包含、不包含、等于、不等于、长度小于、长度等于、长度大于。
8. 匹配值仅允许填写【一个】匹配项，暂时不支持正则匹配，不填写默认为空。



4. 单击【提交】，即可关联配置好的访问控制规则。

编辑规则

1. 在【安全防护】域名列表，单击域名右侧【配置】，可查看配置明细。

2. 在【精准访问控制】部分，可查看已经配置的规则，单击规则右侧【修改】，可调整此条规则中对应的条件。

3. 单击上方【添加规则】，可新增自定义规则。

删除规则

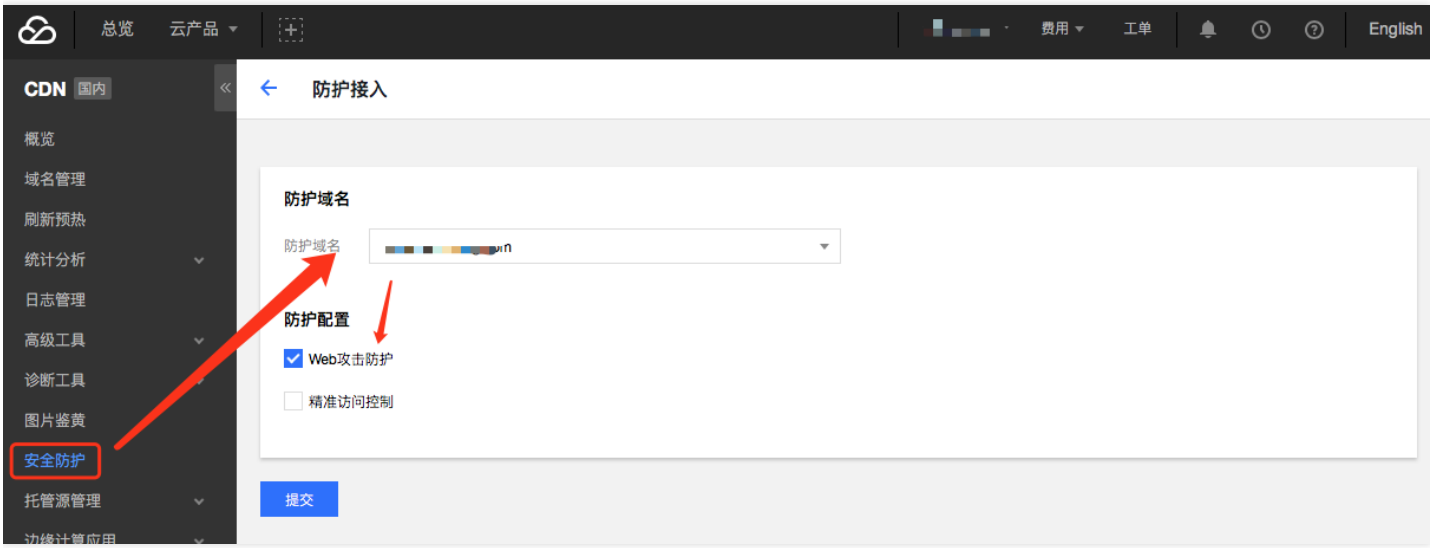
单击每一条规则右侧【删除】按钮，即可删除对应的访问控制规则。

WAF 防护（申请内测）

基于腾讯海量 WAF 攻击样本库，对访问进行特征匹配，有效抵御 SQL 注入、XSS 攻击、本地文件包含、远程文件包含、命令注入、拒绝服务等各类 Web 攻击，实时防护客户站点，保障服务安全。

添加防护

在【安全防护】菜单，选中需要添加 Web 防护的域名，勾选【Web 攻击防护】并提交，即可为域名开通 Web 防护能力。



关闭 Web 防护

单击已开启安全防护的域名右侧【配置】，即可关闭 Web 防护。

Web 攻击防护种类

Web 防护目前具备以下攻击防护能力：

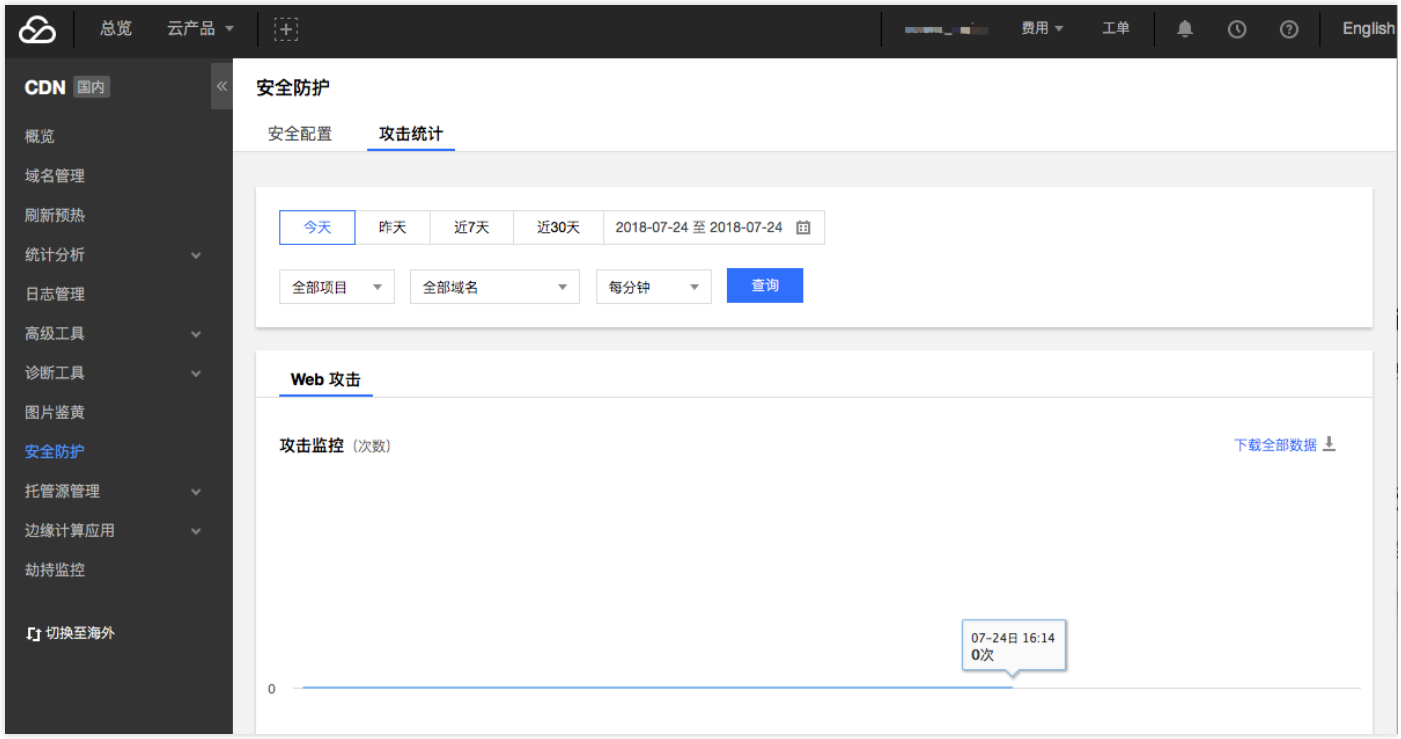
- XSS 跨站脚本
- SQL 注入
- 命令注入攻击
- 文件上传攻击
- Webshell 木马
- struts2 代码执行
- 常见 CMS 漏洞

- 其他漏洞

若用户请求被判定为 Web 攻击，会直接返回**403**状态码，您可以在“攻击统计”页面查看被拦截的攻击详情。

攻击监控（申请内测）

1. 支持 Web 攻击总量实时监控，及指定时间区间的攻击类型分布。
2. 单击【攻击统计】页面，支持选择指定时间区间、域名进行攻击次数、攻击分布查询。



DDoS清洗

基于先进的特征识别算法进行精确清洗，抵御 SYN Flood、TCP Flood、ICMP Flood 等各种大流量攻击，保障正常服务平稳运行，最大可抵御 300Gbps的 DDoS 攻击。

CC 智能识别

多维度自定义精准访问控制，配合人机识别和全局频率控制等手段过滤垃圾访问，最大可抵御10万QPS的 CC 攻击。