目录

访问日志

WAF防护域名的访问日志信息与日志服务(KLog)联动，由KLog提供日志相关功能，助您快速高效实施决策、提升运维效率。

使用说明

1. 使用WAF日志服务无需购买KLog资源包，费用在WAF侧收取。在开通WAF实例时，系统已自动为您创建对应日志项目和日志池。
2. 高级版WAF提供180天日志存储功能，企业版WAF提供360天日志存储功能，不支持延期。
3. 所有版本WAF实例默认包含1T日志存储容量，支持后续扩容。

日志服务操作指南

参见日志服务文档

查看访问日志

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏中，选择**日志管理** > **日志服务**。
3. 点击日志池中操作列中的**搜索**按钮，进入**日志搜索**页面，通过查询功能查看某时间段内的访问日志。

日志文件字段说明

字段名称	字段描述
waf_id	WAF实例ID
user_id	用户主账号ID
timestamp	klog自动生成的时间戳
body_bytes_sent	发送给客户端的HTTP Body的字节数
content_type	Content-Type请求头
http_cookie	Cookie请求头
http_host	请求Host头
http_referer	Referer请求头
http_user_agent	User-Agent请求头
http_x_forwarded_for	X-Forwarded-For请求头
log_pool_name	日志池名称
remote_addr_port	客户端IP地址与端口
request_length	请求长度(包括请求行、头和请求主体)
request_method	请求方法
request_time	请求处理时间以毫秒为单位
request_uri	原始请求uri（包括参数）
scheme	请求协议
server_name	接受请求的服务器的主机名
server_protocol	请求协议
server_real_addr_port	接受请求的服务器IP与端口
server_real_addr_v6	接受请求的服务器端IP与端口，IPv6地址
status	WAF返回给客户端的HTTP响应状态信息
time_iso8601	检测模块的处理时间戳
timestamp	flink处理时间戳
upstream_addr	WAF回源列表
upstream_response_time	源站响应WAF请求的时间
upstream_status	源站返回给WAF的响应状态码

攻击日志

WAF自动采集攻击日志。您在开启Web入侵防护后，WAF拦截到的攻击请求数据将展示在攻击日志页面中。同时，WAF对触发地域封禁和访问控制规则的请求数据也一并记录在攻击日志中，方便您对攻击情况进行实时把控。

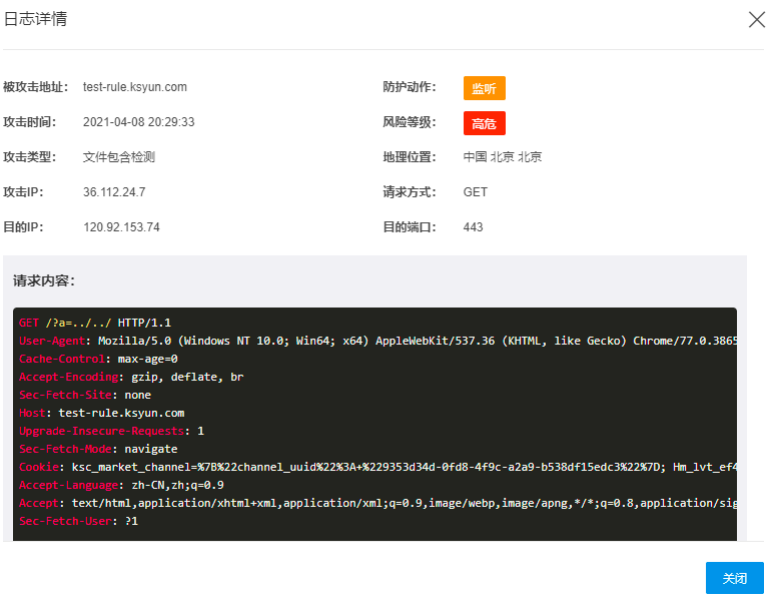
前提条件

- 已开通Web应用防火墙实例。
- 已完成网站接入。
- WAF实例采集到攻击或命中规则的数据。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择**日志管理** > **攻击日志**。
3. 在顶部域名选择区，切换要查看日志的网站域名。

字段名称	描述
攻击时间	攻击开始时间。
攻击IP	攻击方IP。
目的IP	WAF的IP。
攻击类型	检测到攻击请求的类型，详见攻击类型。
被攻击地址	当前网站域名
处理结果	拦截、监听
风险等级	无风险、低危、中危、高危



4. 定位到某条攻击日志，点击**查看详情**。

5.日志详情中可以查看到监听或拦截的请求具体内容，payload表示将该请求识别为攻击的参数值。

攻击类型

SQL注入检测、XSS检测、命令执行检测、文件包含检测、文件上传检测、敏感信息泄漏检测、Webshell检测、Java 代码注入检测、PHP 代码注入检测、NODEJS 代码注入检测、扫描器检测。

CC防护日志

网站域名添加CC防护规则后，WAF将命中规则的请求次数、频率记录，并于控制台汇总，方便用户对受到CC攻击情况进行分析与把控。

前提条件

- 已开通Web应用防火墙实例。
- 已完成网站接入。
- WAF实例采集到攻击或命中规则的数据。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择**日志管理** > **CC防护日志**。
3. 在顶部域名选择区，切换要查看日志的网站域名。

字段名称	描述
攻击时间	攻击开始时间

日志详情	描述了在规则设置的封禁时间内，阻断攻击请求的详细情况。
关联规则	CC攻击命中的规则名称

日志详情说明

对每次CC攻击，日志记录了攻击的起始时间，以及在对应规则设置的封禁时间内，攻击请求访问的IP地址及其次数，和本次封禁过程是否结束。如果您在规则中设置的处置动作为人机识别，也会被记录进CC防护日志。