目录

设置Web入侵防护

网站接入Web应用防火墙后，Web入侵防护引擎功能默认开启。该引擎基于金山云安全团队防护经验内置规则集，支持对SQL注入、XSS跨站，webshell上传、命令注入、文件包含等OWASP常见攻击行为进行防护。您可以根据实际需求调整防护策略。

前提条件

- 已开通Web应用防火墙实例。
- 已完成网站接入。

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**防护配置** > **网站防护**。
3. 在顶部域名选择区，切换要设置的域名。
4. 点击**Web入侵防护**页签，完成如下功能配置。

参数	说明
状态	开启或关闭入侵防护功能。网站接入WAF后默认开启。
模式	检测发现攻击请求时，对攻击请求执行的操作。可选值： **拦截**：直接阻断攻击请求。 **监听**：只触发监听，不阻断攻击请求。
防护规则	要应用的检测策略，支持应用内置规则组和自定义规则组。点击**配置规则组**按钮，将跳转到防护规则组配置页面，您可以根据业务需要自定义防护规则组。详见自定义防护规则组。
解码设置	针对用户请求、提交的数据按照设置的编码类型进行解码操作，以免存在绕过WAF的请求，导致恶意payload被后端执行。在规则状态开关**打开**时，点击**配置解码方式**，根据需要选中或取消选中要解码的格式。默认解码方式：URL解码、JsUnicode解码，二者不可取消勾选。

防护规则说明

检测模块	防护等级
SQL注入检测模块、XSS检测模块、命令执行检测模块、文件包含攻击检测模块、文件上传攻击检测模块、敏感信息泄漏检测模块、Webshell检测模块、Java 代码注入检测模块、PHP 代码注入检测模块、NODEJS 代码注入检测模块、扫描器检测模块	中等、宽松、严格、自定义

解码设置说明

解码方式	操作
URL解码、JsUnicode解码、Hex解码、XML解析、JSON解析、Form解析、Base64解码、路径标准化	选中、取消

设置访问控制规则

网站接入Web应用防火墙后，您自定义基于精准匹配条件的访问控制规则。可用于盗链防护、网站管理后台保护等场景。您可以根据实际需求配置自定义规则。

前提条件

- 已开通Web应用防火墙实例。
- 已完成网站接入。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择防护配置 > 网站防护。
3. 在顶部域名选择区，切换要设置的域名。
4. 点击**访问控制**页签，点击**新建规则**按钮。
5. 在**新增规则**表单中，完成规则定义，详情参见规则匹配条件。

下表描述了新增规则时需设定的参数。 **参数** **说明**

规则名称	为规则命名。
匹配字段	详见规则匹配条件。
匹配方式	详见规则匹配条件。
匹配内容	详见规则匹配条件。
处置动作	详见规则匹配条件。
风险等级	自定义风险等级标签，可选无风险、低威、中威、高危

6. 点击**确定**，规则定义成功，自动启用。您可在规则查看新建的规则。并根据需要关闭、编辑或删除规则。

设置地域封禁

使用地域封禁可以对指定的中国各省份及海外来源IP进行一键黑名单封禁，阻断所有来自指定地区的访问请求。

前提条件

- 已开通Web应用防火墙实例。
- 已完成网站接入。

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**防护配置** > **网站防护**。
3. 在顶部域名选择区，切换要设置的域名。
4. 点击**地域封禁**页签，开启**防护状态**开关。
5. 点击**添加**按钮，勾选需要封禁的地区，完成后点击**确定**。
6. 返回**地域封禁**页签，点击**保存**按钮。

执行结果

完成设置后，来自被封禁地区IP的所有访问请求都将被阻断。

设置CC安全防护

网站接入Web应用防火墙后，您可针对特定的URL路径实现自定义匹配规则、识别方式，自由设置访问频率限制和阻断时间、方式，实现规则自由定义，为网站拦截针对页面请求的CC攻击（拦截后返回403拦截提示页面）。您可以根据实际需求修改CC安全防护的防护策略。

前提条件

- 已开通Web应用防火墙实例。
- 已完成网站接入。

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**防护配置** > **网站防护**。
3. 在顶部域名选择区，切换要设置的域名。
4. 点击**CC防护**页签，点击**新建规则**按钮。
5. 在**新增/编辑规则**表单中，完成以下规则配置。

下表描述了CC防护规则需要配置的参数。	参数	说明
规则名称	为规则命名。	
匹配字段	目前仅支持匹配PATH字段。	
匹配方式	适用的逻辑符，可选： **前缀比配**：匹配字段的前缀包含匹配内容。 **精准匹配**：匹配字段完全符合匹配内容。	

匹配内容	PATH字段的匹配内容为：访问请求的URL路径。
识别方式	识别请求数量的依据。可选： **IP**：单一源IP的请求数量。 **cookie**：具有相同自定义cookie内容的请求数量。
Cookie名称：	识别方式选择**Cookie**时，需填写该参数。
检测时长(秒)	统计周期。
访问次数	统计时长内统计对象的允许数量，超过阈值，则触发限制。
处理动作	定义触发规则后执行的操作。可选： **拦截**：拦截访问请求。 **人机识别**：进行人机验证，完成验证后自动加白1分钟。
加黑时长(秒)	触发规则后，设置封禁时长，范围1~3600

6. 点击**确定**，规则定义成功，自动启用。您可在规则查看新建的规则。并根据需要关闭、编辑或删除规则。

规则匹配条件说明

Web应用防火墙的CC防护规则和访问控制规则（黑白名单设置）都需要定义规则匹配条件。本文档具体描述了规则匹配规则中支持使用的字段及其释义。

匹配条件和处置动作

您可以为您的WAF实例自定义访问控制规则和CC安全防护规则。每条规则由匹配字段与处置动作构成。在创建规则时，您通过设置匹配字段、匹配方式和相应的匹配内容定义匹配条件，并针对符合匹配条件规则的访问请求定义相应的处置动作。

匹配条件

匹配条件由**匹配字段**、**匹配方式**、**匹配内容**组成。匹配内容需按照选择的匹配方式填写对对应格式的内容。访问请求满足匹配条件即命中该规则，并执行相应的处置动作。

处置动作

匹配动作由**拦截**、**监听**、**放行**组成。拦截表示阻断访问请求；监听表示不拦截请求，但在控制台记录监听日志，放行表示将请求加白。

匹配字段详述

下表描述了匹配条件中支持使用的匹配字段。	匹配字段	支持的版本	适用的逻辑符	字段描述
IP	所有版本	等于、不等于 属于网段、不属于网段	访问请求的来源IP，支持填写IP或IP/掩码（例如，1.1.1.1/24）。	
URL	所有版本	包含、不包含、 正则匹配、正则不匹配、 等于、不等于	访问请求的URL地址。	
REFERER	所有版本	包含、不包含、 正则匹配、正则不匹配、等于、 不等于	访问请求的来源网址，即该访问请求是从哪个页面跳转产生的。	
USER-AGENT	所有版本	包含、不包含、 正则匹配、正则不匹配、等于、 不等于	发起访问请求的客户端的浏览器标识、渲染引擎标识和版本信息等浏览器相关信息。	
PATH	仅企业版	包含、不包含、 正则匹配、正则不匹配、等于、 不等于	访问路径；用户请求中从 / 开始到 ？ 结束的部分	
COOKIE	仅企业版	包含、不包含、 正则匹配、正则不匹配、等于、 不等于	访问请求中的Cookie信息。	

COOKIE_ARGS	仅企业版	包含、不包含、正则匹配、正则不匹配、等于、不等于	访问请求中Cookie指定参数值
CONTENT_TYPE	仅企业版	包含、不包含、等于、不等于	访问请求指定的响应HTTP内容类型
X_FORWARDED_FOR	仅企业版	包含、不包含	访问请求的客户端真实IP。X-Forwarded-For（XFF）用来识别通过HTTP代理或负载均衡方式转发的访问请求的客户端最原始的IP地址的HTTP请求头字段，只有通过HTTP代理或者负载均衡服务器转发的访问请求才会包含该项。
REQUEST_HEADERS	仅企业版	包含、不包含、正则匹配、正则不匹配、等于、不等于	访问请求的头部信息
FILES	仅企业版	包含、不包含、正则匹配、正则不匹配、等于、不等于	HTTP 请求中上传文件的文件名
HOST	仅企业版	等于、不等于	HTTP 请求头中的 Host
METHOD	仅企业版	等于、不等于	访问请求的方法，如GET、POST等
URI_ARGS	仅企业版	包含、不包含、正则匹配、正则不匹配、等于、不等于	访问请求中的GET参数值
POST_ARGS	仅企业版	包含、不包含、正则匹配、正则不匹配、等于、不等于	访问请求中的POST参数值
CONTENT_LENGTH	仅企业版	值大于等于、值小于	访问请求的内容所包含的字节数
HEADER_LENGTH	仅企业版	值大于、值小于	访问请求的请求头所包含的原始字节数(包含请求行)，值为WAF回源长度，非客户端原始字段长度

匹配方式中的逻辑符

下表描述了匹配方式中的逻辑符含义

逻辑符	说明
等于、不等于	匹配字段等于、不等于匹配内容。
包含、不包含	匹配字段包含、不包含匹配内容。
值小于、值大于等于	匹配字段的值小于、大于等于匹配内容。
正则匹配、正则不匹配	匹配字段符合、不符合匹配内容中定义的正则表达式。

自定义防护规则组

金山云Web应用防火墙支持用户自定义搭建防护规则组，为具体的检测模块创建有针对性的防护策略。在设置Web入侵防护时，如果三种默认规则组无法满足业务需求，可使用自定义防护规则组。

前提条件

- 已开通Web应用防火墙实例。
- 已完成网站接入。

功能介绍

- 您可在新建规则组后，将其应用到已接入的网站域名。同时，您可按规则组维度修改其关联的网站域名。
- 您可修改自定义规则组的基本信息，默认规则组不支持修改。

新建规则组

1. 进入Web应用防火墙控制台网站防护页面。
2. 点击**Web入侵防护**页签，**配置规则组**按钮，进入规则组配置页面。
3. 点击**新建规则组**按钮，进入**新增规则组**配置页面，完成如下配置。

第一步：设置规则组信息

设置规则组信息包括设置规则组基本信息及设置防护等级，具体说明见下表。

参数	说明
规则组名称	必填，设置自定义规则组的名称
规则组描述	自定义规则组的详细信息描述
应用配置模板	可选择一种默认规则组作为基准后，调整各检测模块的防护等级

完成配置后，点击**下一步**按钮，规则组信息被保存后进入**第二步：应用到网站**配置，或者点击**直接保存**按钮，新建规则组将被保存，页面回退到上一级。

第二步：应用到网站

在**待接入网站**中选择需要关联该规则组的网站，点击右移按钮，将网站移入至**已接入网站**中，点击**保存**按钮。

4. 新建规则组配置完成。

编辑自定义规则组

仅自定义规则组支持编辑，默认规则组不可编辑

1. 进入Web应用防火墙控制台网站防护页面。
2. 点击**Web入侵防护**页签，**配置规则组**按钮，进入规则组配置页面。
3. 点击自定义规则组操作列的**编辑**按钮，进入编辑规则组页面。
4. 完成配置变更后，点击保存按钮，规则组生效。

应用到网站

1. 进入Web应用防火墙控制台网站防护页面。
2. 点击**Web入侵防护**页签，**配置规则组**按钮，进入规则组配置页面。
3. 点击规则组操作列的**应用到网站**按钮，在**待接入网站**中选择需要关联该规则组的网站，点击右移按钮，将网站移入至**已接入网站**中，点击**确定**按钮。

删除自定义规则组

4. 进入Web应用防火墙控制台网站防护页面。
5. 点击**Web入侵防护**页签，**配置规则组**按钮，进入规则组配置页面。
6. 点击自定义规则组操作列的**删除**按钮。
7. 点击**确定**按钮则立即删除，或者点击**取消**按钮返回规则组配置页面。

注意：删除自定义防护规则组前，请确保规则组未被应用到任何网站上。如果需要删除的规则组被应用到网站上，您必须先为网站应用其他规则组，才能删除当前规则组。