Web 应用防火墙

用户指南

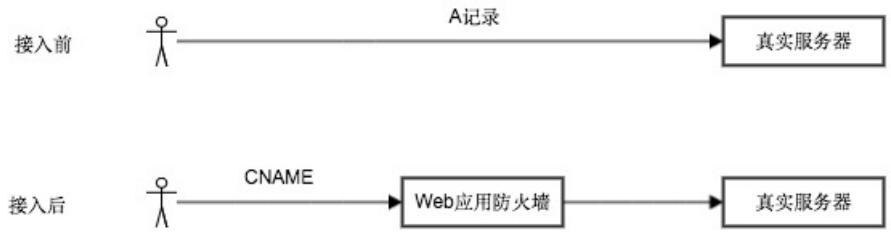
用户指南

接入指南

CNAME接入指南

在Web应用防火墙控制台完成域名配置后，您必须将域名解析指向CNAME，让所有访问流量切换至Web应用防火墙，才能让您的网站域名受到Web应用防护墙的防护。

流量逻辑图



当系统检测到您所配置的网站域名未正确接入Web应用防火墙时，您在**云盾Web应用防火墙管理控制台>管理>域名配置**页面已添加的网站域名的**DNS解析状态**中将收到“未检测到CNAME接入且无流量”的异常提示。

- DNS解析状态自动检测该网站域名的解析是否指向CNAME，并检测最近数分内容内该域名的访问流量是否经过Web应用防火墙。

  DNS解析状态的CNAME接入检测每一小时执行一次，流量检测每数分钟执行一次。如果您确认已将网站域名解析正确接入Web应用防火漆的CNAME，可在一小时后再次查看DNS解析状态。

  说明：该提示仅用于提醒您将网站域名接入Web应用防火墙，不会因此而影响您网站的访问。

如果您在配置完成网站域名解析后，该网站域名的DNS解析状态仍然提示异常，且显示“未检测到CNAME接入且无流量”或是“当前无流量”等错误信息，请查看DNS解析状态异常。

接入前准备

在将您的网站域名通过CNAME方式接入Web应用防火墙进行防护前，您需要完成以下准备工作：

该网站域名必须可以通过公网访问

该网站域名必须已完成备案

说明：您可以通过阿里云为您的网站域名提交备案申请，更多详情请查看备案导航。

确认该网站域名是否已接入或需要接入CDN、高防IP等其它代理型系统

准备DNS管理员权限，修改DNS记录切换防护网站流量

如果该网站域名需要通过HTTPS协议访问，您还需要准备好相应的证书内容和私钥。

说明：一般情况下，您所需准备的证书相关内容包括*.crt（公钥文件）或*.pem（证书文件），和*.key（私钥文件）两个文件。

接入步骤

说明：以下接入步骤适用于仅使用Web应用防火墙对网站域名进行防护的场景，即该网站域名不接入CDN、高防IP等其它代理型服务。关于需要将Web应用防火墙与其它代理型服务结合部署的场景，请查看：

CDN结合Web应用防火墙的配置方法，请参考CDN结合WAF。

DDoS高防服务结合Web应用防火墙的配置方法，请参考高防IP结合WAF。

DDoS高防服务+CDN+Web应用防火墙的配置方法，请参考高防+CDN+WAF。

步骤 1： 网站配置

定位到云盾Web应用防火墙管理控制台>**管理**>**网站配置**页面，点击**“添加网站”**按钮，根据提示结合业务情况进行配置。

回源设置是指您希望WAF把请求转发到的地址，通常来说就是真实服务器的地址（如ECS的IP），也可以是SLB的IP，如果您是线下业务，填写公网IP即可。如果您希望WAF防护的目标使用域名接入（如OSS的CNAME、AWS的CNAME等），则需要选择域名回源，将对应的域名填进去（而不是接入防护的网站域名）

具体配置请点击“控制台配置”

注意事项

如果该网站域名需要支持通过HTTPS协议访问，您还需要参考以下步骤在云盾Web应用防火墙管理控制台中为该网站域名上传相应的证书。

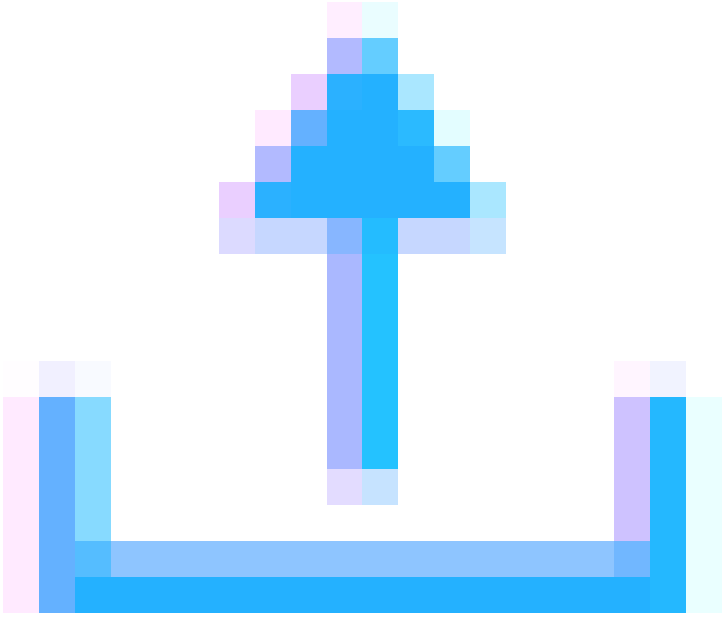
准备所需证书信息。

如果您的证书是通过阿里云云盾证书服务所购买的，您可以在云盾证书服务管理控制台，选择您的证书，单击**下载**，并选择类型下载证书。

说明：所下载的证书一般包括*.pem（证书文件）和*.key（私钥文件）两个文件。

如果您的证书是通过其他渠道所购买的，您可以联系相应的证书供应商获得证书文件或寻求技术支持。

定位到云盾Web应用防火墙管理控制台>**管理**>**域名配置**页面，选择网站域名，单击



（上传证书按钮）上传证书。

说明：如果您的证书是通过阿里云云盾证书服务所购买的，您可以单击**选择已有证书**，直接选择您已购买的证书即可。

步骤2： 本地测试

将业务流量正式切换到Web应用防火墙前，建议您先通过本地验证的方式确保WAF转发规则配置正常后，再修改网站域名的DNS解析记录，防止因配置错误而导致您业务的中断。

关于具体的本地测试方法，请查看本地验证方法。

步骤3： 准备获取访问者真实IP的方法

将业务流量正式切换到Web应用防火墙后，对于该网站的访问就不再是简单地从用户的浏览器直达服务器，中间将至少经过Web应用防火墙进行转发。在这种情况下，您需要通过额外的方法获得真正发起请求的真实客户端IP。

说明：一般情况下，当一个透明的代理服务器将用户的请求转到下一环节的服务器时，会在HTTP的头部增加一条X-Forwarded-For记录，用于记录用户的真实IP，其形式为X-Forwarded-For:用户IP。因此，如果真实客户端与网站服务器中间经历了多个代理服务器，X-Forwarded-For将以该形式来展示所经过的代理服务器IP及真实用户IP：X-Forwarded-For:用户IP, 代理服务器1-IP, 代理服务器2-IP, 代理服务器3-IP, ……。

因此，在将您的网站域名正式接入Web应用防火墙防护后，您可以使用X-Forwarded-For的方式来获取访问者真实IP。关于具体的配置方法，请查看获取访问者真实IP配置方法。

步骤4： 切换DNS解析记录（正式接入Web应用防火墙防护）

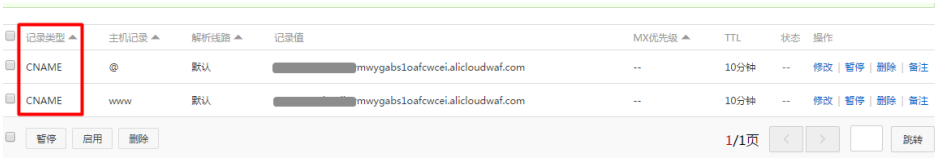
修改您的网站域名的DNS解析，将该网站域名接入Web应用防火墙进行防护。

将鼠标移至已添加的网站域名记录，获取Web应用防火墙已为该域名所分配的CNAME地址。

说明：单击复制**CName**可将该CNAME地址复制到剪贴板。

说明：以下操作步骤以万网域名提供商为例进行描述。如果网站使用的是其它域名提供商，您参考以下操作步骤并结合实际域名管理控制台变更您的网站域名的DNS解析记录。

登录万网控制台，修改您的网站域名的解析记录。



- **记录类型**：修改为CNAME。
- **主机记录**：填写对应的子域名（例如，www.aliyundemo.cn的主机记录为”www”，aliyundemo.cn的主机记录为”@”）。
- **记录值**：填写Web应用防火墙已分配的CNAME地址。
- **TTL**：即域名缓存时间，可按照您的实际需求填写（一般建议设置为600秒）。

填写完成后，单击**保存**，完成解析记录的变更。

注意事项

同一个主机记录，CNAME解析记录值只能填写一个，您需要修改为Web应用防火墙所分配的CNAME地址。

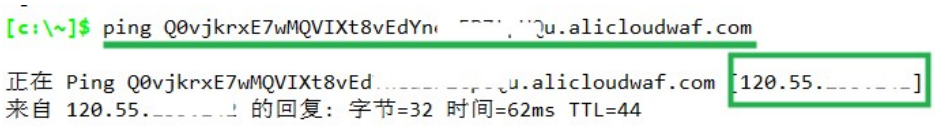
同一个主机记录，A记录和CNAME记录是互斥的。您需要修改为CNAME类型，并填入Web应用防火墙所分配的CNAME地址。

如果DNS服务商不允许直接将A记录的解析记录修改为CNAME记录，您需要先删除该A记录后，再增加CNAME类型的解析记录。

注意：整个删除、新增过程应尽可能在短时间内完成，确保网站访问不中断。如果删除A记录后长时间没有添加CNAME类型解析记录，可能导致域名解析失败。

MX记录和CNAME记录是互斥的。如果您的网站域名必须保留MX记录，可以通过使用A记录指向Web应用防火墙的IP来进接入Web应用防火墙防护。

您可以通过对Web应用防火墙分配的CNAME地址使用Ping命令来获取所分配的Web应用防火墙IP。然后将A记录类型的解析记录中的记录值修改为该Web应用防火墙IP。



警告：如果您采用A记录方式将网站域名接入Web应用防火墙防护，Web应用防火墙将无法进行故障集群调度和故障bypass操作。

步骤5： 源站保护

将网站域名正式接入Web应用防火墙防护后，您还需要为源站配置相应的保护措施。

源站保护是防止攻击者在获取源站服务器的真实IP后，绕过Web应用防火墙直接攻击您的源站，导致您的业务遭受恶意攻击。

说明：源站保护配置不是必须的。即使不配置源站保护，也不会影响正常业务转发。

一般情况下，建议您通过配置源站ECS的安全组或源站SLB的白名单，防止恶意攻击者直接攻击您的源站。关于具体的源站保护方法，请查看源站保护配置。

WAF源站负载均衡

WAF的源站支持最多20个IP，配置如下图：

假设源站有三个，可以按照这样配置。效果是，WAF会按照IP Hash的方式去做负载均衡（注意：IP HASH的方式决定了如果源IP不够分散，可能会出现负载不均的情况），并且会对多个源站做健康检查，当WAF发现有某个IP不可用时，会停止向这个IP分发请求，直到其恢复为止。

注意，如果WAF前面有接高防、CDN等七层代理，务必勾选“是否已使用高防、CDN、云加速等代理”。

HTTPS高级配置

WAF提供灵活的HTTPS功能，可以帮您在不需要改造源站的情况下，一键实现全站HTTPS或强制客户端使用HTTPS认证。

配置步骤

参照以下步骤，来执行HTTPS高级配置：

登录到阿里云云盾Web应用防火墙控制台，并前往 网站配置。

单击目标域名操作列下的 **编辑**。

在 **协议类型** 下，勾选 **HTTPS**，并单击打开 **高级设置** 菜单。

HTTP站点一键HTTPS化（默认回源端口是80端口）

如果您的网站不支持HTTPS回源，请 **开启HTTP回源**，通过WAF实现HTTPS访问。使用该设置后，客户端可以通过HTTP和HTTPS方式访问站点。

注意：使用HTTP回源，可以无需在源站服务器上做任何改动，也不需要配置HTTPS。但是，该配置的前提是 **在WAF上传正确的证书和私钥**（证书可以在阿里云证书免费申请）。

一键强制HTTPS

如果您需要强制客户端使用HTTPS来访问（从安全性考虑，我们也更推荐这样做），可以 **开启HTTPS的强制跳转。**

开启HTTPS强制跳转后，HTTP回源可以根据具体需求来开启/关闭。若同时开启HTTP回源，WAF会将客户端的HTTP请求重定向到HTTPS，并且设置客户端的HSTS属性（周期为一天），支持HSTS的客户端后续会直接使用HTTPS访问，不支持的（目前浏览器基本都支持）通过重定向方式实现，不会受影响。

非标端口支持

Web应用防火墙默认支持下列端口：

- HTTP: 80, 8080
- HTTPS: 443, 8443

在企业版、旗舰版提供更多非标端口支持，其中：

说明： 详细支持端口见后文。

- 每个企业版用户支持**最多10个不同**的端口（包含80/8080/443/8443端口）
- 每个旗舰版用户支持**最多50个不同**的端口（包含80/8080/443/8443端口）
- 按量付费开通的Web应用防火墙支持**最多50个不同**的端口（包含80/8080/443/8443端口）

注意：

- 上述限制是针对每个用户（即每个Web应用防火墙实例）生效。一个WAF实例下有多个域名时，各域名所使用的不同端口总数不能超过上述标准。
- 不支持的端口Web应用防护墙既不会防护，也不会转发。例如，4444端口的业务请求到达Web应用防火墙后，请求会直接被丢弃。

HTTP支持的端口（企业版和旗舰版）：

80,81,82,83,84,88,89,800,808,1000,1090,3333,3501,3601,5000,5222,6001,6666,7000,7001,7002,7003,7004,7005,7006,7009,7010,7011,7012,7013,7014,7015,7016,7018,7019,7020,7021,7022,7023,7024,7025,7026,7070,7081,7082,7083,7088,7097,7777,7800,8000,8001,8002,8003,8008,8009,8020,8021,8022,8025,8026,8077,8078,8080,8081,8082,8083,8084,8085,8086,8087,8088,8089,8090,8091,8106,8181,8334,8336,8800,8686,8888,8889,8999,9000,9001,9002,9003,9080,9200,9999,10000,10001,10080,12601,86,9021,9023,9027,9037,9081,9082,9201,9205,9207,9208,9209,9210,9211,9212,9213,48800,87,97,7510,9180,9898,9908,9916,9918,9919,9928,9929,9939,28080,33702,

HTTPS支持的端口（企业版和旗舰版）：

443,4443,5443,6443,7443,8443,9443,8553,8663,9553,9663,18980

Web应用攻击防护规则策略

功能描述

Web应用防火墙针对攻击防护（防护SQL注入、XSS跨站等常见Web应用攻击）提供不同规格的防护策略，包括：宽松、正常、严格。

配置步骤

按照以下步骤，来配置攻击防护规则策略：

登录到阿里云云盾Web应用防火墙控制台，并前往 **网站配置**。

单击目标域名操作列下的 **防护配置**。

在 **Web应用攻击防护** 下，选择 **防护** 模式，并在 **防护规则策略** 下拉框中选择相应的策略。

规则建议

- 默认使用 **正常** 模式规则。
- 当您发现在正常模式规则下存在较多误拦截，或者业务存在较多不可控的用户输入（例如富文本编辑器、技术论坛等），建议您选择 **宽松** 模式。
- 当您需要更严格地防护路径穿越、SQL注入、命令执行时，建议您选择 **严格** 模式。

恶意IP封禁

行业背景

Web 应用程序往往是黑客们最喜欢下手的攻击目标。通过阿里云云盾的大数据平台分析发现，每个开放在互联网上的Web应用，每天都会遭受数以千计的Web攻击。这些攻击主要可以分为几类：

- 针对全网的工具批量扫描
- 针对某个用户的工具定向扫描
- 黑客手动发起的定向渗透攻击

传统的 Web 应用防火墙产品，基本都是针对 IP-URL 维度的拦截。当判定一个请求是攻击行为后，仅仅把这个请求进行单次阻断。而实际上，恶意攻击者们日复一日地在对您的网站进行扫描、攻击，黑客可能一个通宵都在挖掘您网站的漏洞，研究防护策略并尝试绕过。

功能介绍

针对这种情况，云盾 Web 应用防火墙推出了恶意 IP 惩罚功能。当一个 IP 被 WAF 识别到正在进行持续的攻击行为时，WAF 自动封禁该被标识的恶意 IP。

云盾 WAF 利用阿里云平台积累的海量恶意 IP 库和机器学习功能，对发起攻击的 IP 的行为、攻击频率进行学习分析，生成判定规则。当发起攻击的 IP 的行为被判定为持续攻击行为，直接阻断这个 IP 的所有访问请求。

配置方法

登录云盾Web应用防火墙管理控制台。

单击**域名配置**。

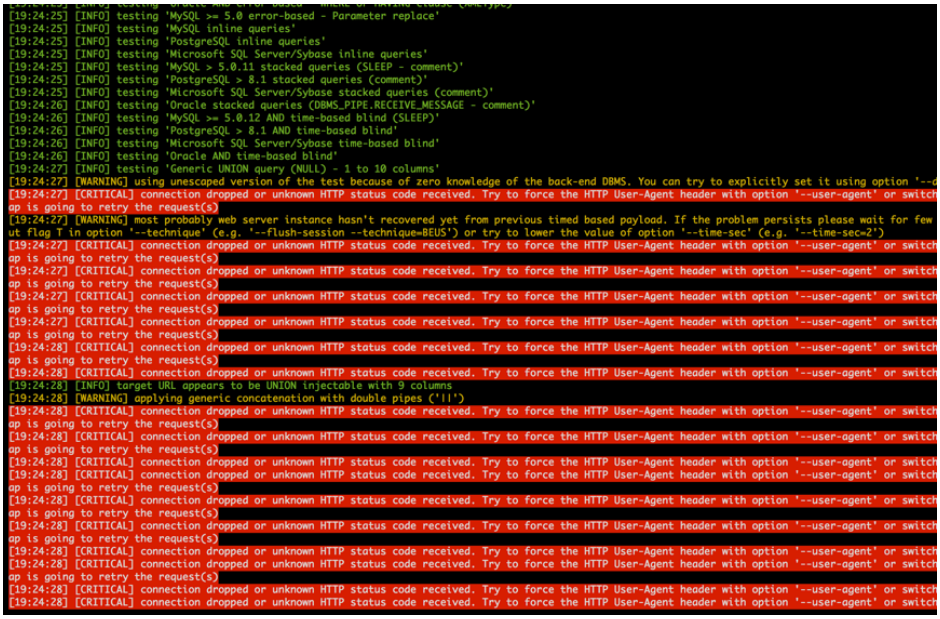
选择您想要防护的域名，单击**防护设置**。

单击启用**恶意IP惩罚**。

启用恶意 IP 惩罚功能之后，当您的防护网站遭受扫描器扫描或黑客持续攻击时，WAF 在很短的时间内就会识别并阻断攻击 IP 的所有访问行为，极大增加黑客的攻击成本。

测试实例

启用恶意 IP 惩罚功能后，使用黑客工具 SQLMAP 对已防护的网站进行 SQL 注入攻击扫描。



云盾 WAF 在短时间内就拦截了这个攻击 IP 的所有请求，阻止攻击者继续攻击。

通过启用 **恶意 IP 惩罚** 功能，可以十分有效地屏蔽各类自动化工具、扫描器发起的攻击，保护您的网站业务安全。

选择CC防护模式

功能描述

Web应用防火墙提供不同模式的CC安全防护（拦截机器恶意CC攻击），包括：正常、攻击紧急。

注意：紧急模式适用于网页/H5页面，但不适用于API/Native App业务（会造成大量误杀），对于后者，建议您使用 自定义CC防护。

配置步骤

您可以参照以下步骤，来配置CC安全防护模式：

登录到阿里云云盾Web应用防火墙控制台，并前往 网站配置。

单击目标域名操作列下的 **防护配置**。

在 **CC安全防护** 下，开启防护并选择相应防护模式。

模式选择建议

- 默认使用 **正常** 模式。此模式误杀较少，只针对特别异常的请求进行拦截。
- 当发现有正常模式无法拦截的CC攻击时，您可以选择 **攻击紧急** 模式。此模式拦截CC攻击效果较强，但可能会造成较多误杀。
- 如果发现 **攻击紧急** 模式仍然漏过较多攻击，建议您检查流量来源是否为WAF回源IP。如果发现有攻击直接攻击源站，您可以设置暂时只允许WAF回源IP访问服务器。
- 如果您希望有更好的防护效果，同时有更低的误杀。您可以选择Web应用防火墙企业版和旗舰版，自定义或让安全专家为您定制针对性的防护算法。

CC防护规格

不同的产品规格针对各种复杂的CC攻击提供不同的防护效果。

- **高级版**：支持默认的防护模式（正常、攻击紧急），阻拦攻击特征明显的CC攻击。
- **企业版**：支持自定义访问控制规则，防护某些具有攻击特征的CC攻击。
- **旗舰版**：专家定制防护规则，保障防护效果。

规格详情请参照 Web应用防火墙价格详情页。

为什么有些CC攻击需要升级企业版才能防护？

阿里云Web应用防火墙，通过人机识别、大数据分析、模型分析等技术识别攻击，对攻击进行拦截。但不同于

与程序交互，安全攻防是人与人的对抗，每个网站的性能瓶颈也不同，黑客会在发现一种攻击无效后，分析网站后进行定向攻击。此时，通过云盾安全专家介入分析，可以提供更高的防护等级和防护效果。

自定义CC防护

功能简介

WAF企业版及以上版本支持CC自定义防护功能。您可以在控制台自定义防护规则，限制特定路径（URL）对您服务器的访问频率。例如，您可以配置如下规则：当单个源IP在10秒内访问 www.abc.com/login.html 超过20次时，封禁该IP一小时。

配置步骤

按照以下步骤，来自定义CC防护规则：

登录到阿里云云盾Web应用防火墙控制台，并前往 网站配置。

单击目标域名操作列下的 **防护配置**。

在 **CC安全防护** 下，选择 **正常** 防护模式，并单击 **前去配置** 配置自定义规则。

单击 **新增规则**，添加一条规则。其中，

- URI：指定需要防护的具体地址。例如，/register。支持输入参数，如 /user?action=login。
- 匹配规则：完全匹配或前缀匹配。
  - 完全匹配即精确匹配，请求地址必须与此处配置完全一样才会统计。
  - 前缀匹配是包含匹配，只要是请求的URI以此处配置开头就会统计（例如，/register.html会被统计）。
- 检测时长：指定统计访问次数的周期。需要和访问次数配合。
- 单一IP访问次数：指定在统计周期内，允许单个源IP访问该URL的次数。
- 阻断类型：指定触发条件后的操作，可以是封禁或人机识别。

- 封禁：触发条件后，直接断开连接。
- 人机识别：触发条件后，用重定向的方式去访问客户端，通过验证后才放行。

阻断时间：指定执行阻断动作的时间。

以图中的配置为例，其含义为：单个IP访问目标地址（精确匹配）时，一旦在10秒内访问超过20次，就封禁该 IP 600 分钟。

精准访问控制

什么是精准访问控制规则

精准访问规则指对常见的HTTP字段（如IP、URL、Referer、UA、参数等）进行条件组合，配置支持业务场景定制化的防护策略，可用于盗链防护、网站管理后台保护等精准访问控制策略配置。

精准访问控制规则由匹配条件与匹配动作构成。

匹配条件

匹配条件包含匹配字段、逻辑符、匹配内容三大要素。通过设置匹配字段、逻辑符和相应的匹配内容定义匹配

条件，针对符合匹配条件规则的访问请求定义相应的动作。

说明：匹配内容暂时不支持通过正则表达式描述；匹配内容允许设置空值。

匹配字段	字段描述	适用逻辑符
IP	IP代表访问请求的来源IP。	- 属于 - 不属于
URL	URL代表访问请求的URL地址。	- 包含 - 不包含 - 等于 - 不等于
Referer	Referer代表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。	- 包含 - 不包含 - 等于 - 不等于 - 长度小于 - 长度等于 - 长度大于 - 不存在
User-Agent	User-Agent代表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。	- 包含 - 不包含 - 等于 - 不等于 - 长度小于 - 长度等于 - 长度大于
Params	Params代表访问请求的URL地址中的参数部分，通常指URL中”?”后面的部分。例如，www.abc.com/index.html?action=login中的action=login就是参数部分。	- 包含 - 不包含 - 等于 - 不等于 - 长度小于 - 长度等于 - 长度大于
Cookie	Cookie代表访问请求中的Cookie信息。	- 包含 - 不包含 - 等于 - 不等于 - 长度小于

		- 长度等于 - 长度大于 - 不存在
Content-Type	Content-Type代表访问请求指定的响应HTTP内容类型，即MIME类型信息。	- 包含 - 不包含 - 等于 - 不等于 - 长度小于 - 长度等于 - 长度大于
X-Forwarded-For	X-Forwarded-For代表访问请求的客户端真实IP。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。	- 包含 - 不包含 - 等于 - 不等于 - 长度小于 - 长度等于 - 长度大于 - 不存在
Content-Length	Content-Length代表访问请求的响应内容所包含的字节数。	- 值小于 - 值等于 - 值大于
Post-Body	Post-Body代表访问请求的响应内容信息。	- 包含 - 不包含 - 等于 - 不等于
Http-Method	Http-Method代表访问请求的方法，如GET、POST等。	- 等于 - 不等于
Header	Header代表访问请求的头部信息，用于自定义HTTP头部字段。	- 包含 - 不包含 - 等于 - 不等于 - 长度小于 - 长度等于 - 长度大于 - 不存在

说明：包年包月模式WAF高级版与按量付费模式WAF的精准访问控制基础防护功能仅支持IP、URL、Referer、User-Agent匹配字段，且最多只能定义10条精准访问控制规则。

注意事项：

- 每一条精准访问控制规则中最多允许设置三个匹配条件进行组合。
- 同一条精准访问控制规则中的多个匹配条件之间是“与”的逻辑关系，即访问请求必须同时满足所有匹配条件才算命中该精准访问控制规则，并执行相应的匹配动作。

匹配动作

精准访问控制规则支持以下四种匹配动作：

- **阻断**：符合匹配条件的访问请求将被直接阻断。
- **放行**：符合匹配条件的访问请求将被放行。
- **告警**：符合匹配条件的访问请求将被放行，同时WAF会对该请求进行告警。
- **captcha**（人机识别验证）：符合匹配条件的访问请求需要通过人机识别验证后方可继续访问。

说明：其中，选择**放行**、**告警**或**captcha**匹配动作后，您可进一步设置该请求是否需要继续经过其它WAF防护功能过滤，包括Web应用攻击防护、CC应用攻击防护、智能防护、地区封禁、数据风控、SDK防护等。即未被精准访问控制规则阻断的请求是否进一步经过其它WAF防护功能的检测。

精准访问控制排序

精准访问控制规则之间是有先后匹配顺序的，即访问请求将根据所设定的精准访问控制规则依次进行匹配，顺序较前的精准访问控制规则优先匹配。

您可以通过规则排序功能对所有精准访问控制规则进行排序，以获得最优的防护效果。

操作步骤

您可以参考以下操作步骤，为已防护的域名配置精准访问控制：

登录到云盾Web应用防火墙控制台，定位到**管理**>**网站配置**。

选择已添加的网站域名记录，单击**防护配置**。

定位到**精准访问控制**功能项，开启该功能并单击**前去配置**配置精准访问控制规则。

单击**新增规则**，设置规则的匹配条件和相应的匹配动作，单击**确定**，即可为该域名添加精准访问控制规则。

说明：在精准访问控制规则列表页面，单击**规则排序**，通过单击**上移**、**下移**等可调整精准访问控制规则的排序。

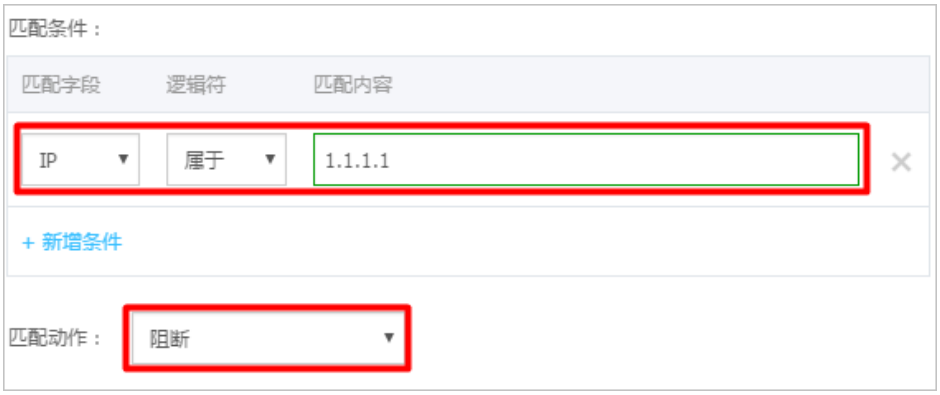
精准访问控制配置示例

精准访问控制规则支持多种配置方法，您可以结合自身业务特点定义相应的规则。

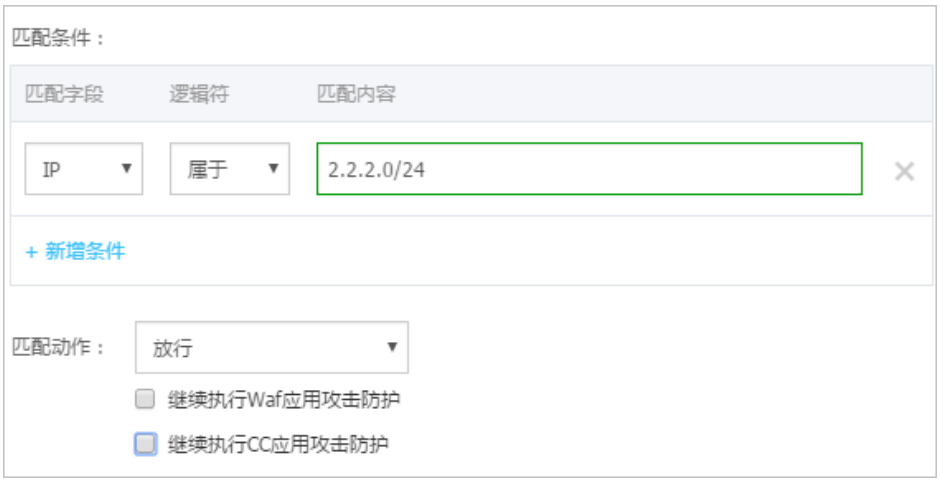
您甚至可以通过设置精准访问控制规则实现特定的Web漏洞防护。

配置IP黑白名单

通过设置以下精准访问控制规则，阻断来自1.1.1.1的所有访问请求。



通过设置以下精准访问控制规则，放行来自2.2.2.0/24网段的所有访问请求。



注意：应用此白名单配置规则时，请不要勾选**继续执行Waf应用攻击防护**和**继续执行CC应用攻击防护**等选项，不然访问请求仍可能被WAF的其它防护功能所拦截。

拦截特定的攻击请求

通过分析某类特定的WordPress反弹攻击，发现其特征是User-Agent字段都包含WordPress。

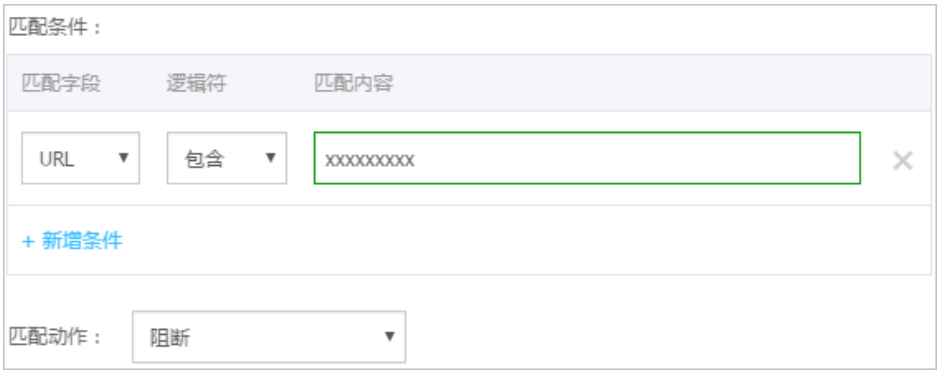
UA
WordPress/4.2.10; http://ascsolutions.vn; verifying pingback from 191.96.249.54
WordPress/4.0.1; http://146.148.63.90; verifying pingback from 191.96.249.54
WordPress/4.6.1; https://www.nokhostinsabt.com; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://eadastage.lib.umd.edu; verifying pingback from 191.96.249.54
WordPress/3.5.1; http://danieljromo.com
WordPress/4.2.4; http://wd.icopy.net.tw; verifying pingback from 191.96.249.54
WordPress/4.6.1; http://kmgproje.com; verifying pingback from 191.96.249.54
WordPress/4.1.6; http://www.vv-atalanta.nl; verifying pingback from 191.96.249.54
WordPress/4.5; http://23.83.236.52; verifying pingback from 191.96.249.54
WordPress/4.6.1; http://playadelrey.news; verifying pingback from 191.96.249.54
WordPress/4.1; http://hostclick.us; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://mosaics.pro; verifying pingback from 191.96.249.54
WordPress/4.0; http://www.chinavrheadset.com; verifying pingback from 191.96.249.54

因此，可以设置以下精准访问控制规则，拦截该类WordPress反弹攻击请求。

关于WordPress攻击的详细防护配置，请参考防御WordPress反射。

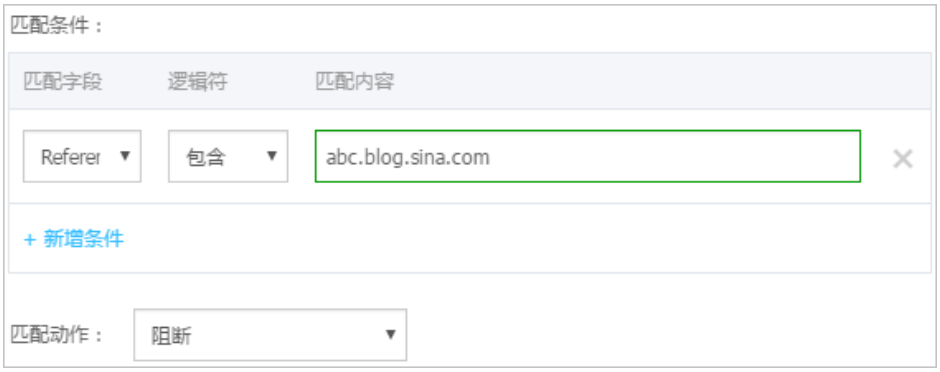
封禁特定的URL

如果您遇到有大量IP在刷某个特定且不存在的URL，您可以通过配置以下精准访问控制规则直接阻断所有该类请求，降低源站服务器的资源消耗。



防盗链

通过配置Referer匹配字段的访问控制规则，您可以阻断特定网站的盗链。例如，您发现abc.blog.sina.com大量盗用本站的图片，您可以配置以下精准访问控制规则阻断相关的访问请求。



黑白名单配置

在WAF中，您可以通过配置精准访问控制规则来添加黑白名单，添加的黑白名单仅针对配置的特定域名生效。

操作步骤

登录云盾Web应用防火墙管理控制台。

定位到**管理**>**网站配置**，找到需要配置黑/白名单的域名，单击**防护配置**。

定位到精准访问控制功能模块，打开精准访问控制开关，单击**前去配置**。

单击**新增规则**，新增一条防护规则。例如，放行源IP属于 1.1.1.1 的所有访问。

说明：如果想完全放行这个IP的所有请求，则不要勾选匹配动作下方的继续执行其它防护选项。如果勾选，则来自这个IP的部分请求仍然可能被相应防护的规则拦截。

同理，您也可以参考此方法为指定域名配置黑名单。

更多信息

同一条防护规则中的多条匹配条件之间是“与”的关系。因此，如果您想添加多个IP/IP段，需要配置多条访问控制规则。

说明：防护规则中的IP支持掩码格式，例如 1.1.1.0/24；逻辑符支持选择“不属于”。例如，当您想只允许来自某个网段（如公司网段）的请求访问某个域名时，可参考以下配置：

多条防护规则之间存在优先级，按照精准访问控制列表展示从上到下的顺序进行匹配，通过单击右上角的**规则排序**可以调整防护规则之间的优先级。

封禁地区

该功能支持对特定地区的来源IP进行封禁，目前在WAF企业版及以上提供支持：

在对应的域名开启防护模块后，可对封禁的地区进行设置，目前支持国内各省份和海外，IP归属地信息来自淘宝IP库（http://ip.taobao.com）：

智能防护引擎

Web应用防火墙的新智能防护引擎针对请求进行语义分析，通过语义化检测引擎深度发现伪装隐藏的恶意Web请求内容，有效拦截攻击者利用攻击混淆、变种等方式发起的恶意攻击。

注意： 启用新智能防护引擎功能项，您需要升级至Web应用防火墙企业版或以上版本。

功能概述

新智能防护引擎针对访问请求进行语义分析，将语义化分析结果在异常攻击集中进行匹配，从而发现伪装、隐藏的恶意Web攻击行为。

说明： 智能防护引擎主要针对SQL注入等Web攻击方式，而非CC攻击。如果您对Web攻击防护有较高的要求，建议您启用新智能防护引擎功能。

- **语义化**： 新智能防护引擎将同类攻击行为中的同类行为特征进行归并，将同一类的攻击行为和攻击特征聚合为一个攻击特征。通过将攻击行为的多个行为特征组成的特定的排列组合来表示同一类攻击，从而实现攻击行为的语义化。
- **异常攻击集**： 基于阿里云云盾自身的海量运营数据，对正常的Web应用进行建模并从正常的模型中区分出异常情况后，从繁多的Web应用攻击中提炼出异常攻击模型，从而形成异常攻击集。

关于智能防护引擎的详细介绍，请查看大道至简：探秘智能语义检测引擎的武林。

操作步骤

登录Web应用防火墙管理控制台。

定位到**管理**>**网站配置**页面。

选择已接入防护的域名，单击**防护配置**。

启用**新智能防护引擎**功能项。

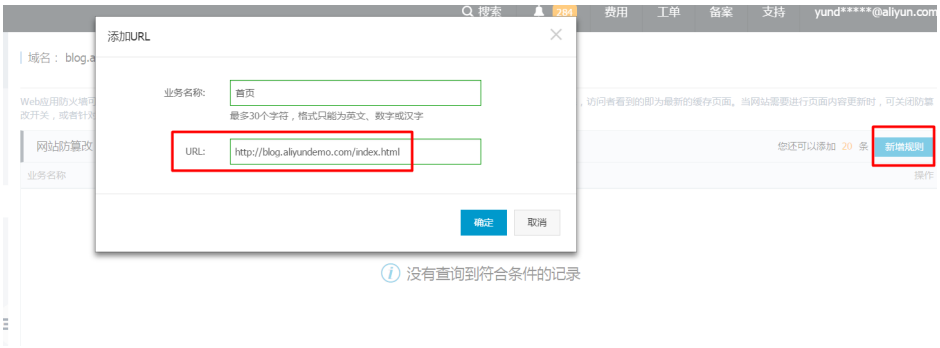
网页防篡改

WAF在**高级版及以上版本**支持网页防篡改功能，可以对指定的敏感页面进行缓存，缓存后即使源站页面内容被

恶意篡改，WAF也会返回预先缓存好的页面内容，从而确保正常用户看到正确的页面。

开启网页防篡改功能，找到对应的域名，点击防护配置->网页防篡改，打开开关：

点击前去配置，新增规则，配置要防护的具体页面：



URL请填写精确的路径，不支持通配符（如/*）或参数（如/abc?xxx=），防篡改的内容格式支持text/html和图片。

配置好后，需要手动打开防护状态的开关后方可开始缓存，否则WAF还是返回源站的实际页面内容：

打开开关后，WAF会对该页面进行缓存，缓存完毕后，对这个页面的请求WAF将全部返回最近一次缓存的页面内容。如果您的页面进行了内容更新，可以手动点击“更新缓存”按钮进行更新，否则WAF将始终返回上一次

更新缓存时的页面内容：

注：缓存的生效时间取决于被缓存页面的大小，一般情况下都在1分钟之内。

数据风控

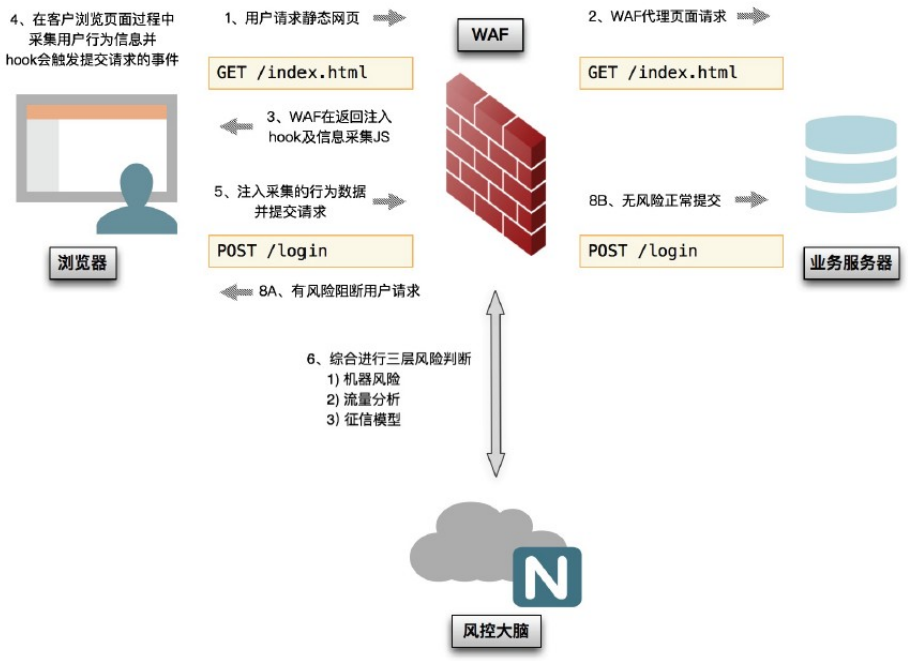
功能说明

数据风控为WAF基于阿里云的大数据能力，通过业内领先的风险决策引擎，结合人机识别技术，防止包括但不限于下列场景的关键业务欺诈行为：

- 垃圾注册
- 短信验证码滥刷
- 撞库、暴力破解
- 恶意抢购、秒杀、薅羊毛、抢红包
- 机器人抢票、刷票、恶意投票
- 垃圾消息等

数据风控在WAF高级版及以上提供。接入数据风控，不需要服务器或客户端做任何改造，只需要接入WAF，即可轻松获取风控能力。

数据风控的工作流程如下图所示：



下面以一个例子来说明数据风控的防护场景：

用户小白有一个网站：www.abc.com， 普通用户可以通过www.abc.com/register.html 注册成为会员。近来小白发现，有黑客在用一些恶意的脚步频繁提交注册请求，注册大量垃圾账户来参与他举办的抽奖活动（江湖人称羊毛党），这些请求跟正常的请求很像，频率又不是太高，传统的CC防护很难分辨出这种恶意请求。

于是小白接入WAF并启用了www.abc.com 这个域名的数据风控。同时因为小白最关心的业务是www.abc.com/register.html， 所以针对这个URL配置了特定请求防护。

从配置生效的那一刻起，WAF会做下面这些事情：

观察和分析每一个访问www.abc.com 这个域名，包括首页及其子路径的用户的各种行为是否有异常，并结合阿里云大数据的信誉库去判断这个源IP是否有风险；

当用户提交注册请求到www.abc.com/register.html 时，由于WAF针对这个URL配置了请求防护，WAF会基于这个用户从开始访问本站，到提交注册请求之间的行为和征信特征来判断这个用户是否可疑。比如如果一个用户没有任何前置操作就直接提交了一个注册请求，则这个请求就很值得怀疑；

如果WAF基于之前的行为判断这是一个正常的用户，则该用户将不会有任何感知的去完成注册过程；

如果WAF觉得这个请求是可疑的，或是该客户端IP曾经有过不良的记录，则会弹出验证滑块去验证用户的身份，通过验证的用户会继续完成注册；

如果滑块验证通过，但通过的方式很可疑（比如用脚本去模仿真人滑动过程等），WAF会继续进行其他的验证，直到完全放心为止；

如果无法通过验证，则WAF会最终阻断该请求。

在整个过程中，数据风控是针对整个域名（www.abc.com）开启的，也就意味着，WAF需要对这个域名下的全部页面插入js代码来判断客户端是否可信。而真正的防护和验证，是针对www.abc.com/register.html 这个特定接口生效的，直到这里WAF才会对具体的请求做出干涉：如果客户端之前的行为可信，则不加干预直接放行，反之则需要通过考验才能继续。

风控的拦截页面如下图所示：

注意事项

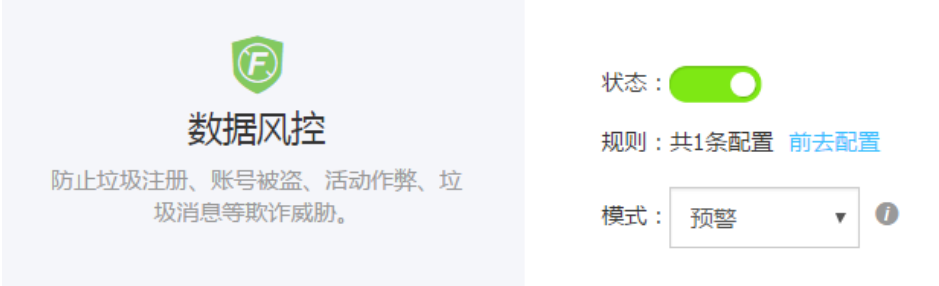
直接请求风控防护的URL一定会被弹出滑块验证，所以请确保配置的防护地址在正常情况下不会被直接提交（即正常用户应该是经过一系列前置的访问才会请求这个地址）。

特别的，直接调用API的场景也不适用于数据风控的场景，会被风控拦截。因API调用也是直接发起的机器行为，会无法通过风控的人机识别验证。当然，如果是真人点击页面某个按钮调用了API服务，是可以使用风控的。

配置方法

找到需要开启风控防护的域名，点击防护配置：

在页面下方，找到数据风控，打开开关，并点击“前去配置”。注意，风控默认是在预警模式，预警模式下，风控不会对任何请求进行拦截，但依然会在页面插入js进行客户端行为分析：



点击新增防护请求来添加一条防护规则，这里以注册接口为例：

注意，**这里填写的地址应该是执行业务动作的接口地址，而不是这个页面本身的地址**，以下面的注册页面为例：

假设这个页面本身的地址为www.abc.com/new_user ，获取验证码按钮对应的接口是www.abc.com/getsmscode ，注册按钮对应的接口是www.abc.com/register.do ，则风控防护的具体地址应该配置为：

```
www.abc.com/getsmscode //防护短信接口被刷
www.abc.com/register.do //防止垃圾注册
```

而不应该是www.abc.com/new_user 这个页面地址（如配这个地址，有正常用户直接访问该页面时也会有验证滑块弹出，影响体验）。

另，风控也支持目录防护，如配置www.abc.com/book/*， 则可防护这个路径下的所有请求，**但不支持配置全站防护（www.abc.com/*），会导致用户访问首页也弹出滑块。**

排查日志

您可以结合日志检索功能来排查风控的监控和拦截情况：

通过风控验证的日志情况如下：

正常用户经过风控验证的访问请求URL会带上一个ua开头的参数，但请求会被转发到源站，也会收到正常响应。

被风控拦截的日志情况如下：

但如果直接请求这个接口，一般不会带上ua参数（或带着伪造的ua参数），请求会被WAF拦截，这时对应的日志是看不到源站响应的。

综上，您可以使用日志检索->高级搜索->URL关键字功能，搜索配置风控的接口，并排查拦截情况。

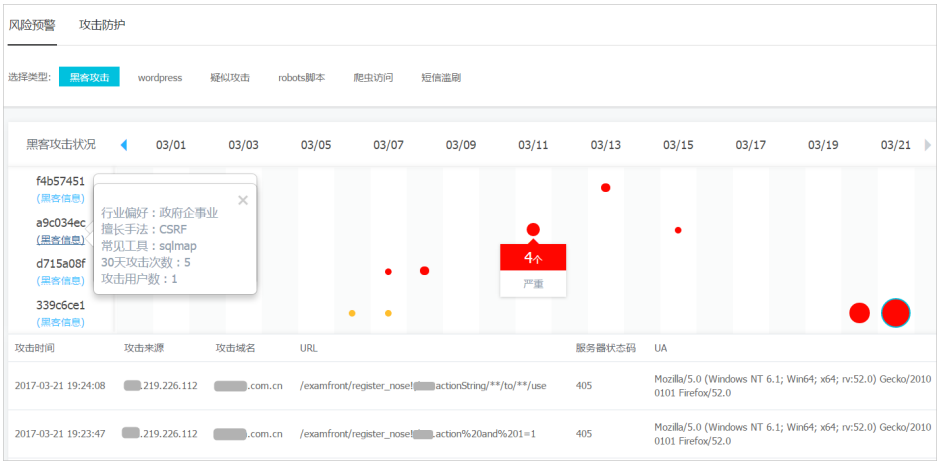
如果有其他问题，请提工单联系我们。

风险预警

Web应用防火墙提供的安全报表，支持根据一些常见攻击的特征对您的业务进行风险预警和提示。您可以登录Web应用防火墙控制台，并前往 风险预警 页面查看具体的风险请求类别、特征、目标接口地址、源IP等信息。本文介绍了支持的预警类型和相应的防护建议。

黑客攻击

风险预警提供基于阿里云大数据分析和攻击溯源能力的黑客画像功能。该功能对在您的网站进行过踩点、扫描、攻击等恶意行为的黑客进行标识和记录，标记出的黑客都是现实中具有真实身份的个人。当您收到这类告警信息时，意味着您的站点已经被某个“记录在案”的黑客盯上了。



图中的圆点代表黑客在相应日期的活动情况，单击具体的圆点可以看到详细的攻击记录。其中：

- 不同的行代表不同的黑客个体，点击黑客信息可以看到这个黑客的特征信息。
- 颜色越深表示攻击行为的危害性越大。
- 圆点越大表示当日攻击次数越多。

防护建议

告警中显示的攻击均已被WAF拦截，您无需担心。建议您保持对服务器非Web业务的安全关注，因为黑客可能会综合采用各种手段渗透您的站点（如SSH、数据库端口等）。

WordPress攻击

风险预警参照 防御WordPress反射 中描述的攻击特征进行检测。如果此类预警数量巨大，极有可能是您的服务器近期遭到了这样的CC攻击。

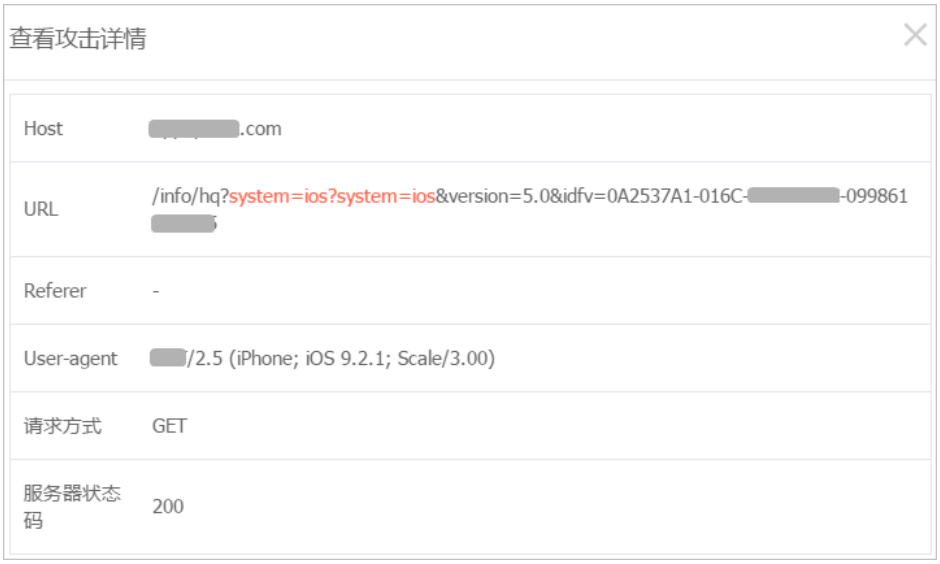
防护建议

参考上述文档中的防护建议，配置 精准防护规则 来进行防护。

疑似攻击

WAF基于大数据分析的异常检测算法模型筛选出可疑的访问请求，其中可能包含异常的参数名称、类型、顺序、特殊符号、语句等，供您结合业务特征做进一步的分析和防护。

风险预警对异常的部分标红提醒。例如，下图中所示的请求包含了两个重复的参数，并且没有用常规的 “&”来连接。



防护建议

此处的告警只是异常请求，可能是特殊业务的正常请求，也可能是变种的攻击，请结合自身业务的特点进行分析。

Robots脚本

WAF支持检测一些常见的机器脚本工具特征（比如python2.2、httpclient）。如果您近期没有用测试工具提交大量请求，该告警数字可能意味着您的站点受到了一些机器脚本工具的恶意请求或探测，也可能包含一些用以进行流量压测或者CC攻击的工具。

防护建议

可结合日志分析排查是否有CC攻击，并结合 精准访问控制、紧急模式、区域封禁 等防护算法拦截恶意攻击。

爬虫访问

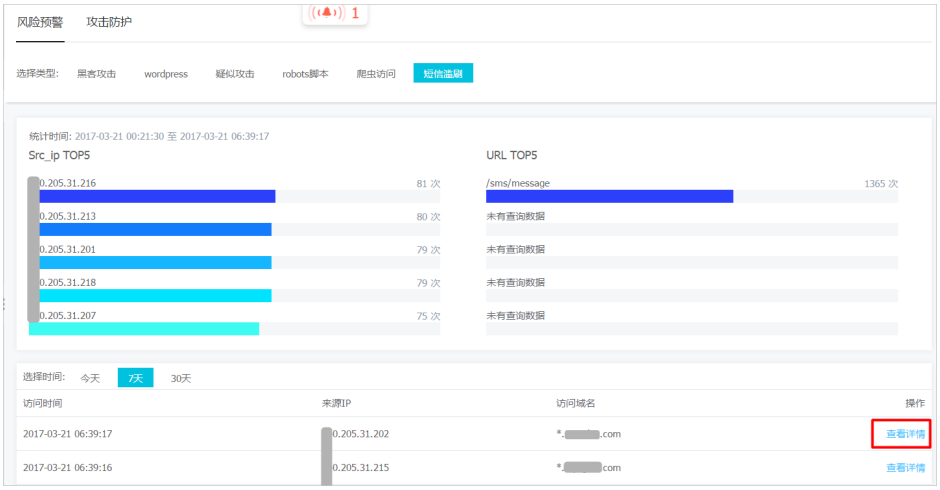
WAF支持检测爬虫请求（包含合法的爬虫，如百度蜘蛛等）。如果该报警数字很大，同时服务器有请求量异常增大，CPU升高等现象，则可能是遇到了伪装成爬虫的CC攻击或恶意爬虫的爬取。

防护建议

可结合日志和服务器性能分析排查是否有CC攻击或恶意爬虫请求。请参考 拦截恶意爬虫 的说明。WAF不会拦截合法的爬虫（如百度爬虫等）请求。

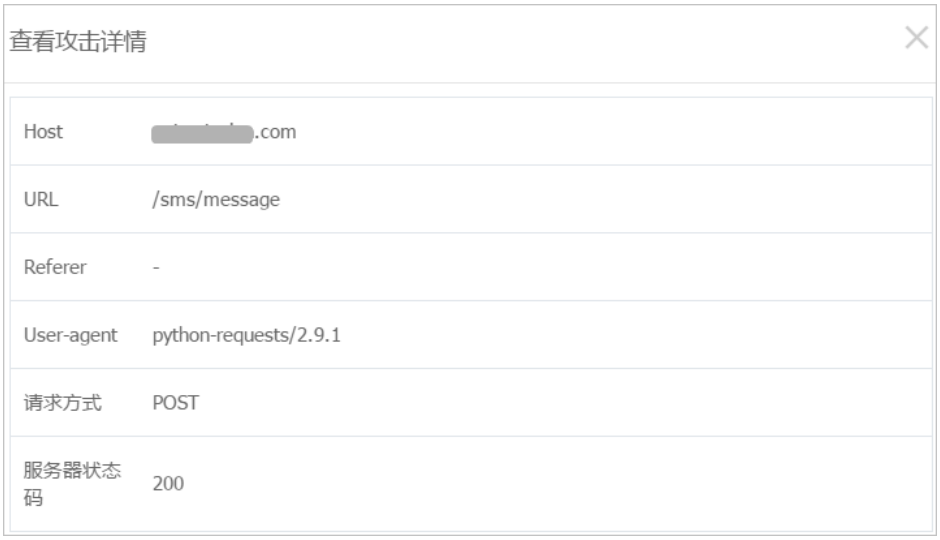
短信滥刷

WAF支持检测对短信注册、短信验证等接口的请求。如果该告警数字数量巨大，则很可能有人在恶意滥刷您的短信接口（可造成高额的短信开销费用）。



防护建议

点击查看详情可以看具体的请求：



您可以结合请求最多的源IP和接口去分析是否是正常的业务调用。如果不是，建议使用 **数据风控** 或 **自定义CC防护功能**，对被刷接口进行防护。

全量日志查询

注意： 如果您使用的是包年包月模式的Web应用防火墙，需要升级至企业版或更高版本（海外地区需要升级至旗舰版）使用全量日志查询功能；如果您使用的是按量付费模式的Web应用防火墙，可以在**云盾Web应用防火墙管理控制台>设置>功能与规格**页面的**高级特性**区域，勾选并付费启用**全量日志查询**功能，启用后将按照按量付费价格总览中的收费标准计费。

功能概述

全量日志功能将记录您网站的所有访问请求日志，通过一键智能搜索快速定位请求记录，满足您在运维、安全方面的管理需求。

通过全量日志功能，您可以轻松地完成以下运维工作：

- 确认某个具体请求是否被WAF拦截或放行
- 确认某个具体拦截是由Web攻击、CC攻击防护或是自定义的访问控制规则触发
- 查询源站对于某个具体请求的响应时间，观察是否超时等
- 通过源IP、URL关键字、cookie、referer、user-agent、X-forwarded-for、服务器响应状态码等条件组合查询具体的请求

说明： 您启用全量日志查询功能，即表示您允许阿里云记录您全部经过WAF的web请求（POST数据不会被记录）。

操作步骤

开启日志检索

使用日志检索功能之前，需要在**网站配置**页面为指定的网站域名开启日志检索功能。只有开启**日志检索**功能后WAF才会开始记录该网站的访问日志。

说明： 只记录开启日志检索功能后的访问记录，而开启前的访问记录不会被记录。

登录云盾Web应用防火墙管理控制台，定位到**管理**>**网站配置**页面。

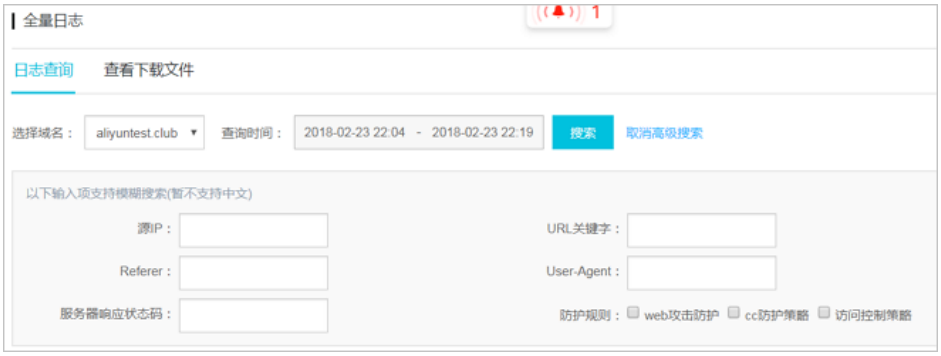
选择**中国大陆**或**海外地区**。

选择已添加的网站域名，在**日志检索**栏，单击开启日志检索功能。

查询全量日志

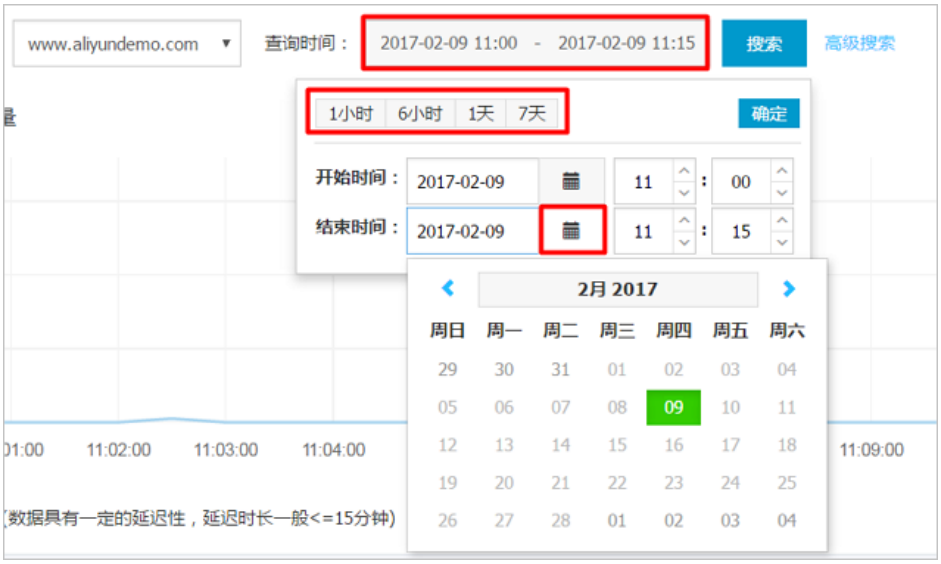
为网站域名开启日志检索功能后，您就可以在**全量日志**页面查询该网站的访问日志。

登录云盾Web应用防火墙管理控制台，定位到**统计**>**全量日志**页面。



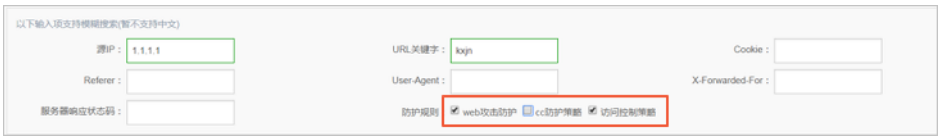
选择**域名**，设置**查询时间**，单击**搜索**。

说明： 全量日志功能最多记录最近一个月内的访问日志。



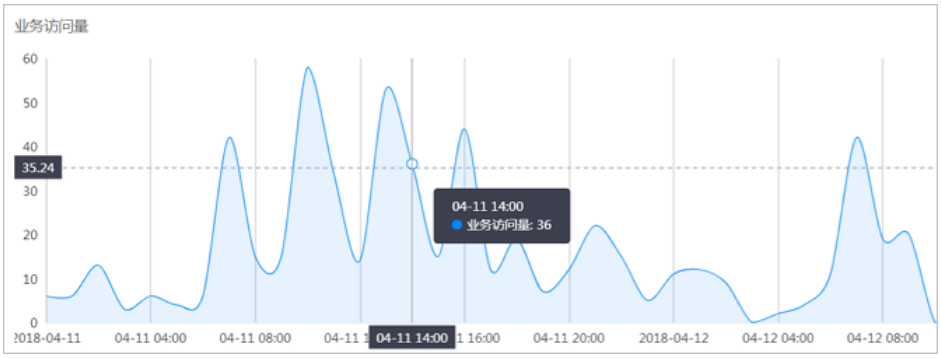
您也可以单击**高级搜索**，设置更详细的检索条件。

说明： 除了支持设置源IP、URL关键字、cookie、referer、user-agent、X-forwarded-for、服务器响应状态码等条件，您还可以通过勾选**防护规则**筛选命中相应WAF防护规则的访问请求记录。



查看日志检索结果。

在**业务访问量**区域，查看检索时间范围内的访问请求量趋势图。



在**访问日志**列表中，查看符合检索条件的访问请求记录。例如，被CC攻击防护规则拦截的访问请求记录如下图所示。

关于源站响应信息中的参数含义说明

- **Status**： 指源站返回给WAF的响应状态。如果返回“-”，表示没有响应（例如该请求被WAF拦截或源站响应超时）。
- **Upstream_ip**：指该请求所对应的源站IP。例如，WAF回源到ECS的情况，该参数即返回源站ECS的IP。
- **Upstream_time**：指源站响应WAF请求的时间。如果返回“-”，代表响应超时。

单击**全量日志**页面右上方的**日志下载**可为当前检索到的日志结果生成下载任务。下载任务生成完成后，在**查看下载文件**页签中即可将相应格式的日志文件下载到本地。

注意： 如果您在开启日志检索功能期间停用日志检索功能，则停用期间的访问请求日志不会被记录；即使重新开启日志检索功能，您也无法查询到停用期间的访问请求日志。

可视化大屏

依托用户接入WAF后的业务日志，WAF产品提供可视化大屏，将数据转化为直观的可视化报表，对WAF实时的攻防态势进行监控和告警，为用户提供可视化、透明化的数据分析、决策能力，让安全攻防一目了然。

功能说明

WAF可视化大屏可以提供以下展示指标项：

- **网络流量态势**

以秒级数据维度，展示出业务访问入方向流量、出方向流量、访问QPS，集中体现了业务运行的稳定性和网络的质量。

- **业务访问态势**

通过访问日志可以展示业务来访者中的出访问最频繁的TOP来访IP、IP全国、省市级地域分布、访问者浏览器占比、UserAgent占比分布、系统占比，以及服务器的响应状态码。

- **安全攻防态势**

展示Web应用防火墙在检测、防御拦截过程中的指标，包括:攻击源TOP IP 、拦截趋势、拦截比例、命中规则TOP、攻击事件类型，体现出实时防御效果。

最终效果

产品SLA

- 展示数据的时间颗粒度、展示维度可以根据用户需求定制；

开通方法

如果您有可视化展示的需求，可以通过钉钉与我们沟通，您将“当面”获得阿里云Web安全大屏专家的建议和定制化方案。

注：

1.服务时间：5*8，不含法定节假日（非此时间内，您遇到紧急问题，仍可以使用该方式沟通）

2.仅限于已经购买使用了WAF服务付费用户。

SDK接入文档

SDK方案简介

SDK方案解决什么问题

SDK方案专门针对原生App端，提供可信通信、防机器脚本滥刷等安全防护，可以有效识别高风险手机、猫池、牧场等特征。

该方案集成了阿里巴巴集团和阿里云多年来对抗黑灰产、羊毛党的经验和技术积累。接入SDK后，您的App将

获得与天猫、淘宝、支付宝等客户端相同的可信通信技术，并共享阿里巴巴集团对抗黑灰产、羊毛党的恶意设备指纹库，从根本上解决App端的安全问题。

SDK方案帮助您解决以下 **原生App** 端的问题：

- 恶意注册、撞库、暴力破解
- 针对App的大流量CC攻击
- 短信/验证码接口被刷
- 薅羊毛、抢红包
- 秒杀限时限购商品
- 恶意查票、刷票（如机票酒店等）
- 价值咨询爬取（如价格、征信、融资、小说）
- 机器批量投票
- 灌水、恶意评论

SDK方案如何接入

参照以下步骤，将您的App接入SDK。

登录 云盾Web应用防火墙控制台，在 **网站配置** 页面，将App使用的域名添加进来，开启WAF防护。

在App域名解析服务商处，添加CNAME记录，将App域名解析指向WAF。

在App中集成WAF提供的SDK组件（点击下载SDK）。该操作通常需要1-2天时间。

注意：集成SDK不需要您在服务器端做任何改动。WAF会过滤掉恶意流量，将合法的请求回源给源站，恶意请求带来的压力也全部由WAF承担。

打包发布新的App版本，享受SDK防护。

SDK的详细接入方法，请参见：

- iOS接入文档
- Android接入文档

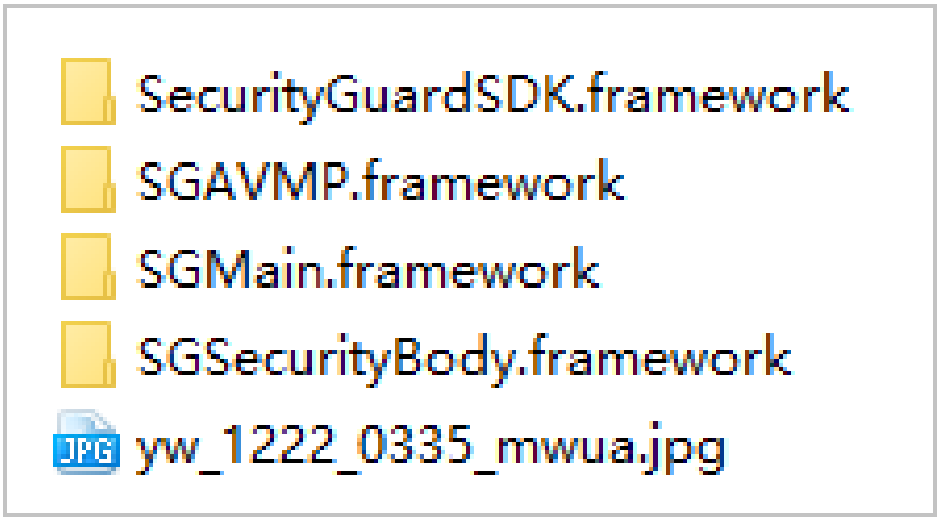
如果您对方案/接入有任何问题，请扫描下方的钉钉二维码联系我们（进群时请说明咨询SDK方案）。

iOS 接入文档

本文介绍了使用 iOS App 接入 WAF SDK 的操作方法。

SDK-iOS 文件说明

下载并解压 WAF SDK 包（点击获取SDK），在 sdk-iOS 文件夹下，提供了以下文件：



各文件说明如下：

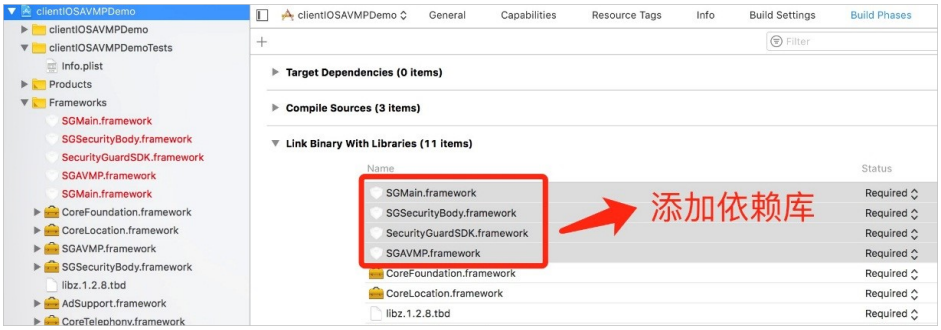
文件	功能
SGMain.framework	主框架SDK
SecurityGuardSDK.framework	基础安全插件
SGSecurityBody.framework	人机识别插件

SGAVMP.framework	虚拟机插件
yw_1222_0335_mwua.jpg	配置文件

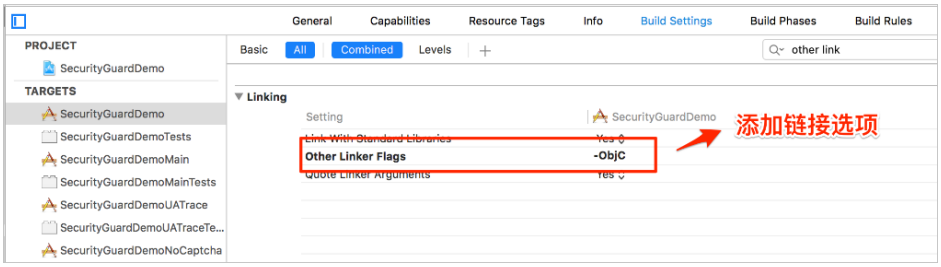
项目工程配置

参照以下步骤，来配置项目工程。

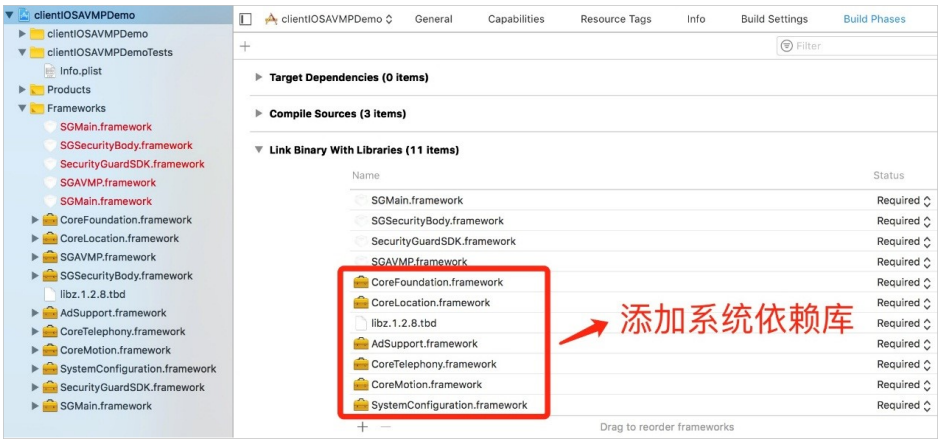
添加 Framework。将 WAF SDK 中提供的 4 个 .framework 文件添加到工程的依赖库中。



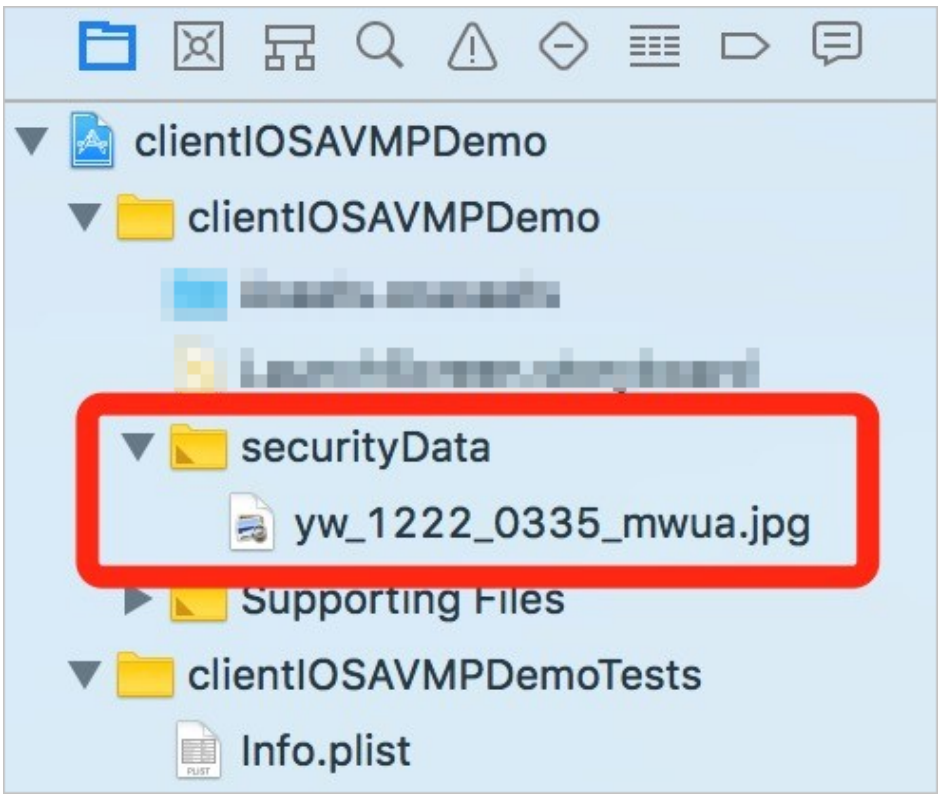
设置链接选项。



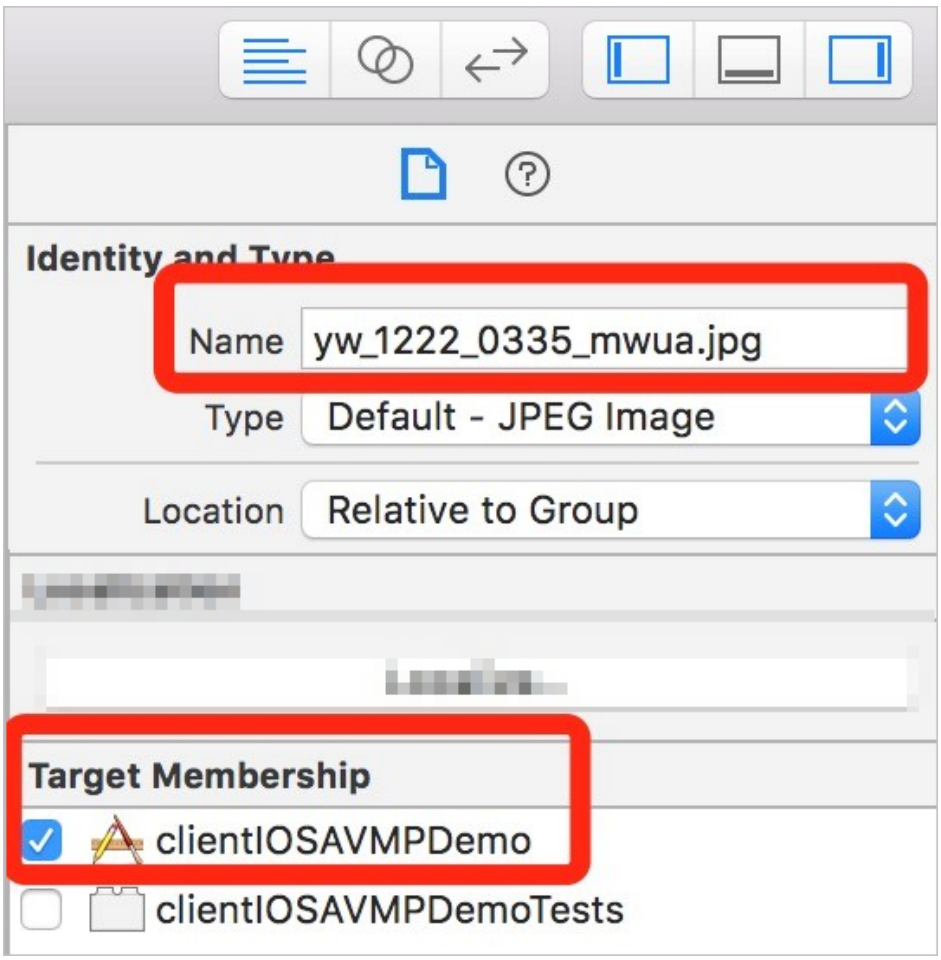
添加系统依赖库。



引入配置文件。将 SDK 中的 yw_1222_0335_mwua.jpg 配置文件加到 mainbunle 下。



在应用集成多个 target 的情况下，请确认 yw_1222_0335_mwua.jpg 配置文件加入到正确的 Target Membership 中。



代码编写

1. 初始化SDK

接口定义

```
+ (BOOL) initialize;
```

接口描述

功能：初始化SDK。

参数：无。

返回值：BOOL类型。初始化成功返回YES，失败返回NO。

调用方式

```
[JAQAVMPSignature initialize];
```

示例代码

```
static BOOL avmpInit = NO;
- (BOOL) initAVMP{
@synchronized(self) { // just initialize once
if(avmpInit == YES){
return YES;
}
avmpInit = [JAQAVMPSignature initialize];
return avmpInit;
}
}
```

2. 签名请求数据

接口定义

```
+ (NSData*) avmpSign: (NSInteger) signType input: (NSData*) input;
```

接口描述

功能：使用 avmp 技术对 input 的数据进行签名处理，并且返回签名串。

参数：见下表。

参数名	类型	是否必须	说明
signType	NSInteger	是	签名使用的算法，目前是固定值，输入 3。
input	NSData*	否	待签名的数据，一般是整个请求体。如果请求体为空，那么此参数使用 null。

返回值：NSData*类型，返回签名串。

调用方式.

```
[JAQAVMPSignature avmpSign: 3 input: request_body];
```

示例代码

客户端向服务器端发送数据时，需要调用 avmpSign 接口对整个 body 数据进行签名处理，之后会得到签名串。该签名串就是 wToken。

```
# define VMP_SIGN_WITH_GENERAL_WUA2 (3)

- (NSString*) avmpSign{

@synchronized(self) {
NSString* request_body = @"i am the request body, encrypted or not!";

if(![self initAVMP]){
[self toast:@"Error: init failed"];
return nil;
}

NSString* wToken = nil;
NSData* data = [request_body dataUsingEncoding:NSUTF8StringEncoding];
NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2 input:data];
if(sign == nil || sign.length <= 0){
return nil;
}else{
wToken = [[NSString alloc] initWithData:sign encoding: NSUTF8StringEncoding];
return wToken;
}
}
}
```

注意：如果请求体为空，也需要调用 avmpSign 接口生成 wToken，第二个参数直接传空即可。示例代码如下。

```
NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2 input:nil];
```

3. 将 wToken 放进协议头

示例代码如下：

```
#define VMP_SIGN_WITH_GENERAL_WUA2 (3)

-(void)setHeader
{
NSString* request_body = @"i am the request body, encrypted or not!";
NSData* body_data = [request_body dataUsingEncoding:NSUTF8StringEncoding];

NSString* wToken = nil;
NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2 input:body_data];
wToken = [[NSString alloc] initWithData:sign encoding: NSUTF8StringEncoding];
```

```
NSString *strUrl = [NSString stringWithFormat:@"http://www.xxx.com/login"];
NSURL *url = [NSURL URLWithString:strUrl];
NSMutableURLRequest *request =
[[NSMutableURLRequest alloc]initWithURL:url cachePolicy:NSURLRequestReloadIgnoringCacheData
timeoutInterval:20];

[request setHTTPMethod:@"POST"];

// set request body info
[request setHTTPBody:body_data];

// set wToken info to header
[request setValue:wToken forHTTPHeaderField:@"wToken"];

NSURLConnection *mConn = [[NSURLConnection alloc]initWithRequest:request delegate:self
startImmediately:true];
[mConn start];
// ...
}
```

4. 发送数据到服务器

将修改好协议头的数据发送到 WAF，并解析 wToken 进行风险识别，拦截恶意请求后，再把合法请求回源。

错误码

上述的 initialize 和 avmpSign 接口有可能会出现异常。如果生成签名串异常或失败，请在 console 中搜索“SG Error”。

常见错误信息及描述见下表。

错误代码	含义
1901	参数不正确，请检查输入的参数。
1902	图片文件有问题。一般是获取图片文件时的 apk 签名和当前程序的 apk 签名不一致。请使用当前程序的 apk 重新生成图片。iOS 可能是因为 BundleID 不匹配。
1903	图片文件格式有问题。
1904	请升级新版本图片。AVMP 签名功能仅支持 v5 图片。
1905	没有找到图片文件。请确保图片文件 yw_1222_0335_mwua.jpg 在工程中。
1906	图片中缺少 AVMP 签名对应的 byteCode。请检查使用的图片是否正确。
1907	初始化 AVMP 失败，请重试。
1910	非法的 avmpInstance 实例。可能原因有： - AVMPInstance 被 destroy 后，调用

	InvokeAVMP。 - 图片 byteCode 版本与 SDK 不匹配。
1911	加密图片的 byteCode 没有相应导出的函数。
1912	AVMP 调用失败。请联系我们。
1913	AVMPInstance 被 destroy 之后，调用 InvokeAVMP 出现该错误。
1915	AVMP 调用内存不足，请重试。
1999	未知错误，请重试。

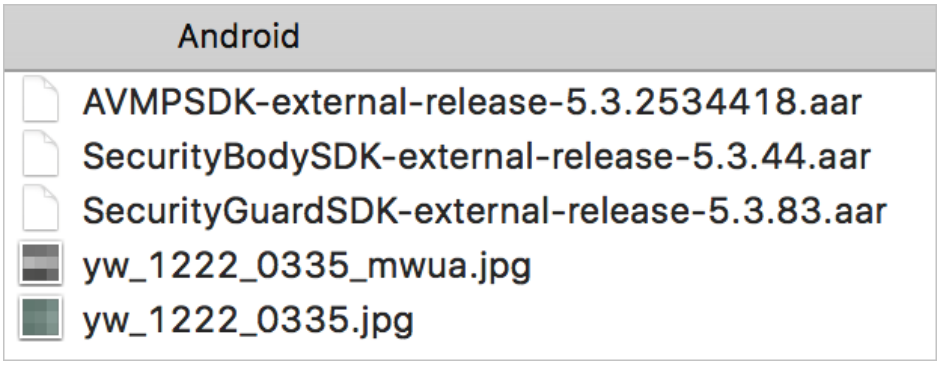
Android 接入文档

本文介绍了使用 Android App 接入 WAF SDK 的操作方法。

SDK-Android 文件说明

下载并解压 WAF SDK 包（点击获取SDK），在 sdk-Android 文件夹下，提供了以下文件：

注意：aar 文件的版本号可能会有不同。

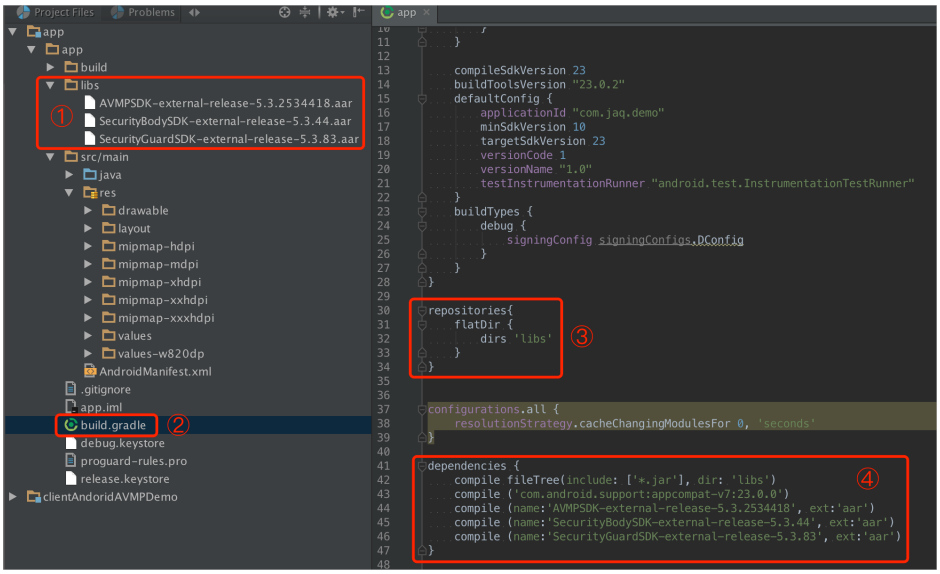


各文件说明（xxx为版本号）：

文件	功能
SecurityGuardSDK-xxx.aar	主框架SDK
AVMPSDK-xxx.aar	虚拟机引擎插件
SecurityBodySDK-xxx.aar	人机识别插件
yw_1222_0335.jpg	主框架配置文件
yw_1222_0335_mwua.jpg	虚拟机引擎配置文件

项目工程配置

参照以下步骤，来配置项目工程。



在 Android Studio 中导入 SDK 中的 aar 文件。将 SDK 中所有的 aar 文件都复制到项目的 libs 目录下。如果没有 libs 目录，请手工创建一个。

打开该 Module 的 build.gradle 文件，在其中增加以下配置（图示 ③ 和 ④ ）。

- 将 libs 目录作为查找依赖的源。

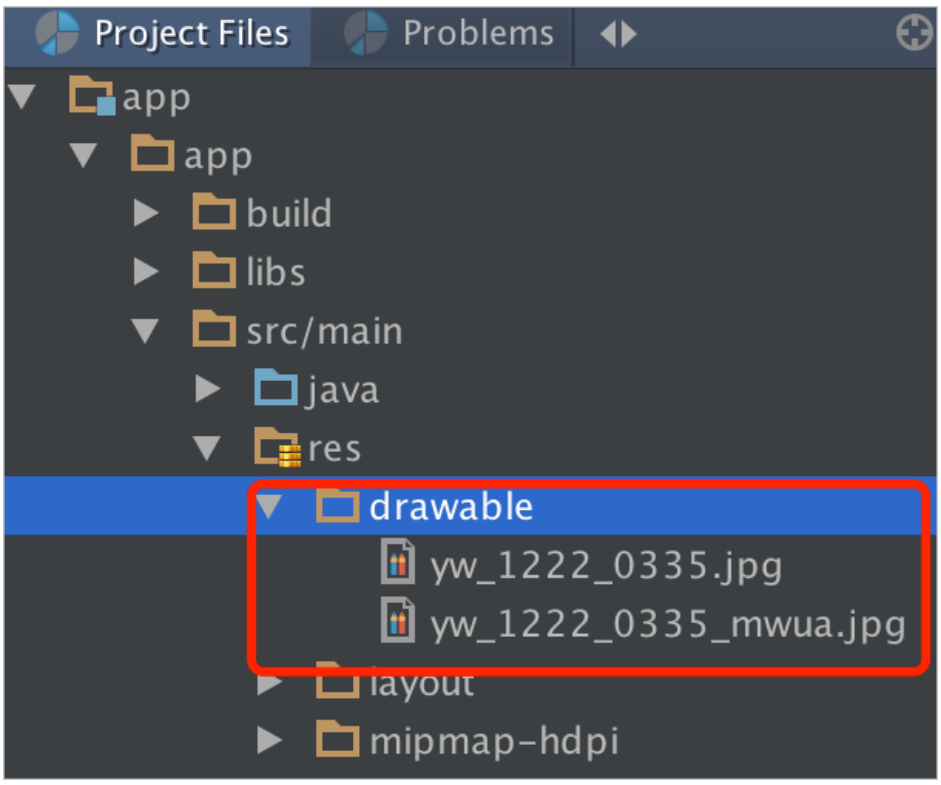
```
repositories{
flatDir {
dirs 'libs'
}
}
```

- 增加编译依赖。**注意**：aar 文件版本号可能会有不同，以下载得到的文件为准。

```
dependencies {
compile fileTree(include: ['*.jar'], dir: 'libs')
compile ('com.android.support:appcompat-v7:23.0.0')
compile (name:'AVMPSDK-external-release-xxx', ext:'aar')
compile (name:'SecurityBodySDK-external-release-xxx', ext:'aar')
compile (name:'SecurityGuardSDK-external-release-xxx', ext:'aar')
}
```

向 drawable 文件夹中导入 jpg 文件。将 SDK 目录下的 yw_1222_0335_mwua.jpg 和 yw_1222_0335.jpg 图片文件放到 Android 应用工程的 drawable 目录下。

注意：如果默认没有 drawable 目录，请手动创建一个。



过滤ABI（删除多余架构SO）。WAF SDK 目前只提供了 armeabi 架构的 SO。因此，您需要对最终导出的 ABI 进行过滤。否则，会造成 App 崩溃。具体操作如下：

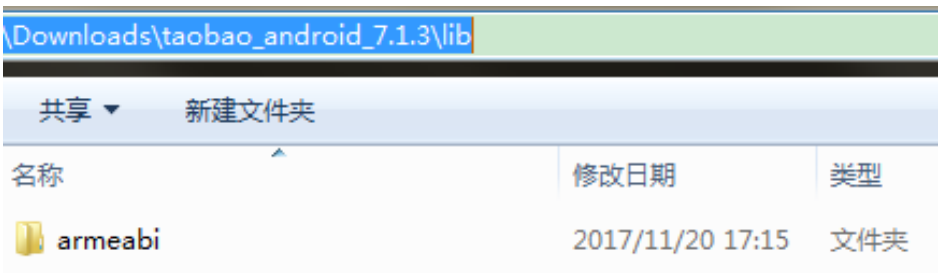
i. 在 Android 工程 lib 目录下，删除除了 armeabi 文件夹之外的所有其他 CPU 架构文件夹，包括 armeabi-v7a、x86、x86_64、arm64-v8a、mips、mips64 等。最终，只保留 armeabi 目录。

在工程的 build.gradle 配置文件中增加过滤规则，被 abiFilters 指定的架构即会被包含在 APK 里面。这里只指定 armeabi 架构，示例代码如下：

```
defaultConfig {
applicationId "com.xx.yy"
minSdkVersion xx
targetSdkVersion xx
versionCode xx
versionName "x.x.x"
ndk {
abiFilters "armeabi"
}
}
```

注意：只保留 armeabi 架构的 SO，不会影响 App 的兼容性，并且还能大大减小 App 的体积。

下图显示了手机淘宝 App 的 ABI 情况。可以看出，手机淘宝 App 只有 armeabi 架构的目录。



添加 App 权限。

如果是 Android Studio 项目，并且使用 aar 方式集成，那么则不需要在项目中额外配置权限，因为在 aar 中已经声明了相关权限。

如果是 Eclipse 项目，需要在 AndroidMenifest.xml 文件中添加下列权限配置：

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
```

添加 ProGuard 配置。如果您使用了 Proguard 进行混淆，则需要添加 ProGuard 配置。ProGuard 配置也根据接入方式的不同，分为 Eclipse 和 AndrodStudio 两种情况。

Android Studio

如果在 build.gradle 中配置了 proguardFiles，并且开启了 minifyEnabled，则表明使用了 proguard-rules.pro 这个配置文件进行混淆。如下图所示。

```
buildTypes {
    release {
        minifyEnabled true
        proguardFiles getDefaultProguardFile('proguard-android.txt'), 'proguard-rules.pro'
    }
}
```

Eclipse

如果在 project.properties 中指定了 proguard 配置，比如在 project.properties 中有如下的语句：proguard.config=proguard.cfg，则表明使用了 proguard 进行混淆。混淆配置在 proguard.cfg 文件中：

添加 keep 规则

为了保证需要的一些类不被混淆，需要在 proguard 的配置文件中添加以下规则。

```
-keep class com.taobao.securityjni.**{*;}
-keep class com.taobao.wireless.security.**{*;}
-keep class com.ut.secbody.**{*;}
-keep class com.taobao.dp.**{*;}
-keep class com.alibaba.wireless.security.**{*;}
```

代码编写

导入包。

```
import com.alibaba.wireless.security.jaq.JAQException;
import com.alibaba.wireless.security.jaq.avmp.IJAQAVMPSignComponent;
import com.alibaba.wireless.security.open.SecurityGuardManager;
import com.alibaba.wireless.security.open.avmp.IAVMPGenericComponent;
```

初始化。

- 接口定义：boolean initialize();
- 接口描述：
  - 功能：初始化 SDK。
  - 参数：无。
  - 返回值：boolean 类型。初始化成功返回 true，失败返回 false。
- 示例代码：

```
```

```
IJAQAVMPSignComponent jaqVMPComp =
SecurityGuardManager.getInstance(getApplicationContext()).getInterface(IJAQAVMPSignComponent.class);
boolean result = jaqVMPComp.initialize();
```

签名请求数据。

- 接口定义：byte[] avmpSign(int signType, byte[] input);

  接口描述：

  - 功能：使用 avmp 技术对 input 的数据进行签名处理，并且返回签名串。

    参数：见下表。

参数名	类型	是否必须	说明
signType	int	是	签名使用的算法，目前是固定值，填写 3。
input	byte[]	否	待签名的数据，一般是整个请求体。如果请求体为空，那么此参数填写 null。

    返回值：byte[] 类型，返回签名串。

  - 示例代码。客户端往服务器端发送数据时，需要调用 avmpSign 接口对整个 body 数据进行签名处理，之后得到签名串，这个签名串就是 wToken。

```
int VMP_SIGN_WITH_GENERAL_WUA2 = 3;
String request_body = "i am the request body, encrypted or not!";
byte[] result = jaqVMPComp.avmpSign(VMP_SIGN_WITH_GENERAL_WUA2, request_body.getBytes("UTF-
8"));
String wToken = new String(result, "UTF-8");
Log.d("wToken", wToken);
```

将 wToken 放进协议头。在 HttpURLConnection 类的对象中增加 wToken 字段的内容。示例代码如下：

```
String request_body = "i am the request body, encrypted or not!";
URL url = new URL("http://www.xxx.com");
HttpURLConnection conn = (HttpURLConnection) url.openConnection();
conn.setRequestMethod("POST");
// set wToken info to header
conn.setRequestProperty("wToken", wToken);
OutputStream os = conn.getOutputStream();
```

```
// set request body info
byte[] requestBody = request_body.getBytes("UTF-8");
os.write(requestBody);
os.flush();
os.close();
```

5. 发送数据到服务器。将修改好协议头的数据发到 App 自有服务器，中间会由 WAF 截获，并解析 wToken 进行风险识别。

错误码

上述 initialize 和 avmpSign 接口有可能会出现异常。如果生成签名串异常或失败，请搜索 Log 中 “SecException” 相关的信息。

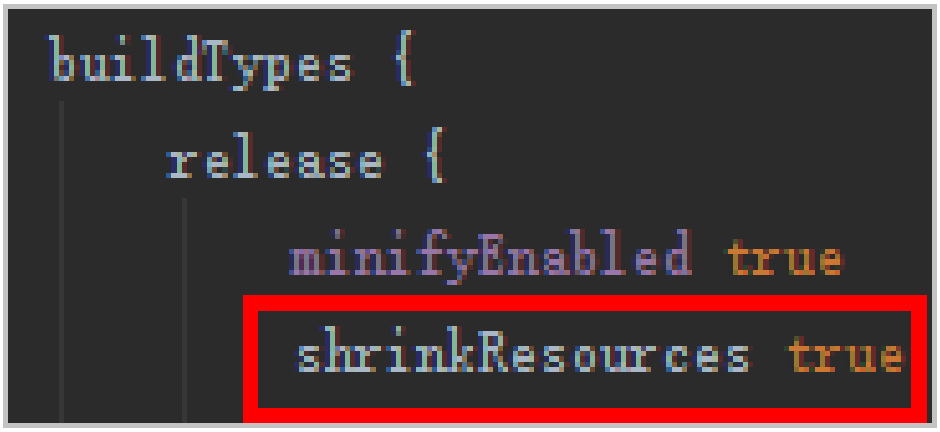
常见错误信息及描述见下表。

错误代码	含义
1901	参数不正确，请检查输入的参数。
1902	图片文件有问题。一般是获取图片文件时的 apk 签名和当前程序的 apk 签名不一致。请使用当前程序的 apk 重新生成图片。iOS 可能是应为 BundleID 不匹配。
1903	图片文件格式有问题。
1904	请升级新版本图片。AVMP 签名功能仅支持 v5 图片。
1905	没有找到图片文件。请确保图片文件在 res\drawable 目录下，AVMP 相关的图片为：yw_1222_0335_mwua.jpg。
1906	图片中缺少 AVMP 签名对应的 byteCode。请检查使用的图片是否正确。
1907	初始化 AVMP 失败，请重试。
1910	非法的 avmpInstance 实例。可能原因如下：AVMPInstance 是否被 destroy 后，调用 InvokeAVMP。图片 byteCode 版本与 SDK 不匹配。
1911	加密图片的 byteCode 没有相应导出的函数。
1912	AVMP 调用失败。请联系我们。
1913	AVMPInstance 被 destroy 之后，调用 InvokeAVMP 出现该错误。
1915	AVMP 调用内存不足，请重试。
1999	未知错误，请重试。

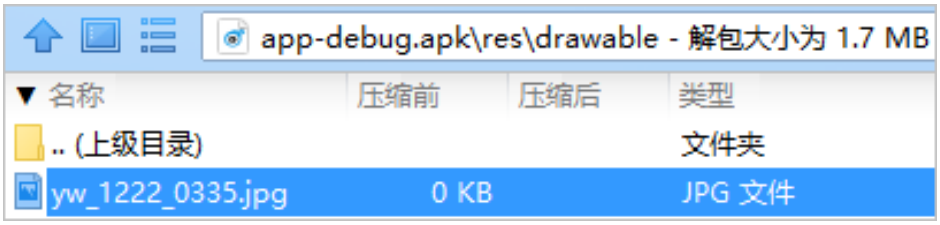
常见问题

指定 shrinkResources 之后，密钥图片被优化掉了

在 Android Studio 中，如果指定了 shrinkResources 为 true，那么，在工程编译的时候会把没有在代码中引用的资源文件给优化掉。



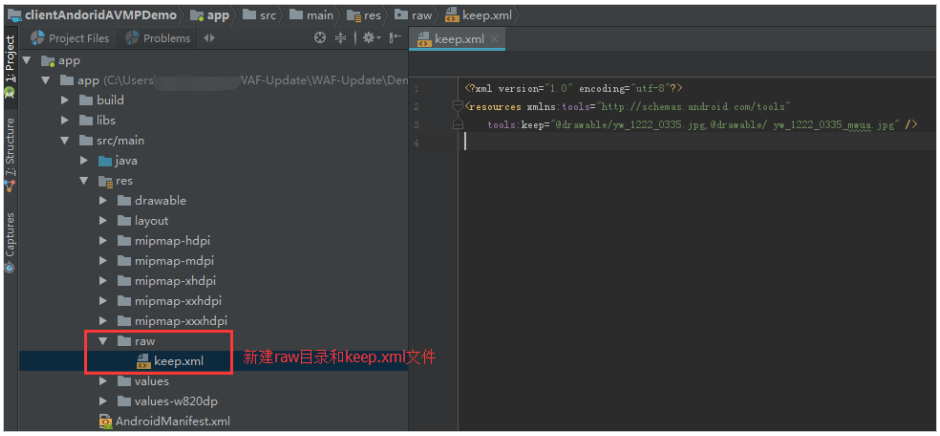
上述操作会使 SDK 中提供的两个 jpg 文件不能正常工作。如下图所示，打包出来的 APK 中，yw_1222_0335.jpg 的配置文件大小为 0KB，表明这个图片被优化掉了。



解决方法

在工程的 res 目录下新建 raw 目录，在 raw 目录下创建 keep.xml 文件。在 keep.xml 中输入如下内容：

```
<?xml version="1.0" encoding="utf-8"?>
<resources xmlns:tools="http://schemas.android.com/tools"
tools:keep="@drawable/yw_1222_0335.jpg,@drawable/yw_1222_0335_mwua.jpg" />
```



添加完上述内容，重新编译工程 apk 即可。

集成效果确认

参照以下步骤确认您的 App 已正确集成了 WAF SDK。

将打包出来的 apk 文件重命名成 zip 文件，然后用解压工具将该文件解压。

解压之后，定位到工程的 lib 目录，确保文件夹下只有 armeabi 文件夹。如果还有其他架构的文件夹，请参考 项目工程配置 步骤 4，移除其他架构的文件夹。

定位到工程的 res/drawable 目录下，确保 yw_1222_0335.jpg 和 yw_1222_0335_mwua.jpg 文件在其中，并且文件大小不为 0。

通过打印日志，确保调用 avmpSign 接口之后能生成正确的签名信息。如果没有生成，则查看是否有错误码产生。

关闭WAF

如果您想要变更WAF的计费方式（例如，从按量付费模式变更为包年包月模式），您需要关闭当前按量计费模式的WAF实例或释放已到期的包年包月模式的WAF实例。

如果您决定不再继续使用按量计费模式的WAF实例，您也可以通过关闭WAF实例功能确保不再产生任何费用。

说明： 包年包月模式的WAF实例到期后，您也可以通过关闭WAF功能释放该实例。

操作步骤

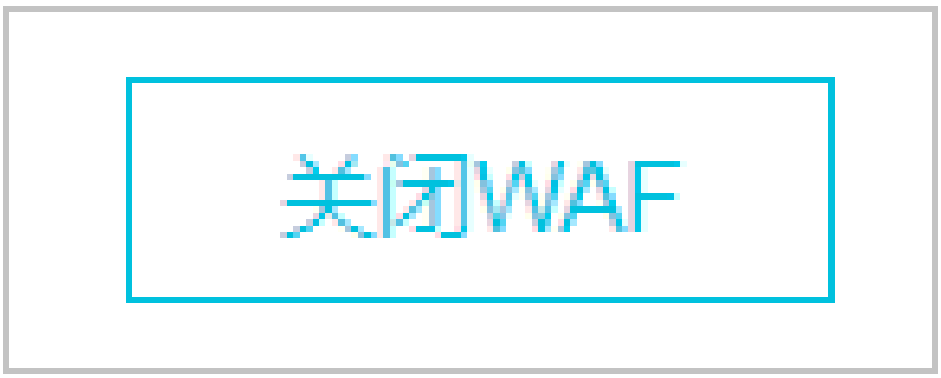
您只能在下列情况关闭或释放WAF实例。

- **包年包月模式**： WAF实例已经到期
- **按量计费模式**： 近两日内仅有少量或没有请求到达WAF实例

注意： 关闭WAF实例前，请您确认当前配置的网站域名DNS已解析回源站。WAF实例关闭或释放后，所有网站域名配置信息将被清空，如果仍有请求到达WAF实例将无法被正常转发，导致网站无法正常访问。

登录云盾Web应用防火墙管理控制台，选择地域。

在页面右上角，单击**关闭WAF**。



确认当前配置的网站域名解析已切换回到源站，单击**确定**，即可关闭WAF。