Web 应用防火墙

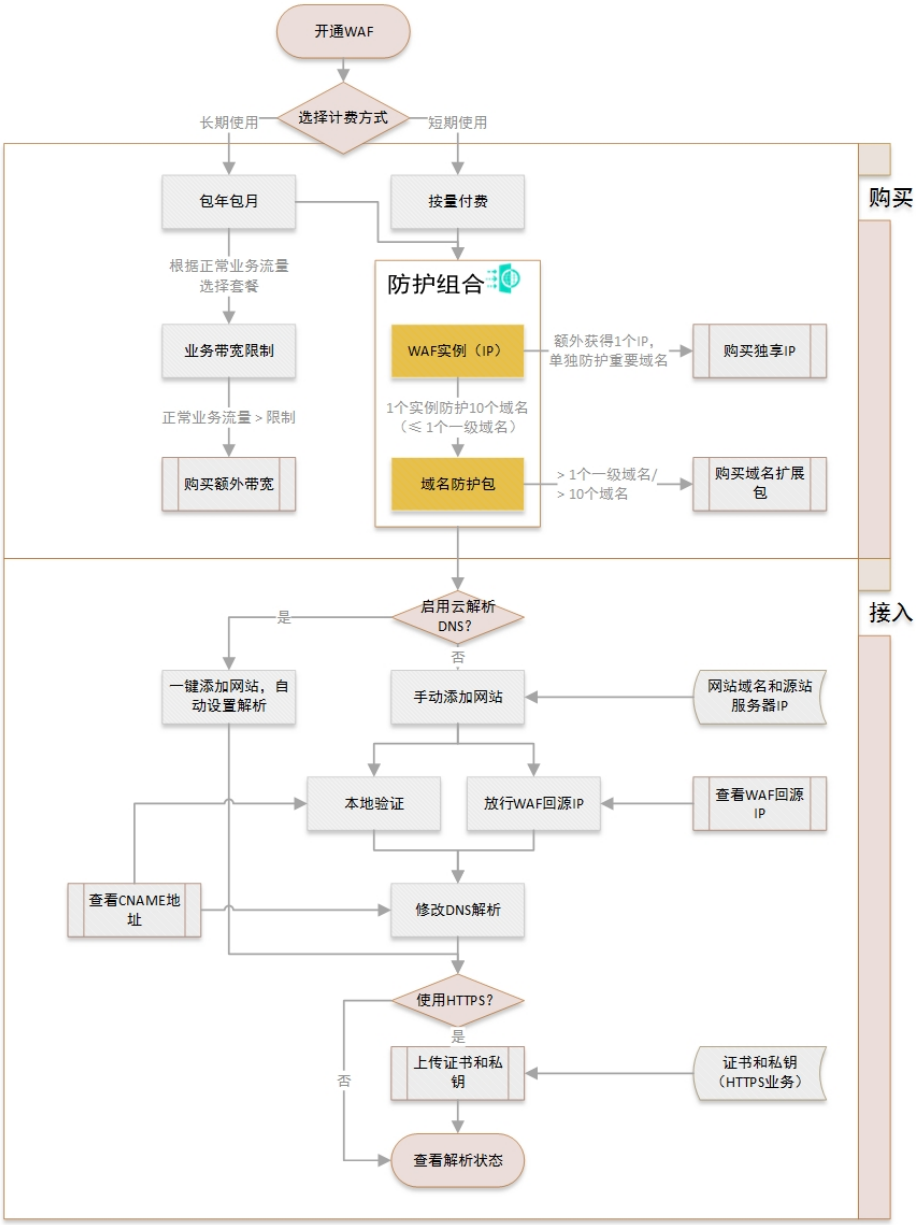
用户指南

用户指南

三分钟看明白WAF

WAF是阿里云云盾提供的Web应用防火墙，帮助您监控您网站上的HTTP/HTTPS访问请求，并通过自定义过滤规则和启用Web防护、安全合规等功能，帮助您部署网站访问控制。

- 您需要开通并接入WAF，使您网站的访问流量全部流转到WAF。下图显示了开通和接入WAF的简要流程，具体操作参见下文说明。
- WAF将按照您配置的过滤规则和启用的Web防护功能，检测并过滤收到的访问请求，只有满足规则条件的合法请求才会经WAF返回到您的服务器（回源）。具体内容参见下文 如何选用WAF防护功能 和 如何用好WAF。



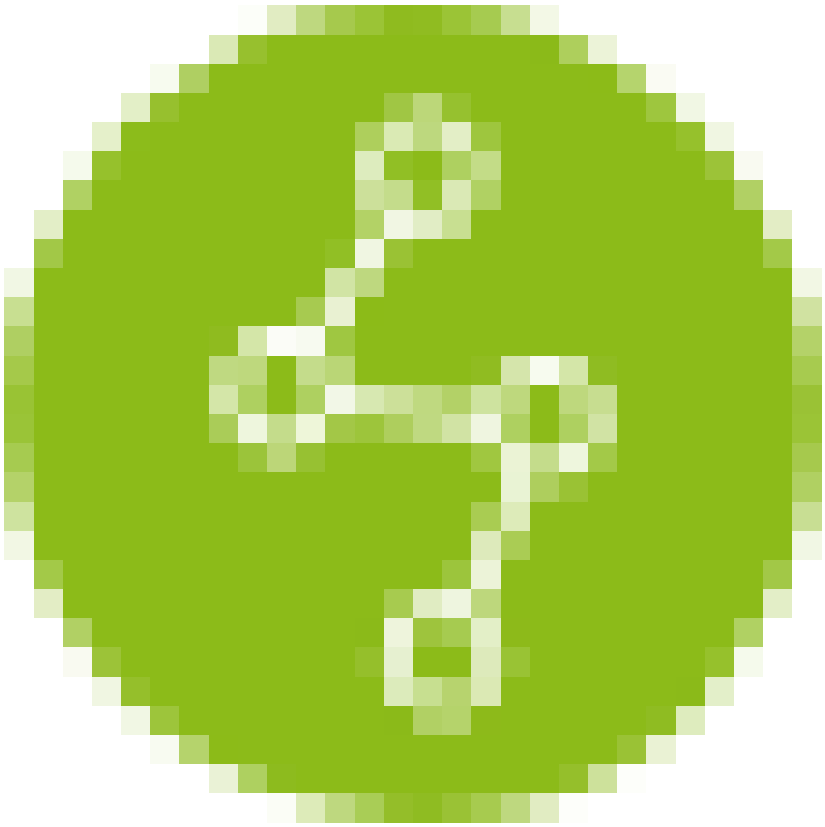
如何开通WAF

您可以使用按量付费或包年包月的计费方式来开通WAF。

- 按量付费按当日被防护网站的访问QPS峰值和当日选用的WAF防护功能，生成后付费账单；每日结算前一日费用。
- 包年包月按月/年计费，由您选购适用的WAF套餐，生成账单后直接付费；您可在选购的时长内享用套餐内的防护服务。

  说明：使用包年包月方式选购WAF套餐时，我们需要了解您的正常业务流量，以便区分DoS攻击等异常流量。每种WAF套餐支持不同的业务带宽，如果您的实际业务正常流量大于套餐内的带宽限制，您需要 购买额外带宽。

关于WAF计费方式的详细描述，请参考 **计费方式**。



关于开通WAF的具体操作，请参考 购买Web应用防火墙。

开通WAF后，您将获得一个WAF实例（对应一个实例IP）；您可以使用这个WAF实例接入最多10个网站，为其开启防护，这10个网站只能包含1个一级域名。

- 如果您希望防护具有不同一级域名的网站，您需要 购买域名扩展包。
- 如果您有很重要的域名需要单独防护，而非使用同一个WAF IP防护所有域名，您可以 购买独享IP包。

如何接入WAF

开通WAF后，您需要通过 域名解析（DNS），将访问您网站的流量流转到您开通的WAF实例（IP）上，并设置由WAF实例在过滤掉恶意请求后，将合法的访问流量再返回到您的源站服务器上。

以上操作就是接入WAF，它分为两个环节：

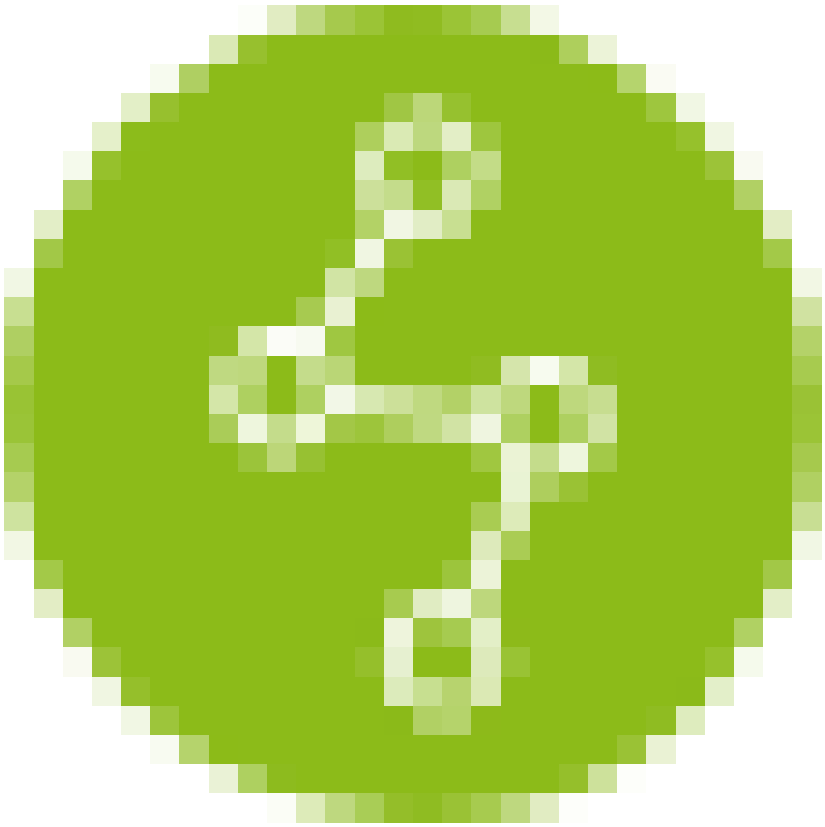
所有访问流量由客户端到WAF

您将要防护的网站（域名）添加到WAF，WAF分配给这个域名一个 CNAME地址。您只要在对应域名的解析记录中添加并应用这条CNAME记录，就可以将通过域名访问您网站的流量导向WAF实例。
说明：我们并没有在控制台上体现您的WAF实例IP，如果您想知道该IP，您可以使用ping命令，ping分配给您的CNAME地址。

过滤后的访问流量由WAF到您的源站服务器

您只需要告诉我们您的源站服务器地址，它可以是IP或其他地址（如对象存储OSS的CNAME等），WAF就会将过滤后的访问流量返还到您指定的源站地址。

如果您的域名使用 阿里云云解析DNS 进行域名解析，我们支持一键式接入WAF；否则，您需要进行手动接入。



关于接入WAF的具体操作，请参考 添加网站配置。

如何选用WAF防护功能

WAF分析客户端使用HTTP/HTTPS协议发送的GET/POST请求，并应用访问规则过滤恶意访问流量。

说明：下述功能项对应不同的（按量付费）收费标准，或（包年包月）套餐，您可以在 Web应用防火墙价格页 了解具体的计费信息。

您可以使用 **精准访问控制**，自定义访问规则，过滤客户端IP、请求URL、以及常见的请求头字段。有关操作请参考 黑白名单配置、精准访问控制。

您也可以直接使用Web防护功能，抵御常见的Web攻击。我们结和Web攻击特征，分析请求头和请

求主体，编写了精准的过滤算法，并将这些复杂的过滤算法封装各类防护功能，方便您直接使用。WAF提供的防护功能包括：

说明：WAF使用多层过滤的机制，即您在启用WAF并配置防护功能后，一个客户端请求在经过WAF时，实际上按顺序经过了多层过滤。默认的防护检测顺序为：精准访问控制 > CC防护 > Web攻击防护 > 智能防护引擎 > 地区封禁 > 数据风控 > SDK防护。

- **Web攻击防护**：帮助您防护SQL注入、XSS跨站攻击等常见的Web攻击。有关操作请参考 Web应用攻击防护规则策略。
- **CC攻击防护**：帮助您防护针对页面请求的CC攻击。有关操作请参考 选择CC防护模式、自定义CC防护。
- **智能防护引擎**：对请求做语义分析，检测经伪装或隐藏的恶意请求，帮助您防护通过攻击混淆、变种等方式发起的恶意攻击。有关操作请参考 智能防护引擎。
- **恶意IP惩罚**：帮助您自动封禁在短时间内进行多次Web攻击的客户端IP。有关操作请参考 恶意IP封禁。
- **地理IP封禁**：帮助您一键封禁来自指定国内省份或海外地区的IP的访问请求。有关操作请参考 封禁地区。
- **数据风控**：帮助您对抗机器威胁，如垃圾注册、账号被盗、活动作弊、垃圾消息等欺诈行为。有关操作请参考 数据风控。

WAF也可以满足您的部分安全合规需求。WAF提供的安全合规功能包括：

- **网页防篡改**：帮助您锁定需要保护的网站页面，被锁定的页面在收到请求时，返回您为其设置的缓存内容。有关操作请参考 网页防篡改。
- **敏感信息防泄漏**：帮助您过滤服务器返回内容（异常页面或关键字）中的敏感信息，如身份证号、银行卡号、电话号码、和敏感词汇等。有关操作请参考 防敏感信息泄露。

此外，WAF还提供了方便的监控管理功能：

- **安全监控**：您可以在 WAF控制台总览页面 查看图表化的业务访问数据以及安全防护统计信息。
- **安全报表**：您可以在这里查询您的域名在30天内受到的攻击详情和风险预警信息。有关操作请参考 攻击防护报表 和 风险预警报表。
- **全量日志**：您可以在这里搜索您的网站日志，并使用在线分析快速定位请求。有关操作请参考 全量日志查询。
- **数据大屏**：您可以在这里查看WAF的实时攻防态势监控和告警。有关操作请参考 可视化大屏。

如何用好WAF

启用WAF后，您的源站服务器收到的所有请求都来自WAF实例，服务器IP对客户端来说是隐藏的。

如果您希望获取一个访问请求的真实客户端IP，请参考 获取访问者真实IP。

如果您的源站服务器IP已公开或不慎泄露，这样的话，攻击者可能越过域名解析，也即越过WAF，直接对您的源站发动攻击。要想有效防护这种情形，您需要 配置源站保护。

如果您同时使用了阿里云 DDoS高防IP服务 或者 CDN服务，您可能需要以下帮助：

说明：这种情况下，您在接入WAF时，应当勾选 **WAF前是否有七层代理** 下的 **是。**

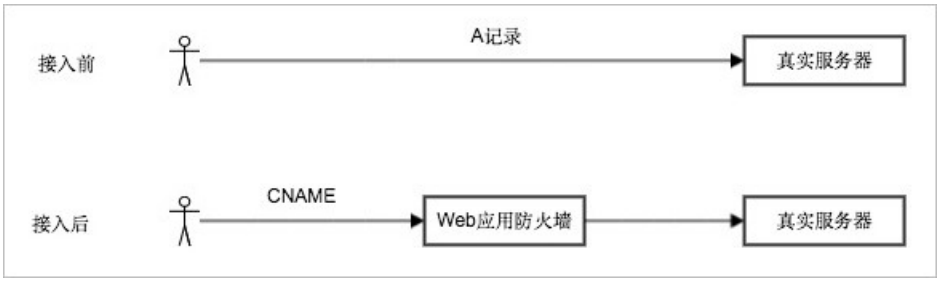
- 高防IP结合WAF
- CDN结合WAF

如果您希望对您的原生App进行安全防护，解决CC攻击、机器滥刷等问题，您可以参考WAF的SDK方案。

接入WAF

CNAME接入指南

要通过WAF（Web应用防火墙）防护您的网站，您必须在Web应用防火墙控制台完成域名配置，并将域名解析指向WAF为域名分配的CNAME地址，让所有访问网站的流量都经过WAF的过滤。接入WAF前后的的流量逻辑如下所示。



本文介绍了将域名接入WAF的完成流程。

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。
- 使用中国大陆WAF时，该网站域名必须已完成ICP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，具体方法请参考备案导航。
- 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。
- 准备被防护域名的DNS管理员权限，用来修改DNS记录，以切换被防护网站的流量。
- 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）
- *.key（私钥文件）

接入流程

说明：以下接入步骤适用于仅使用WAF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WAF与其它代理型服务结合部署的场景，请查看以下内容：

- 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。

步骤1：网站配置

登录云盾Web应用防火墙控制台，前往**管理**>**网站配置**页面，单击**添加网站**，根据提示结合业务情况进行配置。

配置说明如下：

- **域名**：填写要接入的域名。
- **协议类型**：根据网站协议选择**HTTP**和/或**HTTPS**。关于高级设置，请参考HTTPS高级配置。
- **服务器地址**：选择**IP**，并填写源站公网IP。

  说明：服务器地址是您希望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**其它地址**，将对应的域名填进去，而不是接入防护的网站域名。

- **服务器端口**：填写服务器监听的端口。关于自定义端口，请查看**非标端口支持**。
- **WAF前是否有七层代理（高防/CDN等）**：判断是否使用了代理。
- **负载均衡算法**：选择**IP hash**或**轮询**算法，一般保持默认。关于源站负载均衡，请参考**WAF源站负载均衡**。

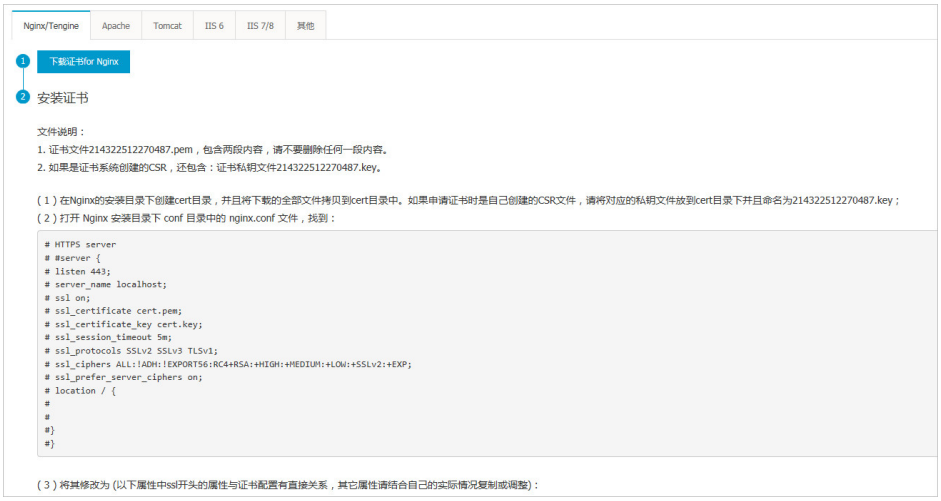
更具体的配置说明，请参考**添加网站配置**。

启用HTTPS

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WAF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。

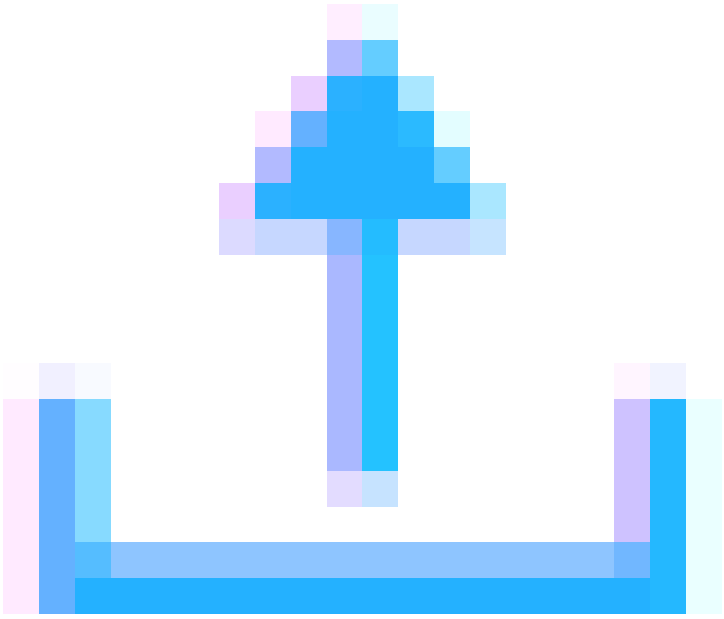
如果您的证书是通过阿里云云盾证书服务所购买的，您可以登录**云盾证书服务管理控制台**，选择您的证书，单击**下载**，并选择类型下载证书。



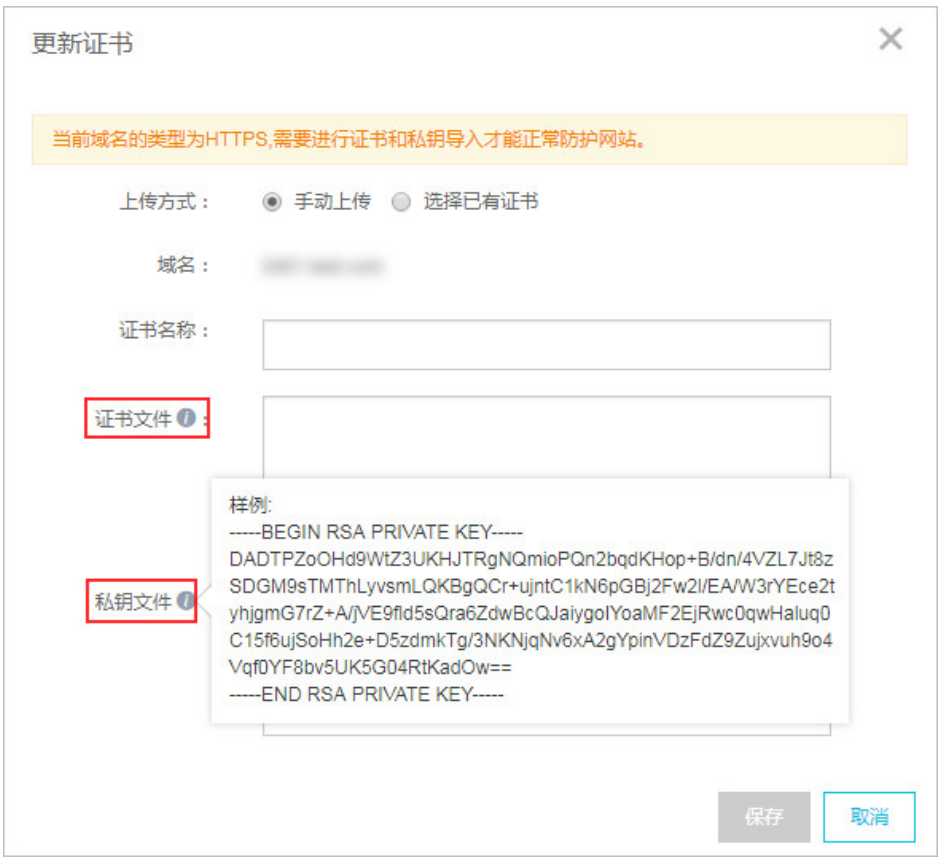
说明：所下载的证书一般包括*.pem（证书文件）和*.key（私钥文件）两个文件。

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。

登录云盾Web应用防火墙控制台，前往**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。选择**手动上传**，并分别上传证书文件和私钥文件中的指定内容，具体说明请参考**添加网站配置**中的**上传HTTPS证书和私钥**部分。



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

查看域名接入状态

配置网站后，您可以登录云盾Web应用防火墙控制台，在**管理**>**域名配置**页面查看已添加的网站域名的**DNS解析状态**，确认其是否正确接入WAF。如果DNS解析状态为异常，且收到**未检测到CNAME接入**、**无流量**的异常提示，则说明您所配置的网站域名未正确接入WAF。

- DNS解析状态自动检测该网站域名的解析是否指向CNAME，并检测最近数分钟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WAF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WAF，不会因此而影响您网站的访问。

如果在配置完网站域名解析后，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**、**无流量**或**当前无流量**等错误信息，请查看DNS解析状态异常。

步骤2：本地测试

将业务流量正式切换到WAF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。

关于本地测试的具体方法，请查看本地验证。

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WAF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WAF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WAF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。

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WAF进行防护。

将鼠标移至已添加的网站域名记录，获取WAF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：以下操作步骤以阿里云云解析DNS为例进行描述。如果网站使用的是其它域名提供商，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。

登录云解析DNS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。

更具体的操作说明，请参考修改DNS解析。

注意事项

- 同一个主机记录，CNAME解析记录值只能填写一个，您需要将其修改为WAF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WAF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。
  说明：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WAF的IP来接入WAF防护。通过对WAF分配的CNAME地址使用Ping命令可以获取所分配的WAF IP，然后将A记录类型的解析记录中的记录值修改为该WAF IP。
  说明：如果您采用A记录方式将网站域名接入WAF防护，WAF将无法进行故障集群调度和故障bypass操作。

步骤5：启用源站保护

将网站域名正式接入WAF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WAF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。

HTTPS高级配置

WAF提供灵活的HTTPS配置功能，帮助您在不改造源站的情况下，一键实现全站HTTPS或强制客户端使用HTTPS访问网站。

说明：如果您使用按量付费模式WAF，您必须在**功能与规格**中勾选**支持HTTPS相关业务**，才能使用HTTPS高级配置。具体操作，请参考功能与规格配置。

操作步骤

参照以下步骤，执行HTTPS高级配置：

登录云盾Web应用防火墙控制台。

前往**管理**>**网站配置**页面。

选择要操作的域名，单击其操作列下的**编辑**。

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

开启HTTP回源

如果您的网站不支持HTTPS回源，请**开启HTTP回源**（默认回源端口是80端口），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。

说明：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）。

开启HTTPS的强制跳转

如果您需要强制客户端使用HTTPS来访问（从安全性考虑，推荐这样做），您可以**开启HTTPS的强制跳转**，且应确保您的网站支持HTTPS业务。

说明：开启HTTPS强制跳转前必须先取消HTTP协议。

选择开启HTTPS的强制跳转后，部分浏览器将被缓存设置为使用HTTPS请求访问网站，请确保您的网站支持HTTPS业务。

开启HTTPS强制跳转后，HTTP请求将显示为HTTPS，默认跳转到443端口。

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

WAF默认支持以下端口：

- HTTP：80、8080
- HTTPS：443、8443

企业版和旗舰版WAF实例支持更多的非标端口，且对被防护域名使用的不同端口的总数有相应限制。

说明：如果您使用按量付费模式WAF，您必须在**功能与规格**中勾选**支持非标端口业务防护**，才能使用非标端口接入WAF。具体操作，请参考功能与规格配置。

不同端口总数限制

针对每个阿里云账号（即每个WAF实例），由WAF防护的全部域名所使用的不同端口的总数有以下限制：

- 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）

支持的端口

说明：WAF仅防护支持的端口，对于不支持的端口WAF既不会防护，也不会转发。例如，4444端口的业务请求到达WAF后，请求会被直接丢弃。

在企业版和旗舰版WAF中，**HTTP**协议支持以下端口：

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

在企业版和旗舰版WAF中，**HTTPS**协议支持以下端口：

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

WAF源站负载均衡

如果您的源站有多个服务器，在将域名接入WAF时，您可以配置多个源站IP。WAF支持最多20个源站IP。

如果您配置了多个源站IP，WAF在将过滤后的访问请求回源时，将按照IP Hash或轮询的方式去做负载均衡。同时，WAF也会对多个源站进行健康检查，对所有回源IP进行接入状态检测，如果某个回源IP没有响应，将不再将请求转发到这个回源IP，直到其接入状态回复正常。

假设源站IP有3个（1.1.1.1、2.2.2.2、3.3.3.3），您可以按照下图所示进行配置。

说明：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**下的**是**。

添加源站IP后，您需要指定负载均衡算法：IP hash、轮询。

说明：使用IP HASH时，如果源IP不够分散，可能会出现负载不均。

防护配置

Web应用攻击防护

功能描述

Web应用攻击防护可防护SQL注入、XSS跨站等常见Web应用攻击，且提供不同规格的防护策略：宽松、正常、严格。将网站接入WAF后，您可以为其开启Web应用攻击防护，并根据实际需求调整相应防护策略。Web应用防护开启后实时生效；如果您不想使用该功能，可将其关闭。

操作步骤

参照以下步骤，配置Web应用攻击防护策略：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

登录云盾Web应用防火墙控制台。

前往**管理**>**网站配置**页面，选择地区。

选择要操作的域名，单击其操作列下的**防护配置**。

在**Web应用攻击防护**下，开启防护，并选择防护**模式**：

- **防护**：发现攻击后直接阻断。
- **预警**：发现攻击后只告警，不阻断。

说明：如果您不想使用该功能，可在此处关闭防护。

在**防护规则策略**下拉框中选择合适的防护策略：

- 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惩罚

功能描述

传统的Web应用防火墙针对IP-URL维度进行拦截。当判定一个请求是攻击行为后，单次阻断该请求。而实际上，攻击者们可能持续不断地在对您的网站进行扫描、攻击，研究防护策略并尝试绕过防火墙，单次阻断的处理方式在这种情况下往往不够高效。

针对这种情况，云盾Web应用防火墙提供恶意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。

说明：包年包月模式的WAF实例均支持恶意IP惩罚。按量付费的WAF实例必须在**功能与规格**中为**Web攻击防护**启用**高级防护**，才能使用恶意IP惩罚。具体操作，请参考**功能与规格配置**。

操作步骤

参照以下步骤，启用恶意IP惩罚功能：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考**CNAME接入指南**。

登录**云盾Web应用防火墙控制台**。

前往**管理**>**网站配置**页面，选择地区。

选择要操作的域名，单击其操作列下的**防护配置**。

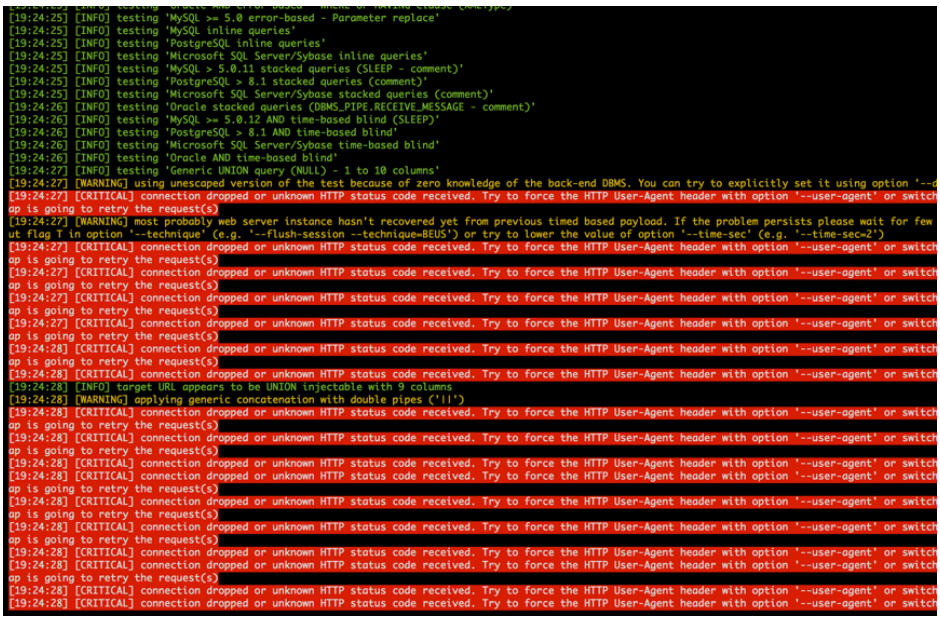
在**恶意IP惩罚**下，启用防护。默认的防护规则是：当WAF在1分钟内拦截到一个IP发动的2次Web攻击时，就封禁该IP的访问请求6分钟。

说明：如果您不想使用恶意IP惩罚功能，您可以在此页面关闭防护。

测试示例

启用恶意IP惩罚后，当您的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。以下是启用该功能后的实际效果测试。

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。



从结果中看到，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。

恶意IP惩罚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。

新智能防护引擎

功能描述

新智能防护引擎针对请求进行语义分析，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，拦截攻击者利用攻击混淆、变种等方式发起的恶意攻击。

说明：包年包月模式的WAF实例均支持新智能防护引擎。按量付费的WAF实例必须在**功能与规格**中为**Web攻击防护**启用**高级防护**，才能使用新智能防护引擎。具体操作，请参考**功能与规格配置**。

说明：新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。

新智能防护引擎的主要特性如下：

语义化：新智能防护引擎归并同类攻击行为的行为特征，并以攻击行为的多个行为特征组成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，即用自然语言的语义来理解并描述同一类攻击。

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，然后从繁多的Web应用攻击中提炼出异常攻击模型，从而形成异常攻击集。

关于新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

参照以下步骤，启用新智能防护引擎：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

登录云盾Web应用防火墙控制台。

前往**管理**>**网站配置**页面，选择地区。

选择要操作的域名，单击其操作列下的**防护配置**。

在**新智能防护引擎**下，启用防护。

说明：如果您不想使用新智能防护引擎，您可以在此页面关闭防护。

CC安全防护

功能描述

CC安全防护可以拦截机器恶意CC攻击，并提供不同模式的防护策略：正常、攻击紧急。将网站接入WAF后，您可以为其开启CC安全防护，并根据实际需求调整相应防护策略。企业版和旗舰版WAF支持更高级的CC防护功能，具体请参考CC防护规格。

说明：攻击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

，建议您将WAF升级到企业版或旗舰版，并使用自定义CC防护。

说明：如果您使用按量付费的WAF实例，您可以在**功能与规格**中为**缓解CC攻击**启用**高级防护**，这样可以自定义CC防护。具体操作，请参考功能与规格配置。

操作步骤

参照以下步骤，配置CC安全防护模式：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

登录云盾Web应用防火墙控制台。

前往**管理**>**网站配置**，选择地区。

选择要操作的域名，单击其操作列下的**防护配置**。

在**CC安全防护**下，开启防护，并选择相应防护模式：

正常：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。建议您在网站无明显流量异常时采用此模式，避免误杀。

攻击紧急：当发现有正常模式无法拦截的CC攻击，并出现网站响应缓慢，流量、CPU、内存等指标异常时，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。

说明：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**源站保护**，只允许WAF回源IP访问服务器。

说明：如果您希望有更好的防护效果，同时有更低的误杀。您可以升级到Web应用防火墙企业版或旗舰版，自定义或找安全专家定制针对性的防护算法。

FAQ

不同WAF规格对应的CC安全防护能力有什么区别？

不同WAF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，防护某些具有特定攻击特征的CC攻击。具体操作请参考**自定义CC防护**。
- **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**。

关于如何升级WAF规格，请参考**续费与升级**。

说明：对于按量付费版Web应用防火墙，您必须登录**云盾Web应用防火墙控制台**，前往**设置**>**功能与规格**页面，启用缓解CC攻击的**高级防护**功能选项，才能选择开启**攻击紧急**模式。

为什么有些CC攻击需要升级企业版才能防护？

云盾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。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。黑客在发现一种攻击无效后，可以调整策略并重新发动定向攻击。此时，通过云盾安全专家介入分析，可以获得更高的防护等级和效果。

自定义CC防护

功能描述

WAF**企业版**和**旗舰版**支持CC自定义防护功能。您可以在控制台自定义防护规则，限制单个IP对您的网站上特定路径（URL）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.yourdomain.com/login.html超过20次时，封禁该IP一小时。

说明：对于WAF高级版，您必须升级到企业版或旗舰版，才能使用自定义CC防护功能。具体操作请参考**续费与升级**。

说明：对于按量付费的WAF实例，您必须登录**云盾Web应用防火墙控制台**，前往**设置**>**功能与规格**页面，启用**缓解CC攻击**的**高级防护**，才能使用自定义CC防护功能。具体操作，请参考**功能与规格配置**。

操作步骤

参照以下步骤，配置自定义CC防护规则：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

登录云盾Web应用防火墙控制台。

前往**管理**>**网站配置**页面，并选择地区。

选择要操作的域名，单击其操作列下的**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。参数描述如下：

- **规则名称**：为该规则命名。

- **URI**：指定需要防护的具体地址，如/register。支持在地址中包含参数，如/user?action=login。
- **匹配规则**：
  - **完全匹配**：即精确匹配，请求地址必须与配置的URI完全一样才会被统计。
  - **前缀匹配**：即包含匹配，只要是请求的URI以此处配置的URI开头就会被统计。例如，如果设置URI为/register，则/register.html会被统计。
- **检测时长**：指定统计访问次数的周期。需要和单一IP访问次数配合。
- **单一IP访问次数**：指定在检测时长内，允许单个源IP访问被防护地址的次数。
- **阻断类型**：指定触发条件后的操作（封禁、人机识别），以及请求被阻断后阻断动作的时长。
  - **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。

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，就直接阻断该IP的访问，阻断操作持续600分钟。

说明：由于WAF需要将集群中的多台服务器的数据进行汇总来统计单一IP的访问频率，统计过程中可能存在一定延时，因此封禁的实际生效时间可能稍有滞后。

规则添加成功后即时生效，您可以选择**编辑**或者**删除**规则。

精准访问控制

功能描述

精准访问控制允许您设置访问控制规则，对常见的HTTP字段（如IP、URL、Referer、UA、参数等）进行条件组合，用来筛选访问请求，并对命中条件的请求设置放行、阻断、或告警操作。精确访问控制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。

精准访问控制规则

精准访问控制规则由**匹配条件**与**匹配动作**构成。匹配条件包含匹配字段、逻辑符、匹配内容三个要素。在创建规则时，您通过设置匹配字段、逻辑符和相应的匹配内容定义匹配条件，并针对符合匹配条件规则的访问请求定义相应的动作。

匹配条件

匹配条件包含匹配字段、逻辑符、匹配内容。匹配内容暂时不支持通过正则表达式描述，但允许设置为空值。

下表罗列了精确访问控制支持的匹配字段及其描述。

说明：包年包月模式下，高级版WAF实例仅支持IP、URL、Referer、User-Agent匹配字段，且每个域名最多只能定义20条规则；企业版和旗舰版的WAF实例支持下表中所有匹配字段，支持为每个域名定义的规则数分别为100条、200条。

说明：按量付费的WAF实例提供两种规格的精准访问控制：基础防护和高级防护。您可以在**规格与配置**中进行调整。具体操作，请参考**功能与规格配置**。

- 基础防护仅支持基于IP和URL的匹配条件，且每个域名可设置10条规则。
- 高级防护支持基于IP、URL、Cookie、User-Agent、Referer、提交参数、X-Forwarded-For等各类常见HTTP头部的逻辑组合判断功能，每个域名可设置100条规则。

匹配字段	字段描述	适用逻辑符
IP	访问请求的来源IP。	- 属于 - 不属于
URL	访问请求的URL地址。	- 包含 - 不包含 - 等于 - 不等于
Referer	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	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	访问请求的URL地址中的参数部分，通常指URL中”?”后面的	- 包含

	部分。例如，www.abc.com/index.html?action=login中的action=login就是参数部分。	- 不包含 - 等于 - 不等于 - 长度小于 - 长度等于 - 长度大于
Cookie	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	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	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。	- 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	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	访问请求的响应内容信息。	- 包含 - 不包含 - 等于 - 不等于

Http-Method	访问请求的方法，如GET、POST等。	- 等于 - 不等于
Header	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：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，且各个条件间是“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。

说明：选择**放行**、**告警**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防护功能检测过滤，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。

规则匹配顺序

如果您设置了多条规则，则多条规则间有先后匹配顺序，即访问请求将根据您设定的精准访问控制规则顺序依次进行匹配，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

参照以下操作步骤，为已防护的域名配置精准访问控制规则：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

登录云盾Web应用防火墙控制台。

前往**管理**>**网站配置**页面，选择地区。

选择要操作的域名，单击其操作列下的**防护配置**。

在**精准访问控制**下，开启防护，并单击**前去配置**。

单击**新增规则**，设置规则的匹配条件和相应的匹配动作，完成后单击**确定**。

说明：关于规则参数说明，请参考**精准访问控制规则**；关于应用示例，请参考**配置示例**。

成功创建规则后，您可以**编辑**其内容或将其**删除**。如果有多条规则，单击**规则排序**，通过**上移**、**下移**、**置顶**、**置底**等操作可调整规则的匹配顺序，越靠上的规则越优先匹配。

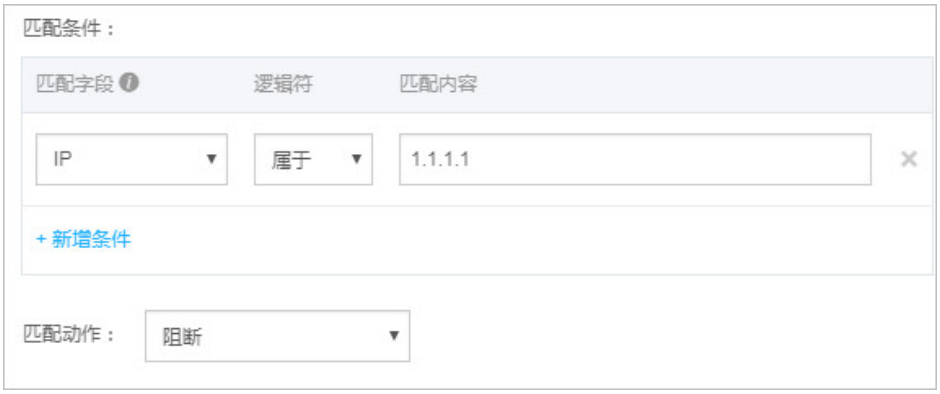
配置示例

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。通过设置精准访问控制规则也可以实现特定的Web漏洞防护。

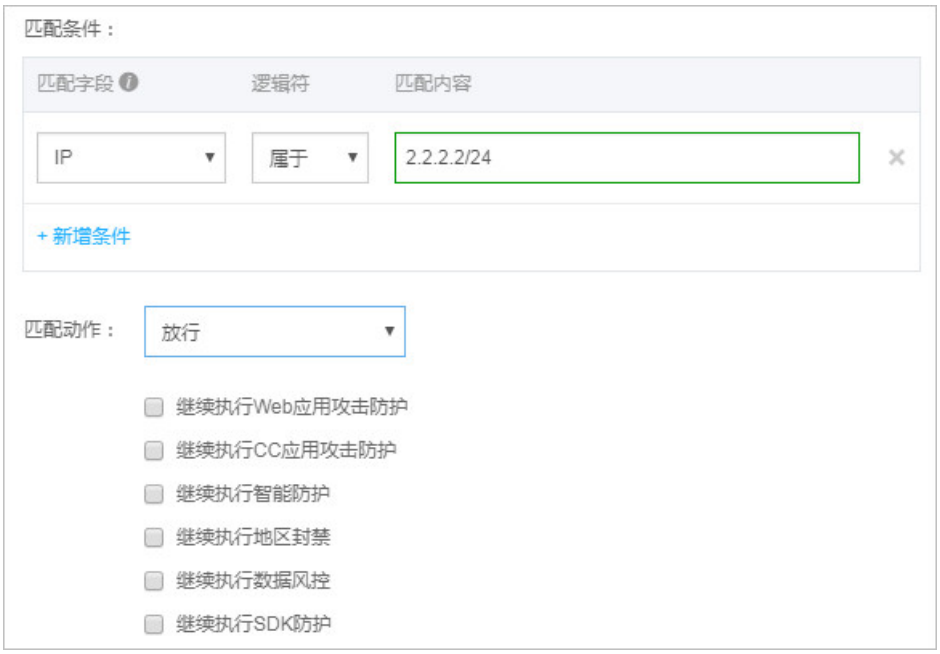
以下罗列了一些常用的精确访问控制配置示例，供您参考。

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。



说明：应用此白名单配置规则时，请不要勾选**继续执行Web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的其它防护功能拦截。

更多关于配置IP黑白名单的操作及注意事项，请参考IP黑白名单配置。

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，如下图所示。

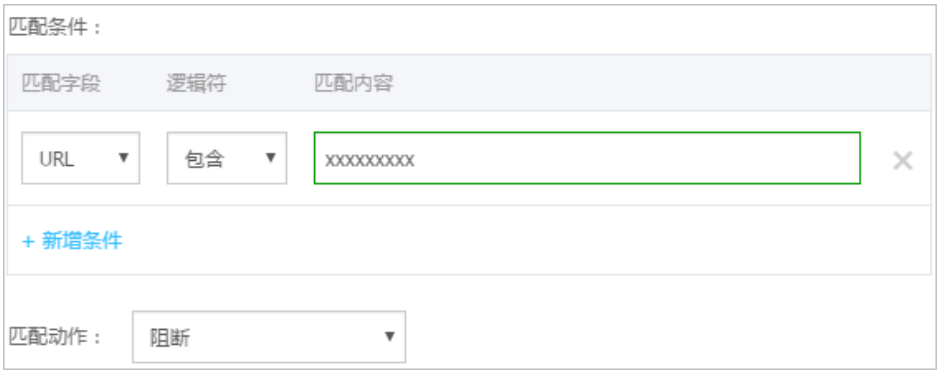
UA
WordPress/4.2.10; http://ascsolutions.vn; verifying pingback from 191.96.249.54
WordPress/4.0.1; http://146.148.63.90; verifying pingback from 191.96.249.54
WordPress/4.6.1; https://www.nokhostinsabt.com; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://eadastage.lib.umd.edu; verifying 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。

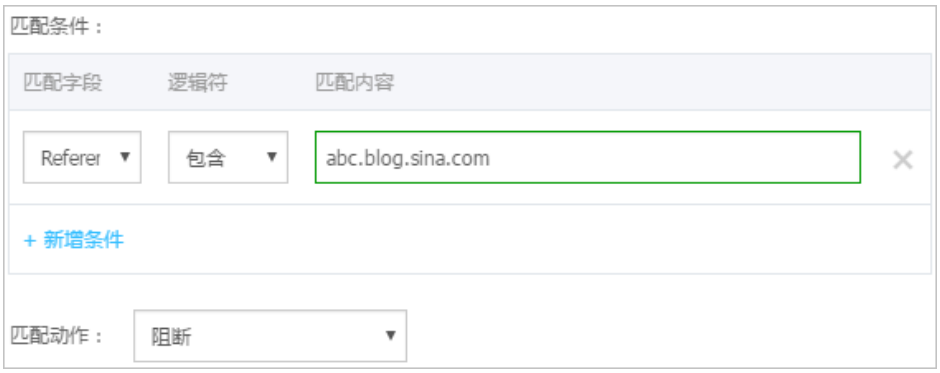
封禁特定的URL

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访问请求。



封禁地区

功能描述

使用封禁地区可以对指定的国内省份或海外地区的来源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。

说明：对于WAF高级版，您必须升级到企业版或旗舰版，才能使用封禁地区功能。具体操作，请参考**续费与升级**。

说明：对于按量付费的WAF实例，您必须在**功能与规格**中勾选**支持基于地理位置的区域封禁**，才能使用该功能。具体操作，请参考**功能与规格配置**。

操作步骤

参照以下步骤，启用并设置封禁地区：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

登录云盾Web应用防火墙控制台。

前往**管理**>**网站配置**页面，并选择地区。

选择要操作的域名，单击其操作列下的**防护配置**。

在**封禁地区**下，启用防护。

说明：如果您不想使用封禁地区，您可以在此页面关闭防护。

单击**设置**，选择要封禁的地区，完成后单击**确定**。

说明：支持的地区包括国内各省份和海外，IP归属地信息以淘宝IP地址库为准。

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。

IP黑白名单配置

在WAF中，您可以配置**精准访问控制规则**来阻断或放行指定IP的访问请求，即设置IP黑/白名单。IP黑白名单仅针对配置的特定域名生效。

操作步骤

参照以下步骤，配置IP黑名单和IP白名单：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考**CNAME接入指南**。

登录**云盾Web应用防火墙控制台**。

前往**管理**>**网站配置**页面，选择地区。

选择要操作的域名，单击其操作列下的**防护配置**。

在**精确访问控制**下，开启防护，并单击**前去配置**。

单击**新增规则**，新增一条防护规则。

白名单配置示例：使用下图配置，放行源IP为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。

黑名单配置示例：使用下图配置，阻断源IP为1.1.1.1的所有访问。

注意事项

同一条防护规则中最多支持3条匹配条件，这些条件之间是“与”的关系。因此，如果您想放行或阻断多个独立的IP/IP段，您需要配置多条访问控制规则。例如，阻断来自1.1.1.1、2.2.2.2、3.3.3.3的所有访问请求，您需要分别配置三条规则。

防护规则中的IP支持掩码格式（如1.1.1.0/24），且逻辑符支持选择“不属于”。因此，如果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，可参考下图配置。

多条防护规则之间存在匹配优先级，按照规则列表中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。

数据风控

功能描述

数据风控帮助您防御网站关键业务（如注册、登录、活动、论坛）中可能发生的欺诈行为，支持防护的场景包括但不限于以下内容：

- 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

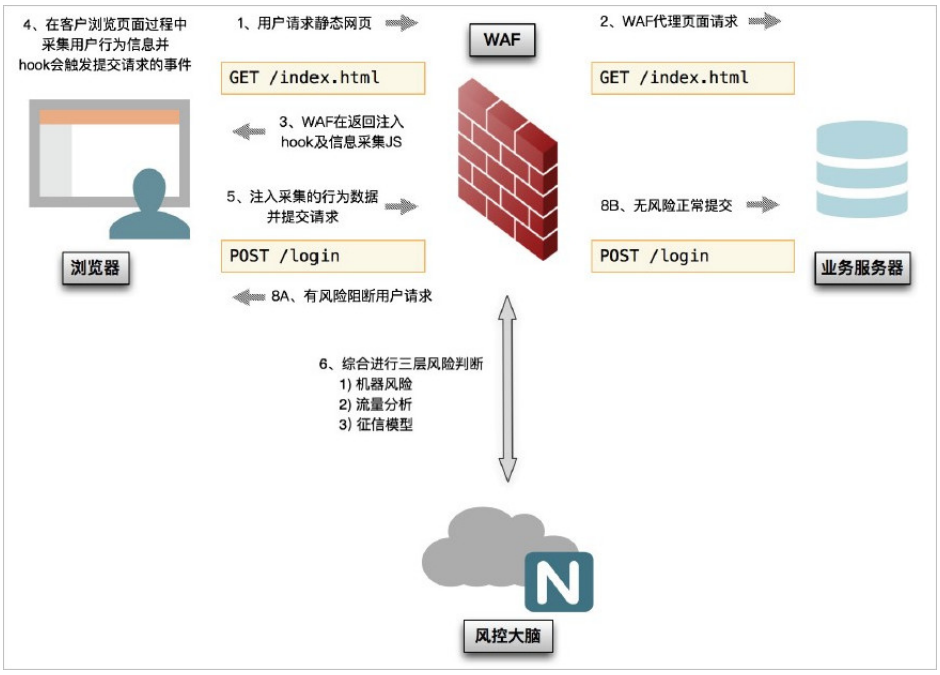
说明：对于WAF高级版，您必须升级到企业版或旗舰版，才能使用数据风控。具体操作请参考续费与升级。

说明：对于按量付费的WAF实例，您必须在**功能与规格**中启用**数据风控**，才能使用该功能。具体操作，请参考功能与规格配置。

说明：数据风控仅适用于网页/H5环境，原生APP防护请参考SDK方案。

数据风控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，防止各类场景的关键业务欺诈行为。您只需接入WAF即可使用数据风控，轻松获取风控能力，而无需在服务器或客户端做任何改造。

下图描述了数据风控的工作流程。



关于接入数据防控的应用场景示例和实际效果，请参考应用示例。

操作步骤

参照以下步骤，启用并配置数据风控：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

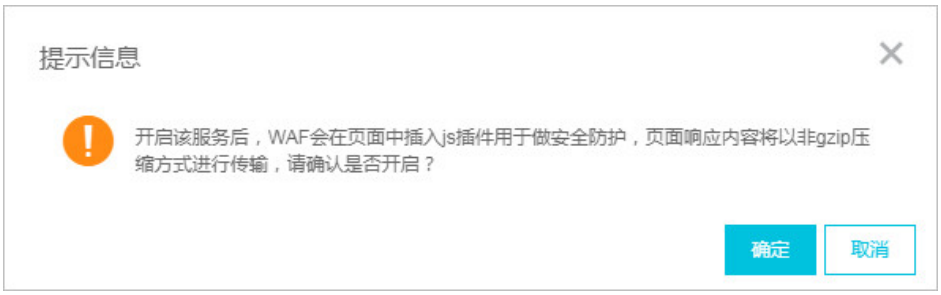
登录云盾Web应用防火墙控制台。

前往**管理**>**网站配置**页面，并选择地区。

选择要操作的域名，单击其操作列下的**防护配置**。

在**数据风控**下，启用防护。

说明：启用数据风控时，您会收到提示，WAF将在页面插入js插件用作安全防护，页面响应内容会以非gzip压缩方式进行传输（即使您的网站使用的是非标端口访问，在配置数据风控时也无需进行额外配置）。确认以上影响后，在**提示信息**对话框中单击**确定**。



说明：如果您不想使用数据风控，您可以在此页面关闭防护。

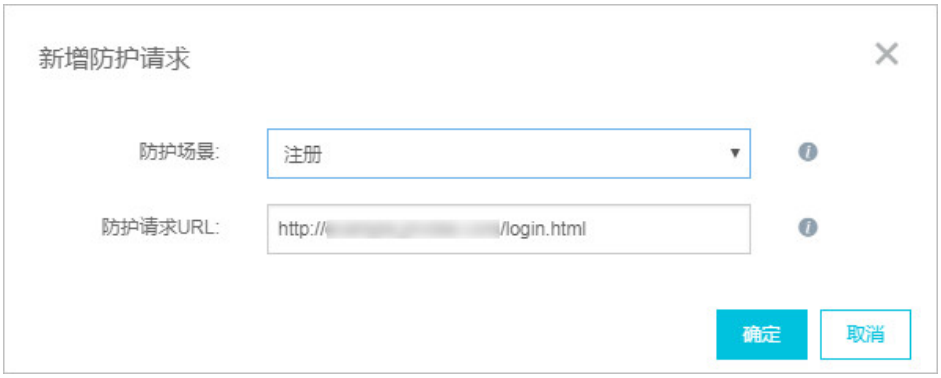
选择防护**模式**：

- **预警**：识别到业务攻击时，只记录日志，不做拦截，攻击情况可通过业务风控报表查看。
- **防护**：识别到业务攻击时，弹出防护页面进行验证。

说明：默认适应预警模式，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。

单击**前去配置**。

单击**新增防护请求**，添加防护规则。



选择**防护场景**：

i. **注册**：防止机器注册、注册短信被攻击。
ii. **登录**：防止刷库撞库、暴力破解。
iii. **论坛**：防止批量发帖、垃圾评论。
iv. **活动**：防止刷红包、抢优惠券、黄牛抢号。

设置**防护请求URL**，即要防护的接口地址。该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。如果设置为页面地址，则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。

说明：防护请求必须精确到请求URL，不支持模糊匹配。如果填写www.test.com/test，则只匹配test，不匹配test下的所有请求。

说明：数据风控支持目录防护，如果您将防护请求URL配置为www.abc.com/book/*，则可防护www.abc.com/book路径下的所有请求。不支持配置全站防护（如

www.abc.com/*），这样会导致用户访问首页也弹出滑块。

说明：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，会被数据拦截。因为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。但是，如果是真人点击页面某个按钮调用了API服务，是可以使用数据风控的。

添加完规则后，您可以**编辑**或者**删除**规则。

启用数据风控后，您可以使用WAF的全量日志功能，查看防护结果。

应用示例

以下为应用数据风控进行防护的一个场景示例，详细解释了数据风控的应用效果，供您参考。

用户小白有一个网站，域名是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（此类黑客即羊毛党）。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并启用了为www.abc.com域名开启数据风控（参考操作步骤步骤4-5）。因为小白最关心的业务是www.abc.com/register.html，所以他针对这个URL配置了特定请求防护（参考操作步骤步骤6-8）。

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。例如，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。数据风控的拦截页面如下图所示：

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。

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地完成注册过程。

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。

查看防护结果

您可以结合WAF的**全量日志查询**功能来排查数据风控的监控和拦截情况。例如，

下图显示了通过风控验证的日志情况。

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。

下图显示了被风控拦截的日志情况。

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**全量日志**功能，在**高级搜索**>**URL关键字**中配置启用数据风控的接口，来排查其拦截情况。

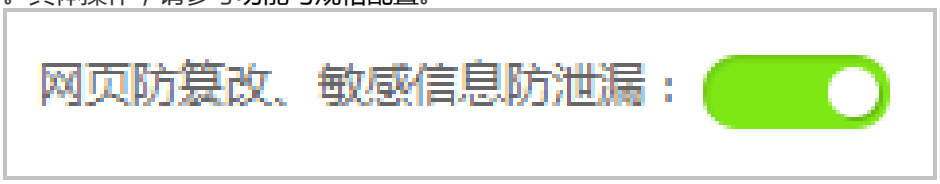
网站防篡改

功能描述

您可以使用网站防篡改对指定的敏感页面设置缓存，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，确保用户看到正确的页面。

说明：对于WAF高级版，您必须升级到企业版或旗舰版，才能使用网站防篡改。具体操作，请参考**续费与升级**。

说明：对于按量付费的WAF实例，您必须在**功能与规格**中启用**网页防篡改、敏感信息防泄露**，才能使用该功能。具体操作，请参考**功能与规格配置**。



操作步骤

参照以下步骤，启用并配置网站防篡改：

说明：执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

登录云盾Web应用防火墙控制台。

前往**管理**>**网站配置**页面，并选择地区。

选择要操作的域名，单击其操作列下的**防护配置**。

在**网站防篡改**下，启用防护，并单击**前去配置**。

单击**新增规则**，在**添加URL**对话框配置要防护的具体页面。

- **业务名称**：为该规则命名。
- **URL**：填写精确的要防护的路径，不支持通配符（如/*）或参数（如/abc?xxx=）。指定页面中可以防止被篡改的内容包括text、html和图片。

添加规则后，手动打开对应规则**防护状态**下的开关。如果您在添加规则后未打开防护开关，则设置不会生效。

打开开关后，WAF会对该页面进行缓存。缓存完毕后，对指定页面的所有请求，WAF将全部返回最近一次缓存的页面内容。

如果被防护页面进行了内容更新，您必须单击**更新缓存**来更新缓存。如果您在页面更新后未更新缓存，WAF将始终返回最近一次缓存的页面内容。

说明：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。

防护统计

总览

云盾Web应用防火墙总览页面提供业务和安全概览信息。

查看业务概览

参照以下步骤，查看业务概览信息：

登录云盾Web应用防火墙控制台。

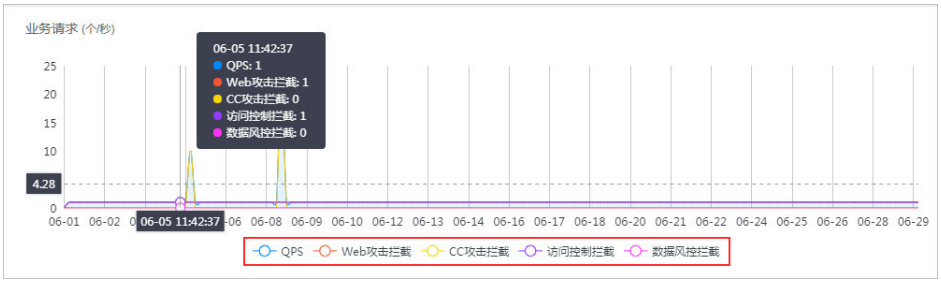
前往**统计**>**总览**页面，选择地域（中国大陆、海外地区）。

在**业务**子页下，选择要查看的域名（可以是一个具体的域名或全部域名）和要查看的历史时间段（实时、6小时、1天、7天、30天、自定义）。

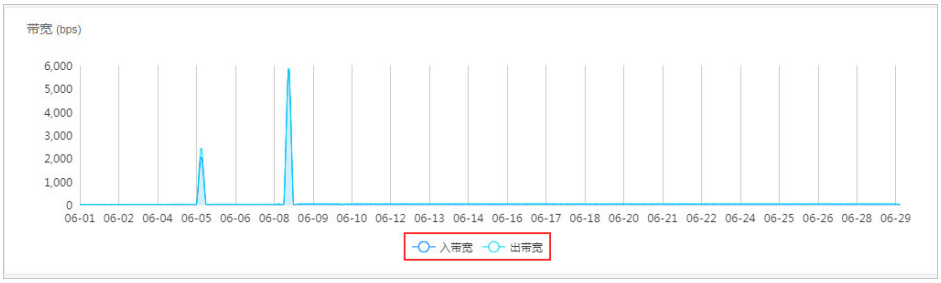
说明：支持查看最近30天内的业务概览信息，使用自定义可以查看最近30天内指定时间段的信息。

支持查看的业务概览信息包括以下内容：

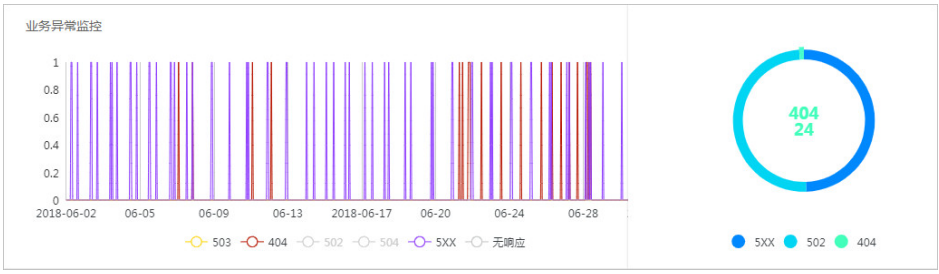
业务请求数和攻击拦截量汇总：展示具体时间段（最小间隔为1分钟）内的QPS、拦截的Web攻击/CC攻击数量、以及命中的访问控制规则、数据风控规则数量。单击图表下方的图例，可以在图中取消/显示对应记录。



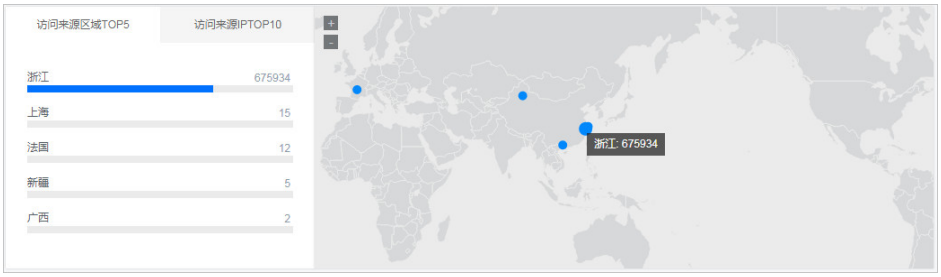
业务带宽统计：展示具体时间段（最小间隔为1分钟）的入带宽和出带宽（单位：bps）。单击图表下方的图例，可以在图中取消/显示对应记录。



业务异常监控：左侧展示具体时间段（最小间隔为1分钟）的业务异常记录，右侧以饼状图展示各类异常的分布。单击图表下方的图例，可以在图中取消/显示对应记录。

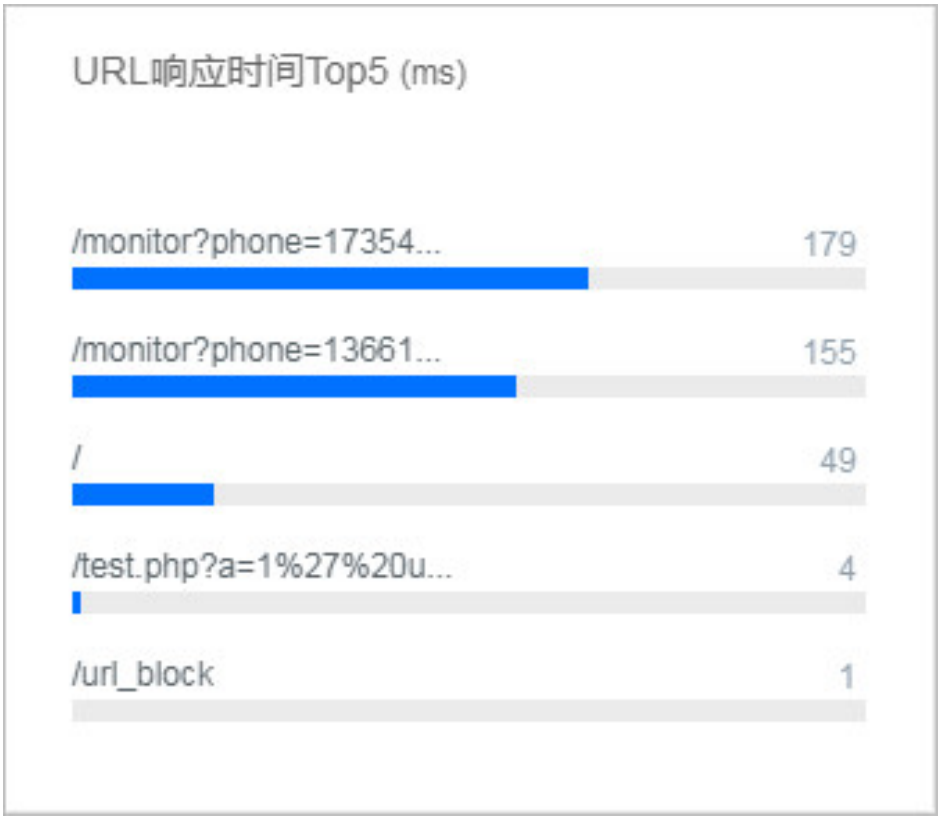


访问分布统计：展示访问来源的分布统计信息，左侧以柱状图展示TOP5访问来源区域和TOP10访问来源IP，右侧地图上以蓝色圆点标识出对应的访问来源。将鼠标放置在圆点上可以显示具体记录。

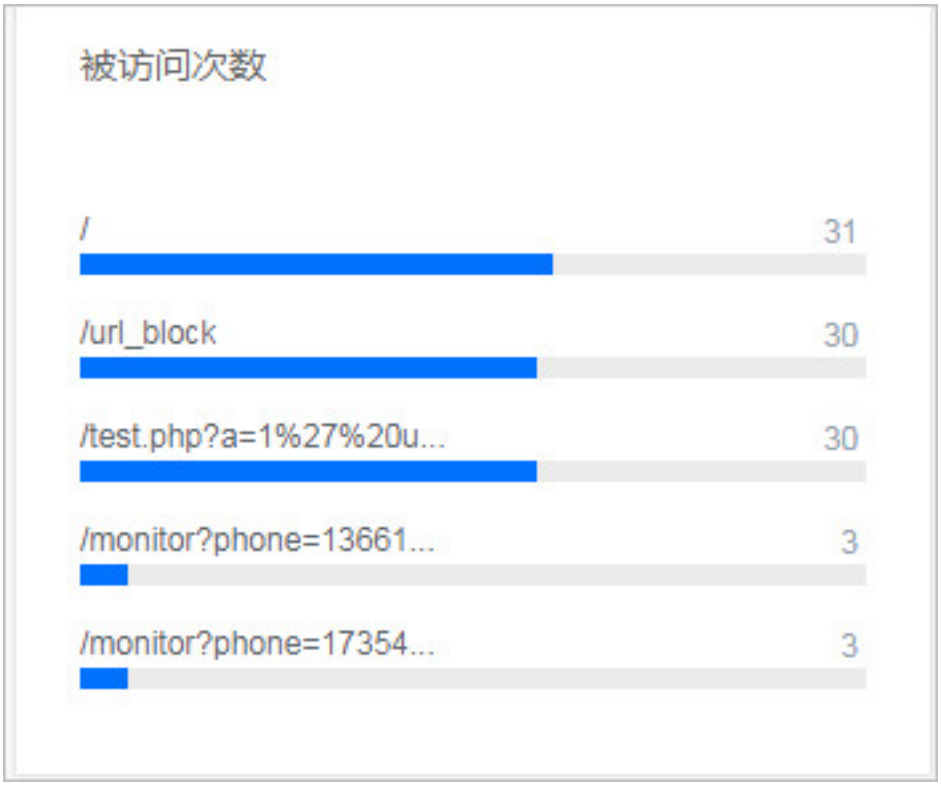


访问源类型分布：分别以饼状图展示移动端访问源的OS类型分布和PC端访问源的浏览器类型分布。

URL响应时间Top5：罗列响应时间最长的Top5 URL和它们的响应时间（单位：ms）。



最常被访问的URL：罗列被访问次数最多的Top5 URL和它们的被访问次数。



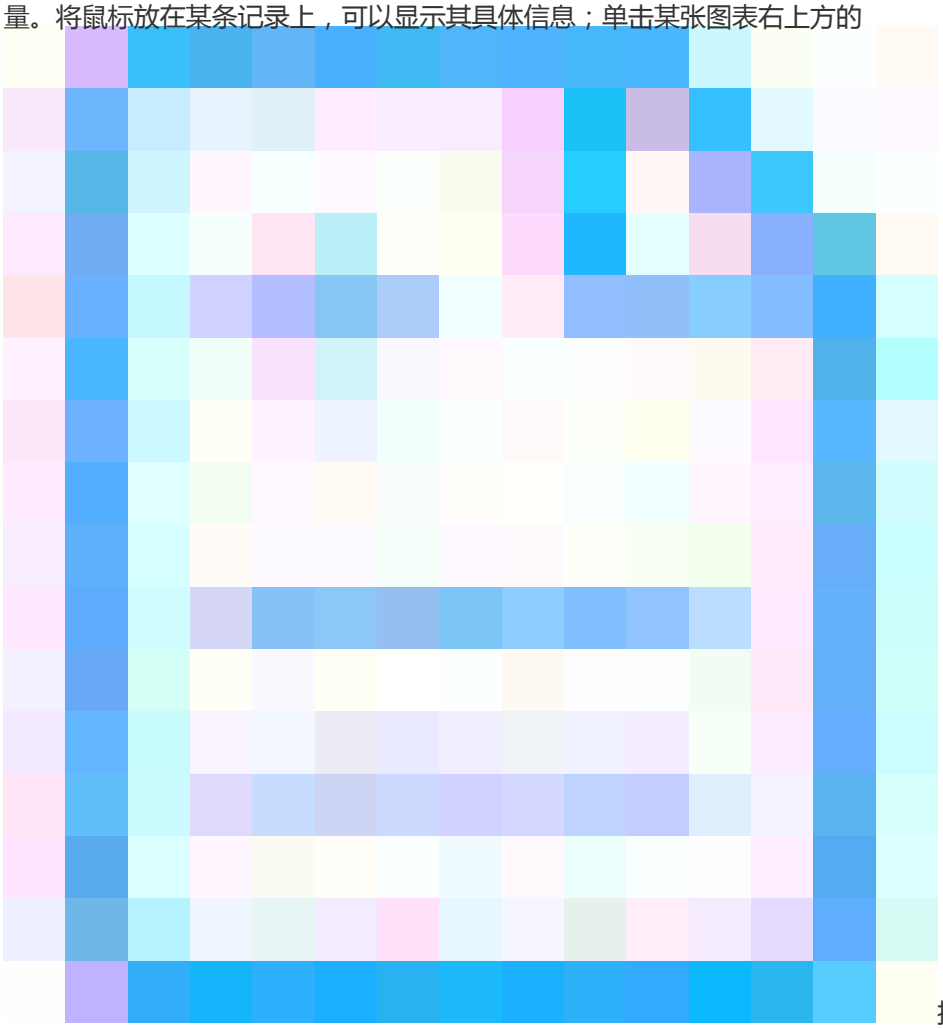
查看安全概览

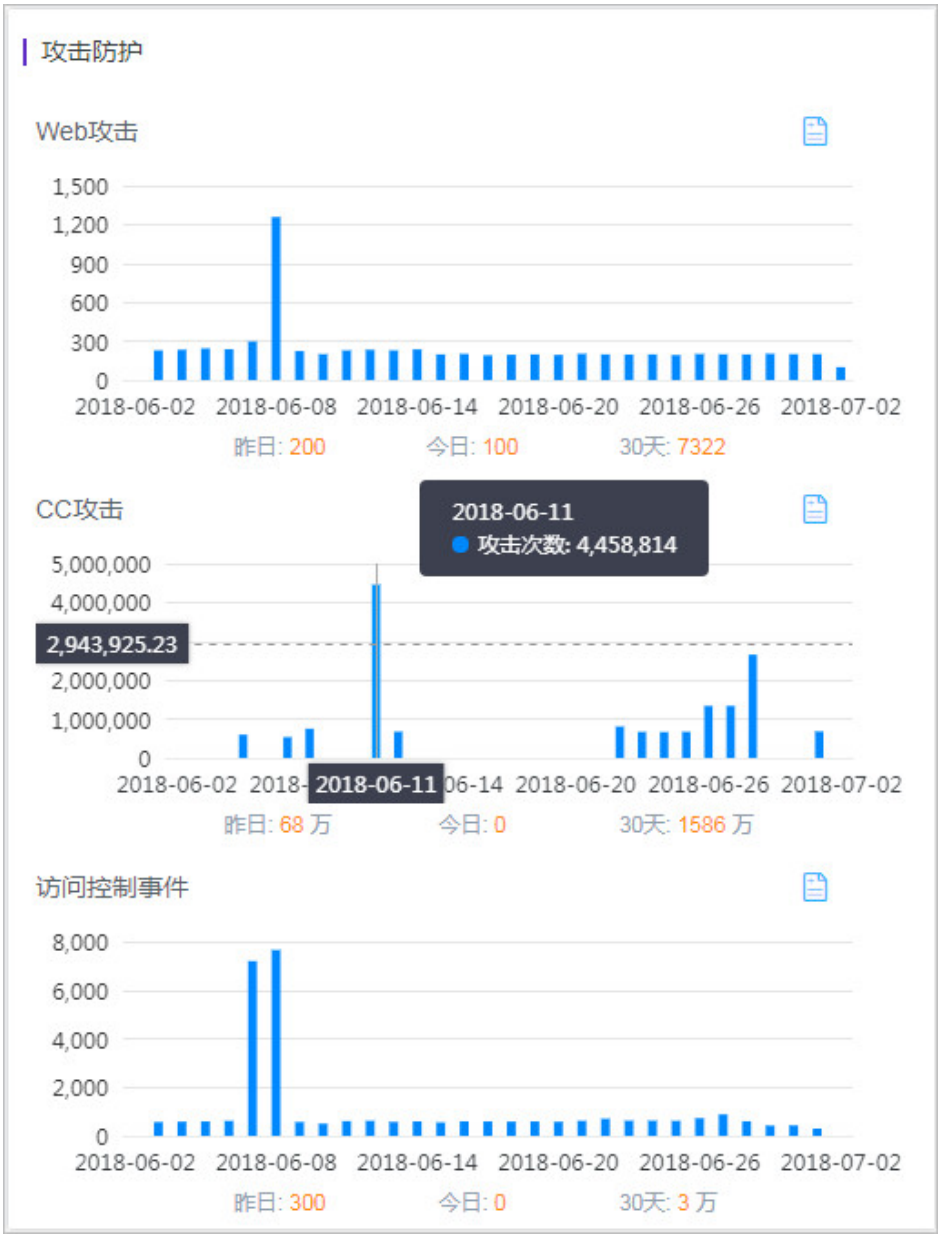
参照以下步骤，查看安全概览信息：

登录云盾Web应用防火墙控制台。

前往**统计**>**总览**页面，选择地域（中国大陆、海外地区）。

在**安全**子页下，查看安全概览信息。支持查看的安全概览信息包括以下内容：

攻击防护统计：分别以柱状图展示最近30天内的Web攻击、CC攻击、和访问控制事件的数量。将鼠标放在某条记录上，可以显示其具体信息；单击某张图表右上方的  按钮可以跳转到对应的**攻击防护报表**，查看其详细记录。



风险预警信息：展示WAF在您的网站上新发现的安全风险和您所在行业最新出现的安全风险，提供对应防护建议。单击**查看报表**可以查看具体的风险预警报表。

消息：展示WAF针对最新披露的漏洞做出的防护规则更新。单击**查看**可以查看具体漏洞公告。

攻击防护报表

WAF提供安全报表，供您查看和了解WAF的所有防护动作。安全报表分为攻击防护和风险预警两个模块，攻击防护集中展示Web应用攻击、CC攻击的防护记录和访问控制事件；风险预警记录并汇总发生在您的网络资产上的常见攻击特征，对您的业务进行风险预警和提示。

说明：对于按量付费的WAF实例，您必须在**功能与规格**中勾选**提供业务分析报表**，才能使用该功能。具体操作，请参考功能与规格配置。

本文介绍了攻击防护报表的使用方法。关于风险预警报表的使用方法，请参考风险预警。

查看攻击防护报表

参照以下步骤，查看攻击防护报表：

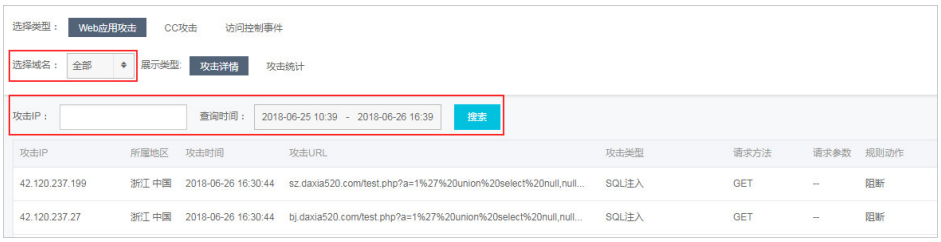
登录云盾Web应用防火墙控制台。

前往**统计**>**安全报表**。

在**攻击防护**子页下，选择要查看的记录类型，查看其防护记录。

Web应用攻击：展示WAF阻断的所有Web攻击记录。您可以使用域名、攻击IP、和攻击时间来筛选您关注的的记录。

说明：关于Web应用攻击防护的功能描述和操作方法，请参考Web应用攻击防护。



默认以攻击详情的形式展示结果，您可以选择查看攻击统计。攻击统计显示了安全攻击类型分布、攻击来源IP TOP5、和攻击来源区域 TOP5。

CC攻击：展示了WAF拦截的针对某个域名的CC攻击记录。您可以选择域名和查询时间，来查看相应记录。

说明：关于CC安全防护的功能描述和操作方法，请参考CC安全防护。

页面上方显示了总QPS和攻击QPS的实时记录，下面罗列了所有恶意CC攻击事件。WAF对CC攻击事件的定义是：攻击持续时间 > 3分钟，且每秒攻击次数 > 100。

访问控制事件：展示了针对某个域名的访问控制事件记录。您可以选择域名和查询时间，来查看相应记录。

说明：关于精准访问控制的功能描述和操作方法，请参考**精准访问控制**。

风险预警报表

WAF提供安全报表，供您查看和了解WAF的所有防护动作。安全报表分为攻击防护和风险预警两个模块，攻击防护集中展示Web应用攻击、CC攻击的防护记录和访问控制事件；风险预警记录并汇总发生在您的网络资产上的常见攻击特征，对您的业务进行风险预警和提示。

说明：对于按量付费的WAF实例，您必须在**功能与规格**中勾选**提供业务分析报表**，才能使用该功能。具体操作，请参考**功能与规格配置**。

本文介绍了风险预警报表的使用方法。关于攻击防护报表的使用方法，请参考**攻击防护**。

查看风险预警报表

WAF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，支持查看的攻击特征记录包括：黑客攻击、Wordpress、疑似攻击、robots脚本、爬虫访问、和短信滥刷。

参照以下步骤，查看风险预警报表：

登录云盾Web应用防火墙控制台。

前往**统计>安全报表**。

在**风险预警**子页下，选择要查看的风险请求类型，查看其记录内容。各类风险请求记录的具体描述，参见下文说明。

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或组织。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，单击一个圆点可以看到详细的攻击记录。其中：

- 不同行代表不同的黑客个体，单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。

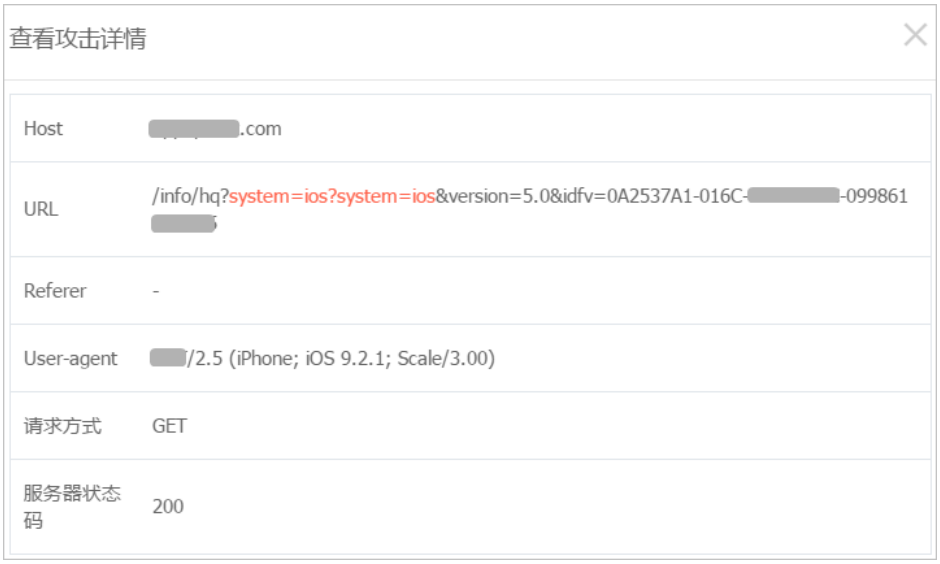
防护建议：

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：

可使用日志分析排查是否有CC攻击，并结合精准访问控制、CC安全防护攻击紧急模式、封禁地区等防护算法拦截恶意攻击。

爬虫访问

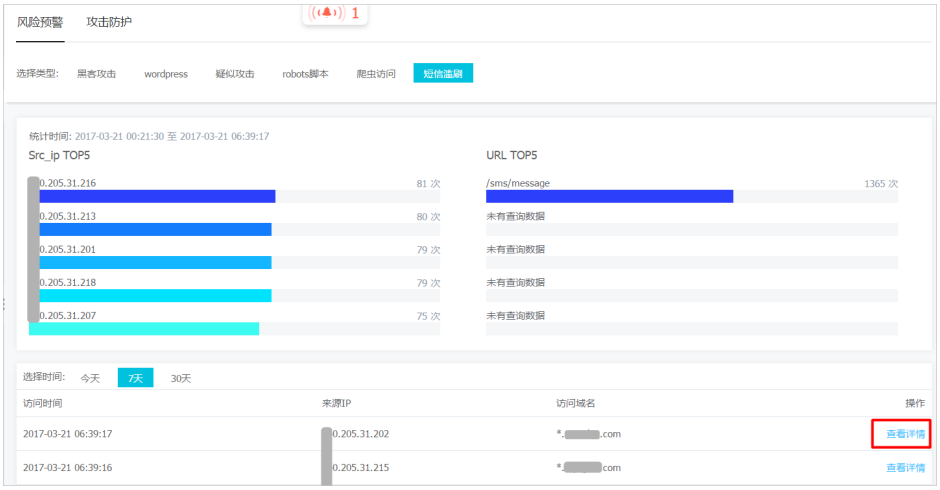
WAF支持检测爬虫请求（包含合法的爬虫，如百度蜘蛛等）。如果该报警数字很大，同时服务器有请求量异常增大，CPU升高等现象，则可能是遇到了伪装成爬虫的CC攻击或恶意爬虫的爬取。

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。

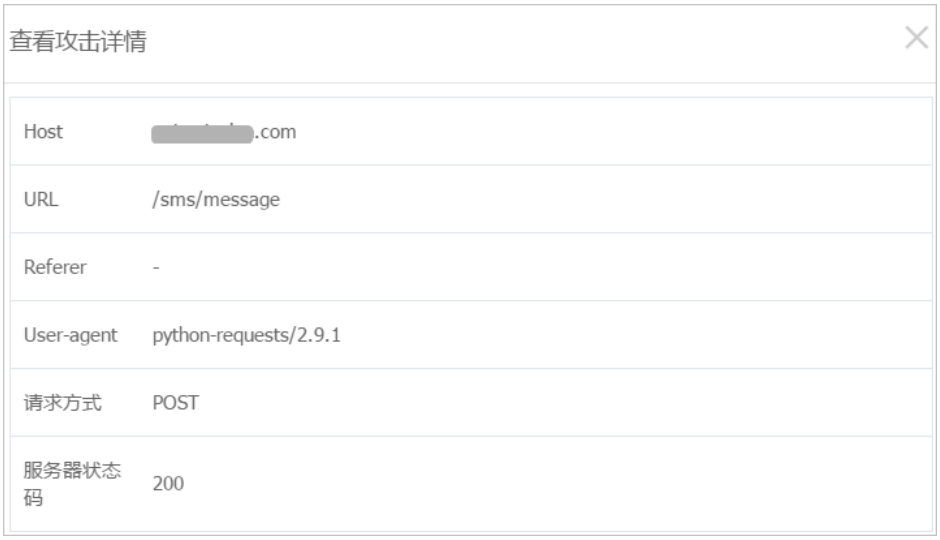
短信滥刷

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：

单击**查看详情**了解具体的请求。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

功能概述

启用全量日志功能后，WAF将记录您网站的所有访问请求日志，您可以通过一键智能搜索快速定位请求记录，满足运维、安全方面的管理需求。

说明：对于WAF高级版，您必须升级到企业版或旗舰版，才能使用全量日志查询。具体操作请参考**续费与升级**。

说明：对于按量付费的WAF实例，您必须在**功能与规格**中勾选**全量日志查询**，才能使用该功能。具体操作，请

参考功能与规格配置。

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：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：WAF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。

前往**管理**>**网站配置**页面，并选择地区。

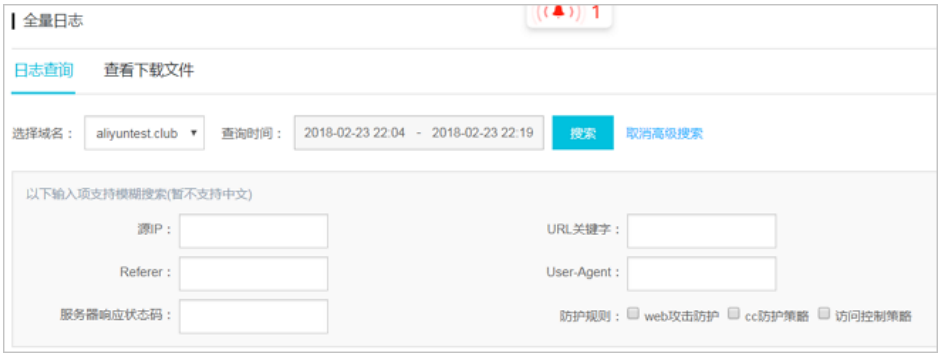
选择已添加的网站域名，在**日志检索**栏，单击开启日志检索功能。

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。

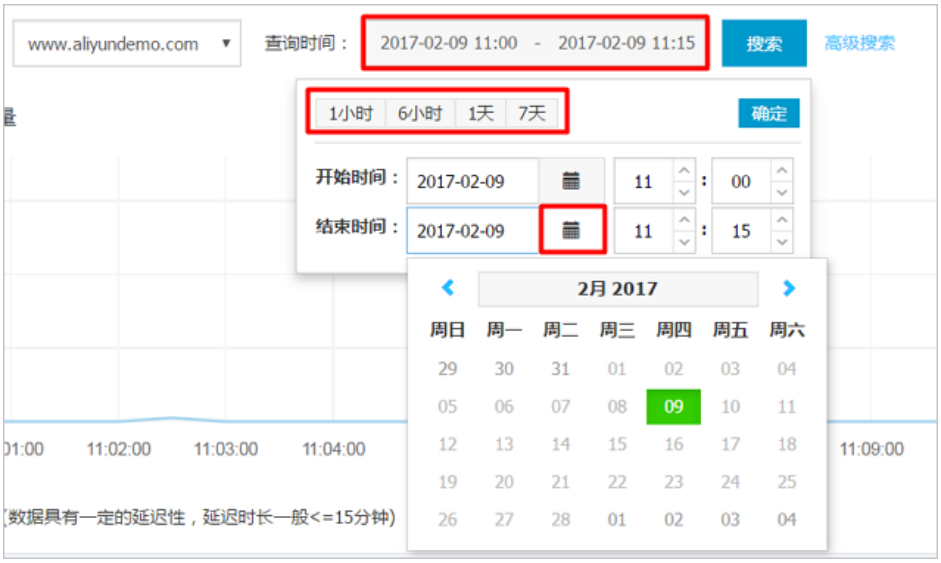
登录云盾Web应用防火墙管理控制台。

前往**统计**>**全量日志**页面。



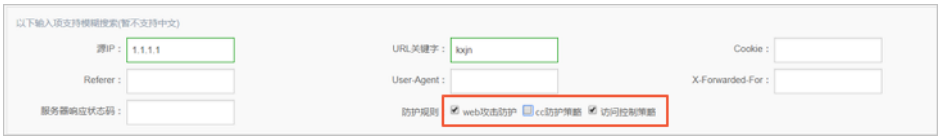
选择**域名**，设置**查询时间**，单击**搜索**。

说明：全量日志功能最多记录最近一个月内的访问日志。



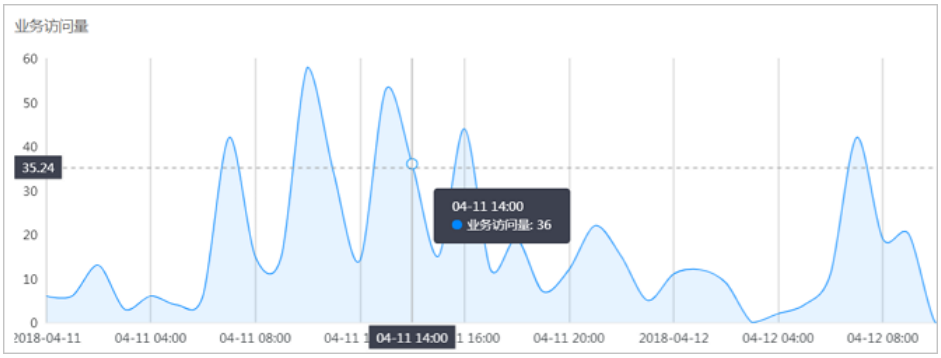
您也可以单击**高级搜索**，设置更详细的检索条件。

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。

说明：如果您停用日志检索功能，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

依托接入WAF后的网站业务日志，WAF提供可视化大屏服务，将数据转化为直观的可视化报表，对WAF的实时攻防态势进行监控和告警，为您提供可视化、透明化的数据分析和决策能力，让安全攻防一目了然。

功能说明

WAF可视化大屏提供以下展示指标：

网络流量态势：以秒级数据维度，展示业务访问出、入方向流量、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：通过访问日志展示业务来访者中的访问最频繁的TOP来访IP、来访IP在全国省市级地域分布、访问者浏览器/UserAgent/操作系统占比，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，如TOP攻击源IP、拦截趋势、拦截比例、TOP命中规则、攻击事件类型，体现实时防御效果。

WAF数据可视化大屏的整体效果如下所示。

如何购买和开通

WAF数据可视化大屏可以根据您的需求定制展示数据的时间颗粒度和展示维度。

可视化大屏目前只开放**线下**购买和开通途径。如果您有相关需求，您可以通过以下方式联系我们，您将获得阿里云Web安全大屏专家的建议和定制化方案：

说明：由于大屏的特殊性，目前仅支持谷歌 Chrome 浏览器版本 56 以上。

扫码加入下方的官方钉钉咨询群。

- 服务时间：5*8，不含法定节假日（非此时间内如遇到紧急问题，仍可以使用该方式沟通）。
- 仅限于已经购买使用了WAF服务付费用户。

提交工单，并注明：WAF数据可视化大屏咨询。

SDK方案

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**管理**>**网站配置**页面，将App使用的域名添加进来，为其开启WAF防护。具体步骤请参考添加网站配置。

在App域名解析服务商处，添加CNAME记录，将App域名解析指向WAF。具体步骤请参考修改DNS解析。

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

关于SDK的详细接入操作，请参考：

- iOS接入文档
- Android接入文档

说明：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。

联系WAF技术支持人员测试集成好的App。您可以扫描文末的二维码，通过钉钉联系WAF技术支持人员。

打包发布新的App版本，享受SDK防护。

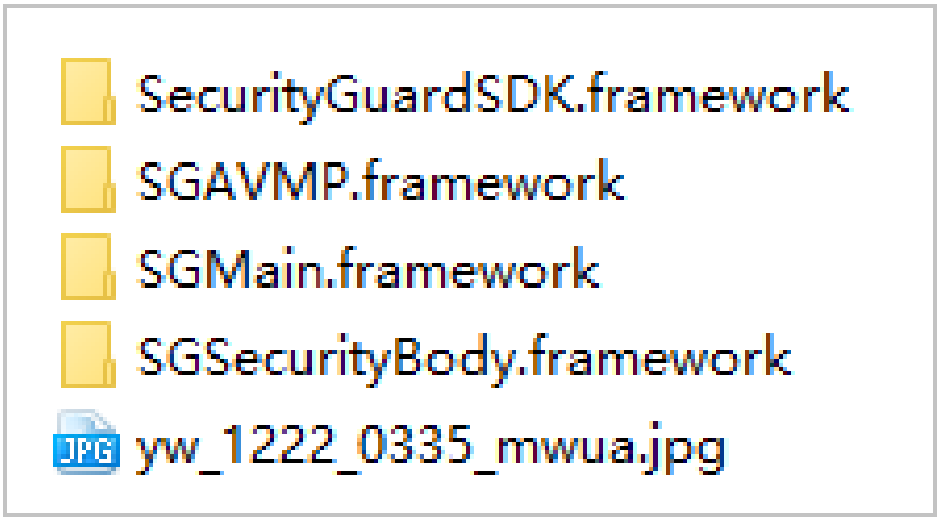
如果您对方案/接入有任何问题，请扫描下方的钉钉二维码联系我们（进群时请说明咨询SDK方案）。

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：

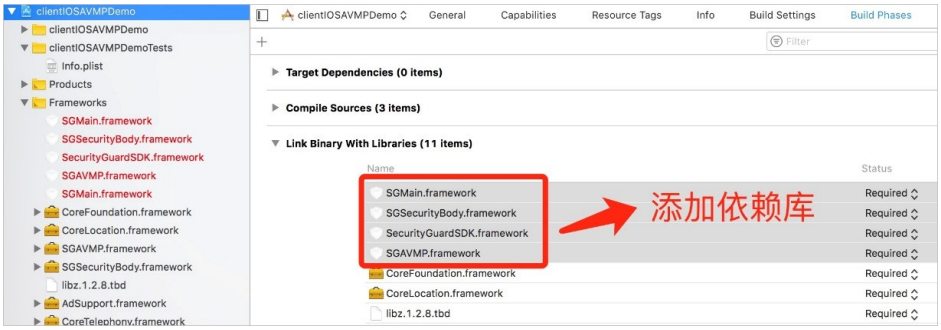
文件	功能
SGMain.framework	主框架SDK
SecurityGuardSDK.framework	基础安全插件
SGSecurityBody.framework	人机识别插件

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

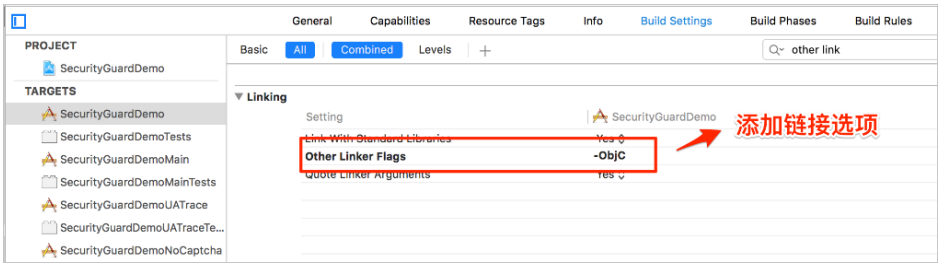
项目工程配置

参照以下步骤，来配置项目工程。

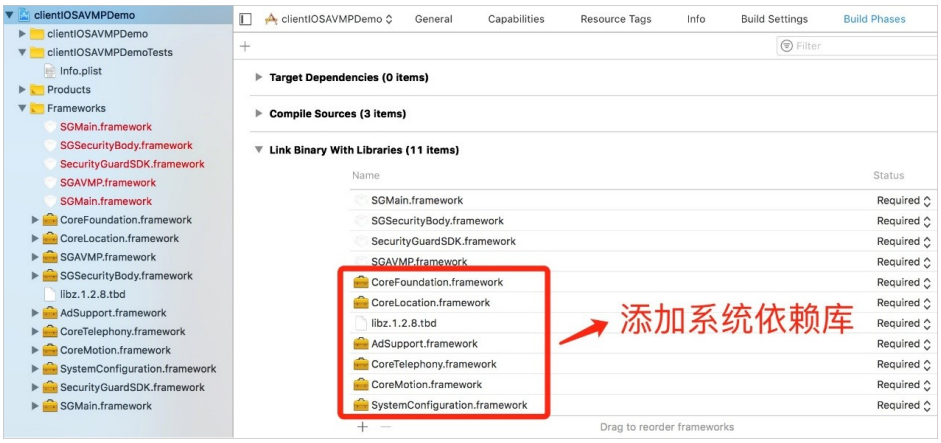
添加 Framework。将 WAF SDK 中提供的 4 个 .framework 文件添加到工程的依赖库中。



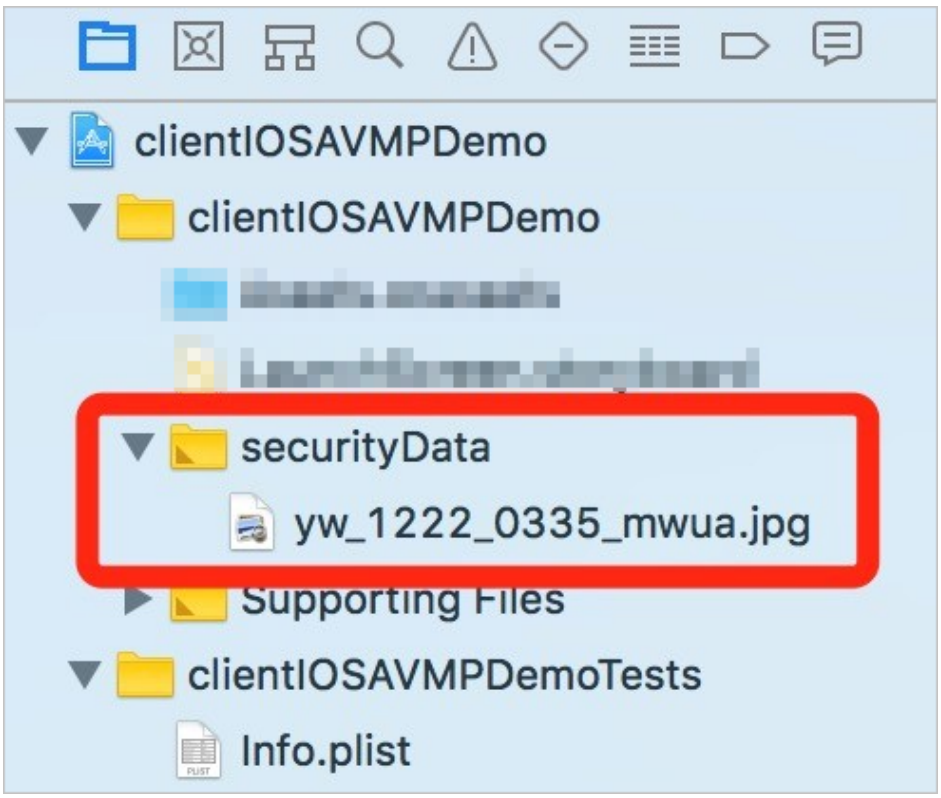
设置链接选项。



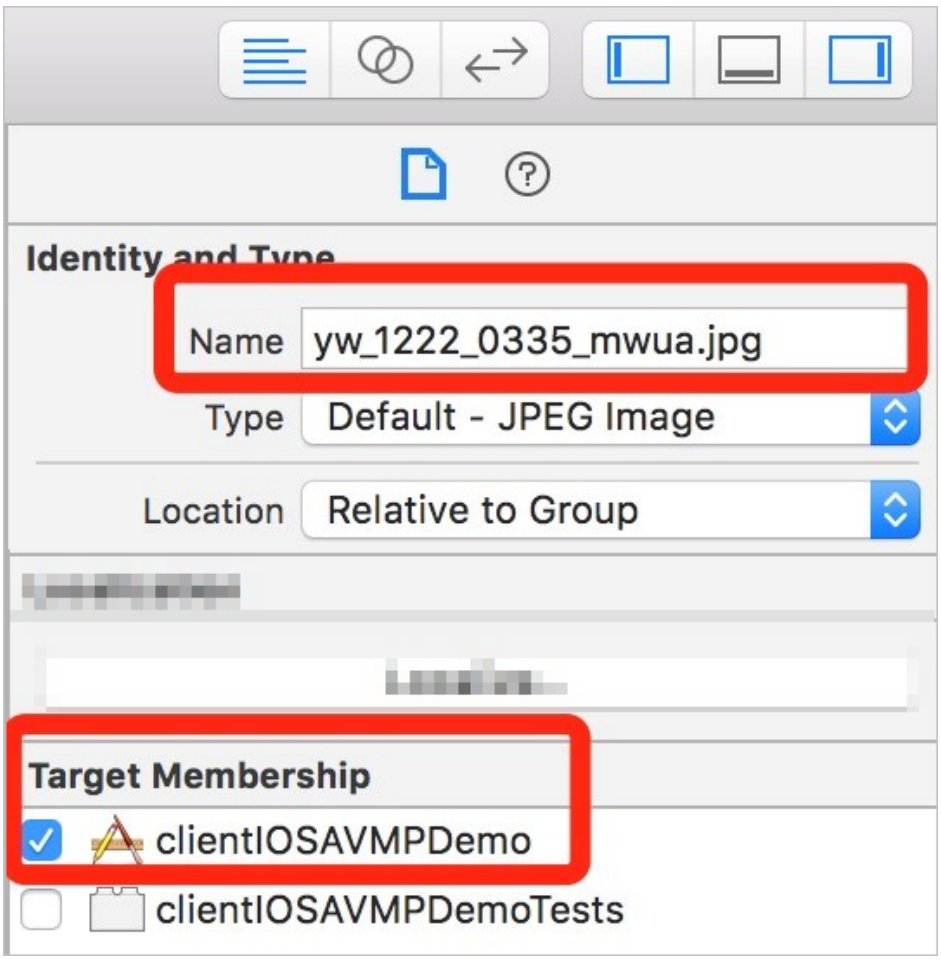
添加系统依赖库。



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。
- 重点注意： **被签名的请求体应该跟客户端实际发送出来的请求体完全一样，完全一样的含义包括请求体中字符串的编码格式、空格、特殊字符以及参数的顺序等等，否则会造成验签失败。**

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（request body）。如果请求体为空（如POST请求的body为空，或是GET请求），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。

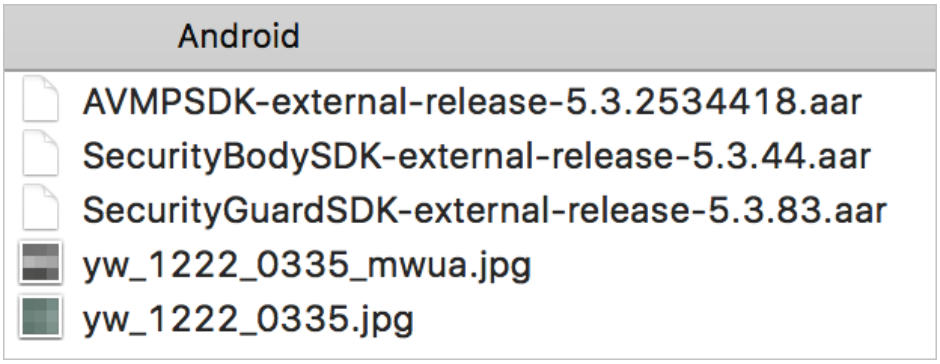
Android 接入文档

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包），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。



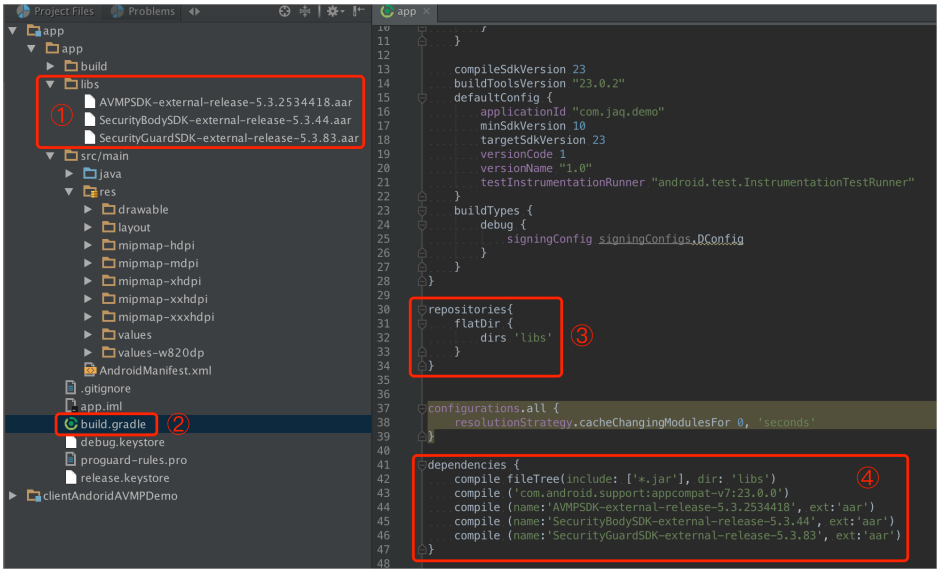
各文件说明（xxx为版本号）：

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'
}
}
```

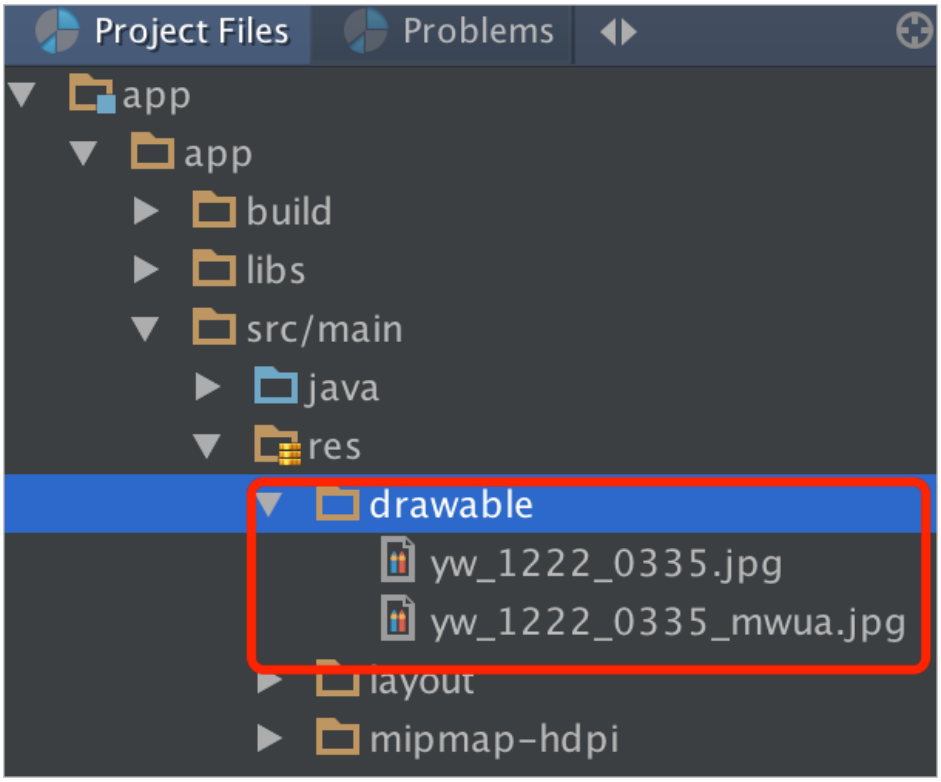
- 增加编译依赖。**注意**：aar 文件版本号可能会有不同，以下载得到的文件为准。

```
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 目前仅支持 armeabi、armeabi-v7a、arm64-v8a 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 架构的文件夹，包括 x86、x86_64、mips、mips64 等。最终，只保留 armeabi、armeabi-v7a、arm64-v8a 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。示例代码如下：

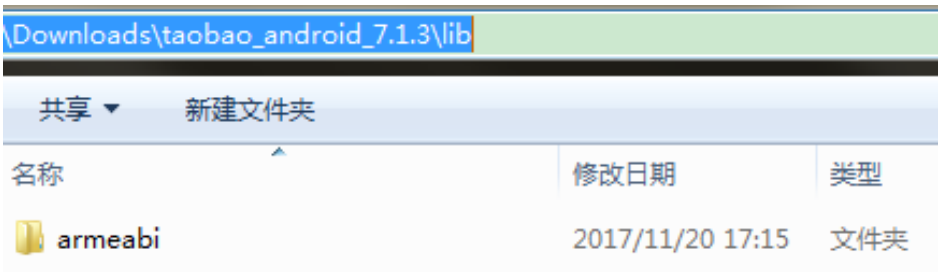
说明： 本代码示例中指定了 armeabi 架构，您可以根据实际情况指定或兼容 armeabi-v7a、arm64-v8a 架构。

```
defaultConfig {
applicationId "com.xx.yy"
minSdkVersion xx
targetSdkVersion xx
versionCode xx
versionName "x.x.x"
ndk {
abiFilters "armeabi"
// abiFilters "armeabi-v7a"
// abiFilters "arm64-v8a"
```

```
}
}
```

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。

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（request body）。如果请求体为空（如POST请求的body为空，或是GET请求），那么此参数使用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。

重点注意： **被签名的请求体应该跟客户端实际发送出来的请求体完全一样，完全一样的含义包括请求体中字符串的编码格式、空格、特殊字符以及参数的顺序等等，否则会造成验签失败。**

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。

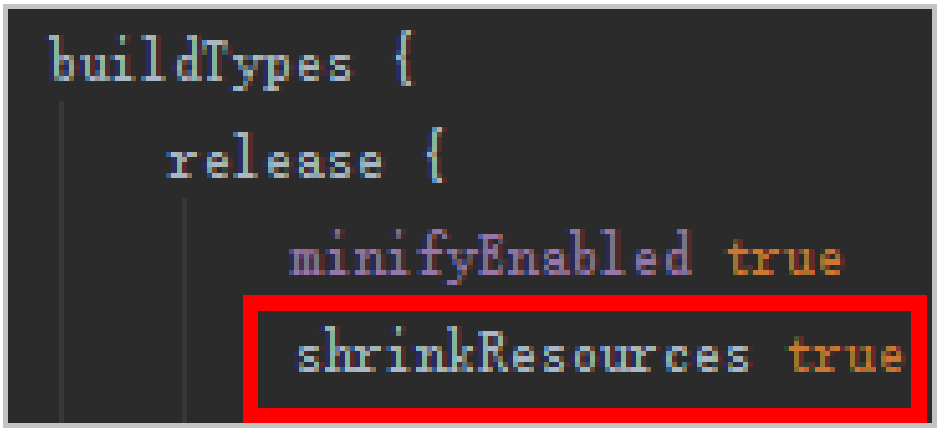
错误代码	含义
1901	参数不正确，请检查输入的参数。
1902	图片文件有问题。一般是获取图片文件时的 apk 签名和当前程序的 apk 签名不一致。请使用当前程序的 apk 重新生成图片。iOS 可能是应为 BundleID 不匹配。
1903	图片文件格式有问题。
1904	请升级新版本图片。AVMP 签名功能仅支持 v5 图片。
1905	没有找到图片文件。请确保图片文件在 res\drawable 目录下，AVMP 相关的图片为：yw_1222_0335_mwua.jpg。
1906	图片中缺少 AVMP 签名对应的 byteCode。请检查使用的图片是否正确。
1907	初始化 AVMP 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。

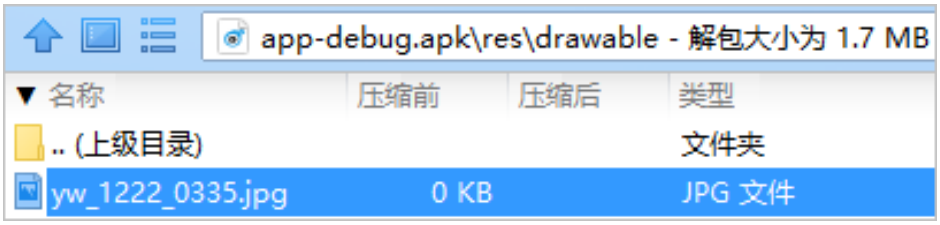
常见问题

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。

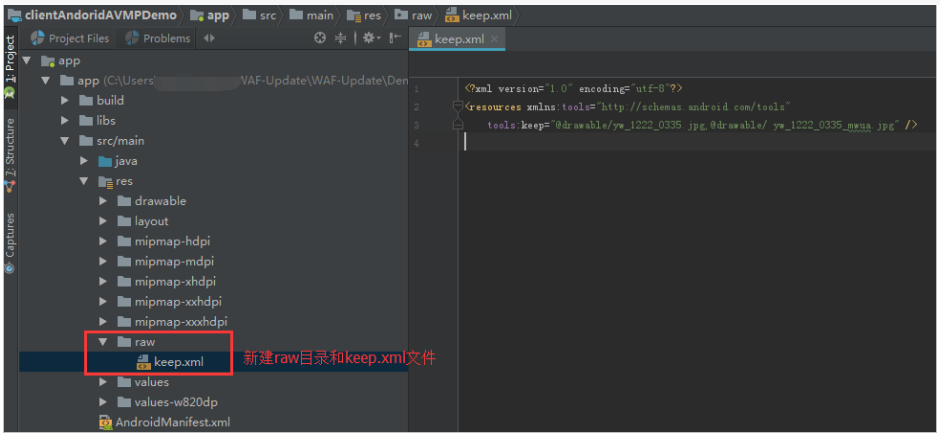


解决方法

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" />
```



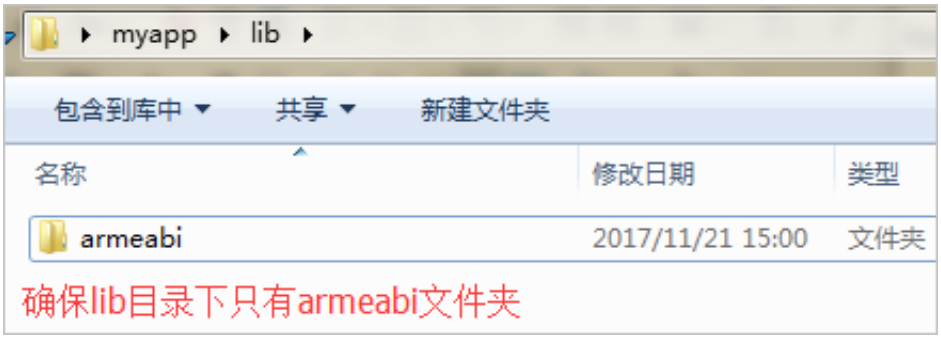
添加完上述内容，重新编译工程 apk 即可。

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。

蚁盾手机号风控服务

配置手册

如有配置问题，您可以通过以下钉钉二维码联系我们。

您可以通过以下方式，和我们建立直达沟通：

在手机 或 电脑上，下载并注册“钉钉”聊天软件（http://www.dingtalk.com/index-b.html#download_block ）

扫描二维码进群，与WAF的产品经理和安全专家在线沟通

功能与规格配置（按量付费模式）

以按量付费模式开通WAF后，您可以实时调整WAF的功能与规格，享受更贴近业务现状的安全防护。功能与规格调整保存后，实时生效；每日账单依据当天最高配置进行计算。

说明：调整WAF的功能规格后，WAF的计费也会发生变化，关于按量付费WAF的计费方式，请参考产品价格页。WAF控制台也提供了基于当前配置的价格预估功能，具体参考查询价格预估。

支持调整的功能

- Web攻击防护：抵御各类Web应用攻击，如SQL注入、命令执行、XSS等。
- 恶意IP封禁：对集中式扫描进行短暂的IP封禁。
- 语义分析引擎：发现SQL注入和XSS高危风险，降低误报率。
- CC安全防护：独家算法防护引擎、结合大数据、秒级拦截机器恶意CC攻击。
- 精准访问控制(黑白名单)：针对性地拦截或放行某次访问。
- 数据风控：防止垃圾注册、账号被盗、活动作弊、垃圾消息等欺诈威胁。
- 网页防篡改：防止指定网站目录页面被篡改。
- 敏感信息防泄露：避免身份证、银行卡、电话号码等敏感数据泄露；针对服务器返回的异常页面或关键字做信息保护。
- 封禁地区：针对指定的国内省份或海外地区的来源IP进行一键黑名单封禁。
- 独享IP：可针对域名开启，使其不受针对其他域名的DDoS攻击的影响。
- 扩展域名包：购买后支持接入更多域名进行防护。

操作步骤

参照以下步骤，调整按量付费WAF实例的功能与规格：

登录云盾Web应用防火墙控制台。

前往**设置**>**功能与规格**页面。

根据需要，在**功能与规格设置**下调整相应设置。

Web攻击防护：提供基础防护和高级防护两种规格。

- 默认使用基础防护，该规格支持预警和拦截模式，以及宽松、正常、严格三种防

护策略。关于防护策略的调整方法，请参考Web应用攻击防护。

- 高级防护在基础防护的基础上，提供恶意IP惩罚和新智能防护引擎功能。关于新增功能的操作，请分别参考恶意IP惩罚和新智能防护引擎。

缓解CC攻击：提供基础防护和高级防护两种规格。

- 默认使用基础防护，该规格依据独家算法引擎，支持秒级拦截恶意CC攻击，并提供正常和攻击紧急两种拦截模式。关于拦截模式的调整方法，请参考CC安全防护。
- 高级防护在基础防护的基础上，提供基于URL设定IP访问频率的功能，即自定义CC防护规格，每个域名可设置50条规则。有关操作，请参考自定义CC防护。

精准访问控制（黑白名单）：提供基础防护和高级防护两种规格。

- 基础防护提供基于IP和URL的黑白名单功能，每个域名可设置10条规则。有关操作，请参考IP黑白名单配置。
- 高级防护提供基于IP、URL、Cookie、User-Agent、Referer、提交参数、X-Forwarded-For等各类常见HTTP头部的逻辑组合判断功能，每个域名可设置100条规则。关于精准访问控制的具体操作，请参考精准访问控制。

数据风控：开启后可以配置防护格则，防止恶意短信注册、恶意登录、活动作弊等机器威胁。有关操作，请参考数据风控。

网页防篡改、敏感信息防泄漏：开启后支持网站防篡改和防敏感信息泄露功能，具体请分别参考网站防篡改和防敏感信息泄露。

支持HTTPS业务：勾选后，可以设置网站一键HTTPS（仅需上传证书私钥，而无需变更源站）和设置HTTP回源，降低网站负载损耗。有关操作，请参考HTTPS高级配置。

全量日志查询：勾选后，WAF会记录网站上所有访问请求日志，并提供一键智能搜索，快速定位请求，方便运维、安全相关管理。有关操作，请参考**全量日志查询**。

支持非标端口业务防护：勾选后，可以使用默认端口（HTTP：80、8080；HTTPS：443、8443）以外的非标端口接入WAF。关于WAF支持的非标端口，请参考**非标端口支持**。

说明：开启非标端口支持后，不支持关闭。

支持基于地理位置的区域封禁：勾选后，可以针对指定国内省份或海外地区的来源IP进行一键黑名单封禁。有关操作，请参考**封禁地区**。

提供业务分析报表：勾选后，可以查看安全报表，包括访问次数、访问IP个数、访问源IP和区域的Top排行，以及响应时间和响应状态码的分布等信息。有关操作，请参考**攻击防护报表和风险预警报表**。

扩展域名包：支持根据需求增加扩展域名包的数量。WAF默认支持接入10个域名(仅限在1个一级域名下)；每增加1个域名包，则可以多使用一个不同的一级域名，且支持多接入10个域名。最多可增加1,000个扩展域名包。具体介绍，请参考**扩展域名包说明**。

说明：增加扩展域名包数量后，不支持减小。

独享IP：支持增加独享IP的数量。每30天内只允许做1次调整。最多可增加10个独享IP。关于独享IP的具体介绍，请参考**独享IP包说明**。

说明：增加独享IP数量后，不支持减小。

调整完功能规格后，单击页面下方的**保存设置**，使设置生效。

查询价格预估

针对当前功能与规格配置，WAF支持预估按量付费的日结费用。

登录云盾Web应用防火墙控制台，前往**设置**>**功能与规格**页面，在**价格预估**下设置被防护网站的QPS日峰值，左侧即显示出当前配置下WAF实例的价格，单位：元/天。

说明：预估价格仅作为计费参考，实际价格以账单为准。

关闭WAF

如果您决定不再继续使用按量计费模式的WAF实例，您可以关闭WAF，确保不再产生任何费用。包年包月模式的WAF实例到期后，您也可以通过关闭WAF来释放该实例。

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：您必须先关闭当前按量付费模式的WAF实例。
- 从包年包月模式变更为按量付费模式：您必须先释放已到期的包年包月模式的WAF实例。

前提条件

您只能在以下情况下关闭或释放WAF实例：

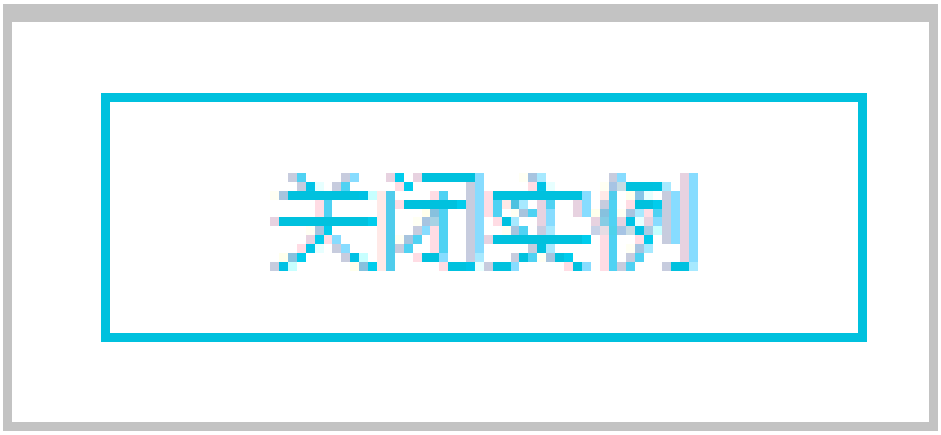
- **包年包月模式**： WAF实例已经到期。
- **按量付费模式**： 近两日内仅有少量或没有请求到达WAF实例。

操作步骤

说明：关闭WAF实例前，请确认当前配置的网站域名DNS已解析回源站。关闭或释放WAF实例后，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，其将无法被正常转发，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**关闭实例**。



说明：包年包月模式的WAF只有在实例到期后，才会出现该按钮。

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。