阿里云
Web应用防火墙

最佳实践

文档版本：20200120

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. **您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。**
2. **未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。**
3. **由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。**
4. **本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。**
5. **阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。**
6. **如若发现本文档存在任何错误，请与阿里云取得直接联系。**

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意:** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击设置 > 网络 > 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击**确定**。
`Courier字体`	命令。	执行`cd /d C:/window`命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{}或者{a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1 Web漏洞防护最佳实践

1.1 FastJSON远程代码执行0day漏洞（2019-7-23）

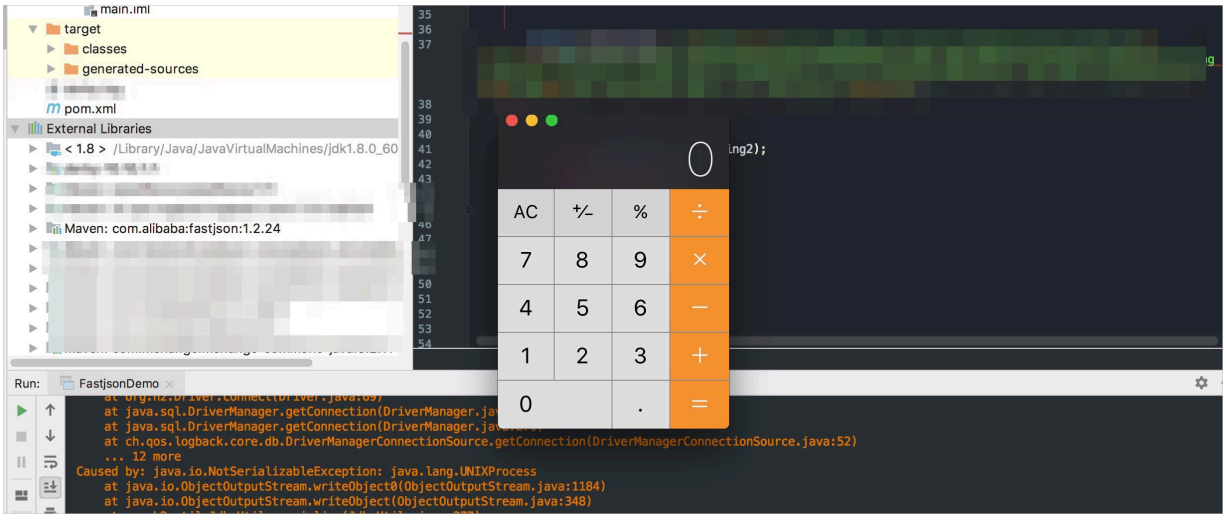
2019年7月23日，阿里云云盾应急响应中心监测到FastJSON存在0day漏洞，攻击者可以利用该漏洞绕过黑名单策略进行远程代码执行。

漏洞名称

FastJSON远程代码执行0day漏洞

漏洞描述

利用该0day漏洞，恶意攻击者可以构造绕过FastJSON黑名单策略补丁的攻击请求，进行远程代码执行攻击。例如，攻击者通过精心构造的请求，绕过FastJSON黑名单策略补丁远程让服务端执行指定命令（以下示例中成功运行计算器程序）。



影响范围

- **FastJSON 1.2.24及以下版本**
- **FastJSON 1.2.41至1.2.45版本**

官方解决方案

升级至FastJSON最新版本，建议升级至1.2.58版本。

> **说明:**
> **强烈建议不在本次影响范围内的低版本FastJSON也进行升级。**

升级方法

您可以通过更新Maven依赖配置，升级FastJSON至最新版本（1.2.58版本）。

```
<dependency>
 <groupId>com.alibaba</groupId>
 <artifactId>fastjson</artifactId>
 <version>1.2.58</version>
</dependency>
```

防护建议

Web应用防火墙的Web攻击防护规则中已默认配置相应规则防护该FastJSON 0day漏洞，启用Web应用防火墙的Web应用攻击防护功能即可。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

1.2 FastJSON远程代码执行0day漏洞（2019-6-22）

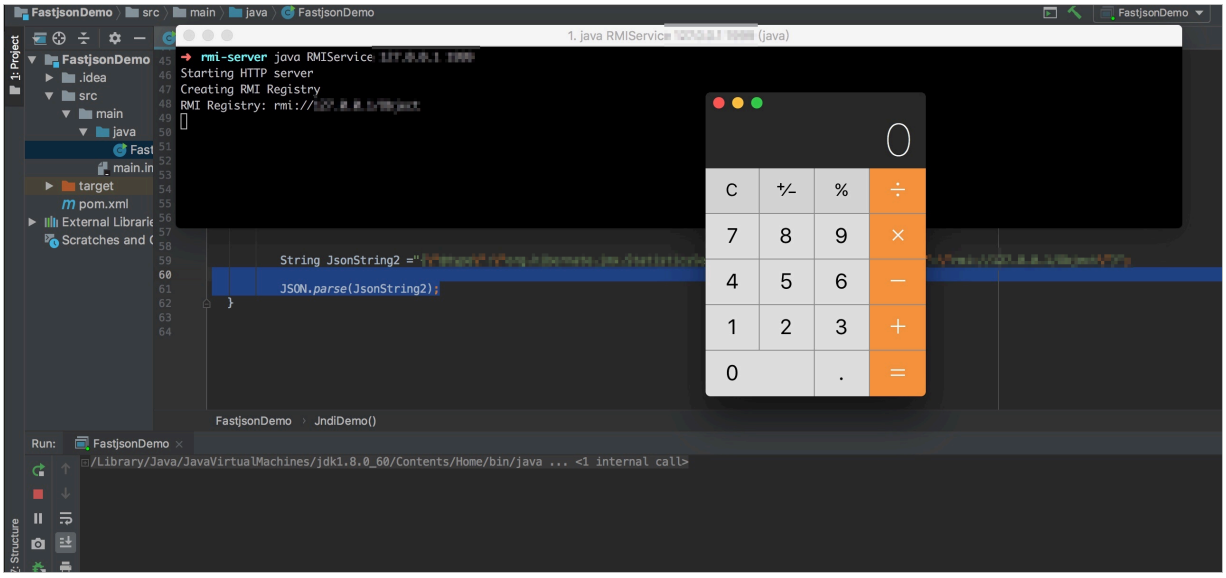
2019年6月22日，阿里云云盾应急响应中心监测到FastJSON存在0day漏洞，攻击者可以利用该漏洞绕过黑名单策略进行远程代码执行。

漏洞名称

FastJSON远程代码执行0day漏洞

漏洞描述

利用该0day漏洞，恶意攻击者可以构造攻击请求绕过FastJSON的黑名单策略。例如，攻击者通过精心构造的请求，远程让服务端执行指定命令（以下示例中成功运行计算器程序）。



影响范围

FastJSON 1.2.48以下版本

官方解决方案

升级至FastJSON最新版本，建议升级至1.2.58版本。

说明:

强烈建议不在本次影响范围内的低版本FastJSON也进行升级。

升级方法

您可以通过更新Maven依赖配置，升级FastJSON至最新版本（1.2.58版本）。

```
<dependency>
 <groupId>com.alibaba</groupId>
 <artifactId>fastjson</artifactId>
 <version>1.2.58</version>
</dependency>
```

防护建议

Web应用防火墙的Web攻击防护规则中已默认配置相应规则防护该FastJSON 0day漏洞，启用Web应用防火墙的Web应用攻击防护功能即可。

说明:

如果您的业务使用*#unique_6*功能自定义所应用的防护规则，请务必在自定义规则组中添加以下规则：

规则	规则ID	危险等级	应用类型	防护类型	规则描述
Fastjson远程代码执行0day漏洞	113164	高危	Fastjson	代码执行	此规则阻止利用Fastjson远程代码执行0da...
Apache axis远程代码执行	113163	高危	其它	代码执行	此规则组织利用Apache axis存在远程代码...
CoreMail未授权访问接口参数注入	115097	高危	其它	本地文件包含	此规则组织利用CoreMail未授权访问接口参...

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

1.3 Consul Service API远程命令执行漏洞

2018年11月27日，Consul在官方博客中发布了关于Consul工具在特定配置下可能导致远程命令执行（RCE）漏洞的公告，并描述了防护该漏洞的配置方案。

Consul是HashiCorp公司推出的一款开源工具，用于实现分布式系统的服务发现与配置。与其他分布式服务注册与发现的方案相比，Consul提供的方案更为“一站式”。Consul内置了服务注册与发现框架、分布一致性协议实现、健康检查、Key/Value存储、多数据中心方案，不再需要依赖其他工具（例如ZooKeeper等），使用方式也相对简单。

Consul使用Go语言编写，因此具有天然的可移植性（支持Linux、Windows和Mac OS X系统）；且安装包中仅包含一个可执行文件，便于部署，可与Docker等轻量级容器无缝配合。

漏洞名称

Hashicorp Consul Service API远程命令执行漏洞

漏洞描述

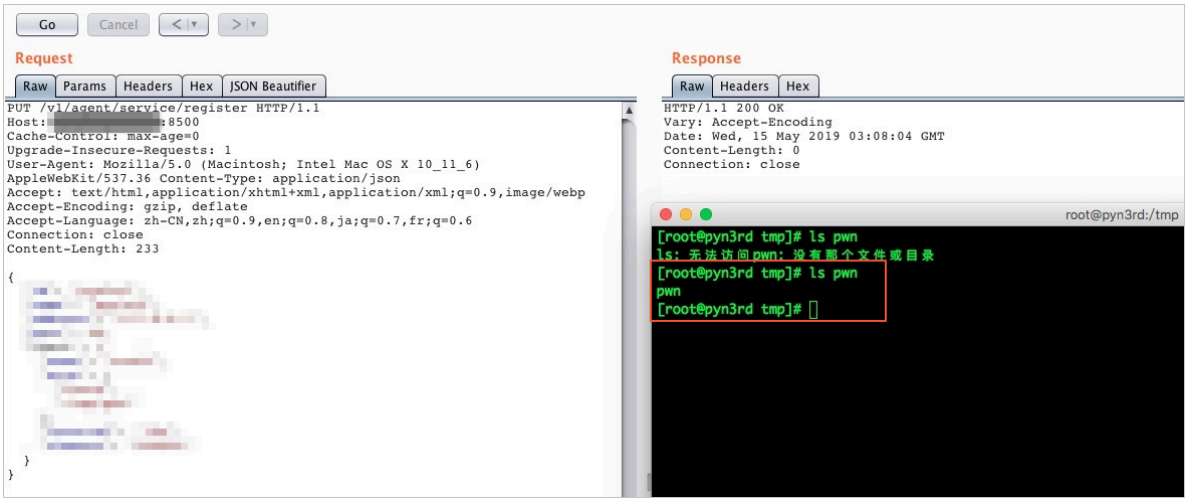
在特定配置下，恶意攻击者可以通过发送精心构造的HTTP请求在未经授权的情况下在Consul服务端远程执行命令。关于该Consul漏洞的更多详细信息，请查看*HashiCorp*官方公告。

漏洞复现过程

1. 验证Consul服务端存在该远程命令执行漏洞。


不安全
[redacted]:8500/v1/agent/self
- DNSAddrs: [
"tcp://0.0.0.0:8600",
"udp://0.0.0.0:8600"
],
DNSAllowStale: true,
DNSCacheMaxAge: "0s",
DNSDisableCompression: false,
DNSDomain: "consul.",
DNSEnableTruncate: false,
DNSMaxStale: "87600h0m0s",
DNSNodeMetaTXT: true,
DNSNodeTTL: "0s",
DNSOnlyPassing: false,
DNSPort: 8600,
DNSRecursorTimeout: "2s",
DNSRecursors: [ ],
- DNSSOA: {
Expire: 86400,
Minttl: 0,
Refresh: 3600,
Retry: 600
},
DNSServiceTTL: { },
DNSUDPAnswerLimit: 3,
DNSUseCache: false,
DataDir: "",
Datacenter: "dc1",
DevMode: true,
DisableAnonymousSignature: true,
DisableCoordinates: false,
DisableHTTPUnprintableCharFilter: false,
DisableHostNodeID: true,
DisableKeyringFile: true,
DisableRemoteExec: true,
DisableUpdateCheck: false,
DiscardCheckOutput: false,
DiscoveryMaxStale: "0s",
EnableAgentTLSForChecks: false,
EnableDebug: true,
EnableLocalScriptChecks: true,
EnableRemoteScriptChecks: true,
EnableSyslog: false,
EnableUI: true,
EncryptKey: "hidden",
EncryptVerifyIncoming: true,
EncryptVerifyOutgoing: true,
- GRPCAddrs: [
"tcp://0.0.0.0:8502"
],

2. 构造HTTP PUT请求，实现在Consul服务端远程执行命令。



影响范围

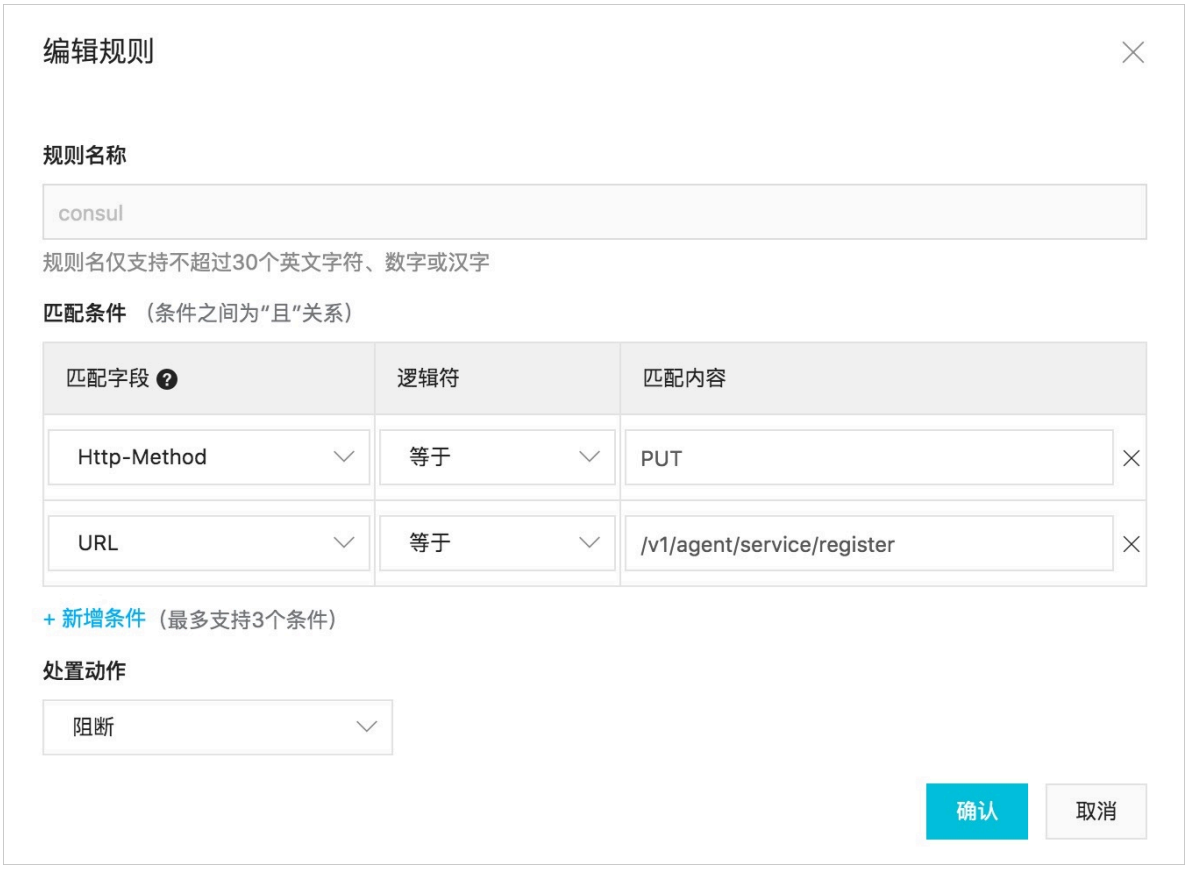
启用了脚本检查参数（`-enable-script-checks`）的所有版本。

防护建议

您可以通过选择以下适合的方案防护该Consul漏洞：

- **禁用Consul服务器上的脚本检查功能。**
- **如果您需要使用Consul的脚本检查功能，请升级至0.9.4、1.0.8、1.1.1、1.2.4中的一个版本（这些版本中包含`-enable-local-script-checks`参数），将Consul配置中的`-enable-script-checks`更改为`-enable-local-script-checks`。**
- **确保Consul HTTP API服务无法通过外网访问或调用。**

- **启用Web应用防火墙的精准访问控制功能，配置以下防护规则。**



更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

1.4 Apache Solr远程反序列化代码执行漏洞（CVE-2019-0192）

2019年3月7日，阿里云云盾应急响应中心监测到Apache官方发布的关于Solr的安全公告。通过调用Config API修改jmx.serviceUrl属性指向恶意的RMI服务，导致Apache Solr出现远程反序列化代码执行的安全漏洞。

漏洞编号

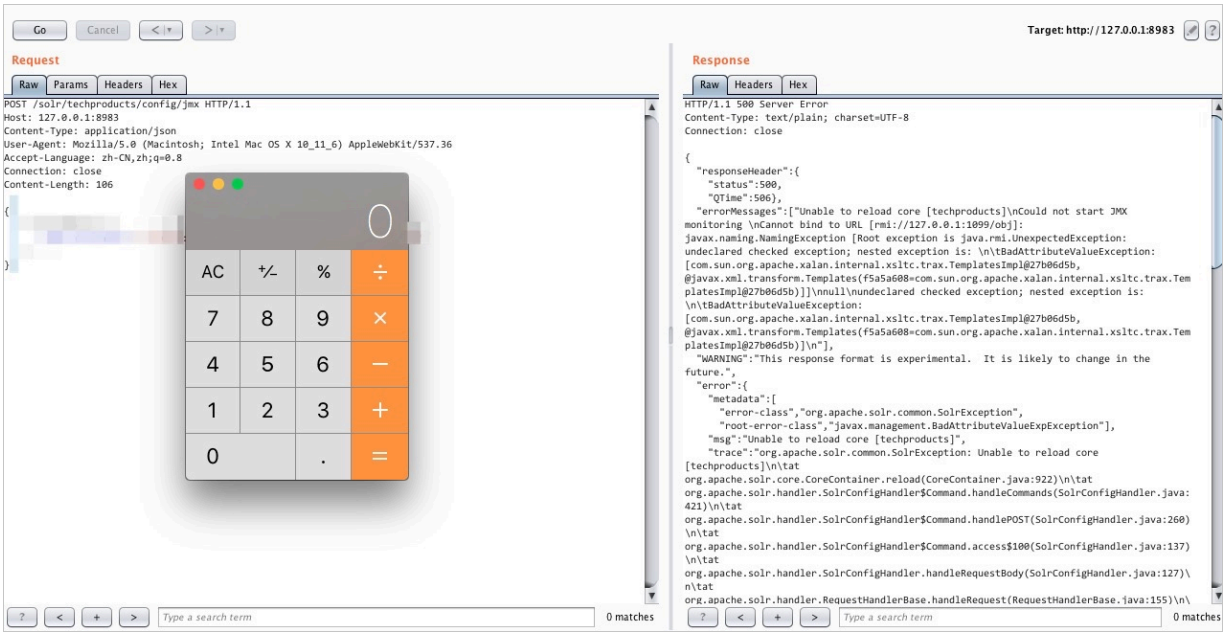
CVE-2019-0192

漏洞名称

Apache Solr jmx.serviceUrl远程反序列化代码执行漏洞

漏洞描述

Config API接口允许通过发送HTTP POST请求配置Apache Solr的JMX服务器，修改jmx.serviceUrl的属性。恶意攻击者通过将其指向恶意的RMI服务器，可以利用Solr的不安全的反序列化触发远程代码执行。



影响范围

- **Apache Solr 5.00至5.5.5版本**
- **Apache Solr 6.00至6.6.5版本**

官方解决方案

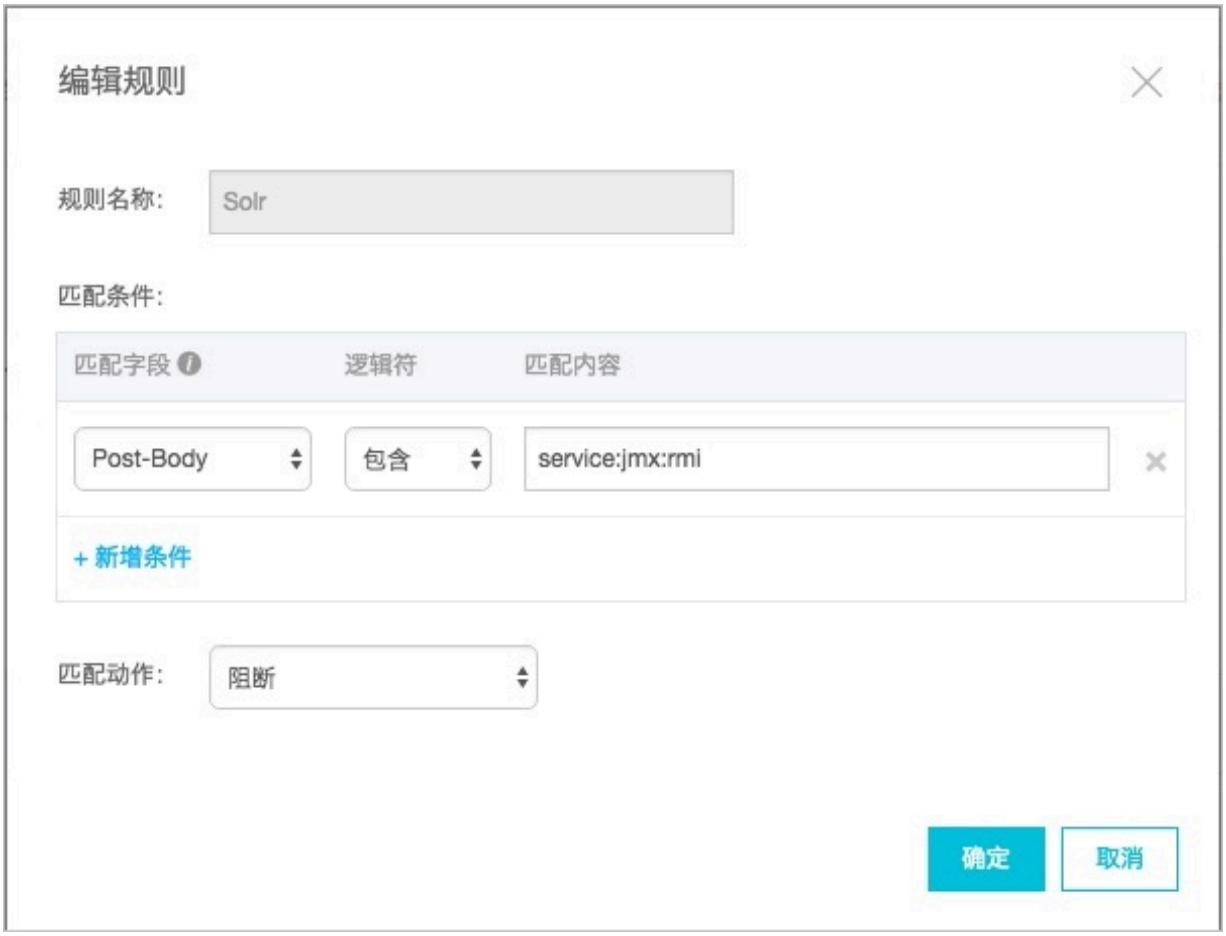
- **将您的Apache Solr升级至7.0或以上版本。**
- **通过修改配置`disable.configEdit=true`，禁用Config API接口。**
- **在网络层确保仅放行受信任的流量访问Solr服务器。**

如果升级版本或禁用Config API都不可行，请申请官方补丁并重新编译Solr。

防护建议

如果您暂时不希望通过升级Solr版本解决该漏洞，建议您使用Web应用防火墙的精准访问控制功能对您的业务进行防护。

通过精准访问控制功能，限制包含特定JSON数据（service:jmx:rmi）的POST请求，拦截利用该漏洞发起的远程代码执行攻击请求。



更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

1.5 Jenkins任意文件读取漏洞（CVE-2018-1999002）

2018年7月18日（美国时间），Jenkins官方发布最新安全通告，披露多个安全漏洞。其中，SECURITY-914是由*Orange*发现的Jenkins未授权任意文件读取漏洞，存在高危风险。

利用该漏洞，攻击者可以读取Windows系统服务器中的任意文件，且在特定而条件下也可以读取Linux系统服务器中的文件。通过利用该文件读取漏洞，攻击者可以获取Jenkins系统的凭证信息，导致用户的敏感信息遭到泄露。同时，Jenkins的部分凭证可能与其用户的帐号密码相同，攻击者获取到凭证信息后甚至可以直接登录Jenkins系统进行命令执行操作等。

漏洞编号

CVE-2018-1999002

漏洞名称

Jenkins任意文件读取漏洞

漏洞描述

在Jenkins的Stapler Web框架中存在任意文件读取漏洞。恶意攻击者可以通过发送精心构造的HTTP请求在未经授权的情况下获取Jenkin主进程可以访问的Jenkins文件系统中的任意文件内容。

关于该漏洞更多信息，请查看官方漏洞公告。

影响范围

- **Jenkins weekly 2.132及此前所有版本**
- **Jenkins LTS 2.121.1及此前所有版本**

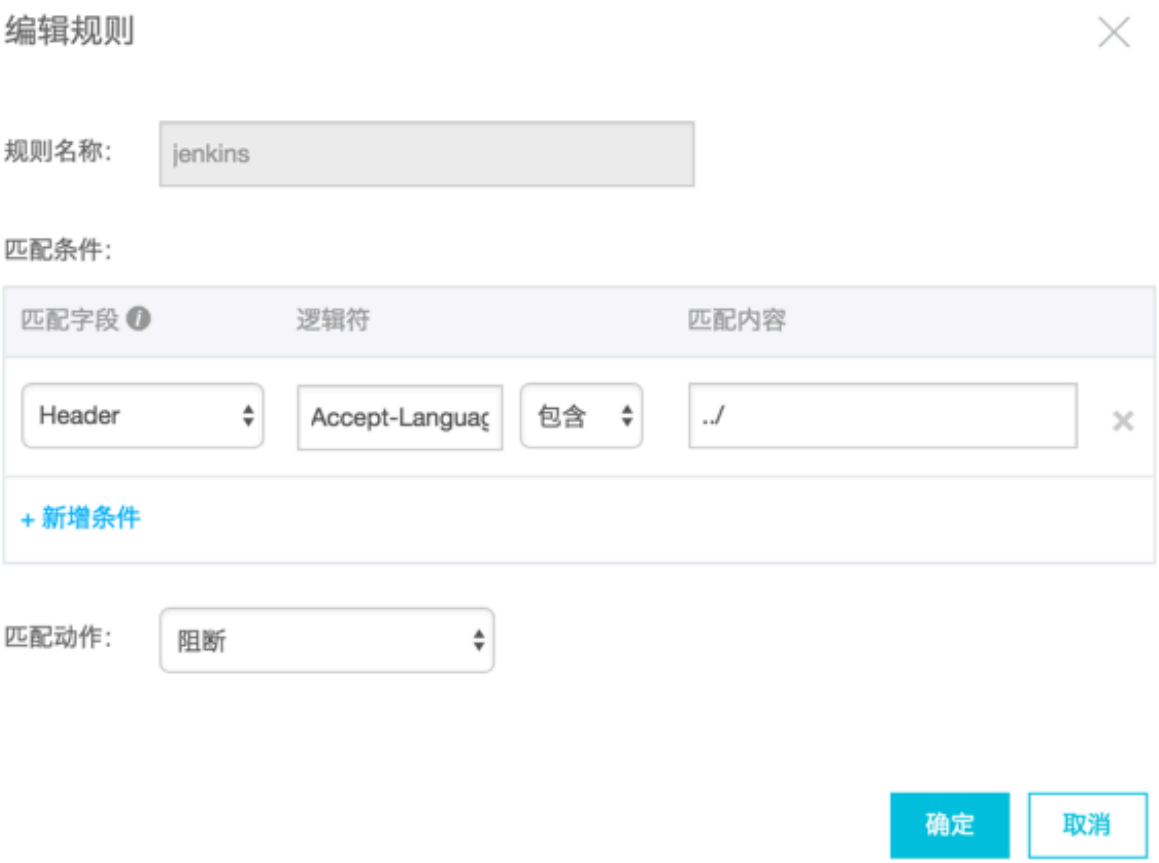
官方解决方案

- **将您的Jenkins weekly升级至2.133版本。**
- **将您的Jenkins LTS升级至2.121.2版本。**

防护建议

如果您暂时不希望通过升级Jenkins版本解决该漏洞，建议您使用Web应用防火墙的精准访问控制功能对您的业务进行防护。

通过精准访问控制功能，针对Accept-Language这个HTTP请求头设置阻断规则过滤该请求头中包含`../`的请求，防止攻击者利用该漏洞通过目录穿越读取任意文件。



实际防护效果

通过配置上述精准访问控制规则，WAF成功阻断试图利用该漏洞的精心构造的HTTP请求。

说明:

关于精准访问控制规则的功能介绍，请查看精准访问控制。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

1.6 Apache Struts2 REST插件DoS漏洞（CVE-2018-1327）防护最佳实践

HPE的两名安全专家（Yevgeniy Grushka和Alvaro Munoz）发现Apache Strust2的REST插件中存在DoS漏洞。如果您在Struts REST插件中使用XStream类库处理程序，攻击者可以构造恶意的XML请求发起DoS攻击。

漏洞编号

CVE-2018-1327

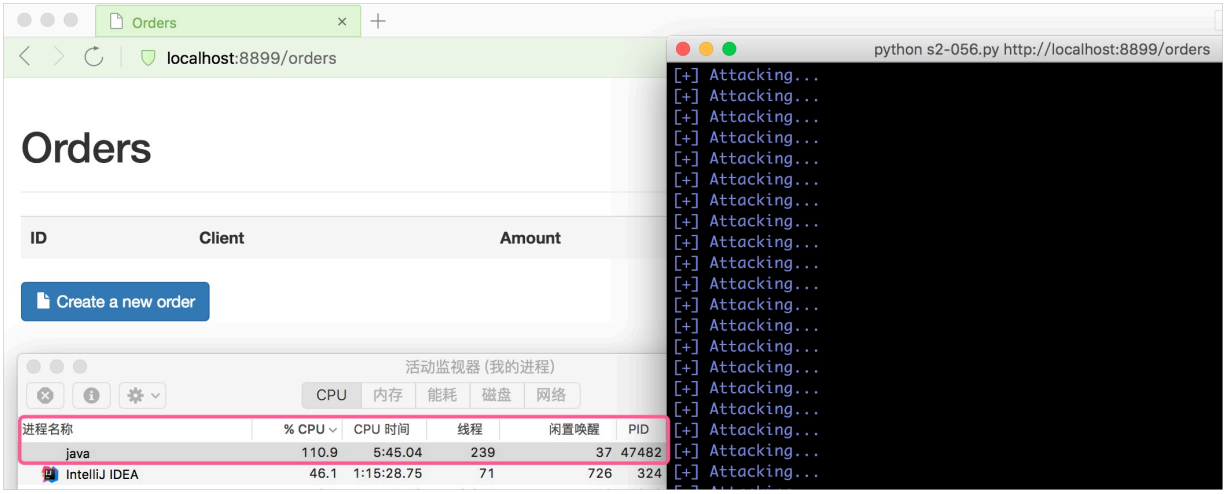
漏洞名称

Apache Struts2 REST插件DoS漏洞（S2-056）

漏洞描述

S2-056漏洞存在于Apache Struts2的REST插件中。当使用XStream组件对XML格式的数据包进行反序列化操作，且未对数据内容进行有效验证时，攻击者可通过提交恶意的XML数据对应用发起远程DoS攻击。

当恶意攻击者发起大量攻击请求时，您的应用所在服务器的CPU资源将被迅速占满。



关于该漏洞更多信息，请查看官方漏洞公告。

影响范围

Struts 2.1.1 - Struts 2.5.14.1

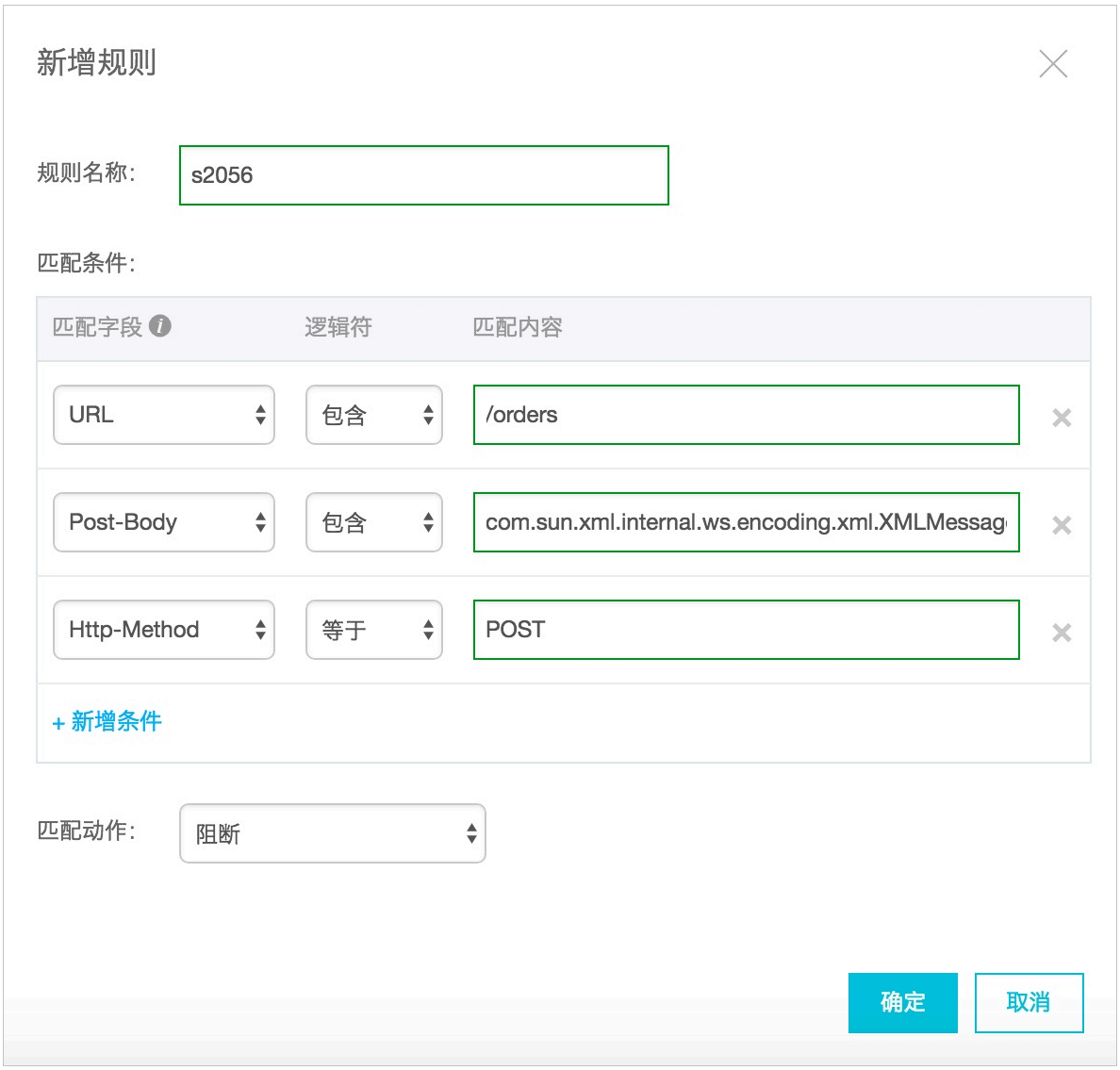
官方解决方案

将您的Apache Struts升级至2.5.16版本。

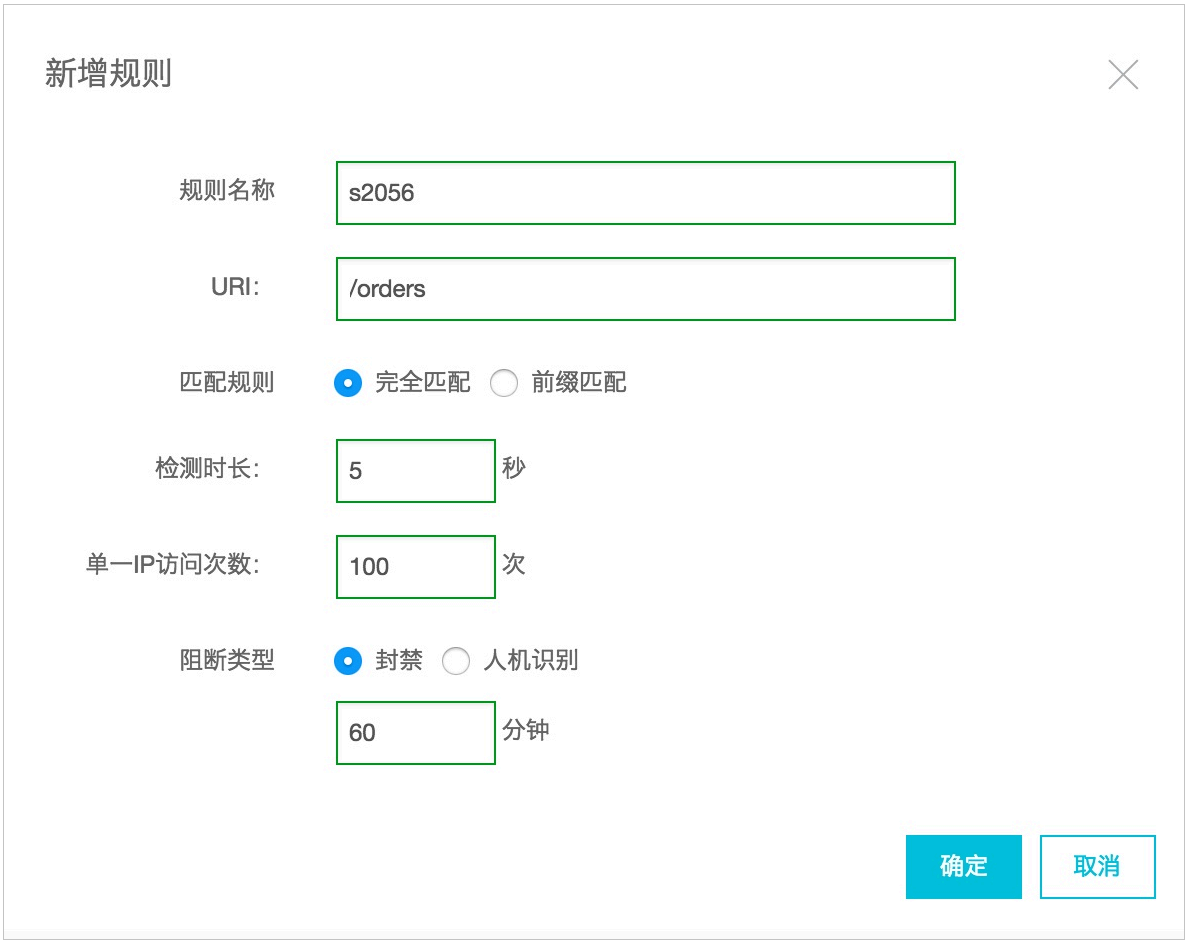
防护建议

如果您暂时不希望通过升级Apache Struts版本解决该漏洞，建议您使用Web应用防火墙的精准访问控制和CC攻击自定义规则功能对您的业务进行防护。

- **通过精准访问控制功能，限制包含特定XML数据（`com.sun.xml.internal.ws.encoding.xml.XMLMessage$XmlDataSource`）的POST请求，阻断利用该漏洞发起的DoS攻击请求。例如，配置以下规则阻断在Apache Strust的REST插件中使用XStream类库应用页面的攻击请求。**



- **通过CC攻击防护自定义功能，限制同一个IP对在Apache Strust的REST插件中使用XStream类库的应用页面的请求频率。例如，配置以下规则限制对指定页面的请求频率不超过每5秒100次。**



关于精准访问控制和CC攻击防护自定义规则的功能介绍，请查看精准访问控制和自定义CC防护。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

1.7 WordPress拒绝服务（CVE-2018-6389）漏洞防护最佳实践

2018年2月5日，国外安全研究人员披露了一个关于Wordpress的拒绝服务（DoS）攻击的漏洞（CVE-2018-6389），WordPress 3.x-4.x各个版本均受该漏洞影响。恶意攻击者可以通过让WordPress在单个请求中加载多个Javascript文件来消耗服务器资源，进而引发拒绝服务。

云盾WAF本身不受该漏洞影响。但如果您的网站业务使用WordPress，建议您配置相应的防护规则。

漏洞描述

该漏洞主要位于*load-scripts.php*文件处，*load-scripts.php*是WordPress CMS的内置脚本。*load-scripts.php*文件通过传递`name`到`load`参数来选择性地调用必需的Javascript文件，这些`name`参数间以”,”隔开。

例如，`https://example.com/wp-admin/load-scripts.php?c=1&load[]=jquery-ui-core,editor&ver=4.9.1`**，这个请求中加载的Javascript文件是*jquery-ui-core*和*editor*。**

由于在*script-loader.php*文件中定义的181个Javascript文件都可以被加载在单个请求中，恶意攻击者在无需授权登录的情况下可以发送大量请求，导致服务器负载增加，从而实现拒绝服务攻击的效果。

防护建议

建议您使用精准访问控制和CC攻击自定义规则功能对您的WordPress网站业务进行防护。

- **通过精准访问控制功能，限制向*load-scripts.php*文件传递参数的数量。例如，配置以下规则限制对*load-scripts.php*文件传递的参数长度不大于50个字符。**

- 通过CC攻击防护自定义功能，限制同一个IP对*load-scripts.php*文件的请求频率。例如，配置以下规则限制对同一个IP对*load-scripts.php*文件的请求频率不超过每5秒100次。

关于精准访问控制和CC攻击防护自定义规则的功能介绍，请查看精准访问控制和自定义CC防护。

更多信息

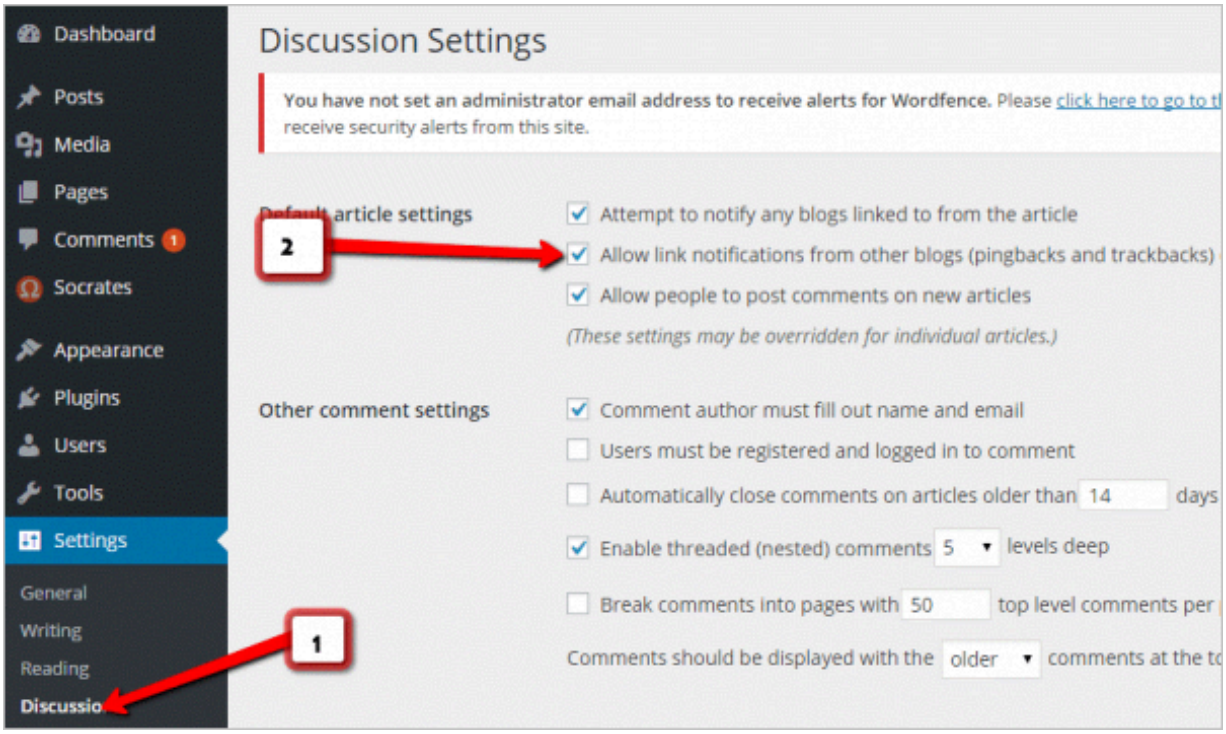
安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击，详情请关注安全管家服务。

1.8 WordPress xmlrpc PingBack反射攻击防护最佳实践

本文用于在遭受WordPress反射攻击时，通过Web应用防火墙防御WordPress反射攻击。

什么是WordPress反射攻击

WordPress是一种使用PHP语言开发的博客平台，pingback是WordPress的一个插件。黑客可以利用pingback对网站发起WordPress反射攻击。



在遭受WordPress攻击后，您可以在服务器日志上看到大量User-Agent中包含WordPress、pingback字样的请求。

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反射攻击是CC攻击的变种，可以造成网页加载极其缓慢、服务器CPU飙升、失去响应等情况。

关于攻击的原理，请参见*WordPress*反弹攻击那点事儿。

如何使用Web应用防火墙进行防御

1. 登录云盾Web应用防火墙控制台。
2. 前往管理 > 网站配置页面。
3. 选择需要防护的域名，单击其操作列下的防护配置。
4. 在精准访问控制下，单击前去配置。
5. 单击新增规则，分别添加以下两条精准访问控制规则。
   - 阻断User-Agent中包含pingback的访问。
     - 规则名称：wp1
     - 匹配字段：User-Agent
     - 逻辑符：包含
     - 匹配内容：pingback
     - 匹配动作：阻断
   - 阻断User-Agent中包含WordPress的访问。
     - 规则名称：wp2
     - 匹配字段：User-Agent
     - 逻辑符：包含
     - 匹配内容：WordPress
     - 匹配动作：阻断

> **说明:**
> 两条规则要分开添加。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效的应对漏洞及黑客攻击，详情请关注安全管家服务。

2 监控与告警最佳实践

2.1 设置Web应用防火墙报警规则

本实践介绍了使用阿里云云监控配置Web应用防火墙报警通知的操作方法。通过设置Web应用防火墙报警通知，您可以及时获知Web应用防火墙实例上的流量、连接数、攻击等异常情况，并在发生故障时第一时间发现问题，缩短故障处理时间，以便尽快恢复业务。

背景信息

云监控（CloudMonitor）是一项针对阿里云资源和互联网应用进行监控的服务。云监控为您提供监控数据的报警功能。您可以通过设置报警规则来定义报警系统如何检查监控数据，并在监控数据满足报警条件时发送报警通知。您对重要监控指标设置报警规则后，便可在第一时间得知指标数据发生的异常，迅速处理故障。

云监控报警功能兼容Web应用防火墙，您可以在云监控中配置Web应用防火墙的报警通知规则。云监控支持监控以下Web应用防火墙的数据指标。

表 2-1: Web应用防火墙监控指标

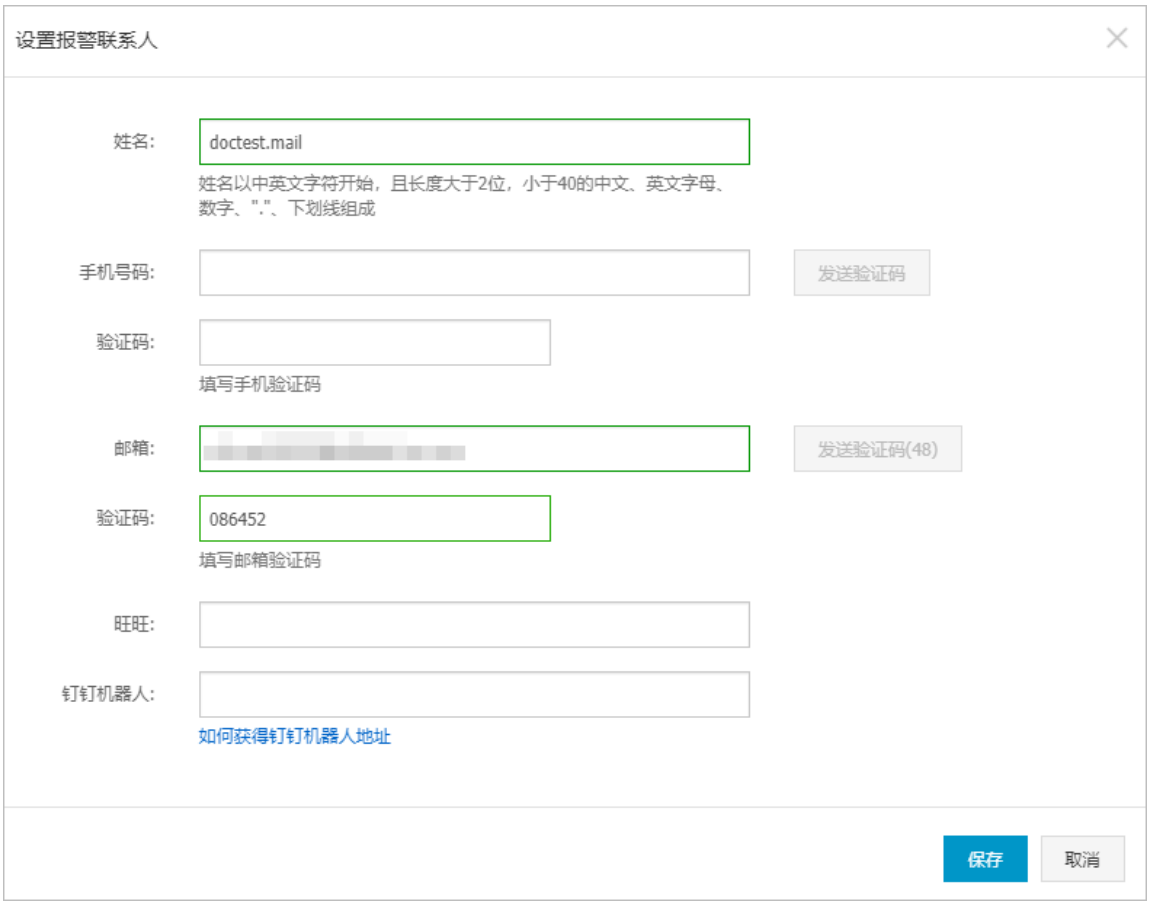
监控项	维度	单位	指标含义	备注
4XX占比	域名	%	每分钟4XX状态码的占比（不包含405）	报警信息以小数形式呈现
5XX占比	域名	%	每分钟5XX状态码的占比	报警信息以小数形式呈现
访问控制拦截量（5m）	域名	个	近5分钟内精准访问控制拦截量	无
访问控制拦截占比（5m）	域名	%	近5分钟内精准访问控制拦截占总请求量的占比	报警信息以小数形式呈现
CC防护拦截量（5m）	域名	个	近5分钟内CC安全防护拦截量	无
CC防护拦截占比（5m）	域名	%	近5分钟内CC安全防护拦截占总请求量的占比	报警信息以小数形式呈现
Web攻击拦截量（5m）	域名	个	近5分钟内Web应用攻击防护拦截量	无
Web攻击拦截占比（5m）	域名	%	近5分钟内Web应用攻击防护拦截占总请求量的占比	报警信息以小数形式呈现
QPS	域名	个/秒	QPS	无

监控项	维度	单位	指标含义	备注
QPS环比增长率	域名	%	每分钟QPS的环比增长率	报警信息以百分比形式呈现
QPS环比下降率	域名	%	每分钟QPS的环比下降率	报警信息以百分比形式呈现

操作步骤

1. 登录阿里云云监控控制台。
2. （可选）创建报警联系人。若已有联系人，请跳过此步骤。
   a) 在左侧导航栏，单击报警服务 > 报警联系人。
   b) 在报警联系人页签下，单击新建联系人。

   c) 在设置报警联系人对话框中，填写联系人信息，通过手机号码或者邮箱完成验证后，单击保存。



   成功新建报警联系人。

3. （可选）创建报警联系组。若已有联系人组，请跳过此步骤。

> **说明:**
> 报警通知的接收对象必须是联系人组，您可以在联系人组中添加一个或多个联系人。

a) 在报警联系组页签下，单击新建联系组。

b) 在新建联系组对话框中，设置组名，从已有联系人中选择并添加联系人到当前组，单击确定。

成功新建报警联系组。

4. 创建报警规则。

a) 在左侧导航栏，单击报警服务 > 报警规则。

b) 在阈值报警页签下，单击创建报警规则。

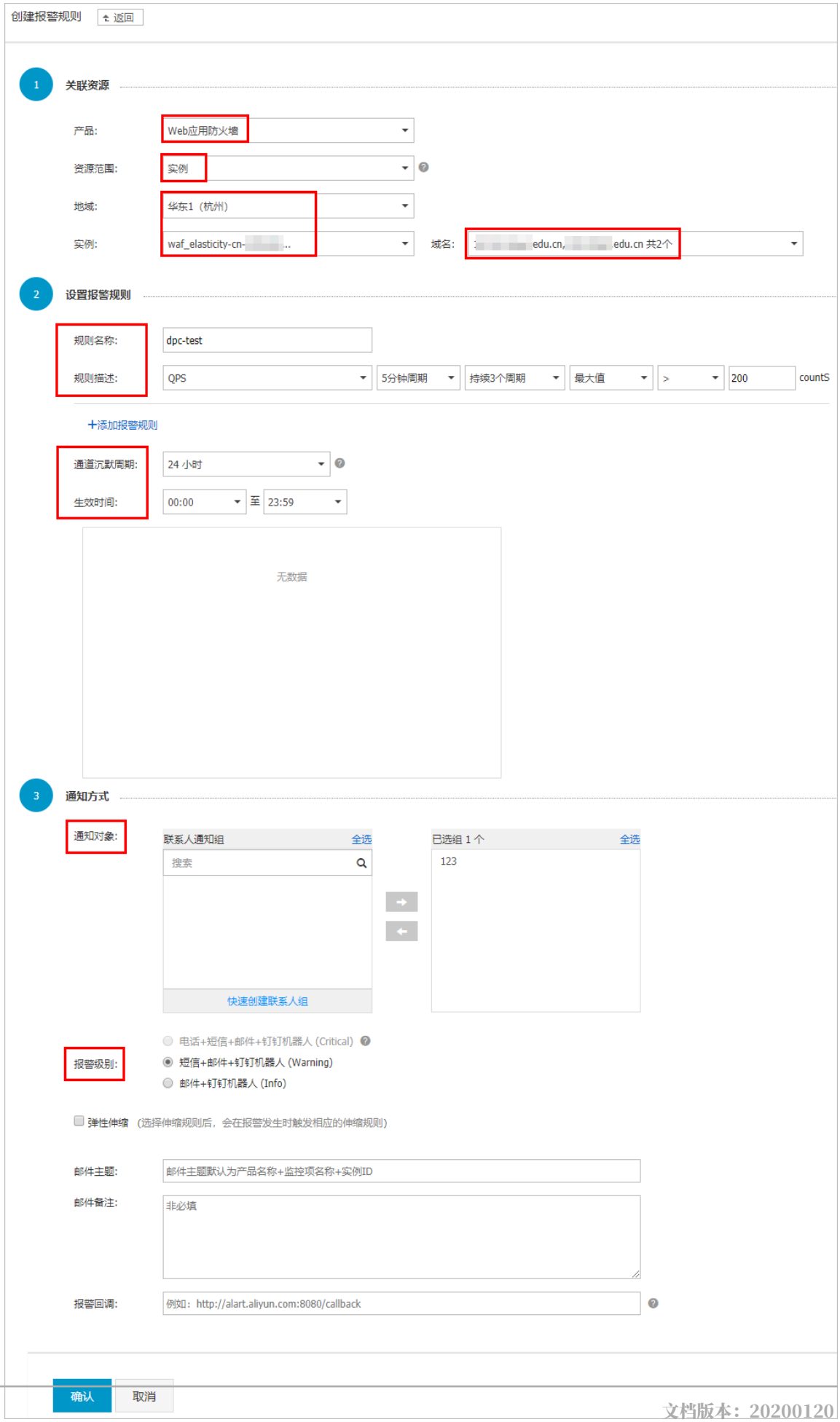
c) 在创建报警规则页面，完成报警规则配置，并单击确认。报警规则的配置描述如下。

类别	配置项	说明
关联资源	产品	选择Web应用防火墙。
	资源范围	报警规则的作用范围，分为全部资源、实例。 · 全部资源：资源范围选择全部资源，则所有Web应用防火墙实例满足报警规则描述时，都会发送报警通知。 · 实例：资源范围选择指定的实例，则选中的Web应用防火墙实例满足报警规则描述时，才会发送报警通知。
	地域	仅在资源范围为实例时配置。选择Web应用防火墙实例的地域。 · 中国大陆的实例，选择华东1（杭州） · 海外地区的实例，选择新加坡
	实例	仅在资源范围为实例时配置。选择地域后，默认选择当前地域下的Web应用防火墙实例。
	域名	仅在资源范围为实例时配置。从已接入当前实例防护的域名中选择需要监控的域名，支持多选。
设置报警规则	规则名称	报警规则的名称。

类别	配置项	说明
	规则描述	报警规则的主体，定义在监控数据满足何种条件时，触发报警规则。 **说明:** 建议您根据实际业务情况设置各项监控指标（参见表 2-1: Web应用防火墙监控指标）的报警阈值。阈值太低会频繁触发报警，影响监控服务体验。阈值太高，在触发阈值后没有足够的预留时间来响应和处理攻击。 报警规则举例说明： QPS 5分钟周期连续3周期最大值>200个， 含义是报警服务会探测任意连续3周期的QPS数据（单个Web应用防火墙监控指标60秒上报一个数据点，5分钟有5个数据点，连续3周期有15个数据点），只要QPS最大值大于200个，结果就符合报警规则，发送报警通知。  单击添加报警规则，可以添加多个规则，每个规则单独设置规则名称和规则描述。
	通道沉默时间	报警发生后如果未恢复正常，间隔多久重复发送一次报警通知。最短为5分钟，最长为24小时。
	生效时间	报警规则的生效时间，报警规则只在生效时间内发送报警通知，非生效时间内产生的报警只记录报警历史。
通知方式	通知对象	接收报警通知的联系人组。
	报警级别	分为Critical 、Warning、Info三个级别，不同级别对应不同的通知方式。 · 电话+短信+邮件+钉钉机器人（Critical） **说明:** 购买云监控电话报警资源包后才可以选择。 · 短信+邮件+钉钉机器人（Warning） · 邮件+钉钉机器人（Info）

类别	配置项	说明
	弹性伸缩	选择弹性伸缩规则后，会在报警发生时触发相应的弹性伸缩规则。无需勾选。
	邮件备注	自定义报警邮件补充信息，非必填。填写邮件备注后，发送报警的邮件通知中会附带您的备注。

类别	配置项	说明
	报警回调	云监控会将报警信息通过POST请求推送到您填写的公网URL地址，目前仅支持HTTP协议。


创建报警规则
返回
1
关联资源
产品:
Web应用防火墙
资源范围:
实例
地域:
华东1（杭州）
实例:
waf_elasticity-cn-
域名:
edu.cn, edu.cn 共2个
2
设置报警规则
规则名称:
dpc-test
规则描述:
QPS
5分钟周期
持续3个周期
最大值
>
200
countS
+添加报警规则
通道沉默周期:
24 小时
生效时间:
00:00
至
23:59
无数据
3
通知方式
通知对象:
联系人通知组
全选
搜索
快速创建联系人组
已选组 1 个
全选
123
报警级别:
电话+短信+邮件+钉钉机器人（Critical）
短信+邮件+钉钉机器人（Warning）
邮件+钉钉机器人（Info）
弹性伸缩 （选择伸缩规则后，会在报警发生时触发相应的伸缩规则）
邮件主题:
邮件主题默认为产品名称+监控项名称+实例ID
邮件备注:
非必填
报警回调:
例如：http://alart.aliyun.com:8080/callback
确认
取消

成功创建Web应用防火墙报警规则。当Web应用防火墙监控指标满足报警条件时，报警规则中指定的联系人组会收到报警通知 。

2.2 设置Web应用防火墙事件监控

本实践介绍了使用阿里云云监控配置Web应用防火墙事件报警通知的操作方法。通过为Web应用防火墙配置事件监控，您能够及时获知已接入Web应用防火墙防护的域名上发生的访问控制、CC攻击、Web攻击、防扫描事件，并在发生故障时第一时间发现问题，缩短故障处理时间，以便尽快恢复业务。

背景信息

云监控（CloudMonitor） 是一项针对阿里云资源和互联网应用进行监控的服务。云监控支持事件监控功能，为您提供各类云产品产生的系统事件的统一查询和统计入口，使您明确知晓云产品的使用状态，让云更透明。

您可以通过事件监控查询Web应用防火墙上域名发生的访问控制、CC攻击、Web攻击和防扫描事件，并为Web应用防火墙添加事件的报警通知。事件监控支持根据事件等级配置报警，通过短信、邮件、钉钉等接收通知或设置报警回调，使您第一时间知晓严重事件并及时进行处理，形成线上自动化运维闭环。更多信息，请参见事件监控概览。

云监控支持监控以下Web应用防火墙事件。

表 2-2: Web应用防火墙事件监控类型

事件名称	含义	类型	状态取值	事件等级
waf_event_aclattack	访问控制事件	acl	start/end	CRITICAL
waf_event_ccattack	CC攻击事件	cc	start/end	CRITICAL
waf_event_webattack	Web攻击事件	web	start/end	CRITICAL
waf_event_webscan	防扫描事件	webscan	start/end	CRITICAL

操作步骤

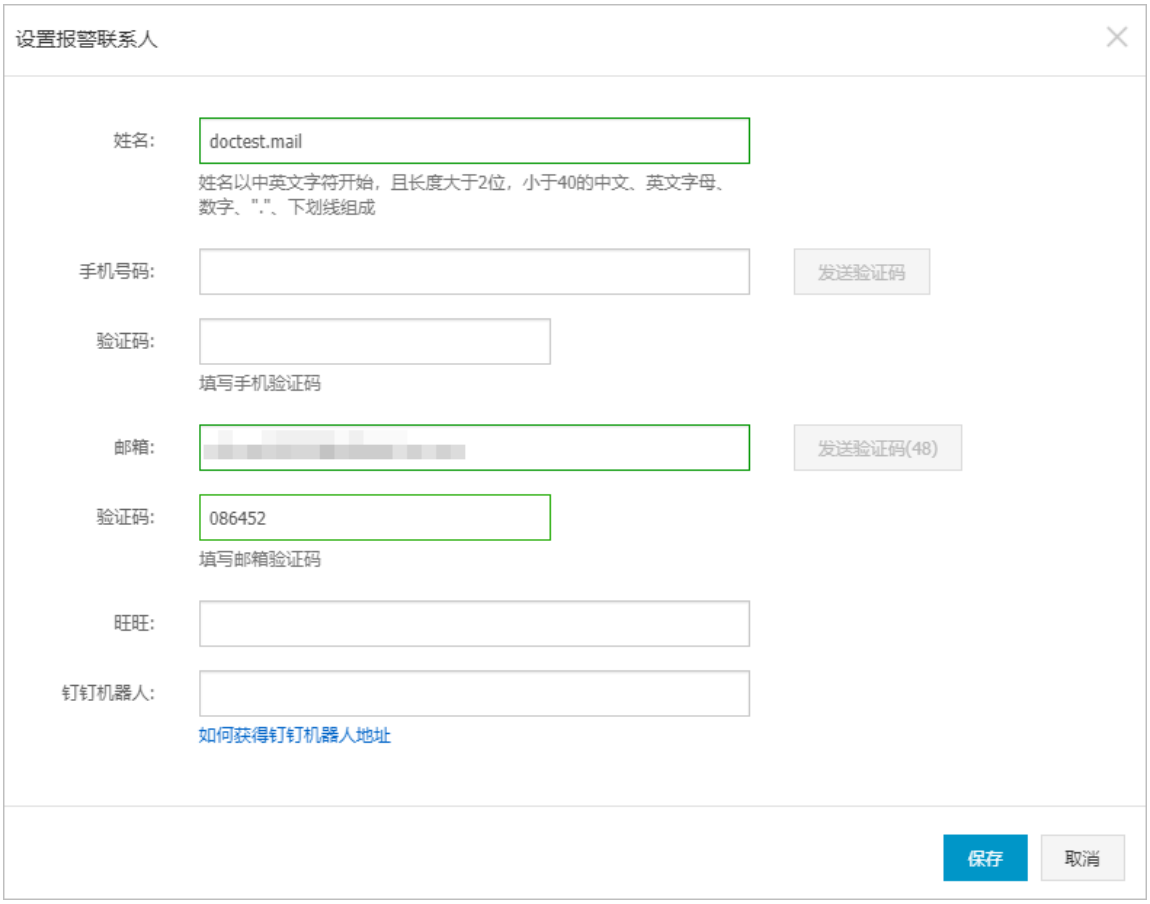
1. 登录阿里云云监控控制台。

2. （可选） 创建报警联系人。若已有联系人，请跳过此步骤。

   a) 在左侧导航栏，单击报警服务 > 报警联系人。

   b) 在报警联系人页签下，单击新建联系人。

   c) 在设置报警联系人对话框中，填写联系人信息，通过手机号码或者邮箱完成验证后，单击保存。



   成功新建报警联系人。

3. （可选） 创建报警联系组。若已有联系人组，请跳过此步骤。

说明:

报警通知的接收对象必须是联系人组，您可以在联系人组中添加一个或多个联系人。

a) 在报警联系组页签下，单击新建联系组。

b) 在新建联系组对话框中，设置组名，从已有联系人中选择并添加联系人到当前组，单击确定。

成功新建报警联系组。

4. 创建云产品事件报警规则。

a) 在左侧导航栏，单击事件监控。

b) 在报警规则页签下，选择系统事件，并单击创建事件报警。

c) 在创建/修改事件报警侧边页，完成报警配置，并单击确定。报警配置的描述如下。

类型	配置项	说明
基本信息	报警规则名称	为报警规则命名。
事件报警规则	事件类型	选择系统事件。
	产品类型	选择Web应用防火墙。
	事件类型	选择WAF攻击事件。
	事件等级	选择要通知的事件等级，支持严重、警告、信息。可以多选，且必须包含严重等级。
	事件名称	选择要通知的事件，可选值： · 访问控制事件 · CC攻击事件 · Web攻击事件 · 防扫描事件 可以多选。 事件等级均为严重。
	资源范围	选择全部资源。
报警方式	报警通知	勾选报警通知，并设置联系人组和通知方式。 · 联系人组：选择一个已有联系人组。 · 通知方式：选择Warning（短息+邮箱+钉钉机器人）或者Info（邮箱+钉钉机器人）方式。 若单击添加操作，可以设置多个联系人组和通知方式。
	消息服务队列	无需勾选。
	函数计算	无需勾选。
	URL回调	无需勾选。

类型	配置项	说明
	日志服务	无需勾选。


创建/修改事件报警
基本信息
报警规则名称
waf_event
事件报警规则
事件类型
系统事件
自定义事件
产品类型
Web应用防火墙
事件类型
WAF攻击事件
事件等级
严重
警告
信息
事件名称
访问控制事件
CC攻击事件
Web攻击事件
资源范围
全部资源
应用分组
报警方式
报警通知
联系人组
删除
123
通知方式
Warning (短信+邮箱+钉钉机器人)
+添加操作
消息服务队列
函数计算 (最佳实践)
URL回调
日志服务
确定
取消

成功创建Web应用防火墙事件监控报警规则。当已接入Web应用防火墙的域名上发生指定的事件时，报警规则中指定的联系人组会收到报警通知 。

5. （可选） 查询事件。您也可以在云监控查询近期发生的Web应用防火墙事件。

a) 前往事件监控页面，并打开事件查询页签。

b) 选择系统事件和Web应用防火墙产品，并设置要查询的事件类型和时间范围，查询相关历史事件。

c) 在历史事件记录中，您可以单击事件后的查看详情，展开事件详情。

2.3 创建Web应用防火墙监控大盘

本实践介绍了使用阿里云云监控创建和自定义Web应用防火墙实时监控大盘和数据图表的操作方法。自定义Web应用防火墙监控大盘和数据图表能够帮助您直观、全面地了解Web应用防火墙的业务防护情况。

背景信息

云监控（CloudMonitor） 是一项针对阿里云资源和互联网应用进行监控的服务。云监控的Dashboard功能为您提供自定义查看监控数据的功能。您可以在一张监控大盘中跨产品、跨实例查看监控数据，将相同业务的不同产品实例集中展现。

云监控Dashboard功能兼容Web应用防火墙，您可以在云监控中配置Web应用防火墙监控大盘。云监控支持监控以下Web应用防火墙的数据指标。

表 2-3: Web应用防火墙监控指标

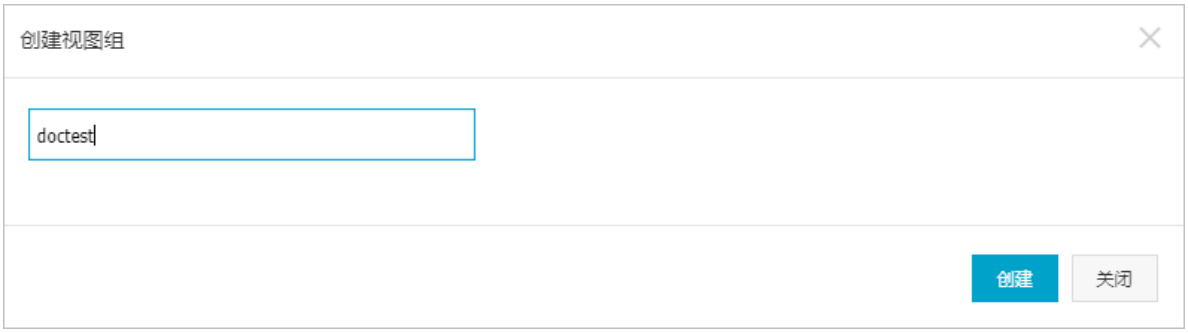
监控项	维度	单位	指标含义	备注
4XX占比	域名	%	每分钟4XX状态码的占比（不包含405）	数据以小数形式呈现
5XX占比	域名	%	每分钟5XX状态码的占比	数据以小数形式呈现

监控项	维度	单位	指标含义	备注
访问控制拦截量（5m）	域名	个	近5分钟内精准访问控制拦截量	无
访问控制拦截占比（5m）	域名	%	近5分钟内精准访问控制拦截占总请求量的占比	数据以小数形式呈现
CC防护拦截量（5m）	域名	个	近5分钟内CC安全防护拦截量	无
CC防护拦截占比（5m）	域名	%	近5分钟内CC安全防护拦截占总请求量的占比	数据以小数形式呈现
Web攻击拦截量（5m）	域名	个	近5分钟内Web应用攻击防护拦截量	无
Web攻击拦截占比（5m）	域名	%	近5分钟内Web应用攻击防护拦截占总请求量的占比	数据以小数形式呈现
QPS	域名	个/秒	QPS	无
QPS环比增长率	域名	%	每分钟QPS的环比增长率	数据以百分比形式呈现
QPS环比下降率	域名	%	每分钟QPS的环比下降率	数据以百分比形式呈现

操作步骤

1. 登录阿里云云监控控制台。
2. 前往Dashboard > 自定义大盘页面，单击创建监控大盘。

3. 在创建视图组对话框中设置大盘名称，单击创建。



成功添加监控大盘，页面跳转到新建的监控大盘。您可以通过当前监控大盘选项切换要查看或操作的监控大盘。

4. 进入监控大盘，单击添加图表，并在添加图表侧边页中自定义图表内容。

   a) 选择图表类型。支持的类型包括折线图、面积图、TopN表格、热力图、饼图。

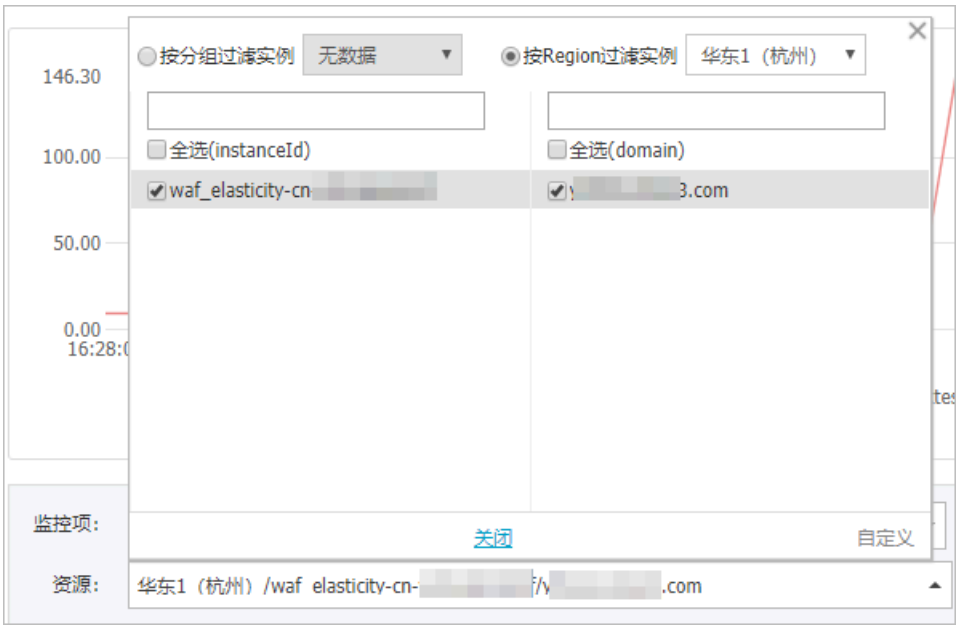
   b) 选择监控项。选择云产品监控，并设置产品为Web应用防火墙，进一步配置监控项和资源。

   - 监控项：选择要监控的Web应用防火墙数据指标（参见表 2-3: Web应用防火墙监控指标）。
   - 资源：选择要监控的域名。

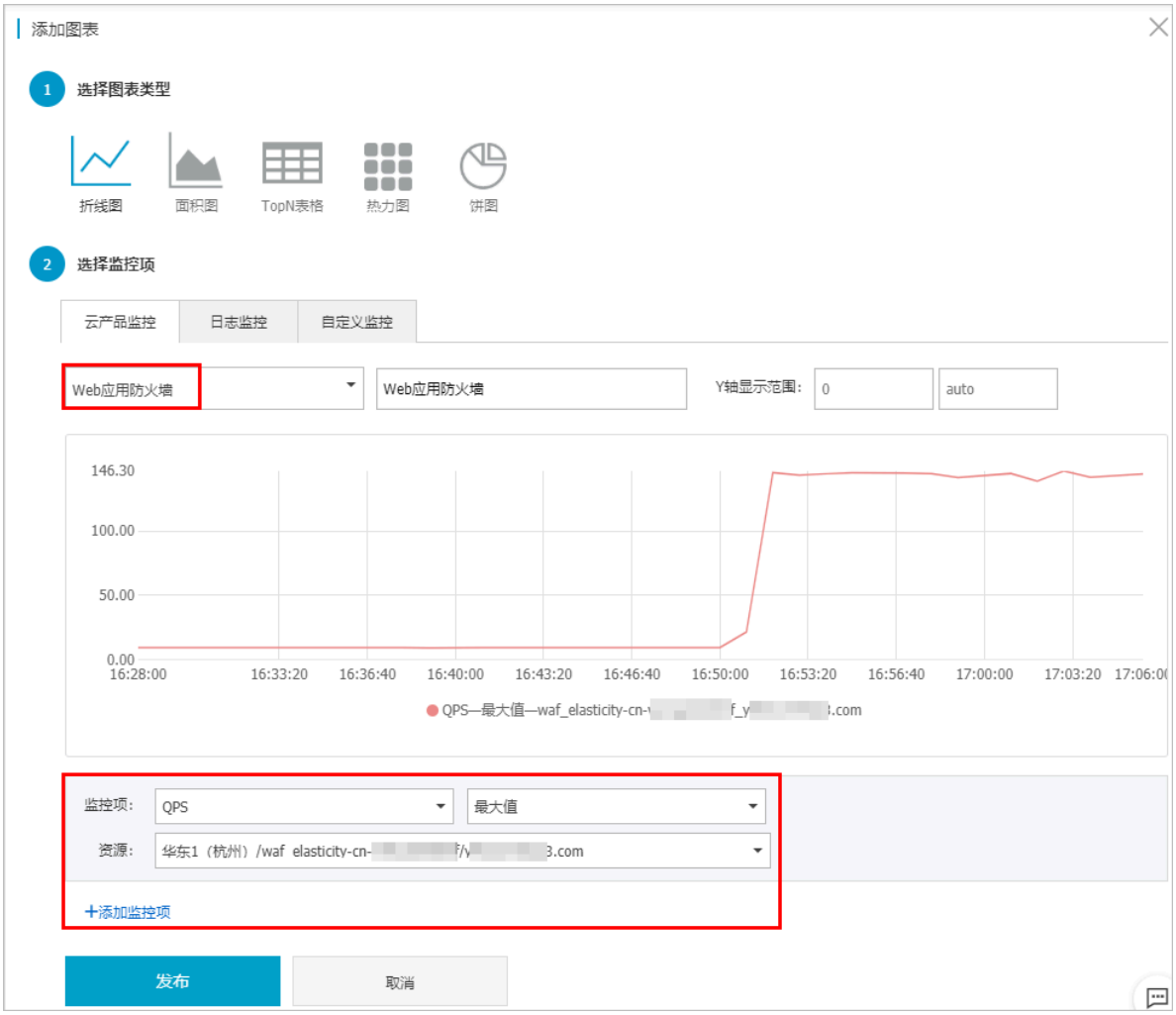
     说明:

域名资源列表中仅展示近12小时内通过当前Web应用防火墙实例产生过业务数据的域名。

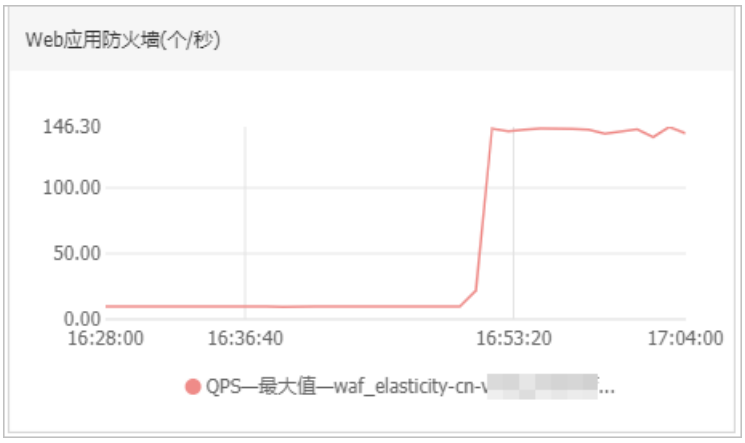


单击添加监控项可以在当前图表中定义多个监控项。

c) 单击发布，生成监控图表。



成功生成Web应用防火墙监控图表。



5. **您可以重复步骤4，在当前监控大盘下继续添加图表。更多信息，请参见**#unique_20、#unique_21。

3 日志服务告警配置最佳实践

3.1 概述

本实践基于阿里云日志服务的告警功能，为接入Web应用防火墙（WAF）并开启了日志服务的业务配置自定义监控图表和告警服务，适用于企业级和个人用户在使用WAF时对业务整体流量和安全状态进行监控和告警。

使用流程

本实践的操作环节包括以下任务。

步骤	说明
步骤1：创建WAF日志分析仪表盘	使用Web应用防火墙日志服务发起查询/分析后，您可以依据当前查询语句创建一个仪表盘。仪表盘默认包含当前查询语句对应的图表。
步骤2：配置日志图表	创建Web应用防火墙日志分析仪表盘后，您可以在仪表盘中编辑/删除已有日志图表或通过复制创建新的日志图表。
步骤3：配置日志告警	创建Web应用防火墙日志分析仪表盘后，您可以在仪表盘中配置日志告警。日志告警必须关联仪表盘中已有的日志图表，并使用关联图表中的参数设置告警触发条件。日志告警支持自定义告警信息发送模板。

配置范例

本实践提供了13个日志图表和告警配置范例供您参考，分别是4XX比例（忽略拦截数据）、5XX比例异常告警、QPS异常告警、QPS突增告警、QPS突降告警、5分钟内ACL拦截情况告警、5分钟内WAF拦截情况告警、5分钟内CC拦截情况告警、5分钟内防扫描拦截情况、5分钟内单IP攻击量预警、5分钟内单IP攻击域名数量告警、5分钟平均时延情况、UID维度流量突降告警场景。

建议您在熟悉日志图表（步骤2）和告警配置（步骤3）后，再参见WAF日志图表及告警配置参考添加图表并在添加图表的过程中直接配置告警。

关于在告警配置中用到的监控指标以及监控指标的阈值设置建议，请参见常用监控指标。

关于围绕监控指标进行查询/分析时用到的SQL查询语句，请参见常用SQL语句。

3.2 步骤1：创建WAF日志分析仪表盘

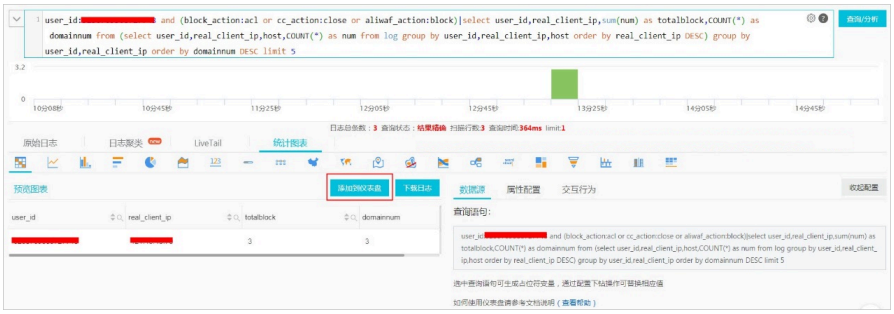
使用Web应用防火墙（WAF）日志服务发起查询/分析后，您可以依据当前查询语句创建一个仪表盘。仪表盘默认包含当前查询语句对应的图表。

前提条件

- **域名已接入Web应用防火墙进行防护。更多信息，请参见*#unique_30*。**
- **域名已开启Web应用防火墙日志服务。更多信息，请参见*#unique_31*。**

操作步骤

1. **登录*Web*应用防火墙控制台。**
2. **进入日志服务高级管理页面。**
   a) **在页面上方选择地域（中国大陆、海外地区），并在左侧导航栏单击市场管理 > 应用管理。**
   b) **在日志服务实时查询分析下，单击配置。**
   c) **在日志服务页面右上角，单击高级管理。**
   d) **在弹出的对话框中，单击确定。**
3. **在Project列表中，定位到要操作的Web应用防火墙日志项目，单击Project名称。**
4. **输入查询语句，并单击查询/分析。**
5. **查询结束后，单击统计图表下的添加到仪表盘。**



6. 在添加到仪表盘对话框，完成以下配置，并单击确定。

配置项	说明
操作类型	选择新建仪表盘。
Dashboard名称	为仪表盘命名。
图表名称	为当前查询语句对应的图表命名。

预期结果

成功创建仪表盘后，页面跳转到新建的仪表盘。仪表盘默认包含步骤4使用的查询语句对应的图表，您可以根据需要在仪表盘编辑当前图表或添加更多的图表。

后续步骤

步骤2：配置日志图表

3.3 步骤2：配置日志图表

创建Web应用防火墙（WAF）日志分析仪表盘后，您可以在仪表盘中编辑/删除已有日志图表或通过复制创建新的日志图表。

前提条件

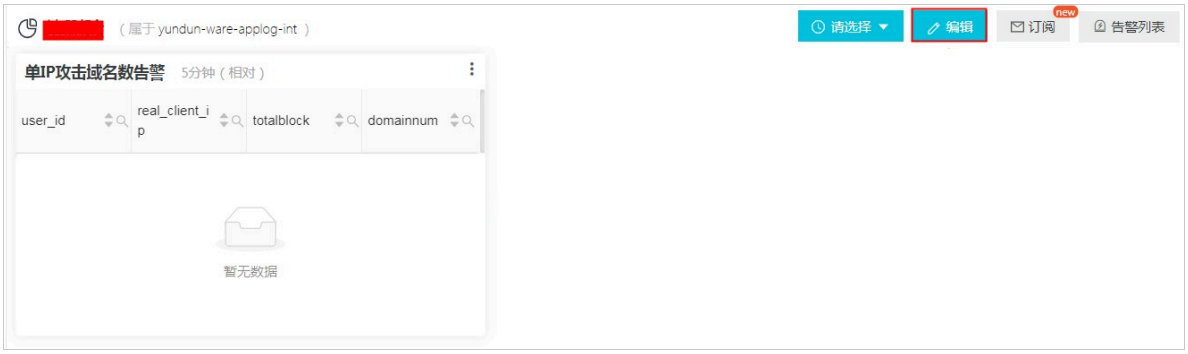
已创建日志分析仪表盘。更多信息，请参见步骤1：创建WAF日志分析仪表盘。

背景信息

本实践提供了13个默认的图表配置范例，具体请参见WAF日志图表及告警配置参考。建议您先参见步骤3：配置日志告警熟悉告警配置步骤，再参见范例添加图表并在添加图表的过程中直接配置告警。

操作步骤

1. 进入自定义的Web应用防火墙日志分析仪表盘。
2. 单击仪表盘右上角的编辑。



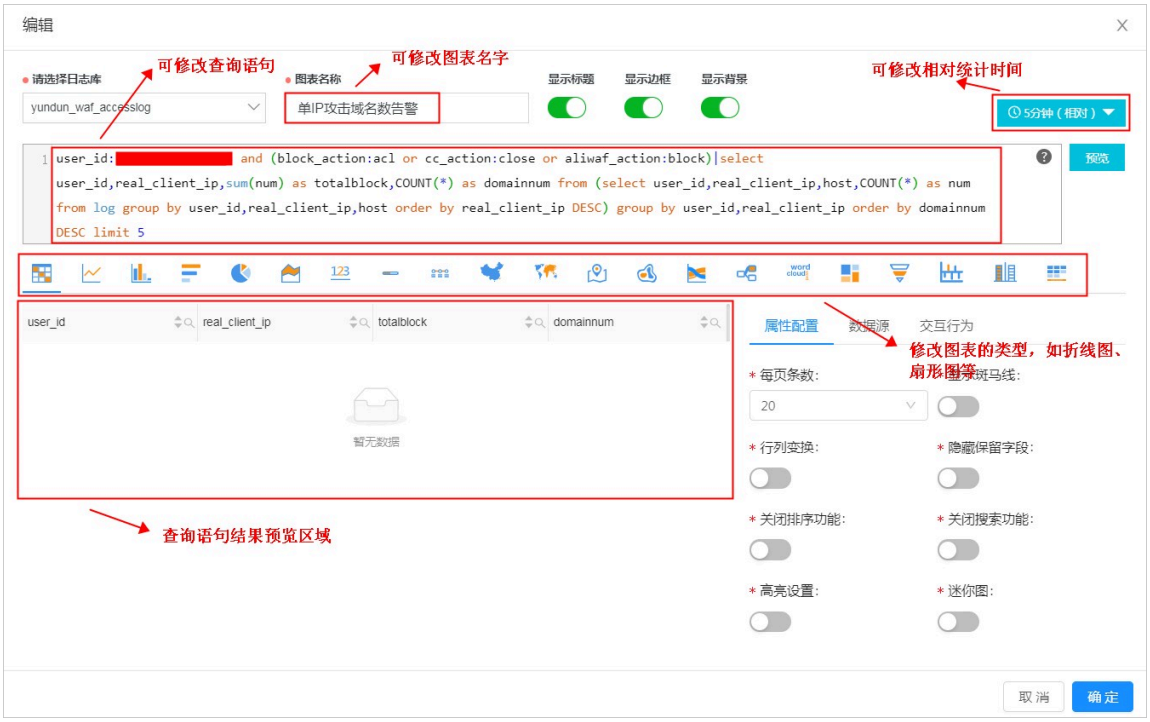
仪表盘切换到编辑模式。在编辑模式下，您可以编辑/删除当前仪表盘中已有图表或通过复制添加新的图表。

3. 编辑已有图表。
   a) 定位到要编辑的图表，将光标悬置在图表右上角的选项图标（⋮）上，并单击编辑。

   b) 在编辑页面，根据需要修改当前图表的配置，例如图表名称、SQL查询语句、相对统计时间、图表类型等，并单击确定。

> **说明:**

如果您修改了SQL查询语句，则必须单击预览，由系统自动检查语句的正确性后才可以单击确定。如果SQL查询语句有问题，您会收到报错信息，这时确定按钮不可操作。只有将SQL查询语句修改正确后，您才可以单击确定。



4. **通过复制添加新的图表。**

   a) **定位到要复制的图表，将光标悬置在图表右上角的选项图标（⋮）上，并单击复制。**

   成功复制图表后，当前图表旁边出现一个相同的图表。

   b) **用光标拖动复制生成的图表到仪表盘上的合适位置。**

   c) **编辑复制生成的图表，修改图表名称、SQL查询语句等信息。**

5. **重复步骤3~步骤4，在仪表盘里添加更多的图表，实现多样化的数据展示以及告警配置。**

后续步骤

步骤3：配置日志告警

3.4 步骤3：配置日志告警

创建Web应用防火墙（WAF）日志分析仪表盘后，您可以在仪表盘中配置日志告警。日志告警必须关联仪表盘中已有的日志图表，并使用关联图表中的参数设置告警触发条件。日志告警支持自定义告警信息发送模板。

前提条件

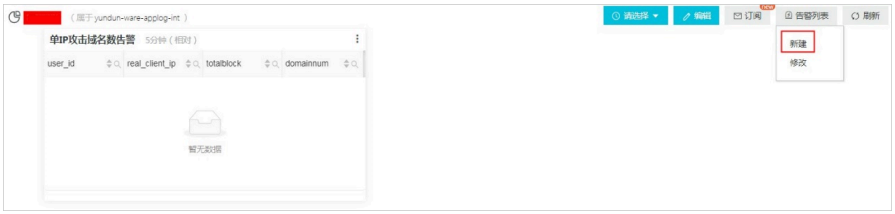
已创建日志分析仪表盘。更多信息，请参见步骤1：创建WAF日志分析仪表盘。

背景信息

本实践提供了13个默认的告警配置范例，具体请参见WAF日志图表及告警配置参考。建议您先参见步骤2：配置日志图表熟悉图表配置步骤，再参见范例添加图表并在添加图表的过程中直接配置告警和通知方式。

操作步骤

1. 进入自定义的Web应用防火墙日志分析仪表盘。
2. 在仪表盘右上角，选择告警列表 > 新建。



3. 在创建告警侧边页，完成以下告警配置，并单击下一步。

配置项	说明
告警名称	告警的名称。名称长度为1~64个字符。

配置项	说明
关联图表	设置告警中关联的图表。 设置关联图表时，查询区间为服务端每次执行查询时，读取的数据时间范围，支持相对时间与整点时间。例如，执行时间点为14:30:06，设置查询区间为15分钟（相对），则查询区间为14:15:06- 14:30:06；设置查询区间为15分钟（整点时间），则查询区间为：14:15:00- 14:30:00。 需要添加多个图表时，只需单击添加并设置即可。最多支持关联三个图表。图表名称前的编号为该图表在告警中的编号，您可以在触发条件中通过编号指定关联的图表。
频率	服务端每次执行告警检查的时间。 说明: 目前服务端只返回检查结果中的前100条数据。
触发条件	判断告警是否触发的条件表达式，满足该条件时会根据执行间隔和通知间隔发送告警通知。 图表默认从0开始编号，在触发条件里用`$0`表示第一个图表。例如，您可以设置`$0.domainnum>=10`，表示第一个图表中`domainnum`字段值大于等于10时触发告警。 多个条件之间使用`&&`连接，表示逻辑与的关系，即必须同时满足；使用`||`连接，表示逻辑或的关系，即满足其中一个即可。 说明: 更多告警条件表达式语法请参见*#unique_32*。
高级选项	
触发通知阈值	累计触发次数达到该阈值时根据通知间隔发送告警。不满足触发条件时不计入统计。 默认触发通知阈值为1，即满足一次触发条件即可检查通知间隔。 通过配置触发通知阈值可以实现多次触发、一次通知。例如，配置触发通知阈值为100，则累计触发次数达到100次时检查通知间隔。如果同时满足触发通知阈值和通知间隔，则发送通知。发送通知之后，累计次数会清零。如果因网络异常等原因执行检查失败，不计入累计次数。

配置项	说明
通知间隔	两次告警通知之间的时间间隔。 如果某次执行满足了触发条件，而且累计的触发次数已经达到触发通知阈值，且距离上次发送通知已经达到了通知间隔，则发送通知。如设置通知间隔为5分钟，则5分钟内至多收到一次通知。默认无间隔。 说明: 通过配置触发通知阈值和通知间隔可以实现告警抑制的功能，防止收到过多的告警信息。

说明:

触发通知阈值、通知间隔、检查频率三个条件配合使用，表示日志系统按照设置的检查频率去检查触发条件是否满足，并在通知间隔内达到触发通知阈值次数时推送告警信息。

4. 在创建告警侧边页，完成通知设置，并单击提交。

日志服务支持多种常用的告警通知方式，例如短信、语音、邮件、WebHook+钉钉机器人等。您必须先在通知列表右侧选择要使用的通知方式，然后完成具体配置。支持选择并配置多种通知方式。

- **短信告警：设置接收告警的手机号码和发送内容。发送内容中可以指定告警字段。单击查看全部变量了解各字段的含义。**

- **语音告警：设置接收告警的手机号码和发送内容。**

- **邮件告警：设置接收告警的收件人邮箱地址、告警邮件的主题和发送内容。**

- **WebHook+钉钉机器人：设置接收告警的钉钉群机器人的webhook地址（请求地址）和发送内容。**

5. 重复步骤2~步骤4，创建更多的告警配置。

3.5 WAF日志图表及告警配置参考

本实践提供了13个典型的Web应用防火墙（WAF）日志查询/分析告警场景的配置范例。您可以参考本文的SQL语句模板在WAF日志仪表盘中配置图表，并按照告警参数配置建议配置告警。

使用须知

使用本参考前，您必须已完成创建WAF日志分析仪表盘。更多信息，请参见步骤1：创建WAF日志分析仪表盘。

- **关于在仪表盘中配置图表的步骤，请参见步骤2：配置日志图表。**
- **关于在仪表盘中配置告警的步骤，请参见步骤3：配置日志告警。**

本参考提供以下13个告警配置范例。

序号	告警场景
1	4XX比例异常告警
2	5XX比例异常告警
3	QPS异常告警
4	QPS突增告警
5	QPS突降告警
6	5分钟内ACL拦截情况告警
7	5分钟内WAF拦截情况告警
8	5分钟内CC拦截情况告警
9	5分钟内扫描拦截情况告警
10	单IP攻击攻击量预警
11	单IP攻击域名数量告警
12	5分钟平均时延情况
13	UID维度流量突降告警

4XX比例异常告警

图表名称：4XX比例（忽略拦截数据）

SQL语句模板

```
user_id:11111111110000 and not
real_client_ip:1.1.1.1|select user_id,host as "域名",Rate_2XX as
"2XX比例",Rate_3XX as "3XX比例",Rate_4XX as "4XX比例",Rate_5XX
as "5XX比例",countall as
"aveQPS",status_2XX,status_3XX,status_4XX,status_5XX,countall
from(select user_id,host,round(round(status_2XX*1.0000/countall,4)*100
,2) as
Rate_2XX,round(round(status_3XX*1.0000/countall,4)*100,2) as Rate_3XX,
round(round

(status_4XX*1.0000/countall,4)*100,2) as
Rate_4XX,round(round(status_5XX*1.0000/countall,4)*100,2) as Rate_5XX,
status_2XX,status_3XX,status_4XX,status_5XX,countall
from(select user_id,

host,count_if(status>=200 and status<300) as
status_2XX,count_if(status>=300 and status<400) as
status_3XX,count_if(status>=400 and status<500 and status<>444 and
status<>405 ) as status_4XX,count_if(status>=500 and

status<600) as
status_5XX,COUNT(*) as countall group by host,user_id)) where
countall>120 order by Rate_4XX DESC  limit 5
```

告警参数配置建议（关联当前图表）

该图表包含以下字段：`aveQPS`**、**`2XX`**比例、**`3XX`**比例、**`4XX`**比例、**`5XX`**比例，分别表示域名QPS和各类型响应状态码的占比。其中，**`4XX`**比例不包含WAF拦截的CC攻击和Web攻击等造成的444和405状态码，以便只展示因业务自身原因造成的状态码变化。在设置告警触发条件时，您可以自由组合上述字段。例如，**`aveQPS>10 && 2XX`**比例**`<60`**表示在设定的统计时间内指定域名的QPS达到10以上且2XX比例小于60%。**

- **查询区间：建议设置为5分钟**
- **频率：建议设置为5分钟**
- **触发条件：**`$0.countall>3000&& $0.4XX`**比例**`>80`
- **触发通知阈值：2次**
- **通知间隔：10分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名:${Results[0].RawResults[0].域名}
- 产品: WAF
- 最近5分钟内总请求数:${Results[0].RawResults[0].countall}
- 2XX比例:${Results[0].RawResults[0].2XX比例} %
- 3XX比例:${Results[0].RawResults[0].3XX比例} %
- 4XX比例:${Results[0].RawResults[0].4XX比例} %
- 5XX比例:${Results[0].RawResults[0].5XX比例} %
```

告警样例

5XX比例异常告警

图表名称：5XX比例

SQL语句模板

```
user_id:11111111110000 and not
real_client_ip:1.1.1.1|select user_id,host as "域名",Rate_2XX as
"2XX比例",Rate_3XX as "3XX比例",Rate_4XX as "4XX比例",Rate_5XX
as "5XX比例",countall as "相对时间内访问量",status_2XX,status_3XX,
status_4XX,status_5XX,countall
from(select user_id,host,round(round(status_2XX*1.0000/countall,4)*100
,2) as
Rate_2XX,round(round(status_3XX*1.0000/countall,4)*100,2) as Rate_3XX,
round(round

(status_4XX*1.0000/countall,4)*100,2) as
Rate_4XX,round(round(status_5XX*1.0000/countall,4)*100,2) as
Rate_5XX,status_2XX,status_3XX,status_4XX,status_5XX,countall from(
select
user_id,

host,count_if(status>=200 and status<300) as
status_2XX,count_if(status>=300 and status<400) as
status_3XX,count_if(status>=400 and status<500) as
status_4XX,count_if(status>=500 and

status<600) as
status_5XX,COUNT(*) as countall group by host,user_id)) where
countall>120 order by Rate_5XX DESC  limit 5
```

告警参数配置建议（关联当前图表）

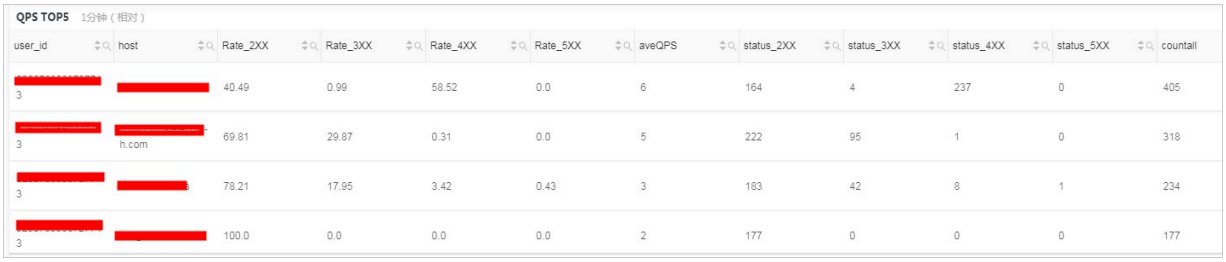
- **查询区间：建议设置为5分钟**
- **频率：建议设置为5分钟**
- **触发条件：**`$0.countall>3000&& $0.5XX比例>80`
- **触发通知阈值：2次**
- **通知间隔：10分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名:${Results[0].RawResults[0].域名}
- 产品: WAF
- 最近5分钟内总请求数:${Results[0].RawResults[0].countall}
- 2XX比例:${Results[0].RawResults[0].2XX比例} %
- 3XX比例:${Results[0].RawResults[0].3XX比例} %
- 4XX比例:${Results[0].RawResults[0].4XX比例} %
- 5XX比例:${Results[0].RawResults[0].5XX比例} %
```

告警样例

QPS异常告警

图表名称：QPS TOP5



SQL语句模板

```
user_id: 11111111110000 and not
real_client_ip:1.1.1.1|select
user_id,host,Rate_2XX,Rate_3XX,Rate_4XX,Rate_5XX,countall/60 as
"aveQPS",status_2XX,status_3XX,status_4XX,status_5XX,countall
```

```
from(select user_id,host,round(round(status_2XX*1.0000/countall,4)*100
,2) as Rate_2XX,round(round(status_3XX*1.0000/countall,4)*100,2)
as Rate_3XX, round(round

(status_4XX*1.0000/countall,4)*100,2) as
Rate_4XX,round(round(status_5XX*1.0000/countall,4)*100,2) as
Rate_5XX,status_2XX,status_3XX,status_4XX,status_5XX,countall from(
select
user_id,

host,count_if(status>=200 and status<300) as
status_2XX,count_if(status>=300 and status<400) as
status_3XX,count_if(status>=400 and status<500 and status<>444 and
status<>405 ) as status_4XX,count_if(status>=500 and

status<600) as
status_5XX,COUNT(*) as countall group by host,user_id)) where
countall>120 order by aveQPS DESC  limit 5
```

告警参数配置建议（关联当前图表）

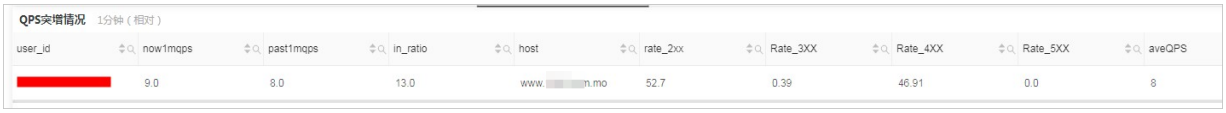
- **查询区间：建议设置为1分钟**
- **频率：建议设置为1分钟**
- **触发条件：** `$0.aveQPS>=50`
- **触发通知阈值：1次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名: ${Results[0].RawResults[0].host}
- 产品: WAF
- 过去1分钟平均QPS: ${Results[0].RawResults[0].aveQPS}
- 响应码 2xx_rate :${Results[0].RawResults[0].Rate_2XX}%
- 响应码 3xx_rate :${Results[0].RawResults[0].Rate_3XX}%
- 响应码 4xx_rate :${Results[0].RawResults[0].Rate_4XX}%
- 响应码 5xx_rate :${Results[0].RawResults[0].Rate_5XX}%
```

告警样例

QPS突增告警

图表名称：QPS突增情况



SQL语句模板

```
user_id: 11111111110000 |select
t1.user_id,t1.now1mQPS,t1.past1mQPS,in_ratio,t1.host,t2.Rate_2XX,
Rate_3XX,Rate_4XX,Rate_5XX,aveQPS
from (

 (

 SELECT
user_id,round(c[1]/60,0) as now1mQPS,round(c[2]/60,0) as past1mQPS,
round(round(c[1]/60,0)/round(c[2]/60,0)*100-100,0) as in_ratio ,host
from

       (SELECT
compare(t, 60) as c,host, user_id from

           (SELECT
COUNT(*) as t,host,user_id from log GROUP by host, user_id )  GROUP by
 host, user_id) where c[3] >1.1
and (c[1]>180 or c[2]>180

        )

  )t1

           join

  (select
user_id,host,Rate_2XX,Rate_3XX,Rate_4XX,Rate_5XX,countall/60 as
"aveQPS",status_2XX,status_3XX,status_4XX,status_5XX,countall from



     (select
user_id,host,round(round(status_2XX*1.0000/countall,4)*100,2) as
Rate_2XX,round(round(status_3XX*1.0000/countall,4)*100,2) as Rate_3XX,
round(round(status_4XX*1.0000/countall,4)*100,2) as
Rate_4XX,round(round(status_5XX*1.0000/countall,4)*100,2) as
Rate_5XX,status_2XX,status_3XX,status_4XX,status_5XX,countall from

        (select
user_id, host,count_if(status>=200 and status<300) as
status_2XX,count_if(status>=300 and status<400) as
status_3XX,count_if(status>=400 and status<500 and status<>444 and
status<>405 ) as status_4XX,count_if(status>=500 and status<600) as
status_5XX,COUNT(*) as countall from log group by host,user_id)

     ) where  countall>1

   )t2

     on t1.host=t2.host) order by in_ratio DESC
```

```
limit 5
```

告警参数配置建议（关联当前图表）

- **查询区间：建议设置为1分钟**
- **频率：建议设置为1分钟**
- **触发条件：** `$0.now1mqps>50&& $0.in_ratio>300`
- **触发通知阈值：1次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名: ${Results[0].RawResults[0].host}
- 产品: WAF
- 过去1分钟平均QPS: ${Results[0].RawResults[0].now1mqps}
- QPS突增率:${Results[0].RawResults[0].in_ratio}%
- 响应码 2xx_Rate :${Results[0].RawResults[0].rate_2xx}%
- 响应码 3xx_rate :${Results[0].RawResults[0].Rate_3XX}%
- 响应码 4xx_rate :${Results[0].RawResults[0].Rate_4XX}%
- 响应码 5xx_rate :${Results[0].RawResults[0].Rate_5XX}%
```

告警样例

QPS突降告警

图表名称：QPS突降情况

SQL语句模板

```
user_id: 11111111110000 |select
t1.user_id,t1.now1mQPS,t1.past1mQPS,de_ratio,t1.host,t2.Rate_2XX,
Rate_3XX,Rate_4XX,Rate_5XX,aveQPS
from (

 (

 SELECT
user_id,round(c[1]/60,0) as now1mQPS,round(c[2]/60,0) as past1mQPS,
round(100-round(c[1]/60,0)/round(c[2]/60,0)*100,2) as de_ratio,host
from

(SELECT compare(t, 60) as c,host, user_id from

    (SELECT
COUNT(*) as t,host,user_id from log GROUP by host, user_id )  GROUP by
 host, user_id ) where c[3] <0.9
and (c[1]>180 or c[2]>180

        )

  )t1

           join

  (select
user_id,host,Rate_2XX,Rate_3XX,Rate_4XX,Rate_5XX,countall/60 as
"aveQPS",status_2XX,status_3XX,status_4XX,status_5XX,countall from

     (select
user_id,host,round(round(status_2XX*1.0000/countall,4)*100,2) as
Rate_2XX,round(round(status_3XX*1.0000/countall,4)*100,2) as

Rate_3XX,
round(round(status_4XX*1.0000/countall,4)*100,2) as
Rate_4XX,round(round(status_5XX*1.0000/countall,4)*100,2) as

Rate_5XX,status_2XX,status_3XX,status_4XX,status_5XX,countall
from

        (select
user_id, host,count_if(status>=200 and status<300) as
status_2XX,count_if(status>=300 and status<400) as status_3XX,count_if

(status>=400 and status<500 and status<>444
and status<>405 ) as status_4XX,count_if(status>=500 and
status<600) as status_5XX,COUNT(*) as countall from log group by host,
user_id)

     ) where  countall>1

)t2 on
t1.host=t2.host) order by de_ratio DESC limit 5
```

告警参数配置建议（关联当前图表）

该图表中包含`now1mpqs`（当前一分钟平均QPS）、`past1mqps`（过去一分钟平均QPS）、`de_ratio`（QPS下降率）、`host`等字段，您可以根据需要使用这些字段设置告警条件。

- **查询区间：建议设置为1分钟**
- **频率：建议设置为1分钟**
- **触发条件：** `$0.now1mqps>10&& $0.de_ratio>50`
- **触发通知阈值：2次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名: ${Results[0].RawResults[0].host}
- 产品: WAF（海外）
- 过去1分钟平均QPS: ${Results[0].RawResults[0].now1mqps}
- QPS突降率:${Results[0].RawResults[0].de_ratio}%
- 响应码 2xx_rate :${Results[0].RawResults[0].rate_2xx}%
- 响应码 3xx_rate :${Results[0].RawResults[0].Rate_3XX}%
- 响应码 4xx_rate :${Results[0].RawResults[0].Rate_4XX}%
- 响应码 5xx_rate :${Results[0].RawResults[0].Rate_5XX}%
```

告警样例

5分钟内ACL拦截情况告警

图表名称：相应时间内ACL拦截情况

SQL语句模板

```
user_id:
11111111110000 |select user_id,host,count_if(block_action='antiscan')
as "防扫描拦截量",count_if(block_action='acl')
as "ACL拦截量",count_if(aliwaf_action='block')
as "WAF拦截量",count_if(cc_action='close') as
"CC拦截量",count_if(block_action='acl' or
```

```
aliwaf_action='block' or cc_action='close' or block_action='antiscan
') as
totalblock  group by host,user_id having
("ACL拦截量" >=0 and "WAF拦截量" >=0 and "CC拦截量">=0
and totalblock>10) order by "ACL拦截量"  DESC limit 5
```

告警参数配置建议（关联当前图表）

- **查询区间：建议设置为5分钟**
- **频率：建议设置为5分钟**
- **触发条件：** `$0.totalblock>=500&&($0.ACL拦截量>=500)`
- **触发通知阈值：1次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名:${Results[0].RawResults[0].host}
- 产品: WAF
- 最近5分钟内拦截总量:${Results[0].RawResults[0].totalblock}
- ACL拦截量:${Results[0].RawResults[0].ACL拦截量}
- WAF拦截量:${Results[0].RawResults[0].WAF拦截量}
- CC拦截量:${Results[0].RawResults[0].CC拦截量}
- 防扫描拦截量:${Results[0].RawResults[0].防扫描拦截量}
```

5分钟内WAF拦截情况告警

图表名称：相应时间内WAF拦截情况

SQL语句模板

```
user_id:111111111110000
|select user_id,host,count_if(block_action='antiscan') as "防扫描拦截
量",count_if(block_action='acl')
as "ACL拦截量",count_if(aliwaf_action='block')
as "WAF拦截量",count_if(cc_action='close') as
"CC拦截量",count_if(block_action='acl' or
aliwaf_action='block' or cc_action='close' or block_action='antiscan
') as
totalblock  group by host,user_id having
("ACL拦截量" >=0 and "WAF拦截量" >=0 and "CC拦截量">=0
and totalblock>10) order by "WAF拦截量"  DESC limit 5
```

告警参数配置建议（关联当前图表）

- **查询区间：建议设置为5分钟**
- **频率：建议设置为5分钟**
- **触发条件：** `$0.totalblock>=500&&($0.WAF拦截量>=500)`

- **触发通知阈值：1次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名:${Results[0].RawResults[0].host}
- 产品: WAF
- 最近5分钟内拦截总量:${Results[0].RawResults[0].totalblock}
- ACL拦截量:${Results[0].RawResults[0].ACL拦截量}
- WAF拦量:${Results[0].RawResults[0].WAF拦截量}
- CC拦截量:${Results[0].RawResults[0].CC拦截量}
- 防扫描拦截量:${Results[0].RawResults[0].防扫描拦截量}
```

5分钟内CC拦截情况告警

图表名称：相应时间内CC拦截情况

SQL语句模板

```
user_id:
111111111110000 |select user_id,host,count_if(block_action='antiscan')
as "防扫描拦截量",count_if(block_action='acl')
as "ACL拦截量",count_if(aliwaf_action='block')
as "WAF拦截量",count_if(cc_action='close') as
"CC拦截量",count_if(block_action='acl' or
aliwaf_action='block' or cc_action='close' or block_action='antiscan
') as
totalblock  group by host,user_id having
("ACL拦截量" >=0 and "WAF拦截量" >=0 and "CC拦截量">=0
and totalblock>10) order by "CC拦截量"  DESC limit 5
```

告警参数配置建议（关联当前图表）

- **查询区间：建议设置为5分钟**
- **频率：建议设置为5分钟**
- **触发条件：** `$0.totalblock>=500&&($0.CC拦截量>=500)`
- **触发通知阈值：1次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名:${Results[0].RawResults[0].host}
- 产品: WAF
- 最近5分钟内拦截总量:${Results[0].RawResults[0].totalblock}
- ACL拦截量:${Results[0].RawResults[0].ACL拦截量}
- WAF拦量:${Results[0].RawResults[0].WAF拦截量}
```

```
- CC拦截量:${Results[0].RawResults[0].CC拦截量}
- 防扫描拦截量:${Results[0].RawResults[0].防扫描拦截量}
```

5分钟内扫描拦截情况告警

图表名称：相应时间内防扫描拦截情况

SQL语句模板

```
user_id:
11111111110000 |select user_id,host,count_if(block_action='antiscan')
as "防扫描拦截量",count_if(block_action='acl')
as "ACL拦截量",count_if(aliwaf_action='block')
as "WAF拦截量",count_if(cc_action='close') as
"CC拦截量",count_if(block_action='acl' or
aliwaf_action='block' or cc_action='close' or block_action='antiscan
') as
totalblock  group by host,user_id having
("ACL拦截量" >=0 and "WAF拦截量" >=0 and "CC拦截量">=0
and totalblock>10) order by "防扫描拦截量"  DESC limit 5
```

告警参数配置建议（关联当前图表）

- **查询区间：建议设置为5分钟**
- **频率：建议设置为5分钟**
- **触发条件：** `$0.totalblock>=500&&($0.防扫描拦截量>=500)`
- **触发通知阈值：1次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名:${Results[0].RawResults[0].host}
- 产品：WAF（海外）
- 最近5分钟内拦截总量:${Results[0].RawResults[0].totalblock}
- ACL拦截量:${Results[0].RawResults[0].ACL拦截量}
- WAF拦量:${Results[0].RawResults[0].WAF拦截量}
- CC拦截量:${Results[0].RawResults[0].CC拦截量}
- 防扫描拦截量:${Results[0].RawResults[0].防扫描拦截量}
```

单IP攻击攻击量预警

图表名称：相应时间内单IP攻击预警

SQL语句模板

```
user_id:
11111111110000 |select user_id,real_client_ip,concat('ACL拦截量:',cast(
aclblock as
varchar(10)),'  ','WAF拦截量:',cast(wafblock as varchar(10)),'
','CC拦截量:',cast(aclblock as varchar(10))) as
blockNum,totalblock,allRequest from (select user_id,real_client_ip,
count_if(block_action='acl')
as aclblock,count_if(aliwaf_action='block') as
wafblock,count_if(cc_action='close') as ccblock,count_if(block_action
='acl' or
aliwaf_action='block' or cc_action='close') as totalblock,COUNT(*) as
allRequest from log group by user_id,real_client_ip having totalblock>
1
order by totalblock DESC  limit 5)
```

告警参数配置建议（关联当前图表）

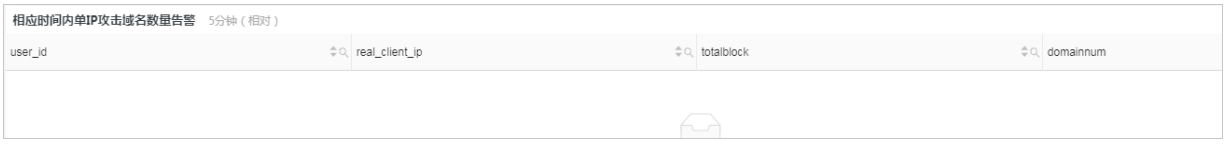
该图表中包含`real_client_ip`、`blockNum`（**含ACL拦截量、WAF拦截量、CC拦截量等数据**）、`totalblock`（**总拦截请求数**）、`allRequest`（**总请求数**）**字段，您可以根据需要使用这些字段设置告警条件**。

- **查询区间：建议设置为5分钟**
- **频率：建议设置为5分钟**
- **触发条件：**`$0.totalblock >=500`
- **触发通知阈值：1次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 产品:WAF
- 最近5分钟内单IP攻击排行Top3:
- ${Results[0].RawResults[0].real_client_ip}  (${Results[0].
RawResults[0].blockNum})
- ${Results[0].RawResults[1].real_client_ip}  (${Results[0].
RawResults[1].blockNum})
-${Results[0].RawResults[2].real_client_ip}  (${Results[0].
RawResults[2].blockNum})
```

单IP攻击域名数量告警

图表名称：相应时间内单IP攻击域名数量告警



SQL语句模板

```
user_id:
11111111110000  and not
upstream_status:504 and not upstream_addr:- and request_time_msec <
5000 and
upstream_status:200 and not ua_browser:bot |SELECT user_id,host,
upstream_time,request_time,ssl_handshake,requestnum
from (select user_id,host,round(avg(upstream_response_time),2)*1000 as
upstream_time,round(avg(request_time_msec),2) as
request_time,round(avg(ssl_handshake_time)*1000,2) as ssl_handshake,
COUNT(*) as
requestnum from log group by host,user_id) where requestnum>30 order
by
request_time DESC limit 5
```

告警参数配置建议（关联当前图表）

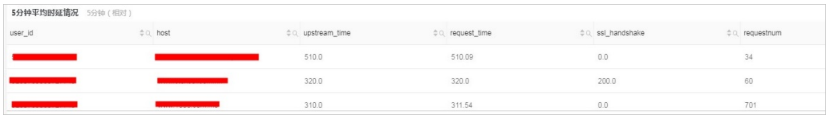
该图表中包含`real_client_ip`（攻击IP）、`totalblock`（总拦截请求数）、`domainnum`（该IP攻击的域名数）等字段。在设置告警触发条件时，您可以自由组合上述字段。例如，`totalblock>500&& domainnum>5`表示某IP在对应时间内总攻击量达到500，并且攻击域名数多于5个。

- **查询区间：建议设置为5分钟**
- **频率：建议设置为1分钟**
- **触发条件：`$0.domainnum>=10`**
- **触发通知阈值：1次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 产品: WAF
- 攻击IP:${Results[0].RawResults[0].real_client_ip}
- 攻击的域名数:${Results[0].RawResults[0].domainnum}
- 最近5分钟总攻击请求数:${Results[0].RawResults[0].totalblock}
- 请及时关注处理
```

5分钟平均时延情况

图表名称：5分钟平均时延情况



SQL语句模板

```
user_id:
11111111110000 and and not upstream_status:504 and not upstream_addr
:- and
```

```
request_time_msec < 5000 and upstream_status:200 and not ua_browser:
bot|SELECT
user_id,host,upstream_time,request_time,ssl_handshake,requestnum from
 (select user_id,host,round(avg(upstream_response_time),2)*1000
as upstream_time,round(avg(request_time_msec),2) as
request_time,round(avg(ssl_handshake_time)*1000,2) as ssl_handshake,
COUNT(*) as
requestnum from log group by host,user_id) where requestnum>30 order
by
request_time DESC limit 5
```

告警参数配置建议（关联当前图表）

- **查询区间：建议设置为5分钟**
- **频率：建议设置为5分钟**
- **触发条件：** `$0.request_time>1000&& $0.requestnum>30`
- **触发通知阈值：2次**
- **通知间隔：10分钟**
- **发送内容**

```
- [时间]:${FireTime}
- [Uid]:${Results[0].RawResults[0].user_id}
- 域名:${Results[0].RawResults[0].host}
- 产品：WAF（海外）
- [触发条件]:${condition}
- 最近5分钟延时情况TOP3（毫秒）
- Host1:${Results[0].RawResults[0].host} Delay_time:${Results[0].
RawResults[0].upstream_time}
- Host2:${Results[0].RawResults[1].host} Delay_time:${Results[0].
RawResults[1].upstream_time}
- Host3:${Results[0].RawResults[2].host} Delay_time:${Results[0].
RawResults[2].upstream_time}
```

UID维度流量突降告警

图表名称：UID维度流量突降告警

SQL语句模板

```
user_id: 11111111110000 |select
t1.user_id,t1.now1mQPS,t1.past1mQPS,de_ratio,t2.Rate_2XX,Rate_3XX,
Rate_4XX,Rate_5XX,aveQPS
from (

 (

 SELECT
user_id,round(c[1]/60,0) as now1mQPS,round(c[2]/60,0) as past1mQPS,
round(100-round(c[1]/60,0)/round(c[2]/60,0)*100,2) as de_ratio from

(SELECT compare(t, 60) as c, user_id from
```

```
    (SELECT
COUNT(*) as t,user_id from log GROUP by user_id )  GROUP by user_id )
where c[3] <0.9 and
(c[1]>180 or c[2]>180

        )

  )t1

          join

  (select
user_id,Rate_2XX,Rate_3XX,Rate_4XX,Rate_5XX,countall/60 as
"aveQPS",status_2XX,status_3XX,status_4XX,status_5XX,countall from



     (select
user_id,round(round(status_2XX*1.0000/countall,4)*100,2) as
Rate_2XX,round(round(status_3XX*1.0000/countall,4)*100,2) as



Rate_3XX,
round(round(status_4XX*1.0000/countall,4)*100,2) as
Rate_4XX,round(round(status_5XX*1.0000/countall,4)*100,2) as



Rate_5XX,status_2XX,status_3XX,status_4XX,status_5XX,countall
from

        (select
user_id,count_if(status>=200 and status<300) as
status_2XX,count_if(status>=300 and status<400) as status_3XX,count_if



(status>=400 and status<500 and status<>444
and status<>405 ) as status_4XX,count_if(status>=500 and
status<600) as status_5XX,COUNT(*) as countall from log group by
user_id)

     ) where  countall>0

)t2 on
t1.user_id=t2.user_id) order by de_ratio DESC limit 5
```

告警参数配置建议（关联当前图表）

- **查询区间：建议设置为1分钟**
- **频率：建议设置为1分钟**
- **触发条件：** `$0.de_ratio>50&& $0.now1mqps>20`
- **触发通知阈值：1次**
- **通知间隔：5分钟**
- **发送内容**

```
- [时间]:${FireTime}
```

```
- [UID]:${Results[0].RawResults[0].user_id}
- 产品: WAF
- 过去1分钟平均QPS: ${Results[0].RawResults[0].now1mqps}
- [触发条件(突降率&QPS)]:${condition}
- QPS突降率:${Results[0].RawResults[0].de_ratio}%
- 响应码 2xx_rate :${Results[0].RawResults[0].rate_2xx}%
- 响应码 3xx_rate :${Results[0].RawResults[0].Rate_3XX}%
- 响应码 4xx_rate :${Results[0].RawResults[0].Rate_4XX}%
- 响应码 5xx_rate :${Results[0].RawResults[0].Rate_5XX}%
```

3.6 常用监控指标

本文介绍了使用Web应用防火墙日志服务发起查询/分析时常用的监控指标及其含义。您可以将这些指标用于告警配置条件中，自定义监控业务的异常情况。本文也提供了在告警配置中建议使用的监控指标阈值和指标异常时的处理建议。

监控指标	指标含义/触发原因	建议阈值	处理建议
200	服务器已成功处理请求，返回了请求的数据	初始化正常业务时，200状态码的告警监控阈值可以配置为90%，具体根据实际业务情况调整。	如果发现低于监控比例，需要分析比例下降的原因，例如是否因为其他错误状态码比例增加。
request_time	客户端请求到返回结果的请求耗时	按实际业务请求所需耗时，设置合适的超时告警监控阈值。	如果发现域名请求耗时较长，需要检查客户端-WAF-源站整体网路链路质量，并排查源站响应状态是否正常。
upstream_response_time	请求回源时，WAF回源站返回数据的响应时间		
ssl_handshake_time	HTTPS协议请求时，客户端与WAF的SSL握手时间		
status:302 and block_action:captcha and block_action:tmd	人机校验JS请求状态码，302表示触发默认策略，200表示触发手动策略	初始化时，建议配置5%~10%的告警阈值比例，后续运营期间可以根据业务拦截情况灵活调整。	· 如果达到告警阈值，建议分析是否受到CC攻击，根据攻击情况设置自定义规则。 · 检查服务器是否出现异常，如大量的5xx状态码、4xx状态码。
200 and block_action:antifraud	数据风控拦截		测试可用后再上线，如弹出率过高，说明场景可能有问题，建议联系我们进行确认。

监控指标	指标含义/触发原因	建议阈值	处理建议
status:404	服务器找不到请求的资源		查询触发告警的IP。 · 如果是个例，则可能存在恶意用户遍历服务器资源。 · 如果是普遍存在，则需要确认服务器是否正常或者是否有文件丢失。
status:405	被Web应用防护规则或精准访问控制规则拦截		通过全量日志分析拦截的规则、请求行为，判断是正常拦截还是误拦截。
status:444	被WAF CC自定义规则拦截		· 如果达到告警阈值，建议分析是否受到CC攻击，根据攻击情况设置自定义规则。 · 如果不是攻击，而是API调用，则需要判断是否需要调整阈值或者单独放行固定服务器的调用。
status:499	客户端发起请求，服务端未返回数据，超过客户端设置的等待时间后，客户端主动断链，服务端返回给客户端该状态码		· 检查源站是否异常，如响应缓慢，数据库存在大量慢查询。 · 存在攻击将源站资源占满。
status:500	（Internal Server Error）服务器内部错误，无法完成请求		建议检查源站处理资源负载、数据库等情况。
status:502	（Bad Gateway）错误网关， 服务器作为网关或代理，从上游服务器收到无效响应。一般由于回源网络质量变差、回源链路有访问控制拦截回源请求导致源站无响应		· 建议检查回源网络链路、回源链路中间的访问控制策略、源站处理资源负载、数据库等情况。 · 检查源站是否拦截了WAF回源IP的请求。
status:503	（Service Unavailable）服务不可用，由于超载或停机维护，服务器目前无法使用		建议检查源站是否异常。

监控指标	指标含义/触发原因	建议阈值	处理建议
status:504	（Gateway Timeout）网关超时，服务器作为网关或代理，但是没有及时从上游服务器收到请求		可能原因如下： · 服务器无法响应，负载过高。 · 源站丢弃请求没有reset。 · 协议通讯不成功。

3.7 常用SQL语句

本文介绍了使用Web应用防火墙日志服务查询/分析具体监控指标时用到的SQL查询语句。

使用Web应用防火墙日志服务发起查询/分析时常用的监控指标包括以下内容，您可以单击关注的指标，查看对应的SQL语句。关于监控指标的更多信息，请参见常用监控指标。

- *request_time_msec*
- *upstream_response_time*
- *ssl_handshake_time*
- *200*
- *status:302 and block_action:tmd/status:200 and block_action:tmd*
- *200 and block_action:‘antifraud’*
- *status:404*
- *status:405 and aliwaf_action='block'*
- *status:405 and aliwaf_action='acl'*
- *status:444*
- *status:499*
- *status:500*
- *status:502*
- *status:503*
- *status:504*

request_time_msec

指标释义：客户端请求到返回结果的请求耗时。

```
* |SELECT user_id,host,round(round(request_time_cnt*1.0000/countall,4
)*100,2)
as percent FROM  (select user_id,host,count_if(request_time_msec>500)
AS request_time_cnt ,COUNT(*)  as countall from log group by user_id,
host)
```

```
group by user_id,host,percent
```

upstream_response_time

指标释义：请求回源时，源站返回数据的响应时间。

```
* |SELECT
user_id,host,round(round(upstream_response_time_cnt*1.0000/countall,4
)*100,2)
as percent FROM  (select
user_id,host,count_if(upstream_response_time>500) AS
upstream_response_time_cnt ,COUNT(*)  as countall from log group by
user_id,host) group by user_id,host,percent
```

ssl_handshake_time

指标释义：HTTPS协议请求时，客户端与WAF的SSL握手时间。

```
* |SELECT
user_id,host,round(round(ssl_handshake_time_cnt*1.0000/countall,4)*100
,2) as
percent FROM  (select user_id,host,count_if(ssl_handshake_time>10) AS
ssl_handshake_time_cnt ,COUNT(*)  as countall from log group by
user_id,host) group by user_id,host,percent
```

200

指标释义：服务器已成功处理请求，返回了请求的数据。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as Rate_502,
round(round(status_503*1.0000/countall,4)*100,2)
as Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405) as status_405,count_if(status=444) as
```

```
status_444,count_if(status=499) as status_499,count_if(status=500) as
status_500,count_if(status=502)
as status_502,count_if(status=503) as status_503,count_if(status=504)
as
status_504,COUNT(*)  as countall from log group by user_id,host))
where  countall>120 order by Rate_200 DESC  limit 5
```

status:302 and block_action:tmd/status:200 and block_action:tmd

指标释义：人机校验JS请求状态码（302表示默认策略，200表示手动策略）。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as Rate_444,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as
Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as Rate_503,
round(round(status_504*1.0000/countall,4)*100,2)
as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200 and

block_action:tmd

) as status_200,count_if(status=302 and

block_action:tmd

) as
status_302,count_if(status=404) as status_404,count_if(status=405) as
status_405,count_if(status=444) as status_444,count_if(status=499) as
status_499,count_if(status=500) as status_500,count_if(status=502) as
status_502,count_if(status=503) as status_503,count_if(status=504) as
status_504,COUNT(*)  as countall from log group by user_id,host))
where  countall>120 order by Rate_200 DESC  limit 5
```

200 and block_action: ‘antifraud’

指标释义：数据风控拦截。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
```

```
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302
, round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as
Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as
Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200 and block_action:‘
antifraud’) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405) as status_405,count_if(status=444) as
status_444,count_if(status=499) as status_499,count_if(status=500) as
status_500,count_if(status=502) as status_502,count_if(status=503) as
status_503,count_if(status=504) as status_504,COUNT(*)  as countall
from
log group by user_id,host)) where  countall>120 order by Rate_200
DESC  limit 5
```

status:404

指标释义：服务器找不到请求的资源。

```
*|select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_500 as "500比例",Rate_502 as "502比例",Rate_503
as "503比例",Rate_504 as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_500,
status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_405,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as
Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as
Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as
Rate_504,status_200,status_302,status_404,status_405,status_500,
status_502,status_503,status_504,countall
```

```
from (select user_id,host,count_if(status=200) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405) as status_405,count_if(status=499) as
status_499,count_if(status=500) as status_500,count_if(status=502) as
status_502,count_if(status=503) as status_503,count_if(status=504) as
status_504,COUNT(*)  as countall from log group by user_id,host))
where  countall>120 order by Rate_404 DESC  limit 5
```

status:405 and aliwaf_action='block'

指标释义：被Web应用防护规则拦截。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as "aveQPS",status_200,status_302,status_404
,status_405,status_444,status_499,status_500,status_502,status_503,
status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as
Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as
Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as Rate_504
,status_200,status_302,status_404,status_405,status_444,status_499,
status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405 and aliwaf_action='block' ) as
status_405,count_if(status=444) as status_444,count_if(status=499) as
status_499,count_if(status=500) as status_500,count_if(status=502) as
status_502,count_if(status=503) as status_503,count_if(status=504) as
status_504,COUNT(*)
as countall from log group by user_id,host)) where  countall>120 order
by Rate_405 DESC  limit 5
```

status:405 and aliwaf_action='acl'

指标释义：被精准访问控制规则拦截。

```
user_id: 1111111111111 |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
```

```
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2)
as Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as
Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405 and aliwaf_action='acl') as
status_405,count_if(status=444) as status_444,count_if(status=499) as
status_499,count_if(status=500) as status_500,count_if(status=502) as
status_502,count_if(status=503) as status_503,count_if(status=504) as
status_504,COUNT(*)  as countall from log group by user_id,host))
where
countall>120 order by Rate_405 DESC  limit 5
```

status:444

指标释义：被WAF CC自定义规则拦截。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as
Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as Rate_503,
round(round(status_504*1.0000/countall,4)*100,2)
as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
```

```
from (select user_id,host,count_if(status=200) as status_200,count_if(
status=302)
as status_302,count_if(status=404) as status_404,count_if(status=405)
as
status_405,count_if(status=444) as status_444,count_if(status=499) as
status_499,count_if(status=500) as status_500,count_if(status=502) as
status_502,count_if(status=503) as status_503,count_if(status=504) as
status_504,COUNT(*)  as countall from log group by user_id,host))
where  countall>120 order by Rate_444 DESC  limit 5
```

status:499

指标释义：客户端请求，服务端未返回数据，超时后，客户端主动断链，服务端返回给客户端该状态码。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as
Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as
Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405) as status_405,count_if(status=444) as
status_444,count_if(status=499) as status_499,count_if(status=500) as
status_500,count_if(status=502) as status_502,count_if(status=503) as
status_503,count_if(status=504) as status_504,COUNT(*)  as countall
from
log group by user_id,host)) where  countall>120 order by Rate_499
DESC  limit 5
```

status:500

指标释义：（Internal Server Error）服务器内部错误，无法完成请求。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
```

```
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as
Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as
Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405) as status_405,count_if(status=444) as
status_444,count_if(status=499) as status_499,count_if(status=500) as
status_500,count_if(status=502) as status_502,count_if(status=503) as
status_503,count_if(status=504) as status_504,COUNT(*)  as countall
from
log group by user_id,host)) where  countall>120 order by Rate_500
DESC  limit 5
```

status:502

指标释义：（Bad Gateway）错误网关， 服务器作为网关或代理，从上游服务器收到无效响应。一般由于回源网络质量变差、回源链路有访问控制拦截回源请求导致源站无响应。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
```

```
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as Rate_502,
round(round(status_503*1.0000/countall,4)*100,2)
as Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405) as status_405,count_if(status=444) as
status_444,count_if(status=499) as status_499,count_if(status=500) as
status_500,count_if(status=502)
as status_502,count_if(status=503) as status_503,count_if(status=504)
as
status_504,COUNT(*)  as countall from log group by user_id,host))
where  countall>120 order by Rate_502 DESC  limit 5
```

status:503

指标释义：（Service Unavailable）服务不可用，由于超载或停机维护，服务器目前无法使用。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as
Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as
Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405)
as status_405,count_if(status=444) as status_444,count_if(status=499)
as
status_499,count_if(status=500) as status_500,count_if(status=502) as
status_502,count_if(status=503) as status_503,count_if(status=504) as
status_504,COUNT(*)
as countall from log group by user_id,host)) where  countall>120 order
```

```
by Rate_503 DESC  limit 5
```

status:504

指标释义：（Gateway Timeout） 网关超时，服务器作为网关或代理，但是没有及时从上游服务器收到请求。

```
* |select user_id,host as "域名",Rate_200 as
"200比例",Rate_302 as "302比例",Rate_404 as "404比例",Rate_405
as "405比例",Rate_444 as "444比例",Rate_499 as "499比例",Rate_500
as "500比例",Rate_502 as "502比例",Rate_503 as "503比例",Rate_504
as "504比例",countall/60 as
"aveQPS",status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from(SELECT user_id,host,round(round(status_200*1.0000/countall,4)*100
,2) as
Rate_200,round(round(status_302*1.0000/countall,4)*100,2) as Rate_302,
round(round

(status_404*1.0000/countall,4)*100,2) as
Rate_404,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_405,round(round

(status_405*1.0000/countall,4)*100,2) as
Rate_444,round(round

(status_405*1.0000/countall,4)*100,2)
as Rate_499,round(round(status_500*1.0000/countall,4)*100,2) as
Rate_500,round(round(status_502*1.0000/countall,4)*100,2) as
Rate_502,round(round(status_503*1.0000/countall,4)*100,2) as
Rate_503,round(round(status_504*1.0000/countall,4)*100,2) as
Rate_504,status_200,status_302,status_404,status_405,status_444,
status_499,status_500,status_502,status_503,status_504,countall
from (select user_id,host,count_if(status=200) as
status_200,count_if(status=302) as status_302,count_if(status=404) as
status_404,count_if(status=405) as status_405,count_if(status=444) as
status_444,count_if(status=499) as status_499,count_if(status=500) as
status_500,count_if(status=502) as status_502,count_if(status=503) as
status_503,count_if(status=504) as status_504,COUNT(*)  as countall
from
log group by user_id,host)) where  countall>120 order by Rate_504 DESC

limit 5
```

4 WAF接入配置最佳实践

将网站域名接入云盾Web应用防火墙（Web Application Firewall，简称WAF），能够帮助您的网站防御OWASP TOP10常见Web攻击和恶意CC攻击流量，避免网站遭到入侵导致数据泄露，全面保障您网站的安全性和可用性。

您可以参考本文中的接入配置和防护策略最佳实践，在各类场景中使用云盾Web应用防火墙更好地保护您的网站。

正常网站业务接入场景

业务梳理

首先，建议您对所需接入WAF进行防护的业务情况进行全面梳理，帮助您了解当前业务状况和具体数据，为后续配置WAF的防护策略提供依据。

梳理项	说明
网站和业务信息	
网站/应用业务每天的流量峰值情况，包括Mbps、QPS	**判断风险时间点，并且可作为WAF实例的业务带宽和业务QPS规格的选择依据。**
业务的主要用户群体（例如，访问用户的主要来源地区）	**判断非法攻击来源，后续可使用地区封禁功能屏蔽非法来源地区。**
业务是否为C/S架构	**如果是C/S架构，进一步明确是否有App客户端、Windows客户端、Linux客户端、代码回调或其他环境的客户端。**
源站是否部署在非中国大陆地域	**判断所配置的实例是否符合最佳网络架构。**
源站服务器的操作系统（Linux、Windows）和所使用的Web服务中间件（Apache、Nginx、IIS等）	**判断源站是否存在访问控制策略，避免源站误拦截WAF回源IP转发的流量。**
域名使用协议	**判断所使用的通信协议WAF是否支持。**
业务端口	**判断源站业务端口是否在*WAF*支持的端口范围内。**
业务是否有获取并校验真实源IP机制	**接入WAF后，真实源IP会发生变化。请确认是否要在源站上调整获取真实源IP配置，避免影响业务。**
业务是否使用TLS 1.0或弱加密套件	**判断业务使用的加密套件是否支持。**
业务是否需要支持IPv6协议	**WAF企业版和旗舰版实例已支持IPv6协议。**

梳理项	说明
（针对HTTPS业务）业务是否使用双向认证	WAF虚拟独享集群目前已支持双向认证。如果您的HTTPS业务采用双向认证，请通过工单或WAF安全专家服务钉钉群联系阿里云技术支持人员。
（针对HTTPS业务）客户端是否支持SNI标准	对于支持HTTPS协议的域名，接入WAF后，客户端和服务端都需要支持SNI标准。
（针对HTTPS业务）是否存在会话保持机制	如果业务部署了阿里云负载均衡（SLB）实例，建议开启Cookie会话保持功能。
业务交互过程	了解业务交互过程、业务处理逻辑，便于后续配置针对性防护策略。
活跃用户数量	便于后续在处理紧急攻击事件时，判断事件严重程度，以采取风险较低的应急处理措施。
业务及攻击情况	
业务类型及业务特征（例如，游戏、棋牌、网站、App等业务）	便于在后续攻防过程中分析攻击特征。
业务流量（入方向）	帮助后续判断是否包含恶意流量。例如，日均访问流量为100 Mbps，则超过100 Mbps时可能遭受攻击。
业务流量（出方向）	帮助后续判断是否遭受攻击，并且作为是否需要额外业务带宽扩展的参考依据。
单用户、单IP的入方向流量范围和连接情况	帮助后续判断是否可针对单个IP制定限速策略。
用户群体属性	例如，个人用户、网吧用户、或通过代理访问的用户。
业务是否遭受过大流量攻击及攻击类型	判断是否需要增加DDoS防护服务。
业务遭受过最大的攻击流量峰值	根据攻击流量峰值判断需要的DDoS防护规格。
业务是否遭受过CC攻击（HTTP Flood）	通过分析历史攻击特征，配置预防性策略。
业务遭受过最大的CC攻击峰值QPS	通过分析历史攻击特征，配置预防性策略。
业务是否提供Web API服务	如果提供Web API服务，不建议使用CC攻击紧急防护模式。通过分析API访问特征配置自定义CC攻击防护策略，避免API正常请求被拦截。
业务是否存在注册、登录、密码找回、短信接口被刷的情况	判断是否开启数据风控防护策略，并提前开启相关测试工作。
业务是否已完成压力测试	评估源站服务器的请求处理性能，帮助后续判断是否因遭受攻击导致业务发生异常。

准备工作

> **注意:**
> 在将网站业务接入WAF时，强烈建议您先使用测试业务环境进行测试，测试通过后再正式接入生产业务环境。

在将网站业务接入WAF前，您需要完成以下准备工作：

- 所需接入的网站域名清单，包含网站的源站服务器IP、端口信息等。
- 所接入的网站域名必须已完成阿里云备案。
- 如果您的网站支持HTTPS协议访问，您需要准备相应的证书和私钥信息，一般包含格式为 .crt 的公钥文件或格式为 .pem 的证书文件、格式为 .key 的私钥文件。
- 具有网站DNS域名解析管理员的账号，用于修改DNS解析记录将网站流量切换至WAF。
- 推荐在将网站业务接入前，完成压力测试。
- 检查网站业务是否已有信任的访问客户端（例如监控系统、通过内部固定IP或IP段调用的API接口、固定的程序客户端请求等）。在将业务接入后，需要将这些信任的客户端IP加入白名单。

WAF配置

1. 域名接入配置

   根据您的业务场景，参考以下接入配置指导，将您的网站域名接入WAF：

   - 单独使用*WAF*配置指导
   - 同时部署*WAF*和*DDoS*高防配置指导
   - 同时部署*WAF*和*CDN*配置指导

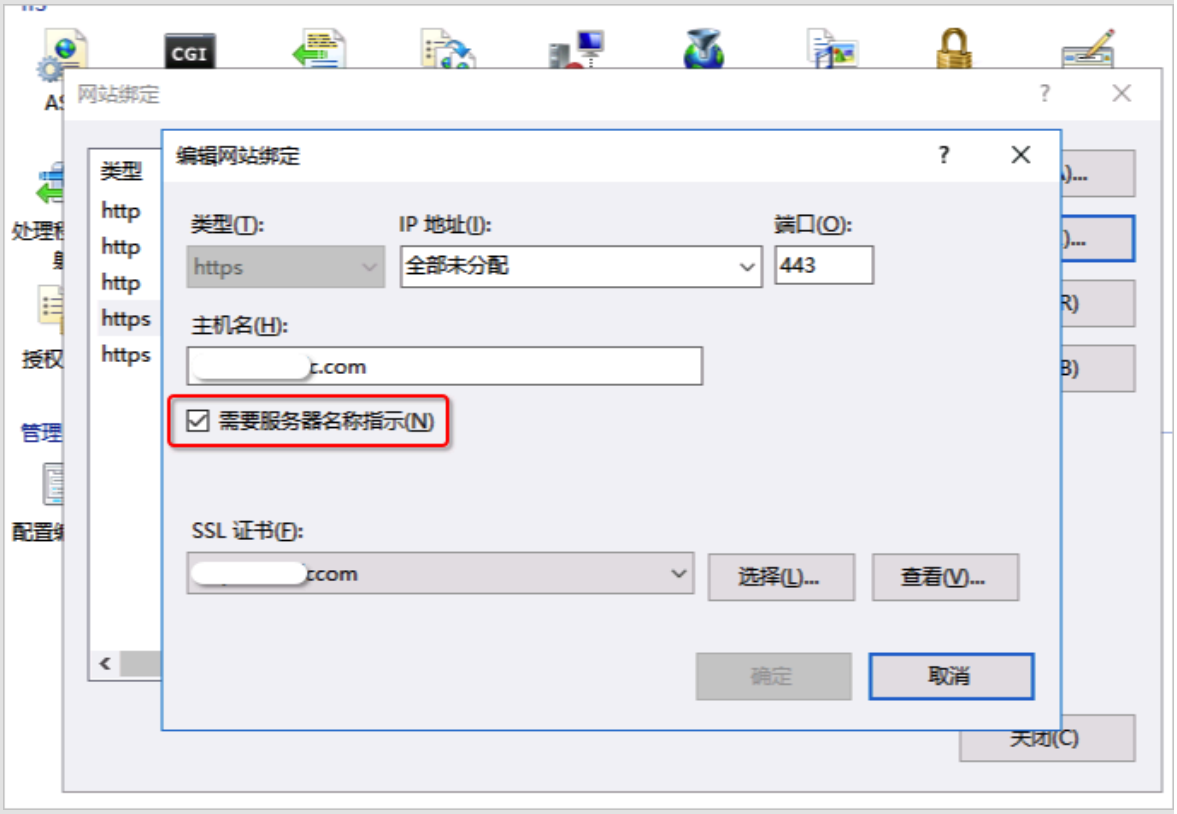
   > **说明:**
   > 如果在添加域名配置时，提示“您配置的域名已被其它用户使用”。建议您检查是否已在其它阿里云账号的WAF实例中添加与该域名冲突的配置记录。如果确实存在，您需要删除造成冲突的域名配置记录后再进行配置。

2. 源站保护配置

- 源站保护：为避免恶意攻击者绕过WAF直接攻击或入侵源站服务器，建议您完成源站保护配置。
- 标记WAF回源流量：将网站域名接入WAF进行防护后，您可以为网站域名设置流量标记。通过设置流量标记的方式，方便地标识经过WAF转发的流量，从而实现精准的源站保护（访问控制）、防护效果分析，有效防止流量绕过WAF请求源站。

说明:

如果您接入WAF的网站域名的业务源站使用的是Windows IIS Web服务，在配置HTTPS域名时，IIS默认会启用需要服务器名称指示（即SNI）。这种情况下，在将域名接入WAF后可能会出现访问空白页502的错误信息，您只需禁用该配置选项即可解决该问题。



3. 防护策略配置

参考以下推荐防护配置对已接入的网站业务进行防护：

- Web攻击防护

  一般情况下，建议选用防护模式，并选用中等规则防护策略。

> **说明:**
> 业务接入WAF防护一段时间后（一般为2-3天），如果出现网站业务的正常请求被WAF误拦截的情况，您可以通过设置自定义规则组的方式提升Web防护效果。

- CC攻击防护

  业务正常运行时，建议采用系统默认配置。

> **说明:**
> 由于CC防护的攻击紧急模式可能产生一定量的误拦截，如果您的业务为App业务或Web API服务，不建议您开启攻击紧急模式。
>
> 如果使用CC安全防护的正常模式仍发现误拦截现象，建议您使用精准访问控制功能放行特定类型请求。

> **说明:**

业务接入WAF防护一段时间后（一般为2-3天），可以通过分析业务日志数据（例如，访问URL、单个IP访问QPS情况等）评估单个IP的请求QPS峰值，提前通过自定义CC攻击防护配置限速策略，避免遭受攻击后的被动响应和临时策略配置。

当您的网站遭受大量CC攻击时，建议您开通日志服务功能。通过访问日志分析，发现恶意访问请求的特征，然后结合以下WAF的安全防护功能进行联合防御：

- **自定义CC攻击防护**：针对URL设置灵活的限速策略，有效缓解CC攻击（HTTP Flood）带来的业务影响。

  说明：

  自定义CC攻击防护的限速策略可能产生误拦截，建议您通过深度日志分析找出攻击特征，配置精准访问控制策略实现精准拦截。

- **精准访问控制**：当攻击源IP比较分散时，可以通过分析访问日志，使用精准访问控制提供的丰富字段和逻辑条件组合，灵活配置访问控制策略实现精准防护，有效降低误拦截。

  - 支持IP、URL、Referer、User Agent、Params、Header等HTTP常见参数和字段的条件组合。
  - 支持包含、不包含、等于、不等于、前缀为、前缀不为等逻辑条件，设置阻断或放行策略。

- **封禁地区**：针对全球来源IP地理位置进行自定义地域访问控制。您可以根据业务的用户分布情况，屏蔽不需要的访问来源地区。

- **数据风控**：通过风险决策引擎和人机识别算法，有效识别和拦截欺诈行为。

  说明：

  数据风控功能目前仅适用于网页/H5环境。

  一般来说，功能性页面遭恶意被刷的风险较低，可不配置数据风控策略。而对于注册、登录、密码找回、营销活动类等静态页面，建议您根据防护需求配置数据风控，有效识别和拦截欺诈行为。

  配置完成后，务必进行兼容性和业务可用性测试，避免数据风控策略配置对正常业务造成影响。

  说明：

部分页面前端代码与数据风控的JavaScript脚本可能存在兼容性问题。如果遇到此类问题，建议您使用指定页面插入JS功能，并在测试通过后开启防护，避免影响正常业务。如果您仍然无法解决，可以联系阿里云技术支持获得帮助。

- 日志功能

  在日志分析方面，WAF提供两大功能供您选择：

  - 全量日志：建议您为网站启用全量日志功能，通过全量日志您可以对网站遭受的七层网络攻击进行分析，发现其攻击行为特征。

    说明:
    全量日志功能仅支持企业版以上的WAF实例。对于按量付费WAF实例，您需要手动启用全量日志功能。

  - 日志服务：根据您的业务和预算情况，选择启用日志服务功能。开通日志服务功能，可记录更多详细的原始日志信息，同时实现更灵活的访问日志自定义分析，发现恶意请求特征。

- 监控告警

  根据您的业务情况，为网站业务设置具体的QPS、4XX、5XX告警触发阈值。通过配置WAF监控告警功能，实时感知攻击事件。

4. 本地测试

完成上述WAF配置后，建议您进行配置准确性检查和验证测试。

说明:
您可以通过修改本地系统Hosts文件方式进行测试。

表 4-1: 配置准确性检查项

编号	检查项
1	接入配置域名是否填写正确（必检项）
2	域名是否备案（必检项）
3	接入配置协议是否与实际协议一致（必检项）
4	接入配置端口是否与实际提供的服务端口一致（必检项）
5	WAF前是否有配置其它七层代理（例如，DDoS高防、CDN等）（必检项）
6	源站填写的IP是否是真实服务器IP，而不是错误地填写了高防IP或其他服务IP（必检项）
7	回源算法是否与预期一致（建议项）

编号	检查项
8	证书信息是否正确上传（必检项）
9	证书是否合法（例如，加密算法不合规、错误上传其他域名的证书等）（必检项）
10	证书链是否完整（必检项）
11	是否配置流量标记（建议项）
12	告警监控配置（建议项）
13	是否已了解按量付费实例的计费方式（必检项） 说明: 仅适用于按量付费WAF实例。

表 4-2: 业务可用性验证项

编号	检查项
1	测试业务（包括Web、App客户端、Windows客户端、Linux客户端、其他环境的客户端）是否能够正常访问（必检项）
2	测试业务登录会话保持功能是否正常（必检项）
3	观察业务返回4XX和5XX响应码的次数，确保回源IP未被拦截（必检项）
4	对于App业务，检查是否存在SNI问题（必检项）
5	是否配置后端真实服务器获取真实源IP（建议项）
6	是否配置源站保护，防止攻击者绕过WAF直接入侵源站（建议项）

5. 正式切换业务流量

必要测试项均检测通过后，建议采用灰度的方式逐个域名修改DNS解析记录，将网站业务流量切换至Web应用防火墙，避免批量操作导致业务异常。如果切换流量过程中出现异常，请快速恢复DNS解析记录。

说明:
修改DNS解析记录后，需要10分钟左右生效。

说明:

如果您域名DNS解析存在MX记录与CNAME记录冲突的情况，建议您通过A记录方式接入WAF。或者，您可以通过创建二级域名的方式区分业务，实现使用CNAME方式接入。

真实业务流量切换后，您需要再次根据上述业务可用性验证项进行测试，确保网站业务正常运行。

6. 日常运维

- 您可以参考以下最佳实践根据所需防护的具体场景，进一步配置具有针对性的防护策略：
  - *Web*攻击防护最佳实践
  - *CC*攻击防护最佳实践
- 如果您使用的是按量付费WAF实例，请仔细阅读*WAF*按量付费实例计费方式，避免出现实际产生的费用超出预算的情况。
- 为避免WAF实例遭受大量DDoS攻击触发黑洞策略，导致网站业务无法访问的情况，建议您根据实际情况选择*DDoS*防护包或*DDoS*高防产品防御DDoS攻击。
- 如果出现业务访问延时或丢包的问题，参考以下建议变更部署方式：
  - 针对源站服务器在海外、WAF实例为中国大陆地区、主要访问用户来自中国大陆地区的情况，如果用户访问网站时存在延时高、丢包等现象，可能是由于回源网络链路问题，推荐您将源站服务器部署在中国大陆地区。
  - 针对源站服务器在海外、WAF实例为海外地区、主要访问用户来自中国大陆地区的情况，如果用户访问网站时存在延时高、丢包等现象，可能存在跨网络运营商导致的访问链路不稳定，推荐您使用中国大陆地区的WAF实例。
- 如果需要删除已防护的域名配置记录，确认网站业务是否已正式接入WAF。
  - 如果尚未正式切换业务流量，直接在Web应用防火墙管理控制台中删除域名配置记录即可。
  - 如果已完成业务流量切换，删除域名配置前务必前往域名DNS解析服务控制台，修改域名解析记录将业务流量切换回源站服务器。

  说明：
  - 删除域名配置前，请务必确认域名的DNS解析已经切换至源站服务器。
  - 删除域名配置后，云盾Web应用防火墙将无法再为您的域名提供专业级安全防护。

业务遭受攻击时的紧急接入场景

如果您的网站业务已经遭受攻击，建议您在将业务接入WAF前执行以下操作：

- 遭受Web攻击入侵

  1. 为避免二次入侵，务必先清理入侵者植入的恶意文件并修复漏洞。

     > 说明:
     > 如果您需要专业的安全运维人员帮助，请选购应急响应服务。

  2. 已对业务系统进行安全加固。
  3. 将网站业务接入WAF。

     > 说明:
     > 根据实际情况将Web攻击防护策略调至高级规则，有效防御Web攻击行为导致的入侵事件。

- 遭受CC攻击或爬虫攻击

  在将网站业务接入WAF后，需要通过日志功能分析网站访问日志，判断攻击特征后进行针对性的防护策略配置。

> 注意:
> 如果您使用的是按量付费WAF实例，请仔细阅读WAF按量付费实例计费方式，避免出现实际产生的费用超出预算的情况。

安全专家服务

购买开通云盾Web应用防火墙后，您可以在管理控制台中通过钉钉扫描二维码直接联系阿里云安全服务专家。

安全专家将针对您的业务场景提供WAF接入配置指导、安全攻击分析和防御相关安全服务，基于业务实际情况帮助您更好地使用WAF对业务进行安全防护，保障您业务的网络应用安全。

说明:

为了便于快速分析和解决问题，在远程技术支持服务过程中，可能需要您授权阿里云安全专家查看业务数据。所有安全专家服务人员都将严格遵循服务授权和保密原则，防止您的信息泄露。

5 源站保护

正确配置源站ECS的安全组和SLB的白名单，可以防止黑客直接攻击您的源站IP。本文介绍了源站服务器保护的相关配置方法。

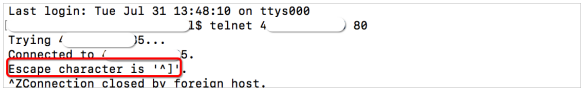
背景信息

> **说明:**
> 源站保护不是必须的。没有配置源站保护不会影响正常业务转发，但可能导致攻击者在源站IP暴露的情况下，绕过Web应用防火墙直接攻击您的源站。

如何确认源站泄露?

您可以在非阿里云环境直接使用Telnet工具连接源站公网IP地址的业务端口，观察是否建立连接成功。如果可以连通，表示源站存在泄露风险，一旦黑客获取到源站公网IP就可以绕过WAF直接访问；如果无法连通，则表示当前不存在源站泄露风险。

例如，测试已接入WAF防护的源站IP 80端口和800端口是否能成功建立连接，测试结果显示端口可连通，说明存在源站泄露风险。



> **注意:**
> 配置安全组存在一定风险。在配置源站保护前，请注意以下事项：
>
> - 请确保该ECS或SLB实例上的所有网站域名都已经接入Web应用防火墙。
> - 当Web应用防火墙集群出现故障时，可能会将域名访问请求旁路回源至源站，确保网站正常访问。这种情况下，如果源站已配置安全组防护，则可能会导致源站无法从公网访问。
> - 当Web应用防火墙集群扩容新的回源网段时，如果源站已配置安全组防护，可能会导致频繁出现5xx错误。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 前往管理 > 网站配置页面，选择WAF实例所在的地区。
3. 单击Web应用防火墙回源IP网段列表，查看Web应用防火墙所有回源IP段。

> **说明:**

WAF回源IP网段会定期更新，请关注定期变更通知。及时将更新后的回源IP网段添加至相应的安全组规则中，避免出现误拦截。

4. 在WAF回源IP段对话框，单击复制IP段，复制所有回源IP。

5. 参照以下步骤，配置源站只允许WAF回源IP进行访问。

   - 源站是ECS

     a. 前往*ECS* 实例列表，定位到需要配置安全组的ECS实例，单击其操作列下的管理。

     b. 切换到本实例安全组页面。

     c. 选择目标安全组，并单击其操作列下的配置规则。

     d. 单击添加安全组规则，并配置如下安全组规则：

     说明：
     安全组规则授权对象支持输入“10.x.x.x/32”格式的IP网段，且支持添加多组授权对象（以“,”隔开），最多支持添加10组授权对象。

     - 网卡类型：内网

       说明：

如果ECS实例的网络类型为经典网络，则网卡类型需设置为公网。

- 规则方向：入方向
- 授权策略：允许
- 协议类型：TCP
- 授权类型：地址段访问
- 端口范围：80/443
- 授权对象：粘贴步骤4中复制的所有Web应用防火墙回源IP段
- 优先级：1

e. 为所有Web应用防火墙回源IP段添加安全组规则后，再添加如下安全组规则，拒绝公网入方向的所有IP段访问，优先级为100。

- 网卡类型：内网

说明：

如果ECS实例的网络类型为经典网络，则网卡类型需设置为公网。

- 规则方向：入方向
- 授权策略：拒绝
- 协议类型：TCP
- 端口范围：80/443
- 授权类型：地址段访问
- 授权对象：0.0.0.0/0
- 优先级：100

说明：

如果本安全组防护的服务器还与其他的IP或应用存在交互，需要将这些交互的IP和端口通过安全组一并加白放行，或者在最后添加一条优先级最小的全端口放行策略。

- 源站是SLB

  通过类似的方式，将Web应用防火墙的回源IP加入相应负载均衡实例的白名单，具体设置方法请参见*#unique_53*。

  a. 登录负载均衡管理控制台，前往访问控制页面，单击创建访问控制策略组。
  b. 填写策略组名称，添加WAF回源IP网段，单击确定。
  c. 在实例管理页面，选择相应的负载均衡实例。
  d. 在监听页签中，选择端口监听记录，单击更多 > 设置访问控制。
  e. 启用访问控制，选择访问控制方式为白名单，并选择所创建的WAF回源IP网段的访问控制策略组，单击确定。

后续步骤

源站保护配置完成后，您可以通过测试已接入WAF防护的源站IP80端口和8080端口是否能成功建立连接验证配置是否生效。如果显示端口无法直接连通，但网站业务仍可正常访问，则表示源站保护配置成功。

6 获取访问者真实IP

本文介绍了业务接入Web应用防火墙（WAF）后，如何获取访问者的真实IP地址。

在大部分实际业务场景中，网站访问请求并不是简单地从用户（访问者）的浏览器直达网站的源站服务器，中间可能经过所部署的CDN、高防IP、WAF等代理服务器。例如，网站可能采用这样的部署架构：用户 > CDN/高防IP/WAF > 源站服务器。这种情况下，访问请求在经过多层加速或代理转发后，源站服务器该如何获取发起请求的真实客户端IP?

一般情况下，透明的代理服务器在将用户的访问请求转发到下一环节的服务器时，会在HTTP的请求头中添加一条X-Forwarded-For记录，用于记录用户的真实IP，其记录格式为`X-Forwarded-For:用户IP`。如果期间经历多个代理服务器，则X-Forwarded-For将以该格式记录用户真实IP和所经过的代理服务器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，常见的Web应用服务器可以使用X-Forwarded-For的方式获取访问者真实IP。以下分别针对Nginx、IIS 6、IIS 7、Apache和Tomcat服务器，介绍相应的X-Forwarded-For配置方案。

> **注意:**
> **在开始配置前，务必对现有环境进行备份，包括ECS快照备份和Web应用服务器配置文件备份。**

Nginx配置方案

1. 确认已安装http_realip_module模块

为实现负载均衡，Nginx使用http_realip_module模块来获取真实IP。

您可以通过执行`# nginx -V | grep http_realip_module`命令查看是否已安装该模块。如未安装，则需要重新编译Nginx服务并加装该模块。

> **说明:**
> **一般情况下，如果通过一键安装包安装Nginx服务器，默认不安装该模块。**

参考以下方法，安装http_realip_module模块。

```
wget http://nginx.org/download/nginx-1.12.2.tar.gz
tar zxvf nginx-1.12.2.tar.gz
cd nginx-1.12.2
./configure --user=www --group=www --prefix=/alidata/server/nginx --
with-http_stub_status_module --without-http-cache --with-http_ssl_m
odule --with-http_realip_module
make
make install
kill -USR2 `cat /alidata/server/nginx/logs/nginx.pid`
```

```
kill -QUIT `cat /alidata/server/nginx/logs/ nginx.pid.oldbin`
```

2. 修改Nginx对应server的配置

打开default.conf配置文件，在location / {}中添加以下内容：

说明:

其中，ip_range1，2，...，x指WAF的回源IP地址，需要分多条分别添加。

```
set_real_ip_from ip_range1;
set_real_ip_from ip_range2;
...
set_real_ip_from ip_rangex;
real_ip_header    X-Forwarded-For;
```

3. 修改日志记录格式 log_format

*log_format*一般在nginx.conf配置文件中的http配置部分。在*log_format*中，添加*x-forwarded-for*字段，替换原来*remote-address*字段，即将*log_format*修改为以下内容：

```
log_format  main  '$http_x_forwarded_for - $remote_user [$time_local
] "$request" ' '$status $body_bytes_sent "$http_referer" ' '"$
http_user_agent" ';
```

完成以上操作后，执行nginx -s reload命令重启Nginx服务。配置生效后，Nignx服务器即可通过X-Forwarded-For的方式记录访问者真实IP。

IIS 6配置方案

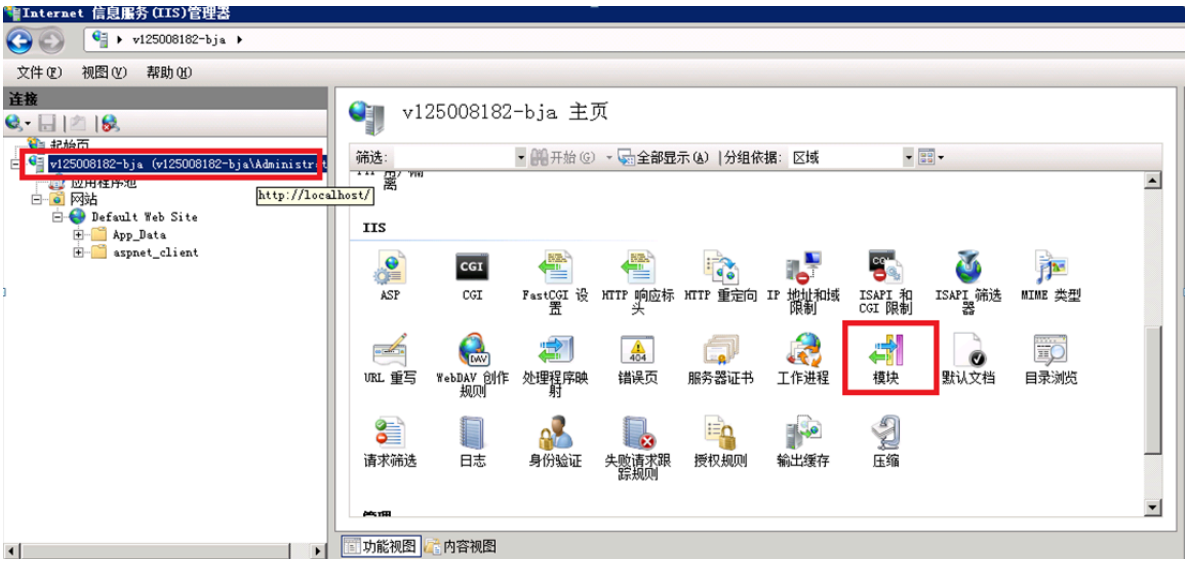
您可以通过安装*F5XForwardedFor.dll*插件，从IIS 6服务器记录的访问日志中获取访问者真实IP地址。

1. **根据您服务器的操作系统版本将*x86\Release*或者*x64\Release*目录中的*F5XForwardedFor.dll*文件拷贝至指定目录（例如，*C:\ISAPIFilters*），同时确保IIS进程对该目录有读取权限。**
2. **打开IIS管理器，找到当前开启的网站，在该网站上右键选择属性，打开属性页。**
3. **在属性页切换至ISAPI筛选器，单击添加。**
4. **在添加窗口下，配置以下参数，并单击确定。**
   - **筛选器名称：F5XForwardedFor**
   - **可执行文件：F5XForwardedFor.dll的完整路径，例如*C:\ISAPIFilters\F5XForwardedFor.dll***
5. **重启 IIS 服务器，等待配置生效。**

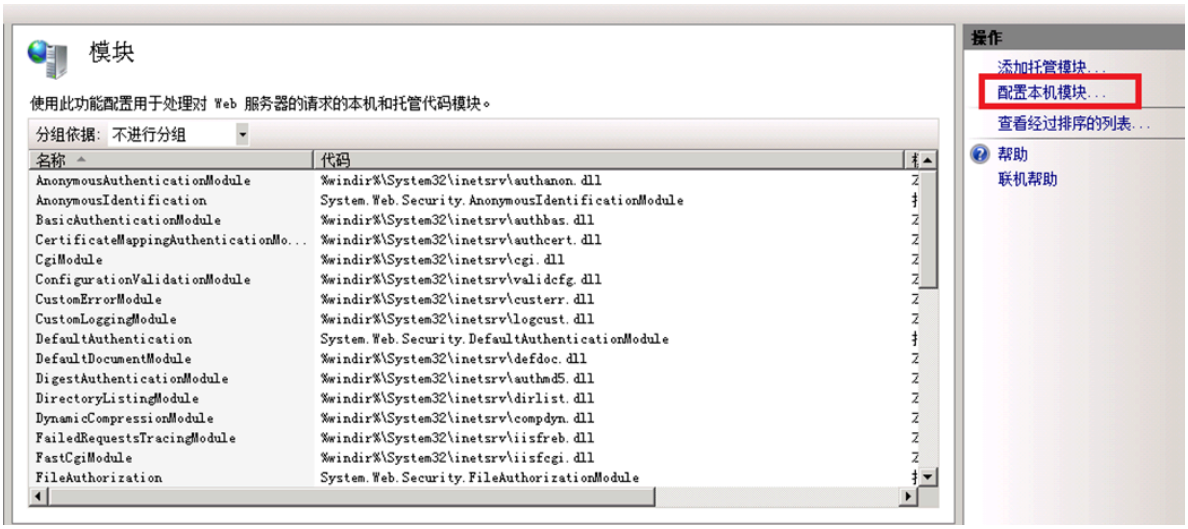
IIS 7配置方案

您可以通过安装*F5XForwardedFor* 模块模块，获取访问者真实IP地址。

1. **根据服务器的操作系统版本将*x86\Release*或者*x64\Release*目录中的*F5XFFHttpModule.dll*和*F5XFFHttpModule.ini*文件拷贝到指定目录（例如，*C:\x_forwarded_for\x86*或*C:\x_forwarded_for\x64*），并确保IIS进程对该目录有读取权限。**
2. **在IIS服务器选项中，双击打开模块。**



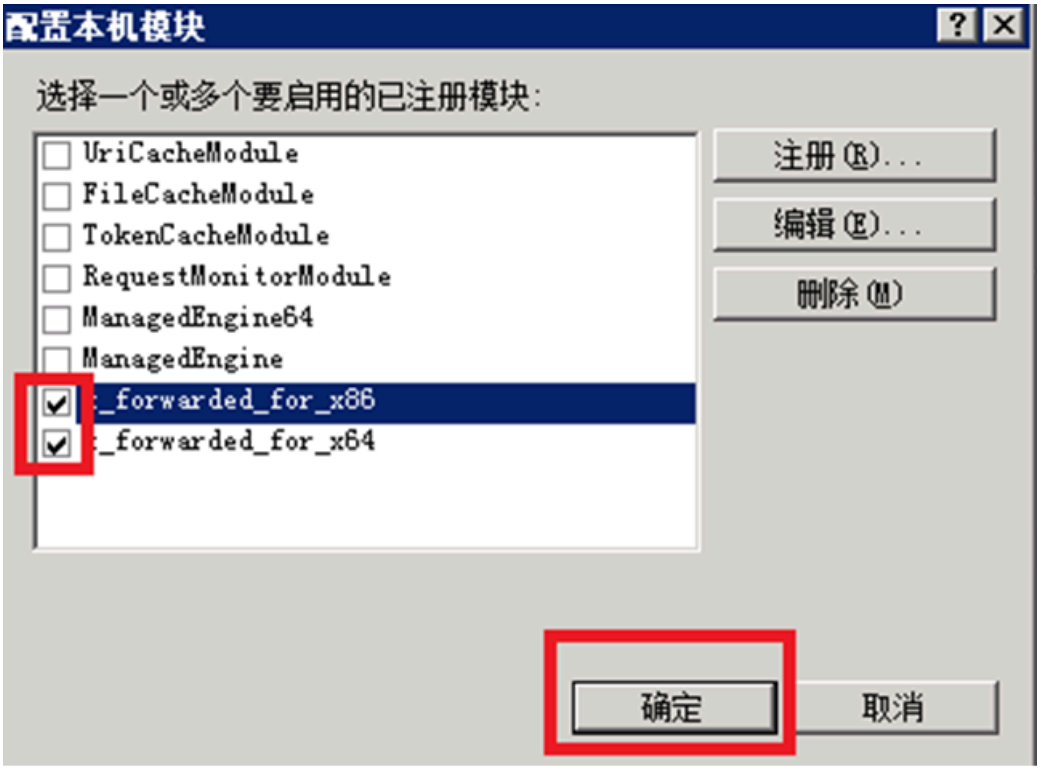
3. **单击配置本机模块。**



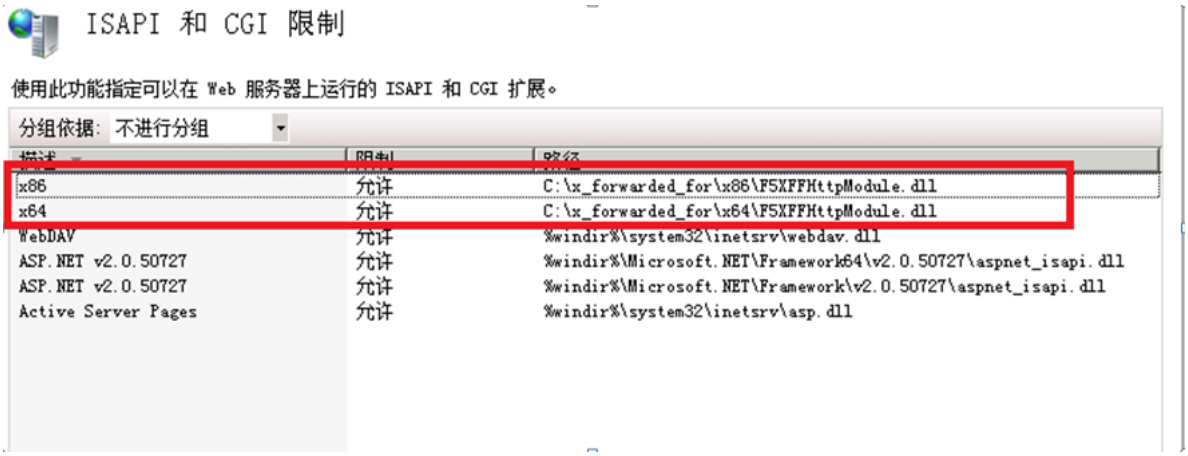
4. 在配置本机模块对话框中，单击注册，分别注册已下载的DLL文件。

   - 注册模块 x_forwarded_for_x86
     - 名称：x_forwarded_for_x86
     - 路径：*C:\x_forwarded_for\x86\F5XFFHttpModule.dll*
   - 注册模块 x_forwarded_for_x64
     - 名称：x_forwarded_for_x64
     - 路径：*C:\x_forwarded_for\x64\F5XFFHttpModule.dll*

5. 注册完成后，勾选新注册的模块（x_forwarded_for_x86 和 x_forwarded_for_x64）并单击确定。



6. 在API 和CGI限制中，分别添加已注册的DLL，并将其限制改为允许。



7. 重启IIS服务器，等待配置生效。

Apache配置方案

Windows操作系统

在Apache 2.4及以上版本的安装包中已自带remoteip_module模块文件（mod_remoteip.so），您可以通过该模块获取访问者真实IP地址。

1. 在Apache的extra配置文件夹（*conf/extra/*）中，新建httpd-remoteip.conf配置文件。

   说明：

   为减少直接修改httpd.conf配置文件的次数，避免因操作失误而导致的业务异常，通过引入remoteip.conf配置文件的方式加载相关配置。

2. 在httpd-remoteip.conf配置文件中，添加以下访问者真实IP的获取规则。

```
#加载mod_remoteip.so模块
LoadModule remoteip_module modules/mod_remoteip.so
#设置RemoteIPHeader头部
RemoteIPHeader X-Forwarded-For
#设置回源IP段
RemoteIPInternalProxy 112.124.159.0/24 118.178.15.0/24 120.27.173.0
/24 203.107.20.0/24 203.107.21.0/24 203.107.22.0/24 203.107.23.0/24
47.97.128.0/24 47.97.129.0/24 47.97.130.0/24 47.97.131.0/24
```

3. 修改*conf/httpd.conf*配置文件，插入httpd-remoteip.conf配置文件。

```
Include conf/extra/httpd-remoteip.conf
```

4. 在httpd.conf配置文件中，修改日志格式。

```
LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}
i\"" combined
LogFormat "%a %l %u %t \"%r\" %>s %b" common
```

5. 重启Apache服务，使配置生效。

Linux操作系统

您可以通过安装Apache的mod_rpaf第三方模块，获取访问者真实IP地址。

1. 执行以下命令，安装mod_rpaf模块。

```
wget http://stderr.net/apache/rpaf/download/mod_rpaf-0.6.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/alidata/server/httpd/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0
.c
```

2. 修改Apache配置文件*/alidata/server/httpd/conf/httpd.conf*，在文件最后添加以下内容：

   说明：

   其中，`RPAFproxy_ips ip`地址不是负载均衡提供的公网IP。具体IP可参考Apache的日志，通常会有两个IP地址。

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips ip地址
```

```
RPAFheader X-Forwarded-For
```

3. 添加完成后，执行以下命令重启Apache服务，使配置生效。

```
/alidata/server/httpd/bin/apachectl restart
```

mod_rpaf模块配置示例

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 10.242.230.65 10.242.230.131
RPAFheader X-Forwarded-For
```

Tomcat配置方案

通过启用Tomcat的X-Forwarded-For功能，获取访问者真实IP地址。

打开*tomcat/conf/server.xml*配置文件，将AccessLogValve日志记录功能部分修改为以下内容：

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory
="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T
" resolveHosts="false"/>
```

7 Web防护功能最佳实践

本文介绍了阿里云云盾Web应用防火墙的Web攻击防护最佳实践，主要从应用场景、防护策略、防护效果、规则更新四个方面进行介绍。

应用场景

Web应用防火墙（Web Application Firewall，简称WAF）主要提供针对Web攻击的防护，例如SQL注入、XSS、远程命令执行、Webshell上传等攻击。关于Web攻击的详细信息，请参见 *OWASP 2017 Top 10*。

> **说明:**
> **主机层服务的安全问题（例如Redis、MySQL未授权访问等）导致的服务器入侵不在WAF的防护范围之内。**

防护策略

在将网站成功接入WAF防护后，登录Web应用防火墙控制台，在管理 > 网站配置页面选择已防护的网站，并单击防护配置，即可查看Web应用攻击防护的防护状态，如图所示。

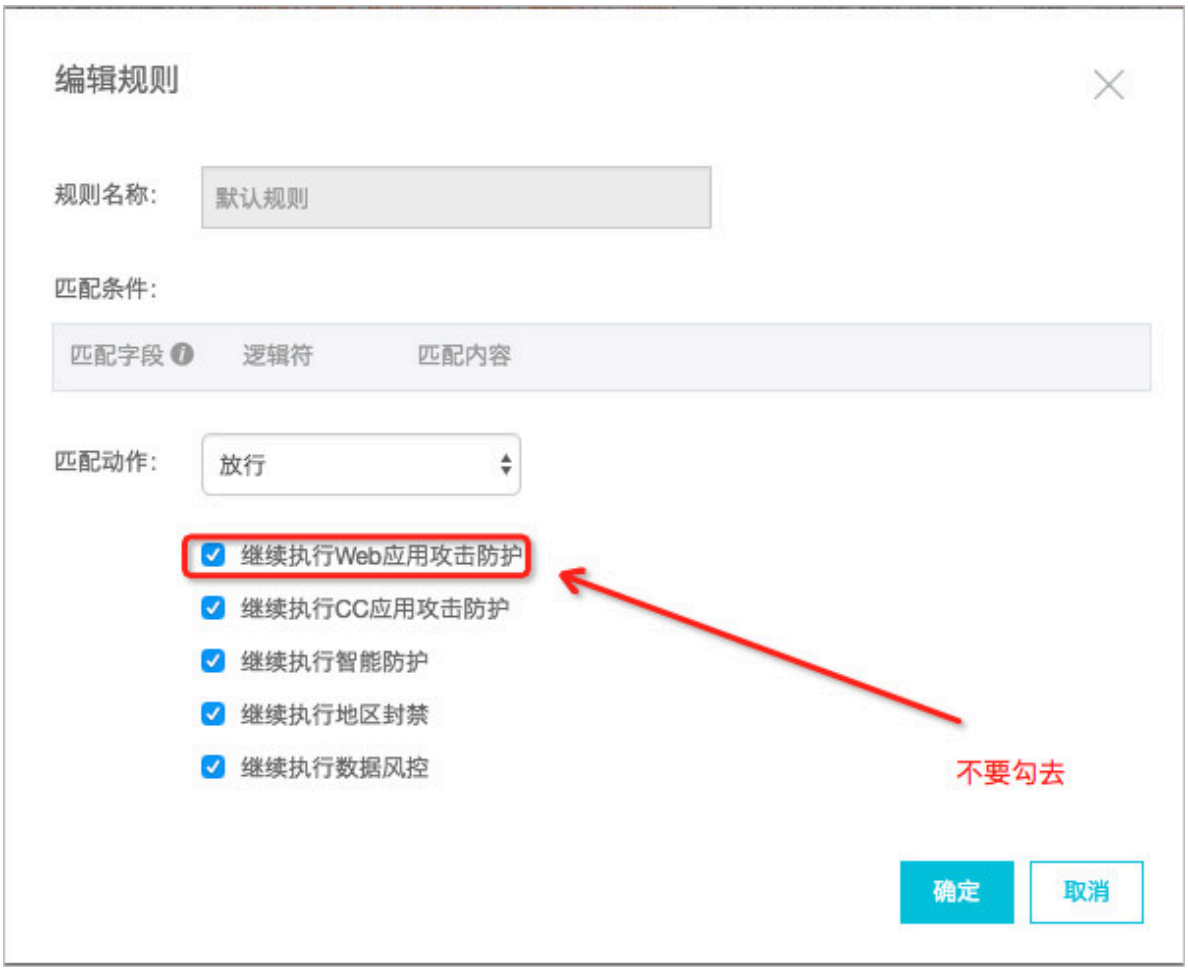
Web应用攻击防护功能默认开启，并使用正常模式的防护规则策略。其中，

- **状态：是否启用Web应用攻击防护模块。**
- **模式：分为防护和预警两种模式。**
  - **防护模式表示当遭受Web攻击时，WAF自动拦截攻击请求，并在后台记录攻击日志。**
  - **预警模式表示当遭受Web攻击时，WAF不会拦截攻击请求，仅在后台记录攻击日志。**
- **防护规则策略：分为宽松、正常、严格三种模式，仅在启用防护模式后生效。**
  - **宽松防护规则策略的防护粒度较粗，只拦截攻击特征比较明显的请求。**
  - **正常防护规则策略的防护粒度较宽松且防护规则策略精准，可以拦截常见的具有绕过特征的攻击请求。**
  - **严格防护规则策略的防护粒度最精细，可以拦截具有复杂的绕过特征的攻击请求。**

使用建议：

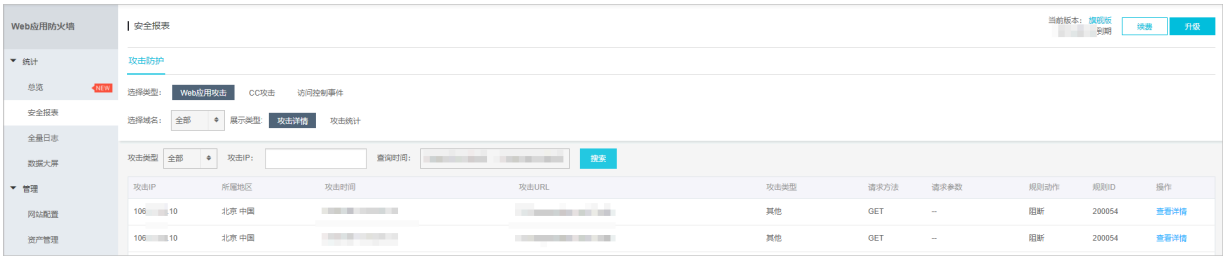
- **如果您对自己的业务流量特征还不完全清楚，建议先切换到预警模式进行观察。一般情况下，建议您观察一至两周，然后分析预警模式下的攻击日志。**
  - **如果没有发现任何正常业务流量被拦截的记录，则可以切换到防护模式启用拦截防护。**
  - **如果发现攻击日志中存在正常业务流量，可以联系阿里云安全专家沟通具体的解决方案。**
- **PHPMyAdmin、开发技术类论坛接入WAF防护可能会存在误拦截的问题，建议联系阿里云安全专家沟通具体的解决方案。**
- **业务操作方面应注意以下问题：**
  - **正常业务的HTTP请求中尽量不要直接传递原始的SQL语句、JAVA SCRIPT代码。**
  - **正常业务的URL尽量不要使用一些特殊的关键字（UPDATE、SET等）作为路径，例如`www.example.com/abc/update/mod.php?set=1`。**
  - **如果业务中需要上传文件，不建议直接通过Web方式上传超过50M的文件，建议使用OSS或者其他方式上传。**

- **开启WAF的Web应用攻击防护功能后，不要禁用默认精准访问控制规则中的Web防护通用防护模块，如图所示。**



防护效果

开启WAF的Web应用攻击防护功能后，您可以在统计 > 安全报表页面，查看攻击的拦截日志，如图所示。



在安全报表页面，您可以查看昨天、当天、7天以及一个月内的攻击详情。同时，单击查看攻击详情，可以查看具体的攻击信息，如图所示。

该截图中的拦截日志即为一条已被WAF拦截的SQL注入攻击请求。

说明:

如果您发现WAF误拦截了正常业务流量，建议您先通过精准访问控制功能对受影响的URL配置白名单策略，然后联系阿里云安全专家沟通具体解决方案。

规则更新

对于互联网披露的已知漏洞和未披露的0day漏洞，云盾WAF将及时完成防护规则的更新，并发布防护公告。

您可以登录*Web*应用防火墙控制台，前往设置 > 产品信息页面，查看最新发布的防护公告，如图所示。

说明:

Web攻击往往存在不止一种概念证明方法（Proof of Concept，简称PoC），阿里云安全专家会对漏洞原理进行深度分析从而确保发布的Web防护规则覆盖已公开和未公开的各种漏洞利用方式。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效的应对漏洞及黑客攻击，详情请关注安全管家服务。

8 通过设置自定义规则组提升Web防护效果

当您发现网站业务的正常请求被WAF误拦截时，您可以通过设置自定义规则组的方式避免该类误拦截。

背景信息

当业务正常请求被WAF的Web应用攻击防护功能误拦截时，您首先要确定触发本次拦截的Web应用防护规则ID，然后通过为该网站域名设置自定义规则组的方式移除该规则，使WAF针对该网站业务不再拦截同样的正常请求。

说明:
自定义规则组功能仅支持企业版以上的包年包月WAF实例。

确定触发拦截的防护规则ID

1. **登录*Web*应用防火墙控制台。**
2. **选择中国大陆或海外地区地域。**
3. **定位到统计 > 安全报表页面，并打开攻击防护页签。**
4. **选择Web应用攻击类型，选择发生误拦截的网站域名，并选择攻击详情展示类型。**
5. **通过设置查询时间范围或访问IP的方式，找到相关的拦截记录日志。**
   您可以在拦截日志中查看拦截该请求的WAF防护规则ID。

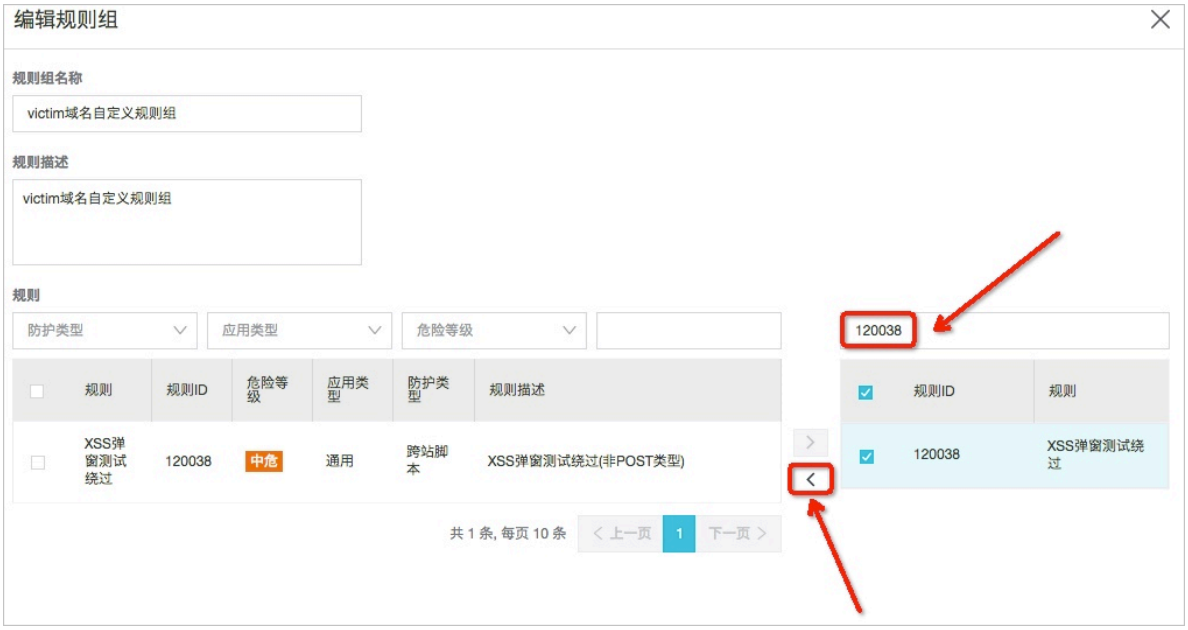
为网站设置自定义规则组

1. **在管理 > 网站配置页面，找到该网站的域名配置记录，单击防护设置，查看当前该网站采用的防护规则策略。**

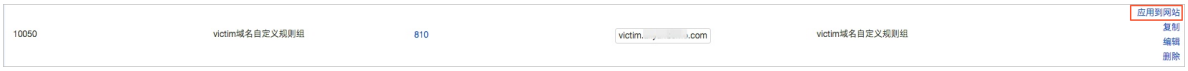
2. **定位到设置 > 自定义规则组页面，找到该网站域名当前采用的规则组，单击复制。**
3. **填写规则组名称和规则描述，单击确认，创建自定义规则组。**
4. **选择已创建的自定义规则组，单击编辑。**
5. **在编辑规则组对话框的右侧的规则列表中，通过规则ID找到触发误拦截的规则ID，选中该规则并单击 将该规则从规则组中移除，单击确认。**

说明:

左侧规则列表列出的是WAF所有的Web应用防护规则，右侧则是该自定义规则组中包含的规则。在将防护规则从自定义规则组移除时，请务必确认防护规则误拦截了网站业务的正常请求。



6. 在自定义规则组页面中，选择该自定义规则组，单击应用到网站，并选择出现误拦截的网站域名。



自定义规则组应用完成后，该网站域名的Web应用攻击防护规则策略将变更为所应用的自定义规则组。

此时，您再次向该网站域名发送同样的请求，将不再被WAF拦截。

说明:

如果访问请求仍然被WAF拦截，您可以根据上述步骤再次确定本次触发拦截的防护规则ID，并在自定义规则组中将该规则移除，避免误拦截。

9 CC攻击防护最佳实践

本文介绍了常见的CC攻击场景，并结合阿里云WAF的相关功能给出具体的防护策略和配置，帮助您有针对性地防御CC攻击。

大流量高频CC攻击

在大规模CC攻击中，单台傀儡机发包的速率往往远超过正常用户的请求频率。这种情况下，直接针对请求源限速拉黑是有效的办法。

您可以使用WAF的自定义CC规则，配置相关的限速策略。示例如下。

将URI配置为前缀匹配“/”，表示防护本域名下所有路径。这条规则的策略为：当一个IP在30秒内访问本域名下任意路径超过1000次，则封禁该IP的请求10个小时。该规则可以作为一般中小型站点的预防性配置。

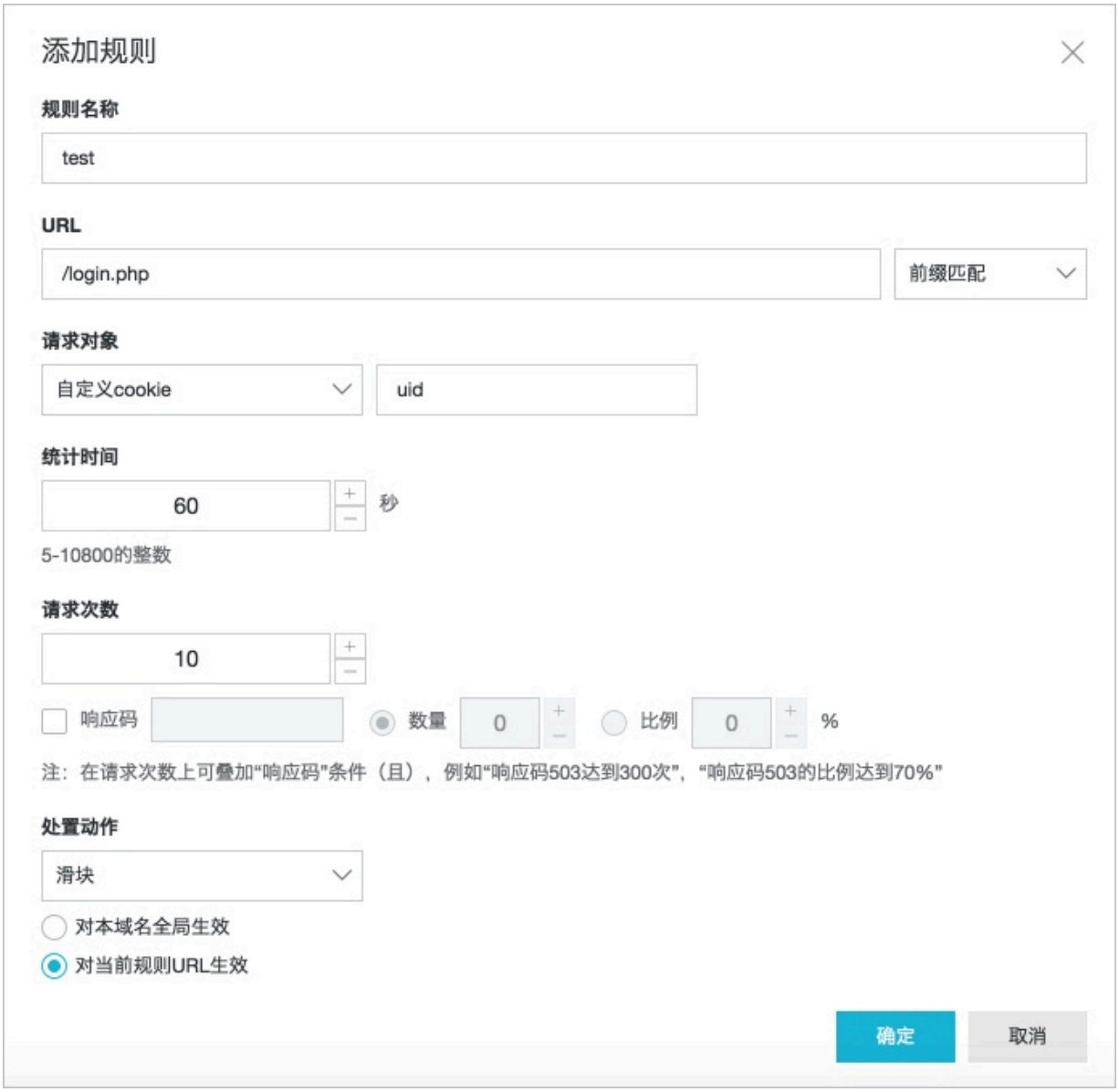
在实际场景中，您可以根据自身业务需求调整防护路径和触发防护的阈值，并选择合适的阻断类型，以达到更有针对性、更精细化的防护效果。例如，为了预防登录接口被恶意高频撞库，您可以配置登录接口的地址（如前缀匹配“/login.php”），60秒内超过20次请求则进行封禁。

在使用CC防护时，请注意以下事项。

- 人机识别（阻断类型）的目的是校验请求是否来自于真实浏览器（而非自动化工具脚本），适用范围仅限于网页/H5，不适用于原生APP、API等环境。针对原生APP、API等环境，请将阻断类型设置为封禁。
- 针对有可能被CC策略误伤的接口或IP，您可以通过精准访问控制功能将其统一加白。
- 不要对APP/API环境开启CC紧急模式。

此外，推荐您使用爬虫风险管理，应用更细粒度、更多维度的限速功能和处置手段。

例如，由于针对IP的封禁会影响NAT出口，您可以使用cookie或者业务中自带的用户级别参数作为统计对象；也可以对有嫌疑的请求设置弹出滑块验证页面的处置动作，避免误拦截。下图配置针对业务中标记用户的cookie（假设cookie格式为uid=12345）进行统计，并使用滑块作为处置动作。



攻击源来自海外/公有云

CC攻击中经常看到很大比例的攻击来源于海外、公有云、IDC机房的IP。对于面向中国用户的站点，在遭受攻击时可以通过封禁海外访问来缓解攻击压力。

您可以使用WAF的封禁地区功能，完成以下配置。

如果需要封禁公有云（如阿里云、腾讯云等）、IDC机房的IP段，您可以通过钉钉联系阿里云售后团队进行处理。

请求特征畸形/不合理

由于很多CC攻击请求是攻击者随意构造的，在仔细观察日志后，往往会发现这些请求有很多与正常请求不相符的畸形报文特征。常见的特征包括以下情形：

- **user-agent异常或畸形：例如，包含Python等自动化工具特征，明显格式错乱的UA（如“Mozilla///”），或者明显不合理的UA（如www.baidu.com）。若发现以上请求特征，可以直接封禁。**
- **user-agent不合理：例如，对于微信推广的H5页面，正常用户都应该通过微信发起访问，如果UA来自于Windows桌面浏览器（如MSIE 6.0），则明显是不合理的。若发现以上请求特征，可以直接封禁。**
- **referer异常：例如，不带referer或referer固定且来自于非法站点，可以考虑封禁这种行为（也要考虑网站首页、第一次访问的情况）。针对只能通过某个站内地址跳转访问的URL，您可以从referer角度分析行为异常，决定是否封禁。**
- **cookie异常：类似于referer，正常用户往往会在请求中带上属于网站本身业务集的一些cookie（第一次访问除外）。很多情况下，CC攻击的报文不会携带任何cookie。**
- **缺少某些HTTP header：例如，针对一些业务中需要的认证头等，正常用户请求会携带，而攻击报文不会。**

- **不正确的请求方法：例如，本来只有POST请求的接口被大量GET请求攻击，则可以直接封禁GET请求。**

上述包含恶意特征的请求，都可以在特征分析的基础上，通过WAF的精准访问控制规则进行封禁。

图 9-1: 配置示例1：拦截不带cookie的请求

图 9-2: 配置示例2：拦截不带authorization头的请求

滥刷接口（登录/注册/短信/投票等）

对于网页环境（包括H5）中的一些关键接口，如登录、注册、投票、短信验证码等，推荐您使用数据风控进行防护。

数据风控在关键接口页面中插入JS代码，采集用户在页面上的操作行为和环境信息，综合判断发送至关键接口的请求是否来自于真实的用户（而不是自动化工具脚本）。数据风控判定的依据主要来自于人机识别的结果，跟发送请求的频率、来源IP并没有关系，针对一些低频、分散的攻击请求有很好的效果。

说明:

数据风控的判定依赖于开启防护后在正常请求中附带的验证参数，该功能不适用于不能执行JS的环境（如API、Native APP等）。为避免误拦截，建议您启用前先在测试环境进行测试，或是先开启观察模式并跟云盾工程师确认后，再开启防护模式。

恶意扫描

大规模扫描行为会给服务器带来很大压力，除了基于频率来限制以外，您还可以通过高频Web攻击IP自动封禁、目录遍历防护、扫描威胁情报等功能来加强防护效果。

一般情况下，包含恶意特征的扫描请求会被WAF的默认规则拦截，而高频Web攻击IP自动封禁则会对连续触发Web防护规则的IP进行直接封禁。

目录遍历防护可以自动封禁在短时间内进行多次目录遍历攻击的客户端IP。

扫描威胁情报可以自动封禁来自常见扫描工具或阿里云恶意扫描攻击IP库中IP的访问请求。

App攻击

针对App攻击，除上述自定义CC防护、封禁地区、精确访问控制等手段外，您也可以接入云盾SDK进行防护。

SDK方案通过将SDK集成到App中，对请求进行安全签名和校验，并结合各种硬件信息，综合识别请求是否来自于合法的App。只要不是来自于官方App的合法请求，一概拦截。这是一种“白名单”思路，只放行合法的请求，而不用去分析非法请求有什么特征。

SDK防护需要使用云盾爬虫风险管理产品，具体请参考*SDK*使用说明。

恶意爬取

对于很多资讯类网站（如征信、租房、机票、小说等），大量的爬虫往往会造成带宽增大、负载飙升等异常，以及数据泄露等问题。针对爬虫问题，如果上述手段不能够很好的防御，推荐您使用爬虫风险管理，更有针对性的防御爬虫。

10 深度学习引擎最佳实践

阿里云Web应用防火墙采用多种Web攻击检测引擎组合的方式为您的网站提供全面防护。Web应用防火墙采用规则引擎、语义分析和深度学习三种引擎组合的方式，充分发挥阿里云强大的情报、数据分析体系和专家漏洞挖掘经验的优势。基于阿里云云上攻击数据分析抓取0day漏洞，由安全专家对漏洞进行主动挖掘和分析，并最终总结沉淀为防护规则策略。Web应用防火墙的规则策略每周更新，远超业界水平，致力于为用户提供最快、最全面的防护能力。

随着互联网的发展，Web攻击手段也在不断演进，传统的单一手段的防护方式已经无法满足对复杂的互联网业务保驾护航的需求，只有通过多种检测引擎协同防护才能起到最佳的防护效果。

阿里云Web应用防火墙采用规则引擎、语义分析和深度学习引擎相结合的方式防护Web攻击。其中，

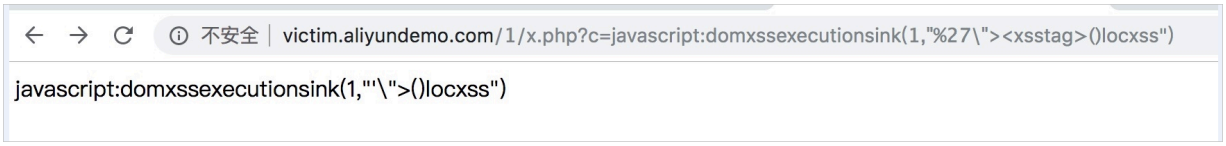
- 规则引擎：依托阿里巴巴集团多年以来攻防实践积累的专家经验整理而成的防护策略规则。
- 语义分析引擎：弥补传统规则引擎在正则文法范畴方面对上下文无关文法特征描述较弱的问题，降低规则的误报和漏洞引发的安全风险。
- 深度学习引擎：通过有监督学习的方式，依托于阿里云强大的算法团队构建的神经网络系统，对阿里云上每日亿级的攻击数据进行分类训练，最终通过模型实时地对未知风险请求进行在线检测拦截，弥补其它防御引擎对未知0day漏洞风险检测的不足。

深度学习引擎防护案例

一般来说，规则引擎使用的正则规则的描述性比较强，对于强攻击特征的请求，正则规则的防护效果最佳。而当面对一些弱特征的攻击请求（例如XSS特征请求），即便您启用Web应用攻击防护的严格模式，依然可能因无法检测到而存在潜在的安全风险。

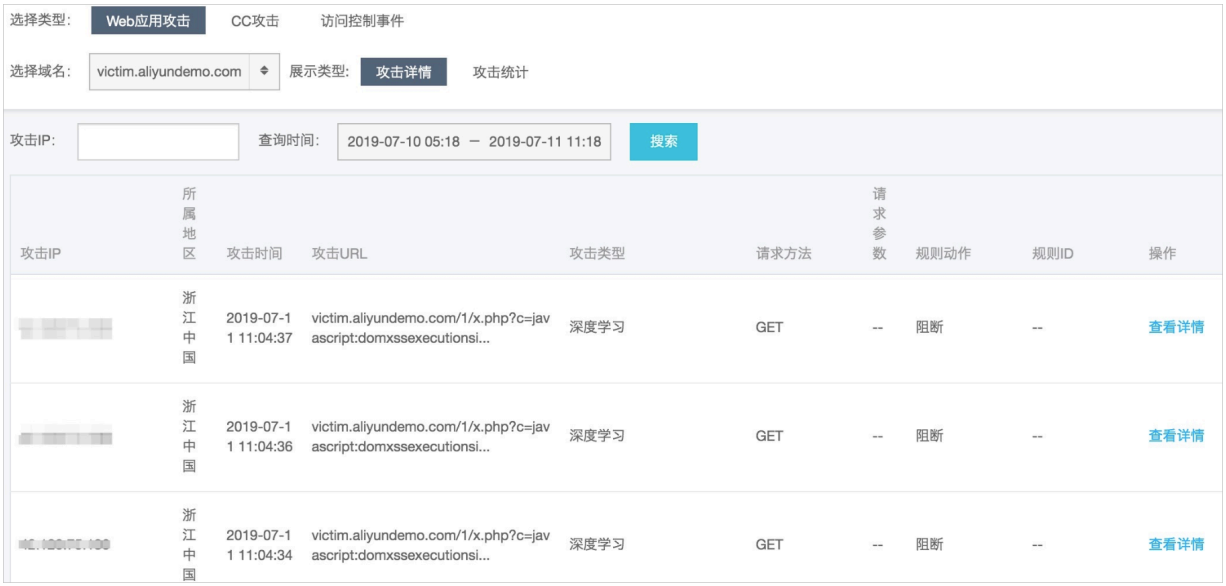
例如，您可以通过启用Web应用防火墙的大数据深度学习引擎功能，识别并拦截Web应用攻击防护的严格规则无法识别的弱特征攻击请求。

在本案例中，以下XSS攻击请求未被Web应用攻击防护规则拦截。



启用Web应用防火墙的大数据深度学习引擎防护功能后，该超出正则规则引擎检测能力的XSS攻击请求被成功拦截。

同时，在Web应用攻击报表中可以查看到详细的攻击日志信息，攻击类型为深度学习。



攻击IP	所属地区	攻击时间	攻击URL	攻击类型	请求方法	请求参数	规则动作	规则ID	操作
[redacted]	浙江中国	2019-07-11 11:04:37	victim.aliyundemo.com/1/x.php?c=javascript:domxssexecutionsi...	深度学习	GET	--	阻断	--	查看详情
[redacted]	浙江中国	2019-07-11 11:04:36	victim.aliyundemo.com/1/x.php?c=javascript:domxssexecutionsi...	深度学习	GET	--	阻断	--	查看详情
[redacted]	浙江中国	2019-07-11 11:04:34	victim.aliyundemo.com/1/x.php?c=javascript:domxssexecutionsi...	深度学习	GET	--	阻断	--	查看详情

11 拦截恶意爬虫

当今互联网爬虫的种类繁多，您可以通过WAF提供的各种功能来拦截部分恶意爬虫。

值得注意的是，为了绕过网站管理员的防爬策略，专业的爬虫往往会不断变换爬取手段。因此，依靠固定的规则来实现一劳永逸的完美防护是不太可能的。此外，爬虫风险管理往往与业务自身的特性有很强的关联性，需要专业的安全团队进行对抗才能取得较好的效果。

如果您对防爬效果有较高的要求，或者缺乏专业的安全团队来配置相应的安全策略，欢迎您使用阿里云提供的更全面、更专业的爬虫风险管理产品进行防御。

恶意爬虫的危害和特征

正常爬虫通常会带有包含xxspider的user-agent标识，并且爬取的请求量不大，爬取的URL和时间段都比较分散。合法的爬虫IP通过执行反向nslookup或tracert，一般都可以看到合法的来源地址。例如，对百度的爬虫IP执行反向nslookup，即可查询到其来源地址信息。

```
root@ubuntu:~# nslookup 220.181.108.184
Server:         192.168.254.2
Address:        192.168.254.2#53

Non-authoritative answer:
184.108.181.220.in-addr.arpa    name = baiduspider-220-181-108-184.crawl.baidu.com.

Authoritative answers can be found from:
```

而恶意爬虫则可能会在某个时间段大量请求某个域名的特定地址或接口，这种情况很可能是伪装成爬虫的CC攻击，或是经第三方伪装后针对性爬取敏感信息的请求。当恶意爬虫请求量大到一定程度，往往造成服务器的CPU飙升，导致网站无法访问等业务中断问题。

WAF针对恶意爬虫进行风险预警，提示用户昨日的爬虫请求情况。您可以结合具体的业务情况，有针对性地配置下列规则中的一种或几种，拦截对应的爬虫请求。

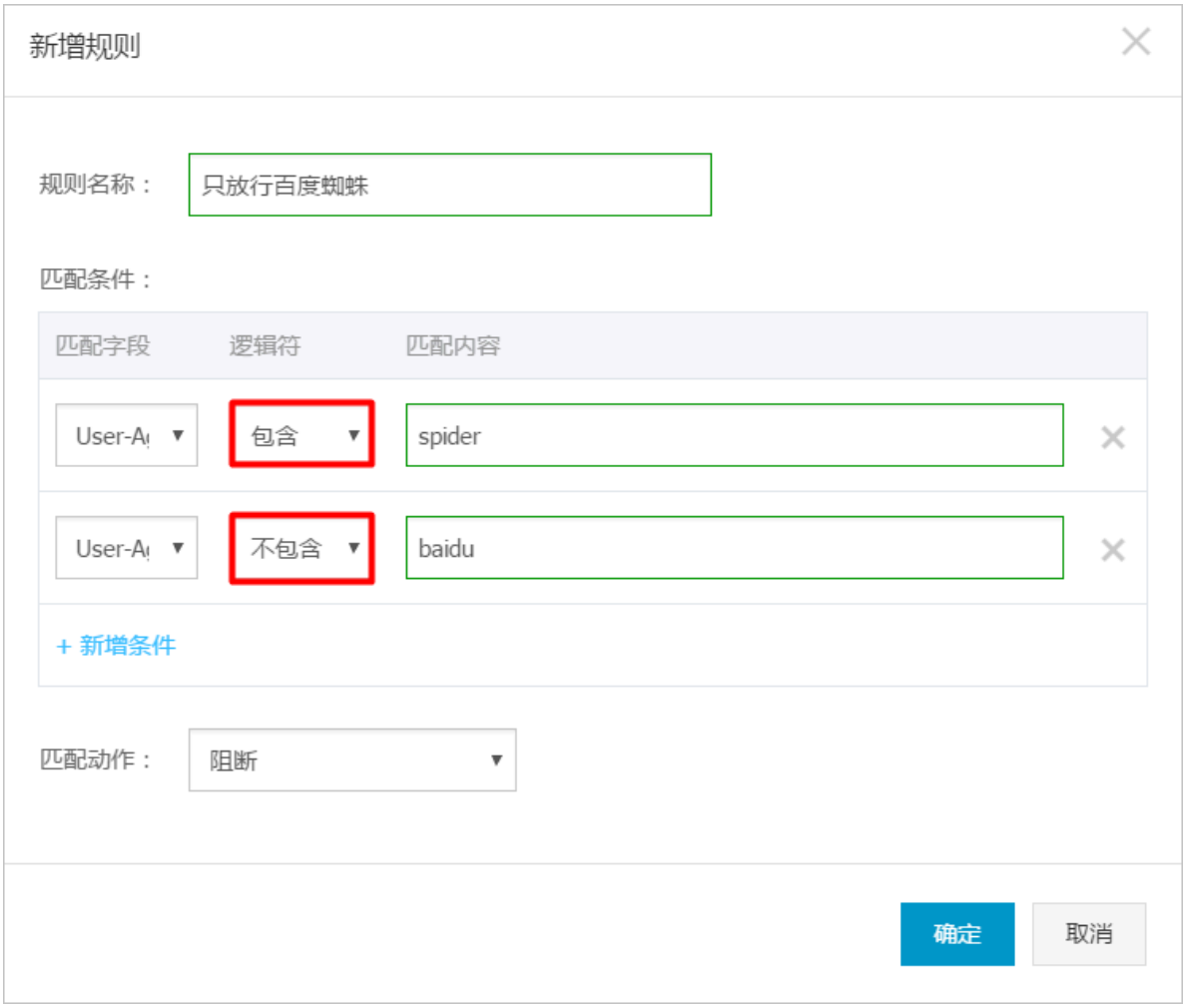
配置精准访问控制拦截特定爬虫

通过配置精准访问控制规则，您可以灵活地结合User-Agent和URL等关键字段来过滤恶意爬虫请求。

- 例如，配置以下精准访问控制规则，即可实现只放行百度爬虫，而过滤其他的爬虫请求。

> **说明:**

匹配内容中的关键字对于大小写不敏感。



- 配置以下精准访问控制规则，可以禁止任何爬虫访问/userinfo目录下的所有内容。

说明:

需要注意的是，通过限制User-Agent字段的方式在面对恶意攻击者精心构造的爬虫攻击时很容易被绕过。例如，恶意攻击者可以通过在恶意爬虫请求的User-Agent字段中带有baidu字符，则可伪装成百度爬虫而不被该精准访问控制规则所拦截。甚至，恶意攻击者可以通过在User-Agent字段中去除spider字符，隐藏爬虫身份，则该精准访问控制规则将无法拦截。

正如在本文开头部分提到的，依靠固定的规则来实现一劳永逸的完美防护是不太可能的。面对更具有针对性、更高级的恶意爬虫风险，爬虫风险管理产品通过爬虫情报能力实现更强大的防爬能力。基于阿里云对全网威胁情报实时计算得到的恶意爬虫IP情报库、动态更新的各大公有云、IDC机房IP库等情报信息，爬虫风险管理产品可以帮助您直接放行合法爬虫请求并对来自威胁情报库的恶意请求进行防护处置。

配置自定义CC规则拦截恶意请求

如果您发现恶意爬虫请求具备高频特征，您还可以使用自定义CC规则，针对特定的路径配置基于IP的访问频率的检测和阻断规则。

说明:

如果您遭受的恶意爬虫攻击难以通过设置基于IP的访问频次限制规则进行防御，建议您选择爬虫风险管理产品提供的更细粒度的频次限制功能。爬虫风险管理的频次限制功能，支持针对URL路径配置基于自定义字段作为统计对象的访问频率限制，并且支持在访问频率中叠加特定响应码的数量或比例来进一步限制该请求对象的访问请求。

配置区域封禁拦截恶意请求

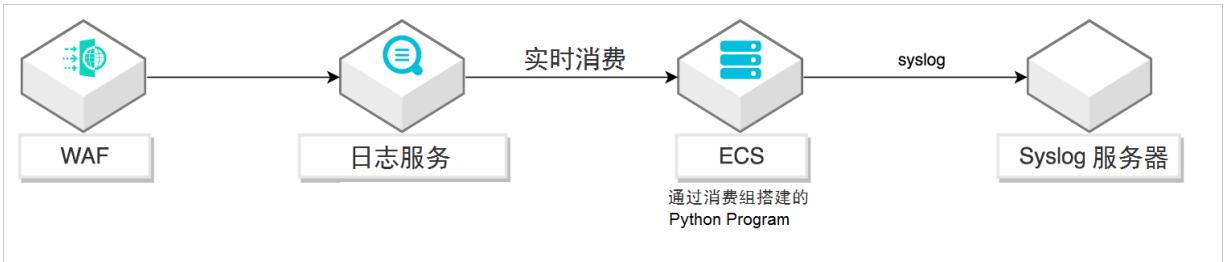
如果您发现恶意爬虫请求大量来自于特定区域，且正常的业务访问都没有来自该区域的请求，则可以通过启用区域封禁直接拦截该特定区域的所有访问请求。

12 集成Web应用防火墙日志到syslog系统

本文介绍了如何将Web应用防火墙（WAF）的日志集成到syslog日志系统中，以实现合规、审计等要求，也方便您在安全操作中心统一管理所有相关日志。

概览

该方案的整体集成架构如下图所示：



阿里云日志服务为日志数据提供一站式服务，被广泛应用于阿里巴巴集团的许多大数据场景中。日志服务在无需开发介入的前提下，帮助您快速完成数据采集、消费、投递、查询和分析，提高运维运营效率，建立DT时代海量数据的处理能力。更多信息，请查看什么是日志服务。

Python Program 是运行在ECS上的一段日志投递程序，帮助您将WAF日志投递到syslog服务器。消费库（Consumer Library）是对LogHub消费者提供的高级模式，它使用消费组（Consumer Group）统一处理消费端问题。相比于直接使用SDK读取数据，消费库让您只关注业务逻辑，而无需在意日志服务的实施细节或多消费者间的容错问题。更多信息，请查看消费组消费。

Syslog服务器是一个集中的日志消息管理服务器，它可以从多个syslog源接收数据。

前提条件

进行配置前，请确保满足以下条件：

- **您已购买企业版或旗舰版Web应用防火墙，并为您的网站配置防护。更多信息，请查看购买*Web*应用防火墙和业务接入*WAF*配置。**
- **您拥有一个Linux ECS服务器，该服务器满足以下推荐配置：**
  - **Ubuntu操作系统**
  - **8核处理器，2.0Ghz以上主频率**
  - **32GB内存**
  - **可用磁盘空间大于2GB（建议在10GB以上）**
- **您拥有一个syslog服务器，并开放UDP协议514端口用来接收syslog数据。**

操作步骤

1. **开启Web应用防火墙日志功能。**

   参照以下步骤，在Web应用防火墙控制台开启日志功能：

   a. **登录云盾*Web*应用防火墙控制台。**

   b. **在左侧导航栏，选择市场管理 > 应用管理。**

   c. **在日志服务实时查询分析应用下，单击升级。**

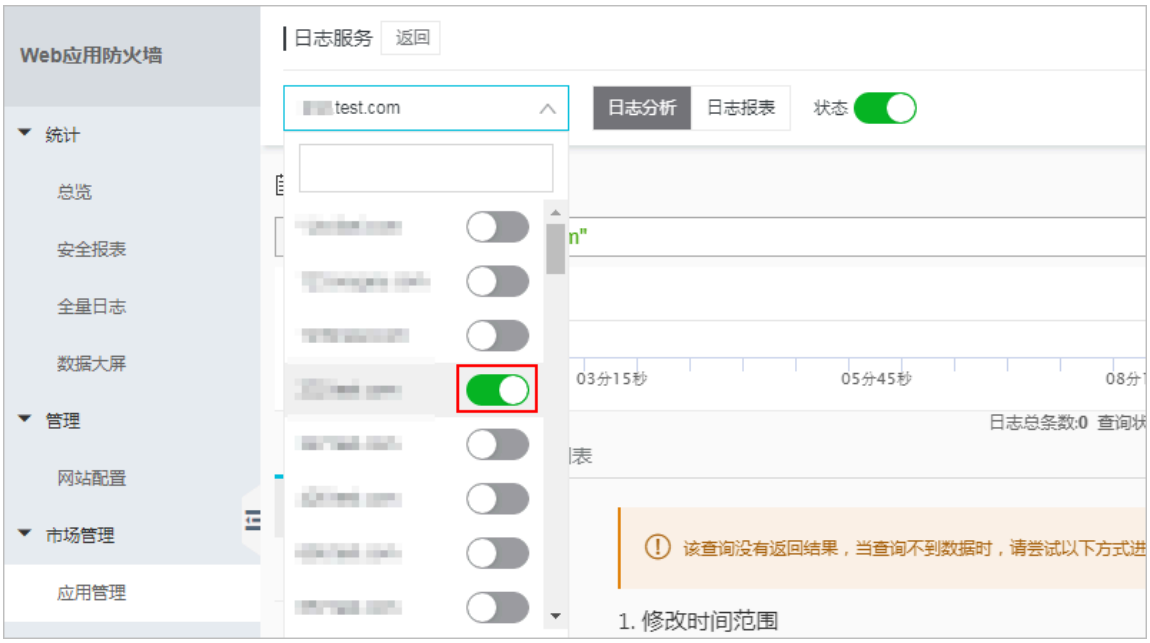
   d. **在变配页面，开通日志服务， 并根据实际需求选择日志存储时长和日志存储容量。**

   e. **开通日志服务后，在日志服务实时查询分析应用下，单击授权。**

   f. **在云资源访问授权页面，单击同意授权。**

g. 在日志服务实时查询分析应用下，单击配置。

h. 在下拉框中选择要配置的域名，并打开功能开关。



2. 在ECS中配置Python环境。

   参照以下步骤在ECS实例中安装日志服务的Python SDK：

   a. 通过SSH或控制台登录到ECS。具体操作请参考连接ECS实例。

   b. 安装Python3、pip和aliyun-log-python-sdk。关于日志服务Python SDK的介绍，请参考用户指南。

```
apt-get update
apt-get install -y python3-pip python3-dev
cd /usr/local/bin
ln -s /usr/bin/python3 python
pip3 install --upgrade pip
pip install aliyun-log-python-sdk
```

3. 配置Python Program。

   参照以下步骤配置Python Program，投递WAF日志到syslog服务器：

   a. 从GitHub下载最新的集成示例代码。

```
wget https://raw.githubusercontent.com/aliyun/aliyun-log-python-sdk/master/tests/consumer_group_examples/sync_data_to_syslog.py
```

   b. 替换示例代码Python Program中与日志服务（SLS）、syslog相关的配置参数，具体包括：

参数	释义	描述
SLS Project	日志项目名称	日志项目是日志服务的资源管理单元，用来划分和操作资源。您可以在阿里云日志服务控制台上查看项目名称。 
SLS Endpoint	日志服务入口	日志服务入口是访问一个日志项目及其内部日志数据的URL。它和项目所在的阿里云地域及日志项目名称相关。您可以在服务入口中查看服务入口URL。
SLS Logstore	日志库	日志库是日志服务用来采集、存储和查询日志数据的单元。每个日志库归属在一个项目下，每个项目可以拥有多个日志库。您可以在阿里云日志服务控制台，特定日志服务项目下查看日志库的名称。 

参数	释义	描述
SLS accessKeyId和accessKey	访问密钥	访问密钥是您在使用API（而非控制台）访问云资源时的“密码”。您需要使用AccessKey为API请求内容签名，使其能够通过日志服务的安全认证。具体请参考访问密钥。您可以在用户信息管理控制台查看您的AccessKey信息。 
Syslog Host	Syslog主机	Syslog服务器的IP地址或主机名称。
Syslog Port	Syslog端口	接收syslog的端口。UDP协议使用514，TCP协议使用1468。
Syslog protocol	Syslog协议	指定使用UDP或TCP协议来接收syslog，具体取决于syslog服务器的配置。
Syslog separator	Syslog分隔符	指定用于分隔syslog键值对的分隔符。

以下是Python Program的配置示例。

- 日志服务配置

```
endpoint = os.environ.get('SLS_ENDPOINT', 'http://ap-southeast-
1.log.aliyuncs.com')
accessKeyId = os.environ.get('SLS_AK_ID', '替换成您自己的AccessKey
 ID')
accessKey = os.environ.get('SLS_AK_KEY', '替换成您自己的AccessKey
')
project = os.environ.get('SLS_PROJECT', 'waf-project-5486134142
76****-ap-southeast-1')
logstore = os.environ.get('SLS_LOGSTORE', 'waf-logstore')
consumer_group = os.environ.get('SLS_CG', 'WAF-SLS')
```

- Syslog配置

```
settings = {
                "host": "1.2.3.4",
                "port": 514,
                "protocol": "udp",
                "sep": ",",
                "cert_path": None,
                "timeout": 120,
                "facility": syslogclient.FAC_USER,
                "severity": syslogclient.SEV_INFO,
                "hostname": None,
                "tag": None
```

```
            }
```

c. **启用Python Program。假设Python program被保存为"sync_data_to_syslog.py"，您可以使用以下命令启用它：**

```
python sync_data_to_syslog.py
```

启用Python Program后，会显示成功投递日志到syslog服务器。

```
*** start to consume data...
consumer worker "WAF-SLS-1" start
heart beat start
heart beat result: [] get: [0, 1]
Get data from shard 0, log count: 6
Complete send data to remote
Get data from shard 0, log count: 2
Complete send data to remote
heart beat result: [0, 1] get: [0, 1]
```

完成以上操作后，您可以在syslog服务器中查询WAF日志。

13 WAF独享集群最佳实践

Web应用防火墙（WAF）独享集群在WAF公共集群防护能力的基础上，为您提供与实际业务特性相结合的定制化服务，包括非标端口接入、SNI认证、自定义防护响应页面、HTTPS协议加密设置、长链接超时设置。若您的业务系统包含上述非常规设计/需求，您可以依据业务体系配置独享集群，并将网站业务接入独享集群进行防护。

独享集群vs公共集群

对比项	WAF公共集群	WAF独享集群
集群地区	公共集群在全球共部署14个防护节点，分布在以下地区：北京、上海、杭州、深圳、中国香港、新加坡、马来西亚、美东、美西、澳洲、德国、印度、印尼、迪拜。 业务接入公共集群防护时，根据源站IP自动匹配最佳地区的防护资源。	独享集群包括主、备集群。使用独享集群时，您可以从支持的地区中指定独享集群主集群的地区，备集群地区不可选择。 说明: 主集群地区一经设置，不可更改。 业务接入独享集群防护时，默认使用独享集群主集群地区的防护资源；备集群则提供备用服务，在主集群出故障时承担业务，或在攻击来临时进行防御。
集群端口	若您的业务使用特殊端口，则在WAF添加网站配置时，您需要自定义端口。公共集群支持有限的非标端口，具体请参见非标端口支持。	独享集群比公共集群支持范围更广的非标端口，理论上仅不支持22、53、9100、4431、4646、8301、6060、特定的系统端口。 使用独享集群自定义端口时，您必须先在独享集群设置中开启服务器端口，然后在添加网站到独享集群防护时，选择应用已开启的端口。 说明: 独享集群最多支持开启50个自定义端口，默认只开启了80和443端口。

对比项	WAF公共集群	WAF独享集群
SNI认证	业务接入WAF公共集群后，若客户端不兼容SNI，则可能导致HTTPS业务访问异常，具体请参见*SNI*兼容性导致*HTTPS*访问异常。	配置独享集群时，您可以上传默认SNI证书。这样，在业务接入独享集群后，即使暂不支持标准SNI协议的客户端设备也能正常访问网站。
防护响应页面	WAF公共集群使用默认的防护响应页面，例如异常访问被拦截时返回默认的拦截提示页面。	若您希望防护响应页面与您的网站设计风格保持一致，您可以使用独享集群自定义防护响应页面。 您可以将设计好的静态页面上传至阿里云CDN，并配置静态页面URL作为WAF的防护响应页面，提升网站用户体验。
HTTPS协议加密设置	公共集群不支持该项配置。	在独享集群配置中，您可以根据业务安全需求选择合适的TLS协议版本和加密套件。
长链接超时限制	公共集群不支持该项配置。	在独享集群配置中，您可以根据业务需求设置长链接限制时长，减少网络连接问题占用资源。

业务接入WAF独享集群

前提条件

要使用WAF独享集群，您必须首先购买WAF独享版或升级现有WAF版本到独享版。更多信息，请参见开通*Web*应用防火墙、续费与升级。

操作步骤

开通WAF独享版后，您可以参照以下步骤接入网站业务到WAF独享集群进行防护。假设您的业务端口是90（不在公共集群支持的非标端口范围内）。

1. 配置独享集群。

   a) 登录*Web*应用防火墙控制台。

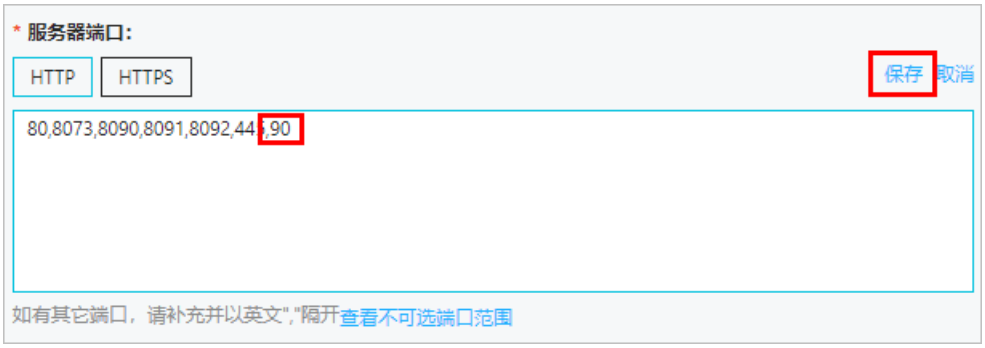
   b) 在左侧导航栏，单击设置 > 独享集群设置。

   c) 在独享集群设置页面，根据您的业务特性配置独享集群。

   本示例中，您需要在服务器端口中添加HTTP协议的90端口。操作步骤如下。

   A. 在服务器端口下，单击自定义。

   B. 在HTTP协议下添加90端口，并单击保存。



   C. 确认90端口已开启。

   更多信息，请参见设置独享集群。

   d) 单击保存设置。

   系统将根据所设定的集群配置为您配置独享集群。

2. 将具有定制化需求的业务（例如端口是90的业务）接入独享集群进行防护。

   · 已添加网站配置

   a. 前往管理 > 网站配置页面。

   b. 定位到要接入独享集群防护的网站，将其防护资源设置为独享集群。

   说明:

在切换独享集群防护时，请确认网站配置的业务端口包含在独享集群设置中。例如当前网站配置的业务端口是HTTP协议80端口，则请确认独享集群设置下的服务器端口中包含HTTP协议80端口。

c. **根据需要编辑网站配置（例如服务器端口修改为HTTP协议90端口）。更多信息，请参见编辑网站配置。**

- **新添加网站配置**

a. **前往管理 > 网站配置页面。**

b. **单击添加网站，并选择手动添加其它网站。**

c. **在填写网站信息任务中，将防护资源设置为独享集群，并填写实际业务信息（例如服务器端口选择HTTP协议90端口）。**

说明:

选择独享集群防护后，则服务器端口只能从独享集群设置中已开启的服务器端口范围内选择，具体请参见配置独享集群。

更多信息，请参见手动添加网站配置。

d. 单击下一步，并根据页面提示修改域名的DNS解析，将实际业务切换到WAF进行防护。

更多信息，请参见业务接入*WAF*配置。

3. 业务接入WAF独享集群防护后，若业务特性发生变化且涉及到独享集群配置，请参见步骤1（更新集群配置）、步骤2（编辑网站配置）进行调整。

14 账户安全最佳实践

Web应用防火墙（WAF）的账户安全功能为您提供账户风险的识别能力。本文针对如何防护账户风险给出不同攻击场景和业务场景下的防护建议，指导您更好地保护自己业务中与账户关联的接口。

背景信息

WAF支持账户安全检测，在Web攻击防护基础上帮助您识别与账户关联的业务接口（例如注册、登录等）上发生的账户安全风险事件，具体包括撞库、暴力破解、垃圾注册、弱口令嗅探和短信验证码接口滥刷。配置WAF账户安全检测后，您可以在WAF安全报表中查看相关检测结果。更多信息，请参见账户安全。

使用验证码（适用于普通网页/H5）

为普通PC页面或H5页面启用验证码是防护重点接口最简单和有效的防护手段。通常来说，接入验证码服务需要您在业务代码中做少许改动，一般一至二个工作日即可完成。一般的验证码能够有效拦截使用简单工具脚本发起的接口直接调用；但随着黑灰产攻击手段和攻击工具的进化，普通的验证码越来越容易被绕过。当您需要更高强度的攻防对抗时，建议您选择专业的验证码服务，例如阿里云验证码服务。

阿里云验证码服务基于阿里巴巴集团多年来对抗黑灰产的经验所形成的一套完整的人机识别和风控体系，提供包括无痕验证在内的多种验证方式，帮助您有效对抗职业黑灰产的攻击，同时避免对正常用户的干扰。

推荐您前往人机验证在线体验页面，直观感知产品功能。

使用SDK签名（适用于APP）

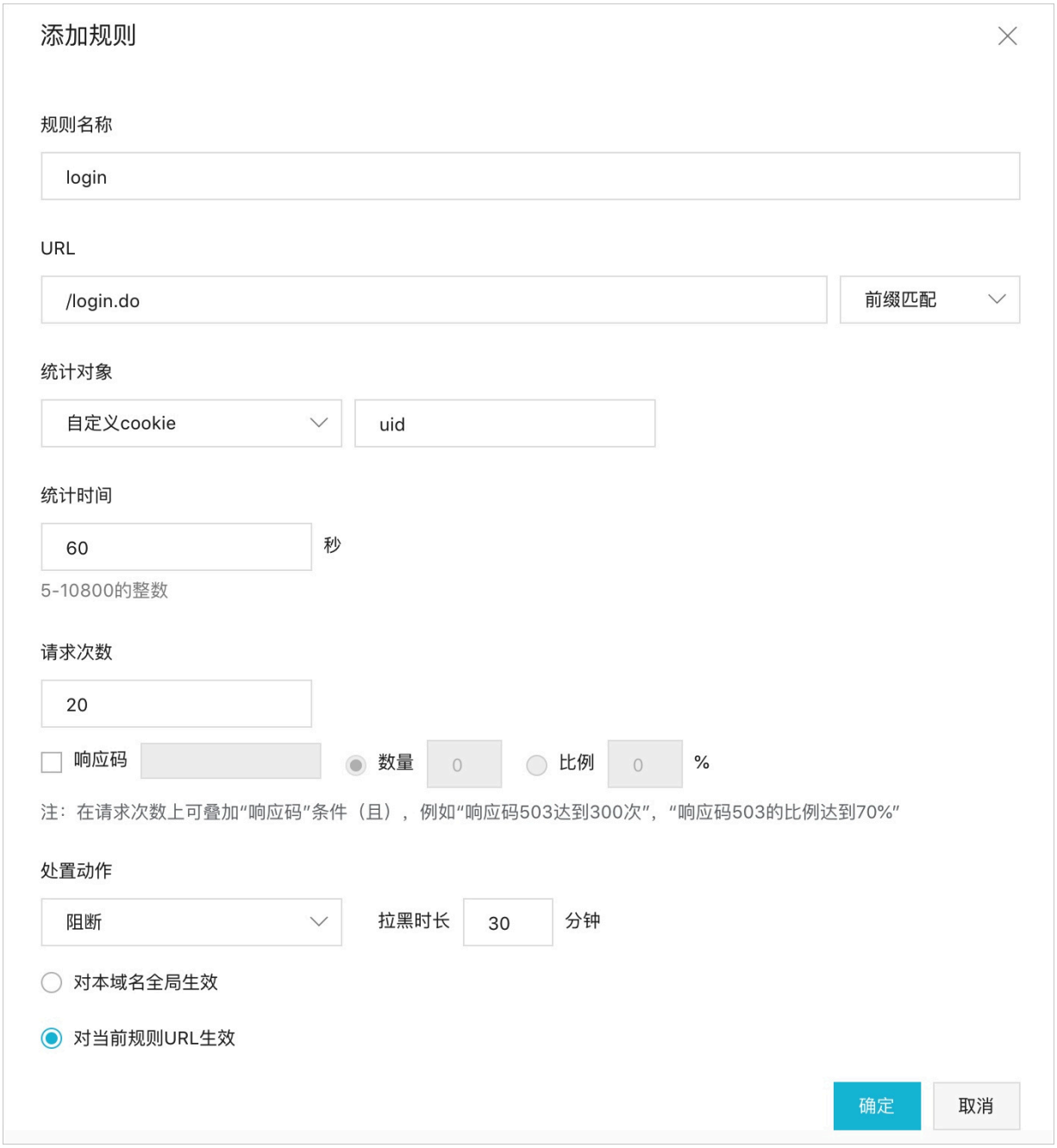
对于不适合使用验证码的原生APP，阿里云提供了一套SDK方案。SDK方案通过采集移动端的各种硬件信息、环境信息，并且对请求进行签名和验签，确保只有通过合法的官方APP（而不是来自脚本、自动化程序、模拟器等非正常途径）发出来的请求才会被放行回源站。更多信息，请参见*SDK*方案概述。

多维度的频次限制（适用于高频攻击）

对于攻击请求中包含某个高频特征字段（例如IP、session、cookie、参数、header等）的行为，您可以使用多维度的频次限制，将攻击源拉黑。例如，当攻击请求使用大量代理/秒拨IP，但复用同一个登录态的cookie（例如uid）时，您可以基于cookie设置限速，这样就将防护对象由原始的IP转变为跟业务逻辑有关的“账号”维度。

爬虫风险管理服务提供频次限制功能，以下是频次限制规则的配置示例。

更多信息，请参见爬虫风险管理。



分析异常的请求特征

对于绝大部分攻击，通过细心观察和分析，总会发现攻击请求与正常用户请求在特征上的差异。以下是一些常见的异常请求特征，供您参考。

- **HTTP Header不完整。例如缺失referer、cookie、content-type等字段。**
- **User-agent的值异常。例如对于普通Web站点的请求中出现大量Java或是Python的UA特征；或者对于微信小程序应用的请求中出现大量桌面版PC浏览器的UA特征等。**

- Cookie不完整。一般的应用都会有多个具备业务含义的cookie，例如SessionID、userid、deviceid、lastvisit等，而爬虫程序在编写的时候有可能只会提交获取结果所必需的一到二个cookie，而忽略其他看似“没用”的cookie。
- 参数内容异常。类似cookie异常，有些参数对于爬虫来说意义不大，缺失或者重复提交都不影响获取结果，这也可以作为同一类异常来处理。
- 业务字段异常。例如邮箱、手机号、账户信息中包含某一些异常或不合理的关键字等。

WAF和爬虫风险管理中内置SLS日志服务，帮助您方便快速地分析请求特征，例如Top IP排序、某一特征在整体流量中的占比等。

更多信息，请参见常用日志查询分析语句。

开启撞库/爬虫威胁情报

爬虫风险管理将基于阿里云全网流量监测到的有撞库行为聚集的恶意IP通过算法提取出来，形成撞库IP情报库，并动态更新。您可以在爬虫风险管理 > 威胁情报中，一键开启撞库IP检测（观察模式）或是对命中的IP进行拦截、人机识别等处置。更多信息，请参见爬虫情报。

使用安全托管服务

如果上述解决方案都不能满足您的防护需求，或者防护效果不够理想，或是您希望有专业的安全团队直接帮助您解决问题，推荐您使用安全托管服务。阿里云提供专业的攻防技术团队，根据您的具体业务场景和需求来定制防护方案，并提供实时的分析、监控、攻防对抗，最大程度地保证防护效果。