

Web 应用防火墙

用户指南

文档版本 207

发布日期 2025-01-23



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 创建用户组并授权使用 WAF.....	1
2 购买 WAF.....	3
2.1 购买 WAF 云模式.....	3
2.2 购买 WAF 独享模式.....	8
3 网站接入 WAF.....	15
3.1 网站接入概述.....	15
3.2 将网站接入 WAF 防护（云模式-CNAME 接入）.....	20
3.2.1 将网站接入 WAF 防护（云模式-CNAME 接入）.....	20
3.2.2 配置示例.....	35
3.3 将网站接入 WAF 防护（云模式-ELB 接入）.....	40
3.4 将网站接入 WAF 防护（独享模式）.....	44
3.5 WAF 支持的端口范围.....	56
4 查看防护事件.....	62
4.1 查询防护事件.....	62
4.2 处理误报事件.....	65
4.3 通过 LTS 记录 WAF 全量日志.....	71
5 配置防护策略.....	84
5.1 防护配置概述.....	84
5.2 配置 Web 基础防护规则防御常见 Web 攻击.....	88
5.3 配置智能访问控制规则精准智能防御 CC 攻击.....	93
5.4 配置 CC 攻击防护规则防御 CC 攻击.....	96
5.5 配置精准访问防护规则定制化防护策略.....	106
5.6 配置 IP 黑白名单规则拦截/放行指定 IP.....	118
5.7 配置地理位置访问控制规则拦截/放行特定区域请求.....	126
5.8 配置威胁情报访问控制规则拦截/放行指定 IP 库的 IP.....	135
5.9 配置网页防篡改规则避免静态网页被篡改.....	137
5.10 配置网站反爬虫防护规则防御爬虫攻击.....	141
5.11 配置防敏感信息泄露规则避免敏感信息泄露.....	150
5.12 配置全局白名单规则对误报进行忽略.....	156
5.13 配置隐私屏蔽规则防隐私信息泄露.....	160
5.14 配置扫描防护规则自动阻断高频攻击.....	166
5.15 创建引用表对防护指标进行批量配置.....	169

5.16 配置攻击惩罚标准封禁访问者指定时长.....	172
5.17 条件字段说明.....	177
5.18 WAF 覆盖的应用类型.....	180
6 查看总览.....	184
7 网站设置.....	188
7.1 网站接入后推荐配置.....	188
7.1.1 配置 PCI DSS/3DS 合规与 TLS.....	188
7.1.2 开启 IPv6 防护.....	196
7.1.3 开启 HTTP2 协议.....	198
7.1.4 配置 WAF 到网站服务器的连接超时时间.....	198
7.1.5 开启熔断保护功能保护源站安全.....	200
7.1.6 配置攻击惩罚的流量标识.....	201
7.1.7 配置 Header 字段转发.....	203
7.1.8 修改拦截返回页面.....	205
7.1.9 开启 Cookie 安全属性.....	207
7.2 网站管理.....	208
7.2.1 查看网站基本信息.....	208
7.2.2 导出网站设置列表.....	210
7.2.3 切换防护模式.....	210
7.2.4 修改负载均衡算法.....	211
7.2.5 更换网站绑定的防护策略.....	212
7.2.6 更新网站绑定的证书.....	212
7.2.7 修改服务器配置信息.....	214
7.2.8 查看防护网站的云监控信息.....	216
7.2.9 批量跨企业项目迁移域名.....	217
7.2.10 删除防护网站.....	218
8 策略管理.....	220
8.1 新增防护策略.....	220
8.2 添加策略适用的防护域名.....	221
8.3 批量添加防护规则.....	222
9 安全报告.....	225
10 高阶功能.....	230
10.1 配置内容安全检测.....	230
11 对象管理.....	234
11.1 管理证书.....	234
11.1.1 上传证书.....	234
11.1.2 绑定证书到防护网站.....	237
11.1.3 查看证书信息.....	238
11.1.4 共享企业项目证书.....	240
11.1.5 删除证书.....	241

11.2 管理黑白名单 IP 地址组.....	242
11.2.1 添加黑白名单 IP 地址组.....	242
11.2.2 修改或删除黑白名单 IP 地址组.....	243
12 系统管理.....	245
12.1 管理独享引擎.....	245
12.2 查看产品信息.....	252
12.3 变更 WAF 云模式版本和规格.....	253
12.4 开启告警通知.....	256
13 权限管理.....	260
13.1 授权并关联企业项目.....	260
13.2 IAM 权限管理.....	261
13.2.1 WAF 自定义策略.....	261
13.2.2 WAF 权限及授权项.....	262
13.3 WAF 控制台的权限依赖.....	267
14 监控与审计.....	269
14.1 使用 CES 监控 WAF.....	269
14.1.1 WAF 监控指标说明.....	269
14.1.2 设置监控告警规则.....	281
14.1.3 查看监控指标.....	282
14.2 使用 CTS 审计 WAF.....	282
14.2.1 云审计服务支持的 WAF 操作列表.....	282
14.2.2 在 CTS 事件列表查看云审计事件.....	287

1 创建用户组并授权使用 WAF

如果您需要对您所拥有的WAF进行精细的权限管理，您可以使用[统一身份认证服务](#)（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用WAF资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将WAF资源委托给更专业、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用WAF服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如[图1-1](#)所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的WAF权限，并结合实际需求进行选择，WAF支持的系统权限如[表1-1](#)所示。如果您需要对除WAF之外的其它服务授权，IAM支持服务的所有权限请参见[系统权限](#)。

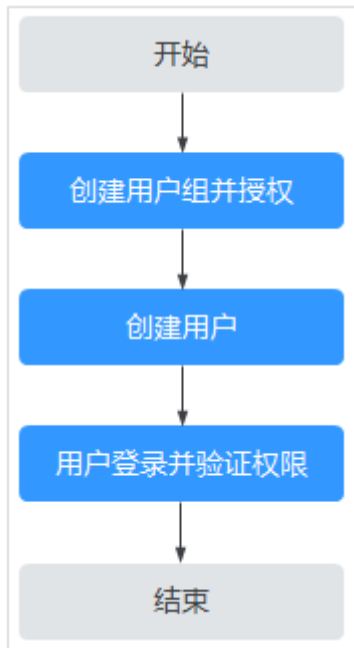
表 1-1 WAF 系统角色

系统角色/策略名称	描述	类别	依赖关系
WAF Administrator	Web应用防火墙服务的管理员权限。	系统角色	依赖Tenant Guest和Server Administrator角色。 <ul style="list-style-type: none">• Tenant Guest：全局级角色，在全局项目中勾选。• Server Administrator：项目级角色，在同项目中勾选。
WAF FullAccess	Web应用防火墙服务的所有权限。	系统策略	无。

系统角色/策略名称	描述	类别	依赖关系
WAF ReadOnlyAccess	Web应用防火墙的只读访问权限。	系统策略	

示例流程

图 1-1 给用户授权服务权限流程



1. **创建用户组并授权**

在IAM控制台创建用户组，并授予Web应用防火墙权限“WAF Administrator”。

2. **创建用户并加入用户组**

在IAM控制台创建用户，并将其加入1中创建的用户组。

3. **用户登录并验证权限**

新创建的用户登录控制台，切换至授权区域，验证权限：

在“服务列表”中选择除Web应用防火墙外（假设当前策略仅包含“WAF Administrator”）的任一服务，如果提示权限不足，表示“WAF Administrator”已生效。

2 购买 WAF

2.1 购买 WAF 云模式

Web应用防火墙云模式支持包年/包月（预付费）计费方式。同时，包周期（包年/包月）提供四个服务版本：入门版、标准版、专业版和铂金版，三种扩展包：域名扩展包、QPS扩展包和规则扩展包。您可以根据业务需求购买WAF云模式。

📖 说明

- 云模式的ELB接入方式需要[提交工单](#)申请开通后才能使用，支持使用的Region请参考[功能总览](#)。
- 购买了云模式标准版、专业版或铂金版后，才支持使用ELB接入方式，域名、QPS、规则扩展包的配额与云模式的CNAME接入方式共用，且ELB接入方式的业务规格与购买的云模式版本的对应规格一致。
- WAF的API接口目前是免费支持调用，暂不收费。

前提条件

登录WAF控制台的账号需要拥有WAF Administrator与BSS Administrator权限。

约束条件

- 入门版不支持购买扩展包。
- 同一账号在同一个大区域（例如，华东区域：华东-上海一、华东-上海二）只能选择一个服务版本。

📖 说明

有关支持购买WAF的区域说明，请参见[Web应用防火墙支持防护哪些区域？](#)。

原则上，在任何一个区域购买的WAF支持防护所有区域的Web业务。但是为了提高WAF的转发效率，建议您在购买WAF时，根据防护业务的所在区域就近选择购买的WAF区域。

- 专业版和铂金版支持定制非标准端口，您可以[提交工单](#)申请开通定制的非标准端口。

规格限制

- 一个域名扩展包支持10个域名。

- 一个QPS扩展包的QPS限制和带宽限制：
 - 对于部署在华为云的Web应用
业务带宽：50Mbit/s
每秒钟的请求量：1000QPS（Queries Per Second，例如一个HTTP GET请求就是一个Query）
 - 对于未部署在华为云的Web应用
业务带宽：20Mbit/s
每秒钟的请求量：1000QPS（Queries Per Second，例如一个HTTP GET请求就是一个Query）
- 一个规则扩展包包含10条IP黑白名单防护规则。

须知

- 购买了云模式标准版、专业版或铂金版后，才支持使用ELB接入方式，域名、QPS、规则扩展包的配额与云模式的CNAME接入方式共用，且ELB接入方式的业务规格与购买的云模式版本的对应规格一致。
- 带宽限制仅对云模式-CNAME方式接入的网站有限制，通过ELB模式接入的网站，没有带宽限制，仅有QPS限制。

应用场景


业务服务器部署在华为云、非华为云或线下，且防护对象为域名。


各服务版本推荐使用的场景说明如下：

- 入门版
个人网站防护
- 标准版
中小型网站，对业务没有特殊的安全需求
- 专业版
中型企业级网站或服务对互联网公众开放，关注数据安全且具有高标准的安全需求
- 铂金版
中大型企业网站，具备较大的业务规模，或是具有特殊定制的安全需求

包年月方式购买云模式 WAF

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在页面的右上角，单击“购买WAF实例”。

步骤5 在“购买Web应用防火墙”界面，“WAF模式”选择“云模式”。

步骤6 选择“区域”。

说明

原则上，在任何一个区域购买的WAF支持防护所有区域的Web业务。但是为了提高WAF的转发效率，建议您在购买WAF时，根据防护业务的所在区域就近选择购买的WAF区域。

如果您需要切换区域，请在“区域”下拉框里选择区域。同一个区域只支持购买一个WAF版本。

步骤7 选择“版本规格”。

图 2-1 选择服务版本



步骤8 选择标准版、专业版和铂金版时，可以设置“域名扩展包”、“QPS扩展包”或“规则扩展包”的数量，如图2-2所示。

可参照[域名扩展包](#)、[QPS扩展包](#)和[规则扩展包](#)进行详细了解。

图 2-2 选择扩展包



步骤9 选择“购买时长”。单击时间轴的点，选择购买时长，可以选择1个月~3年的时长。

说明

- 勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。
- 如果您需要使用内容安全检测服务，可单击“前往购买”，跳转到“购买内容安全检测服务”页面。

步骤10 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤11 确认订单详情无误后，阅读并勾选“我已经阅读并同意《Web应用防火墙免责声明》”，单击“去支付”，完成购买操作。

步骤12 进入“付款”页面，选择付款方式进行付款。

----结束

生效条件

付款成功后，您可以在管理控制台右上方查看当前购买的WAF版本以及到期的天数。

扩展包说明

Web应用防火墙提供了域名扩展包、带宽扩展包和规则扩展包，当您购买的WAF云模式版本匹配的扩展包数量不能满足业务需求时，可以通过增加扩展包数量提高域名、带宽、规则的防护配额。

域名扩展包

一个域名扩展包支持防护10个域名。如果当前云模式版本的防护域名数量不能满足业务需求时，您可以通过购买域名扩展包增加防护域名配额。

云模式各版本支持防护的域名个数说明如下：

- 入门版/标准版：支持防护10个域名。
- 专业版：支持防护50个域名。
- 铂金版：支持防护80个域名。

说明

同一个域名对应不同端口视为不同的域名，例如www.example.com:8080和www.example.com:8081视为两个不同的域名，将占用两个不同的域名配额。

您也可以通过变更云模式规格增加域名配额。详细操作请参见[变更WAF云模式版本和规格](#)。

QPS 扩展包

通过包年/包月模式购买WAF云模式时，标准版、专业版和铂金版存在一定量的业务请求限制，各版本支持的最大业务请求限制请参见[各版本支持的业务规格](#)。您可以购买QPS扩展包以满足更大的业务请求需求。

例如，您当前的业务流量需求为6,000QPS，您已经购买了WAF专业版套餐（业务请求限制为5,000QPS），这种情况下您需要额外购买1,000QPS的QPS扩展包，确保您的业务访问正常。您可以通过[变更WAF云模式版本和规格](#)来增加QPS扩展配置，满足更大的业务带宽需求。

什么是业务带宽限制？

- WAF的业务带宽是指所有该WAF防护的域名、站点中正常业务流量的大小，单位为Mbit/s。一个QPS扩展包包含：
 - 对于部署在华为云的Web应用
业务带宽：50Mbit/s
每秒钟的请求量：1000QPS（Query Per Second，例如一个HTTP GET请求就是一个Query）
 - 对于未部署在华为云的Web应用
业务带宽：20Mbit/s
每秒钟的请求量：1000QPS（Query Per Second，例如一个HTTP GET请求就是一个Query）

说明

WAF中的实际业务带宽由WAF单独计算，与其他华为云产品（如CDN、ELB、ECS等）的带宽或者流量限制没有任何关联。

- 通过包年/包月模式购买WAF时，标准版、专业版和铂金版都存在一定量的业务带宽限制，且在华为云内的源站服务器（如ECS、ELB实例等）可享有更高的业务带宽。例如，在WAF铂金版套餐中，对于华为云内的源站的业务带宽限制为300Mbit/s，而对于华为云外的服务器（如IDC机房等）的业务带宽限制则为100Mbit/s。

超过业务带宽限制和请求限制会有什么影响？

如果您的正常业务流量超过您已购买的WAF版本的业务带宽和请求限制，您在WAF中配置的全部业务的流量转发将可能受到影响。

超出业务请求限制后，可能出现限流、随机丢包等现象，导致您的正常业务在一定时间内不可用、卡顿、延迟等。例如，页面提示“Website is under maintenance (Protected by WAF)”。

如果出现这种情况，您需要升级WAF版本或者扩展业务请求，避免正常业务流量超出业务请求限制所产生的影响。

如何选择QPS扩展包？

购买WAF时，您需要提前考虑准备通过WAF配置防护的所有站点的日常入方向和出方向总流量的峰值，确保您选购的WAF所对应的业务带宽限制大于入、出方向总流量峰值中较大的值。

说明

一般情况下，出方向的流量会比较大。

您可以参考云服务器（ECS）管理控制台中的流量统计，或者通过您站点服务器上的其它监控工具来评估您的实际业务流量大小。

流量指的是业务去掉攻击流量后的正常流量。例如，您需要将所有站点对外访问的流量都接入WAF进行防护，在正常访问（未遭受攻击）时，WAF将这些正常访问流量回源到源站ECS实例；而当站点遭受攻击（CC攻击或DDoS攻击）时，WAF将异常流量拦截、过滤后，将正常流量回源到源站ECS实例。因此，您在云服务器（ECS）管理控制台中查看您源站ECS实例的入方向及出方向的流量就是正常的业务流量。如果存在多个源站ECS实例，则需要统计所有源站ECS实例流量的总和。例如：假设您需要通过WAF配置防护六个站点，每个站点的出方向的正常业务流量峰值都不超过2,000QPS，流量

总和不超过12,000QPS。这种情况下，您只需选择购买Web应用防火墙铂金版套餐即可。

规则扩展包

通过包年/包月模式购买WAF云模式时，如果当前版本的IP黑白名单防护规则数不能满足要求，您可以通过购买规则扩展包增加IP黑白名单防护规则数，以满足的防护配置需求。

一个规则扩展包包含10条IP黑白名单防护规则。

您可以在购买云模式或变更云模式规格时购买规则扩展包。

详细操作请参见[变更WAF云模式版本和规格](#)。

相关操作

- [变更WAF云模式版本和规格](#)

购买了云模式后，您可以从较低版本的WAF升级到任一更高版本，也可以根据需求增加扩展包的数量。

- [如何退订Web应用防火墙？](#)

- [如何为Web应用防火墙续费？](#)

2.2 购买 WAF 独享模式

如果您的业务服务器部署在华为云，您可以通过购买WAF独享引擎实例对重要的域名或仅有IP的Web服务进行防护。购买独享引擎实例后，您还需要为实例配置弹性负载均衡，弹性负载均衡可以通过流量分发扩展应用系统对外的服务能力，同时通过消除单点故障提升应用系统的可用性。

独享模式支持按需计费模式，按使用时长收费。

说明

独享模式在部分区域已经停售，详见[独享模式停售通知](#)。

建议至少购买2个WAF实例，并将业务分别部署到WAF实例上。当业务部署多个WAF实例时，如果某个WAF实例发生故障时，WAF会自动将流量切换到其它正在运行的WAF实例上，确保业务正常运行。

前提条件

- 登录WAF控制台的账号必须具有“WAF Administrator”或者“WAF FullAccess”权限。
- 建议您使用租户账号购买WAF独享模式。如果您需要使用IAM用户购买WAF独享模式，需要为该IAM用户创建统一身份认证服务管理权限。
 - 首次购买，需要授予IAM系统角色权限“Security Administrator”。
 - 非首次购买，需要授予IAM系统策略权限“IAM ReadOnlyAccess”或授予自定义权限，具体权限如下：
 - iam:agencies:listAgencies
 - iam:agencies:getAgency

- iam:permissions:listRolesForAgency
- iam:permissions:listRolesForAgencyOnProject
- iam:permissions:listRolesForAgencyOnDomain

具体操作请参见[创建用户组并授权使用WAF](#)。

- 已成功创建虚拟私有云VPC，详见[创建虚拟私有云和子网](#)。
- 当前Organizations服务正在公测中，使用组织合规规则功能需先申请Organizations服务公测。

约束条件

- 如果WAF独享引擎实例与源站不在同一个VPC中，可通过[对等连接](#)打通两个VPC之间网络，但受限于网络的不稳定性，建议WAF独享引擎实例与源站在同一个VPC中。
- 原则上，在任何一个区域购买的WAF支持防护所有区域的Web业务。但是为了提高WAF的转发效率，建议您在购买WAF时，根据防护业务的所在区域就近选择购买的WAF区域。有关支持购买WAF的区域说明，请参见[Web应用防火墙支持防护哪些区域?](#)。
- 开启“反亲和”后，最多只能创建5个独享引擎实例。

规格限制

购买独享引擎实例后，实例规格不能修改。


应用场景


业务服务器部署在华为云，防护对象为域名或IP。

大型企业网站，具备较大的业务规模且基于业务特性具有制定个性化防护规则的安全需求。

购买 WAF 独享实例

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在页面的右上角，单击“购买WAF实例”。


步骤5 在“购买Web应用防火墙”界面，“WAF模式”选择“独享模式”。

步骤6 配置WAF实例参数，相关参数说明如[表2-1](#)所示。

表 2-1 WAF 独享引擎实例参数说明

参数名称		说明	取值样例
基础配置	计费模式	仅支持“按需计费”模式。	按需计费

参数名称		说明	取值样例
	区域	支持购买WAF独享模式的区域说明，请参见 Web应用防火墙支持防护哪些区域？ 。 原则上，在任何一个区域购买的WAF支持防护所有区域的Web业务。但是为了提高WAF的转发效率，减少网络时延，提高网络速度，建议您在购买WAF时，根据防护业务的所在区域就近选择购买的WAF区域。	-
	通用可用区	选择区域中的可用区。 说明 可用区选定后不支持更换。	-
版本规格	规格选择	选择实例的规格，支持“WI-500”和“WI-100”。 <ul style="list-style-type: none">WAF实例规格选择WI-500，参考性能：<ul style="list-style-type: none">HTTP业务：建议5,000QPSHTTPS业务：建议 4,000QPSWebsocket业务：支持最大并发连接5,000最大回源长连接：60,000WAF实例规格选择WI-100，参考性能：<ul style="list-style-type: none">HTTP业务：建议1,000QPSHTTPS业务：建议800QPSWebsocket业务：支持最大并发连接1,000最大回源长连接：60,000	WI-500
	版本选择	选择独享引擎版本，建议选择最新的独享引擎版本。WAF支持的独享引擎版本详见 独享引擎版本迭代 。	-
	WAF实例创建类别	选择实例的资源类型，仅支持“资源租户类”。 WAF实例通过弹性网卡接入用户网络。仅支持与独享型ELB配套使用，接入方式请参见 网站接入流程（独享模式） 。 说明 如果需要选择“普通租户类”（WAF实例将直接创建在租户ECS中，租户可以在ECS服务页面看到WAF实例所在的弹性云服务器），需要 提交工单 申请，且仅部分Region支持，具体信息请以申请回复情况为准。	资源租户类

参数名称		说明	取值样例
网络配置	虚拟私有云	选择源站所在的VPC。	-
	子网	选择VPC中已配置的子网。	-
	安全组	<p>选择区域中已有的安全组，或者单击“新建安全组”，创建新的安全组。选择安全组后，该实例将受到该安全组访问规则的保护。</p> <p>新建安全组时，WAF提供了三种安全组模板，您可以根据实际情况进行选择：</p> <ul style="list-style-type: none"> 通用Web服务器：默认放通22、3389、80、443端口和ICMP协议。适用于需要远程登录实例、使用ping命令验证实例的网络连通性，以及实例对外提供网站访问服务的场景。 开放全部端口：开放全部端口即允许任意流量出入安全组内的实例，此操作存在一定安全风险，请您谨慎选择。 快速添加规则：您可以勾选常见协议端口，在入方向快速添加规则放通对应的协议及端口。若您未勾选任何协议端口，则不会放通任何端口。您可在安全组创建后，根据实际访问需求添加或修改安全组规则。 <p>单击  展开“查看模板规则”，可查看选择的对应安全组模板的入方向和出方向的访问规则。</p> <p>须知</p> <ul style="list-style-type: none"> 您也可以在虚拟私有云 VPC 的控制台创建安全组建议配置以下访问规则： <ul style="list-style-type: none"> 入方向规则 根据业务需求添加指定端口入方向规则，放通指定端口入方向网络流量。例如，需要放通“80”端口时，您可以添加“策略”为“允许”的“TCP”、“80”协议端口规则。 出方向规则 默认。放通全部出方向网络流量。 详细操作请参见添加安全组规则。 如果WAF独享引擎实例与源站不在同一个VPC中，需要在安全组中设置实例与源站的子网互通。 	-

参数名称		说明	取值样例
高级配置 (可选)	WAF实例名称前缀	设置WAF实例名称前缀，购买多个实例时，实例前缀名称相同。	WAF
	企业项目	<p>企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请开通企业管理功能。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。</p> <p>说明</p> <ul style="list-style-type: none"> “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。 只有注册的华为账号购买WAF时，“企业项目”下拉列表中才可以选择到“default”。 	default
	标签	<p>如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签。</p> <p>如您的组织已经设定Web应用防火墙（Web Application Firewall，WAF）服务的相关标签策略，则需按照标签策略规则为独享引擎实例添加标签。标签不符合标签策略的规则，则可能会导致独享引擎实例创建失败，请联系组织管理员了解标签策略详情。</p>	-
	服务授权	首次购买WAF时，可配置此参数。勾选后，WAF将代您在IAM中创建委托，开通相关权限。	-
	反亲和	<ul style="list-style-type: none"> 开启后，最多只能创建5个独享引擎实例。 开启后，独享引擎在创建时，将尽量分散地创建在不同的物理主机上，以提高业务的可靠性。 	-
用量配置	购买数量	<p>设置购买的WAF实例个数。</p> <p>建议至少购买2个WAF实例，并将业务分别部署到WAF实例上。当业务部署多个WAF实例时，如果某个WAF实例发生故障时，WAF会自动将流量切换到其它正在运行的WAF实例上，确保业务正常运行。</p>	2

步骤7 确认参数配置无误后，在页面右下角单击“立即购买”。

📖 说明

如果您需要使用内容安全检测服务，可单击“前往购买”，跳转到“购买内容安全检测服务”页面。

步骤8 确认订单详情无误后，阅读并勾选“我已经阅读并同意《Web应用防火墙免责声明》”后，单击“去支付”，完成购买操作。

步骤9 进入“付款”页面，选择付款方式进行付款。

步骤10 成功付款后，单击“返回独享引擎列表”，在独享引擎实例列表界面，可以查看实例的创建情况。

----结束

生效条件

创建实例大约需要5分钟。当实例的运行状态为“运行中”时，说明实例已经创建成功。

相关操作

管理独享引擎

创建WAF独享引擎实例后，您可以查看实例信息、查看实例的监控信息、升级实例版本以及删除实例。

WAF 通信安全授权

如果业务使用WAF独享模式部署方式，直接访问VPC内的数据需要开通相应的安全组规则，而开通相应的安全组规则需要获取用户授权，此授权过程称为通信安全授权。

成功购买WAF独享引擎后，WAF默认开启通信安全授权，即开通如表2-2所示的安全组规则。

表 2-2 WAF 通信安全授权安全组规则

协议端口	类型	源地址	描述
入方向规则			
TCP: 22	IPv4	100.64.0.0/10	WAF远程运维
出方向规则			
TCP: 9011	IPV4	100.125.0.0/16	WAF事件日志上报
TCP: 9012	IPV4	100.125.0.0/16	WAF事件日志上报
TCP: 9013	IPV4	100.125.0.0/16	WAF事件日志上报
TCP: 9018	IPV4	100.125.0.0/16	WAF策略同步
TCP: 9019	IPV4	100.125.0.0/16	WAF心跳日志上报
TCP: 4505	IPV4	100.125.0.0/16	WAF策略同步

协议端口	类型	源地址	描述
TCP: 4506	IPV4	100.125.0.0/16	WAF策略同步
TCP: 50051	IPV4	100.125.0.0/16	WAF性能日志上报
TCP: 443	IPV4	100.125.0.0/16	WAF策略同步

3 网站接入 WAF

3.1 网站接入概述

如果要使用Web应用防火墙（Web Application Firewall，WAF）防护您的Web业务，您必须先将Web业务接入WAF。WAF支持云模式-CNAME接入、云模式-ELB接入和独享模式三种接入方式，您可以根据Web业务的部署特征，选择合适的接入方式。本文通过实现原理、推荐场景、接入对象和接入方式的对比进行介绍。

📖 说明

独享模式在部分区域已经停售，详见[独享模式停售通知](#)。

使用场景

根据不同模式的使用场景、防护对象选择网站接入方式。

- 云模式-CNAME接入：
 - 业务服务器部署在华为云、非华为云或线下
 - 防护对象：域名
 - 接入方式：[将网站接入WAF防护（云模式-CNAME接入）](#)
- 云模式-ELB接入：
 - 业务服务器部署在华为云。
大型企业网站，对业务稳定性有较高要求的安全防护需求。
 - 防护对象：域名或IP（公网IP/私网IP）
 - 接入方式：[网站接入WAF（云模式-ELB接入）](#)
- 独享模式：
 - 业务服务器部署在华为云。
大型企业网站，具备较大的业务规模且基于业务特性具有制定个性化防护规则的安全需求。
 - 防护对象：域名或IP（公网IP/私网IP）
 - 接入方式：[将网站接入WAF防护（独享模式）](#)

约束限制

WAF不同接入模式的约束限制如下。

云模式-CNAME 接入

使用云模式-CNAME接入方式将网站接入WAF防护时，有如下限制：

限制项	限制条件
域名限制	<ul style="list-style-type: none">同一防护域名不能重复添加到WAF云模式。同一个域名对应不同非标准端口视为不同的防护对象，例如www.example.com:8080和www.example.com:8081为两个不同的防护对象，且占用两个域名防护配额。如果您需要防护同一域名的多个端口，您需要将该域名和端口逐一添加到WAF。请确保域名经过ICP（Internet Content Provider）备案，WAF会检查域名备案情况，未备案域名将无法添加。
服务版本限制	<ul style="list-style-type: none">入门版不支持添加泛域名。仅专业版和铂金版支持IPv6防护、HTTP2协议、负载均衡算法。入门版、标准版“策略配置”只能选择“系统自动生成策略”。
证书限制	<ul style="list-style-type: none">WAF当前仅支持PEM格式证书。目前华为云SCM证书只能推送到“default”企业项目下。如果您使用其他企业项目，则不能选择使用SCM推送的SSL证书。拥有“SCM Administrator”和“SCM FullAccess”权限的账号才能选择SCM证书。
WebSocket协议限制	WAF支持WebSocket协议，且默认为开启状态。 <ul style="list-style-type: none">“对外协议”选择“HTTP”时，默认支持WebSocket“对外协议”选择“HTTPS”时，默认支持WebSockets
HTTP2协议限制	HTTP2协议仅适用于客户端到WAF之间的访问，且“对外协议”必须包含HTTPS才支持使用。 <ul style="list-style-type: none">“服务器配置”中至少有一条源站地址的“对外协议”配置为HTTPS，开启后才会生效。当客户端最大支持TLS 1.2时，HTTP2才生效。
规格限制	将网站接入WAF后，网站的文件上传请求限制为1G。

云模式-ELB 接入

使用云模式-ELB接入方式将网站接入WAF防护时，有如下限制：

- 仅支持与独享型ELB配套使用，且“规格”必须为“应用型（HTTP/HTTPS）”，不支持“网络型（TCP/UDP）”的独享型的ELB。

- “策略配置”：只有专业版和铂金版支持选择自定义的防护策略。
- 规格限制：将网站接入WAF后，网站的文件上传请求限制为10G。

独享模式

使用独享模式将网站接入WAF防护时，有如下限制：

限制项	限制条件
ELB限制	<p>将网站以独享模式接入WAF时，仅支持与独享型ELB配套使用。有关ELB类型的详细介绍，请参见共享型弹性负载均衡与独享型负载均衡的功能区别。</p> <p>说明 2023年4月之前的独享引擎版本，不支持与独享ELB网络型配合使用。因此，如果您使用了独享ELB网络型（TCP/UDP）负载均衡，请确认独享WAF实例已升级到最新版本（2023年4月及之后的版本），独享引擎版本详情请参见独享引擎版本迭代。</p>
域名限制	<ul style="list-style-type: none">● WAF支持添加“*”的泛域名，域名配置为“*”时，只能防护除80、443端口以外的非标端口。● 同一防护对象不能重复添加到WAF。 同一个域名对应不同非标准端口视为不同的防护对象，例如www.example.com:8080和www.example.com:8081为两个不同的防护对象，且占用两个域名防护配额。如果您需要防护同一域名的多个端口，您需要将该域名和端口逐一添加到WAF。
代理限制	<p>如果WAF前有使用CDN、云加速等七层代理服务器，“是否使用七层代理”务必选择“是”，选择“是”后，WAF将从配置的Header头中字段中获取用户真实访问IP，详见配置攻击惩罚的流量标识。</p>
证书限制	<ul style="list-style-type: none">● WAF当前仅支持PEM格式证书。● 目前华为云SCM证书只能推送到“default”企业项目下。如果您使用其他企业项目，则不能选择使用SCM推送的SSL证书。● 拥有“SCM Administrator”和“SCM FullAccess”权限的账号才能选择SCM证书。
WebSocket协议限制	<p>WAF支持WebSocket协议，且默认为开启状态。</p> <ul style="list-style-type: none">● “对外协议”选择“HTTP”时，默认支持WebSocket● “对外协议”选择“HTTPS”时，默认支持WebSockets
规格限制	<p>将网站接入WAF后，网站的文件上传请求限制为10G。</p>

网站接入流程

WAF不同接入模式的网站接入流程如下。

云模式-CNAME 接入

以云模式CNAME接入方式接入网站时，您可以参照图3-1所示的配置流程，快速使用WAF。

图 3-1 网站接入 WAF 的操作流程图-云模式（CNAME 接入）

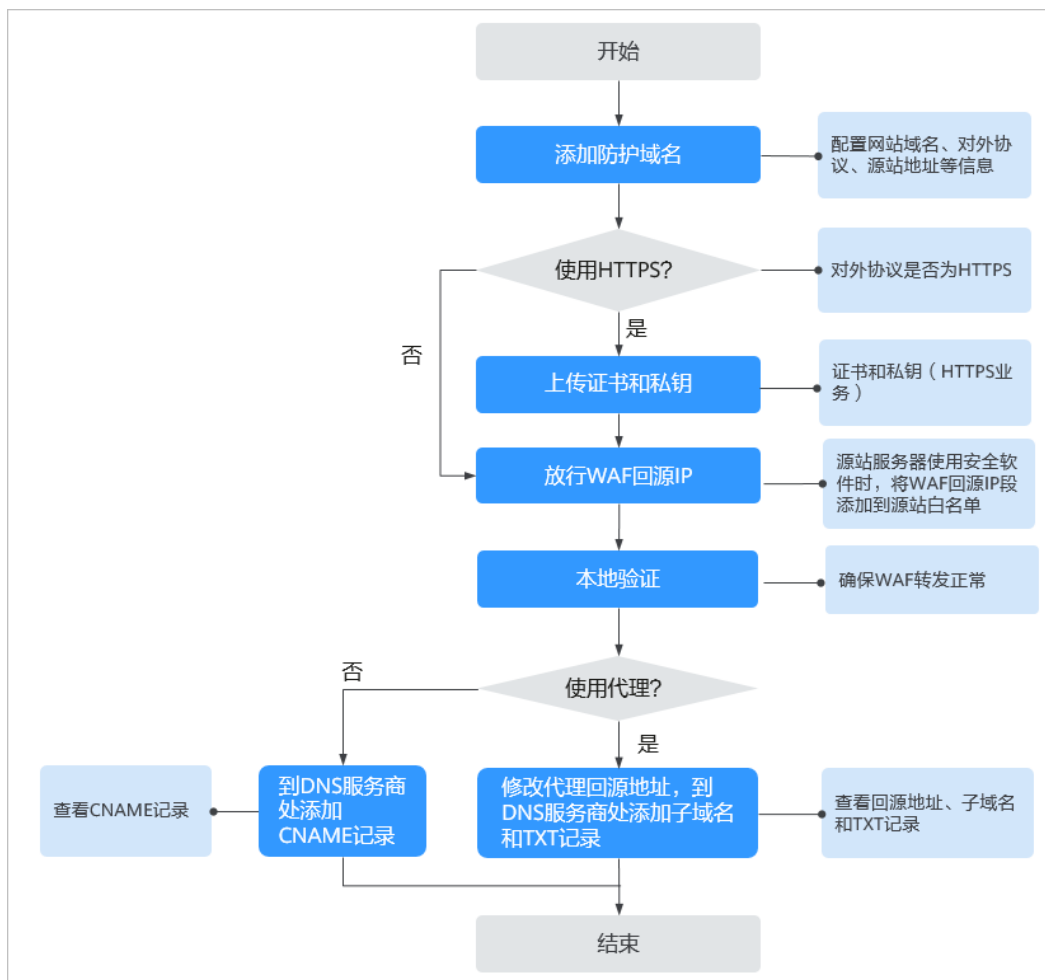


表 3-1 域名接入 WAF 操作流程说明

操作步骤	说明
添加防护域名	配置域名、协议、源站等相关信息。
WAF回源IP加白	如果您的源站服务器安装了其他安全软件或防火墙，建议您配置只允许来自WAF的访问请求访问您的源站，这样既可保证访问不受影响，又能防止源站IP暴露后被黑客直接攻击。
本地验证	添加域名后，为了确保WAF转发正常，建议您先通过本地验证确保一切配置正常，然后再修改DNS解析。

操作步骤	说明
修改域名DNS解析设置	<ul style="list-style-type: none"> 域名在接入WAF前未使用代理到该域名的DNS服务商处，配置防护域名的别名解析。 域名在接入WAF前使用代理（DDoS高防、CDN等）将使用的代理类服务（DDoS高防、CDN等）的回源地址修改为目标域名的“CNAME”值。

云模式-ELB 接入

一站式将网站接入WAF即可，具体操作请参见[将网站接入WAF防护（云模式-ELB接入）](#)。

独享模式

以WAF独享模式接入网站时，您可以参照图3-2所示的配置流程，快速使用WAF。

图 3-2 网站接入 WAF 的操作流程图-独享模式

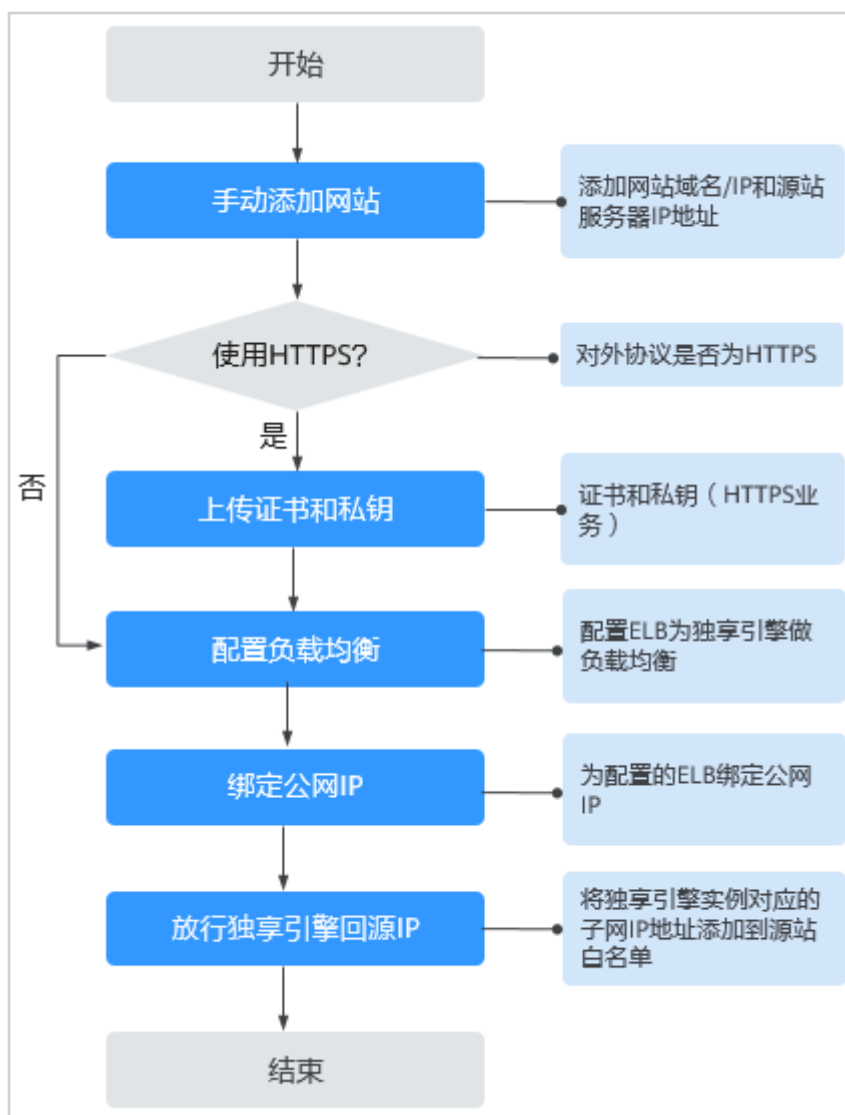


表 3-2 域名接入 WAF 操作流程说明

操作步骤	说明
添加防护网站	配置防护网站（域名或IP）、协议、源站等相关信息。
为WAF独享引擎实例配置负载均衡	添加防护网站后，您需要使用华为云弹性负载均衡（Elastic Load Balance，简称ELB）为WAF独享引擎实例配置负载均衡和健康检查，以确保WAF的可靠性和稳定性。
为弹性负载均衡绑定弹性公网IP	解绑源站服务器的弹性公网IP（Elastic IP，简称EIP），将解绑的弹性公网IP绑定到WAF独享引擎实例配置的负载均衡上。绑定后，请求流量会先经过WAF独享引擎进行攻击检测，然后转发到源站服务器，从而确保源站安全、稳定、可用。
放行独享引擎回源IP	源站服务器上的安全软件很容易认为独享引擎的回源IP是恶意IP，有可能触发屏蔽WAF回源IP的操作。一旦WAF的回源IP被屏蔽，WAF的请求将无法得到源站的正常响应，因此，网站以“独享模式”接入WAF防护后，您需要在源站服务器上设置放行创建的独享引擎实例对应的子网IP，不然可能会出现网站打不开或打开极其缓慢等情况。
验证WAF独享引擎实例转发正常	添加防护网站后，验证WAF转发和ELB运行是否正常。

3.2 将网站接入 WAF 防护（云模式-CNAME 接入）

3.2.1 将网站接入 WAF 防护（云模式-CNAME 接入）

如果您的业务服务器部署在华为云、非华为云或云下，您可以使用云模式的CNAME接入方式将网站的域名添加到WAF进行防护。业务开通WAF后，您需要将网站接入WAF才能开启防护。CNAME模式下，WAF将作为一个反向代理，使用特定的回源IP段将经过WAF检测后的正常流量转发回Web业务的源站服务器。

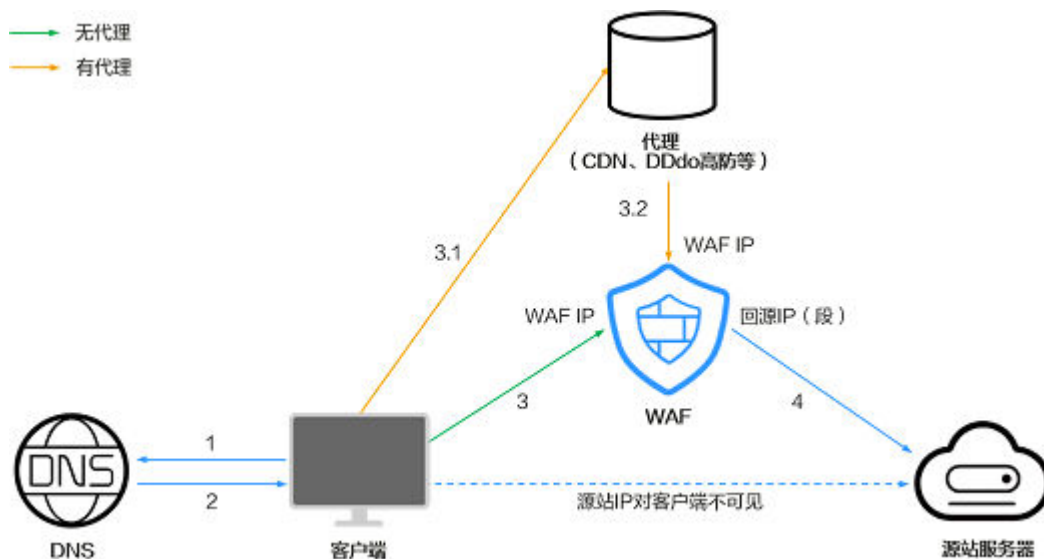
说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，在该企业项目下添加防护网站。

方案概述

CNAME模式下，将网站接入WAF，就是实现将网站流量牵引到WAF进行检测，再将检测后的流量转发到源站的过程。网站接入WAF后，流量访问示意图如图3-3所示。

图 3-3 网站流量访问示意图



流量访问说明如下：

1. 用户在浏览器输入域名后，客户端会向DNS发送请求，查询域名解析地址。
2. DNS返回域名解析地址。
3. 如果无代理（例如CDN、DDos高防等），DNS返回的域名解析地址为WAF IP，客户端通过WAF IP访问WAF。如果存在代理：
 - a. DNS返回的域名解析地址为代理IP，客户端通过代理IP访问代理。
 - b. 代理通过WAF IP访问WAF。
4. WAF对流量进行检测后，拦截异常流量，使用回源IP（段）将正常流量转发到源站服务器。

接入流程

根据网站是否使用代理（例如高防、CDN、云加速等），您需要完成如下接入操作。

操作步骤	说明
步骤一：添加防护域名	介绍如何将防护域名、源站信息等添加到WAF。
步骤二：放行回源IP	介绍如何获取回源IP，放行回源IP。
步骤三：本地验证	介绍如何在本地计算机验证域名接入配置是否生效。
步骤四：修改域名DNS解析设置	<ul style="list-style-type: none"> ● 未使用代理：介绍如何修改DNS解析为WAF CNAME。 ● 使用代理：介绍如何修改代理的回源地址为WAF CNAME。
步骤五：接入验证	介绍如何验证域名是否接入成功、基础防护是否生效。


前提条件


- 已购买WAF云模式，并已了解[网站接入](#)的相关信息。
- 确保域名经过ICP（Internet Content Provider）备案，WAF会检查域名备案情况，未备案域名将无法添加。

步骤一：添加防护域名

为了将业务接入WAF防护，您需要将防护域名、源站信息等，添加到WAF。

步骤1 [登录管理控制台](#)。

步骤2 在管理控制台左上角，单击 ，选择区域或项目。

步骤3 在页面左上方，单击 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，单击“网站设置”，进入“网站设置”页面。

步骤5 在网站列表左上角，单击“添加防护网站”。

步骤6 选择“云模式-CNAME接入”并单击“开始配置”。

步骤7 基础信息配置，如[图3-4](#)所示，参数说明如[表3-3](#)所示。

图 3-4 基础信息配置



防护域名 

[快速添加云内域名](#)

请确保域名已经过ICP备案 (<https://beian.xinnet.com/>)，WAF会检查域名备案情况，未备案域名将无法添加。

网站名称(可选)

网站备注(可选)

防护端口

[查看可添加端口](#)

标准端口为HTTP对外协议80和HTTPS对外协议443

服务配置 

对外协议	源站协议	源站地址	源站端口	权重	操作
<input type="text" value="HTTP"/>	<input type="text" value="HTTP"/>	<input type="text" value="IPv4"/> <input type="text" value="公网IP地址或者域名"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	删除

[添加地址](#) 您还可以添加159个源站地址

是否使用七层代理 

是 否

七层代理：使用了DDoS高防（七层代理）、CDN、云加速等Web代理产品。注：设置七层代理后，WAF将从Header头中的相关字段获取用户真实访问IP。 [查看详情](#)

表 3-3 基础信息参数说明

参数	参数说明	取值样例
防护域名	<p>需要添加到WAF进行防护的域名，支持单域名（例如，一级域名example.com，二级域名www.example.com等）和泛域名（例如，*.example.com）。</p> <p>须知</p> <ul style="list-style-type: none">入门版不支持添加泛域名。泛域名添加说明如下：<ul style="list-style-type: none">如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。同一个域名对应不同端口视为不同的域名，例如www.example.com:8080和www.example.com:8081视为两个不同的域名，将占用两个不同的域名防护额度。请确保域名经过ICP（Internet Content Provider）备案，WAF会检查域名备案情况，未备案域名将无法添加。	-
网站名称 (可选)	自定义网站名称。	WAF
网站备注 (可选)	网站的备注信息。	wafstest
防护端口	<p>要防护的端口。</p> <ul style="list-style-type: none">配置为80、443端口时，在下拉框中选择“标准端口”。配置为其他端口时，所选端口必须在可选端口范围内。您可以单击“查看可添加端口”，查看WAF支持的HTTP和HTTPS端口。更多信息请参见WAF支持的端口范围。 <p>说明</p> <p>如果配置了除80/443以外的其他端口，访问网站时，需要在网址后面增加非标准端口进行访问，否则访问网站时会出现404错误。</p>	81

参数	参数说明	取值样例
服务器配置	<p>网站服务器相关信息，包括对外协议、源站协议、源站地址、源站端口和权重。</p> <ul style="list-style-type: none"> ● 对外协议：客户端请求访问服务器的协议类型，包括“HTTP”、“HTTPS”两种。HTTPS协议是HTTP的安全版本，它在HTTP下增加了SSL/TLS协议，提供了数据加密、完整性校验和身份验证。因此，选择HTTPS协议时，需要配置证书。 “对外协议”选择“HTTPS”时，支持开启HTTP2协议。 <p>说明 “防护端口”选择“标准端口”时，HTTPS协议默认防护的443端口，HTTP协议默认防护的80端口。</p> <ul style="list-style-type: none"> ● 源站协议：网站服务器支持的协议类型。也是Web应用防火墙转发客户端请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。 <p>说明 如果“对外协议”与“源站协议”不一致，WAF会将“对外协议”转换为“源站协议”，使用“源站协议”来转发客户端的请求。</p> <ul style="list-style-type: none"> ● 源站地址：客户端访问的网站服务器的公网IP地址（一般对应该域名在DNS服务商处配置的A记录）或者域名（一般对应该域名在DNS服务商处配置的CNAME）。支持以下两种IP格式： <ul style="list-style-type: none"> - IPv4，例如：XXX.XXX.1.1 - IPv6，例如： fe80:0000:0000:0000:0000:0000:0000:0000 <p>须知 仅专业版和铂金版支持IPv6防护。</p> <ul style="list-style-type: none"> ● 源站端口：WAF转发客户端请求到服务器的业务端口。 ● 权重：负载均衡算法将按权重将请求分配给源站。 	<p>对外协议： HTTP</p> <p>源站协议： HTTP</p> <p>源站地址： IPv4 XXX.XXX.1.1</p> <p>源站端口：80</p>

参数	参数说明	取值样例
证书选择	<p>“对外协议”设置为“HTTPS”时，需要选择证书。</p> <ul style="list-style-type: none"> 如果您未创建证书，单击“导入新证书”，在“导入新证书”对话框，填写证书相关参数。更多信息，请参见上传证书。成功导入的新证书，将同步添加到“证书管理”页面的证书列表。 如果已创建证书，在下拉框“已有证书”中选择正确、有效的证书。 如果您已经在同一个账号下使用了CCM中证书，也可以直接在下拉框中选择SCM证书，此处选择的SCM证书名称与CCM里证书名称一致。 <p>须知</p> <ul style="list-style-type: none"> WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考如何将非PEM格式的证书转换为PEM格式?将证书转换为PEM格式，再上传。 目前华为云SCM证书只能推送到“default”企业项目下。如果您使用其他企业项目，则不能选择使用SCM推送的SSL证书。 选择的SCM证书会自动在“证书管理”页面生成一条记录，该证书支持在“证书管理”页面修改证书名称，但不会同步修改CCM里显示的证书名称。 如果您的证书即将到期，为了不影响网站的使用，建议您在到期前重新使用新的证书，并在WAF中同步更新网站绑定的证书。WAF支持证书过期时发送告警通知，您可以在“告警通知”界面配置证书过期提醒，具体的操作请参见开启告警通知。 域名和证书需要一一对应，泛域名只能使用泛域名证书。如果您没有泛域名证书，只有单域名对应的证书，则只能在WAF中按照单域名的方式逐条添加域名进行防护。 	-
最低TLS版本和加密套件	<p>选择证书后，需要选择最低TLS版本和加密套件。WAF默认配置的最低TLS版本为TLS v1.0，加密套件为“安全加密套件”。更多信息，请参见配置PCI DSS/3DS合规与TLS。</p>	<p>最低TLS版本：TLS v1.0</p> <p>加密套件：安全加密套件</p>
是否使用七层代理	<ul style="list-style-type: none"> 是：使用了DDoS高防（七层代理）、CDN、云加速等Web代理产品。 否：没有使用七层代理。 <p>须知</p> <ul style="list-style-type: none"> 选择“是”后，即在WAF前使用了七层代理，WAF将从配置的Header头中的相关字段获取用户真实访问IP，详见配置攻击惩罚的流量标识。 如果WAF前使用的是华为云DDoS高防，要获取客户端真实IP，需要在域名基本信息页面的“流量标识”栏，将“IP标记”配置为“\$remote_addr”详细操作请参见配置攻击惩罚的流量标识。 	无代理

步骤8 高级配置，如图3-5所示。

图 3-5 高级配置



表 3-4 高级配置参数说明

参数	参数说明	取值样例
负载均衡算法	<p>存在多个源站服务器地址时, 需选择多源站服务器间的负载均衡算法。</p> <ul style="list-style-type: none"> 源IP Hash: 将某个IP的请求定向到同一个服务器。 加权轮询: 所有请求将按权重轮流分配给源站服务器, 权重越大, 回源到该源站的几率越高。 Session Hash: 将某个Session标识的请求定向到同一个源站服务器, 请确保在域名添加完毕后配置攻击惩罚的流量标识, 否则Session Hash配置不生效。 <p>更多信息请见修改负载均衡算法。</p>	加权轮询

参数	参数说明	取值样例
IPv6防护	<p>如果该域名存在IPv6协议的访问请求，请选择“开启”，开启后WAF将为域名分配IPv6的接入地址。更多信息请参见开启IPv6防护。</p> <p>说明</p> <ul style="list-style-type: none"> 仅专业版和铂金版支持IPv6防护。 “源站地址”选择“IPv6”时，默认开启“IPv6防护”。 “源站地址”选择“IPv4”时，开启“IPv6防护”后，WAF将为域名分配IPv6的接入地址，即将IPv4源站转化成IPv6网站，将外部IPv6访问流量转化成对内的IPv4流量。具体的请参见WAF如何解析/访问IPv6源站?。 当源站存在IPv6地址，默认开启IPv6防护。WAF为了防止客户IPv6的业务中断，禁止关闭IPv6的开关，如果确定不需要IPv6防护，需要先修改服务器配置，在源站删除IPv6的配置，具体的操作方法请参见修改服务器配置信息。 	开启
HTTP2协议	<p>如果您的网站需要支持HTTP2协议的访问，则选择“使用”。</p> <p>HTTP2协议仅适用于客户端到WAF之间的访问，且“对外协议”必须包含HTTPS才支持使用。</p> <p>须知</p> <ul style="list-style-type: none"> 仅专业版和铂金版支持HTTP2协议。 “服务器配置”中至少有一条源站地址的“对外协议”配置为HTTPS，开启后才会生效。 当客户端最大支持TLS 1.2时，HTTP2才生效。 	使用
防护策略	<p>选择要启用的防护策略。</p> <ul style="list-style-type: none"> “系统自动生成策略”（默认）：详细说明如表 3-5所示。如果已添加的防护策略达到配额，不支持选择该项。 自定义防护策略：根据防护需求创建的防护策略。更多信息，请参见配置防护策略。 <p>须知</p> <p>入门版、标准版只能选择“系统自动生成策略”。</p>	系统自动生成策略

表 3-5 系统自动生成策略说明

版本	防护策略	策略说明
入门版、标准版	Web基础防护（“仅记录”模式、常规检测）	仅记录SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击行为。

版本	防护策略	策略说明
专业版、铂金版	Web基础防护（“仅记录”模式、常规检测）	仅记录SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击行为。
	网站反爬虫（“仅记录”模式、扫描器）	仅记录漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap的爬虫行为。

📖 说明

“仅记录”模式：发现攻击行为后WAF只记录攻击事件不阻断攻击。

步骤9 单击“下一步”，添加域名完成。

根据界面提示，完成放行WAF回源IP、本地验证和修改域名DNS解析设置的配置操作。

图 3-6 添加域名完成



----结束

步骤二：放行回源 IP

回源IP是WAF转发正常客户端请求到服务器时用的源IP，在服务器看来，接入WAF后所有源IP都会变成WAF的回源IP，而真实的客户端地址会被加在HTTP头部的XFF字段中。

如果源站使用了其他防火墙、网络ACL、安全组、杀毒软件等，很容易把WAF的回源IP当作恶意IP进行拦截。因此，建议在源站服务器上配置只放行WAF回源IP全部端口的访问控制策略，防止黑客获取源站IP后绕过WAF直接攻击源站。

📖 说明

- WAF的回源IP会因为扩容/新建集群而增加，对于一个客户的存量域名，一般回源IP会固定在2~4个集群的几个C类IP地址（192.0.0.0~223.255.255.255）上。
- 一般情况下，在没有灾备切换或其他调度切换集群的场景下，回源IP不会变。且WAF后台做集群切换时，会探测源站安全组配置，确保不会因为安全组配置导致业务整体故障。

步骤1 获取WAF的回源IP。


完成**步骤一：添加防护域名**后展开“步骤一：放行回源IP”，或者在“网站设置”页面，在目标网站所在行的“接入状态”栏中，单击“回源IP加白”，单击, 复制所有回源IP。

图 3-7 复制回源 IP



步骤2 打开源站服务器上的安全软件，将复制的IP段添加到白名单。

- 源站服务器部署在华为云ECS上，请参考[源站服务器部署在ECS上，放行WAF回源IP](#)进行操作。
- 源站服务器部署在华为云ELB上，请参考[源站服务器部署在华为云ELB上，放行WAF回源IP](#)进行操作。
- 如果您同时使用了华为云云防火墙（CFW），请参考[添加防护规则](#)放行WAF的回源IP。
- 如果后端资源在其他云厂商，请在对应安全组、访问控制等中添加信任WAF的回源IP。
- 如果源站服务器只安装了个人版杀毒软件，通常这些软件没有配置加白IP的界面。如果是对外提供Web业务的服务器，建议您安装服务器版本的企业安全软件，或华为云主机安全服务产品，这些产品会识别一些请求量较大的IP的socket，并偶发断开连接，一般情况下不会拦截WAF的回源IP。

步骤3 完成以上操作后，勾选“已完成回源IP加白”。

---结束

步骤三：本地验证


您可以修改本地计算机的hosts文件，设置本地计算机的域名寻址映射（仅对本地计算机生效的DNS解析记录），在本地计算机上将网站域名的解析指向WAF的IP地址。这样就可以通过本地计算机访问被防护的域名，验证WAF中添加的域名接入设置是否正确有效，避免域名接入配置异常导致网站访问异常。

须知

进行此操作前请确认：

- 确保**添加的域名**（例如：www.example5.com）的源站服务器协议、地址、端口配置正确，如果“对外协议”选择了“HTTPS”，也必须确保上传的证书和私钥正确。
- 已完成**步骤二：放行回源IP**。

步骤1 获取CNAME值。

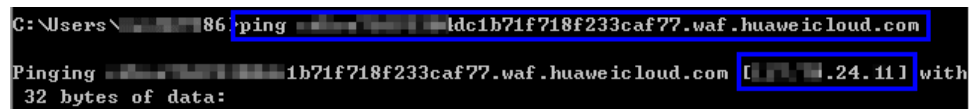
- 方式一：完成**步骤二：放行回源IP**后展开“步骤二：本地验证”，或者在“网站设置”页面中“接入状态”列单击“本地验证”，在弹出的页面中复制CNAME值。
- 方式二：在网站设置页面，在目标域名所在行中，单击目标域名名称，进入域名基本信息页面，在“CNAME”信息行，单击 ，复制“CNAME”值。

步骤2 ping “CNAME” 值并记录“CNAME” 对应的IP地址。

以域名www.example5.com为例，该域名已添加到WAF的网站配置中，且WAF为其分配了以下CNAME值：xxxxxxdc1b71f718f233caf77.waf.huaweicloud.com。

在Windows中打开cmd命令行工具或者Linux中的bash工具，运行ping xxxxxxxdc1b71f718f233caf77.waf.huaweicloud.com获取WAF的接入IP。如**图3-8**所示，在响应结果中可以看到用来防护您的域名的WAF接入IP。

图 3-8 ping cname



说明

如果ping cname没有获取到WAF的接入IP，可能是由于您的网络不稳定，请确保您的网络运行正常，再执行以上操作。

步骤3 在本地修改hosts文件，将域名及“CNAME” 对应的WAF接入IP添加到“hosts” 文件。

1. 用文本编辑器打开hosts文件，hosts文件路径如下：
 - Windows：“C:\Windows\System32\drivers\etc\”
 - Linux：“/etc/hosts”
2. 在hosts文件添加如**图3-9**内容，前面的IP地址即在**步骤2**中获取的WAF接入IP地址，后面的域名即被防护的域名。

图 3-9 追加记录

```
# Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# 192.168.1.1       # source server
# 192.168.1.2       # x client host
#
# localhost name resolution is handled within DNS itself.
#
#       localhost
#       ::1       localhost
24.11 www.example5.com
```

- 3. 修改hosts文件后保存，然后在命令行工具运行ping一下被防护的域名。

图 3-10 ping 域名

```
C:\Users\...> ping www.example5.com
Pinging www.example5.com [24.11] with 32 bytes of data:
```

预期此时解析到的IP地址应该是2中绑定的WAF的接入IP地址。如果依然是源站地址，可尝试刷新本地的DNS缓存（Windows的cmd下可以使用ipconfig/flushdns命令，Linux的bash下可以使用systemd-resolved命令）。

步骤4 访问验证。

- 1. 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。
如果hosts绑定已经生效（域名已经本地解析为WAF回源IP）且WAF的配置正确，访问该域名，预期网站能够正常打开。
- 2. 手动模拟简单的Web攻击命令，测试Web攻击请求。
 - a. 将Web基础防护的状态设置为“拦截”模式，具体方法请参见配置Web基础防护规则。
 - b. 清理浏览器缓存，在浏览器中输入模拟SQL注入攻击的测试域名，测试WAF是否拦截了此条攻击，如图3-11所示。

图 3-11 访问被拦截



- c. 在左侧导航树中，选择“防护事件”，进入“防护事件”页面，查看防护域名测试的各项数据。

步骤5 完成上述步骤后，勾选“已完成本地验证”。

----结束

步骤四：修改域名 DNS 解析设置

将域名添加到WAF后，WAF作为一个反向代理存在于客户端和服务端之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址，所以您必须将域名的DNS解析指向WAF提供的CNAME地址，才可以使域名的Web请求解析到WAF进行安全防护。本地验证通过后，您需要在DNS服务商处修改DNS解析设置，将网站的Web请求解析到WAF进行安全防护。


须知

修改域名DNS解析设置前请确认：

- 已完成**步骤一：添加防护域名**、**步骤二：放行回源IP**、**步骤三：本地验证**。
- 您拥有在域名的DNS服务商处修改域名解析设置的权限。

未使用代理

步骤1 获取WAF的CNAME。

- 方式一：完成**步骤三：本地验证**后展开“步骤三：DNS解析”，或者在“网站设置”页面中“接入状态”列单击“修改DNS解析”，在弹出的页面复制CNAME值。
- 方式二：在网站设置页面，在目标域名所在行中，单击目标域名名称，进入域名基本信息页面，在“CNAME”信息行，单击，复制“CNAME”值。

步骤2 修改域名DNS解析为WAF的CNAME值。

到该域名的DNS服务商处，配置防护域名的别名解析，具体操作请咨询您的域名服务提供商。

以下为华为云DNS的CNAME绑定方法，仅供参考。如与实际配置不符，请以各自域名服务商的信息为准。


1. 单击页面左上方的，选择“网络 > 云解析服务 DNS”。
2. 在左侧导航栏中，选择“公网域名”，进入“公网域名”页面。
3. 在目标域名所在行的“操作”列，单击“管理解析”，进入“解析记录”页面。

图 3-12 解析记录



域名	DNS记录集名称	记录个数	状态	记录	TTL (秒)	创建时间	最后修改时间	描述	全局设置	操作
test.com	test.com	2	--	waf.cname.huaweicloud.com	300	2024/02/11 15:55:00	2024/02/11 15:55:00		default	管理解析 域名信息 删除 更多
test.com	test.com	11	--	test.com	300	2024/05/09 17:55:00	2024/05/09 17:55:00	Domain Name Res.	default	管理解析 域名信息 删除 更多

4. 在目标记录集的所在行“操作”列，单击“修改”。

5. 在弹出的“修改记录集”对话框中修改记录值。
 - “主机记录”：在WAF中配置的域名。
 - “记录类型”：选择“CNAME-将域名指向另外一个域名”。
 - “线路类型”：全网默认。
 - “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
 - “记录值”：修改为已复制的WAF CNAME地址。
 - 其他的设置保持不变。

图 3-13 修改记录集

修改记录集

主机记录: www .examplel.com

记录类型: CNAME - 将域名指向另外一个域名

别名: 是 否

线路类型: ② 全网默认

* TTL (秒): 300

* 记录值: de35f9627af342199580534f0:waf.com.

CNAME记录: 填写您要指向的别名, 只能写一个域名。
例如:
www.example.com

权重: 请输入0~1,000之间的数字
当域名在同一解析线路中有多条相同类型的解析记录时, 可以通过“权重”设置解析记录集的响应比例。 [查看详情](#)

描述: 0/255

说明

关于修改解析记录:

- 对于同一个主机记录, CNAME解析记录不能重复, 您需要将已存在的解析记录的CNAME修改为WAF CNAME地址。
- 同一解析记录下, 不同DNS解析记录类型间可能存在冲突。例如, 对于同一个主机记录, CNAME记录与A记录、MX记录、TXT记录等其他记录互相冲突。在无法直接修改记录类型的情况下, 您可以先删除存在冲突的其他记录, 再添加一条新的CNAME记录。删除其他解析记录并新增CNAME解析记录的过程应尽可能在短时间内完成。如果删除A记录后没有添加CNAME解析记录, 可能导致域名无法正常解析。


域名解析类型的限制规则请参见[添加记录集时, 为什么会提示“与已有解析记录冲突”?](#)

6. 单击“确定”, 完成DNS配置, 等待DNS解析记录生效。

----结束

使用代理


步骤1 获取WAF的CNAME。

- 方式一：完成**步骤三：本地验证**后单击“步骤三：修改回源地址”，或者在“网站设置”页面中“接入状态”列单击“修改代理回源地址”，在弹出的页面中复制CNAME值。
- 方式二：在网站设置页面，在目标域名所在行中，单击目标域名名称，进入域名基本信息页面，在“CNAME”信息行，单击，复制“CNAME”值。

步骤2 确认DNS的解析已指向代理，同时将使用的代理类服务（高防、CDN服务等）的回源地址修改为复制的目标域名的CNAME，具体的方法请参见[网站业务接入](#)。

说明

为了防止其他用户提前将您的域名配置到Web应用防火墙上，从而对您的域名防护造成干扰，建议您的DNS服务商处添加“子域名”和“TXT记录”。

1. 获取“子域名”和“TXT记录”：在域名基本信息页面顶部，单击“未接入”旁边的, 在弹出的对话框中，复制“子域名”和“TXT记录”。
2. 到DNS服务商处添加“子域名”，并为它配置“TXT记录”。具体的配置方法请参见[未配置子域名和TXT记录的影响](#)。

WAF会根据配置“子域名”和“TXT记录”判断域名的所有权属于哪个用户。

----结束

配置验证

完成如上配置后，您需要验证域名的CNAME是否配置成功。

步骤1 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”。

步骤2 执行nslookup命令，查询CNAME。

如果回显的域名是配置的CNAME，则表示配置成功，示例如[图3-14](#)所示。

以域名www.example.com为例。

```
nslookup www.example.com
```

图 3-14 查询 CNAME




步骤3 完成以上步骤，勾选“已完成DNS解析”。

----结束

步骤五：接入验证

- 接入状态验证。
一般情况下，如果您确认已完成域名接入，“接入状态”为“已接入”，表示域名接入成功。

📖 说明

如果防护域名已接入WAF，“接入状态”仍然为“未接入”或“DNS解析异常”，可单击，刷新状态，如果仍然为“未接入”，可参照[域名/IP接入状态显示“未接入”，如何处理？](#)重新完成域名接入。

- 网站访问验证。
 - 在浏览器中输入防护域名，测试网站域名是否能正常访问。

📖 说明

如果配置了非标准端口，访问网站时，需要在网址后面增加非标准端口进行访问，否则访问网站时会出现[404错误](#)。

- 手动模拟简单的Web攻击命令，验证WAF防护是否生效。具体操作，请参见[步骤4.2](#)。

后续操作

域名接入成功后建议您完成以下操作：

- [网站接入后推荐配置](#)
 - 防护网站的“对外协议”使用了“HTTPS”协议时，支持[配置PCI DSS/3DS合规与TLS](#)、[开启HTTP2协议](#)、[开启Cookie安全属性](#)。
 - [开启IPv6防护](#)：帮助源站实现IPv6协议请求的安全防护。
 - [配置WAF到网站服务器的连接超时时间](#)：WAF到源站的连接超时时长默认为30秒，支持自定义“连接超时”、“读超时”、“写超时”的时间。
 - [配置攻击惩罚的流量标识](#)：配置客户端IP标识、Session标识或User标识，实现IP、Cookie或Params恶意请求的攻击惩罚功能。
 - [配置Header字段转发](#)：添加Header字段后，WAF会将该字段插入到Header中，转发给源站，用以标记请求。
 - [修改拦截返回页面](#)：自定义触发WAF拦截时的返回页面。
- 根据防护需求，调整防护域名配置的防护策略，详见[防护配置概述](#)。

3.2.2 配置示例

添加防护域名时，可根据您的业务场景参考以下示例进行配置。

- [示例一：80/443端口业务防护配置](#)
- [示例二：客户端请求转发到不同的源站服务器](#)
- [示例三：同一域名对应不同的防护端口](#)
- [示例四：不同访问模式的协议配置规则](#)

示例一：80/443 端口业务防护配置

配置场景：需要防护域名对应的80或者443端口的业务。

1. 防护端口：选择“标准端口”。
2. 对外协议：
 - 防护80端口：选择“HTTP”协议。
 - 防护443端口：选择“HTTPS”协议。

- 同时防护80端口和443端口：配置两条服务器地址，“对外协议”分别选择HTTP、HTTPS，如图3-15所示。

图 3-15 同时防护 80 端口和 443 端口

防护端口

标准端口 查看可添加端口

标准端口为HTTP对外协议80和HTTPS对外协议443

服务器配置 ?

对外协议	源站协议	源站地址	源站端口	权重	操作
HTTP	HTTP	IPv4 公网IP地址或者域名			删除
HTTPS	HTTP	IPv4 公网IP地址或者域名			删除

[添加地址](#) 您还可以添加48个源站地址

说明

- 图3-15中红框内的参数配置是固定的配置，其他参数配置根据实际情况进行配置。
- 此场景下，访问网站时，域名后可以不加端口号进行访问。例如，在浏览器中直接输入“http://www.example.com”访问网站。

示例二：客户端请求转发到不同的源站服务器

配置场景：同一个防护对象，需要WAF将客户端请求转发到不同的源站服务器。

例如，需要将防护域名www.example.com，防护端口8080添加到WAF防护，并需要WAF将请求转发到两台后端服务器。

1. 防护域名：www.example.com
2. 防护端口：8080
3. 对外协议：系统会根据选择的防护端口，自动匹配对外协议。仅HTTP协议支持防护8080端口，因此，添加的两条服务器地址中的“对外协议”都配置为HTTP，具体配置如图3-16所示。

图 3-16 客户端请求转发到不同的源站服务器

基础信息

防护域名 ?

www.example.com [快速添加云内域名](#)

请确保域名已经过ICP备案 (https://beian.xinnet.com/)，WAF会检查域名备案情况，未备案域名将无法添加。

网站名称 (可选)

您可以自定义域名名称

网站备注 (可选)

您可以填写备注信息

防护端口

8080 [查看可添加端口](#)

标准端口为HTTP对外协议80和HTTPS对外协议443

服务器配置 ?

对外协议	源站协议	源站地址	源站端口	权重	操作
HTTP	HTTP	IPv4 12	12		删除
HTTP	HTTP	IPv4 12	12		删除

[添加地址](#) 您还可以添加48个源站地址

说明

- 图3-16中红框内的参数配置是固定的配置，其他参数配置根据实际情况进行配置。
- 此场景下，访问网站时，域名后必须加端口号进行访问，否则会报404错误。例如，在浏览器中输入“http://www.example.com:8080”访问网站。

示例三：同一域名对应不同的防护端口

同一个域名对应不同非标准端口视为不同的防护对象，例如www.example.com:8080和www.example.com:8081为两个不同的防护对象，且占用两个域名防护配额。如果您需要防护同一域名的多个端口，您需要将该域名和端口逐一添加到WAF。

示例四：不同访问模式的协议配置规则

根据您的业务场景的不同，WAF提供灵活的协议类型配置。假设您的网站为www.example.com，WAF可配置如下四种访问模式：

- HTTP访问模式，“对外协议”和“源站协议”都配置为HTTP，如图3-17所示。此场景下，客户端访问网站和WAF转发请求到源站，均使用HTTP传输，适用于不需要加密传输的场景。

图 3-17 HTTP 协议访问模式

防护域名

www.example.com [快速添加云内域名](#)

请确保域名已经过ICP备案 (https://beian.xinnet.com/)，WAF会检查域名备案情况，未备案域名将无法添加。

网站名称 (可选)

您可以自定义域名名称

网站备注 (可选)

您可以填写备注信息

防护端口

标准端口 [查看可添加端口](#)

标准端口为HTTP对外协议80和HTTPS对外协议443

服务器配置

对外协议	源站协议	源站地址	源站端口	权重	操作
HTTP	HTTP	IPv4	公网IP地址或者域名		删除

须知

- 图3-17中红框内的参数配置是固定的配置，其他参数配置根据实际情况进行配置。
 - 此种配置表示用户只能通过http://www.example.com访问网站，如果用户通过https://www.example.com访问网站，会收到302跳转响应，浏览器跳转到http://www.example.com。
-
- HTTPS访问模式，“对外协议”和“源站协议”全部配置为HTTPS时，当使用HTTP协议访问服务器时，会强制跳转为HTTPS协议，如图3-18所示。
此场景下，客户端访问网站和WAF转发请求到源站，均使用HTTPS加密传输，适用于需要加密传输的场景。

图 3-18 HTTPS 协议访问强制跳转模式

防护域名

www.example.com [快速添加云内域名](#)

请确保域名已经过ICP备案 (https://beian.xinnet.com/)，WAF会检查域名备案情况，未备案域名将无法添加。

网站名称 (可选)

您可以自定义域名名称

网站备注 (可选)

您可以填写备注信息

防护端口

标准端口 [查看可添加端口](#)

标准端口为HTTP对外协议80和HTTPS对外协议443

服务器配置

对外协议	源站协议	源站地址	源站端口	权重	操作
HTTPS	HTTPS	IPv4	公网IP地址或者域名		删除

须知

- **图3-18**中红框内的参数配置是固定的配置，其他参数配置根据实际情况进行配置。
 - 用户直接通过https://www.example.com访问网站，网站返回正常内容。
 - 用户通过http://www.example.com访问网站，用户会收到301跳转响应，浏览器跳转到https://www.example.com。
-
- HTTP/HTTPS分别转发模式，配置两条服务器配置，一条“对外协议”和“源站协议”全部配置为HTTP，一条“对外协议”和“源站协议”全部配置为HTTPS，如**图3-19**所示。
此场景仅适用于防护标准端口（80/443）的场景。

图 3-19 HTTP/HTTPS 分别转发模式

基础信息

防护域名 ?

www.example.com [快速添加云内域名](#)

请确保域名已经过ICP备案 (https://beian.xinnet.com/)，WAF会检查域名备案情况，未备案域名将无法添加。

网站名称 (可选)

您可以自定义域名名称

网站备注 (可选)

您可以填写备注信息

防护端口

标准端口 查看可添加端口

标准端口为HTTP对外协议80和HTTPS对外协议443

服务器配置 ?

对外协议	源站协议	源站地址	源站端口	权重	操作
HTTP	HTTP	IPv4 公网IP地址或者域名			删除
HTTPS	HTTPS	IPv4 公网IP地址或者域名			删除

[添加地址](#) 您还可以添加48个源站地址

须知

- **图3-19**中红框内的参数配置是固定的配置，其他参数配置根据实际情况进行配置。
 - 用户通过http://www.example.com访问网站，网站返回正常内容，没有跳转，网站内容不加密传输。
 - 用户通过https://www.example.com访问网站，网站返回正常内容，没有跳转，网站内容加密传输。
-
- 使用WAF做HTTPS卸载模式，“对外协议”选择“HTTPS”，“源站协议”选择“HTTP”，如**图3-20**所示。
此场景下，客户端访问网站时，采用HTTPS协议加密传输，WAF转发请求到源站使用HTTP协议。

图 3-20 使用 WAF 做 HTTPS 卸载模式

防护域名

www.example.com [快速添加云内域名](#)

请确保域名已经过ICP备案 (https://beian.xinnet.com/)，WAF会检查域名备案情况，未备案域名将无法添加。

网站名称 (可选)

您可以自定义域名名称

网站备注 (可选)

您可以填写备注信息

防护端口

标准端口 [查看可添加端口](#)

标准端口为HTTP对外协议80和HTTPS对外协议443

服务器配置

对外协议	源站协议	源站地址	源站端口	权重	操作
HTTPS	HTTP	IPv4	公网IP地址或者域名		删除

[添加地址](#) 您还可以添加49个源站地址

须知

- 图3-20中红框内的参数配置是固定的配置，其他参数配置根据实际情况进行配置。
- 用户通过https://www.example.com访问网站，但是WAF到源站依然使用HTTP协议。

3.3 将网站接入 WAF 防护（云模式-ELB 接入）

如果您的业务服务器部署在华为云，您可以使用云模式的ELB接入方式将网站的域名或IP添加到WAF进行防护。

已经使用了华为云独享型ELB进行流量转发的网站，才支持使用“云模式-ELB接入”将网站接入WAF，该方式WAF是旁路检测，不参与流量转发。建议您使用该方式前，先完成独享型ELB的配置。

说明

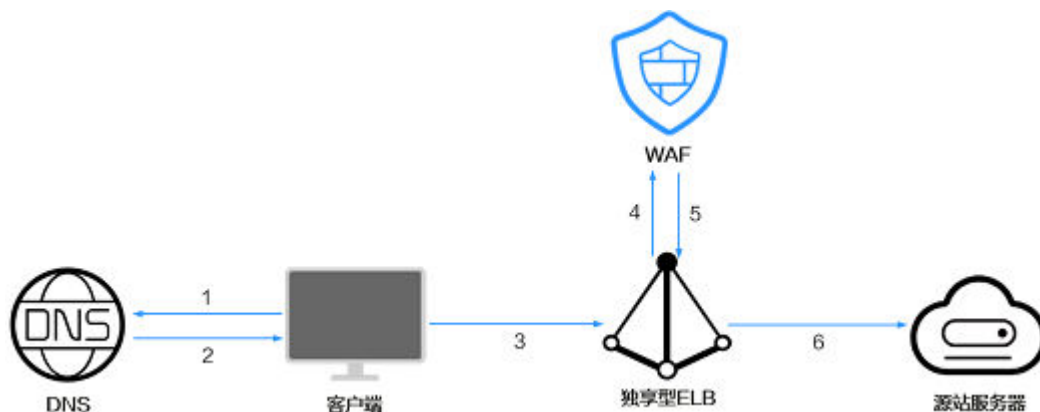
如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，在该企业项目下添加防护网站。

方案概述

ELB接入模式下，WAF通过SDK模块化的方式集成在ELB网关中。将网站接入WAF后，网站流量会被ELB镜像给WAF。WAF检测后，将结果同步给ELB，由ELB根据WAF检测结果决定是否将客户端请求转发到源站。该过程中，WAF不参与流量转发，避免因额外引入一层转发而带来各种兼容性和稳定性问题。

接入WAF后，网站访问示意图如图3-21所示。

图 3-21 网站访问示意图



流量访问说明如下：

1. 用户在浏览器输入域名后，客户端会向DNS发送请求，查询域名解析地址。
2. DNS返回域名解析地址。
3. 客户端通过EIP访问ELB。
4. ELB将流量镜像给WAF。
5. WAF检测后，将检测结果同步给ELB。
6. ELB根据WAF检测结果，将正常流量转发给源站服务器。

前提条件

- 已购买WAF的云模式，并已了解[网站接入](#)的相关信息。

📖 说明

- 云模式的ELB接入方式需要[提交工单](#)申请开通后才能使用，支持使用的Region请参考[功能总览](#)。
- 购买了云模式标准版、专业版或铂金版后，才支持使用ELB接入方式，域名、QPS、规则扩展包的配额与云模式的CNAME接入方式共用，且ELB接入方式的业务规格与购买的云模式版本的对应规格一致。
- 已在购买WAF云模式的账号下购买了独享型负载均衡，且“规格”为“应用型（HTTP/HTTPS）”，详见[创建独享型负载均衡器](#)。

网站以“云模式-ELB 接入”方式接入 WAF

步骤1 创建独享型负载均衡器。

- “规格”选择“应用型（HTTP/HTTPS）”
- 其他参数根据业务需要进行配置。

步骤2 为步骤1中创建的负载均衡添加监听器，详细操作请参见[添加HTTP监听器](#)或[添加HTTPS监听器](#)。

步骤3 创建后端服务器组。

- “所属负载均衡器”：选择“关联已有”，并在下拉框中选择[步骤1](#)中创建的负载均衡器。
- 后端服务器配置为[步骤5](#)中需要添加到WAF中的网站对应的服务器地址。

步骤4 执行以下命令，测试业务联通性是否正常。

```
curl -kv -H "Host: {源站域名}" {监听器对应的协议}://{ELB的IP}:{监听器端口}
```

返回码为“200”，则表示业务流量联通正常。

步骤5 在WAF中配置需要检测流量的网站。


1. 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。
2. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
3. 在网站列表左上角，单击“添加防护网站”。
4. 选择“云模式-ELB接入”，并单击“开始配置”。
5. 配置域名基本信息，如图3-22所示，相关参数说明如表3-6所示。

图 3-22 配置防护网站基本信息



该截图展示了配置防护网站基本信息的表单。表单包含以下字段：

- * ELB (负载均衡器)**: 下拉菜单，显示“-请选择ELB-”，右侧有刷新图标。
- * ELB监听器**: 两个按钮，分别为“所有监听器”（蓝色）和“指定监听器”（灰色）。
- 网站名称**: 输入框，提示文字为“您可以为域名自定义名称”。
- * 防护域名**: 输入框，显示“*”，表示必填。
- 网站备注**: 输入框。
- * 策略配置**: 下拉菜单，显示“系统自动生成策略”，右侧有问号帮助图标。

表 3-6 基本信息参数说明

参数	参数说明	取值样例
ELB (负载均衡器)	选择步骤1中创建的负载均衡，确认防护网站对应的服务器地址已添加到该ELB。	elb-waf-test
ELB监听器	选择的ELB配置的监听器。 - “所有监听器” - “指定监听器”	所有监听器
网站名称	可选参数，自定义网站名称。	-

参数	参数说明	取值样例
防护域名	<p>配置为您想防护的域名或IP（公网IP/私网IP），且该域名已解析到步骤1中创建的负载均衡器的弹性公网IP上。</p> <p>域名：支持单域名和泛域名。</p> <ul style="list-style-type: none"> - 单域名：输入防护的单域名。例如： www.example.com。 - 泛域名 <ul style="list-style-type: none"> ▪ 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：子域名 a.example.com, b.example.com和 c.example.com对应的服务器IP地址相同，可以直接添加泛域名 *.example.com。 ▪ 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。 ▪ WAF支持添加“*”的泛域名。 <p>说明 WAF支持防护公网IP、私网IP，如果配置为私网IP，必须确保相应的网络路径是可访问的，以便于WAF能够正确地对流量进行监控和过滤。</p>	<p>单域名： www.example.com</p> <p>泛域名： *.example.com</p> <p>IP： XXX.XXX.1.1</p>
网站备注	可选参数，网站补充信息。	-
策略配置	<p>默认为“系统自动生成策略”，您也可以选择已创建的防护策略或在域名接入后根据防护需求配置防护规则。</p> <p>系统自动生成的策略说明如下：</p> <ul style="list-style-type: none"> - Web基础防护（“仅记录”模式、常规检测） 仅记录SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击行为。 - 网站反爬虫（“仅记录”模式、扫描器） 仅记录漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap的爬虫行为。 <p>说明</p> <ul style="list-style-type: none"> - “仅记录”模式：发现攻击行为后WAF只记录攻击事件不阻断攻击。 - 只有专业版和铂金版支持选择自定义的防护策略。 	系统自动生成策略

6. 单击“确定”，防护网站添加成功。

流量访问说明如下：

1. 用户在浏览器输入域名后，客户端会向DNS发送请求，查询域名解析地址。
2. DNS返回域名解析地址。
3. 如果无代理（例如CDN、DDoS高防等），DNS返回的域名解析地址为ELB的公网IP地址，客户端通过该公网IP访问ELB。如果存在代理：
 - a. DNS返回的域名解析地址为代理IP，客户端通过代理IP访问代理。
 - b. 代理通过ELB的公网IP访问ELB。
4. ELB将流量传给WAF。
5. 经过WAF检测后，异常请求将被拦截，正常请求会通过WAF独享引擎回源IP转发到源站服务器。

接入流程

根据网站是否使用代理（例如高防、CDN、云加速等），您需要完成如下接入操作。

操作步骤	说明
步骤一：添加防护网站	介绍如何将防护域名、源站信息等添加到WAF。
步骤二：为WAF独享引擎实例配置负载均衡	介绍如何为WAF独享引擎实例配置负载均衡器和健康检查。
步骤三：为弹性负载均衡绑定弹性公网IP	介绍如何为WAF独享引擎实例的负载均衡器绑定源站服务器的弹性公网IP，使网站请求流量经过WAF独享引擎检测。
步骤四：放行独享引擎回源IP	介绍如何放行独享引擎的回源IP。
步骤五：验证WAF独享引擎实例转发正常	介绍如何验证WAF转发和ELB运行是否正常、基础防护是否生效。

前提条件

- 已购买独享型负载均衡。有关ELB类型的详细介绍，请参见[共享型弹性负载均衡与独享型负载均衡的功能区别](#)。

📖 说明


- 2023年4月之前的独享引擎版本，不支持与独享ELB网络型配合使用。因此，如果您使用了独享ELB网络型（TCP/UDP）负载均衡，请确认独享WAF实例已升级到最新版本（2023年4月及之后的版本），独享引擎版本详情请参见[独享引擎版本迭代](#)。
- 在该独享引擎实例所在安全组中已放开了相关端口。
安全组建议配置以下访问规则：
 - 入方向规则
根据业务需求添加指定端口入方向规则，放通指定端口入方向网络流量。例如，需要放通“80”端口时，您可以添加“策略”为“允许”的“TCP”、“80”协议端口规则。
 - 出方向规则
默认。放通全部出方向网络流量。


有关添加安全组规则的详细操作，请参见[添加安全组规则](#)。

步骤一：添加防护网站

为了将业务接入WAF防护，您需要将防护域名、源站信息等，添加到WAF。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在网站列表左上角，单击“添加防护网站”。

步骤6 选择“独享模式接入”并单击“开始配置”。

步骤7 基础信息配置，如[图3-24](#)所示，参数说明如[表3-7](#)所示。

图 3-24 基础信息配置



The screenshot shows the 'Basic Information' configuration page for a WAF protection site. It includes input fields for protection target, site name, and site remarks. A dropdown menu for protection port is set to 'Standard Port' (80). Below this is a table for service forwarding configuration with columns for external protocol, source protocol, VPC, source address, source port, and action. The table contains one row with 'HTTP' for both protocols, 'sona...' for VPC, 'IPv4' for source address, '内网IP地址' for source port, and '80' for the port number. There is a 'Delete' button for this row. At the bottom, there is a checkbox for 'Use 7-layer proxy' which is checked.

对外协议	源站协议	VPC	源站地址	源站端口	操作
HTTP	HTTP	sona...	IPv4	内网IP地址	80 删除

表 3-7 基本信息参数说明

参数	参数说明	取值样例
防护对象	<p>防护的域名或IP（公网IP/私网IP），域名支持单域名和泛域名。</p> <p>说明</p> <ul style="list-style-type: none"> WAF支持添加“*”泛域名，表示可以防护任意的域名。“防护对象”配置为“*”时，只能防护除80、443端口以外的非标端口。 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。 WAF支持防护公网IP、私网IP，如果配置为私网IP，必须确保相应的网络路径是可访问的，以便于WAF能够正确地对流量进行监控和过滤。 	-
网站名称 (可选)	自定义网站名称。	WAF
网站备注 (可选)	网站的备注信息。	wafstest
防护端口	<p>要防护的端口。</p> <ul style="list-style-type: none"> 配置为80、443端口时，在下拉框中选择“标准端口”。 配置为其他端口时，所选端口必须在可选端口范围内。您可以单击“查看可添加端口”，查看WAF支持的HTTP和HTTPS端口。更多信息请参见WAF支持的端口范围。 <p>说明</p> <p>如果配置了除80/443以外的其他端口，访问网站时，需要在网址后面增加非标准端口进行访问，否则访问网站时会出现404错误。</p>	81

参数	参数说明	取值样例
服务器配置	<p>网站服务器地址的配置。包括对外协议、源站协议、VPC、源站地址和源站端口。</p> <ul style="list-style-type: none"> ● 对外协议：客户端请求访问服务器的协议类型。包括“HTTP”、“HTTPS”两种协议类型。 ● 源站协议：网站服务器支持的协议类型。也是Web应用防火墙转发客户端请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。 <p>说明</p> <ul style="list-style-type: none"> - 如果“对外协议”与“源站协议”不一致，WAF会将“对外协议”转换为“源站协议”，使用“源站协议”来转发客户端的请求。 - WAF支持WebSocket/WebSockets协议，且默认为开启状态。 <ul style="list-style-type: none"> ● VPC：选择独享引擎实例所在的VPC。 <p>说明</p> <p>为了实现业务双活，避免业务单点故障，建议在同一VPC下购买两个WAF实例。</p> <ul style="list-style-type: none"> ● 源站地址：网站服务器的私有IP地址。登录ECS或ELB控制台，在实例列表中查看对应服务器的私有IP地址。 <p>说明</p> <p>源站地址不能与防护对象一致。</p> <p>支持以下两种IP格式：</p> <ul style="list-style-type: none"> - IPv4，例如：XXX.XXX.1.1 - IPv6，例如： fe80:0000:0000:0000:0000:0000:0000:0000 <ul style="list-style-type: none"> ● 源站端口：WAF独享引擎转发客户端请求到服务器的业务端口。 	<p>对外协议： HTTP</p> <p>源站协议： HTTP</p> <p>源站地址： IPv4 XXX.XXX.1.1</p> <p>源站端口：80</p>

参数	参数说明	取值样例
证书名称	<p>“对外协议” 设置为 “HTTPS” 时，需要选择证书。</p> <ul style="list-style-type: none"> 如果您未创建证书，单击“导入新证书”，在“导入新证书”对话框，填写证书相关参数。更多信息，请参见上传证书。成功导入的新证书，将同步添加到“证书管理”页面的证书列表。 如果已创建证书，在下拉框“已有证书”中选择正确、有效的证书。 如果您已经在同一个账号下使用了CCM中证书，也可以直接在下拉框中选择SCM证书，此处选择的SCM证书名称与CCM里证书名称一致。 <p>须知</p> <ul style="list-style-type: none"> WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考如何将非PEM格式的证书转换为PEM格式?将证书转换为PEM格式，再上传。 目前华为云SCM证书只能推送到“default”企业项目下。如果您使用其他企业项目，则不能选择使用SCM推送的SSL证书。 如果您的证书即将到期，为了不影响网站的使用，建议您在到期前重新使用新的证书，并在WAF中同步更新网站绑定的证书。 WAF支持证书过期时发送告警通知，您可以在“告警通知”界面配置证书过期提醒，具体的操作请参见开启告警通知。 域名和证书需要一一对应，泛域名只能使用泛域名证书。如果您没有泛域名证书，只有单域名对应的证书，则只能在WAF中按照单域名的方式逐条添加域名进行防护。 	--
是否使用七层代理	<ul style="list-style-type: none"> 是：使用了DDoS高防（七层代理）、CDN、云加速等Web代理产品。 否：没有使用七层代理。 <p>须知</p> <p>选择“是”后，即在WAF前使用了七层代理，WAF将从配置的Header头中的相关字段获取用户真实访问IP，详见配置攻击惩罚的流量标识。</p>	七层代理

步骤8 高级配置。

选择“防护策略”：默认为“系统自动生成策略”，您也可以选择已创建的防护策略或在域名接入后根据防护需求配置防护规则。

系统自动生成的策略说明如下：

- Web基础防护（“仅记录”模式、常规检测）
仅记录SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击行为。
- 网站反爬虫（“仅记录”模式、扫描器）
仅记录漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap的爬虫行为。

📖 说明

“仅记录”模式：发现攻击行为后WAF只记录攻击事件不阻断攻击。

步骤9 单击“确定”，添加域名完成。

可根据界面提示，完成配置负载均衡、为弹性负载均衡绑定弹性公网IP和放行独享引擎回源IP的操作，建议单击“稍后”。后续参照**步骤二：为WAF独享引擎实例配置负载均衡**、**步骤三：为弹性负载均衡绑定弹性公网IP**和**步骤四：放行独享引擎回源IP**完成相关操作。

---结束

步骤二：为 WAF 独享引擎实例配置负载均衡

添加防护网站后，您需要使用华为云弹性负载均衡（Elastic Load Balance，简称ELB）为WAF独享引擎实例配置负载均衡和健康检查，以确保WAF的可靠性和稳定性。

须知


华为云ELB按流量单独计费。有关ELB的计费详情，请参见[ELB价格详情](#)。

步骤1 为负载均衡添加监听器，详细操作请参见[添加HTTP监听器](#)或[添加HTTPS监听器](#)。

📖 说明

添加监听器时，相关参数的配置说明如下：

- “前端端口”：客户端与负载均衡监听器建立流量分发连接的端口，可配置为任意端口，此处建议配置为WAF中配置的源站端口。
- “前端协议”：只能选择HTTP或HTTPS协议。
- “分配策略类型”选择“加权轮询算法”时，请关闭“会话保持”，如果开启会话保持，相同的请求会转发到相同的WAF独享引擎实例上，当WAF独享引擎实例出现故障时，再次到达该引擎的请求将会出错。
- 配置健康检查后，“健康检查结果”的“状态”必须为“正常”，否则会导致网站不能正常接入WAF。有关配置健康检查的详细操作，请参见[配置健康检查](#)。

步骤2 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙”，进入“安全总览”页面。

步骤3 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

步骤4 在目标实例所在行的“操作”列，单击“更多 > 添加到ELB”。

步骤5 在“添加到ELB”页面中，选择**步骤1**中配置的“ELB（负载均衡器）”、“ELB监听器”和“后端服务器组”。

图 3-25 添加到 ELB



须知

“健康检查结果”的“状态”必须为“正常”，否则会导致网站不能正常接入WAF。健康检查异常的排查思路请参见[健康检查异常](#)。


步骤6 单击“确定”，为WAF实例配置业务端口，“业务端口”需要配置为WAF独享引擎实例实际监听的业务端口，即[步骤一：添加防护网站](#)中配置的“防护端口”。

---结束

步骤三：为弹性负载均衡绑定弹性公网 IP

如果WAF独享引擎实例已配置负载均衡，请解绑源站服务器的弹性公网IP（Elastic IP，简称EIP），将解绑的弹性公网IP绑定到WAF独享引擎实例[配置的负载均衡](#)上。绑定后，请求流量会先经过WAF独享引擎进行攻击检测，然后转发到源站服务器，从而确保源站安全、稳定、可用。

本章节以解绑源站服务器的弹性公网IP（Elastic IP，简称EIP），将解绑的EIP绑定到WAF独享引擎的弹性负载均衡（Elastic Load Balance，简称ELB）上为例说明，具体操作请以实际业务为准。

步骤1 单击页面左上方的 ，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。

步骤2 在“负载均衡器”页面，解绑源站服务器的弹性公网IP。

- 解绑IPv4公网IP，在目标源站的负载均衡器所在行“操作”列，选择“更多 > 解绑IPv4公网IP”。
- 解绑IPv6公网IP，在目标源站的负载均衡器所在行“操作”列，选择“更多 > 解绑IPv6公网IP”。

图 3-26 解绑弹性公网 IP

名称	状态	实例规格类型	服务器地址与所属网络	监听器 (端口协议/端口)	EIP计费信息	计费模式	企业项目	操作
elb_internet2	运行中	共享型	192.168.0.6 (私有IP地址) 私网2.217.189 (弹性公网) vpc-d9b3-cy3 (虚拟私有云)	listener-b8a3 (HTTP/80)	5 Mbit/s 按带宽	...	default	修改带宽 删除 更多 解绑弹性公网IP 查看访问日志
web-server	运行中	共享型	192.168.0.5 (私有IP地址) vpc-d9b3-cy3 (虚拟私有云)	listener-36cf (HTTP/8002)	default	修改带宽

步骤3 在弹出的对话框中，单击“是”，解绑EIP。

步骤4 在“负载均衡器”页面，找到WAF独享引擎的ELB的负载均衡器，绑定源站服务器的弹性公网IP。

- 绑定IPv4公网IP，在WAF独享引擎的ELB的负载均衡器所在行“操作”列，选择“更多 > 绑定IPv4公网IP”。
- 绑定IPv6公网IP，在WAF独享引擎的ELB的负载均衡器所在行“操作”列，选择“更多 > 绑定IPv6公网IP”。

步骤5 在弹出对话框中，选择**步骤2**中解绑的EIP，单击“确定”，绑定EIP。

----结束

步骤四：放行独享引擎回源 IP


网站以“独享模式”成功接入WAF后，所有网站访问请求将先经过独享引擎配置的ELB然后流转到独享引擎实例进行监控，经独享引擎实例过滤后再返回到源站服务器，流量经独享引擎实例返回源站的过程称为回源。在服务器看来，接入WAF后所有源IP都会变成独享引擎实例的回源IP（即独享引擎实例对应的子网IP），以防止源站IP暴露后被黑客直接攻击。

源站服务器上的安全软件很容易认为独享引擎的回源IP是恶意IP，有可能触发屏蔽WAF回源IP的操作。一旦WAF的回源IP被屏蔽，WAF的请求将无法得到源站的正常响应，因此，网站以“独享模式”接入WAF防护后，您需要在源站服务器上设置放行创建的独享引擎实例对应的子网IP，不然可能会出现网站打不开或打开极其缓慢等情况。

根据您的源站服务器部署位置，选择以下方式进行操作。

回源到 ECS

如果您的源站服务器直接部署在华为云ECS上，请参考以下操作步骤设置安全组规则，放行独享模式回源IP。


步骤1 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙”，进入“安全总览”页面。

步骤2 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

图 3-27 独享引擎列表

实例名	运行状态	防护策略	VPC	子网	IP地址	接入状态	版本	模式	规格	计费模式	操作
hgw-2011	运行中	未绑定	vpc-890-wafest	subnet-890c	192.168.10.224 (...)	未接入	202309	独享模式 (按实例计费)	V6-100 47 Instance 4	按量计费	云监控 升级 更多 >
hgwkey-0122	运行中	未绑定	vpc-890-wafest	subnet-890c	192.168.10.183 (...)	未接入	202309	独享模式 (按实例计费)	V6-100 47 Instance 4	按量计费	云监控 升级 更多 >

步骤3 在独享引擎列表的“IP地址”栏，获取所有创建的独享引擎对应的子网IP地址。

步骤4 单击页面左上方的 ，选择“计算 > 弹性云服务器”。

步骤5 在目标ECS所在行的“名称/ID”列中，单击目标ECS实例名称，进入ECS实例的详情页页面。

步骤6 选择“安全组”页签，单击“更改安全组”。

步骤7 在“更改安全组”对话框中，选择目标安全组或新建安全组并单击“确定”。

步骤8 单击安全组ID，进入安全组基本信息页面。

步骤9 选择“入方向规则”页签，单击“添加规则”，进入“添加入方向规则”页面，参数配置说明如表3-8所示。

图 3-28 添加入方向规则

添加入方向规则 教我设置

1 安全组规则对不同规格云服务器的生效情况不同，为了避免您的安全组规则不生效，请您添加规则前，单击[此处](#)了解详情。当源地址选择IP地址时，您可以在一个IP地址框内同时输入多个IP地址，一个IP地址对应一条安全组规则。

安全组 WAF-DONOTDELETE-yYo7

如您要添加多条规则，建议单击 [导入规则](#) 以进行批量导入。

优先级	策略	类型	协议端口	源地址	描述	操作
1-100	允许	IPv4	基本协议/自定义TCP 80	IP地址 0.0.0.0/0		复制 删除

+ 增加1条规则

取消
确定

表 3-8 入方向规则参数配置说明

参数	配置说明
协议端口	安全组规则作用的协议和端口。选择“自定义TCP”后，在TCP框下方输入源站的端口。

参数	配置说明
源地址	逐一添加 步骤3 中获取的所有独享引擎实例的子网IP地址。 说明 一条规则配置一个IP。单击“增加1条规则”，可配置多条规则，最多支持添加10条规则。

步骤10 单击“确定”，安全组规则添加完成。

成功添加安全组规则后，安全组规则将允许独享引擎回源IP地址的所有入方向流量。

您可以使用Telnet工具测试已接入WAF防护的源站IP对应的业务端口是否能成功建立连接验证配置是否生效。

例如，执行以下命令，测试已接入WAF防护的源站IP对外开放的443端口是否能成功建立连接。如果显示端口无法直接连通，但网站业务仍可正常访问，则表示安全组规则配置成功。


Telnet 源站IP 443


----结束

回源到 ELB

如果您的源站服务器使用华为云ELB进行流量分发，请参考以下操作步骤设置访问控制（白名单）策略，只放行独享模式回源IP。

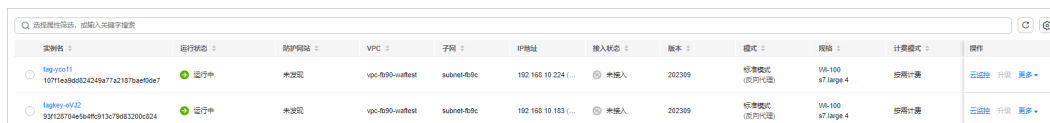
步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙”，进入“安全总览”页面。


步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

图 3-29 独享引擎列表



实例名	运行状态	防护策略	VPC	子网	IP地址	插入状态	版本	模式	规格	计费模式	操作
hgw-ec11 1071e486824249a77a2187baef0e7	运行中	未策略	vpc-b95-wafest	subnet-89c	192.168.10.224 (...)	未插入	202309	独享模式 (原网代理)	V6-100 87 large.4	按量计费	云连接 升级 更多
hgw-ec12 03f12370e4b648c913c79a83206cd24	运行中	未策略	vpc-b95-wafest	subnet-89c	192.168.10.183 (...)	未插入	202309	独享模式 (原网代理)	V6-100 87 large.4	按量计费	云连接 升级 更多

步骤5 在独享引擎列表的“IP地址”栏，获取所有创建的独享引擎对应的子网IP地址。

步骤6 单击页面左上方的，选择“网络 > 弹性负载均衡”。

步骤7 在独享引擎绑定的ELB所在行的“名称”列中，单击ELB名称，进入ELB的详情页面。

步骤8 在目标监听器所在行的“访问控制”列，单击“设置”。

图 3-30 监听器列表



名称/ID	监控	监听协议/端口	健康检查	后端服务器组 (默认)	访问控制	操作
listener-77c f723dfde-b6d2-480e-b512-77084b127a29		HTTP80	 正常	server_group-8081 查看/添加后端服务器	允许所有IP访问 设置	添加/编辑/删除/重置

步骤9 在弹出的对话框中，“访问控制”选择“白名单”。

1. 单击“创建IP地址组”，将**步骤5**中WAF的接入IP地址添加到“IP地址组”。
2. 在“IP地址组”的下拉框中选择**步骤9.1**中创建的IP地址组。

步骤10 单击“确定”，白名单访问控制策略添加完成。

成功配置访问控制策略后，访问控制策略将允许独享引擎回源IP地址的所有入方向流量。

您可以使用Telnet工具测试已接入WAF防护的源站IP对应的业务端口是否能成功建立连接验证配置是否生效。

例如，执行以下命令，测试已接入WAF防护的源站IP对外开放的443端口是否能成功建立连接。如果显示端口无法直接连通，但网站业务仍可正常访问，则表示安全组规则配置成功。

Telnet *源站IP* 443

----结束

步骤五：验证 WAF 独享引擎实例转发正常

添加防护网站后，验证WAF转发和ELB运行是否正常。

（可选）验证独享 WAF 是否正常工作

步骤1 创建一台与独享WAF实例在同一VPC下的ECS用于发送请求。

步骤2 通过**步骤1**中创建的ECS向独享WAF发送请求。

- 转发测试

```
curl -kv -H "Host: {添加到WAF的防护对象}" {服务器配置中的对外协议}://{独享WAF的IP}:{防护对象端口}
```

例如：

```
curl -kv -H "Host: a.example.com" http://192.168.0.1
```

返回码为 200 则说明转发成功。如果转发未成功，请参见[如何排查404/502/504错误？](#)进行排查。

- 攻击拦截测试。

a. 确保网站对应策略已开启基础防护的拦截模式。

b. 执行以下命令：

```
curl -kv -H "Host: {添加到WAF的防护对象}" {服务器配置中的对外协议}://{独享WAF的IP}:{防护对象端口} --data "id=1 and 1=' 1"
```

例如：

```
curl -kv -H "Host: a.example.com" http:// 192.168.X.X --data "id=1 and 1=' 1"
```

返回码为 418 则说明拦截成功，独享WAF工作正常。

----结束

验证独享 WAF 和 ELB 是否都正常工作

- 转发测试

```
curl -kv -H "Host: {添加到WAF的防护对象}" {ELB对外协议}://{ELB私网的IP}:{ELB监听端口}
```

如果 ELB 添加了 EIP，可以使用任意公网机器直接进行测试。

```
curl -kv -H "Host: {添加到WAF的防护对象}" {ELB对外协议}://{ELB公网的IP}:{ELB监听端口}
```

例如:

```
curl -kv -H "Host: a.example.com" http://192.168.X.Y  
curl -kv -H "Host: a.example.com" http://100.10.X.X
```

返回码为200则说明转发成功。

在确保独享引擎工作正常的情况下，如果转发失败，则优先检查ELB配置是否有误（如果ELB健康检查异常可先关闭ELB健康检查再重新执行以上的操作）。

- 攻击拦截测试

- a. 确保网站对应策略已开启基础防护的拦截模式。

- b. 执行以下命令:

```
curl -kv -H "Host: {添加到WAF的防护对象}" {ELB对外协议}://{ELB私网的IP}:{ELB监听端口} --data "id=1 and 1=' 1"
```

如果ELB添加了EIP，可以使用任意公网机器直接进行测试。

```
curl -kv -H "Host: {添加到WAF的防护对象}" {ELB对外协议}://{ELB公网的IP}:{ELB监听端口} --data "id=1 and 1=' 1"
```

例如:

```
curl -kv -H "Host: a.example.com" http:// 192.168.0.2 --data "id=1 and 1=' 1"  
curl -kv -H "Host: a.example.com" http:// 100.10.X.X --data "id=1 and 1=' 1"
```

返回码为418则说明拦截成功，独享WAF、ELB均工作正常。

后续操作

- 防护网站的初始“接入状态”为“未接入”，当访问请求到达该网站的WAF时，该防护网站的接入状态将自动切换为“已接入”。如果接入失败，请参见[域名/IP接入状态显示“未接入”，如何处理？](#) 排查处理。
- **网站接入后推荐配置**
 - 防护网站的“对外协议”使用了“HTTPS”协议时，支持[配置PCI DSS/3DS合规与TLS](#)、[开启HTTP2协议](#)、[开启Cookie安全属性](#)。
 - [开启IPv6防护](#)：帮助源站实现IPv6协议请求的安全防护。
 - [配置WAF到网站服务器的连接超时时间](#)：WAF到源站的连接超时时长默认为30秒，支持自定义“连接超时”、“读超时”、“写超时”的时间。
 - [配置攻击惩罚的流量标识](#)：配置客户端IP标识、Session标识或User标识，实现IP、Cookie或Params恶意请求的攻击惩罚功能。
 - [配置Header字段转发](#)：添加Header字段后，WAF会将该字段插入到Header中，转发给源站，用以标记请求。
 - [修改拦截返回页面](#)：自定义触发WAF拦截时的返回页面。
- 根据防护需求，调整防护域名配置的防护策略，详见[防护配置概述](#)。

3.5 WAF 支持的端口范围

Web应用防火墙（Web Application Firewall，简称WAF）支持防护标准端口和非标准端口。您在网站接入配置中添加防护网站对应的业务端口，WAF将通过您设置的业务端口为网站提供流量的接入与转发服务。本文介绍WAF支持防护的标准端口和非标准端口。

例如，如[表3-9](#)中，云模式标准版及以上版本、独享模式的HTTP协议支持防护9001端口，如果您需要防护网站的9001业务端口，则需要购买云模式标准版及以上版本中任一版本或者独享模式，且在[将网站接入WAF防护](#)中，配置如[图3-31](#)所示。

图 3-31 端口配置

对外协议	源站协议	源站地址	源站端口	权重	操作
HTTP	HTTP	IPv4 公网IP地址或者域名	80	1	删除

须知

不同Region支持的端口范围略有差异，以实际的支持范围为准。

云模式的专业版和铂金版支持定制非标准端口，您可以[提交工单](#)申请开通定制的非标准端口。

标准端口

WAF支持防护如下标准端口：

- HTTP协议端口：80
- HTTPS协议端口：443

WAF 支持的非标端口

WAF支持的除80，443以外的非标端口如下。

云模式

云模式支持的非标端口是由WAF指定的任意非标端口，而不是您业务中的任意一个自定义非标端口。不同版本的WAF支持的非标准端口范围有所不同。

表 3-9 云模式支持的非标端口

服务版本	支持的非标端口范围	
	HTTP协议	HTTPS协议
入门版	不支持	不支持

服务版本	支持的非标端口范围	
	HTTP协议	HTTPS协议
标准版	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 7009, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8999, 9001	4443, 5048, 5049, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8712, 8803, 8804, 8805, 8843, 9443, 8553, 8663, 9553, 9663, 18000, 18110, 18381, 18443, 18980, 19000, 28443

服务版本	支持的非标端口范围	
	HTTP协议	HTTPS协议
专业版	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, 888, 1000, 1090, 1135, 1139, 1180, 1688, 3128, 3333, 3501, 3601, 4444, 5000, 5001, 5080, 55222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7080, 77081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8004, 8007, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8813, 8814, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9020, 9021, 9022, 9023, 9024, 9025, 9026, 9027, 9028, 9029, 9037, 9050, 9077, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 9770, 10000, 10001, 10080, 10087, 11000, 12601, 13000, 14000, 18080, 18081, 18180, 18280, 19101, 19501, 21028, 23333, 27777, 28080, 30002, 30086, 33332, 33334, 33702, 40010, 48299, 48800, 52725, 52726, 60008, 60010	90, 447, 882, 1446, 1448, 1451, 1452, 1818, 4006, 4430, 4433, 4443, 5048, 5049, 5100, 5443, 6022, 6130, 6133, 6140, 6141, 6142, 6150, 6443, 7072, 7073, 7443, 8033, 8043, 8079, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8840, 8842, 8843, 8990, 8991, 9005, 9053, 9090, 9300, 9443, 9553, 9663, 9681, 9682, 9999, 10002, 10003, 10006, 10300, 10301, 11001, 11003, 12340, 12341, 12342, 12343, 12344, 12345, 12346, 12347, 12348, 12349, 12350, 12351, 12352, 12353, 12354, 13001, 13003, 13080, 14003, 14443, 17618, 17718, 17818, 17918, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 19999, 20000, 28443, 60009

服务版本	支持的非标端口范围	
	HTTP协议	HTTPS协议
铂金版	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, 888, 1000, 1090, 1135, 1139, 1688, 1180, 3128, 3333, 3501, 3601, 4444, 5000, 5001, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8004, 8006, 8007, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8813, 8814, 8888, 8889, 8899, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9020, 9021, 9022, 9023, 9024, 9025, 9026, 9027, 9028, 9029, 9037, 9050, 9077, 9080, 9081, 9082, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 10000, 10001, 10080, 10087, 11000, 12601, 13000, 14000, 18080, 18081, 18180, 18280, 23333, 27777, 28080, 30086, 33702, 48299, 48800	90, 447, 882, 1446, 1448, 1451, 1452, 1818, 4006, 4430, 4433, 4443, 5048, 5049, 5443, 6022, 6130, 6133, 6140, 6141, 6142, 6150, 6443, 7072, 7073, 7443, 8033, 8043, 8079, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8840, 8842, 8843, 8848, 8910, 8920, 8950, 8990, 8991, 9005, 9053, 9090, 9182, 9184, 9190, 9300, 9443, 9553, 9663, 9681, 9682, 9999, 10002, 10003, 10006, 10300, 10301, 11001, 11003, 12340, 12341, 12342, 12343, 12344, 12345, 12346, 12347, 12348, 12349, 12350, 12351, 12352, 12353, 12354, 13001, 13003, 13080, 14003, 17618, 17718, 17818, 17918, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 19999, 28443, 60009

独享模式

使用独享模式接入WAF时，支持防护表3-10中的任意非标端口。

表 3-10 独享模式支持的非标端口

HTTP协议	HTTPS协议
81, 82, 83, 84, 86, 87, 88, 89, 97, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7080, 7081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9021, 9023, 9027, 9037, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9945, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 10000, 10001, 10080, 12601, 19101, 19501, 19998, 21028, 28080, 30002, 33332, 33334, 33702, 40010, 48800, 52725, 52726, 60008, 60010	4443, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8843, 9443, 9553, 9663, 9999, 18000, 18010, 18110, 18381, 18443, 18980, 19000, 28443

4 查看防护事件

4.1 查询防护事件

Web应用防火墙会对在所选时间段的攻击事件、受攻击站点、攻击源IP、受攻击URL的TOP 10网站进行统计，并将拦截或者仅记录攻击事件记录在“防护事件”页面。您可以查看WAF的防护日志，包括事件发生的时间、源IP、源IP所在地理位置、恶意负载、命中规则等信息。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目的防护日志。

前提条件


防护网站已接入WAF


约束条件

- 在WAF控制台只能查看所有防护域名最近30天的防护事件数据。您可以通过开启全量日志长期保存日志，并查看攻击日志和访问日志的详细信息。有关开启全量日志的详细操作，请参见[通过LTS记录WAF全量日志](#)。
- 如果您将防护网站的工作模式切换为“暂停防护”模式，WAF将对防护网站所有的流量请求只转发不检测，同时日志也不会记录。

查看防护日志

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护事件”，进入“防护事件”页面。

步骤5 选择“查询”页签，在网站或实例下拉列表中选择待查看的防护网站，可查看“昨天”、“今天”、“3天”、“7天”、“30天”或者自定义时间范围内的防护日志。


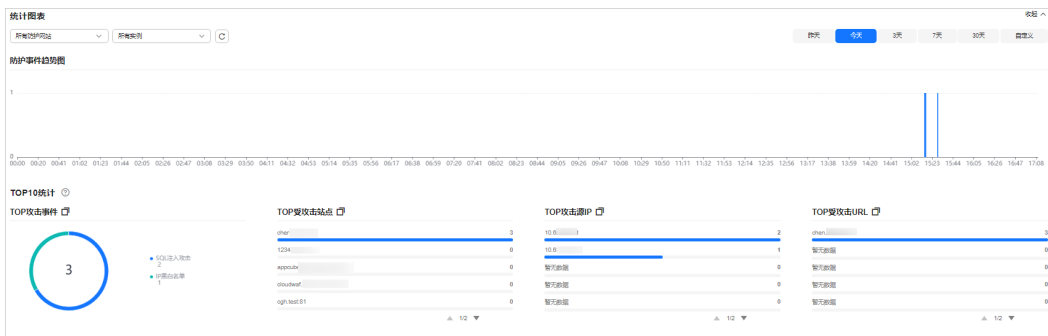
- “防护事件趋势图”：展示所选网站在选择的时段内WAF的防护情况。
- “TOP10统计”：针对当前所选时间段的攻击事件、受攻击站点、攻击源IP、受攻击URL的TOP 10网站进行统计，单击可复制统计图表的数据。

图 4-1 防护事件



步骤6 在“防护事件列表”中，查看防护详情。


- 根据筛选条件字段匹配值进行筛选，可设置多项匹配条件，单击“确定”后，匹配条件会展示在事件列表的上方，条件字段参数说明如表4-2所示。
- 在事件列表的左上角，单击“导出”，可导出防护事件列表数据，防护事件数据小于200条将直接导出到本地。
- 单击，可选择防护事件列表展示的字段。
- 在目标事件的“操作”列单击“详情”，可查看目标域名攻击事件详情。

图 4-2 防护事件列表



表 4-1 支持筛选搜索的条件字段

参数名称	参数说明
事件ID	标识该防护事件的ID。
事件类型	发生攻击的类型。 默认选择“全部”，查看所有攻击类型的日志信息，也可以根据需求，选择攻击类型查看攻击日志信息。
规则ID	内置Web基础防护规则ID。

参数名称	参数说明
防护动作	防护配置中设置的防护动作，包含：拦截、仅记录、人机验证、不匹配等。 <ul style="list-style-type: none">• 人机验证：CC防护规则中，“防护动作”支持配置“人机验证”。即当访问的请求频率超过设定的“限速频率”后将弹出验证码提示，输入正确的验证码，请求将不受访问限制。• 不匹配：配置网页防篡改、防敏感信息泄露、隐私屏蔽防护规则后，如果访问请求命中这些防护规则，则防护日志中记录的防护事件，“防护动作”显示为“不匹配”。
源IP	Web访问者的公网IP地址（攻击者IP地址）。 默认选择“全部”，查看所有的日志信息，也可以根据需要，选择或者自定义攻击者IP地址查看攻击日志信息。
URL	攻击的防护域名的URL。
状态码	拦截页面返回的HTTP状态码。
防护域名	被攻击的防护域名。

表 4-2 防护事件列表可展示字段参数说明

参数	说明	示例
时间	本次攻击发生的时间。	2021/02/04 13:20:04
源IP	Web访问者的公网IP地址（攻击者IP地址）。	-
防护域名	被攻击的防护域名。	www.example.com
地理位置	攻击者来源IP所在地区。	-
规则ID	内置Web基础防护规则ID。	-
URL	攻击的防护域名的URL。	/admin
事件类型	发生攻击的类型。	SQL注入攻击
防护动作	防护配置中设置的防护动作，包含：拦截、仅记录、人机验证等。 说明 配置网页防篡改、防敏感信息泄露、隐私屏蔽防护规则后，如果访问请求命中防护规则，则防护动作显示为“不匹配”。	拦截
状态码	拦截页面返回的HTTP状态码。	418

参数	说明	示例
恶意负载	本次攻击对防护域名造成伤害的位置、组成部分或访问URL的次数。 说明 <ul style="list-style-type: none">对于CC攻击事件，恶意负载表示当时访问URL的次数。对于黑名单防护事件，恶意负载为空。	id=1 and 1='1
企业项目	网站所在的企业项目。	default

----结束

4.2 处理误报事件

对于“防护事件”页面中的攻击事件，如果排查后您确认该攻击事件为误报事件，即未发现该攻击事件相关的恶意链接、字符等，您可以通过设置URL和规则ID的忽略（Web基础防护规则）、删除或关闭对应的防护规则（自定义防护规则）、将攻击源IP添加至黑白名单地址组或黑白名单策略中，屏蔽该攻击事件。将攻击事件处理为误报事件后，“防护事件”页面中将不再出现该攻击事件，您也不会收到该攻击事件的告警通知。

当WAF根据内置的Web基础防护规则和网站反爬虫的特征反爬虫，以及自定义防护规则（CC攻击防护规则、精准访问防护规则、黑白名单规则、地理位置访问控制规则等）检测到符合规则的恶意攻击时，会按照规则中的防护动作（仅记录、拦截等）在“防护事件”页面中记录检测到的攻击事件。

📖 说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能处理该企业项目下的误报事件。

前提条件

事件详情列表中包含误报攻击事件。

约束条件


- 仅基于WAF内置的Web基础防护规则和网站反爬虫的特征反爬虫拦截或记录的攻击事情可以进行“误报处理”操作。
- 基于自定义规则（CC攻击防护规则、精准访问防护规则、黑白名单规则、地理位置访问控制规则等）拦截或记录的攻击事件，无法执行“误报处理”操作，如果您确认该攻击事件为误报，可在自定义规则页面，将该攻击事件对应的防护规则删除或关闭。
- 同一个攻击事件不能重复进行误报处理，即如果该攻击事件已进行了误报处理，则不能再对该攻击事件进行误报处理。
- 拦截事件处理为误报后，“防护事件”页面中将不再出现该事件，您也不会收到该类事件的告警通知。
- 独享模式2022年6月之前的版本“不检测模块”不支持配置“所有检测模块”选项，仅支持配置“Web基础防护模块”。


使用场景

业务正常请求被WAF拦截。例如，您在华为云ECS服务器上部署了一个Web应用，将该Web应用对应的公网域名接入WAF并开启Web基础防护后，该域名的请求流量命中了Web基础防护规则被WAF误拦截，导致通过域名访问网站显示异常，但直接通过IP访问网站正常。

处理误报事件

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护事件”，进入“防护事件”页面。

步骤5 选择“查询”页签，在网站或实例下拉列表中选择待查看的防护网站，可查看“昨天”、“今天”、“3天”、“7天”、“30天”或者自定义时间范围内的防护日志。

步骤6 在“防护事件列表”中，根据实际情况对防护事件进行处理。

- 确认事件为误报，在目标防护事件所在行的“操作”列，单击“误报处理”，添加误报处理策略。

图 4-3 误报处理



表 4-3 参数说明

参数	参数说明	取值样例
防护方式	<ul style="list-style-type: none">- “全部域名”：默认防护当前策略下绑定的所有域名。- “指定域名”：选择策略绑定的防护域名或手动输入泛域名对应的单域名。	指定域名

参数	参数说明	取值样例
防护域名	<p>“防护方式”选择“指定域名”时，需要配置此参数。</p> <p>需要手动输入当前策略下绑定的需要防护的泛域名对应的单域名，且需要输入完整的域名。</p> <p>单击“添加”，支持配置多个域名。</p>	www.example.com
条件列表	<ul style="list-style-type: none"> - 单击条件框内的“添加”增加组内新的条件，一个防护规则至少包含一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。 - 单击条件框外的“添加”可增加1组新的条件，最多可添加3组条件，多组条件之间是“或”的关系，即满足其中1组条件时，本条规则即生效。 <p>条件设置参数说明如下：</p> <ul style="list-style-type: none"> - 字段 - 子字段：当字段选择“IPv4”、“IPv6”、“Params”、“Cookie”或者“Header”时，请根据实际使用需求配置子字段。 <p>须知</p> <p>子字段的长度不能超过2048字节。</p> <ul style="list-style-type: none"> - 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 - 内容：输入或者选择条件匹配的内容。 	“路径”包含“/product”

参数	参数说明	取值样例
不检测模块	<ul style="list-style-type: none"> “所有检测模块”：通过WAF配置的其他所有的规则都不会生效，WAF将放行该域名下的所有请求流量。 “Web基础防护模块”：选择此参数时，可根据选择的“不检测规则类型”，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。 “非法请求”：可对非法请求加白。 <p>说明 非法请求判定标准：</p> <ul style="list-style-type: none"> 请求头中参数个数超过512。 URL中参数个数超过2048。 Content-Type:application/x-www-form-urlencoded，且请求体中参数个数超过8192。 	Web基础防护模块
不检测规则类型	<p>“不检测模块”选择“Web基础防护模块”时，您可以选择以下三种方式进行配置：</p> <ul style="list-style-type: none"> 按ID：按攻击事件的ID进行配置。 按类别：按攻击事件类别进行配置，如：XSS、SQL注入等。一个类别会包含一个或者多个规则id。 所有内置规则：Web基础防护规则里开启的所有防护规则。 	按类别
不检测规则ID	<p>当“不检测规则类型”选择“按ID”时，需要配置此参数。</p> <p>“防护事件”列表中事件类型为非自定义规则的攻击事件所对应的规则编号。建议您直接在防护事件页面进行误报处理。</p>	041046
不检测规则类别	<p>当“不检测规则类型”选择“按类别”时，需要配置此参数。</p> <p>在下拉框中选择事件类别。</p> <p>WAF支持的防护事件类别有：XSS攻击、网站木马、其他类型攻击、SQL注入攻击、恶意爬虫、远程文件包含、本地文件包含、命令注入攻击。</p>	SQL注入攻击
规则描述	可选参数，设置该规则的备注信息。	不拦截SQL注入攻击

参数	参数说明	取值样例
不检测字段	<p>如果您只想忽略来源于某攻击事件下指定字段的攻击，可在“高级设置”里选择指定字段进行配置，配置完成后，WAF将不再拦截指定字段的攻击事件。</p> <p>在左边第一个下拉列表中选择目标字段。支持的字段有：Params、Cookie、Header、Body、Multipart。</p> <ul style="list-style-type: none"> - 当选择“Params”、“Cookie”或者“Header”字段时，可以配置“全部”或根据需求配置子字段。 - 当选择“Body”或“Multipart”字段时，可以配置“全部”。 - 当选择“Cookie”字段时，“防护域名”可以为空。 <p>说明 当字段配置为“全部”时，配置完成后，WAF将不再拦截该字段的所有攻击事件。</p>	Params 全部

- 将源IP添加到地址组。在目标防护事件所在行的“操作”列，单击“更多 > 添加到地址组”，添加成功后将根据该地址组所应用的防护策略进行拦截或放行。“添加方式”可选择已有地址组或者新建地址组。

图 4-4 添加至地址组

✕

添加至地址组

将攻击源IP添加至地址组，添加成功后将根据该地址组所应用的防护策略进行拦截或放行。

★ 攻击源IP

★ 添加方式 选择已有地址组 新建地址组

★ 地址组名称 应用于1个策略

确定
取消

- 将源IP添加至对应防护域名下的黑白名单策略。在目标防护事件所在行的“操作”列，单击“更多 > 添加至黑白名单”，添加成功后该策略将始终对添加的攻击源IP进行拦截或放行。

图 4-5 添加至黑白名单

✕

添加至黑白名单

将攻击源IP添加至对应防护域名下的策略，添加成功后该策略将始终对添加的攻击源IP进行拦截或放行。

防护域名 www. .com 防护策略 policy_UGY2QBz1

您还可以添加 1,009 个IP/IP段。如需增加配额，请购买 [规则扩展包](#)

* 攻击源IP 10.

* 添加方式 选择已有规则 新建规则

* 规则名称 ?

* 防护动作

确定
取消

表 4-4 参数说明

参数	参数说明
添加方式	<ul style="list-style-type: none"> - 选择已有规则 - 新建规则
规则名称	<ul style="list-style-type: none"> - 添加方式选择“选择已有规则”时，在下拉框中选择规则名称。 - 添加方式选择“新建规则”时，自定义黑白名单规则的名字。
IP/IP段或地址组	添加方式选择“新建规则”时，需要配置此参数。支持添加黑白名单规则的方式，“IP/IP段”或“地址组”。
地址组名称	“IP/IP段或地址组”选择“地址组”时，需要配置此参数。 在下拉列表框中选择已添加的地址组。您也可以单击“新建地址组”创建新的地址组，详细操作请参见 添加黑白名单IP地址组 。
防护动作	<ul style="list-style-type: none"> - 拦截：IP地址或IP地址段设置的是黑名单且需要拦截，则选择“拦截”。 - 放行：IP地址或IP地址段设置的是白名单，则选择“放行”。 - 仅记录：需要观察的IP地址或IP地址段，可选择“仅记录”。

参数	参数说明
攻击惩罚	当“防护动作”设置为“拦截”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据惩罚标准设置的拦截时长来封禁访问者。
规则描述	可选参数，设置该规则的备注信息。

----结束

生效条件

设置误报处理后，1分钟左右生效，攻击事件详情列表中将不再出现此误报。您可以刷新浏览器缓存，重新访问设置了全局白名单规则的页面，验证是否配置成功。

相关操作

拦截事件处理为误报后，该误报事件对应的规则将添加到全局白名单规则列表中，您可以在“防护策略”界面的全局白名单页面查看、关闭、删除或修改该规则。有关配置全局白名单规则的详细操作，请参见[配置全局白名单规则对误报进行忽略](#)。

4.3 通过 LTS 记录 WAF 全量日志

启用WAF全量日志功能后，您可以将攻击日志、访问日志记录到云日志服务（Log Tank Service，简称LTS）中，通过LTS记录的WAF日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。

LTS对于采集的日志数据，通过海量日志数据的分析与处理，可以为您提供一个实时、高效、安全的日志处理能力。LTS默认存储日志的时间为7天，存储时间可以在1~30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）或者数据接入服务（DIS）中长期保存。

须知

- 在WAF管理控制台，您可以查看最近30天的防护日志。
- LTS按流量单独计费。有关LTS的计费详情，请参见[LTS价格详情](#)。
- 如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能开启该企业项目的全量日志。

前提条件

- [已购买WAF](#)。
- [防护网站已接入WAF](#)。


系统影响

开启全量日志功能是将WAF日志记录到LTS，不影响WAF性能。

将防护日志配置到 LTS

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护事件”，进入“防护事件”页面。

步骤5 选择“全量日志”页签，开启全量日志 ，并选择日志组和日志流，相关参数说明如表4-5所示。

图 4-6 配置全量日志



表 4-5 全量日志配置参数

参数	参数说明	取值样例
选择日志组	选择已创建的日志组，或者单击“查看日志组”，跳转到LTS管理控制台创建新的日志组。	lts-group-waf
记录攻击日志	选择已创建的日志流，或者单击“查看日志流”，跳转到LTS管理控制台创建新的日志流。 攻击日志记录每一个攻击告警信息，包括攻击事件类型、防护动作、攻击源IP等信息。	lts-topic-waf-attack

参数	参数说明	取值样例
记录访问日志	选择已创建的日志流，或者单击“查看日志流”，跳转到LTS管理控制台创建新的日志流。 访问日志记录每一个HTTP访问的关键信息，包括访问时间、访问客户端IP、访问资源URL等信息。	lts-topic-waf-access

步骤6 单击“确定”，全量日志配置成功。


您可以在LTS管理控制台查看WAF的防护日志。


----结束

在 LTS 上查看并下载 WAF 防护日志

当您将WAF防护日志配置记录到LTS上后，请参考以下操作步骤，在LTS管理控制台查看、分析、下载记录的WAF日志数据。


步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“管理与监管 > 云日志服务 LTS”，进入“日志管理”页面。

步骤4 在日志组列表中，单击  展开waf日志组（例如，“lts-group-waf”）。

步骤5 在日志流列表，单击日志流名称，进入日志流日志页面，查看并分析日志。

步骤6 在“日志搜索”页签，单击  可下载日志流中的上报日志。

支持两种下载方式：

- 本地下载：将日志文件直接下载到本地，单次下载支持最大5,000条日志。在下拉框中选择“.csv”或“.txt”，单击“开始下载日志”，可将日志导出至本地。
- 前往创建转储：通过OBS转储任务下载日志文件，详细请参考[日志转储至OBS](#)。

图 4-7 下载日志



----结束

WAF 访问日志 access_log 字段说明

字段	类型	字段说明	描述
access_log.req_id	string	随机ID标识	与攻击日志的“req_id”字段末尾8个字符一致。
access_log.time	string	访问请求的时间	日志内容记录的GMT时间。
access_log.connection_requests	string	标识该长链接第几个请求	-
access_log.engine_ip	string	WAF引擎IP	-
access_log.pid	string	标识处理该请求的引擎	引擎（worker PID）。
access_log.hostid	string	访问请求的域名标识	防护域名ID(upstream_id)。
access_log.tenantid	string	防护域名的租户ID	一个华为账号对应一个租户ID。
access_log.projectid	string	防护域名的项目ID	用户在对应区域下的项目ID。
access_log.remote_ip	string	标识请求的四层远端IP	请求的客户端IP。 须知 如果在WAF前部署了7层代理，本字段表示最靠近WAF的代理节点的IP地址。此时，真实访问者IP参考“x-forwarded-for”，“x_real_ip”字段。
access_log.remote_port	string	标识请求的四层远端端口号	请求的客户端端口号。
access_log.sip	string	标识请求的客户端IP	如，XFF等。
access_log.scheme	string	请求协议类型	请求所使用的协议有： <ul style="list-style-type: none"> • http • https
access_log.response_code	string	请求响应码	源站返回给WAF的响应状态码。
access_log.method	string	请求方法	请求行中的请求类型。通常为“GET”或“POST”。

字段	类型	字段说明	描述
access_log.http_host	string	请求的服务器域名	浏览器的地址栏中输入的地址，域名或IP地址。
access_log.url	string	请求URL	URL链接中的路径（不包含域名）。
access_log.request_length	string	请求的长度	包括请求地址、HTTP请求头和请求体的字节数。
access_log.bytes_send	string	发送给客户端的总字节数	WAF返回给客户端的总字节数。
access_log.body_bytes_sent	string	发送给客户端的响应体字节数	WAF返回给客户端的响应体字节数。
access_log.upstream_addr	string	选择的后端服务器地址	请求所对应的源站IP。例如，WAF回源到ECS，则返回源站ECS的IP。
access_log.request_time	string	标识请求处理时间	从读取客户端的第一个字节开始计时（单位：s）。
access_log.upstream_response_time	string	标识后端服务器响应时间	后端服务器响应WAF请求的时间（单位：s）。
access_log.upstream_status	string	标识后端服务器的响应码	后端服务器返回给WAF的响应状态码。
access_log.upstream_connect_time	string	源站与后端服务器建立连接的时间，单位为秒。	在使用SSL的情况下，握手过程所消耗的时间也会被记录下来。多次请求建立的时间，使用逗号分隔。
access_log.upstream_header_time	string	后端服务器接收到第一个响应头字节的用时，单位为秒。	多次请求响应的时间，使用逗号分隔。
access_log.bind_ip	string	WAF引擎回源IP	引擎回源用网卡的具体IP值，若引擎通过挂载EIP回源，此值并非EIP的值。
access_log.group_id	string	对接LTS服务的日志组ID	WAF对接云日志服务日志组ID。

字段	类型	字段说明	描述
access_log.access_stream_id	string	日志流ID	与“group_id”相关，是日志组下用户的access_stream的ID。
access_log.engine_id	string	WAF引擎标识	WAF引擎的唯一标识。
access_log.time_iso8601	string	日志的ISO 8601格式时间	-
access_log.sni	string	通过SNI请求的域名	-
access_log.tls_version	string	建立SSL连接的协议版本	请求所使用的TLS协议版本。
access_log.ssl_ciphers	string	客户端支持的曲线列表	-
access_log.ssl_session_reused	string	SSL会话是否被重用。	表示SSL会话是否被重用。 r: 是 . : 否
access_log.process_time	string	引擎的检测用时（单位：ms）	-
access_log.args	string	标识URL中的参数数据	-
access_log.x_forwarded_for	string	当WAF前部署代理时，代理节点IP链	代理节点IP链，为1个或多个IP组成的字符串。 最左边为最原始客户端的IP地址，代理服务器每成功收到一个请求，就将请求来源IP地址添加到右边。
access_log.cdn_src_ip	string	当WAF前部署CDN时CDN识别到的客户端IP	当WAF前部署CDN时，此字段记录的为CDN节点识别到的真实客户端IP。 须知 部分CDN厂商可能使用其他字段，WAF仅记录最常见的字段。
access_log.x_real_ip	string	当WAF前部署代理时，真实的客户端IP	代理节点识别到的真实客户端IP。

字段	类型	字段说明	描述
access_log.intel_crawler	string	用于情报反爬虫分析	-
access_log.ssl_ciphers_md5	string	标识ssl_ciphers的md5值	-
access_log.ssl_cipher	string	标识使用的ssl_cipher	-
access_log.web_tag	string	标识网站名称	-
access_log.user_agent	string	标识请求header中的user-agent	-
access_log.upstream_response_length	string	标识后端响应的大小	-
access_log.region_id	string	标识请求所属Region	-
access_log.enterprise_project_id	string	标识请求域名所属企业项目ID	-
access_log.referrer	string	标识请求头中的Referer内容	最大长度为128字符，大于128字符会被截断。
access_log.rule	string	标识请求命中的规则	命中多条规则此处也只会显示一条。
access_log.category	string	标识请求命中的日志分类	-
access_log.waf_time	string	访问请求的时间	-
access_log.geo	string	标记地理位置信息	<ul style="list-style-type: none"> • c: 地理位置国家名 • r: 地理位置地区名

WAF 攻击日志 attack_log 字段说明

字段	类型	字段说明	描述
attack_log.category	string	日志分类	值为“attack”。
attack_log.time	string	日志时间	-
attack_log.time_iso8601	string	日志的ISO 8601格式时间	-
attack_log.policy_id	string	防护策略ID	-
attack_log.level	string	防护策略层级	表示Web基础防护策略级别。 <ul style="list-style-type: none">• 1: 宽松• 2: 中等• 3: 严格

字段	类型	字段说明	描述
attack_log.attack	string	发生攻击的类型	<p>发生攻击的类型，仅在攻击日志中出现。</p> <ul style="list-style-type: none"> • default: 默认 • sqli: SQL注入攻击 • xss: 跨站脚本攻击 • webshell: WebShell攻击 • robot: 恶意爬虫 • cmdi: 命令注入攻击 • rfi: 远程文件包含 • lfi: 本地文件包含 • illegal: 非法请求 • vuln: 漏洞攻击 • cc: 命中CC防护规则 • custom_custom: 命中精准防护规则 • custom_whiteblackip: 命中IP黑白名单规则 • custom_geoip: 命中地理位置控制规则 • antitamper: 命中网页防篡改规则 • anticrawler: 命中JS挑战反爬虫规则 • leakage: 命中敏感信息泄露规则 • antiscan_high_freq_scan: 防扫描-高频扫描攻击。 • followed_action: 攻击惩罚，详见配置攻击惩罚标准封禁访问者指定时长。
attack_log.action	string	防护动作	<p>WAF防护攻击动作。</p> <ul style="list-style-type: none"> • block: 拦截 • log: 仅记录 • captcha: 人机验证
attack_log.sub_type	string	爬虫的子类型	<p>当attack为robot时，该字段不为空。</p> <ul style="list-style-type: none"> • script_tool: 脚本工具 • search_engine: 搜索引擎 • scanner: 扫描工具 • uncategorized: 其他爬虫
attack_log.rule	string	触发的规则ID或者自定义的策略类型描述	-

字段	类型	字段说明	描述
attack_log.rule_name	string	标识自定义的策略类型描述。	命中基础防护规则时该字段为空。
attack_log.location	string	触发恶意负载的位置	-
attack_log.req_body	string	标识请求体	-
attack_log.resp_headers	string	响应头	-
attack_log.hit_data	string	触发恶意负载的字符串	-
attack_log.resp_body	string	响应体	-
attack_log.backend.protocol	string	标识当前后端协议	-
attack_log.backend.alive	string	标识当前后端状态	-
attack_log.backend.port	string	标识当前后端端口	-
attack_log.backend.host	string	标识当前后端Host值	-
attack_log.backend.type	string	标识当前后端Host类型	IP 或域名
attack_log.backend.weight	number	标识当前后端权重	-
attack_log.status	string	请求的响应状态码	-
attack_log.upstream_status	string	标识请求的源站响应状态码	-
attack_log.req_id	string	随机ID标识	由引擎IP尾缀、请求时间戳、NGINX分配的请求ID组成。
attack_log.requestid	string	标识请求唯一ID	NGINX分配的请求ID。
attack_log.id	string	攻击ID	攻击的ID标识。
attack_log.method	string	请求方法	-
attack_log.sip	string	客户端请求IP	-

字段	类型	字段说明	描述
attack_log.sport	string	客户端请求端口	-
attack_log.host	string	请求的服务器域名	-
attack_log.http_host	string	请求的服务器域名	-
attack_log.hport	string	请求的服务器端口	-
attack_log.uri	string	请求URL	不包括域名。
attack_log.header	json string , decode后为 json table	请求header信息	-
attack_log.multipart	json string , decode后为 json table	请求multipart header	用于文件上传。
attack_log.cookie	json string , decode后为 json table	请求Cookie信息	-
attack_log.params	json string , decode后为 json table	请求URI后的参数信息	-
attack_log.body_bytes_sent	string	发送给客户端的响应体字节数	WAF发送给客户端的响应体字节数。

字段	类型	字段说明	描述
attack_log.upstream_response_time	string	后端服务器从上游服务接收响应内容所经过的时间，单位为秒。	多次请求响应的时间，使用逗号分隔。
attack_log.engine_id	string	引擎的唯一标识	-
attack_log.region_id	string	标识引擎所在region的ID	-
attack_log.engine_ip	string	标识引擎IP	-
attack_log.process_time	string	引擎的检测用时	-
attack_log.remote_ip	string	标识请求的四层客户端IP	-
attack_log.x_forwarded_for	string	标识请求头中“X-Forwarded-For”的内容	-
attack_log.cdn_src_ip	string	标识请求头中“Cdn-Source-Ip”的内容	-
attack_log.x_real_ip	string	标识请求头中“X-Real-IP”的内容	-
attack_log.group_id	string	日志组ID	对接LTS服务的日志组ID。
attack_log.attack_stream_id	string	日志流ID	与“group_id”相关，是日志组下用户的access_stream的ID。
attack_log.host_id	string	防护域名ID (upstream_id)	-
attack_log.tenant_id	string	防护域名的租户ID	-
attack_log.project_id	string	防护域名的项目ID	-
attack_log.enterprise_project_id	string	标识请求域名所属企业项目ID	-

字段	类型	字段说明	描述
attack_log.web_tag	string	标识网站名称	-
attack_log.req_body	string	识请求体（超过 1K 记录时会被截断）	-

5 配置防护策略

5.1 防护配置概述

本文介绍Web应用防火墙（Web Application Firewall，WAF）服务的防护策略的配置流程以及WAF引擎检测机制及规则的检测顺序。

防护规则概览

网站接入WAF防护后，您需要为网站配置防护策略。

表 5-1 可配置的防护规则

防护规则	说明	参考文档
Web基础防护规则	覆盖OWASP（Open Web Application Security Project，简称OWASP）TOP 10中常见安全威胁，通过预置丰富的信誉库，对恶意扫描器、IP、网马等威胁进行检测和拦截。	配置Web基础防护规则防御常见Web攻击
CC攻击防护规则	可以自定义CC防护规则，限制单个IP/Cookie/Referer访问者对您的网站上特定路径（URL）的访问频率，WAF会根据您配置的规则，精准识别CC攻击以及有效缓解CC攻击。	配置CC攻击防护规则防御CC攻击
精准访问防护规则	精准访问防护策略可对HTTP首部、Cookie、访问URL、请求参数或者客户端IP进行条件组合，定制化防护策略，为您的网站带来更精准的防护。	配置精准访问防护规则定制化防护策略
黑白名单规则	配置黑白名单规则，阻断、仅记录或放行指定IP的访问请求，即设置IP黑/白名单。	配置IP黑白名单规则拦截/放行指定IP

防护规则	说明	参考文档
攻击惩罚规则	当恶意请求被拦截时，可设置自动封禁访问者一段时间，该功能和其他规则结合使用。	配置攻击惩罚标准封禁访问者指定时长
地理位置访问控制规则	针对指定国家、地区的来源IP自定义访问控制。	配置地理位置访问控制规则拦截/放行特定区域请求
网页防篡改规则	当用户需要防护静态页面被篡改时，可配置网页防篡改规则。	配置网页防篡改规则避免静态网页被篡改
网站反爬虫规则	动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别爬虫行为。	配置网站反爬虫防护规则防御爬虫攻击
防敏感信息泄露规则	该规则可添加两种类型的防敏感信息泄露规则： <ul style="list-style-type: none">敏感信息过滤。配置后可对返回页面中包含的敏感信息做屏蔽处理，防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露。响应码拦截。配置后可拦截指定的HTTP响应码页面。	配置防敏感信息泄露规则避免敏感信息泄露
全局白名单规则	针对特定请求忽略某些攻击检测规则，用于处理误报事件。	配置全局白名单规则对误报进行忽略
隐私屏蔽规则	隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。	配置隐私屏蔽规则防隐私信息泄露
扫描防护规则	扫描防护模块通过识别扫描行为和扫描器特征，阻止攻击者或扫描器对网站的大规模扫描行为，自动阻断高频Web攻击、高频目录遍历攻击，并封禁攻击源IP一段时间，帮助Web业务降低被入侵的风险并减少扫描带来的垃圾流量。	配置扫描防护规则自动阻断高频攻击

WAF 引擎规则检测顺序

Web应用防火墙内置的防护规则，可帮助您防范常见的Web应用攻击，包括XSS攻击、SQL注入、爬虫检测、Webshell检测等。同时，您也可以根据自己网站防护的需要，灵活配置防护规则，Web应用防火墙根据您配置的防护规则更好的防护您的网站业务。WAF引擎内置防护规则的检测流程如[图5-1](#)所示，自定义规则的检测顺序如[图5-2](#)所示。

📖 说明

在防护配置页面，勾选“按检测顺序排序”，所有的防护规则将按WAF的检测顺序进行重新排序。

图 5-1 WAF 引擎检测图

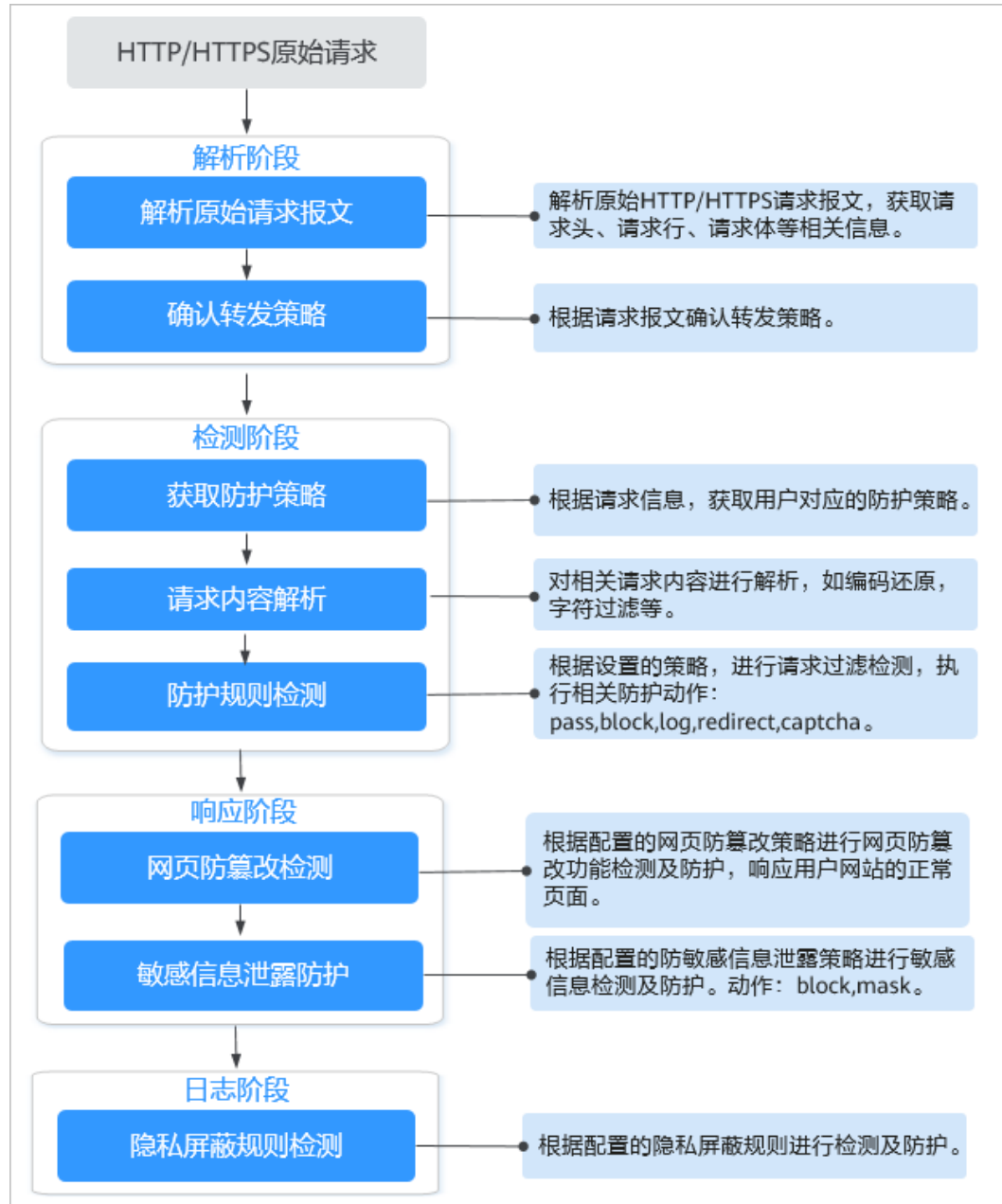


图 5-2 防护规则的检测顺序



响应动作:

- pass: 命中规则后无条件放行当前请求。
- block: 命中规则后拦截当前请求。
- captcha: 命中规则后执行人机验证动作。
- redirect: 命中规则后通知客户端执行重定向动作。

- log: 命中规则后仅记录攻击信息。
- mask: 命中规则后对相关敏感信息进行脱敏处理。

5.2 配置 Web 基础防护规则防御常见 Web 攻击

Web基础防护开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。您还可以根据实际使用需求，开启Webshell检测、深度反逃逸检测和header全检测等Web基础防护。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件


- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#)章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。


约束条件

- Web基础防护支持“拦截”和“仅记录”模式。
- 当Web基础防护设置为“拦截”模式时，您可以[配置攻击惩罚标准](#)。配置攻击惩罚后，如果访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据攻击惩罚设置的拦截时长来封禁访问者。
- 目前华北-北京一、华北-北京四、华东-上海一、华东-上海二、华南-广州、华南-深圳、西南-贵阳一、中国-香港和亚太-曼谷区域支持深度检测和header全检测功能。
- 目前华北-北京四、中国-香港区域支持Shiro解密检测功能。

开启 Web 基础防护规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“Web基础防护”配置框，用户可根据自己的需要开启或关闭Web基础防护策略。

- ：开启状态。
- ：关闭状态。

步骤7 配置Web基础防护规则，如图5-3所示。

图 5-3 配置防护规则



1. 默认开启“常规检测”，防护SQL注入、XSS跨站脚本、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击。其中，SQL注入攻击主要基于语义进行检测。
2. 选择“防护等级”。

Web基础防护设置了三种防护等级：“默认规则集【宽松】”、“默认规则集【中等】”、“默认规则集【严格】”，默认情况下，选择“默认规则集【中等】”。

表 5-2 防护等级说明

防护等级	说明
默认规则集【宽松】	防护粒度较粗，只拦截攻击特征比较明显的请求。当误报情况较多的场景下，建议选择“宽松”模式。
默认规则集【中等】	默认为“中等”防护模式，满足大多数场景下的Web防护需求。
默认规则集【严格】	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，例如jolokia网络攻击、探测CGI漏洞、探测Druid SQL注入攻击。 建议您等待业务运行一段时间后，根据防护效果配置全局白名单规则，再开启“严格”模式，使WAF能有效防护更多攻击。

单击“查看规则集详情”，可查看Web基础防护规则中“防护等级”为“宽松”、“中等”、“严格”的所有规则的详细信息。

📖 说明

单击🔍，您可以根据“CVE编号”、“危险等级”、“应用类型”或“防护类型”，搜索指定规则。

表 5-3 防护规则说明

参数	说明
规则ID	防护规则的ID，由系统自动生成。
规则描述	防护规则对应的攻击详细描述。
CVE编号	防护规则对应的CVE（Common Vulnerabilities & Exposures，通用漏洞披露）编号。对于非CVE漏洞，显示为--。
危险等级	防护规则防护漏洞的危险等级，包括： <ul style="list-style-type: none"> - 高危 - 中危 - 低危
应用类型	防护规则对应的应用类型，WAF覆盖的应用类型见 WAF覆盖的应用类型 。
防护类型	防护规则的类型，WAF覆盖的防护类型：SQL注入、命令注入、跨站脚本、XXE注入、表达式注入攻击、SSRF、本地文件包含、远程文件包含、网站木马、恶意爬虫、会话固定漏洞攻击、反序列化漏洞、远程命令执行、信息泄露、拒绝服务、源码/数据泄露。

3. 根据实际业务情况，开启“检测范围”中的检测项。

表 5-4 检测项说明

检测项	说明
深度检测	防护同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等深度反逃逸。 说明 开启“深度检测”后，WAF将对深度反逃逸进行检测防护。
header全检测	默认关闭。关闭状态下WAF会检测常规存在注入点的header字段，包含User-Agent、Content-type、Accept-Language和Cookie。 说明 开启“header全检测”后，WAF将对请求里header中所有字段进行攻击检测。

检测项	说明
Shiro解密检测	<p>默认关闭。开启后，WAF会对Cookie中的rememberMe内容做AES，Base64解密后再检测。Web应用防火墙检测机制覆盖了几百种已知泄露密钥。</p> <p>说明 如果您的网站使用的是Shiro 1.2.4及之前的版本，或者升级到了Shiro 1.2.5及以上版本但是未配置AES密钥，强烈建议您开启“Shiro解密检测”，以防攻击者利用已泄露的密钥构造攻击。</p>

4. 配置“Webshell检测”。

开启“Webshell检测”后，WAF将对通过上传接口植入的网页木马进行检测。

步骤8 配置防护措施，选择“防护动作”。

- 拦截：发现攻击后立即阻断并记录。
设置为“拦截”时，您可以根据需要选择已配置的攻击惩罚。有关配置攻击惩罚的详细操作，请参见[配置攻击惩罚标准封禁访问者指定时长](#)。
- 仅记录：发现攻击后只记录不阻断。

----结束

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“仅记录”模式进行观察。一般情况下，建议您观察一至两周，然后分析仅记录模式下的攻击日志。
 - 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“拦截”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，建议调整防护等级或者设置全局白名单来避免正常业务的误拦截。
- 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、JavaScript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：“https://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，建议使用对象存储服务或者其他方式上传。

防护效果

假如已添加域名“www.example.com”，且已开启了Web基础防护的“常规检测”，防护模式为“拦截”。您可以参照以下步骤验证WAF防护效果：

步骤1 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

- 不能正常访问，参照[网站设置](#)章节重新完成域名接入。
- 能正常访问，执行2。

步骤2 清理浏览器缓存，在浏览器中输入“http://www.example.com?id=1%27%20or%201=1”模拟SQL注入攻击。

步骤3 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志。

----结束

配置示例-拦截 SQL 注入攻击

假如防护域名“www.example.com”已接入WAF，您可以参照以下操作步骤验证WAF拦截SQL注入攻击。

步骤1 开启Web基础防护的“常规检测”，并将防护模式设置为“拦截”。

图 5-4 开启“常规检测”



步骤2 开启Web基础防护。

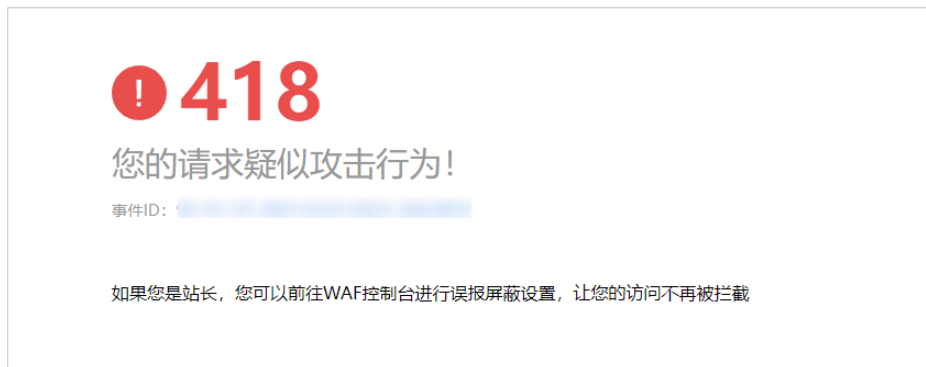
图 5-5 Web 基础防护配置框



步骤3 清理浏览器缓存，在浏览器中输入模拟SQL注入攻击（例如，http://www.example.com?id=' or 1=1）。

WAF将拦截该访问请求，拦截页面示例如图5-6所示。

图 5-6 WAF 拦截攻击请求



步骤4 返回Web应用防火墙管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

5.3 配置智能访问控制规则精准智能防御 CC 攻击

开启智能访问控制规则后，WAF中的压力学习模型会根据源站返回的HTTP状态码和时延等来实时地感知源站的压力，从而识别源站是否被CC攻击了，WAF再根据异常检测模型实时地检测源站在HTTP协议上的特征的异常行为，然后基于这些异常特征，使用AI算法生成精准防护规则和CC防护规则，来防御CC攻击，保护您的网站安全。

须知

智能访问控制功能现处于公测阶段，如需使用请[提交工单](#)申请开通智能访问控制功能。

前提条件

- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#) 章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。


约束条件


- “云模式”仅专业版和铂金版支持智能访问控制规则。
- 仅“华北”区域支持智能访问控制规则。
- 智能访问控制规则的优先级最低。
- 通过“云模式-ELB接入”方式添加网站时，ELB配置的监听器中使用的“前端协议”为TCP、UDP、QUIC时，使用该规则不生效。

- 关闭智能“生成CC防护规则”，智能CC生成的所有规则同步删除。
- 关闭智能“生成精准防护规则”，智能精准防护规则生成的所有规则同步删除。

配置智能访问控制规则

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“智能访问控制”配置框，用户可根据自己的需要开启或关闭智能访问控制策略。

- ：开启状态。
- ：关闭状态。

步骤7 单击“智能生成规则设置”，进入“智能生成规则设置”页面，参数配置参考表5-5。

图 5-7 智能生成规则设置



智能生成规则设置

1 使用说明

1.生成智能规则后，需要打开相应CC攻击防护规则或精准访问控制规则状态后智能规则才会生效。
2.当智能访问控制规则状态关闭后，所有智能生成的规则都将会被同步删除。

生成CC防护规则

动作 仅记录 拦截 JS挑战

老化时间 秒

生成精准防护规则

动作 仅记录 拦截

老化时间 自动 自定义 秒

智能动态限速

确定 取消

表 5-5 智能生成规则参数说明

规则	参数	参数说明
生成CC防护规则	动作	<p>支持“仅记录”、“拦截”和“JS挑战”。</p> <ul style="list-style-type: none"> 仅记录：发现攻击行为后只记录不阻断攻击。 拦截：发现攻击行为后立即阻断并记录。 JS挑战：表示WAF向客户端返回一段正常浏览器可以自动执行的JavaScript代码。如果客户端正常执行了JavaScript代码，则WAF在一段时间（默认30分钟）内放行该客户端的所有请求（不需要重复验证），否则拦截请求。 <p>说明 请求的Referer跟当前的Host不一致时，JS挑战不生效。</p>
	老化时间	当攻击结束，生成的防护规则会在经过老化时间后被删除。
生成精准防护规则	动作	<p>支持“仅记录”、“拦截”。</p> <ul style="list-style-type: none"> 仅记录：发现攻击行为后只记录不阻断攻击。 拦截：发现攻击行为后立即阻断并记录。
	老化时间	当攻击结束，生成的防护规则会在经过老化时间后被删除。
智能动态限速	防护动作	<p>支持“仅记录”、“拦截”和“JS挑战”。</p> <ul style="list-style-type: none"> 仅记录：发现攻击行为后只记录不阻断攻击。 拦截：发现攻击行为后立即阻断并记录。 JS挑战：表示WAF向客户端返回一段正常浏览器可以自动执行的JavaScript代码。如果客户端正常执行了JavaScript代码，则WAF在一段时间（默认30分钟）内放行该客户端的所有请求（不需要重复验证），否则拦截请求。 <p>说明 请求的Referer跟当前的Host不一致时，JS挑战不生效。</p>

规则	参数	参数说明
	防护等级	当发现防护规则拦截了您的正常业务时，可调整防护等级。宽松等级对业务的误报率降低，但漏报率可能会增高；而严格等级对业务的误报率可能会增高，但漏报率降低。 支持“宽松”、“正常”、“严格”三个等级。
	最小阈值	<ul style="list-style-type: none">如果对源站所学习到的基线小于“最小阈值”，就以“最小阈值”为限速频率。如果所学习到的基线大于“最小阈值”，就以所学习到基线作为限速频率。


步骤8 单击“确定”，规则配置完成。

单击“查看智能生成规则”，可查看WAF检测到CC攻击后自动生成的防护规则。

----结束

5.4 配置 CC 攻击防护规则防御 CC 攻击

CC攻击防护规则支持通过限制单个IP/Cookie/Referer访问者对防护网站上源端的访问频率，同时支持策略限速（同一策略下对应的所有域名请求次数合并限速）、域名限速（每个域名单独统计总请求次数）和URL限速（每个URL请求单独统计请求次数），精准识别CC攻击以及有效缓解CC攻击；当您配置完CC攻击防护规则并开启CC攻击防

护后（即“CC攻击防护”配置框的“状态”为 ），WAF才能根据您配置的CC攻击防护规则进行CC攻击防护。

CC攻击防护规则可以添加引用表，引用表防护规则对所有防护域名都生效，即所有防护域名都可以使用CC攻击防护规则的引用表。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件

- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见[将网站接入WAF防护（云模式-ELB接入）](#)章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#)章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。

约束条件

- 云模式入门版和标准版不支持引用表管理功能。
- 当“逻辑”关系选择“包含任意一个”、“不包含任意一个”、“等于任意一个”、“不等于任意一个”、“前缀为任意一个”、“前缀不为任意一个”、“后缀为任意一个”或者“后缀不为任意一个”时，需要选择引用表，创建引用表的详细操作请参见[创建引用表对防护指标进行批量配置](#)。
- 仅云模式的CNAME接入方式支持配置“全局计数”。
- 使用云模式WAF时，如果WAF前使用了高防、CDN（Content Delivery Network，内容分发网络）、云加速等代理时，建议“限速模式”选择“源限速 > 用户限速”，并勾选“全局计数”。

📖 说明


如果网站在接入WAF前，已经使用了CDN、高防等其他代理服务，WAF收到的访问IP会被分散到各个WAF节点进行流量转发，WAF默认为WAF节点单独计数。因此，WAF针对单个Web访问者的访问次数的计数会分散，所以“限速频率”中访问次数的设置原则如下：

- 云模式CNAME接入：该模式支持“全局计数”，即支持将已经标识的请求在一个或多个WAF节点上的计数聚合，因此，配置时勾选“全局计数”即可。
- 独享模式：该模式暂不支持“全局计数”，因此配置“限速频率”中访问次数应配置为允许单个Web访问者在限速周期内访问网站的次数/MIN(WAF前使用的代理服务总数：WAF节点数)。
例如，WAF前已使用3个代理服务，WAF节点数（防护该网站的独享引擎实例数）为2，则取其最小值为2，如果您想当单个Web访问者在限速周期内访问网站的次数不能超过1000次，则“限速频率”中访问次数应配置为1000除以2，500。
- “云模式-ELB接入”方式不支持“Response Code”、“Response Length”、“Response Time”、“Response Header”和“Response Body”字段，且“云模式-CNAME”仅铂金版支持响应字段。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

配置 CC 攻击防护规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“CC攻击防护”配置框，用户可根据自己的需要开启或关闭CC攻击防护策略。

- ：开启状态。
- ：关闭状态。

步骤7 在“CC攻击防护”规则配置列表左上方，单击“添加规则”。

步骤8 在弹出的对话框中，根据[表5-6](#)配置CC防护规则。

例如，通过配置CC攻击防护规则实现以下功能：根据Cookie标识的用户字段（例如 name），当WAF识别到同一name值的用户在60秒内访问您域名下的URL（例如，/admin*）页面超过10次时，封禁该用户访问目标网址600秒。

图 5-8 添加 CC 防护规则

添加CC防护规则

限速模式 [?]

源限速 目的限速

对源端限速，如果IP（或用户）的访问频率超过限速频率，就会对该IP（或用户）的访问限速。

限速类型

IP限速 用户限速 其他

域名聚合统计 [?]

当开启时，如配置的泛域名为*.a.com，会将所有子域名（b.a.com, c.a.com）的请求一起聚合统计。

限速条件

字段	子字段	逻辑	内容	大小写敏感	操作
路径	--	包含	/admin	<input checked="" type="checkbox"/>	删除

+ 添加条件 您还可以添加29项条件。（多个条件同时成立才生效） 添加引用表

限速频率 [?]

- 10 + 次 - 60 + 秒

全局计数 [?]

采取防护措施

防护动作 [?]

阻断 动态阻断 人机验证 仅记录 JS挑战

阻断方式

攻击惩罚 **阻断时长**

阻断时长 [?]

- 600 + 秒

取消 确定

表 5-6 CC 防护规则参数说明

参数	参数说明	取值样例
规则名称	自定义规则名称。	wafptest
规则描述	可选参数，设置该规则的备注信息。	--

参数	参数说明	取值样例
限速模式	<ul style="list-style-type: none"> “源限速”：对源端限速，如某IP（或用户）的访问频率超过限速频率，就会对该IP（或用户）的访问限速。 <ul style="list-style-type: none"> “IP限速”：根据IP区分单个Web访问者。 “用户限速”：根据Cookie键值或者Header区分单个Web访问者。 “其他”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。 <p>说明 选择“其他”时，“Referer”对应的“内容”填写为包含域名的完整URL链接，仅支持前缀匹配和精准匹配的逻辑，“内容”里不能含有连续的多条斜线的配置，如“///admin”，WAF引擎会将“///”转为“/”。 例如：如果用户不希望访问者从“www.test.com”访问网站，则“Referer”对应的“内容”设置为“http://www.test.com”。</p> <ul style="list-style-type: none"> “目的限速”：选择该参数时，可选择以下限速类型进行配置： <ul style="list-style-type: none"> “策略限速”：当多个域名共用一个策略时，该策略下对应的所有域名请求次数合并限速（不区分访问IP）；泛域名防护场景时，该泛域名对应的所有子域名的请求次数合并限速（不区分访问IP）。 “域名限速”：每个域名单独统计总请求次数，超过设定值则触发防护动作（不区分访问IP）。 “URL限速”：每个URL请求单独统计请求次数，超过设定值则触发防护动作（不区分访问IP）。 	--
用户标识	<p>“限速模式”选择“源限速 > 用户限速”时，需要配置此参数：</p> <ul style="list-style-type: none"> 选择Cookie时，设置Cookie字段名，即用户需要根据网站实际情况配置唯一可识别Web访问者的Cookie中的某属性变量名。用户标识的Cookie，不支持正则，必须完全匹配。 例如：如果网站使用Cookie中的某个字段name唯一标识用户，那么可以用name字段来区分Web访问者。 选择Header时，设置需要防护的自定义HTTP首部，即用户需要根据网站实际情况配置可识别Web访问者的HTTP首部。 	name

参数	参数说明	取值样例
域名聚合统计	<p>“限速模式”选择“目的限速 > 策略限速”时，不需要配置此参数。</p> <p>默认关闭，开启后，泛域名对应的所有子域名的请求次数合并限速(不区分访问IP)。例如，配置的泛域名为“*.a.com”，会将所有子域名（b.a.com，c.a.com等）的请求一起聚合统计。</p>	--
限速条件	<p>单击“添加条件”增加新的条件，至少配置一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。</p> <ul style="list-style-type: none"> • 字段 • 子字段：当“字段”选择IPv4、IPv6、Cookie、Header、Params等字段时，请根据实际需求配置子字段。 <p>须知 子字段的长度不能超过2048字节。</p> <ul style="list-style-type: none"> • 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 <p>说明 当“逻辑”关系选择“包含任意一个”、“不包含任意一个”、“等于任意一个”、“不等于任意一个”、“前缀为任意一个”、“前缀不为任意一个”、“后缀为任意一个”或者“后缀不为任意一个”时，需要选择引用表，创建引用表的详细操作请参见创建引用表对防护指标进行批量配置。</p> <ul style="list-style-type: none"> • 内容：输入或者选择条件匹配的内容。 • 大小写敏感：开启后，系统在检测配置的内容时，将区分大小写。能够帮助系统更准确地识别和处理各种请求，从而有效提升策略的精确度和有效性。 	“路径”包含“/admin/”

参数	参数说明	取值样例
限速频率	<p>单个Web访问者在限速周期内可以正常访问的次数，如果超过该访问次数，Web应用防火墙服务将根据配置的“防护动作”来处理。</p> <p>“全局计数”：根据不同的限速模式，将已经标识的请求在一个或多个WAF节点上的计数聚合。默认为每WAF节点单独计数，开启后本区域所有节点合并计数。“IP限速”不能满足针对某个用户进行限速，需要选择“用户限速”或“其他”的Referer限速，此时标识的请求可能会访问到不同的WAF节点，开启全局计数后，将请求访问的一个或多个WAF节点访问量聚合，达到全局统计的目的。</p> <p>说明</p> <p>如果网站在接入WAF前，已经使用了CDN、高防等其他代理服务，WAF收到的访问IP会被分散到各个WAF节点进行流量转发，WAF默认为WAF节点单独计数。因此，WAF针对单个Web访问者的访问次数的计数会分散，所以“限速频率”中访问次数的设置原则如下：</p> <ul style="list-style-type: none">• 云模式CNAME接入：该模式支持“全局计数”，即支持将已经标识的请求在一个或多个WAF节点上的计数聚合，因此，配置时勾选“全局计数”即可。• 独享模式：该模式暂不支持“全局计数”，因此配置“限速频率”中访问次数应配置为允许单个Web访问者在限速周期内访问网站的次数/MIN(WAF前使用的代理服务总数：WAF节点数)。 <p>例如，WAF前已使用3个代理服务，WAF节点数（防护该网站的独享引擎实例数）为2，则取其最小值为2，如果您想当单个Web访问者在限速周期内访问网站的次数不能超过1000次，则“限速频率”中访问次数应配置为1000除以2，500。</p>	10次/60秒

参数	参数说明	取值样例
防护动作	<p>当访问的请求频率超过“限速频率”时，可设置以下防护动作：</p> <ul style="list-style-type: none"> ● 人机验证：表示超过“限速频率”后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。人机验证目前支持英文。 ● 阻断：表示超过“限速频率”将直接阻断。 ● 动态阻断：上一个限速周期内，请求频率超过“限速频率”将被阻断，那么在下一个限速周期内，请求频率超过“放行频率”将被阻断。 ● 仅记录：表示超过“限速频率”将只记录不阻断。 ● JS挑战：表示WAF向客户端返回一段正常浏览器可以自动执行的JavaScript代码。如果客户端正常执行了JavaScript代码，则WAF在一段时间（默认30分钟）内放行该客户端的所有请求（不需要重复验证），否则拦截请求。 <p>说明 请求的Referer跟当前的Host不一致时，JS挑战不生效。</p>	阻断
锁定验证	<p>当“防护动作”选择“人机验证”时，需要配置该参数。</p> <p>当人机验证未通过时，在设定时间内的访问都要进行验证。</p>	300秒
生效模式	<ul style="list-style-type: none"> ● 立即生效：防护规则开启后，规则立即生效。 ● 自定义：自定义规则生效时间段。 	立即生效
放行频率	<p>当“防护动作”选择“动态阻断”时，可配置放行频率。</p> <p>如果在一个限速周期内，访问超过“限速频率”触发了拦截，那么，在下一个限速周期内，拦截阈值动态调整为“放行频率”。</p> <p>“放行频率”小于等于“限速频率”。</p> <p>说明 当“放行频率”设置为0时，表示如果上一个限速周期发生过拦截后，下一个限速周期所有的请求都不放行。</p>	8次/60秒

参数	参数说明	取值样例
阻断方式	<p>当“防护动作”选择“阻断”时，支持两种阻断方式。</p> <ul style="list-style-type: none"> 攻击惩罚：设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据惩罚标准设置的拦截时长来封禁访问者。 阻断时长：可设置阻断后恢复正常访问页面的时间。 	阻断时长
阻断时长	当“防护动作”选择“阻断”时，可设置阻断后恢复正常访问页面的时间。	600秒
阻断页面	<p>当“防护动作”选择“阻断”时，需要设置该参数，即当访问超过限速频率时，返回的错误页面。</p> <ul style="list-style-type: none"> 当选择“默认设置”时，返回的错误页面为系统默认的阻断页面。 当选择“自定义”时，返回错误信息由用户自定义。 当选择“重定向”时，根据界面提示配置重定向URL。 	自定义
HTTP返回码	当“阻断页面”选择“自定义”时，支持配置HTTP返回码。	418
响应标头	<p>当“阻断页面”选择“自定义”时，支持配置响应标头。</p> <p>单击“添加响应标头字段”，配置响应标头参数及参数值。</p>	-
页面类型	当“阻断页面”选择“自定义”时，可选择阻断页面的类型“application/json”、“text/html”或者“text/xml”。	text/html
页面内容	当“阻断页面”选择“自定义”时，可设置自定义返回的内容。	<p>不同页面类型对应的页面内容样式：</p> <ul style="list-style-type: none"> text/html: <pre><html><body>Forbidden</body></html></pre> application/json: {"msg": "Forbidden"} text/xml: <pre><?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error></pre>

步骤9 单击“确定”，添加的CC攻击防护规则展示在CC规则列表中。

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果需要修改添加的CC攻击防护规则时，可单击待修改的CC攻击防护规则所在行的“修改”，修改CC攻击防护规则。
- 如果需要删除用户自行添加的CC攻击防护规则时，可单击待删除的CC攻击防护规则所在行的“删除”，删除CC攻击防护规则。

----结束

防护效果

假如已添加域名“www.example.com”，且配置了如图5-8所示“阻断”防护动作的CC防护规则。可参照以下步骤验证防护效果：

步骤1 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

- 不能正常访问，参照[网站设置](#)章节重新完成域名接入。
- 能正常访问，执行2。

步骤2 清理浏览器缓存，在浏览器中访问满足Cookie条件的“http://www.example.com/admin”页面，在60秒内刷新页面10次，正常情况下，在第11次访问该页面时，返回自定义的拦截页面；60秒后刷新目标页面，页面访问正常。

如果您设置了“人机验证”防护动作，当用户访问超过限制后需要输入验证码才能继续访问。

图 5-9 人机验证



步骤3 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志。

----结束

配置示例-人机验证

假如防护域名“www.example.com”已接入WAF，您可以参照以下操作步骤验证人机验证防护效果。

步骤1 添加防护动作为“人机验证”CC防护规则。

图 5-10 添加“人机验证”防护规则



步骤2 开启CC攻击防护。

图 5-11 开启 CC 防护



步骤3 清理浏览器缓存，在浏览器中访问“http://www.example.com/admin/”页面。

当您在60秒内访问页面10次，在第11次访问该页面时，页面弹出验证码。此时，您需要输入验证码才能继续访问。

图 5-12 人机验证



步骤4 返回Web应用防火墙管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

5.5 配置精准访问防护规则定制化防护策略

精准访问防护规则可对常见的HTTP字段（如IP、路径、Referer、User Agent、Params等）进行条件组合，用来筛选访问请求，并对命中条件的请求设置仅记录、放行或阻断操作。同时支持“JS挑战”验证，即WAF向客户端返回一段正常浏览器可以自动执行的JavaScript代码。如果客户端正常执行了JavaScript代码，则WAF在一段时间（默认30分钟）内放行该客户端的所有请求（不需要重复验证），否则拦截请求。

精准访问防护规则可以添加引用表，引用表防护规则对所有防护域名都生效，即所有防护域名都可以使用精准防护规则的引用表。

📖 说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件

- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#) 章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。

约束条件

- 云模式入门版不支持该功能。
- 云模式入门版和标准版不支持“全检测”检测模式。
- 云模式入门版和标准版不支持引用表管理功能。
- “云模式-ELB接入”方式不支持“Response Code”、“Response Length”、“Response Time”、“Response Header”和“Response Body”字段，且“云模式-CNAME”仅铂金版支持响应字段。
- 当精准访问防护规则的“防护动作”设置为“阻断”时，您可以[配置攻击惩罚标准封禁访问者指定时长](#)。配置攻击惩罚后，如果访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据攻击惩罚设置的拦截时长来封禁访问者。
- 配置的“路径”的“内容”不能包含特殊字符（<>*）。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。


应用场景

精准访问防护支持业务场景定制化的防护策略，可用于盗链防护、网站管理后台保护等场景。

配置精准访问防护规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“精准访问防护”配置框，用户可根据自己的需要开启或关闭精准访问防护策略。

- ：开启状态。
- ：关闭状态。

步骤7 在“精准访问防护配置”页面，设置“检测模式”。

精准访问防护规则提供了两种检测模式：

- 短路检测：当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
- 全检测：当用户的请求符合精准防护中的拦截条件时，不会立即拦截，它会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。

步骤8 在“精准访问防护”规则配置列表左上方，单击“添加规则”。

步骤9 在弹出的对话框中，根据[表5-7](#)添加精准访问防护规则。

以[图5-13](#)的配置为例，其含义为：当用户访问目标域名下包含“/admin”的URL地址时，WAF将阻断该用户访问目标URL地址。

须知

如果不确定配置的精准访问防护规则是否会使WAF误拦截正常的访问请求，您可以先将精准访问防护规则的“防护动作”设置为“仅记录”，在“防护事件”页面查看防护事件，确认WAF不会误拦截正常的访问请求后，再将该精准访问防护规则的“防护动作”设置为“阻断”。

图 5-13 添加精准访问防护规则

The screenshot shows a configuration window titled "添加精准访问防护规则" (Add Precise Access Protection Rule). It contains the following elements:

- Rule Name:** A text input field.
- Rule Description (Optional):** A text input field.
- Conditions List:** A table with columns: 字段 (Field), 子字段 (Sub-field), 逻辑 (Logic), 内容 (Content), 大小写敏感 (Case Sensitive), and 操作 (Action). One condition is added: Path (路径) contains (包含) "/admin".
- Take Protection Measures (采取防护措施):**
 - Protection Action (防护动作):** Radio buttons for 阻断 (Block), 放行 (Allow), 仅记录 (Log), and JS挑战 (JS Challenge). "Block" is selected.
 - Block Page (阻断页面):** Radio buttons for 默认设置 (Default), 自定义 (Custom), and 重定向 (Redirect). "Default" is selected.
 - Attack Penalty (攻击惩罚):** A dropdown menu set to "无攻击惩罚" (No attack penalty).
 - Effective Mode (生效模式):** Buttons for 立即生效 (Take effect immediately) and 自定义 (Custom). "Take effect immediately" is selected.
 - Priority (优先级):** A numeric input field set to 50. Below it, text reads "值越小, 优先级越高" (The smaller the value, the higher the priority).
- Buttons:** 取消 (Cancel) and 确定 (Confirm) buttons at the bottom right.

表 5-7 规则参数说明

参数	参数说明	取值样例
规则名称	自定义规则名称。	wafstest
规则描述	可选参数，设置该规则的备注信息。	--

参数	参数说明	取值样例
条件列表	<p>单击“添加条件”增加新的条件，一个防护规则至少包含一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。</p> <p>条件设置参数说明如下：</p> <ul style="list-style-type: none"> • 字段 • 子字段：当字段选择“IPv4”、“IPv6”、“Params”、“Cookie”、“Response Header”或者“Header”时，请根据实际使用需求配置子字段。 <p>须知 子字段的长度不能超过2048字节。</p> <ul style="list-style-type: none"> • 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 <p>说明</p> <ul style="list-style-type: none"> - 选择“包含任意一个”、“不包含任意一个”、“等于任意一个”、“不等于任意一个”、“前缀为任意一个”、“前缀不为任意一个”、“后缀为任意一个”或者“后缀不为任意一个”时，“内容”需要选择引用表名称，创建引用表的详细操作请参见创建引用表对防护指标进行批量配置。 - “不包含任意一个”、“不等于任意一个”、“前缀不为任意一个”、“后缀不为任意一个”是指当访问请求中字段不包含、不等于、前/后缀不为引用表中设置的任何一个值时，WAF将进行防护动作（阻断、放行或仅记录）。例如，设置“路径”字段的逻辑为“不包含所有”，选择了“test”引用表，如果“test”引用表中设置的值为test1、test2和test3，则当访问请求的路径不包含test1、test2或test3时，WAF将进行防护动作。 <ul style="list-style-type: none"> • 内容：输入或者选择条件匹配的内容。 <p>说明 具体的配置请参见表5-19。</p> <ul style="list-style-type: none"> • 大小写敏感：开启后，系统在检测配置的内容时，将区分大小写。能够帮助系统更准确地识别和处理各种请求，从而有效提升策略的精确度和有效性。 	<ul style="list-style-type: none"> • “路径”包含“/admin/” • “User Agent”前缀不为“mozilla/5.0” • “IP”等于“192.168.2.3” • “Cookie[key1]”前缀不为“jsessionid”

参数	参数说明	取值样例
防护动作	<ul style="list-style-type: none"> ● 阻断：表示拦截命中规则的请求，并向发起请求的客户端返回拦截响应页面。WAF默认使用统一的拦截响应页面，您也可以自定义拦截响应页面。 ● 放行：表示不拦截命中规则的请求，直接放行。 ● 仅记录：表示不拦截命中规则请求，只通过日志记录请求命中了规则。您可以通过WAF日志，查询命中当前规则请求，分析规则的防护效果。例如，是否有误拦截等。 ● JS挑战：表示WAF向客户端返回一段正常浏览器可以自动执行的JavaScript代码。如果客户端正常执行了JavaScript代码，则WAF在一段时间（默认30分钟）内放行该客户端的所有请求（不需要重复验证），否则拦截请求。 <p>说明 请求的Referer跟当前的Host不一致时，JS挑战不生效。</p>	“阻断”
攻击惩罚	当“防护动作”设置为“阻断”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据惩罚标准设置的拦截时长来封禁访问者。	长时间IP拦截
优先级	<p>设置该条件规则检测的顺序值。如果您设置了多条规则，则多条规则间有先后匹配顺序，即访问请求将根据您设定的精准访问控制规则优先级依次进行匹配，优先级较小的精准访问控制规则优先匹配。</p> <p>您可以通过优先级功能对所有精准访问控制规则进行排序，以获得最优的防护效果。</p> <p>须知 如果多条精准访问控制规则的优先级取值相同，则WAF将根据添加防护规则的先后顺序进行排序匹配。</p>	5
生效模式	<p>用户可以选择“立即生效”或者自定义设置生效时间段。</p> <p>自定义设置的时间只能为将来的某一时间段。</p>	“立即生效”

参数	参数说明	取值样例
阻断页面	<p>当“防护动作”选择“阻断”时，可配置返回的错误页面。</p> <ul style="list-style-type: none"> 当选择“默认设置”时，返回的错误页面为系统默认的阻断页面。 当选择“自定义”时，返回错误信息由用户自定义。 当选择“重定向”时，根据界面提示配置重定向URL。 	自定义
HTTP返回码	当“阻断页面”选择“自定义”时，支持配置HTTP返回码。	418
响应标头	<p>当“阻断页面”选择“自定义”时，支持配置响应标头。</p> <p>单击“添加响应标头字段”，配置响应标头参数及参数值。</p>	-
页面类型	当“阻断页面”选择“自定义”时，可选择阻断页面的类型“application/json”、“text/html”或者“text/xml”。	text/html
页面内容	当“阻断页面”选择“自定义”时，可设置自定义返回的内容。	<p>不同页面类型对应的页面内容样式：</p> <ul style="list-style-type: none"> text/html: <html><body>Forbidden</body></html> application/json: {"msg": "Forbidden"} text/xml: <?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error>

步骤10 单击确定，添加的精准访问防护规则展示在精准访问防护规则列表中。

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果需要修改添加的精准访问防护规则时，可单击待修改的精准访问防护规则所在行的“修改”，修改精准访问防护规则。
- 如果需要删除添加的精准访问防护规则时，可单击待删除的精准访问防护规则所在行的“删除”，删除精准访问防护规则。

----结束

防护效果

假如已添加域名“www.example.com”，且配置了如图5-13所示的精准访问防护规则。可参照以下步骤验证防护效果：

步骤1 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

- 不能正常访问，参照[网站设置](#)章节重新完成域名接入。
- 能正常访问，执行2。

步骤2 清理浏览器缓存，在浏览器中访问“http://www.example.com/admin”页面或者包含/admin的任意页面，正常情况下，WAF会阻断满足条件的访问请求，返回拦截页面。

步骤3 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志。

----结束

配置示例-拦截特定的攻击请求

通过分析某类特定的WordPress反弹攻击，发现其特征是User-Agent字段都包含WordPress，如图5-14所示。

图 5-14 WordPress 反弹攻击

UA
WordPress/4.2.10; http://[redacted].s.vn; verifying pingback from [redacted] 249.54
WordPress/4.0.1; http://[redacted]:90; verifying pingback from [redacted].249.54
WordPress/4.6.1; https://[redacted].sabt.com; verifying pingback from [redacted].249.54
WordPress/4.5.3; http://[redacted].lib.umd.edu; verifying pingback from [redacted].9.54
WordPress/3.5.1; http://[redacted].o.com
WordPress/4.2.4; http://[redacted].t.tw; verifying pingback from [redacted] 249.54
WordPress/4.6.1; http://[redacted].om; verifying pingback from [redacted].249.54

因此，可以设置精准访问控制规则，拦截该类WordPress反弹攻击请求。

图 5-15 User Agent 配置

添加精准访问防护规则 ×

规则描述(可选)

条件列表

字段	子字段	逻辑	内容	大小写敏感	操作
User Agent	-	包含	WordPress	<input type="checkbox"/>	删除

[+ 添加条件](#) 您还可以添加29项条件。(多个条件同时成立才生效) [添加引用表](#)

采取防护措施

防护动作 ⓘ
 阻断 放行 仅记录 JS挑战

阻断页面
 默认设置 自定义 重定向

攻击惩罚 ⓘ
无攻击惩罚 [设置攻击惩罚](#)

生效模式 ⓘ

优先级 ⓘ
 50
值越小, 优先级越高

配置示例-拦截特定的 URL 请求

如果您遇到有大量IP在访问某个特定且不存在的URL, 您可以通过配置以下精准访问防护规则直接阻断所有该类请求, 降低源站服务器的资源消耗, 如图5-16所示。

图 5-16 特定的 URL 拦截

The screenshot shows the 'Add precise access protection rule' configuration page. At the top, there is a text input field containing 'wafest'. Below it is an optional rule description field. The main section is 'Conditions List', which contains a table with columns: 'Field', 'Sub-field', 'Logic', 'Content', 'Case Sensitivity', and 'Action'. A single condition is added: 'Path' (Field), '-' (Sub-field), 'Contains' (Logic), 'hxxx' (Content), 'Off' (Case Sensitivity), and 'Delete' (Action). Below the table, there are options to '+ Add condition' and '+ Add reference table'. The 'Take protection measures' section includes: 'Protection action' with 'Block' selected; 'Block page' with 'Default settings' selected; 'Attack penalty' set to 'No attack penalty'; and 'Effective mode' set to 'Take effect immediately'. The 'Priority' is set to 50.

配置示例-拦截字段为空值的请求

如果您需要拦截某个为空值的字段，您可以通过配置精准访问防护规则直接阻断该类请求，如图5-17所示。

图 5-17 Referer 空值拦截

The screenshot shows the configuration page for a 'Referer empty value interception' rule. In the 'Conditions List' table, a condition is configured: 'Header' (Field), 'Custom' (Sub-field), 'referer' (Content), 'Does not exist' (Logic), and '-' (Action). Below the table, there are options to '+ Add condition' and '+ Add reference table'. The 'Deep detection' toggle is turned off. In the 'Take protection measures' section, 'Block' is selected as the protection action.

配置示例-拦截指定文件类型（zip、tar、docx 等）

通过配置路径字段匹配的文件类型，您可以阻断特定的文件类型。例如，您需要拦截“.zip”格式文件，您可以配置精准防护规则阻断“.zip”文件类型访问请求，如图5-18所示。

图 5-18 阻断特定文件类型请求

添加精准访问防护规则 ×

规则名称

规则描述(可选)

条件列表

字段	子字段	逻辑	内容	大小写敏感	操作
路径	-	后缀为	.zip	<input type="checkbox"/>	删除

[+ 添加条件](#) 您还可以添加29项条件。(多个条件同时成立才生效) [添加引用表](#)

深度检测 ?

采取防护措施

防护动作 ?
 阻断 放行 仅记录 JS挑战

阻断页面
 默认设置 自定义 重定向

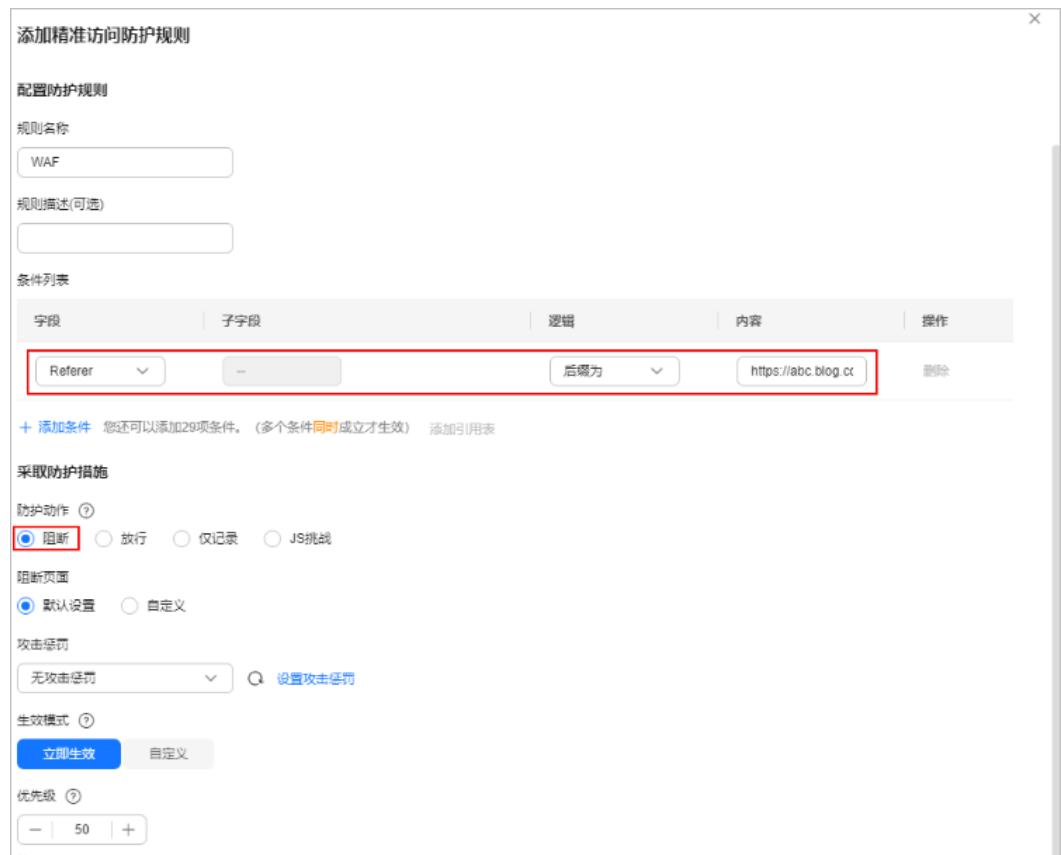
攻击惩罚 ?
 [设置攻击惩罚](#)

生效模式 ?

配置示例-防盗链

通过配置Referer匹配字段的访问控制规则，您可以阻断特定网站的盗链。例如，您发现“https://abc.blog.com”大量盗用本站的图片，您可以配置精准访问防护规则阻断相关访问请求。

图 5-19 防盗链



配置示例-单独放行指定 IP 的访问

配置两条精准访问防护规则，一条拦截所有的请求，如图5-20所示，一条单独放行指定IP的访问，如图5-21所示。

图 5-20 阻断所有的请求



图 5-21 放行指定 IP



配置示例-放行指定 IP 的特定 URL 请求

通过配置多条“条件列表”，当访问请求同时满足条件列表时，可以实现放行指定IP的特定URL请求，如图5-22所示。

图 5-22 放行指定 IP 访问特定路径



5.6 配置 IP 黑白名单规则拦截/放行指定 IP

IP地址默认全部放行，您可以通过配置黑白名单规则，阻断、仅记录或放行指定IP地址/IP地址段的访问请求，白名单规则优先级高于黑名单规则。配置黑白名单规则时，WAF支持单个添加或通过引用地址组批量导入黑白名单IP地址/IP地址段。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件

- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#) 章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。

约束条件

- 云模式入门版不支持该功能。
- 通过“云模式-ELB接入”方式添加网站时，ELB配置的监听器中使用的“前端协议”为TCP、UDP、QUIC时，使用该规则不生效。
- WAF支持批量导入黑白名单，如果您需要配置多个IP/IP地址段规则，请添加地址组，详细操作请参见[添加黑白名单IP地址组](#)。
- 云模式仅专业版和铂金版支持IPv6地址/IPv6地址段。
- 如果独享模式/云模式-ELB接入所在的ELB支持IPv6，独享模式/云模式-ELB接入也支持IPv6地址/IPv6地址段。
- WAF黑白名单规则支持配置0.0.0.0/0 和::/0 IP地址段，分别实现IPv4全流量拦截和IPv6全流量拦截。白名单规则优先级高于黑名单规则，如果您需要放行某个网段指定的IP并拦截某个网段其他所有IP，请先添加黑名单规则，拦截该网段的所有IP，然后添加白名单规则，放行指定IP。

须知

如果您需要拦截所有来源IP或仅允许指定IP访问防护网站，也可以请参见[拦截所有来源IP或仅允许指定IP访问防护网站，如何配置？](#)进行配置。

- 当黑白名单规则的“防护动作”设置为“拦截”时，您可以[配置攻击惩罚标准自动封禁访问者指定时长](#)，但攻击惩罚的“拦截类型”不支持选择“长时间IP拦截”和“短时间IP拦截”。配置攻击惩罚后，如果访问者的Cookie或Params恶意请求被拦截时，WAF将根据攻击惩罚设置的拦截时长来封禁访问者。

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

规格限制


- 云模式各版本、独享模式支持创建的IP黑白名单规则条数请参见[服务版本差异](#)。
- 如果您购买了云模式，当前版本的IP黑白名单防护规则条数不能满足要求时，您可以通过购买规则扩展包或升级云模式版本增加IP黑白名单防护规则条数，以满足的防护配置需求。
一个规则扩展包包含10条IP黑白名单防护规则。有关升级规则的详细操作，请参见[升级WAF云模式版本和规格](#)。


系统影响

将IP或IP地址段配置为黑名单/白名单后，来自该IP或IP地址段的访问，WAF将不会做任何检测，直接拦截/放行。

配置 IP 黑白名单规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“黑白名单设置”配置框，用户可根据自己的需要开启或关闭黑白名单策略。

- ：开启状态。
- ：关闭状态。

步骤7 在“黑白名单设置”配置列表的左上方，单击“添加规则”。

步骤8 在弹出的对话框中，添加黑白名单规则，如[图5-23](#)和[图5-24](#)所示，参数说明如[表5-8](#)所示。

说明

- 将IP配置为仅记录后，来自该IP的访问，WAF将根据防护规则进行检测并记录该IP的防护事件数据。
- 其他的IP将根据配置的WAF防护规则进行检测。

图 5-23 添加单个 IP/IP 地址段黑白名单规则

The dialog box is titled "添加黑白名单设置规则" (Add Whitelist Rule) and contains the following fields and options:

- 规则名称** (Rule Name): Input field with "wafest".
- IP/IP段或地址组** (IP/Segment or Address Group): Radio buttons for "IP/IP段" (selected) and "地址组" (Address Group).
- IP/IP段** (IP/Segment): Input field.
- 防护动作** (Protection Action): Dropdown menu with "拦截" (Intercept).
- 攻击惩罚** (Attack Penalty): Dropdown menu with "无攻击惩罚" (No Attack Penalty) and a "添加攻击惩罚" (Add Attack Penalty) link.
- 生效模式** (Effective Mode): Radio buttons for "立即生效" (Immediate Effect) (selected) and "自定义" (Custom).
- 规则描述** (Rule Description): Input field.
- Buttons: "确定" (Confirm) and "取消" (Cancel).

图 5-24 批量添加 IP/IP 地址段黑白名单规则

The dialog box is titled "添加黑白名单设置规则" (Add Whitelist Rule) and contains the following fields and options:

- 规则名称** (Rule Name): Input field with "wafest".
- IP/IP段或地址组** (IP/Segment or Address Group): Radio buttons for "IP/IP段" and "地址组" (selected).
- 选择地址组** (Select Address Group): Dropdown menu with "test_170_ip" and a "添加地址组" (Add Address Group) link. A warning message below reads: "如果您所选择的地址组IP数量超出您所剩余黑白名单规则配额, 则无法进行引用" (If the number of IP addresses in the selected address group exceeds the remaining quota of the whitelist/blacklist rule, it cannot be referenced).
- 防护动作** (Protection Action): Dropdown menu with "拦截" (Intercept).
- 攻击惩罚** (Attack Penalty): Dropdown menu with "无攻击惩罚" (No Attack Penalty) and a "添加攻击惩罚" (Add Attack Penalty) link.
- 生效模式** (Effective Mode): Radio buttons for "立即生效" (Immediate Effect) (selected) and "自定义" (Custom).
- 规则描述** (Rule Description): Input field.
- Buttons: "确定" (Confirm) and "取消" (Cancel).

表 5-8 黑白名单参数说明

参数	参数说明	取值样例
规则名称	用户自定义黑白名单规则的名字。	wafest

参数	参数说明	取值样例
IP/IP段或地址组	支持添加黑白名单规则的方式，“IP/IP段”或“地址组”。	IP/IP段
IP/IP段	<p>当“IP/IP段或地址组”选择“IP/IP段”时需要设置该参数。</p> <p>支持IPv4和IPv6格式的IP地址或IP地址段。</p> <ul style="list-style-type: none"> IP地址：添加黑名单或者白名单的IP地址。 IP地址段：IP地址与子网掩码。 <p>须知 仅专业版和铂金版支持IPv6防护。</p>	<ul style="list-style-type: none"> IPv4格式： <ul style="list-style-type: none"> 192.168.2.3 10.1.1.0/24 IPv6格式： <ul style="list-style-type: none"> fe80:0000:0000:0000:0000:0000:0000:0000 ::/0
选择地址组	当“IP/IP段或地址组”选择“地址组”时需要设置该参数，在下拉列表框中选择已添加的地址组。您也可以单击“添加地址组”创建新的地址组，详细操作请参见 添加黑白名单IP地址组 。	groupwaf
防护动作	<ul style="list-style-type: none"> 拦截：IP地址或IP地址段设置的是黑名单且需要拦截，则选择“拦截”。 放行：IP地址或IP地址段设置的是白名单，则选择“放行”。 仅记录：需要观察的IP地址或IP地址段，可选择“仅记录”。再根据防护事件数据判断该IP地址或IP地址段是黑名单还是白名单。 	拦截
攻击惩罚	<p>当“防护动作”设置为“拦截”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的Cookie或Params恶意请求被拦截时，WAF将根据惩罚标准设置的拦截时长来封禁访问者。</p> <p>说明 不支持选择“长时间IP拦截”和“短时间IP拦截”。</p>	长时间Cookie拦截
规则描述	可选参数，设置该规则的备注信息。	--

参数	参数说明	取值样例
生效时间	可选择“立即生效”或自定义生效时间段。 当超过设置的生效结束时间后，该规则的“规则状态”为“已开启（未生效）”，您可以修改生效时间使规则重新生效或者删除该未生效规则。	立即生效

步骤9 输入完成后，单击“确定”，添加的黑白名单展示在黑白名单规则列表中。

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果需要修改添加的黑白名单规则时，可单击待修改的黑白名单IP规则所在行的“修改”，修改黑白名单规则。
- 如果需要删除添加的黑白名单规则时，可单击待删除的黑白名单IP规则所在行的“删除”，删除黑白名单规则。

---结束

防护效果

假如已添加域名“www.example.com”。可参照以下步骤验证防护效果：

步骤1 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

- 不能正常访问，参照[网站设置](#)章节重新完成域名接入。
- 能正常访问，执行**2**。

步骤2 参照[配置IP黑白名单规则](#)，将您的客户端IP配置为黑名单。

步骤3 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面，正常情况下，WAF会阻断该IP的访问请求，返回拦截页面。

步骤4 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志。

---结束

配置示例-放行指定 IP

假如防护域名“www.example.com”已接入WAF，您可以参照以下操作步骤验证放行指定IP防护效果。

步骤1 添规则拦截所有来源IP。

- **方法一**：添加以下2条黑名单规则，拦截所有来源IP，如[图5-25](#)和[图5-26](#)所示。

图 5-25 拦截 1.0.0.0/1 IP 地址段

The screenshot shows a dialog box titled "添加黑白名单设置规则" (Add Whitelist Rule) with a close button (X) in the top right corner. The form contains the following fields and options:

- 规则名称** (Rule Name): Input field containing "all01".
- IP/IP段或地址组** (IP/IP Range or Address Group): Radio buttons for "IP/IP段" (selected) and "地址组" (Address Group).
- IP/IP段** (IP/IP Range): Input field containing "1.0.0.0/1".
- 防护动作** (Protection Action): Dropdown menu set to "拦截" (Block).
- 攻击惩罚** (Attack Penalty): Dropdown menu set to "无攻击惩罚" (No Attack Penalty), with a link "添加攻击惩罚" (Add Attack Penalty) to the right.
- 生效模式** (Effective Mode): Radio buttons for "立即生效" (Take Effect Immediately, selected) and "自定义" (Custom).
- 规则描述** (Rule Description): Empty text area.

At the bottom right, there are two buttons: "确定" (Confirm) and "取消" (Cancel).

图 5-26 拦截 128.0.0.0/1 IP 地址段

The screenshot shows a dialog box titled "添加黑白名单设置规则" (Add Whitelist Rule) with a close button (X) in the top right corner. The form contains the following fields and options:

- 规则名称** (Rule Name): Input field containing "all01".
- IP/IP段或地址组** (IP/IP Range or Address Group): Radio buttons for "IP/IP段" (selected) and "地址组" (Address Group).
- IP/IP段** (IP/IP Range): Input field containing "128.0.0.0/1".
- 防护动作** (Protection Action): Dropdown menu set to "拦截" (Block).
- 攻击惩罚** (Attack Penalty): Dropdown menu set to "无攻击惩罚" (No Attack Penalty), with a link "添加攻击惩罚" (Add Attack Penalty) to the right.
- 生效模式** (Effective Mode): Radio buttons for "立即生效" (Take Effect Immediately, selected) and "自定义" (Custom).
- 规则描述** (Rule Description): Empty text area.

At the bottom right, there are two buttons: "确定" (Confirm) and "取消" (Cancel).

- **方法二**：添加一条精准访问防护规则，拦截所有访问请求，如图5-27所示。

图 5-27 拦截所有访问请求

添加精准访问防护规则

本规则生效后，请关注业务情况，如有异常，可以删除本规则。

配置防护规则

规则名称
WAF

规则描述(可选)

条件列表

字段	子字段	逻辑	内容	大小写敏感	操作
路径	-	包含	/	<input type="checkbox"/>	删除

+ 添加条件 您还可以添加29项条件。(多个条件同时成立才生效) 添加引用表

深度检测

采取防护措施

防护动作 阻断 放行 仅记录 JS挑战

阻断页面 默认设置 自定义 重定向

- 方法三：添加0.0.0.0/0 和::/0 IP地址段，可实现IPv4全流量拦截和IPv6全流量拦截。

图 5-28 IPv4 全流量拦截

添加黑白名单设置规则

* 规则名称 wafitest

* IP/IP段或地址组 IP/IP段 地址组

* IP/IP段 0.0.0.0/0

* 防护动作 拦截

攻击惩罚 无攻击惩罚 添加攻击惩罚

* 生效模式 立即生效 自定义

规则描述

确定 取消

图 5-29 IPv6 全流量拦截



The screenshot shows a dialog box titled "添加黑白名单设置规则" (Add Black and White List Rule) with a close button (X) in the top right corner. The form contains the following fields and options:

- * 规则名称** (Rule Name): Input field containing "waftest".
- * IP/IP段或地址组** (IP/IP Range or Address Group): Radio buttons for "IP/IP段" (selected) and "地址组" (Address Group).
- * IP/IP段** (IP/IP Range): Input field containing "::/0".
- * 防护动作** (Protection Action): Dropdown menu showing "拦截" (Intercept).
- 攻击惩罚** (Attack Penalty): Dropdown menu showing "无攻击惩罚" (No Attack Penalty), with a link "添加攻击惩罚" (Add Attack Penalty) to the right.
- * 生效模式** (Effective Mode): Radio buttons for "立即生效" (Immediate Effect) (selected) and "自定义" (Custom).
- 规则描述** (Rule Description): Empty input field.
- Buttons: "确定" (Confirm) and "取消" (Cancel) at the bottom right.

步骤2 参照图5-30示例添加黑白名单规则，放行指定IP，例如，192.168.2.3。

图 5-30 放行指定 IP



The screenshot shows a dialog box titled "添加黑白名单设置规则" (Add Black and White List Rule) with a close button (X) in the top right corner. The form contains the following fields and options:

- * 规则名称** (Rule Name): Input field containing "all01".
- * IP/IP段或地址组** (IP/IP Range or Address Group): Radio buttons for "IP/IP段" (selected) and "地址组" (Address Group).
- * IP/IP段** (IP/IP Range): Input field containing "192.168.2.3".
- * 防护动作** (Protection Action): Dropdown menu showing "放行" (Allow).
- * 生效模式** (Effective Mode): Radio buttons for "立即生效" (Immediate Effect) (selected) and "自定义" (Custom).
- 规则描述** (Rule Description): Empty input field.
- Buttons: "确定" (Confirm) and "取消" (Cancel) at the bottom right.

步骤3 开启黑白名单防护规则。

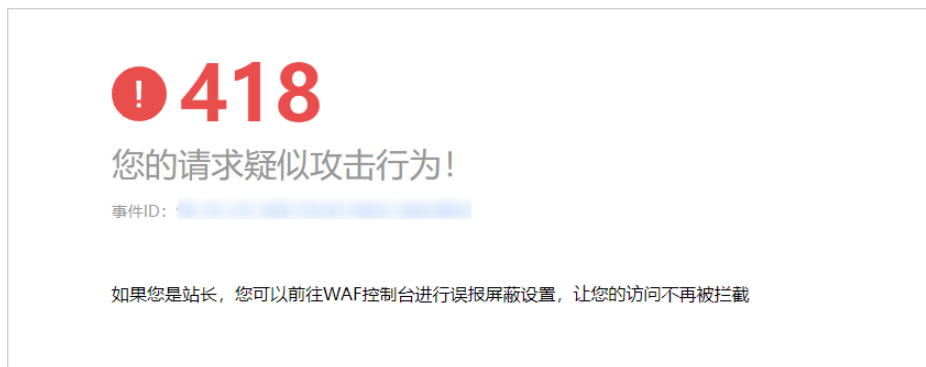
图 5-31 黑白名单配置框



步骤4 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当访问者的源IP不属于**步骤2**中设置的放行IP地址时，WAF将拦截该访问请求，拦截页面示例如图5-32所示。

图 5-32 WAF 拦截攻击请求



步骤5 返回Web应用防火墙管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

5.7 配置地理位置访问控制规则拦截/放行特定区域请求

网站接入Web应用防火墙后，您可以设置地理位置访问控制规则，WAF通过识别客户端访问请求的来源区域，一键封禁来自特定区域的访问或者允许特定区域的来源IP的访问，解决部分地区高发的恶意请求问题。可针对指定国家、地区的来源IP自定义访问控制。

如果您仅允许某一地区的来源IP访问防护网站，请参见[配置示例-仅允许某一地区来源IP访问请求](#)进行配置。

📖 说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件


- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#) 章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。


约束条件

- 云模式入门版和标准版不支持该功能。
- 如果您使用的独享模式，需要[将独享引擎实例版本升级到最新版本](#)，“IP范围”配置为IPv6，才会生效。
- 通过“云模式-ELB接入”方式添加网站时，ELB配置的监听器中使用的“前端协议”为TCP、UDP、QUIC时，使用该规则不生效。
- 同一个地区只能配置到一条地理位置访问控制规则中。例如，如果某个地理位置访问控制规则已设置了“上海”地区，那么“上海”地区不能再添加到其他地理位置访问控制规则。
- 添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

配置地理位置访问防护规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“地理位置访问控制”配置框，用户可根据自己的需要开启或关闭地理位置访问控制防护策略。

- ：开启状态。
- ：关闭状态。

步骤7 在“地理位置访问控制”配置列表的左上方，单击“添加规则”。

步骤8 在弹出的对话框中，添加地理位置访问控制规则，如图5-33所示，根据表5-9配置参数。

图 5-33 添加地理位置访问控制规则

表 5-9 添加地理位置访问控制规则参数说明

参数	参数说明	取值样例
规则名称	用户自定义地理位置控制规则的名字。	-
规则描述	可选参数，设置该规则的备注信息。	waf
地理位置	IP访问的地理范围，可以选择“中国境内”和“中国境外”地区。	-

参数	参数说明	取值样例
IP范围	<ul style="list-style-type: none"> IPv4 IPv6 任意（IPv4和IPv6） <p>说明 如果您使用的独享模式，需要将独享引擎实例版本升级到最新版本，选择IPv6，配置才会生效。</p>	IPv4
防护动作	可以根据需要选择“拦截”、“放行”或者“仅记录”。	“拦截”

步骤9 单击“确定”，添加的地理位置访问控制规则展示在地理位置访问控制规则列表中。

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果需要修改添加的地理位置访问控制规则时，可单击待修改的地理位置访问控制规则所在行的“修改”，修改地理位置访问控制规则。
- 如果需要删除添加的地理位置访问控制规则时，可单击待删除的地理位置访问控制规则所在行的“删除”，删除地理位置访问控制规则。

----结束

配置示例-仅允许某一地区来源 IP 访问请求

假如防护域名“www.example.com”已接入WAF，当您只允许某一地区的IP可以访问防护域名，例如，只允许来源“上海”地区的IP可以访问防护域名，请参照以下步骤处理。

步骤1 添加一条地理位置访问控制规则，添加“上海”地区的“放行”防护动作。

图 5-34 添加“放行”防护动作

添加地理位置访问控制规则

* 规则名称

规则描述

* 地理位置

中国境内 (1) 全选

<input type="checkbox"/> 北京	<input checked="" type="checkbox"/> 上海	<input type="checkbox"/> 天津	<input type="checkbox"/> 重庆
<input type="checkbox"/> 广东	<input type="checkbox"/> 浙江	<input type="checkbox"/> 江苏	<input type="checkbox"/> 安徽
<input type="checkbox"/> 福建	<input type="checkbox"/> 甘肃	<input type="checkbox"/> 广西	<input type="checkbox"/> 贵州
<input type="checkbox"/> 河南	<input type="checkbox"/> 湖北	<input type="checkbox"/> 河北	<input type="checkbox"/> 海南
<input type="checkbox"/> 香港	<input type="checkbox"/> 黑龙江	<input type="checkbox"/> 湖南	<input type="checkbox"/> 吉林
<input type="checkbox"/> 江西	<input type="checkbox"/> 辽宁	<input type="checkbox"/> 澳门	<input type="checkbox"/> 内蒙古
<input type="checkbox"/> 宁夏	<input type="checkbox"/> 青海	<input type="checkbox"/> 四川	<input type="checkbox"/> 山东
<input type="checkbox"/> 陕西	<input type="checkbox"/> 山西	<input type="checkbox"/> 台湾	<input type="checkbox"/> 新疆
<input type="checkbox"/> 西藏	<input type="checkbox"/> 云南		

中国境外 (0)

* IP范围 IPv4 IPv6 任意

* 防护动作

步骤2 开启地理位置访问控制。

图 5-35 地理位置访问控制配置框



步骤3 配置一条精准访问防护规则，拦截所有的请求。

图 5-36 拦截所有访问请求

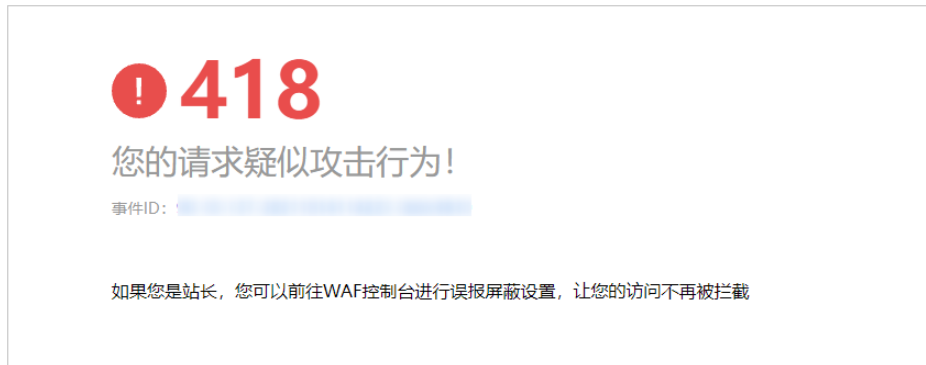


有关配置精准访问防护规则的详细介绍，请参见[配置精准访问防护规则定制化防护策略](#)。

步骤4 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当非“上海”地区的源IP访问页面时，WAF将拦截该访问请求，拦截页面示例如图5-37所示。

图 5-37 WAF 拦截攻击请求



步骤5 返回Web应用防火墙管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看到非“上海”地区的源IP都被拦截。

----结束

配置示例-拦截某一地区来源 IP 访问请求

假如防护域名“www.example.com”已接入WAF，您需要拦截所有来源“北京”地区的IP访问防护域名，可以参照以下操作步骤验证防护效果。

步骤1 添加一条地理位置访问控制规则，设置“北京”地区“拦截”动作。

图 5-38 拦截某一地区访问请求

添加地理位置访问控制规则

* 规则名称

规则描述

* 地理位置

中国境内 (1) 全选

<input checked="" type="checkbox"/> 北京	<input type="checkbox"/> 上海	<input type="checkbox"/> 天津	<input type="checkbox"/> 重庆
<input type="checkbox"/> 广东	<input type="checkbox"/> 浙江	<input type="checkbox"/> 江苏	<input type="checkbox"/> 安徽
<input type="checkbox"/> 福建	<input type="checkbox"/> 甘肃	<input type="checkbox"/> 广西	<input type="checkbox"/> 贵州
<input type="checkbox"/> 河南	<input type="checkbox"/> 湖北	<input type="checkbox"/> 河北	<input type="checkbox"/> 海南
<input type="checkbox"/> 香港	<input type="checkbox"/> 黑龙江	<input type="checkbox"/> 湖南	<input type="checkbox"/> 吉林
<input type="checkbox"/> 江西	<input type="checkbox"/> 辽宁	<input type="checkbox"/> 澳门	<input type="checkbox"/> 内蒙古
<input type="checkbox"/> 宁夏	<input type="checkbox"/> 青海	<input type="checkbox"/> 四川	<input type="checkbox"/> 山东
<input type="checkbox"/> 陕西	<input type="checkbox"/> 山西	<input type="checkbox"/> 台湾	<input type="checkbox"/> 新疆
<input type="checkbox"/> 西藏	<input type="checkbox"/> 云南		

中国境外 (0)

* IP范围 IPv4 IPv6 任意

* 防护动作

步骤2 开启地理位置访问控制。

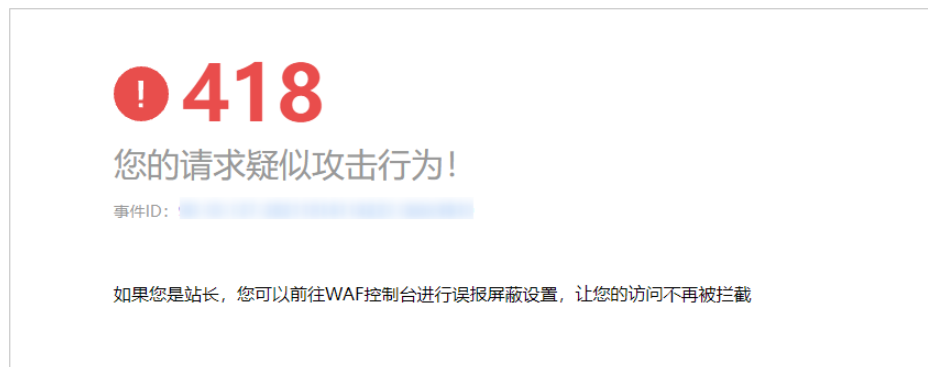
图 5-39 地理位置访问控制配置框



步骤3 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当“北京”地区的源IP访问页面时，WAF将拦截该访问请求，拦截页面示例如图5-40所示。

图 5-40 WAF 拦截攻击请求



步骤4 返回Web应用防火墙管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

图 5-41 查看防护事件-拦截某一地区 IP 访问请求

时间	源IP	地理位置	防护域名	URL	恶意负载	事件类型	防护动作	操作
2021/11/19 15:24:37 GMT...	...	北京	www.example.com	/		地理位置控制	拦截	详情 误报处理
2021/11/19 15:24:37 GMT...	...	北京	www.example.com	/		地理位置控制	拦截	详情 误报处理
2021/11/19 01:13:22 GMT...	...	北京	www.example.com	/		地理位置控制	拦截	详情 误报处理
2021/11/19 00:19:23 GMT...	...	北京	www.example.com	/		地理位置控制	拦截	详情 误报处理
2021/11/19 00:19:22 GMT...	...	北京	www.example.com	/		地理位置控制	拦截	详情 误报处理

----结束

防护效果

假如已添加域名“www.example.com”。可参照以下步骤验证防护效果：

- 步骤1** 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。
 - 不能正常访问，参照[网站设置](#)章节重新完成域名接入。
 - 能正常访问，执行**2**。
- 步骤2** 参照[配置地理位置访问防护规则](#)，将您的客户端IP来源地配置为拦截。
- 步骤3** 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面，正常情况下，WAF会阻断该来源地IP的访问请求，返回拦截页面。
- 步骤4** 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志。

----结束

5.8 配置威胁情报访问控制规则拦截/放行指定 IP 库的 IP

基于互联网数据中心(Internet Data Center, 简称IDC)机房的IP库进行访问控制，可选的IP库平台，包括：鹏博士、谷歌公司、腾讯、美团网等其他平台。配置后，当目标IP库平台内的来源IP向域名下任意路径发起访问请求时，将触发控制规则，即拦截、放行或者仅记录请求。

前提条件


- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#)章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。


约束条件

- “云模式”仅专业版和铂金版支持威胁情报访问控制规则。
- 独享模式仅2022年9月及之后的版本支持配置威胁情报访问控制规则，独享引擎版本详情请参见[独享引擎版本迭代](#)。
- ELB模式不支持配置威胁情报访问控制规则。

配置威胁情报访问控制规则

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“威胁情报访问控制”配置框，用户可根据自己的需要开启或关闭威胁情报访问控制防护策略。

- ：开启状态。
- ：关闭状态。

步骤7 在规则列表的左上方，单击“添加规则”。

步骤8 在弹出的对话框中，添加威胁情报访问控制规则，参数说明如表5-10所示。

图 5-42 添加威胁情报访问控制规则



表 5-10 参数说明

参数	参数说明	取值样例
规则名称	自定义规则名称	WAFtest
规则描述	可选参数，设置该规则的备注信息。	--

参数	参数说明	取值样例
信息类型	在下拉框中选择“IDC数据中心”，并勾选IDC机房的IP库平台。 可勾选IDC机房的IP库平台，包括：鹏博士、谷歌公司、腾讯、美团网等其他平台。	IDC数据中心 华为
防护动作	可以根据需要选择“拦截”、“放行”或者“仅记录”。 <ul style="list-style-type: none">拦截：表示拦截命中规则的请求，并向发起请求的客户端返回拦截响应页面。WAF默认使用统一的拦截响应页面，您也可以自定义拦截响应页面。放行：表示不拦截命中规则的请求，直接放行。仅记录：表示不拦截命中规则请求，只通过日志记录请求命中了规则。	放行

步骤9 单击“确定”，添加的威胁情报访问控制规则将展示在规则列表中。

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果需要修改添加的威胁情报访问控制规则时，可单击待修改的威胁情报访问控制规则所在行的“修改”。
- 如果需要删除用户自行添加的威胁情报访问控制规则时，可单击待删除的威胁情报访问控制规则所在行的“删除”。

----结束

5.9 配置网页防篡改规则避免静态网页被篡改

网站接入WAF后，您可以通过设置网页防篡改规则，锁定需要保护的网站页面（例如敏感页面）。当被锁定的页面在收到请求时，返回已设置的缓存页面，预防源站页面内容被恶意篡改。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为该企业项目下域名配置防护策略。

工作原理

- 当WAF接收到正常的访问请求时，直接将缓存的网页返回给Web访问者，加速请求响应。
- 如果攻击者篡改了网站的静态网页，WAF将缓存的未被篡改的网页返回给Web访问者，保证Web访问者访问的是正确的页面。

- WAF将对页面路径下的所有相关资源进行防护。例如，对“www.example.com/index.html”静态页面配置了网页防篡改规则，则WAF将防护“/index.html”的网页以及这个网页关联的相关资源。
即如果请求中Referer请求头的值中的URL路径与您配置的防篡改路径一致，如“/index.html”，则该请求命中的资源（结尾为png、jpg、jpeg、gif、bmp、css、js的所有资源）也会同时被缓存下来。
- 同时，WAF支持缓存自定义的Header字段。在网页防篡改页面上方，单击“修改字段”可配置需要通过WAF缓存的Header字段。

前提条件

已添加防护网站或已[新增防护策略](#)。

- 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
- 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#)章节。

约束条件

- 云模式的入门版和云模式-ELB接入不支持该防护规则。
- 添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 请确保源站响应中包括Content-Type响应头，否则可能导致WAF无法缓存源站响应。


应用场景

- 加速请求的响应
配置网页防篡改规则后，Web应用防火墙将对服务端的静态网页进行缓存。当Web应用防火墙接收到Web访问者的请求时，直接将缓存的网页返回给Web访问者。
- 网页防篡改
攻击者将服务端的静态网页篡改后，Web应用防火墙将缓存的未被篡改的网页返回给Web访问者，以保证Web访问者访问的是正确的页面。
Web应用防火墙具有如下功能：随机抽取Web访问者的一个请求，将请求的页面与服务端页面进行对比，如果发现页面被篡改，您将接收到告警通知（通知方式由您设置），告警通知的设置请参考[开启告警通知](#)。

配置网页防篡改规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“网页防篡改”配置框，用户可根据自己的需要开启或关闭网页防篡改策略。

-  : 开启状态。
-  : 关闭状态。

步骤7 在“网页防篡改”规则配置列表的左上方，单击“添加规则”。

步骤8 在弹出的对话框中，添加网页防篡改规则，参数说明如表5-11所示。

图 5-43 添加网页防篡改规则



表 5-11 参数说明

参数	参数说明	取值样例
域名	设置防篡改的域名。	www.example.com
路径	<p>设置防篡改的URL链接中的路径（不包含域名）。</p> <p>URL用来定义网页的地址。基本的URL格式如下： 协议名://域名或IP地址[:端口号]/[路径名/.../文件名]。</p> <p>例如，URL为“http://www.example.com/admin”，则“路径”设置为“/admin”。</p> <p>说明</p> <ul style="list-style-type: none"> • 该路径不支持正则。 • 路径里不能含有连续的多条斜线的配置，如“///admin”，WAF引擎会将“///”转为“/”。 	/admin
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确定”，添加的网页防篡改规则展示在网页防篡改规则列表中。

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果被防护页面进行了内容修改，必须单击待更新的网页防篡改规则所在行的“更新缓存”来更新缓存，如果您在页面更新后未更新缓存，WAF将始终返回最近一次缓存的页面内容。
- 如果需要删除添加的网页防篡改规则时，可单击待删除的网页防篡改规则所在行的“删除”，删除网页防篡改规则。

配置示例-静态页面防篡改

假如防护域名“www.example.com”已接入WAF，需要防止“/admin”静态页面被篡改，您可以参照以下操作步骤验证防护效果。

步骤1 添加一条网页防篡改规则。

图 5-44 添加网页防篡改规则



添加网页防篡改规则 ✕

* 域名

* 路径

规则描述

确定

步骤2 开启网页防篡改。

图 5-45 网页防篡改配置框



步骤3 模拟篡改“http://www.example.com/admin”网页。

步骤4 在浏览器中访问“http://www.example.com/admin”，等待WAF缓存静态页面。

步骤5 在浏览器中访问篡改后的页面。

此时，显示的是被篡改前的页面。

----结束

5.10 配置网站反爬虫防护规则防御爬虫攻击

您可以通过配置网站反爬虫防护规则，防护搜索引擎、扫描器、脚本工具、其它爬虫等爬虫，以及自定义JS脚本反爬虫防护规则。

📖 说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件

- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#) 章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。

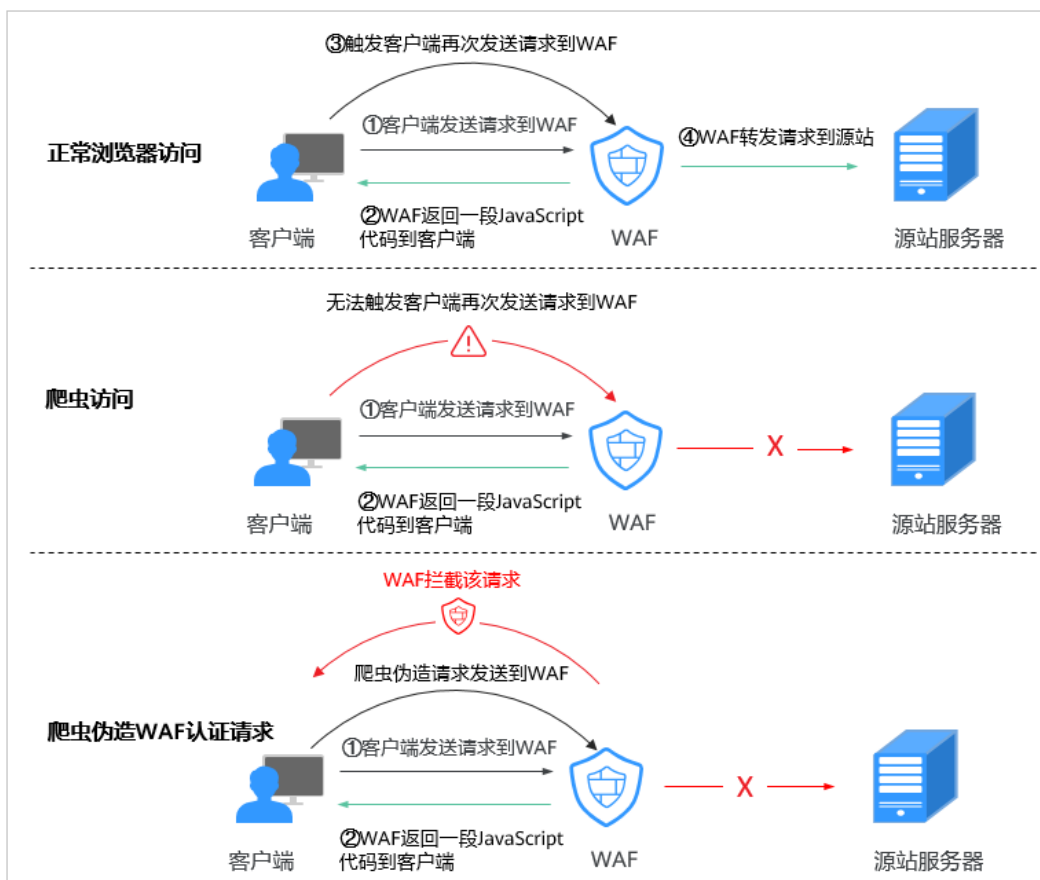
约束条件

- JS脚本反爬虫依赖浏览器的Cookie机制、JavaScript解析能力，如果客户端浏览器不支持Cookie，此功能无法使用，开启后会造成长久无法访问源站。
- 如果您的业务接入了CDN服务，请谨慎使用JS脚本反爬虫。
由于CDN缓存机制的影响，JS脚本反爬虫特性将无法达到预期效果，并且有可能造成页面访问异常。
- 云模式入门版和标准版本不支持该功能。
- 防护网站部署模式为“云模式-ELB接入”时，不支持JS脚本反爬虫功能。
- 开启JS脚本反爬虫后，如果不能查看拦截记录，请参见[开启JS脚本反爬虫后，为什么有些请求被WAF拦截但查不到拦截记录？](#)。
- 网站反爬虫“js挑战”的防护动作为“仅记录”，“js验证”的防护动作为人机验证（即js验证失败后，弹出验证码提示，输入正确的验证码，请求将不受访问限制）。
- WAF的JS脚本反爬虫功能只支持get请求，不支持post请求。

JS 脚本反爬虫检测机制

JS脚本检测流程如[图5-46](#)所示，其中，①和②称为“js挑战”，③称为“js验证”。

图 5-46 JS 脚本检测流程说明



开启JS脚本反爬虫后，当客户端发送请求时，WAF会返回一段JavaScript代码到客户端。

- 如果客户端是正常浏览器访问，就可以触发这段JavaScript代码再发送一次请求到WAF，即WAF完成js验证，并将该请求转发给源站。
- 如果客户端是爬虫访问，就无法触发这段JavaScript代码再发送一次请求到WAF，即WAF无法完成js验证。
- 如果客户端爬虫伪造了WAF的认证请求，发送到WAF时，WAF将拦截该请求，js验证失败。

通过统计“js挑战”和“js验证”，就可以汇总出JS脚本反爬虫防御的请求次数。例如，图5-47中JS脚本反爬虫共记录了18次事件，其中，“js挑战”（WAF返回JS代码）为16次，“js验证”（WAF完成JS验证）为2次，“其他”（即爬虫伪造WAF认证请求）为0次。

图 5-47 JS 脚本反爬虫防护数据





须知

网站反爬虫“js挑战”的防护动作为“仅记录”，“js验证”的防护动作为人机验证（即js验证失败后，弹出验证码提示，输入正确的验证码，请求将不受访问限制）。

配置网站反爬虫防护规则

步骤1 登录管理控制台。


步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“网站反爬虫”配置框，用户可根据自己的需要开启或关闭网站反爬虫策略。

- ：开启状态。
- ：关闭状态。

步骤7 选择“特征反爬虫”页签，根据您的业务场景，开启合适的防护功能，如图5-48所示，检测项说明如表5-12所示。

特征反爬虫规则提供了两种防护动作：

- 拦截
发现攻击行为后立即阻断并记录。

注意

开启拦截后，可能会有以下影响：

- 拦截搜索引擎请求，可能影响网站的搜索引擎优化。
- 拦截脚本工具，可能会影响部分APP访问（部分APP的User-Agent未做修改，会匹配脚本工具类爬虫规则）。

• 仅记录

默认防护动作，发现攻击行为后只记录不阻断攻击。

默认开启“扫描器”防护检测，用户可根据业务需要，配置防护动作并开启其他需要防护的检测类型。

图 5-48 特征反爬虫防护

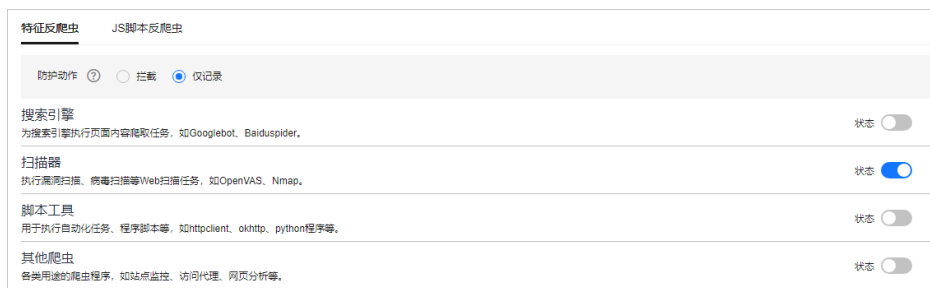




表 5-12 特征反爬虫检测项说明

检测项	说明	功能说明
搜索引擎	搜索引擎执行页面内容爬取任务，如Googlebot、Baiduspider。	开启后，WAF将检测并阻断搜索引擎爬虫。 说明 如果不开启“搜索引擎”，WAF针对谷歌和百度爬虫不会拦截，如果您希望拦截百度爬虫的POST请求，可参照 配置示例-搜索引擎 进行配置。
扫描器	执行漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap。	开启后，WAF将检测并阻断扫描器爬虫。
脚本工具	用于执行自动化任务、程序脚本等，如httpclient、okhttp、python程序等。	开启后，WAF将检测并阻断执行自动化任务、程序脚本等。 说明 如果您的应用程序中使用了httpclient、okhttp、python程序等脚本工具，建议您关闭“脚本工具”，否则，WAF会将使用了httpclient、okhttp、python程序等脚本工具当成恶意爬虫，拦截该应用程序。

检测项	说明	功能说明
其他爬虫	<p>各类用途的爬虫程序，如站点监控、访问代理、网页分析等。</p> <p>说明 “访问代理”是指当网站接入WAF后，为避免爬虫被WAF拦截，爬虫者使用大量IP代理实现爬虫的一种技术手段。</p>	开启后，WAF将检测并阻断各类用途的爬虫程序。

步骤8 选择“JS脚本反爬虫”页签，用户可根据业务需求更改JS脚本反爬虫的“状态”。

默认关闭JS脚本反爬虫，单击 ，在弹出的“警告”提示框中，单击“确定”，开启JS脚本反爬虫 。

防护动作：拦截、仅记录、人机验证（JavaScript挑战失败，弹出验证码提示，输入正确的验证码，请求将不受访问限制）。

须知

- JS脚本反爬虫依赖浏览器的Cookie机制、JavaScript解析能力，如果客户端浏览器不支持Cookie，此功能无法使用，开启后会造成永远无法访问源站。
- 如果您的业务接入了CDN服务，请谨慎使用JS脚本反爬虫。
由于CDN缓存机制的影响，JS脚本反爬虫特性将无法达到预期效果，并且有可能造成页面访问异常。

步骤9 根据业务配置JS脚本反爬虫规则，相关参数说明如表5-13所示。

JS脚本反爬虫规则提供了“防护所有请求”和“防护指定请求”两种防护动作。

- 除了指定请求规则以外，防护其他所有请求
“防护模式”选择“防护所有请求”，单击“添加排除请求规则”，配置排除请求规则后，单击“确定”。

图 5-49 添加排除防护请求



添加排除请求规则

不同模式使用限制和注意事项 ⓘ

下面条件同时满足，此规则生效。一条规则最多支持30个条件。

* 规则名称

规则描述

* 条件列表

字段	子字段	逻辑	内容	大小写敏感
路径	--	包含	<input type="text"/>	<input checked="" type="checkbox"/>

⊕ 添加 您还可以添加29项条件。(多个条件同时成立才生效)

* 生效模式 立即生效

* 优先级 值越小，优先级越高

确定 取消

- 只防护指定请求时
“防护模式”选择“防护指定请求”，单击“添加请求规则”，配置请求规则后，单击“确定”。

图 5-50 添加请求规则

表 5-13 JS 脚本反爬虫参数说明

参数	参数说明	示例
规则名称	自定义规则名称。	waf
规则描述	可选参数，设置该规则的备注信息。	-
生效时间	立即生效。	立即生效

参数	参数说明	示例
条件列表	<p>条件设置参数说明如下：</p> <ul style="list-style-type: none">• 字段：在下拉列表中选择需要防护的字段，当前仅支持“路径”、“User Agent”。• 子字段• 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 <p>说明 当“逻辑”关系选择“包含任意一个”、“不包含任意一个”、“等于任意一个”、“不等于任意一个”、“前缀为任意一个”、“前缀不为任意一个”、“后缀为任意一个”或者“后缀不为任意一个”时，需要选择引用表。</p> <ul style="list-style-type: none">• 内容：输入或者选择条件匹配的内容。• 大小写敏感：“字段”选择“路径”时，可配置该参数。开启后，系统在检测配置的路径时，将区分大小写。能够帮助系统更准确地识别和处理各种爬虫请求，从而有效提升反爬虫策略的精确度和有效性。	“路径”包含“/admin/”
优先级	设置该条件规则检测的顺序值。如果您设置了多条规则，则多条规则间有先后匹配顺序，即访问请求将根据您设定的优先级依次进行匹配，优先级较小的规则优先匹配。	5

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果需要修改添加的JS脚本反爬虫规则，可单击待修改的路径规则所在行的“修改”，修改该规则。
- 如果需要删除添加的JS脚本反爬虫规则时，可单击待删除的路径规则所在行的“删除”，删除该规则。

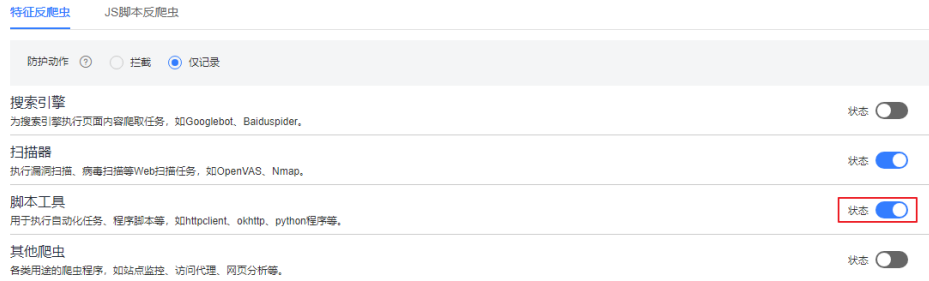
配置示例-仅记录脚本工具爬虫

假如防护域名“www.example.com”已接入WAF，您可以参照以下操作步骤验证反爬虫防护效果。

步骤1 执行JS脚本工具，爬取网页内容。

步骤2 在“特征反爬虫”页签，开启“脚本工具”，“防护动作”设置为“仅记录”（WAF检测为攻击行为后，只记录不阻断）。

图 5-51 开启“脚本工具”



步骤3 开启网站反爬虫。

图 5-52 网站反爬虫配置框



步骤4 在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

图 5-53 查看防护事件-脚本爬虫




时间	源IP	防护域名	地理位置	规则ID	URL	事件类型	防护动作	状态码	响应负载	企业项目	操作
2024/03/21 15:35...	100	vswaf	unknown	061059	/	恶意爬虫	仅记录	200	cur/7.69.1	default	详情 降级处理 更多
2024/03/21 15:35...	100	vswaf	unknown	061059	/	恶意爬虫	仅记录	200	cur/7.69.1	default	详情 降级处理 更多

----结束

配置示例-搜索引擎

放行百度或者谷歌的搜索引擎，同时拦截百度的POST请求。

步骤1 参照**步骤6**将“搜索引擎”设置为放行，即将“搜索引擎”的“状态”设置为 。

步骤2 参照**配置精准访问防护规则定制化防护策略**配置如**图5-54**的规则。

图 5-54 拦截 POST 请求

添加精准访问防护规则



1 WAF为您提供了几种常见的防护策略配置案例，供您学习参考！[了解详情](#)
本规则生效后，请关注业务情况，如有异常，可以删除本规则。

配置防护规则

规则名称

规则描述(可选)

条件列表

字段	子字段	逻辑	内容	大小写敏感	操作
Method	--	等于	POST	--	删除
User Agent	--	包含	Baiduspider	<input checked="" type="checkbox"/>	删除

+ 添加条件 您还可以添加20项条件。(多个条件同时成立才生效) [添加引用表](#)

采取防护措施

防护动作

阻断 放行 仅记录 JS挑战

----结束

5.11 配置防敏感信息泄露规则避免敏感信息泄露

您可以添加两种类型的防敏感信息泄露规则：

- 敏感信息过滤。配置后可对返回页面中包含的敏感信息做屏蔽处理，防止用户的敏感信息（身份证号、电话号码（11位中国境内的手机号码）、电子邮箱）泄露。
- 响应码拦截。配置后可拦截指定的HTTP响应码页面。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件

已添加防护网站或已[新增防护策略](#)。


- 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
- 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#)章节。


约束条件

- 云模式的入门版、标准版，以及云模式-ELB接入不支持该防护规则。
- 添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

配置防敏感信息泄露规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“防敏感信息泄露”配置框，用户可根据自己的需要开启或关闭防敏感信息泄露策略。

- ：开启状态。
- ：关闭状态。

步骤7 在“防敏感信息泄露”规则配置列表的左上方，单击“添加规则”。

步骤8 在弹出的对话框，添加防敏感信息泄露规则，如[图5-55](#)和[图5-56](#)所示，参数说明如[表5-14](#)所示。

“防敏感信息泄露”规则既能防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露，也能够拦截指定的HTTP响应码页面。

敏感信息过滤：针对网站页面中可能存在的电话号码和身份证等敏感信息，配置相应的规则对其进行屏蔽处理。例如，您可以通过设置以下防护规则，屏蔽身份证号、电话号码和电子邮箱敏感信息。

图 5-55 敏感信息泄露

✕

添加防敏感信息泄露规则

* 路径

* 类型

* 内容 身份证号 电话号码 电子邮箱

* 防护动作

规则描述

响应码拦截：针对特定的HTTP请求状态码，可配置规则将其拦截，避免服务器敏感信息泄露。例如，您可以通过设置以下防护规则，拦截HTTP 404、502、503状态码。

图 5-56 响应码拦截

✕

添加防敏感信息泄露规则

* 路径

* 类型

* 内容 400 401 402 403 404
 405 500 501 502 503
 504 507

* 防护动作

规则描述

表 5-14 参数说明

参数名称	参数说明	取值样例
路径	<p>需要过滤敏感信息（例如：身份证号、电话号码、电子邮箱等）或者拦截响应码的URL不包含域名的路径。</p> <ul style="list-style-type: none"> 前缀匹配：填写的路径前缀与需要防护的路径相同即可。 如果防护路径为“/admin”，该规则填写为“/admin*”，该规则生效。 精准匹配：需要防护的路径需要与此处填写的路径完全相等。 如果防护路径为“/admin”，该规则必须填写为“/admin”。 <p>说明</p> <ul style="list-style-type: none"> 该路径不支持正则，仅支持前缀匹配和精准匹配的逻辑。 路径里不能含有多条斜线的配置，如“///admin”，访问时，引擎会将“///”转为“/”。 	/admin*
类型	<ul style="list-style-type: none"> 敏感信息过滤：防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露。 响应码拦截：拦截指定的HTTP响应码页面。 	敏感信息过滤
内容	防护“类型”对应的防护内容，支持多选。	身份证号码
防护动作	可选择“过滤”或者“仅记录”。	过滤
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确定”，添加的防敏感信息泄露规则展示在防敏感信息泄露规则列表中。

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 当您需要修改添加的防敏感信息泄露规则时，在待修改的防敏感信息泄露规则所在行，单击“修改”，修改防敏感信息泄露规则。
- 当您需要删除添加的防敏感信息泄露规则时，在待删除的防敏感信息泄露规则所在行，单击“删除”，删除防敏感信息泄露规则。

配置示例-敏感信息过滤

假如防护域名“www.example.com”已接入WAF，您可以参照以下操作步骤验证敏感信息过滤防护效果。

步骤1 添加一条敏感信息过滤规则。

图 5-57 敏感信息泄露

添加防敏感信息泄露规则



* 路径

* 类型

* 内容 身份证号 电话号码 电子邮箱

* 防护动作

规则描述

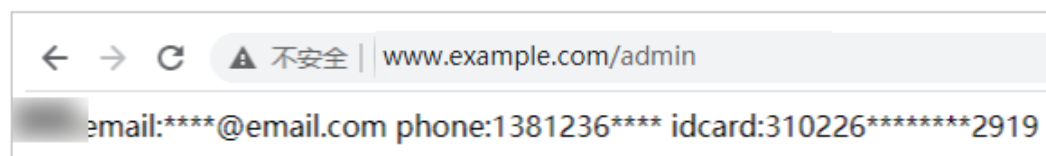
步骤2 开启防敏感信息泄露。

图 5-58 防敏感信息泄露配置框



步骤3 清理浏览器缓存，在浏览器中访问“<http://www.example.com/admin/>”页面。
该页面的电子邮箱、电话号码和身份号码信息被屏蔽。

图 5-59 敏感信息屏蔽示例



----结束

5.12 配置全局白名单规则对误报进行忽略

当WAF根据您配置的Web基础防护规则或网站反爬虫的“特征反爬虫”规则检测到符合规则的恶意攻击时，会按照规则中的防护动作（仅记录、拦截等），在“防护事件”页面中记录检测到的攻击事件。

对于误报情况，您可以添加白名单对误报进行忽略，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。

- “不检测模块”选择“所有检测模块”时：通过WAF配置的其他所有的规则都不会生效，WAF将放行该域名下的所有请求流量。
- “不检测模块”选择“Web基础防护模块”时：可根据选择的“不检测规则类型”，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。
- “不检测模块”选择“非法请求”时：可对非法请求进行加白。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件

- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#)章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。


约束条件


- 当“不检测模块”配置为“所有检测模块”时，通过WAF配置的其他所有的规则都不会生效，WAF将放行该域名下的所有请求流量。
- 当“不检测模块”配置为“Web基础防护模块”时，仅对WAF预置的Web基础防护规则和网站反爬虫的“特征反爬虫”拦截或记录的攻击事件可以配置全局白名单规则，防护规则相关说明如下：
 - Web基础防护规则
防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击，以及Webshell检测、深度反逃逸检测等Web基础防护。
 - 网站反爬虫的“特征反爬虫”规则
可防护搜索引擎、扫描器、脚本工具、其它爬虫等爬虫。
- 您可以通过[处理误报事件](#)来配置全局白名单规则，处理误报事件后，您可以在全局白名单规则列表中查看该误报事件对应的全局白名单规则。

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

配置全局白名单规则

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“全局白名单”配置框，用户可根据自己的需要开启或关闭全局白名单策略。

- ：开启状态。
- ：关闭状态。

步骤7 在“全局白名单”规则配置列表的左上方，单击“添加规则”。

步骤8 添加全局白名单规则，参数说明如表5-15所示。

图 5-60 添加全局白名单规则



添加全局白名单规则

不同模式使用限制和注意事项

* 防护方式 全部域名 指定域名

* 条件列表

字段	子字段	逻辑	内容
路径	--	包含	/product

添加 您还可以添加29项条件。(多个条件同时成立才生效)

添加 您还可以添加2组“或”条件

* 不检测模块 所有检测模块 Web基础防护模块 非法请求

* 不检测规则类型 按ID 按类别 所有内置规则

* 不检测规则类别 XSS攻击

规则描述

不检测字段

确定 取消

表 5-15 参数说明

参数	参数说明	取值样例
防护方式	<ul style="list-style-type: none"> “全部域名”：默认防护当前策略下绑定的所有域名。 “指定域名”：选择策略绑定的防护域名或手动输入泛域名对应的单域名。 	指定域名
防护域名	<p>“防护方式”选择“指定域名”时，需要配置此参数。</p> <p>需要手动输入当前策略下绑定的需要防护的泛域名对应的单域名，且需要输入完整的域名。</p> <p>单击“添加”，支持配置多个域名。</p>	www.example.com
条件列表	<ul style="list-style-type: none"> 单击条件框内的“添加”增加组内新的条件，一个防护规则至少包含一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。 单击条件框外的“添加”可增加1组新的条件，最多可添加3组条件，多组条件之间是“或”的关系，即满足其中1组条件时，本条规则即生效。 <p>条件设置参数说明如下：</p> <ul style="list-style-type: none"> 字段 子字段：当字段选择“IPv4”、“IPv6”、“Params”、“Cookie”或者“Header”时，请根据实际使用需求配置子字段。 须知 子字段的长度不能超过2048字节。 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 内容：输入或者选择条件匹配的内容。 	“路径”包含“/product”

参数	参数说明	取值样例
不检测模块	<ul style="list-style-type: none"> “所有检测模块”：通过WAF配置的其他所有的规则都不会生效，WAF将放行该域名下的所有请求流量。 “Web基础防护模块”：选择此参数时，可根据选择的“不检测规则类型”，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。 “非法请求”：可对非法请求加白。 说明 非法请求判定标准： <ul style="list-style-type: none"> 请求头中参数个数超过512。 URL中参数个数超过2048。 Content-Type:application/x-www-form-urlencoded，且请求体中参数个数超过8192。 	Web基础防护模块
不检测规则类型	<p>“不检测模块”选择“Web基础防护模块”时，您可以选择以下三种方式进行配置：</p> <ul style="list-style-type: none"> 按ID：按攻击事件的ID进行配置。 按类别：按攻击事件类别进行配置，如：XSS、SQL注入等。一个类别会包含一个或者多个规则id。 所有内置规则：Web基础防护规则里开启的所有防护规则。 	按类别
不检测规则ID	<p>当“不检测规则类型”选择“按ID”时，需要配置此参数。</p> <p>“防护事件”列表中事件类型为非自定义规则的攻击事件所对应的规则编号。建议您直接在防护事件页面进行误报处理。</p>	041046
不检测规则类别	<p>当“不检测规则类型”选择“按类别”时，需要配置此参数。</p> <p>在下拉框中选择事件类别。</p> <p>WAF支持的防护事件类别有：XSS攻击、网站木马、其他类型攻击、SQL注入攻击、恶意爬虫、远程文件包含、本地文件包含、命令注入攻击。</p>	SQL注入攻击
规则描述	可选参数，设置该规则的备注信息。	不拦截SQL注入攻击

参数	参数说明	取值样例
不检测字段	<p>如果您只想忽略来源于某攻击事件下指定字段的攻击，可在“高级设置”里选择指定字段进行配置，配置完成后，WAF将不再拦截指定字段的攻击事件。</p> <p>在左边第一个下拉列表中选择目标字段。支持的字段有：Params、Cookie、Header、Body、Multipart。</p> <ul style="list-style-type: none">当选择“Params”、“Cookie”或者“Header”字段时，可以配置“全部”或根据需求配置子字段。当选择“Body”或“Multipart”字段时，可以配置“全部”。当选择“Cookie”字段时，“防护域名”可以为空。 <p>说明 当字段配置为“全部”时，配置完成后，WAF将不再拦截该字段的所有攻击事件。</p>	Params 全部

步骤9 单击“确定”。

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果需要修改添加的全局白名单规则时，可单击待修改的全局白名单规则所在行的“修改”，修改全局白名单规则。
- 如果需要删除添加的全局白名单规则时，可单击待删除的全局白名单规则所在行的“删除”，删除全局白名单规则。

5.13 配置隐私屏蔽规则防隐私信息泄露

您可以通过Web应用防火墙服务配置隐私屏蔽规则。隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件

- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。

- 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
- 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#) 章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。

约束条件

入门版不支持该功能。


添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。


系统影响

配置隐私屏蔽规则后，防护事件中将屏蔽敏感数据，防止用户隐私泄露。

配置隐私屏蔽规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“隐私屏蔽”配置框，用户可根据自己的需要开启或关闭隐私屏蔽策略。

- ：开启状态。
- ：关闭状态。

步骤7 在“隐私屏蔽”规则配置列表的左上方，单击“添加规则”。

步骤8 添加隐私屏蔽规则，根据[表5-16](#)配置参数。

图 5-61 添加隐私屏蔽规则

添加隐私屏蔽规则

×

* 路径

* 屏蔽字段

* 屏蔽字段名

规则描述

确定
取消

表 5-16 添加隐私屏蔽规则参数说明

参数	参数说明	取值样例
路径	<p>完整的URL链接，不包含域名。</p> <ul style="list-style-type: none"> 前缀匹配：以*结尾代表以该路径为前缀。例如，需要防护的路径为“/admin/test.php”或“/adminabc”，则路径可以填写为“/admin*”。 精准匹配：需要防护的路径需要与此处填写的路径完全相等。例如，需要防护的路径为“/admin”，该规则必须填写为“/admin”。 <p>说明</p> <ul style="list-style-type: none"> 该路径不支持正则，仅支持前缀匹配和精准匹配的逻辑。 路径里不能含有连续的多条斜线的配置，如“///admin”，访问时，引擎会将“///”转为“/”。 	<p>/admin/login.php</p> <p>例如：需要防护的URL为“http://www.example.com/admin/login.php”，则“路径”设置为“/admin/login.php”。</p>

参数	参数说明	取值样例
屏蔽字段	设置为屏蔽的字段。 <ul style="list-style-type: none"> Params: 请求参数。 Cookie: 根据Cookie区分的Web访问者。 Header: 自定义HTTP首部。 Form: 表单参数。 	<ul style="list-style-type: none"> “屏蔽字段”为“Params”时，屏蔽字段名请根据实际使用需求设置，如果设置为“id”，设置后，与“id”匹配的内容将被屏蔽。
屏蔽字段名	根据“屏蔽字段”设置字段名，被屏蔽的字段将不会出现在日志中。	<ul style="list-style-type: none"> “屏蔽字段”为“Cookie”时，屏蔽字段名请根据实际使用需求设置，如果设置为“name”，设置后，与“name”匹配的内容将被屏蔽。
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确定”，添加的隐私屏蔽规则展示在隐私屏蔽规则列表中。

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果需要修改添加的隐私屏蔽规则时，可单击待修改的隐私屏蔽规则所在行的“修改”，修改隐私屏蔽规则。
- 如果需要删除添加的隐私屏蔽规则时，可单击待删除的隐私屏蔽规则所在行的“删除”，删除隐私屏蔽规则。

配置示例-屏蔽 Cookie 字段

假如防护域名“www.example.com”已接入WAF，您可以参照以下操作步骤验证屏蔽Cookie字段名“jsessionid”防护效果。

步骤1 添加一条隐私屏蔽规则。

图 5-62 添加“jsessionId”字段名隐私屏蔽规则

添加隐私屏蔽规则 ✕

* 路径

* 屏蔽字段

* 屏蔽字段名

规则描述

步骤2 开启隐私屏蔽。

图 5-63 隐私屏蔽配置框



步骤3 在左侧导航树中，单击“防护事件”，进入“防护事件”页面。

步骤4 在目标防护事件所在行的“操作”列中，单击“详情”，查看事件详细信息。
该防护事件的Cookie字段名“jsessionid”信息被屏蔽。

图 5-64 查看防护事件-隐私屏蔽

事件信息

时间	2021/11/18 20:15:58 GMT+08:00	事件类型	SQL注入攻击
源IP	[REDACTED]	地理位置	江苏
防护域名	[REDACTED]	URL	/test
恶意负载位置	body	防护动作	拦截
事件ID	[REDACTED]	状态码	418
响应时间 (毫秒)	0	返回大小 (字节)	3,533

恶意负载

```
id=' and 1=1--
```

请求详情

```
POST /test
authorization: Basic cm9vdDpyb290
content-length: 14
accept-language: zh-CN,zh;q=0.9, zh-CN,zh;q=0.9
host: [REDACTED]
upgrade-insecure-requests: 1
content-type: application/x-www-form-urlencoded
connection: Keep-Alive
cache-control: max-age=0
user-agent: Mozilla/5.0 (Linux; U; Android 10; id-id; Redmi 9C Build/QP1A.190711.020) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/89.0.4389.116 Mobile Safari/537.36 XiaoMi/MiuiBrowser/12.13.0-gn
via: proxy A
Cookie: HWWAFSESID=f3ece7308c3e8feff3; HWWAFSESTIME=1637135543680; jsessionid=***mask***
```

----结束

5.14 配置扫描防护规则自动阻断高频攻击

扫描防护模块通过识别扫描行为和扫描器特征，阻止攻击者或扫描器对网站的大规模扫描行为，自动阻断高频Web攻击、高频目录遍历攻击，并封禁攻击源IP一段时间，帮助Web业务降低被入侵的风险并减少扫描带来的垃圾流量。

- “高频扫描封禁”：将短时间内多次触发当前防护对象下基础防护规则的攻击源封禁一段时间。
- “目录遍历防护”：将短时间内访问当前防护对象下大量且不存在（返回404）目录的攻击源拉黑一段时间。

前提条件

已添加防护网站或已[新增防护策略](#)。


- 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
- 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#)章节。


约束条件

- 云模式的入门版、标准版，以及云模式-ELB接入不支持该防护规则。
- 添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

配置扫描防护规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“扫描防护”配置框，用户可根据自己的需要开启或关闭扫描防护规则。

- ：开启状态。
- ：关闭状态。

步骤7 配置“高频扫描封禁”。

将短时间内多次触发当前防护对象下基础防护规则的攻击源封禁一段时间。



1. 单击 开启高频扫描封禁。
2. 选择防护动作：
 - 拦截：发现攻击行为后立即阻断并记录。
 - 仅记录：发现攻击行为后只记录不阻断攻击。
3. 单击 编辑规则信息。
默认配置：检测时间范围在60秒内，基础防护规则触发大于20次且触发规则大于2条，则封禁1800秒。
可根据需要调整配置值。

图 5-65 高频扫描封禁



步骤8 配置“目录遍历防护”。

将短时间内多次触发当前防护对象下基础防护规则的攻击源封禁一段时间。

1. 单击 开启目录遍历防护。
2. 选择防护动作：
 - 拦截：发现攻击行为后立即阻断并记录。
 - 仅记录：发现攻击行为后只记录不阻断攻击。
3. 单击 编辑规则信息。

默认配置：检测时间范围在10秒内，针对当前防护对象请求次数超过50次且404响应码比例超过70%，同时不存在的目录数量超过50个，则封禁1800秒。

可根据需要调整配置值。

图 5-66 目录遍历防护



----结束

5.15 创建引用表对防护指标进行批量配置

该章节指导您创建引用表，即可对路径、User Agent、IP、Params、Cookie、Referer、Header等这些单一类型的防护指标进行批量配置，引用表能够被CC攻击防护规则、精准访问防护规则和网站反爬虫防护规则所引用。

当配置CC攻击防护规则、精准访问防护规则和网站反爬虫防护规则时，“条件列表”中的“逻辑”关系选择“包含任意一个”、“不包含任意一个”、“等于任意一个”、“不等于任意一个”、“前缀为任意一个”、“前缀不为任意一个”、“后缀为任意一个”或者“后缀不为任意一个”时，可在“内容”的下拉框中选择适合的引用表名称。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件

- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#) 章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。

约束条件

入门版和标准版不支持该功能。


应用场景

CC攻击防护规则、精准访问防护规则和网站反爬虫防护规则批量配置防护字段时，可以使用引用表。

创建引用表

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“CC攻击防护”或者“精准访问防护”配置框。

- 步骤7** 在列表左上角，单击“引用表管理”。
- 步骤8** 在“引用表管理”界面，单击“添加引用表”。
- 步骤9** 在弹出的“添加引用表”对话框中，添加引用表，参数说明如表5-17所示。

图 5-67 添加引用表

表 5-17 添加引用表参数说明

参数名称	参数说明	取值样例
名称	用户自定义引用表的名字。	test

参数名称	参数说明	取值样例
类型	<ul style="list-style-type: none"> ● 路径：设置的防护路径，不包含域名。 ● User Agent：设置为需要防护的扫描器的用户代理。 ● IP：设置为需要防护的访问者IP地址。支持IPv4和IPv6两种格式的IP地址。 <ul style="list-style-type: none"> - IPv4，例如：192.168.1.1 - IPv6，例如： fe80:0000:0000:0000:0000:0000:0000:0000 <p>须知</p> <ul style="list-style-type: none"> - 云模式仅专业版和铂金版支持IPv6防护。 - 支持配置0.0.0.0/0 和::/0 IP地址段，分别实现ipv4全流量拦截和ipv6全流量拦截。 <ul style="list-style-type: none"> ● Params：设置为需要防护的请求参数。 ● Cookie：根据Cookie区分的Web访问者。 ● Referer：设置为需要防护的自定义请求访问的来源。 例如：防护路径设置为“/admin/xxx”，如果用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“值”设置为“http://www.test.com”。 ● Header：设置为要防护的自定义HTTP首部。 ● Request Body：HTTP 请求中包含的数据。 ● Response Code：请求返回的状态代码。 ● Response Body：响应的消息体。 ● Response Header：响应头。 	路径
值	<p>对应“类型”的取值，该值不支持通配符。</p> <p>可批量添加多个值，以回车作为分隔符。</p>	/buy/phone/
规则描述	设置该规则的备注信息。	-

步骤10 单击“确定”，添加的引用表展示在引用表列表。

---结束

相关操作

- 如果需要修改创建的引用表，可单击待修改的引用表所在行的“修改”，修改引用表。
- 如果需要删除创建的引用表，可单击待删除的引用表所在行的“删除”，删除引用表。

5.16 配置攻击惩罚标准封禁访问者指定时长

当访问者的IP、Cookie或Params恶意请求被WAF拦截时，您可以通过配置攻击惩罚，使WAF按配置的攻击惩罚时长来自动封禁访问者。例如，访问者的源IP（192.168.1.1）为恶意请求，如果您配置了IP攻击惩罚拦截时长为500秒，该攻击惩罚生效后，则该IP被WAF拦截时，WAF将封禁该IP，时长为500秒。

配置的攻击惩罚标准规则会同步给Web基础防护规则、CC攻击防护、精准访问防护规则和IP黑白名单等规则使用。当配置Web基础防护规则、CC攻击防护、精准访问防护规则和IP黑白名单规则时，防护动作为“拦截”或“阻断”时，可使用攻击惩罚标准功能。

📖 说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名配置防护策略。

前提条件

- 已添加防护网站或已[新增防护策略](#)。
 - 云模式-CNAME接入的接入方式参见[将网站接入WAF防护（云模式-CNAME接入）](#)章节。
 - 云模式-ELB接入的接入方式参见 [将网站接入WAF防护（云模式-ELB接入）](#) 章节。
 - 独享模式的接入方式参见[将网站接入WAF防护（独享模式）](#) 章节。
- 如果使用独享WAF，确保独享引擎已升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。

约束条件

- Web基础防护、精准访问防护和黑白名单设置支持攻击惩罚功能，当攻击惩罚标准配置完成后，您还需要在Web基础防护、精准访问防护或黑白名单规则中选择攻击惩罚，该功能才能生效。

须知

黑白名单规则中，不支持选择“长时间IP拦截”和“短时间IP拦截”的攻击惩罚。

- 在配置Cookie或Params恶意请求的攻击惩罚标准前，您需要在域名详情页面设置对应的流量标识。相关操作请参见[配置攻击惩罚的流量标识](#)。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。


规格限制

- WAF支持设置6种拦截类型，每个拦截类型只能设置一条攻击惩罚标准。
- 最大拦截时长：
 - **长时间拦截**（包括“长时间IP拦截”、“长时间Cookie拦截”、“长时间Params拦截”）：3个月。
 - **短时间拦截**（包括“短时间IP拦截”、“短时间Cookie拦截”、“短时间Params拦截”）：1800秒。

设置攻击惩罚标准

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 单击“设置攻击惩罚”，用户可根据自己的需要开启或关闭攻击惩罚策略。

- ：开启状态。
- ：关闭状态。

步骤7 首次添加时，单击“添加攻击惩罚”，参数配置如[表5-18](#)所示。

说明

需要增加攻击惩罚标准规则时，单击“添加规则”。

图 5-68 设置攻击惩罚标准



表 5-18 攻击惩罚参数说明

参数	参数说明	取值样例
拦截类型	支持以下拦截方式： <ul style="list-style-type: none"> • 长时间IP拦截 • 短时间IP拦截 • 长时间Cookie拦截 • 短时间Cookie拦截 • 长时间Params拦截 • 短时间Params拦截 须知 黑白名单规则中，不支持选择“长时间IP拦截”和“短时间IP拦截”的攻击惩罚。	长时间IP拦截
拦截时长（秒）	拦截时长需要设置为整数。 <ul style="list-style-type: none"> • 短时间拦截：“拦截类型”设置为“短时间IP拦截”、“短时间Cookie拦截”或“短时间Params拦截”，支持按“秒”配置拦截时长，设置范围为1~300秒。 • 长时间拦截：“拦截类型”设置为“长时间IP拦截”、“长时间Cookie拦截”或“长时间Params拦截”，支持按“秒”、“分钟”、“小时”、“天”、“个月”配置拦截时长，设置范围为： <ul style="list-style-type: none"> - 单位为“秒”时：301~7,776,000 - 单位为“分钟”时：6~129,600 - 单位为“小时”时：1~2,160 - 单位为“天”时：1~90 - 单位为“个月”时：1~3 	3个月
规则描述	可选参数，设置该规则的备注信息。	-

步骤8 配置完成后，单击“保存”，添加的攻击惩罚标准展示在列表中。

----结束

相关操作

- 如果需要修改添加的攻击惩罚标准，可单击待修改的攻击惩罚标准所在行的“修改”，修改该标准的拦截时长。
- 如果需要删除添加的攻击惩罚标准，可单击待删除的攻击惩罚标准所在行的“删除”，删除该标准。

配置示例-Cookie 拦截攻击惩罚

假如防护域名“www.example.com”已接入WAF，访问者IP XXX.XXX.248.195为恶意请求，而您需要对来自该IP地址Cookie标记为jsessionId的访问请求封禁10分钟。您可以参照以下操作步骤验证封禁效果。

步骤1 在“网站设置”页面，单击“www.example.com”，进入域名基本信息页面。

步骤2 配置防护域名的Cookie流量标识，即“Session标记”。

图 5-69 流量标识



步骤3 添加一条拦截时长为600秒的“长时间Cookie拦截”的攻击惩罚标准。

图 5-70 添加 Cookie 拦截攻击惩罚



步骤4 开启攻击惩罚。

图 5-71 攻击惩罚配置框



- 步骤5** 添加一条黑白名单规则，拦截XXX.XXX.248.195，且“攻击惩罚”选择“长时间Cookie拦截”。

图 5-72 选择攻击惩罚规则

The screenshot shows a configuration window titled "添加黑白名单设置规则". It contains the following fields and options:

- 规则名称: cf001
- IP/IP段或地址组: IP/IP段 地址组
- IP/IP段: 195
- 防护动作: 拦截
- 攻击惩罚: 长时间Cookie拦截 (with a "添加攻击惩罚" button next to it)
- 规则描述: (empty text box)

At the bottom, there are "确认" (Confirm) and "取消" (Cancel) buttons.

- 步骤6** 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当XXX.XXX.248.195源IP访问页面时，会被WAF拦截。当WAF检测到来自该源IP的Cookie标记为jsessionid访问请求时，WAF将封禁该访问请求，时长为10分钟。

图 5-73 WAF 拦截攻击请求



- 步骤7** 返回Web应用防火墙管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

5.17 条件字段说明

您在设置CC攻击防护规则、精准访问防护规则或全局白名单规则时，需要在规则中配置条件字段，定义要匹配的请求特征。本文介绍了规则匹配条件支持使用的字段及其释义。

什么是条件字段

条件字段指需要WAF检测的请求特征。您在设置**CC攻击防护规则**、**精准访问防护规则**或**配置全局白名单规则**时，通过定义条件字段，指定要检测的请求特征。如果某个请求满足规则中设置的条件，则该请求命中对应规则；WAF会依据规则中设置的规则动作，对请求执行相应处置（例如，放行、拦截、仅记录等）。

图 5-74 条件字段

条件字段由字段、子字段、逻辑、和内容组成。配置示例如下：

- 示例1：“字段”为“路径”、“逻辑”为“包含”、内容为“/admin”，表示被请求的路径包含“/admin”时，则请求命中该规则。
- 示例2：“字段”为“IPv4”、“子字段”为“客户端IP”、“逻辑”为“等于”、内容为“192.XX.XX.3”，表示当发起连接的客户端IP为192.XX.XX.3时，则请求命中该规则。

支持的条件字段

表 5-19 条件列表配置

字段	子字段	逻辑	内容（举例）
“路径”：设置的防护路径，不包含域名，仅支持精准匹配（需要防护的路径需要与此处填写的路径完全相等。例如，需要防护的路径为“/admin”，该规则必须填写为“/admin”）	--	在“逻辑”下拉列表框中选择逻辑关系。	<i>/buy/phone/</i> 须知 <ul style="list-style-type: none">• 路径设置为“/”时，表示防护网站所有路径。• 配置的“路径”的“内容”不能包含特殊字符（<>*）。
“User Agent”：设置为需要防护的扫描器的用户代理。	--		<i>Mozilla/5.0 (Windows NT 6.1)</i>

字段	子字段	逻辑	内容（举例）
<p>“IP”：设置为需要防护的访问者IP地址。</p> <p>支持IPv4和IPv6两种格式的IP地址。</p> <p>须知 仅专业版和铂金版支持IPv6防护。</p>	<ul style="list-style-type: none"> 客户端IP X-Forwarded-For TCP连接IP 3层源IP 		<ul style="list-style-type: none"> IPv4，例如： 192.168.1.1 IPv6，例如： fe80:0000:0000:0000:0000:0000:0000:0000
Params：设置为需要防护的请求参数。	<ul style="list-style-type: none"> 所有子字段 任意子字段 自定义 		201901150929
<p>Referer：设置为需要防护的自定义请求访问的来源。</p> <p>例如：防护路径设置为“/admin/xxx”，如果用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“内容”设置为“http://www.test.com”。</p>	--		http://www.test.com
Cookie：根据Cookie区分的Web访问者。	<ul style="list-style-type: none"> 所有子字段 任意子字段 自定义 		jsessionId
Header：设置为需要防护的自定义HTTP首部。	<ul style="list-style-type: none"> 所有子字段 任意子字段 自定义 		<i>text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8</i>
Method：需要防护的自定义请求的方法。	--		GET、POST、PUT、DELETE、PATCH
Request Line：需要防护的自定义请求行的长度。	--		50

字段	子字段	逻辑	内容（举例）
Request: 需要防护的自定义请求的长度。包含请求头、请求行、请求体。	--		--
Protocol: 需要防护的请求的协议。	--		http
Response Code: 请求返回的状态代码。	--	<ul style="list-style-type: none"> • 等于 • 不等于 • 等于任意一个 • 不等于任意一个 	404
Response Length: 请求返回的响应长度。	--	<ul style="list-style-type: none"> • 长度等于 • 长度不等于 • 长度大于 • 长度小于 	--
Response Time: 响应时间。	--	<ul style="list-style-type: none"> • 长度等于 • 长度不等于 • 长度大于 • 长度小于 	--
Response Header: 响应头。	<ul style="list-style-type: none"> • 所有子字段 • 任意子字段 • 自定义 	<ul style="list-style-type: none"> • 包含 • 不包含 • 等于 • 不等于 • 前缀为 • 前缀不为 • 后缀为 • 后缀不为 • 包含任意一个 • 不包含任意一个 • 等于任意一个 • 不等于任意一个 • 前缀为任意一个 • 前缀不为任意一个 • 后缀为任意一个 • 正则匹配 	--

字段	子字段	逻辑	内容（举例）
Response Body: 响应的消息体。	--	<ul style="list-style-type: none"> 包含 不包含 包含任意一个 不包含任意一个 正则匹配 	--
Request Body: 请求的消息体。	--	<ul style="list-style-type: none"> 包含 不包含 包含任意一个 不包含任意一个 正则匹配 	--

5.18 WAF 覆盖的应用类型

Web基础防护规则支持防护的应用类型如表5-20。

表 5-20 WAF 覆盖的应用类型

4images	Dragon-Fire IDS	Log4j2	ProjectButler
A1Stats	Drunken Golem GP	Loggix	Pulse Secure
Achievo	Drupal	lpswitch IMail	Quest CAPTCHA
Acidcat CMS	DS3	Lussumo Vanilla	QuickTime Streaming Server
Activist Mobilization Platform	Dubbo	MAGMI	R2 Newsletter
AdaptBB	DynPG CMS	ManageEngine ADSelfService Plus	Radware AppWall
Adobe	DZCP basePath	MassMirror Uploader	Rezervi root
Advanced Comment System	ea-gBook inc ordner	Mavili	Ruby
agendax	EasyBoard	MAXcms	RunCMS
Agora	EasySiteEdit	ME Download System	Sahana-Agasti

AIOCP	e-cology	Mevin	SaurusCMS CE
AjaxFile	E-Commerce	Microsoft Exchange Server	School Data Navigator
AJSquare	Elvin	Moa Gallery MOA	Seagull
Alabanza	Elxis-CMS	Mobius	SGI IRIX
Alfresco Community Edition	EmpireCMS	Moodle	SilverStripe
AllClubCMS	EmuMail	Movabletype	SiteEngine
Allwebmenus Wordpress	eoCMS	Multi-lingual E-Commerce	Sitepark
Apache	E-Office	Multiple PHP	Snipe Gallery
Apache APISIX Dashboard	EVA cms	mxCamArchive	SocialEngine
Apache Commons	eXtropia	Nakid CMS	SolarWinds
Apache Druid	EZPX Photoblog	NaviCOPA Web Server	SQuery
Apache Dubbo	F5 TMUI	NC	Squid
Apache Shiro	Faces	NDS iMonitor	StatCounteX
Apache Struts	FAQEngine	Neocrome Seditio	Subdreamer-CMS
Apache Tomcat	FASTJSON or JACKSON	NetIQ Access Manager	Sumsung IOT
Apache-HTTPD	FCKeditor	Netwin	Sun NetDynamics
Apple QuickTime	FileSeek	Nginx	SuSE Linux Sdbsearch
ardeaCore	fipsCMSLight	Nodesforum	SweetRice-2
AROUNDMe	fipsForum	Nucleus Plugin Gallery	Tatantella
Aurora Content Management	Free PHP VX Guestbook	Nucleus Plugin Twitter	Thecartpress Wordpress
AWCM final	FreeSchool	Nukebrowser	Thinkphp
AWStats	FreshScripts	NukeHall	ThinkPHP5 RCE
Baby Gekko	FSphp	Nullsoft	Tiki Wiki

BAROSmini Multiple	FusionAuth	Ocean12 FAQ Manager	Tomcat
Barracuda Spam	Gallo	OCPortal CMS	Trend Micro
BizDB	GetSimple	Open Education	Trend Micro Virus Buster
Blackboard	GetSimple CMS	OpenMairie openAnnuaire	Tribal Tribiq CMS
BLNews	GLPI	OpenPro	TYPO3 Extension
Caldera	GoAdmin	openUrgence Vaccin	Uebimiau
Cedric	Gossamer Threads DBMan	ORACLE Application Server	Uiga Proxy
Ciamos CMS	Grayscalecms	Oramon	Ultrize TimeSheet
ClearSite Beta	Hadoop	OSCommerce	VehicleManager
ClodFusion Tags	Haudenschilt Family	PALS	Visitor Logger
CMS S Builder	Havalite	Pecio CMS	VMware
ColdFusion	HIS Auktion	PeopleSoft	VoteBox
ColdFusion Tags	HP OpenView Network Node Manager	Persism Content Management	WayBoard
Commvault CommCell CVSearchService	HPInsightDiagnos tics	PhotoGal	WebBBS
Concrete5	Huawei D100	PHP Ads	WebCalendar
Confluence Server and Data Center	HUBScript	PHP Classifieds	WEB-CGI
Coremail	IIS	PHP CMS	WebFileExplorer
Cosmicperl Directory Pro	iJoomla Magazine	PHP Paid 4 Mail Script	WebGlimpse
CPCcommerce	ILIAS	PHPAddressBoo k	webLogic
DataLife Engine	Indexu	PHP-Calendar	WebLogic Server wls9- async

DCScripts	IRIX	phpCow	Webmin
DDL CMS	JasonHines PHPWebLog	PHPGenealogy	WEB-PHP Invision Board
DELL TrueMobile	JBOSS	PHPGroupWare	WebRCSdiff
Digitaldesign CMS	JBossSeam	phpMyAdmin	Websense
Dir2web	Joomla	phpMyAdmin Plugin	WebSphere
Direct News	JRE	PHPMyGallery	WikiBlog WBmap
Discourse	jsfuck	PHPNews	WordPress
Diskos CMS Manager	justVisual	Pie Web Masher	WORK system
DiY-CMS	Katalog Stron Hurricane	PlaySMS	Wpeasystats Wordpress
D-Link	KingCMS	Plogger	XOOPS
DMXReady Registration Manager	koesubmit	Plone	Xstream
DoceboLMS	Kontakt Formular	PointComma	YABB SE
Dokuwiki	KR-Web	Postgres	YP Portal MS-Pro Surumu
dompdf	Landray	PrestaShop	ZenTao
DotNetNuke	Livesig Wordpress	ProdLer	Zingiri Web Shop Wordpress
ZOHO ManageEngine	-	-	-

6 查看总览

在“安全总览”页面，您可以查看昨天、今天、3天、7天、30天或自定义30天任意时间段内所有防护网站或所有实例以及指定防护网站或实例的防护日志。包括请求与各攻击类型统计次数，QPS、带宽、响应码信息，以及事件分布、受攻击域名 Top5、攻击源IP Top5、受攻击URL Top5、攻击来源区域 Top5和业务异常监控 Top5等防护数据。

安全总览页面统计数据每隔2分钟刷新一次。

📖 说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目的安全总览信息。

前提条件

- 已将网站接入WAF。
- 已为防护域名添加了一个或者多个防护规则。

规格限制

最多可以查看30天的防护数据。

QPS 计算方式

不同时间段的QPS计算方式不同，QPS在各时间段的取值说明如表6-1所示。

表 6-1 QPS 取值说明

时间段	QPS平均取值说明	QPS峰值取值说明
“昨天”、“今天”	间隔1分钟，取1分钟内的平均值	间隔1分钟，取1分钟内的最大值
“3天”	间隔5分钟，取5分钟内的平均值	间隔5分钟，取5分钟内的最大值
“7天”	间隔10分钟，取每5分钟内平均值的最大值	间隔10分钟，取10分钟内最大值


时间段	QPS平均取值说明	QPS峰值取值说明
“30天”	间隔1小时，取每5分钟内平均值的最大值	间隔1小时，取1小时内最大值


说明

QPS (Queries Per Second) 即每秒钟的请求量，例如一个HTTP GET请求就是一个Query。请求次数是间隔时间内请求的总量。

查看安全总览

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”，进入“安全总览”页面。

步骤4 在页面上方，选择“企业项目”。选择后，将为您展示该企业项目下添加到WAF防护的网站数据。

步骤5 “资源防护概况”模块数据展示，如[图6-1](#)所示。

- 查看域名总数，已接入WAF域名数，以及未成功接入WAF的域名数和DNS解析异常域名数。
- 产品信息：产品版本信息展示，单击>可跳转到“产品信息”页面，查看版本配额详情。

图 6-1 资源防护概况



步骤6 “安全统计”模块数据展示，如[图6-2](#)所示。

- 默认统计的是该账号所有项目下添加到WAF的所有网站的相关数据，您也可以根据需要选择要查询的网站、实例以及查询时间，查询时间可选择昨天、今天、3天、7天、30天，也可以自定义30天内的任意时间段。
- 支持选择“对比模式”或者“平铺模式”两种模式查看数据。
- “按天统计”：勾选后，显示的是间隔一天统计一次的数据；不勾选，统计的数据周期根据选择的时间段而定，具体如下：
 - “昨天”、“今天”：间隔1分钟统计一次数据。
 - “3天”：间隔5分钟统计一次数据。
 - “7天”：间隔10分钟统计一次数据。
 - “30天”：间隔1小时统计一次数据。

图 6-2 安全统计模块



表 6-2 安全统计模块

板块	参数说明
①查看总的请求数、攻击次数以及各类型攻击的页面总数	<ul style="list-style-type: none"> “请求次数”中统计的次数为网站的PV（Page Views）值，即用户每次访问网站，在某个时间内被访问的页面总数。 “攻击次数”中统计的次数为网站被各类型攻击的总次数。 各攻击类型统计的次数为用户每次访问网站，在某个时间内被该类型攻击的页面总数。 单击“查看网站TOP统计”，可查看请求次数、攻击次数、Web基础防护、精准防护、CC攻击防护、爬虫攻击防护、BOT管理排名TOP 10的数据。
②按请求次数、QPS、发送/接收带宽、响应码分别展示各项数据	<ul style="list-style-type: none"> 请求次数：统计的是域名被访问的总请求量、攻击总量以及被各类攻击类型攻击的页面总数。 QPS：域名平均每秒钟的请求量。QPS的取值说明参考QPS 计算方式。 QPS（Queries Per Second）即每秒钟的请求量，例如一个HTTP GET请求就是一个Query。 发送/接收带宽：域名访问的占用带宽。 发送、接收字节数是通过request_length, upstream_bytes_received按时间进行累加统计，与EIP上监控的网络带宽值存在差异。此外，造成两者差异的原因，还可能跟网页压缩、连接复用、TCP重传、接入模式等因素相关。详细说明，请参见为什么WAF显示的流量大小与源站上显示的不一致？。 响应码：可以查看“WAF返回客户端”和“源站返回给WAF”对应响应码以及响应次数。 响应码的数量是按照图表下方响应码的顺序（从左至右）累加进行显示，对应响应码的数量是为两条线的差值（如果某个响应码值为0，会与前一个的响应码显示的线重合）。

步骤7 “TOP事件源统计” 模块数据展示，如图6-3所示。

图 6-3 TOP 事件源统计



表 6-3 安全统计参数说明

参数	说明
事件分布	查看攻击事件类型。 单击“事件分布”中的任意一个区域，可查看指定域名被攻击的类型、攻击的次数、以及攻击占比。
受攻击对象	受攻击统计次数Top 5的域名以及各域名受攻击的次数。 单击“查看更多”，可以跳转到“防护事件”页面，查看更多防护数据。
攻击源IP	攻击次数Top 5的攻击源IP以及各源IP发起的攻击次数。 单击“查看更多”，可以跳转到“防护事件”页面，查看更多防护数据。 说明 “49.4.121.70”为WAF拨测IP。如果该IP的探测请求被拦截，且次数达到Top 5，也会在显示在攻击源IP中。
受攻击URL	受攻击统计次数Top 5的URL以及各URL受攻击的次数。 单击“查看更多”，可以跳转到“防护事件”页面，查看更多防护数据。
攻击来源区域	攻击次数Top 5的地区以及来源各地区发起的攻击次数。
业务异常监控	业务异常的Top 5防护网站。可以查看业务异常为“404”、“500”、“502”的防护网站。 单击“业务异常排查”，参照操作指导排查相应业务异常以及其他业务异常。

----结束

7 网站设置

7.1 网站接入后推荐配置

7.1.1 配置 PCI DSS/3DS 合规与 TLS

安全传输层协议（Transport Layer Security, TLS）在两个通信应用程序之间提供保密性和数据完整性。HTTPS协议是由TLS+HTTP协议构建的可进行加密传输、身份认证的网络协议。当防护网站的部署模式为“云模式”或“独享模式”且“对外协议”为“HTTPS”时，您可以通过WAF为网站设置最低TLS版本和加密套件（多种加密算法的集合），对于低于最低TLS版本的请求，将无法正常访问网站，以满足行业客户的安全需求。

WAF默认配置的最低TLS版本为TLS v1.0，加密套件为“安全加密套件”。

同时，WAF支持开启PCI DSS和PCI 3DS合规认证功能，开启合规认证后，最低TLS版本将设置为TLS v1.2，以满足PCI DSS和PCI 3DS合规认证要求。

📖 说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下的域名配置PCI DSS/3DS合规与TLS。

前提条件

已[添加防护网站](#)且配置的“对外协议”包含HTTPS。

约束条件

- 防护网站的部署模式为“云模式-CNAME接入”或“独享模式”。

📖 说明

如果您使用“云模式-ELB接入”方式接入网站，需要在ELB控制界面[配置TLS安全策略实现加密通信](#)。

- 当防护网站的“对外协议”为“HTTP”时，HTTP协议不涉及TLS，请忽略该章节。
- 如果防护网站配置了多个服务器时，“对外协议”都配置为“HTTPS”时，才支持配置PCI DSS/3DS合规。

- 开启PCI DSS/3DS合规后，将不支持修改“对外协议”，也不支持添加服务器。

应用场景

WAF默认配置的最低TLS版本为“TLS v1.0”，为了确保网站安全，建议您根据业务实际需求进行配置，支持配置的最低TLS版本如表7-1所示。

表 7-1 支持配置的最低 TLS 版本说明

场景	最低TLS版本（推荐）	防护效果
网站安全性能要求很高（例如，银行金融、证券、电子商务等有重要商业信息和重要数据的行业）	TLS v1.2	WAF将自动拦截TLS v1.0和TLS v1.1协议的访问请求。
网站安全性能要求一般（例如，中小企业门户网站）	TLS v1.1	WAF将自动拦截TLS1.0协议的访问请求。
客户端APP无安全性要求，可以正常访问网站	TLS v1.0	所有的TLS协议都可以访问网站。

说明

在配置TLS前，您可以先[查看网站TLS版本](#)。

WAF推荐配置的加密套件为“安全加密套件”，可以满足浏览器兼容性和安全性，各加密套件相关说明如表7-2所示。

表 7-2 加密套件说明

加密套件名称	支持的加密算法	不支持的加密算法	说明
经典加密套件 说明 WAF默认给网站配置的是“安全加密套件”，但是如果请求信息不携带sni信息，WAF就会选择缺省的“经典加密套件”。	<ul style="list-style-type: none"> • ECDHE-RSA-AES256-SHA384 • AES256-SHA256 • RC4 • HIGH 	<ul style="list-style-type: none"> • MD5 • aNULL • eNULL • NULL • DH • EDH • AESGCM 	<ul style="list-style-type: none"> • 兼容性：较好，支持的客户端较为广泛 • 安全性：一般

加密套件名称	支持的加密算法	不支持的加密算法	说明
加密套件1	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • HIGH 	<ul style="list-style-type: none"> • MEDIUM • LOW • aNULL • eNULL • DES • MD5 • PSK • RC4 • kRSA • 3DES • DSS • EXP • CAMELLIA 	<p>推荐配置。</p> <ul style="list-style-type: none"> • 兼容性：较好，支持的客户端较为广泛 • 安全性：较高
加密套件2	<ul style="list-style-type: none"> • ECDH+AESGCM • EDH+AESGCM 	-	<ul style="list-style-type: none"> • 兼容性：一般，严格符合PCI DSS的FS要求，较低版本浏览器可能无法访问。 • 安全性：高
加密套件3	<ul style="list-style-type: none"> • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • RC4 • HIGH 	<ul style="list-style-type: none"> • MD5 • aNULL • eNULL • NULL • DH • EDH 	<ul style="list-style-type: none"> • 兼容性：一般，较低版本浏览器可能无法访问。 • 安全性：高，支持ECDHE、DHE-GCM、RSA-AES-GCM多种算法。

加密套件名称	支持的加密算法	不支持的加密算法	说明
加密套件4	<ul style="list-style-type: none">• ECDHE-RSA-AES256-GCM-SHA384• ECDHE-RSA-AES128-GCM-SHA256• ECDHE-RSA-AES256-SHA384• AES256-SHA256• RC4• HIGH	<ul style="list-style-type: none">• MD5• aNULL• eNULL• NULL• EDH	<ul style="list-style-type: none">• 兼容性: 较好, 支持的客户端较为广泛• 安全性: 一般, 新增支持GCM算法。
加密套件5	<ul style="list-style-type: none">• AES128-SHA:AES256-SHA• AES128-SHA256:AES256-SHA256• HIGH	<ul style="list-style-type: none">• MEDIUM• LOW• aNULL• eNULL• EXPORT• DES• MD5• PSK• RC4• DHE	仅支持RSA-AES-CBC算法。

加密套件名称	支持的加密算法	不支持的加密算法	说明
加密套件6	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 	-	<ul style="list-style-type: none"> • 兼容性：一般 • 安全性：较好
安全加密套件	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • HIGH 	<ul style="list-style-type: none"> • MEDIUM • LOW • aNULL • eNULL • DES • MD5 • PSK • RC4 • kRSA • SRP • 3DES • DSS • EXP • CAMELLIA • SHA1 • SHA256 • SHA384 	<p>在“加密套件1”的基础上，去除了对CBC算法的支持。推荐的安全配置，满足大多数安全场景。</p> <ul style="list-style-type: none"> • 兼容性：一般，核心套件为 ECDHE-ECDSA-AES256-GCM-SHA384，禁用了旧协议和弱加密算法，较低版本浏览器可能无法访问 • 安全性：高

加密套件名称	支持的加密算法	不支持的加密算法	说明
加密套件8	<ul style="list-style-type: none"> • AESGCM • HIGH • ECDHE • RSA 	<ul style="list-style-type: none"> • DH • EXPORT • RC4 • MEDIUM • LOW • aNULL • eNULL 	支持AES-GCM，提供强加密和数据完整性保护。 <ul style="list-style-type: none"> • 兼容性：较好，支持的客户端较为广泛 • 安全性：较好

WAF提供的TLS加密套件对于高版本的浏览器及客户端都可以兼容，不能兼容部分老版本的浏览器，以TLS v1.0协议为例，加密套件不兼容的浏览器及客户端参考说明如表7-3所示。

须知

建议您以实际客户端环境测试的兼容情况为准，避免影响现网业务。

表 7-3 加密套件不兼容的浏览器/客户端参考说明（TLS v1.0）

浏览器/客户端	经典加密套件	加密套件1	加密套件2	加密套件3	加密套件4	加密套件5	加密套件6	安全加密套件	加密套件8
Google Chrome 63 / macOS High Sierra 10.13.2	x	√	√	√	x	√	√	√	√
Google Chrome 49/ Windows XP SP3	x	x	x	x	x	√	√	x	√
Internet Explorer 6/Windows XP	x	x	x	x	x	x	x	x	x
Internet Explorer 8/Windows XP	x	x	x	x	x	x	x	x	x

浏览器/客户端	经典加密套件	加密套件1	加密套件2	加密套件3	加密套件4	加密套件5	加密套件6	安全加密套件	加密套件8
Safari 6/iOS 6.0.1	√	√	×	√	√	√	√	×	√
Safari 7/iOS 7.1	√	√	×	√	√	√	√	√	√
Safari 7/OS X 10.9	√	√	×	√	√	√	√	√	√
Safari 8/iOS 8.4	√	√	×	√	√	√	√	√	√
Safari 8/OS X 10.10	√	√	×	√	√	√	√	√	√
Internet Explorer 7/Windows Vista	√	√	×	√	√	×	√	×	√
Internet Explorer 8~10/Windows 7	√	√	×	√	√	×	√	×	√
Internet Explorer 10/Windows Phone 8.0	√	√	×	√	√	×	√	×	√
Java 7u25	√	√	×	√	√	×	√	×	√
OpenSSL 0.9.8y	×	×	×	×	×	×	×	×	√
Safari 5.1.9/OS X 10.6.8	√	√	×	√	√	×	√	×	√
Safari 6.0.4/OS X 10.8.4	√	√	×	√	√	×	√	×	√


系统影响


- PCI DSS

- 开启PCI DSS合规认证后，不能修改TLS最低版本和加密套件，且最低TLS版本将设置为“TLS v1.2”，加密套件设置为EECDH+AESGCM:EDH+AESGCM。
- 开启PCI DSS合规认证后，如果您需要修改TLS最低版本和加密套件，请关闭该认证。
- PCI 3DS
 - 开启PCI 3DS合规认证后，不能修改TLS最低版本，且最低TLS版本将设置为“TLS v1.2”。
 - 开启PCI 3DS合规认证后，您将不能关闭该认证，请根据业务实际需求进行操作。

配置 PCI DSS/3DS 合规与 TLS

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。


步骤6 在“合规认证”行，可以勾选“PCI DSS”或“PCI 3DS”开启合规认证，也可以在“TLS配置”所在行，单击  修改TLS配置。

图 7-1 修改 TLS 配置



- 勾选“PCI DSS”，系统弹出“警告”对话框，单击“确定”，开启该合规认证。

须知

选择开启PCI DSS合规认证后，您将不能修改TLS最低版本和加密套件。

- 勾选“PCI 3DS”，系统弹出“警告”对话框，单击“确定”，开启该合规认证。

须知

- 选择开启PCI 3DS合规认证后，您将不能修改TLS最低版本。
- 选择开启PCI 3DS合规认证后，您将不能关闭该认证，请根据业务实际需求进行操作。

步骤7 在“国际证书”所在行的TLS加密套件后，单击“修改”。

步骤8 在弹出的“TLS配置”对话框中，选择最低TLS版本和加密套件，如**图7-2**所示。

图 7-2 “TLS 配置”对话框

TLS配置

证书名称
zrj-fun

证书类型
国际证书

最低TLS版本
TLS v1.2

注意：低于最低TLS版本的请求，将无法正常使用。
建议您使用更安全的TLS v1.2

加密套件选择
加密套件1

兼顾一定的安全性与兼容性。
加密算法
ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:MEDIUM:LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH

选择“最低TLS版本”，相关说明如下：

- 默认为TLS v1.0版本，TLS v1.0及以上版本的请求可以访问域名。
- 选择TLS v1.1版本时，TLS v1.1及以上版本的请求可以访问域名。
- 选择TLS v1.2版本时，TLS v1.2及以上版本的请求可以访问域名。

步骤9 单击“确定”，TLS配置完成。

----结束

生效条件

如果“最低TLS版本”配置为“TLS v1.2”，则TLS v1.2协议可以正常访问网站，TLS v1.1及以下协议不能正常访问网站。

7.1.2 开启 IPv6 防护

如果您的网站需要IPv6的防护，可以参考本章节开启IPv6防护，开启后，WAF将为域名分配IPv6的接入地址，WAF默认在CNAME中增加IPv6地址解析，IPv6的所有访问请求将先流转到WAF，WAF检测并过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。

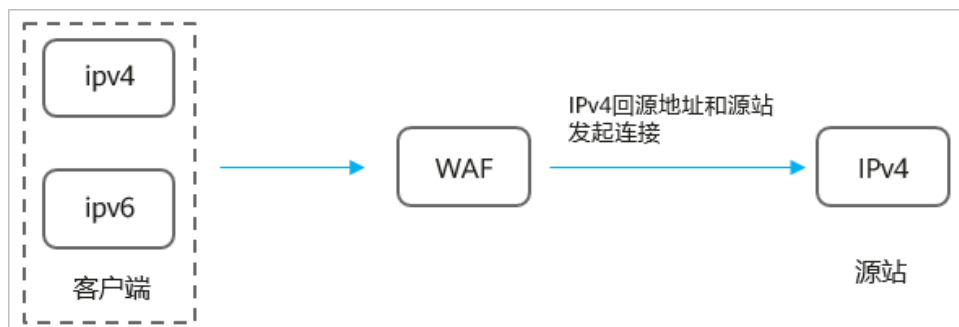
- 当防护网站的源站地址配置为IPv6地址时，默认开启IPv6防护。WAF使用IPv6回源地址和源站发起连接。

图 7-3 源站地址只有 IPv6 时



- 当防护网站的源站地址配置为IPv4地址时，手动开启IPv6防护后，WAF将通过NAT64机制（NAT64是一种通过网络地址转换（NAT）形式促成IPv6与IPv4主机间通信的IPv6转换机制）将外部IPv6访问流量转化成对内的IPv4流量。WAF使用IPv4回源地址和源站发起连接。

图 7-4 源站地址只有 IPv4 时



前提条件

防护网站已接入WAF


约束条件

- 防护网站的部署模式为“云模式-CNAME接入”，而且仅专业版和铂金版支持IPv6防护。
- 支持IPv6防护的区域请参考[功能总览](#)。
- 当源站存在IPv6地址，默认开启IPv6防护。WAF为了防止客户IPv6的业务中断，禁止关闭IPv6的开关，如果确定不需要IPv6防护，需要先修改服务器配置，在源站删除IPv6的配置，具体的操作方法请参见[修改服务器配置信息](#)。

开启 IPv6 防护

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

- 步骤3** 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。
- 步骤4** 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
- 步骤5** 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。
- 步骤6** 在“IPv6防护”所在行，单击“修改”，在弹出的对话框中，选择“开启”并单击“确定”。
- 结束

7.1.3 开启 HTTP2 协议

如果您的网站需要支持HTTP2协议的访问，可参考本章节开启HTTP2协议。HTTP2协议仅适用于客户端到WAF之间的访问，且“对外协议”必须包含HTTPS才能支持使用。



前提条件

已[添加防护网站](#)且配置的“对外协议”包含HTTPS。

约束条件

- 防护网站的部署模式为“云模式-CNAME接入”，而且仅专业版和铂金版支持HTTP2协议。
- 支持HTTP2协议防护的区域，请参考[功能总览](#)。

开启 HTTP2 协议

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击管理控制台左上角的 ，选择区域或项目。
- 步骤3** 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。
- 步骤4** 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
- 步骤5** 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。
- 步骤6** 在“是否使用HTTP2协议”所在行，单击“修改”，选择“是”并单击“确定”。
- 结束

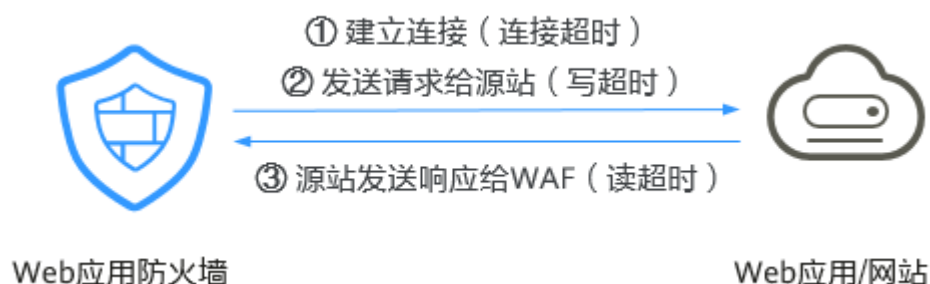
7.1.4 配置 WAF 到网站服务器的连接超时时间

如果您需要针对域名的每个请求设置超时时间，可参考本章节开启WAF到客户源站的“超时配置”并设置“连接超时”、“读超时”、“写超时”的时间。开启后不支持关闭。

- 连接超时**：WAF转发客户端请求时，TCP三次握手超时时间。
- 写超时**：WAF向源站发送请求的超时时间，如果在设定的写超时时间内源站未接收到请求，则认为连接超时。
- 读超时**：WAF从源站读取响应的超时时间，如果在设定的读超时时间内未收到来自源站的响应，则认为连接超时。

WAF转发请求给源站的三个步骤如图7-5所示。

图 7-5 WAF 转发请求给源站



说明

- 浏览器到WAF引擎的连接超时时长是120秒，该值取决于浏览器的配置，该值在WAF界面不可以手动设置。
- WAF到客户源站的连接超时时长默认为30秒，该值可以手动设置，但仅“独享模式”和“云模式”的专业版、铂金版支持手动设置连接超时、读超时、写超时的时长。

前提条件


防护网站已接入WAF


约束条件

- 防护网站的部署模式为“云模式-CNAME接入”或者“独享模式”。
- 云模式仅专业版、铂金版支持手动设置连接超时时长。
- WAF不支持手动设置浏览器到WAF引擎的连接超时时长，仅支持配置WAF到客户源站的连接超时时长。
- 开启后不支持关闭。
- 支持配置网站连接超时时间的区域，请参考[功能总览](#)。

配置 WAF 到网站服务器的连接超时时间


步骤1 [登录管理控制台](#)。


步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤6 在“超时配置”所在行，单击 ，开启超时配置。

步骤7 单击 ，设置“连接超时”、“读超时”、“写超时”的时间，并单击“确定”保存设置。

----结束

7.1.5 开启熔断保护功能保护源站安全

网站接入WAF防护之后，如果您访问网站时出现大量的502 Bad Gateway，504 Gateway Timeout错误或者等待处理的请求，为了保护源站的安全，可使用WAF的宕机保护和连接保护功能。当502/504请求数量或读等待URL请求数量以及占比阈值达到您设置的值时，将触发WAF熔断功能开关，实现宕机保护和读等待URL请求保护。

前提条件


- 已[添加防护网站](#)。
- 已将独享引擎版本升级到最新版本，具体的操作请参见[升级独享引擎实例](#)。


约束条件

- 防护网站的部署模式为“独享模式”。
- 开启“熔断保护”前，必须[将独享引擎实例版本升级到最新版本](#)，否则开启后可能会对业务产生影响。
- 网站连接保护功能开放的区域，请参考[功能总览](#)。

开启熔断保护

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。


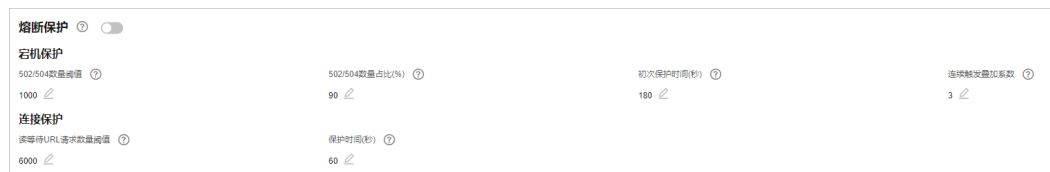
步骤6 在“熔断保护”所在行，单击，开启熔断保护。

图 7-6 熔断保护




步骤7 根据业务需要，在各参数所在行，单击，配置“宕机保护”和“连接保护”参数值，并单击“确定”保存设置，参数说明如[表7-4](#)所示。

表 7-4 连接保护参数说明

参数	参数说明	示例
宕机保护	502/504数量阈值	每30s累加的502/504数量阈值

参数		参数说明	示例
	502/504数量占比 (%)	总请求数量中502/504数量占比达到所设定值，并且与数量阈值同时满足时触发宕机保护。	90
	初次保护时间(秒)	初次触发宕机的保护时间，即WAF将停止转发用户请求的时间。	180
	连续触发叠加系数	连续触发时，保护时间延长最大倍数，叠加周期为3600s。 例如，“初次保护时间”设置为180s，“连续触发叠加系数”设置为3。 <ul style="list-style-type: none">当触发次数为2（即小于3）时，保护时间为360s。当次数大于等于3时，保护时间为540s。当累计保护时间超过1小时（3600s），叠加次数会从头计数。	3
连接保护	读等待URL请求数量阈值	读等待URL请求数量到达设定值即触发连接保护	6000
	保护时间(秒)	达到数量阈值所触发的保护时间，即WAF将停止转发用户请求的时间。	60

📖 说明

以图7-6中设置的值为例进行解释：

- “宕机保护”：当防护网站的502/504错误返回量达到1000条以上且占网站的所有访问请求量的90%及以上时，第一次触发时，WAF将停止转发用户请求180s（即阻止用户访问网站180s）；连续第二次触发时，WAF将停止转发用户请求360s；连续第三次及以上触发时，WAF将停止转发用户请求540s。当累计保护时间超过1小时（3600s），叠加次数会从头计数。
- “连接保护”：访问网站的读等待URL请求数量达到6000以上时，WAF将停止转发用户请求60s，且将返回网站的维护页面。

----结束

7.1.6 配置攻击惩罚的流量标识

WAF根据配置的流量标识识别客户端IP、Session或User标记，以分别实现IP、Cookie或Params恶意请求的攻击惩罚功能。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为该企业项目下的域名配置攻击惩罚的流量标识。

前提条件


防护网站已接入WAF


约束条件

- 如果配置了IP标记，为了确保IP标记生效，请您确认防护网站在接入WAF前已使用了7层代理，且防护网站的“是否使用七层代理”为“是”。
如果未配置IP标记，WAF默认通过客户端IP进行识别。
- 使用Cookie或Params恶意请求的攻击惩罚功能前，您需要分别配置对应域名的Session标记或User标记。

配置攻击惩罚的流量标识

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。


步骤6 在“流量标识”栏中，单击“IP标记”、“Session标记”或“User标记”后的 ，分别设置流量标识，相关参数说明如表7-5所示。

图 7-7 流量标识





流量标识 	Session标识	User标识
- 	- 	- 

表 7-5 流量标识参数说明

标识	说明	配置样例
IP标记	<p>客户端最原始的IP地址的HTTP请求头字段。</p> <p>如果配置该标识，请确保网站在接入WAF前已使用了7层代理，且防护网站的“是否使用七层代理”为“是”，IP标记功能才能生效。</p> <p>该字段用于保存客户端的真实IP地址，可自定义字段名且支持配置多个字段（多个字段名以英文逗号隔开），配置后，WAF优先从配置的字段中获取客户端真实IP（配置多个字段时，WAF从左到右依次读取）。</p> <p>须知</p> <ul style="list-style-type: none">• 如果想以TCP连接IP作为客户端IP，“IP标记”应配置为“\$remote_addr”。• 如果从自定义字段中未获取到客户端真实IP，WAF将依次从cdn-src-ip, x-real-ip, x-forwarded-for, \$remote_addr字段获取客户端IP。	X-Forwarded-For
Session标记	用于Cookie恶意请求的攻击惩罚功能。在选择Cookie拦截的攻击惩罚功能前，必须配置该标识。	jssessionid
User标记	用于Params恶意请求的攻击惩罚功能。在选择Params拦截的攻击惩罚功能前，必须配置该标识。	name

步骤7 单击“确定”，完成标记信息配置。

---结束

相关操作

[配置攻击惩罚标准封禁访问者指定时长](#)

7.1.7 配置 Header 字段转发

如果您想通过WAF添加额外的Header头部信息，例如\$request_id让整个链路的请求都可以关联起来，可参考本章节配置字段转发，WAF会将添加的字段插入到Header中，转发给源站。

前提条件

已[添加防护网站](#)且部署模式为“云模式-CNAME接入”或“独享模式”。


约束条件


- 仅“云模式-CNAME接入”和“独享模式”支持配置Header字段转发。
- 支持配置Header字段转发的区域，请参考[功能总览](#)。
- 最多支持配置8个Key/Value值。
- 不支持请求头带“.”转发。
- Value值可以自定义一个字符串，也可以配置为以\$开头的变量。以\$开头的变量仅支持配置如下字段：

```
$time_local  
$request_id  
$connection_requests  
$tenant_id  
$project_id  
$remote_addr  
$remote_port  
$scheme  
$request_method  
$http_host  
$origin_uri  
$request_length  
$ssl_server_name  
$ssl_protocol  
$ssl_curves  
$ssl_session_reused
```

配置 Header 字段转发

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤6 在“字段转发”列，单击“修改”，在弹出的“字段转发”弹框中，输入Key/Value值，并单击“添加”，可添加多个字段。

图 7-8 字段转发



步骤7 确认字段添加完成后，单击“确定”。

----结束

7.1.8 修改拦截返回页面

当访问者触发WAF拦截时，默认返回WAF“系统默认”的拦截返回页面，您也可以根据自己的需要，配置“自定义”或者“重定向”的拦截返回页面。

📖 说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下域名修改拦截返回页面。

前提条件


防护网站已接入WAF


约束条件

- 防护网站部署模式为“云模式-ELB接入”时，不支持“重定向”模板。
- “自定义”的拦截返回页面支持配置text/html、text/xml和application/json三种页面类型的页面内容。
- “重定向”地址的根域名必须和当前被防护的域名（包括泛域名）保持一致。例如，被防护的域名为www.example.com，端口为8080，则重定向URL可设置为“http://www.example.com:8080/error.html”。

修改拦截返回页面

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤6 在“告警页面”所在行的页面模板名称后，单击“修改”，在弹出的“告警页面”对话框中，选择“页面模板”进行配置。

- “页面模板”选择“系统默认”时，默认返回WAF内置的HTTP返回码为418的拦截页面。
- “页面模板”选择“自定义”时，如图7-9所示。
 - HTTP返回码：自定义页面配置的返回码。
 - 响应标头：单击“添加响应标头字段”，可配置响应标头参数及参数值。
 - 页面类型：可选择text/html、text/xml和application/json三种类型。
 - 页面内容：根据选择的“页面类型”配置对应的页面内容。

图 7-9 自定义告警页面



- “页面模板”选择“重定向”时，根据界面提示配置重定向URL。

图 7-10 重定向告警页面



重定向URL的根域名必须和当前被防护的域名（包括泛域名）保持一致。例如，被防护的域名为www.example.com，端口为8080，则重定向URL可设置为“http://www.example.com:8080/error.html”。

步骤7 单击“确定”，告警页面配置成功。

----结束

7.1.9 开启 Cookie 安全属性

当“对外协议”配置为HTTPS时，WAF支持开启“Cookie安全属性”，开启后会将Cookie的HttpOnly和Secure属性设置为true。

Cookie是后端Web Server插入的，可以通过框架配置或set-cookie实现，其中，Cookie中配置Secure，HttpOnly有助于防范XSS等攻击获取Cookie，对于Cookie劫持有一定的防御作用。

Appscan扫描器在扫描网站后发现客户站点没有向扫描请求Cookie中插入HttpOnly Secure等安全配置字段将记录为安全威胁。

前提条件


已[添加防护网站](#)且部署模式为“独享模式”或“云模式-CNAME接入”。


约束条件

- “云模式-ELB接入”不支持该功能。
- “对外协议”包含“HTTP”时，“Cookie安全属性”默认为关闭状态，不支持开启。

开启 Cookie 安全属性

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。


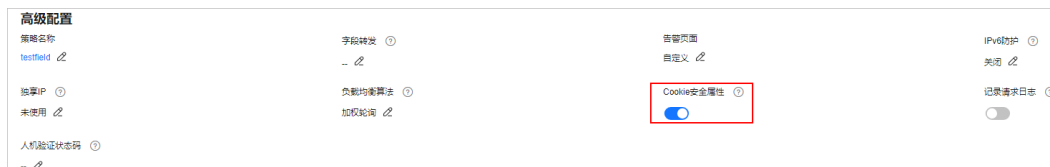
- 步骤4** 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
- 步骤5** 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。
- 步骤6** 在“高级配置”栏中“Cookie安全属性”列单击 ，开启Cookie安全属性

图 7-11 开启 Cookie 安全属性



----结束

7.2 网站管理

7.2.1 查看网站基本信息

您可以通过WAF管理控制台，查看防护域名的对外协议类型、策略名称、告警页面、CNAME、CNAME IP等信息。

前提条件

防护网站已接入WAF

查看网站基本信息



- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击管理控制台左上角的 ，选择区域或项目。
- 步骤3** 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。
- 步骤4** 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
- 步骤5** 查看防护网站信息，参数说明如[表7-6](#)所示。

图 7-12 网站列表

域名	接入模式	接入状态	运行状态(近3天威胁)	证书文件	防护策略	源站IP/端口	创建时间	企业项目	操作
*.com	云模式-CNAME接入 359ca85a9c04c3...	未接入  回源IP地址	未防护 未发现攻击	--	policy_pKj1WW96 已开启防护 	9.80	2024/05/30 16:21...	default	开启防护 Bypass 更多 >
*.com	云模式-CNAME接入 d90f43771a9462f...	未接入  回源IP地址	Bypass 未发现攻击	--	policy_pKj1WW96 已开启防护 	1.80	2024/05/30 16:20...	default	开启防护 防护防护 更多 >

表 7-6 参数说明

参数名称	参数说明
域名	防护的域名或IP。

参数名称	参数说明
接入模式	防护网站的部署模式，包括“云模式-CNAME接入”、“云模式-ELB接入”、和“独享模式”。
接入状态	展示网站接入WAF未完成的步骤或者接入状态。 <ul style="list-style-type: none">“未接入”：网站未接入WAF或者接入不成功。“已接入”：网站接入WAF成功。“DNS解析异常”：“接入模式”为“云模式-CNAME接入”时，当域名未直接解析到WAF（WAF前使用了CDN等代理产品，DNS解析到CDN等代理），且无流量经过WAF。 须知 防护网站“接入模式”为“独享模式”或“云模式-ELB接入”时，防护网站的初始接入状态为“未接入”，当访问请求到达该网站的实例时，该防护网站的接入状态将自动切换为“已接入”。
运行状态/近3天威胁	防护模式及该域名3天内的防护情况。 WAF支持以下几种防护模式： <ul style="list-style-type: none">“防护中”：开启状态。“未防护”：关闭状态。如果大量的正常业务被拦截，比如大量返回418返回码，可以将工作模式切换为“暂停防护”。该模式下，WAF对所有的流量请求只转发不检测。该模式存在风险，建议您优先选择全局白名单规则处理正常业务拦截问题。
证书/套件	绑定该域名的证书及加密套件。单击证书名称，可跳转到“证书管理”页面。
防护策略	显示通过WAF配置的防护策略总数。单击数字可跳转到规则配置页面，配置具体的防护规则，具体的配置方法参见 配置防护策略 。
源站IP/端口	客户端访问的网站服务器的公网IP地址和WAF转发客户端请求到服务器的业务端口。
创建时间	在WAF中添加该网站的时间。
企业项目	该域名所在的企业项目。

步骤6 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤7 查看防护网站的信息，如[图7-13](#)所示。

如果需要修改某项信息，在目标参数所在行，单击编辑按钮进行修改。

图 7-13 查看基本信息



----结束

7.2.2 导出网站设置列表


在Web应用防火墙的网站设置页面，可以导出该账号下添加到WAF的所有网站设置信息。


前提条件

防护网站已接入WAF

导出网站设置列表

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在网站列表的上方，单击“导出”，网站信息列表将导出到本地。

----结束

7.2.3 切换防护模式

网站接入WAF防护后，默认开启WAF防护，WAF会根据您配置的防护策略进行流量检测。如果大量的正常业务被拦截，比如大量返回418返回码，可以暂停防护。暂停防护后，WAF对所有的流量请求只转发不检测，日志也不会记录。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能切换该企业项目下域名的工作模式。

前提条件


防护网站已接入WAF


系统影响

切换为暂停模式后，WAF只转发流量请求，网站安全可能存在风险，建议您优先选择全局白名单规则处理正常业务拦截问题。

切换防护模式（开启防护/暂停防护）

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

- 开启防护：在目标域名所在行的“操作”列，单击“开启防护”并在弹框中单击“确定”。“开启防护”后，该域名的“运行状态”为“防护中”。
- 暂停防护：在目标域名所在行的“操作”列，单击“暂停防护”并在弹框中单击“确定”。“暂停防护”后，该域名的“运行状态”为“未防护”。

----结束

相关操作

- [处理误报事件](#)
- [如何排查404/502/504错误?](#)

7.2.4 修改负载均衡算法

防护网站配置了一个或多个源站地址时，WAF支持配置多源站间的负载均衡算法，WAF支持的算法如下：

- 源IP Hash：将某个IP的请求定向到同一个服务器。
- 加权轮询：所有请求将按权重轮流分配给源站服务器，权重越大，回源到该源站的几率越高。
- Session Hash：将某个Session标识的请求定向到同一个源站服务器，请确保在域名添加完毕后[配置攻击惩罚的流量标识](#)，否则Session Hash配置不生效。

前提条件


[防护网站已接入WAF](#)


约束条件

- 防护网站的部署模式为“云模式-CNAME接入”，而且仅专业版和铂金版支持配置负载均衡算法。
- 支持配置负载均衡算法的区域，请参考[功能总览](#)。

修改负载均衡算法

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤6 在“负载均衡算法”所在行，单击“修改”，在弹出的对话框中，选择“负载均衡算法”并单击“确定”。

----结束

7.2.5 更换网站绑定的防护策略

如果您需要更换网站绑定的防护策略，可参照本章节操作。

前提条件


已[配置防护策略](#)。


约束条件

“云模式-CNAME接入”仅专业版和铂金版支持更换网站绑定的防护策略。

更换网站绑定的防护策略

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤6 在“高级配置”栏的“防护策略”所在列，单击“修改”，在弹出的对话框中，选择防护策略并单击“确定”。

----结束

7.2.6 更新网站绑定的证书

当防护网站的部署模式为“云模式-CNAME接入”或“独享模式”且“对外协议”为“HTTPS”时，您需要上传证书使证书绑定到防护网站。

- 如果您的证书即将到期，为了不影响网站的使用，建议您在到期前重新使用新的证书，并在WAF中同步更新网站绑定的证书。
WAF支持证书过期时发送告警通知，您可以在“告警通知”界面配置证书过期提醒，具体的操作请参见[开启告警通知](#)。
- 如果您需要更新网站绑定证书的信息，可以在WAF中为网站绑定新的证书。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目下的域名更新证书。

前提条件

已[添加防护网站](#)且配置的“对外协议”包含HTTPS。

约束条件


- 域名和证书需要一一对应，泛域名只能使用泛域名证书。如果您没有泛域名证书，只有单域名对应的证书，则只能在WAF中按照单域名的方式逐条添加域名进行防护。
- WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考[步骤6](#)将证书转换为PEM格式，再上传。
- 拥有“SCM Administrator”和“SCM FullAccess”权限的账号才能选择SCM证书。
- 更新证书前，请确认WAF和更新的证书在同一账号下。


系统影响

- 证书过期后，对源站的影响是覆灭性的，比主机崩溃和网站无法访问的影响还要大，且会造成WAF的防护规则不生效，故建议您在证书到期前及时更新证书。
- 更新证书不会影响业务，更换过程中会使用旧证书，更新成功后，自动切为新证书，新证书立刻生效。
- 同时更新后端服务器上的证书配置和WAF域名绑定证书的配置会影响网站访问业务，建议您在业务量少时进行更新。

更新网站绑定的证书

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤6 在证书所在行的证书名称后，单击“修改”，在弹出的“更新证书”对话框中，上传新证书或者选择已有证书。

- “更新方式”选择“添加证书”时，在对话框中输入“证书名称”，并将证书内容和私钥内容粘贴到对应的文本框中。

成功导入的新证书，将添加到“证书管理”页面的证书列表中。有关证书管理的操作，请参见[上传证书](#)。

说明

Web应用防火墙将对私钥进行加密保存，保障证书私钥的安全性。

WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考[表7-7](#)在本地将证书转换为PEM格式，再上传。

表 7-7 证书转换命令

格式类型	转换方式
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。

格式类型	转换方式
PFX	<ul style="list-style-type: none">- 提取私钥命令，以“cert.pfx”转换为“key.pem”为例。 openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes- 提取证书命令，以“cert.pfx”转换为“cert.pem”为例。 openssl pkcs12 -in cert.pfx -nokeys -out cert.pem
P7B	<ol style="list-style-type: none">1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer2. 将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	<ul style="list-style-type: none">- 提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem- 提取证书命令，以“cert.cer”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.cer -out cert.pem

📖 说明

- 执行openssl命令前，请确保本地已安装[openssl](#)。
 - 如果本地为Windows操作系统，请进入“命令提示符”对话框后，再执行证书转换命令。
- “更新方式”选择“选择已有证书”时，在“证书”下拉框中选择已有的证书。

📖 说明

- 如果没有可使用的证书，可单击“购买证书”，购买新的证书并推送到WAF。WAF支持SCM提供的所有证书类型，可参考[SCM概述](#)章节详细了解SSL证书。
- 更新方式选择“SCM证书”时，可选择托管在CCM里证书（已签发或者用户上传的证书）。

⚠️ 注意

选择的SCM证书需要与目标域名匹配，即该证书绑定的域名与添加到WAF的域名一致。

步骤7 单击“确定”，证书更新完成。

----结束

相关操作

[上传证书](#)

7.2.7 修改服务器配置信息

当您以“云模式-CNAME接入”或“独享模式”添加防护网站后，如果需要修改防护网站的服务器信息或者需要添加服务器信息时，可以修改服务器配置信息。

本章节可对以下场景提供指导：

- 修改服务器信息。
 - 云模式-CNAME接入：修改对外协议、源站协议、源站地址、源站端口
 - 独享模式：修改对外协议、源站协议、VPC、源站地址、源站端口
- 添加服务器配置。
- 更新证书，关于证书更新的详细内容可参见[更新网站绑定的证书](#)。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为该企业项目下域名的服务器配置信息。

前提条件

[防护网站已接入WAF](#)

约束条件


- 开启PCI DSS/3DS合规后，将不支持修改“对外协议”，也不支持添加源站地址。
- 同一种接入模式的域名才支持批量修改服务器配置信息。


系统影响

修改服务器配置信息对业务无影响。

修改单个网站的服务器配置信息

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤6 在“源站服务器”栏中，单击“编辑”。

步骤7 在“修改服务器信息”页面，根据需要修改服务器的各项配置以及已绑定的证书。

- 关于证书更新的详细内容可参见[更新网站绑定的证书](#)。
- WAF支持配置多个后端服务器，如果需要增加后端服务器，可单击“添加”，增加服务器。
- 如果需要开启IPv6防护，在“IPv6防护”所在行，单击“开启”。

步骤8 单击“确定”，完成服务器信息修改。

----结束

批量修改网站的源站服务器信息

同一种接入模式的域名支持批量修改服务器配置。

步骤1 在左侧导航栏中，单击“网站设置”，进入“网站设置”页面。

步骤2 批量勾选需要修改服务器配置的域名，在网站列表的上方，单击“批量修改配置”。

步骤3 根据需要修改服务器的各项配置以及已绑定的证书。

WAF支持配置多个后端服务器，如果需要增加后端服务器，可单击“添加地址”，增加服务器。

步骤4 单击“确定”，完成服务器信息修改。

批量修改过程中可能会持续一段时间，请耐心等待。修改成功后会展示修改成功的域名。

----结束

生效条件

修改服务器信息，大约需要2分钟同步生效。

7.2.8 查看防护网站的云监控信息

将防护网站接入WAF后，可查看防护网站的云监控信息。

说明


如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能查看该企业项目下防护网站的云监控信息。


前提条件

防护网站已接入WAF

查看防护网站的云监控信息

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

图 7-14 网站列表



域名	接入模式	接入状态	运行状态(近3天威胁)	证书状态	防护策略	源站IP/端口	创建时间	企业项目	操作
example.com	云模式-CNAME接入 35fca85ae04c3...	未接入  回源IP地址	未防护 未发现攻击	--	policy_pKjWWW6 已开启防护 	9.80	2024/05/30 16:21...	default	开启防护 Bypass 更多 >
example.com	云模式-CNAME接入 659f43771a0942f...	未接入  回源IP地址	防护中 未发现攻击	--	policy_pKjWWW6 已开启防护 	1.1111111111111111:80	2024/05/30 16:20...	default	开启防护 暂停防护 更多 >

步骤5 在目标防护域名所在行的“操作”列中，单击“更多 > 云监控”，跳转到云监控，查看防护网站的云监控信息。

----结束

7.2.9 批量跨企业项目迁移域名

WAF支持将目标企业项目下的域名迁移到其他企业项目下，迁移后，原企业项目下将不再保留已迁移的域名。

证书和策略不会随域名一起迁移，需要为迁移的域名重新适配证书和策略。

前提条件


[防护网站已接入WAF](#)


约束条件

- “云模式”仅专业版、铂金版支持跨企业项目迁移域名。
- “独享模式”网站迁移时，需要保证目的企业项目下已经购买了独享引擎实例。
- 证书和策略不会随域名一起迁移，需要为迁移的域名重新适配证书和策略。

批量跨企业项目迁移域名

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 批量勾选需要迁移的域名，在网站列表的右上角，单击“批量迁域名”。

- “目标企业项目”：选择需要将域名迁移到的新的企业项目。
- “目标策略配置”：当前域名绑定的策略不会一起迁移，需要选择新企业项目下的策略。
- “目标证书名称”：当前域名绑定的证书不会一起迁移，需要选择新企业项目下的证书。

图 7-15 跨企业项目迁域名



---结束

7.2.10 删除防护网站

您可以通过Web应用防火墙服务对不再防护的网站执行删除操作。

删除云模式的CNAME方式接入的防护网站前，请您先到DNS服务商处将域名重新解析，指向源站服务器IP地址，否则该域名的流量将无法切回服务器，影响正常访问。

防护网站删除后，如果需要再次添加到WAF中进行防护，需要重新按照[网站接入WAF](#)的操作完成域名接入。

📖 说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能删除该企业项目下域名。

前提条件

[防护网站已接入WAF](#)

系统影响

- 防护网站“部署模式”为“云模式-CNAME接入”时，如果要删除的防护网站已经接入Web应用防火墙，在删除防护网站前，请您先到DNS服务商处将域名重新解析，指向源站服务器IP地址，否则该域名的流量将无法切回服务器，影响正常访问。
- 勾选“强制删除WAF的接入CNAME”后，WAF不再检测业务域名解析配置，立即删除WAF的CNAME，如果业务域名解析未做修改，可能会导致业务异常。


📖 说明


不勾选“强制删除WAF的接入CNAME”，WAF会将该域名的CNAME保留约30天后再删除该CNAME。

- 删除网站后，1分钟内生效，且不可恢复，请谨慎删除防护网站。

删除防护网站

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标防护域名所在行的“操作”列中，单击“更多 > 删除”，进入删除防护域名对话框界面。

步骤6 在删除防护网站对话框中，确认删除防护网站。

- 云模式
 - 未使用代理

说明

- 确保已完成并勾选“已经在DNS服务商处将域名的CNAME删除并配置A记录到源站地址，或该域名业务已下线”。
- 勾选“强制删除WAF的接入CNAME”后，WAF不再检测业务域名解析配置，立即删除WAF的CNAME，如果业务域名解析未做修改，可能会导致业务异常。
- 如果需要保留该域名绑定的防护策略，可以勾选“保留该域名的防护策略”。

- 使用代理

说明

- 确保已完成并勾选“已经在高防、CDN或云加速等代理处将域名回源到源站，或该域名业务已下线”。
- 勾选“强制删除WAF的接入CNAME”后，WAF不再检测业务域名解析配置，立即删除WAF的CNAME，如果业务域名解析未做修改，可能会导致业务异常。
- 如果需要保留该域名绑定的防护策略，可以勾选“保留该域名的防护策略”。

- 云模式-ELB接入/独享模式
 - 如果需要保留该域名绑定的防护策略，可以勾选“保留该域名的防护策略”。

步骤7 单击“确定”，页面右上角弹出“删除成功”，则说明删除操作成功。

----结束

相关操作

如果您想批量删除域名，批量勾选域名后，在网站列表上方，单击“批量删除”。

8 策略管理

8.1 新增防护策略

防护策略是多种防护规则的合集，用于配置和管理Web基础防护、黑白名单、精准访问防护等防护规则，一条防护策略可以适用于多个防护域名，但一个防护域名只能绑定一个防护策略。该任务指导您通过Web应用防火墙添加防护策略。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，为企业项目添加防护策略。

约束条件

- 云模式入门版和标准版不支持该功能。
- 一个防护域名只能绑定一条防护策略。
- 同一企业项目下支持复制策略。

操作步骤


您可以选择以下两种方式新增防护策略。

添加防护策略

一条防护策略可以适用于多个防护域名，但一个防护域名只能绑定一个防护策略。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 在列表的左上角，单击“添加防护策略”。

步骤6 在弹出的对话框中，输入策略名称，单击“确定”，添加的策略会展示在策略列表中。

步骤7 在目标策略所在行，单击策略名称，进入防护规则配置页面，参见[防护策略](#)为策略添加防护规则。

----结束


复制防护策略


同一企业项目下支持复制策略。

说明

如果本策略的防护规则配置了攻击惩罚，策略复制后，新策略中的相应防护规则的攻击惩罚会被重置为无攻击惩罚，您需重新对该防护规则配置攻击惩罚。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。


步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 在目标策略所在行的“操作”列，单击“更多 > 复制”。

步骤6 在弹出的对话框中，输入新策略名称，并单击“确定”。

----结束

相关操作

- 如果您想修改策略名称，单击目标策略名称后的 ，在弹出的对话框中，重新输入新的策略名称即可。
- 如果您想删除添加的防护策略，在目标策略所在行的“操作”列，单击“更多 > 删除”。
- 如果您想批量删除防护策略，勾选需要删除的策略，单击策略列表上方的“批量删除”。

8.2 添加策略适用的防护域名

您可以通过Web应用防火墙服务添加策略适用的防护域名，添加的域名将从原有策略迁移到当前策略。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目批量添加防护规则。

前提条件


[防护网站已接入WAF](#)


约束条件

云模式入门版和标准版不支持该功能。

添加策略适用的防护域名

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 在目标策略所在行的“操作”列，单击“添加防护域名”。

步骤6 在“防护域名”下拉框中选择适用于该策略的防护域名。

须知

- 一个防护域名有且只能配置一条防护策略。
- 一条防护策略可以适用于多个防护域名。
- 如果想删除已绑定域名的防护策略，请先将此防护策略绑定的所有域名添加到其它防护策略，再在目标策略名称所在行的“操作”列中，单击“更多 > 删除”。

图 8-1 添加策略适用的防护域名



步骤7 单击“确定”。

----结束

8.3 批量添加防护规则

您可以通过Web应用防火墙服务为防护策略批量添加防护规则。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目批量添加防护规则。


约束条件


入门版仅支持批量添加全局白名单规则。

“企业项目”选择“所有项目”时，不支持添加防护规则。

批量添加防护规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 （可选）如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目批量添加防护规则。

须知

“企业项目”选择“所有项目”时，不支持添加防护规则。

步骤6 在策略列表左上方，单击“我的所有策略规则”。

步骤7 在待配置规则列表的左上角，单击“批量添加”，进入对应的规则配置页面。

步骤8 选择策略名称，在“防护策略”的下拉框中选择策略名，可批量多选。

步骤9 完成除“防护策略”以外其它参数的配置。

- “CC攻击防护”请参见[表5-6](#)进行参数配置。
- “精准访问防护”请参见[表5-7](#)进行参数配置。
- “黑白名单设置”请参见[表5-8](#)进行参数配置。
- “地理位置访问控制”请参见[表5-9](#)进行参数配置。
- “网页防篡改”请参见[表5-11](#)进行参数配置。
- “防敏感信息泄露”请参见[表5-14](#)进行参数配置。
- “全局白名单”请参见[表5-15](#)进行参数配置。
- “隐私屏蔽”请参见[表5-16](#)进行参数配置。

步骤10 单击“确定”，批量添加防护规则成功。

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该策略生效，可在目标策略所在行的“操作”列，单击“关闭”，也可以批量勾选多条策略规则，单击列表上方的“批量关闭”，同时关闭多条策略规则。
- 当您需要修改添加的规则时，在待修改的规则所在行，单击“修改”，修改规则，也可以批量勾选不同策略下的多条规则，单击列表上方的“批量修改”，同时修改多条策略规则。

- 当您需要删除添加的规则时，在待删除的规则所在行，单击“删除”，删除规则，也可以批量勾选多条策略规则，单击列表上方的“批量删除”，同时删除多条策略规则。
- 当您需要批量开启策略规则时，批量勾选多条策略规则，单击列表上方的“批量开启”，同时开启多条策略规则。

9 安全报告

WAF可根据您创建的日志报告模板，生成安全日报、周报、月报、或者自定义安全报告统计的时间范围内的报告，并将报告在您设置的报告发送时间段以您配置的接收方式发送给您。

前提条件

防护网站已接入WAF


约束条件

- WAF对创建安全报告模板的配额有限制。
 - 云模式专业版：10个
 - 云模式铂金版、独享模式：20个。
 - 云模式入门版、标准版：5个。
- WAF仅保留6个月的安全报告，建议您定期下载，以满足等保测评以及审计的需要。

创建安全报告模板

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“安全报告”，进入“安全报告”页面。

步骤5 在列表的左上角，单击“创建报告模板”，进入“创建报告模板”页面，参数说明如 [表9-1](#)所示。


图 9-1 创建报告模板

The screenshot shows a configuration interface for creating a report template. It includes the following elements:

- Report Template Name:** A text input field containing 'waf'.
- Report Type:** A set of tabs with '安全日报' (Security Daily Report) selected. Other options are '安全周报' (Security Weekly Report), '安全月报' (Security Monthly Report), and '自定义报告' (Custom Report).
- Reporting Period:** Text indicating '统计周期: 每天00:00:00 ~ 23:59:59' and a note that reports will be sent the day after generation.
- Send Time:** A dropdown menu set to '每天' (Daily) with a time range of '00:00~06:00'.
- Report Reception Method:** Radio buttons for '消息中心' (Message Center), '消息主题' (Message Topic - selected), and '无需发送到邮箱' (No need to send to email).
- Message Topic Selection:** A dropdown menu showing 'report_topic_14188088-f3...' and a '创建消息主题' (Create Message Topic) button.
- Footer Note:** A note stating '下拉框只展示订阅状态为“已确认”的消息通知主题。' (The dropdown only displays message notification topics with a subscription status of 'Confirmed').

表 9-1 创建报告模板参数说明

参数名称	参数说明	取值样例
数据来源	当前报告统计的企业项目范围。	所有项目
报告模板名称	自定义安全报告模板名称。	WAF
报告类型	<ul style="list-style-type: none"> 安全日报 统计周期: 每天00:00:00 ~ 23:59:59 报告将在生成后的次日自动发送至您设置的报告接收人。 安全周报 统计周期: 周一00:00:00 ~ 周日23:59:59 报告将在生成后的次周周一自动发送至您设置的报告接收人。 安全月报 统计周期: 每月1日00:00:00 ~ 31日23:59:59 报告将在生成后的次月1日自动发送至您设置的报告接收人。 自定义报告 自定义日志统计周期。 	安全周报
统计周期	“报告类型”选择“自定义报告”时, 需要配置日志统计周期。	-
发送时间	设置日报发送时间段。 <ul style="list-style-type: none"> 安全日报、安全周报、安全月报: WAF分别在每日、每周一、每月一日的设置时间段内发送WAF防护的日志报告。 自定义报告: 报告生成后自动发送。 	18:00~24:00

参数名称	参数说明	取值样例
报告接收文式	<p>您可以选择以下两种方式接收报告：</p> <ul style="list-style-type: none">“消息中心”：单击界面右上角的，进入消息中心，添加接收人信息。“消息主题”：在下拉列表选择已创建的主题或者单击“创建消息主题”创建新的主题，用于配置接收安全报告的终端。 <p>说明 如果您不希望将报告发送到邮箱，选择“无需发送到邮箱”。</p>	消息主题

步骤6 单击“下一步：设置报告内容”，选择要展示的安全报告内容。

图 9-2 选择报告内容




步骤7 单击“保存报告”，安全报告模板创建完成。


----结束

下载安全报告

WAF仅保留6个月的安全报告，建议您定期下载，以满足等保测评以及审计的需要。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“安全报告”，进入“安全报告”页面。

步骤5 在目标报告模板所在行的“操作”列，单击“下载最新报告”。

----结束

相关操作

- 安全报告模板创建完成后，默认为“已开启”状态，如果您暂时不想使用该模板，在目标报告模板所在行的“操作”列，单击“更多 > 关闭”。
- 删除安全报告模板：在目标报告模板所在行的“操作”列，单击“更多 > 删除”。
- 复制安全报告模板：在目标报告模板所在行的“操作”列，单击“更多 > 复制”。
- 修改安全报告模板：在目标报告模板所在行的“操作”列，单击“编辑”。

10 高阶功能

10.1 配置内容安全检测

Web应用防火墙提供内容安全检测服务，基于丰富的违规样例库和内容审核专家经验，通过机器审核加人工审核结合的方式，帮助您准确检测出Web网站和新媒体平台上的关于涉黄、涉赌、涉毒、暴恐、涉政、惊悚、违禁广告等敏感违规内容，并提供文本内容纠错审校（错别字、生僻字、语法表述不当等有违准确性内容）。并提供专业检测报告助您自纠自查，降低内容违规风险。

说明

使用该功能前，需[提交工单](#)申请开通。

使用须知


- 购买内容安全检测服务后，系统立即执行检测。
- 检测过程中，不支持修改检测域名、暂停任务、退费等操作。
- 确定网站检测配额，请参见[购买内容安全检测服务时，如何确定网站检测配额？](#)。
- “检测类型”选择“内容安全单次检测”时，下单后的7个工作日内出报告。
- “检测类型”选择“文本安全监测”时，下单后的检测周期（1个月）后的7个工作日内出报告。


步骤一：购买内容安全检测

购买内容安全检测，配置“检测类型”和“检测对象”，可对“检测对象”对应的文本类型进行安全检测。

支持批量购买内容安全检测，可一次输入一个或多个“检测对象”进行安全检测。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航栏，选择“高阶功能 > 内容安全检测”，进入“内容安全检测”页面。

步骤5 在页面右上角，单击“购买内容安全检测服务”，进入购买页面，参见表10-1配置相关参数。

图 10-1 购买内容安全检测服务

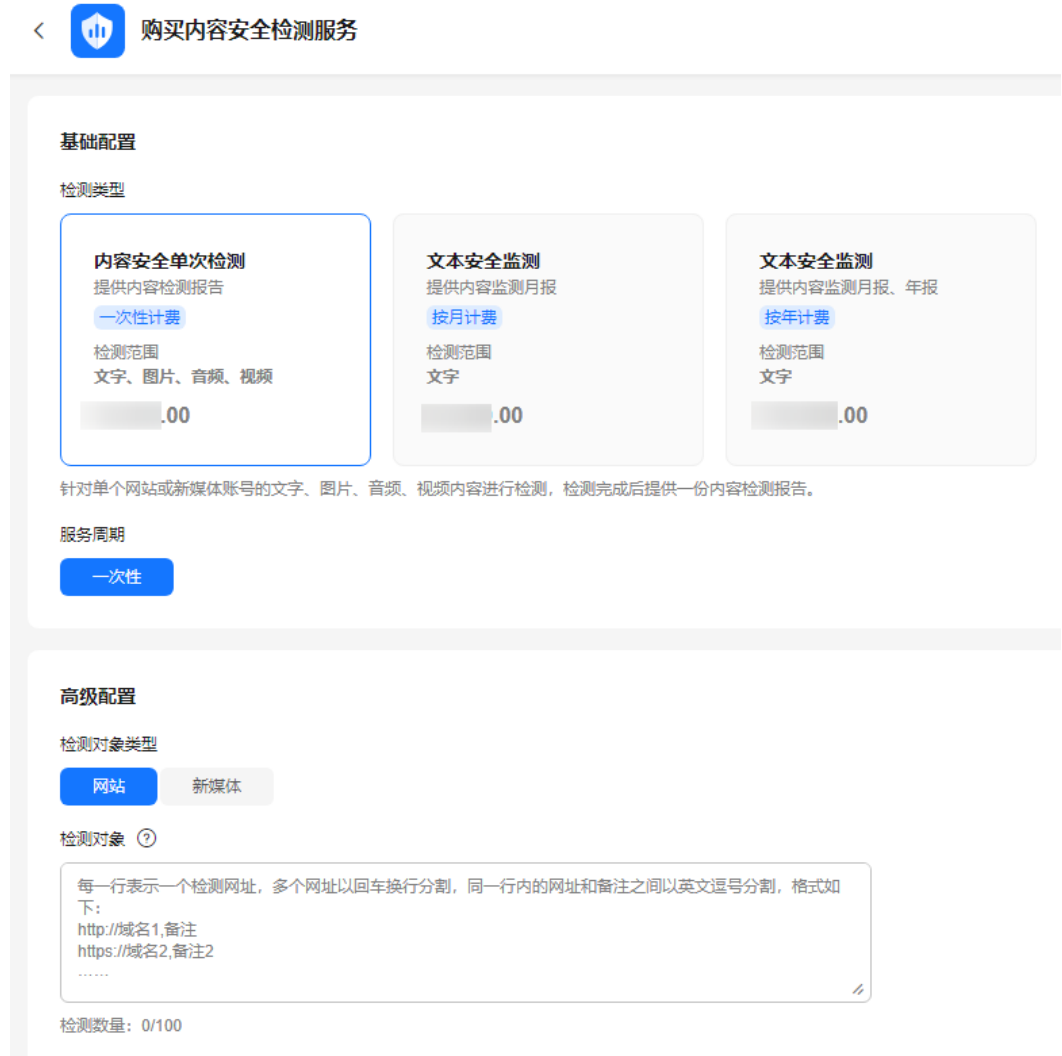


表 10-1 参数说明

参数	说明	示例
检测类型	<ul style="list-style-type: none"> “内容安全单次检测”：针对单个网站或新媒体账号的文字、图片、音频、视频内容进行检测，检测完成后提供一份内容检测报告。 “文本安全监测”（按月）：针对单个网站或新媒体账号的文字内容进行内容安全监测，并在一个自然月后输出内容监测月报。 “文本安全监测”（按年）：针对单个网站或新媒体账号的文字内容进行内容安全监测，并在每一个自然月后输出内容监测月报，一个自然年后输出内容监测年报。 	内容安全单次检测
服务周期	<ul style="list-style-type: none"> “内容安全单次检测”：一次性。 “文本安全监测”（按月）：包周期，“监测时长”可以选择“1个月”、“2个月”、“3个月”。 “文本安全监测”（按年）：包周期，按年计费。 	一次性
检测对象类型	<p>检测对象类型包含：</p> <ul style="list-style-type: none"> “网站”：支持网站内容审查，可根据URL检测网站内容，可自行排查检测站内网页、链接内容，包括文本、图片、音频、视频等。 “新媒体”：支持主流新媒体平台的内容审查，包括文本、图片、音频、视频等。 	新媒体

参数	说明	示例
检测对象	<ul style="list-style-type: none">“检测对象类型”选择“新媒体”时：输入需要检测的账号名称，并备注新媒体平台。 说明 每一行表示一个新媒体账号，多个新媒体账号以回车换行分隔；同一行内的新媒体账号和备注之间以英文逗号分隔，每行最多支持500个英文字符（1个中文字符等于2个英文字符）。“检测对象类型”选择“网站”时：输入被检测网站完整域名与备注信息。 说明 每一行表示一个检测网址，多个网址以回车换行分隔；同一行内的网址和备注之间以英文逗号分隔，如无备注，可只输入网址，每行最多支持500个英文字符（1个中文字符等于2个英文字符）。	<ul style="list-style-type: none">检测对象类型：新媒体检测对象：华为云备注：微博。如果未备注平台名称，默认为微博平台。 或 <ul style="list-style-type: none">检测对象类型：网站检测对象： https:// www.huaweicloud.com备注：华为云官网

步骤6 确认订单详情无误后，单击“立即购买”。

步骤7 确认检测数量，并勾选“我已阅读并同意《云Web应用防火墙免责声明》”。

步骤8 单击“立即购买”，完成付款操作。

----结束

步骤二：下载检测报告

步骤1 在左侧导航栏选择“高阶功能 > 内容安全检测”，进入“内容安全检测”页面。

步骤2 在目标检测对象所在行的“操作”列，单击“下载报告”，可将检测报告下载到本地。

报告中呈现检测出的合规性风险、内容安全风险等相关内容。用户根据报告内容选择整改或者保留。

说明

“检测状态”为“检测完成”时，才支持下载报告。

----结束

其他操作

如果您需要对检测对象进行再次检测时，在该检测对象所在行的“操作”列，单击“复购”。

11 对象管理

11.1 管理证书

11.1.1 上传证书

当防护网站的部署模式为“云模式-CNAME接入”或“独享模式”且“对外协议”为“HTTPS”时，您需要选择证书使证书绑定到防护网站。

将证书上传到WAF，添加防护网站时可直接选择上传到WAF的证书。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，为企业项目上传证书。

前提条件

已获取证书文件和证书私钥信息。

规格限制

WAF支持上传的证书套数和WAF支持防护的域名的个数相同。例如，购买了标准版WAF（支持防护10个域名）、1个独享版WAF（支持防护2,000个域名）和域名扩展包（20个域名），WAF可以防护2,030个域名，则WAF支持上传2,030套证书。

约束条件

- 如果您在SCM管理控制台购买证书并成功推送到WAF，该证书将直接添加到“证书管理”页面的证书列表中，且该证书会统计到创建的证书套数中。有关SCM证书推送到WAF的详细操作，请参见[推送证书到云产品](#)。

须知

目前华为云SCM证书只能推送到“default”企业项目下。如果您使用其他企业项目，则不能选择使用SCM推送的SSL证书。

表 11-1 证书转换命令

格式类型	转换方式
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	<ul style="list-style-type: none">提取私钥命令，以“cert.pfx”转换为“key.pem”为例。 openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes提取证书命令，以“cert.pfx”转换为“cert.pem”为例。 openssl pkcs12 -in cert.pfx -nokeys -out cert.pem
P7B	<ol style="list-style-type: none">证书转换，以“cert.p7b”转换为“cert.cer”为例。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	<ul style="list-style-type: none">提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem提取证书命令，以“cert.cer”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.cer -out cert.pem

📖 说明

- 执行openssl命令前，请确保本地已安装**openssl**。
- 如果本地为Windows操作系统，请进入“命令提示符”对话框后，再执行证书转换命令。


步骤7 单击“确定”，证书创建成功。

----结束

生效条件

成功创建的证书将显示在证书列表中。

相关操作

- 当鼠标移到目标证书的名称后时，单击，您可以修改证书的名称。

须知

如果证书正在使用中，请先解除域名和证书的绑定关系，否则无法修改证书名称。

- 在目标证书所在行的“操作”列中，单击“查看”，您可以查看证书的证书文件和证书私钥信息。
- 在目标证书所在行的“操作”列中，单击“应用”，您可以将证书绑定到对应的域名。
- 在目标证书所在行的“操作”列中，单击“更多 > 删除”，您可以删除该证书。

- 在目标证书所在行的“操作”列中，单击“更多 > 更新”，您可以重新更新该域名绑定的证书。
- 在目标证书所在行的“操作”列中，单击“更多 > 共享”，您可以将证书共享给其他企业项目使用。
- 在目标证书所在行的“操作”列中，单击“更多 > 停止共享”，您可以将证书取消共享给其他企业项目使用。

11.1.2 绑定证书到防护网站

当您的防护网站“对外协议”为“HTTPS”时，您可以将上传的证书绑定到防护网站。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，为企业项目绑定证书到防护网站。

前提条件

- 证书未到期。
- 防护网站的“对外协议”使用了HTTPS协议。

约束条件


- 同一证书可以绑定多个防护网站。
- 同一防护网站只能绑定一个证书。


应用场景

当域名的“对外协议”设置为“HTTPS”时，需要配置证书。

绑定证书到防护网站

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“对象管理 > 证书管理”，进入“证书管理”页面。

步骤5 在目标证书所在行的“操作”列中，单击“应用”。

步骤6 在弹出的“应用域名”对话框中，选择应用该证书的防护网站。


步骤7 单击“确定”，将证书绑定到防护网站。

----结束

生效条件

证书的“应用域名”列显示已应用该证书的防护网站。

相关操作

- 当鼠标移到目标证书的名称后时，单击，您可以修改证书的名称。

须知

如果证书正在使用中，请先解除域名和证书的绑定关系，否则无法修改证书名称。

- 在目标证书所在行的“操作”列中，单击“查看”，您可以查看证书的证书文件和证书私钥信息。
- 在目标证书所在行的“操作”列中，单击“更多 > 删除”，您可以删除该证书。
- 在目标证书所在行的“操作”列中，单击“更多 > 更新”，您可以重新更新该域名绑定的证书。
- 在目标证书所在行的“操作”列中，单击“更多 > 共享”，您可以将证书共享给其他企业项目使用。
- 在目标证书所在行的“操作”列中，单击“更多 > 停止共享”，您可以将证书取消共享给其他企业项目使用。

11.1.3 查看证书信息

您可以查看证书的名称、绑定的域名和到期时间等详细信息。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目下的证书信息。

前提条件


已有华为云CCM证书或在WAF上[上传了证书](#)。


约束条件

- 在“系统管理 > 告警通知”页面配置证书到期通知，才能在证书到期前收到告警提醒。
- “证书来源”为“SCM”，即添加防护网站或更新证书时，同步的SCM证书，仅支持“应用”和“删除”操作。

查看证书信息

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“对象管理 > 证书管理”，进入“证书管理”页面。

步骤5 查看证书信息，相关参数说明如[表11-2](#)所示。

图 11-2 证书列表


名称	证书类型	到期时间	应用域名	证书来源	共享状态	企业项目	操作
scm-3120a5	国际证书	2025-05-15 07:59:59 GMT+08:00 ● 正常使用	dcm.com cootest.com	SCM	未共享	default	应用 删除
hyjdfsa	国际证书	2024-05-17 10:54:30 GMT+08:00 ● 正常使用	vip.1.com 1.2	WAF	未共享	default	查看 应用 更多

表 11-2 证书参数说明

参数名称	参数说明
名称	证书名称。
证书类型	仅支持“国际证书”。
到期时间	证书到期时间。 证书过期后，对源站的影响是覆灭性的，比主机崩溃和网站无法访问的影响还要大，且会造成WAF的防护规则不生效，建议您在证书到期前及时更新证书。有关更新证书的详细操作，请参见 更新网站绑定的证书 。
应用域名	已使用该证书的域名。域名与证书是一一对应的，同一个证书可以绑定到多个域名。
证书来源	<ul style="list-style-type: none"> WAF：通过WAF控制台添加的证书。 SCM：添加域名或更新证书时，拉取的SCM证书。该来源的证书仅支持“应用”和“删除”操作。
企业项目	该证书在哪个企业项目下。
共享状态	该证书是否已共享给其他企业项目使用。 <ul style="list-style-type: none"> 已共享给其它企业项目 未共享

----结束

相关操作

- 当鼠标移到目标证书的名称后时，单击 ，您可以修改证书的名称。

须知

如果证书正在使用中，请先解除域名和证书的绑定关系，否则无法修改证书名称。

- 在目标证书所在行的“操作”列中，单击“查看”，您可以查看证书的证书文件和证书私钥信息。
- 在目标证书所在行的“操作”列中，单击“应用”，您可以将证书绑定到对应的域名。

- 在目标证书所在行的“操作”列中，单击“更多 > 删除”，您可以删除该证书。
- 在目标证书所在行的“操作”列中，单击“更多 > 更新”，您可以重新更新该域名绑定的证书。
- 在目标证书所在行的“操作”列中，单击“更多 > 共享”，您可以将证书共享给其他企业项目使用。
- 在目标证书所在行的“操作”列中，单击“更多 > 停止共享”，您可以将证书取消共享给其他企业项目使用。

11.1.4 共享企业项目证书

如果您需要将该项目下的证书共享给其他企业项目使用，可参照本章节操作。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目下的证书信息。

前提条件


已在WAF控制台[上传证书](#)。


约束条件

通过CCM推送的SCM证书不支持企业项目内共享。

共享企业项目证书

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。


步骤4 在左侧导航树中，选择“对象管理 > 证书管理”，进入“证书管理”页面。

步骤5 在目标证书所在列的“操作”列，单击“更多 > 共享”。

步骤6 在弹出的对话框中，选择企业项目，并单击“确定”。

----结束

相关操作

- 当鼠标移到目标证书的名称后时，单击，您可以修改证书的名称。

须知

如果证书正在使用中，请先解除域名和证书的绑定关系，否则无法修改证书名称。

- 在目标证书所在行的“操作”列中，单击“查看”，您可以查看证书的证书文件和证书私钥信息。

- 在目标证书所在行的“操作”列中，单击“应用”，您可以将证书绑定到对应的域名。
- 在目标证书所在行的“操作”列中，单击“更多 > 删除”，您可以删除该证书。
- 在目标证书所在行的“操作”列中，单击“更多 > 更新”，您可以重新更新该域名绑定的证书。
- 在目标证书所在行的“操作”列中，单击“更多 > 停止共享”，您可以将证书取消共享给其他企业项目使用。

11.1.5 删除证书

当证书过期或证书无效时，您可以删除该证书。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能删除该企业项目下的证书。

前提条件

证书没有被使用，即证书未绑定防护网站。

约束条件


如果证书已绑定防护网站，删除证书前需要解除该证书与域名绑定关系。


系统影响

- 删除证书不会影响业务。
- 证书删除后不可恢复，请谨慎删除证书。

删除证书

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“对象管理 > 证书管理”，进入“证书管理”页面。

步骤5 在目标证书所在行的“操作”列中，单击“更多 > 删除”。

步骤6 在弹出的提示框中，单击“确定”，删除证书。


---结束

相关操作

如果证书已绑定防护网站，删除证书前需要解除该证书与域名绑定关系。

请参考以下操作步骤，解除证书与域名绑定关系。

步骤1 在目标证书所在行的“应用域名”列中，单击防护域名，进入域名基本信息页面。

步骤2 在“证书名称”后单击，在弹出的对话框中，上传新证书或者选择其他已有证书。

----结束

11.2 管理黑白名单 IP 地址组

11.2.1 添加黑白名单 IP 地址组

IP地址组集中管理IP地址或网段，被黑白名单规则引用时可以批量设置IP/IP地址段。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，为企业项目添加IP/IP段地址组。

前提条件

[已成功购买WAF](#)。

约束条件


- 云模式仅专业版和铂金版支持IPv6地址/IPv6地址段。
- 如果独享模式/云模式-ELB接入所在的ELB支持IPv6，独享模式/云模式-ELB接入也支持IPv6地址/IPv6地址段。
- 添加地址组前，请确保当前版本有剩余的IP黑白名单规则配额。


说明

- 您可以参见[配置IP黑白名单规则拦截/放行指定IP](#)，查看当前IP黑白名单规则配额。有关各版本规格的详细介绍，请参见[服务版本差异](#)。
- 如果您购买了云模式，当前版本的IP黑白名单防护规则条数不能满足要求时，您可以通过购买规则扩展包或升级云模式版本增加IP黑白名单防护规则条数，以满足的防护配置需求。一个规则扩展包包含10条IP黑白名单防护规则。有关升级规则的详细操作，请参见[升级WAF云模式版本和规格](#)。

添加黑白名单 IP 地址组

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“对象管理 > 地址组管理”，进入“地址组管理”页面。

步骤5 选择“我的地址组”页签，进入地址组页面。

步骤6 在地址组列表左上方，单击“添加地址组”。

步骤7 在弹出的“添加地址组”对话框中，输入“地址组名称”和“IP/IP段”。

步骤8 单击“确定”，地址组创建成功。

----结束

11.2.2 修改或删除黑白名单 IP 地址组

您可以通过修改或删除IP地址，管理IP地址组信息。

说明


如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能修改或删除该企业项目下的地址组。


约束条件

如果地址组已被黑白名单规则引用，删除地址组前需要解除该地址组与黑白名单规则的绑定关系。

修改或删除黑白名单 IP 地址组

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。


步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“对象管理 > 地址组管理”，进入“地址组管理”页面。

步骤5 选择“我的地址组”页签，进入地址组页面。

步骤6 在地址组列表中，查看地址组信息。

表 11-3 参数说明

参数名称	参数说明
地址组名称	用户自定义的地址组名称。 单击地址组名称后的  ，可修改地址组名称。
IP/IP段数量	地址组添加的IP地址/IP地址段数量。
应用规则	引用地址组的防护规则。
描述	地址组补充信息。

步骤7 修改或删除IP地址组。

- 修改IP/IP段

在目标地址组所在行的“操作”列中，单击“修改IP/IP段”，在弹出的对话框中，添加新的IP/IP段后单击“添加到列表”，也可在列表中单击“删除”，移除IP/IP段。

- 删除地址组

在目标地址组所在行的“操作”列中，单击“删除”，在弹出的提示框中，单击“确定”。

----结束

12 系统管理

12.1 管理独享引擎

创建WAF独享引擎实例后，您可以查看实例信息、查看实例的监控信息、升级实例版本以及删除实例。

说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能管理该企业项目下的独享引擎。

前提条件

- [已购买独享引擎实例](#)。
- 登录账号已授予“IAM ReadOnly”权限。

独享引擎版本迭代

在目标独享引擎实例列表中的“版本”列可查看WAF实例版本。

表 12-1 独享引擎版本


引擎版本	特性
202412	<ul style="list-style-type: none">• 地理位置防护支持IPv6。• WAF支持自研BOT能力。• 支持转发自定义响应头。• 修复已知问题。
202410	<ul style="list-style-type: none">• 自定义拦截页面支持自定义响应头。• 引擎增加对TOA字段的获取及处置能力。
202408	修复已知问题。


引擎版本	特性
202407	<ul style="list-style-type: none"> ● 精准防护规则支持深度解码。 ● 修复已知问题。
202405	<ul style="list-style-type: none"> ● 支持健康检查接口 “health-check”。 ● 支持检测非法的Cookie字符串。 ● CC攻击防护规则中“防护动作”支持“JS挑战”。 ● 精准访问防护规则中支持“已知特征爬虫”条件。 ● 精准访问防护规则中支持配置“生效模式”。 ● 用户可配置仅记录异常响应码（4xx 和 5xx）的请求日志，开关为 upstream.extend.only_log_abnormal_status。 ● 独享模式下“X-Real-IP”和“X-Hwwaf-Real-IP”默认值从“\$remote_addr”恢复为“\$client_ip”。
202312	<ul style="list-style-type: none"> ● 支持用户配置“不检测非法请求”的全局白名单。 ● JS反爬虫可单独设定动作，支持拦截、仅记录以及人机验证。
202308	<ul style="list-style-type: none"> ● IP标识增加\$remote_addr，可直接取TCP连接IP。 ● CC、精准防护、黑白名单支持使用TCP连接IP。 ● 支持CC人机验证锁定时长。
202305	<ul style="list-style-type: none"> ● HTTP2全局开启，不需要手动开启。 ● 默认支持流量可通过四次WAF，如果回源还是失败，会返回523错误码。 ● 支持multipart严格格式校验。 ● 支持独享型-网络型规格ELB实例（历史版本仅支持共享型ELB、独享型-应用型ELB实例）。
202211	<ul style="list-style-type: none"> ● 命中内置规则后攻击日志（hit_data）增加内置标签信息。 ● CC规则支持目的限速和响应码条件。
202209	<ul style="list-style-type: none"> ● 支持TLS v1.3。 ● 支持IDC检测功能。 ● 新增多种类型的攻击数据统计至心跳日志。 ● 增加 300 个 HTTPS 端口：60700-60999。
202207	<ul style="list-style-type: none"> ● 支持泛域名标准匹配逻辑。 ● 支持全局白名单功能。
202205	新增基于实例配置TLS最低版本的功能。

引擎版本	特性
202204	<ul style="list-style-type: none"> 支持从管理面下发更新规则。 误报屏蔽支持全流量域名及全流量自定义域名。 误报屏蔽支持配置所有条件。
202202	优化请求日志机制。
202201	优化部分正则匹配机制。
202111	<ul style="list-style-type: none"> 敏感信息泄露规则增加仅记录模式。 新增非法请求类的攻击日志。 精准防护IP条件支持全匹配XFF请求头内所有IP（仅限IPv4）。 新增按域名设置超时时间功能。 优化部分功能。
202110	提升部分功能的性能。
202109	<ul style="list-style-type: none"> 支持对“request body”的精准防护。 精准防护支持正则匹配功能、全部子字段选择。 部分日志支持对接到 LTS 服务。
202106	<ul style="list-style-type: none"> HTTPS 端口支持 HTTP/2 协议。 在请求日志（access log）中增加“region ID”。 在攻击日志中增加“region ID”和引擎 IP。

查看独享引擎实例信息

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”，进入“安全总览”页面。

步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

图 12-1 独享引擎列表



实例名	运行状态	所属区域	VPC	子网	IP地址	拥有人	版本	模式	规格	计费模式	操作
hnp-yc011 10717ea98824248977a2187bae80e7	运行中	华东云	vpc-b90-waf-test	subnet-b90c	192.168.10.224 (...)	未输入	202309	标准模式 (定向代理)	V6-100 x7.large.4	按量计费	云链接 升级 更多
hnp-ey-012 59f128784e5e4f6b913c79683206c824	运行中	华东云	vpc-b90-waf-test	subnet-b90c	192.168.10.183 (...)	未输入	202309	标准模式 (定向代理)	V6-100 x7.large.4	按量计费	云链接 升级 更多

步骤5 查看独享引擎实例信息，如表12-2所示。

表 12-2 独享引擎实例关键参数说明


参数	说明	示例
实例名	创建实例时自动生成的名称。	-
防护网站	实例当前防护的网站。	www.example.com
VPC	实例所在的VPC。	vpc-waf
子网	实例所在的子网。	subnet-62bb
IP地址	实例所在业务VPC的子网IP地址。	192.168.0.186
接入状态	实例的接入状态。	已接入
运行状态	实例的运行状态。	运行中
版本	独享引擎版本。	202304
模式	实例的部署模式。	标准模式(反向代理)
规格	实例的资源规格。	8vCPUs 16GB


----结束

查看独享实例的云监控信息

当实例的“运行状态”为“运行中”时，您可以查看实例的云监控信息。

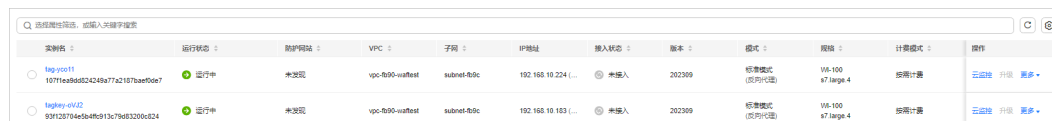
步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”，进入“安全总览”页面。

步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

图 12-2 独享引擎列表



实例名	运行状态	部署模式	VPC	子网	IP地址	接入状态	版本	模式	规格	计费模式	操作
hxy-v011 10716a868524249477a2187baef06a7	运行中	标准	vpc-890-waf-test	subnet-890c	192.168.10.224 [...]	未接入	202309	标准模式 (反向代理)	V6-100 a7.large.4	按量计费	云监控 升级 更多+
hxy-v012 83f128794e5848f913c796832006824	运行中	标准	vpc-890-waf-test	subnet-890c	192.168.10.183 [...]	未接入	202309	标准模式 (反向代理)	V6-100 a7.large.4	按量计费	云监控 升级 更多+

步骤5 在目标实例所在行的“操作”列，单击“云监控”，跳转到云监控，查看实例的CPU、内存、带宽等监控信息。

----结束

升级独享引擎实例版本

当实例的“运行状态”为“运行中”时，您可以通过升级操作，将WAF独享引擎实例升级到最新版本。根据独享引擎实例个数不同选择不同升级方法：

单独享引擎实例节点升级

如果您的业务只部署了一个独享引擎实例，请参照以下操作升级实例。

步骤1 建议申请一个新的独享引擎实例。

- 新申请的独享引擎实例为最新版本。当实例为最新版本时，“升级”按钮为灰化状态。
- 确保新申请的实例，虚拟私有云，子网，安全组等配置，与原实例一致。在这些参数都一致的情况下，新实例会自动同步原实例的所有WAF防护配置。

步骤2 在原独享引擎实例所属VPC下的任一ECS上，执行curl命令，验证业务是否正常。

- HTTP业务
`curl http://WAF独享引擎实例IP.业务端口 -H "host: 业务域名" -H "User-Agent: Test"`
- HTTPS业务
`curl https://WAF独享引擎实例IP.业务端口 -H "host: 业务域名" -H "User-Agent: Test"`

检查业务是否正常，如果业务正常，请执行**步骤3**；如果业务异常，请参照[域名/IP接入状态显示“未接入”，如何处理？](#)和[如何排查404/502/504错误](#)排查故障后，再执行**步骤3**。


📖 说明

执行curl命令的主机需要满足以下条件：

- 网络通信正常。
- 已安装curl命令。Windows操作系统的主机需要手动安装curl，其他操作系统自带curl。

步骤3 将新购买的独享引擎实例添加到ELB的后端服务器上。

以添加共享型后端服务器为例说明，添加后端服务器操作步骤如下。

1. 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙”，进入“安全总览”页面。
2. 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。
3. 在目标实例所在行的“操作”列，单击“更多 > 添加到ELB”。
4. 在“添加到ELB”页面中，选择原独享引擎实例配置的“ELB（负载均衡器）”、“ELB监听器”和“后端服务器组”。
5. 单击“确定”，为WAF实例配置业务端口，“业务端口”需要配置为原WAF独享引擎实例实际监听的业务端口。

步骤4 参见[修改后端云服务器权重](#)，在ELB管理控制台上，将原独享引擎实例的流量权重设置为“0”。

新的请求不会转发到权重为0的后端。

步骤5 待业务流量降下来后，删除原独享引擎实例。

[查看独享实例的云监控信息](#)，“新建连接数”较小时（例如，小于5），说明业务流量已经降下来。

1. 在WAF控制台的左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

2. 在目标实例所在行的“操作”列，单击“更多 > 删除”。
3. 在弹出的提示框中，单击“确定”。
删除实例后，该实例上的资源将被释放且不可恢复。

----结束

多独享引擎实例节点升级

如果您的业务部署了多个独享引擎实例，请参照以下操作升级实例。

步骤1 参见[修改后端云服务器权重](#)，在ELB管理控制台上，记录任一独享引擎实例的流量权重后，将该实例的流量权重设置为“0”。

新的请求不会转发到权重为0的后端。

步骤2 待业务流量降下来后，升级独享引擎实例版本。

[查看独享实例的云监控信息](#)，“新建连接数”较小时（例如，小于5），说明业务流量已经降下来。

1. 在WAF控制台的左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。
2. 在目标实例所在行的“操作”列，单击“升级”。
3. 在弹出的对话框中，确认并勾选业务已满足提示框中所描述的相关配置后，单击“确定”，升级实例版本。

升级大约需要5分钟。

步骤3 在独享引擎实例所属VPC下的任一ECS上，执行curl命令，验证业务是否正常。

- HTTP业务

```
curl http://WAF独享引擎实例IP.业务端口 -H "host: 业务域名" -H "User-Agent: Test"
```

- HTTPS业务

```
curl https://WAF独享引擎实例IP.业务端口 -H "host: 业务域名" -H "User-Agent: Test"
```

检查业务是否正常，如果业务正常，请执行[步骤4](#)；如果业务异常，请参照[域名/IP接入状态显示“未接入”，如何处理？](#)和[如何排查404/502/504错误](#)排查故障后，再执行[步骤4](#)。

说明

执行curl命令的主机需要满足以下条件：

- 网络通信正常。
- 已安装curl命令。Windows操作系统的主机需要手动安装[curl](#)，其他操作系统自带curl。

步骤4 参见[修改后端云服务器权重](#)，在ELB管理控制台上，将引擎实例的流量权重从0调整为[步骤1](#)中记录的原值。


步骤5 参照[步骤1~步骤4](#)，分别对其他独享引擎实例节点执行升级操作。


----结束

回退独享引擎实例版本

仅支持回退到升级前的版本。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”，进入“安全总览”页面。

步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

步骤5 在目标实例所在行的“操作”列，单击“更多 > 回退”。

步骤6 在弹出的对话框中，确认满足并勾选以下三个条件后单击“确定”。

必须满足以下条件，才支持回退实例：


- 实例所在的ELB后端服务器组中存在多个活动实例，或该实例未接入业务。
- ELB已开启HTTP/HTTPS健康检查。
- ELB已关闭会话保持。


----结束

切换独享引擎实例安全组

当“实例类别”为“资源租户类”时，您可以切换独享引擎所属的安全组。切换安全组后，实例将受到该安全组访问规则的保护。

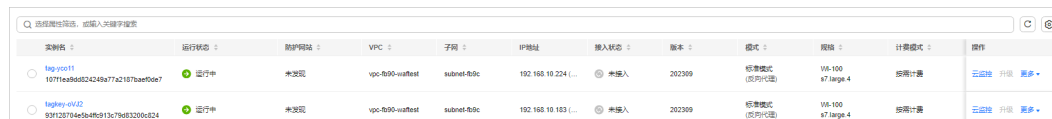
步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”，进入“安全总览”页面。

步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

图 12-3 独享引擎列表



实例名	运行状态	防护策略	VPC	子网	IP地址	接入状态	版本	模式	规格	计费模式	操作
hgw-vc011 10711ea9d8024249a77a2107bae00e7	运行中	未绑定	vpc-b90-ua8eat	subnet-b90c	192.168.10.224	未接入	202309	标准模式 (应用代理)	V6-100 e7.large.4	按量计费	云监控 升级 更多
hgw-vc012 93f128764e58a8f6913c796832006214	运行中	未绑定	vpc-b90-ua8eat	subnet-b90c	192.168.10.183	未接入	202309	标准模式 (应用代理)	V6-100 e7.large.4	按量计费	云监控 升级 更多

步骤5 在目标实例所在行的“操作”列，单击“更多 > 切换安全组”。

步骤6 在弹出的对话框中，选择目标安全组后，单击“确定”，切换独享引擎实例安全组。

----结束


删除独享引擎实例


当您不需要使用独享引擎实例时，您可以删除实例，删除实例时将结束计费。

须知

删除实例后，该实例上的资源将被释放且不可恢复，请谨慎操作。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”，进入“安全总览”页面。

步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

图 12-4 独享引擎列表

实例名称	运行状态	账户名称	VPC	子网	IP地址	接入状态	版本	模式	规格	计费模式	操作
hgw-cc011 1071ea96824249a77a2157bae05a7	运行中	未绑定	vpc-b95-va-test	subnet-b9c	192.168.10.224(L...)	未接入	202309	经典模式 (原计划)	V6-100 s7.large.4	按量计费	云监控 升级 更多
hgw-ey-0VJ2 93f128704e5e486913c79683206e824	运行中	未绑定	vpc-b95-va-test	subnet-b9c	192.168.10.183(L...)	未接入	202309	经典模式 (原计划)	V6-100 s7.large.4	按量计费	云监控 升级 更多

步骤5 在目标实例所在行的“操作”列，单击“更多 > 删除”。

步骤6 在弹出的对话框中，输入“DELETE”后单击“确定”。

----结束

12.2 查看产品信息

您可以在产品信息界面查看WAF产品信息，包括购买的WAF版本、域名规格等信息。

说明


如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目的产品信息。

前提条件

已成功购买WAF。

查看产品信息

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤3 在左侧导航树中，选择“系统管理 > 产品信息”，进入“产品信息”页面。

步骤4 在“产品信息”界面，查看WAF版本、产品规格、到期时间等信息。

- 单击“规格详情”，可以查看当前WAF版本的详细规格信息。
- 如果产品版本已到期，可单击“续费”，完成续费操作。
- 在云模式配置框中，单击“规格变更”可变更云模式版本或购买扩展包。

- 在订单信息列，单击“退订”，可退订购买的资源。
- 服务到期后，在订单信息列，单击“释放”，可释放“已过期”的资源。更多了解请参见[释放资源](#)。

----结束

12.3 变更 WAF 云模式版本和规格

购买了WAF云模式后，您可以变更服务版本和扩展包数量，即可以升级或者降低WAF的版本，也可增加或者退订多余的域名扩展包、QPS扩展包、规则扩展包的数量。

前提条件

- 已获取管理控制台的登录账号（拥有WAF Administrator与BSS Administrator权限）与密码。
- [已购买任一版本的云模式WAF](#)。

规格限制

- 入门版不支持购买扩展包，需要升级到标准版或更高版本才能购买。
- 变更规格不改变计费模式与到期时间。
- 一个域名扩展包支持10个域名。
- 一个QPS扩展包的QPS限制和带宽限制：
 - 对于部署在华为云的Web应用
业务带宽：50Mbit/s
每秒钟的请求量：1000QPS（Queries Per Second，例如一个HTTP GET请求就是一个Query）
 - 对于未部署在华为云的Web应用
业务带宽：20Mbit/s
每秒钟的请求量：1000QPS（Queries Per Second，例如一个HTTP GET请求就是一个Query）
- 一个规则扩展包包含10条IP黑白名单防护规则。

约束条件

- 已到期的服务版本，不支持变更规格，请先完成续费再变更规格。
- 已使用仅该服务版本支持的相关功能或者防护域名数、QPS或IP黑白名单防护规则数没有多余时，不支持降低服务版本，域名扩展包、QPS扩展包、规则扩展包的数量。

应用场景


- **场景一：**当前云模式版本不支持相关功能，或者防护域名数、QPS或IP黑白名单防护规则不能满足业务需求时，可使用该功能升级服务规格。有关各服务支持的功能特性说明，请参见[服务版本差异](#)。
- **场景二：**购买的云模式版本过高，或者域名扩展包、QPS扩展包、规则扩展包的数量过剩时，可使用该功能降低服务版本，或者退订多余的域名扩展包、QPS扩展包、规则扩展包。


系统影响

变更服务版本和扩展包（域名扩展包、QPS扩展包、规则扩展包）时，对已防护的网站业务没有任何影响。

变更云模式版本

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航栏中，选择“系统管理 > 产品信息”，进入产品信息页面。

步骤5 单击“规格变更”，进入“变更Web应用防火墙规格”页面。

- **变更版本：**在“版本”所在行的“变更详情”列，单击“变更版本”，选择规格版本并单击“确定”。
- **计费信息：**变更规格不改变计费模式与到期时间。

步骤6 在页面右下角，单击“下一步”。

步骤7 确认订单详情无误并阅读《Web应用防火墙免责声明》后，勾选“我已阅读并同意《Web应用防火墙免责声明》”，单击“去支付”，完成购买操作。

步骤8 进入“付款”页面，选择付款或退款方式进行付款或退款。

----结束


变更扩展包规格


WAF支持增减域名扩展包、QPS扩展包、规则扩展包的数量。

变更域名扩展包规格

本章节为您讲解如何增减域名扩展包数量。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航栏中，选择“系统管理 > 产品信息”，进入产品信息页面。

步骤5 在“域名扩展包”列，单击“购买扩展包”。

步骤6 在“变更详情”列，增加或减少扩展包数量。

步骤7 在页面右下角，单击“下一步”。

步骤8 确认订单详情无误并阅读《Web应用防火墙免责声明》后，勾选“我已阅读并同意《Web应用防火墙免责声明》”，单击“去支付”，完成购买操作。


步骤9 进入“付款”页面，选择付款或退款方式进行付款或退款。


----结束

变更 QPS 扩展包数量

本章节为您讲解如何增减QPS扩展包数量。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航栏中，选择“系统管理 > 产品信息”，进入产品信息页面。

步骤5 在“QPS扩展包”列，单击“购买扩展包”。

步骤6 在“变更详情”列，增加或减少扩展包数量。

步骤7 在页面右下角，单击“下一步”。

步骤8 确认订单详情无误并阅读《Web应用防火墙免责声明》后，勾选“我已阅读并同意《Web应用防火墙免责声明》”，单击“去支付”，完成购买操作。

步骤9 进入“付款”页面，选择付款或退款方式进行付款或退款。


----结束

变更规则扩展包数量

本章节为您讲解如何增减规则扩展包数量。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航栏中，选择“系统管理 > 产品信息”，进入产品信息页面。

步骤5 在“规则扩展包”列，单击“购买扩展包”。

步骤6 在“变更详情”列，增加或减少扩展包数量。

步骤7 在页面右下角，单击“下一步”。

步骤8 确认订单详情无误并阅读《Web应用防火墙免责声明》后，勾选“我已阅读并同意《Web应用防火墙免责声明》”，单击“去支付”，完成购买操作。

步骤9 进入“付款”页面，选择付款或退款方式进行付款或退款。

----结束

12.4 开启告警通知

通过对攻击日志进行通知设置，WAF可将仅记录和拦截的攻击日志通过用户设置的接收通知方式（例如邮件或短信）发送给用户。

同时，您也可以配置证书到期通知，证书即将到期时，WAF将通过用户设置的接收通知方式（例如邮件或短信）通知用户。

说明


- 消息通知服务为付费服务，价格详情请参见[SMN价格详情](#)。
- 在设置告警通知前，建议您先在“消息通知服务”中创建“消息主题”。


约束条件

- 仅“云模式-CNAME接入”和“独享模式”支持配置证书告警通知，而且“云模式-CNAME接入”仅专业版和铂金版支持。
- 需要依赖消息通知服务，该服务按实际用量付费，详见[SMN计费说明](#)。
- 在设置时间间隔内，当攻击次数大于或等于您设置的阈值时才会发送告警通知。
- 同一企业项目内，同一类型的告警通知仅支持配置一个。

开启告警通知

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“系统管理 > 告警通知”，进入“告警通知”页面。

步骤5 单击“添加通知”，配置告警通知参数，参数说明如[表12-3](#)。

图 12-5 添加通知

添加通知
✕

通知类型 防护事件 证书到期

通知名称

企业项目 所有项目 ▼

通知群组 waf_cc_test ▼ 🔍 [查看主题](#)

通过SMN服务发送通知可能产生费用。[价格计算器](#)

告警频率 30 ▼ 分钟 - 1 + 次

在该时间间隔内，当攻击次数大于或等于您设置的阈值时才会发送告警通知。

事件类型

全选

CC攻击

命令注入

网站反爬虫

BOT攻击

精准防护

非法请求

SQL注入

本地文件包含

第三方BOT

恶意爬虫

网页防篡改

地理位置访问控制

远程文件包含

IDC情报

目录遍历防护

高级BOT

其他类型攻击

XSS攻击

IP黑白名单

高频扫描封禁

网站木马

网站信息泄露

通知描述(可选)

取消
确定

表 12-3 通知设置参数说明

参数	参数说明
通知类型	选择告警通知的类型： <ul style="list-style-type: none"> • 防护事件：WAF可将仅记录和拦截的攻击日志通过用户设置的接收通知方式（例如邮件或短信）发送给用户。 • 证书到期：证书即将到期时，WAF将通过用户设置的接收通知方式（例如邮件或短信）通知用户。
通知名称	自定义该条告警的名称。
通知描述	可选参数，备注该条告警的用途。
企业项目	在下拉框中选择企业项目，该通知在选择的企业项目下生效。

参数	参数说明
通知群组	<p>单击下拉列表选择已创建的主题或者单击“查看主题”创建新的主题，用于配置接收告警通知的终端。</p> <p>单击“查看主题”创建新主题的操作步骤如下：</p> <ol style="list-style-type: none"> 1. 参见创建主题创建一个主题。 2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见添加订阅。 3. 确认订阅。添加订阅后，完成订阅确认。 <p>更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。</p>
告警频率	<p>“通知类型”选择“防护事件”时，需要设置告警频率。</p> <p>说明 在设置时间间隔内，当攻击次数大于或等于您设置的阈值时才会发送告警通知。</p>
事件类型	<p>“通知类型”选择“防护事件”时，需要配置此参数。</p> <p>设置告警的事件类型，系统默认选择“全部”，用户也可以单击“自定义”，勾选需要告警的事件类型。</p>
到期提前通知	<p>“通知类型”选择“证书到期”时，需要配置此参数。</p> <p>在下拉框中选择证书到期提前通知的时间，可选择“1周”、“1个月”、“2个月”。</p> <p>例如：选择“1周”，那么证书到期前1周时，WAF将以短信或邮件的方式通知您更换证书。</p>
提前通知频率	<p>“通知类型”选择“证书到期”时，需要配置此参数。</p> <p>在下拉框中选择证书到期提前通知的频率，可配置为“每周”或“每天”。</p>

步骤6 配置完成后，单击“确定”，告警通知设置成功。

- 如果需要关闭该告警通知，在目标告警所在行的“操作”列，单击“关闭”。
- 如果需要删除该告警通知，在目标告警所在行的“操作”列，单击“删除”。
- 如果需要修改该告警通知，在目标告警所在行的“操作”列，单击“修改”。

----结束

告警通知邮件示例

如果您开启告警通知并成功设置以邮件方式接收告警通知，WAF会将记录和拦截的攻击日志发送给您，接收的告警通知邮件示例如图12-6所示。

图 12-6 告警通知邮件示例



13 权限管理

13.1 授权并关联企业项目

华为云企业管理服务提供统一的云资源按企业项目管理，以及企业项目内的资源管理、成员管理，企业项目可以授权给一个或者多个用户组进行管理。您可以在企业管理服务创建相关WAF的企业项目来集中管理您的WAF资源。

创建企业项目并授权

- 创建企业项目

进入管理控制台页面，单击右上方的“企业 > 项目管理”，进入企业项目管理页面。单击“创建企业项目”，输入名称。

说明

开通了企业项目的客户，或者权限为企业主账号的客户才可以看到控制台页面上方的“企业”入口。如需使用该功能，请[开通企业管理功能](#)。

- 授权

通过为企业项目添加用户组，并设置策略，实现企业项目和用户组的关联。将用户加入到用户组，使用户具有用户组中的权限，从而精确地控制用户所能访问的项目，以及所能操作的资源。具体步骤如下：

- a. 在企业项目管理页面，单击企业项目的名称，进入企业项目详情页面。
- b. 在“权限管理”页签，单击“用户组授权”，系统跳转至IAM的用户组页面，在“用户组”页签中为企业项目关联用户组并授权。具体的操作请参见[创建用户组并授权使用WAF](#)。

- 关联资源与企业项目

企业项目可以将云资源按企业项目统一管理。

- 购买Web应用防火墙时选择企业项目

在购买页面，“企业项目”下拉列表中选择目标企业项目，实现资源与企业项目关联。

- 资源迁入

对于账号下购买的WAF计费资源，您可以在“企业项目管理”页面将资源迁入目标企业项目。

“default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。

有关企业项目的详细介绍，请参见《[企业管理用户指南](#)》。

13.2 IAM 权限管理

13.2.1 WAF 自定义策略

如果系统预置的WAF权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见[WAF权限及授权项](#)。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：[创建自定义策略](#)。本章为您介绍常用的WAF自定义策略样例。

WAF 自定义策略样例

- 示例1：授权用户查询防护域名列表

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "waf:instance:list"
      ]
    }
  ]
}
```

- 示例2：拒绝用户删除网页防篡改规则

拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

如果您给用户授予“WAF FullAccess”的系统策略，但不希望用户拥有“WAF FullAccess”中定义的删除网页防篡改规则的权限

（waf:antiTamperRule:delete），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为“Deny”，然后同时将“WAF FullAccess”和拒绝策略授予用户，根据Deny优先原则用户可以对WAF执行除了删除网页防篡改规则的所有操作。以下策略样例表示：拒绝用户删除网页防篡改规则。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "waf:antiTamperRule:delete"
      ]
    }
  ],
}
```

- 多个授权项策略

一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务。多个授权语句策略描述如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "waf:instance:get",
        "waf:certificate:get"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "hss:hosts:switchVersion",
        "hss:hosts:manualDetect",
        "hss:manualDetectStatus:get"
      ]
    }
  ]
}
```

13.2.2 WAF 权限及授权项

如果您需要对您所拥有的WAF进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management, IAM），如果华为账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用WAF服务的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供了一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

权限	授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
查询防敏感信息泄 漏规则	waf:antiLeakageRule:get	√	√
查询网页防篡改规 则	waf:antiTamperRule:get	√	√

权限	授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
查询CC攻击防护规则	waf:ccRule:get	√	√
查询精准访问防护规则	waf:preciseProtectionRule:get	√	√
查询全局白名单规则	waf:falseAlarmMaskRule:get	√	√
查询隐私屏蔽规则	waf:privacyRule:get	√	√
查询黑白名单规则	waf:whiteBlackIpRule:get	√	√
查询地址位置访问控制规则	waf:geolpRule:get	√	√
查询证书	waf:certificate:get	√	√
修改WAF证书	waf:certificate:put	√	√
应用证书到域名	waf:certificate:apply	√	√
查询防护事件	waf:event:get	√	√
查询防护域名	waf:instance:get	√	√
查询防护策略	waf:policy:get	√	√
查询用户套餐信息	waf:bundle:get	√	√
查询防护事件下载链接	waf:dumpEventLink:get	√	√
查询页面配置信息	waf:consoleConfig:get	√	√
查询回源IP段	waf:sourcelp:get	√	√
更新防敏感信息泄漏规则	waf:antiLeakageRule:put	√	√
更新网页防篡改规则	waf:antiTamperRule:put	√	√
更新CC攻击防护规则	waf:ccRuleRule:put	√	√
更新精准访问防护规则	waf:preciseProtectionRule:put	√	√
更新全局白名单规则	waf:falseAlarmMaskRule:put	√	√
更新隐私屏蔽规则	waf:privacyRule:put	√	√
更新黑白名单规则	waf:whiteBlackIpRule:put	√	√

权限	授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
更新地址位置访问控制规则	waf:geolpRule:put	√	√
更新防护域名	waf:instance:put	√	√
更新防护策略	waf:policy:put	√	√
删除防敏感信息泄漏规则	waf:antiLeakageRule:delete	√	√
删除网页防篡改规则	waf:antiTamperRule:delete	√	√
删除CC攻击防护规则	waf:ccRule:delete	√	√
删除精准访问防护规则	waf:preciseProtectionRule:delete	√	√
删除全局白名单规则	waf:falseAlarmMaskRule:delete	√	√
删除隐私屏蔽规则	waf:privacyRule:delete	√	√
删除黑白名单规则	waf:whiteBlackIpRule:delete	√	√
删除地址位置访问控制规则	waf:geolpRule:delete	√	√
删除防护域名	waf:instance:delete	√	√
删除防护策略	waf:policy:delete	√	√
创建防敏感信息泄漏规则	waf:antiLeakageRule:create	√	√
创建网页防篡改规则	waf:antiTamperRule:create	√	√
创建CC攻击防护规则	waf:ccRule:create	√	√
创建精准访问防护规则	waf:preciseProtectionRule:create	√	√
创建全局白名单规则	waf:falseAlarmMaskRule:create	√	√
创建隐私屏蔽规则	waf:privacyRule:create	√	√
创建黑白名单规则	waf:whiteBlackIpRule:create	√	√

权限	授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
创建地址位置访问控制规则	waf:geolpRule:create	√	√
创建证书	waf:certificate:create	√	√
创建防护域名	waf:instance:create	√	√
创建防护策略	waf:policy:create	√	x
查询防敏感信息泄漏规则列表	waf:antiLeakageRule:list	√	√
查询网页防篡改规则列表	waf:antiTamperRule:list	√	√
查询CC攻击防护规则列表	waf:ccRuleRule:list	√	√
查询精准访问防护规则列表	waf:preciseProtectionRule:list	√	√
查询全局白名单规则列表	waf:falseAlarmMaskRule:list	√	√
查询隐私屏蔽规则列表	waf:privacyRule:list	√	√
查询黑白名单规则列表	waf:whiteBlackIpRule:list	√	√
查询地址位置访问控制规则列表	waf:geolpRule:list	√	√
查询防护域名列表	waf:instance:list	√	√
查询防护策略列表	waf:policy:list	√	√
查询云模式计费资源	waf:subscription:get	√	√
查询告警通知配置	waf:alert:get	√	√
更新告警通知配置	waf:alert:put	√	√
查询云日志配额	waf:ltsConfig:get	√	√
更新云日志配额	waf:ltsConfig:put	√	√
创建云模式包周期订单	waf:prepaid:create	√	√
查询独享引擎实例列表	waf:premiumInstance:list	√	√
查询独享引擎	waf:premiumInstance:get	√	√

权限	授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
创建独享引擎实例	waf:premiumInstance:create	√	√
删除独享引擎实例	waf:premiumInstance:delete	√	√
更新独享引擎	waf:premiumInstance:put	√	√
查看WAF实例组详情	waf:pool:get	√	√
修改WAF实例组配置	waf:pool:put	√	√
创建WAF实例组	waf:pool:create	√	√
删除WAF实例组	waf:pool:delete	√	√
查看WAF实例组列表	waf:pool:list	√	√
查询WAF实例组绑定详情	waf:poolBinding:get	√	√
绑定WAF实例组	waf:poolBinding:create	√	√
取消绑定WAF实例组	waf:poolBinding:delete	√	√
查询WAF实例组绑定详情	waf:poolBinding:list	√	√
查询WAF实例组健康检查配置	waf:poolHealthMonitor:get	√	√
修改WAF实例组健康检查配置	waf:poolHealthMonitor:put	√	√
创建WAF实例组健康检查配置	waf:poolHealthMonitor:create	√	√
删除WAF实例组健康检查配置	waf:poolHealthMonitor:delete	√	√
查询WAF实例组健康检查配置列表	waf:poolHealthMonitor:list	√	√
修改共享IP地址组	waf:ipGroupShare:put	√	√
批量更新攻击惩罚规则	waf:punishmentRule:batch-delete	√	√
查询DNS域名	waf:dnsDomain:get	√	√

权限	授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
查询重复名称的IP 地址组列表	waf:duplicateIpGroup:list	√	√

13.3 WAF 控制台的权限依赖

WAF对其他云服务有诸多依赖关系，因此在您开启IAM系统策略授权后，在WAF Console控制台的各项功能需要配置相应的服务权限后才能正常查看或使用，依赖服务的权限配置均基于您已设置了IAM系统策略授权的WAF FullAccess或WAF ReadOnlyAccess策略权限，详细设置方法请参见[创建用户组并授权使用WAF](#)。

依赖服务的权限设置

如果IAM用户需要在WAF Console控制台拥有相应功能的查看或使用权限，请确认已经对该用户所在的用户组设置了WAF Administrator、WAF FullAccess或WAF ReadOnlyAccess策略的权限，再按照如[表13-1](#)增加依赖服务的角色或策略。

表 13-1 WAF Console 中依赖服务的角色或策略

Console控制台功能	依赖服务	需配置角色/策略
安全总览	企业项目管理服务 EPS	需要增加EPS ReadOnlyAccess的系统策略后，才能查看企业项目下总览中数据图表。
购买WAF实例（专属云）	云硬盘 EVS	需要增加EVS ReadOnlyAccess的系统策略，获取云硬盘资源的查询权限。
管理独享引擎	网络控制台 VPC 弹性公网IP EIP 弹性负载均衡 ELB	<ul style="list-style-type: none"> 需要增加VPC ReadOnlyAccess的系统策略，才能查询虚拟私有云。 需要增加EIP ReadOnlyAccess的系统策略，才能查询独享引擎实例绑定的EIP。 需要增加ELB ReadOnlyAccess的系统策略，才能查询独享引擎实例绑定的ELB信息。
添加防护网站（ELB模式）	弹性负载均衡 ELB	需要增加ELB Administrator的系统角色，赋予IAM用户弹性负载均衡服务（ELB）管理员的角色，同时需要增加ELB FullAccess、ELB ReadOnlyAccess的权限，才能查询独享引擎实例绑定的ELB信息。
实例组管理	弹性负载均衡 ELB	需要增加ELB ReadOnlyAccess的系统策略，才能查询WAF实例组绑定的ELB信息。

Console控制台功能	依赖服务	需配置角色/策略
添加防护网站（云模式、独享模式）	云证书管理服务 CCM	需要增加SCM ReadOnlyAccess系统策略，才能查询证书信息。
修改服务器信息	云证书管理服务 CCM	
网站设置列表	云证书管理服务 CCM	
告警通知	消息通知服务 SMN	需要增加SMN ReadOnlyAccess的系统策略，才能获取消息通知服务的主题群组。
开启全量日志	云日志服务 LTS	需要增加LTS ReadOnlyAccess的系统策略，才能选择在云日志服务中创建的日志组和日志流名称。

14 监控与审计

14.1 使用 CES 监控 WAF

14.1.1 WAF 监控指标说明

功能说明

本节定义了Web应用防火墙上报云监控服务的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控服务提供管理控制台或API接口来检索Web应用防火墙产生的监控指标和告警信息。

命名空间

SYS.WAF

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

防护域名监控指标

表 14-1 WAF 防护域名监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
requests	请求量	该指标用于统计测量对象近5分钟内WAF返回的请求量的总数。 单位：次 采集方式：统计防护域名请求量的总数	≥0 次 值类型： Float	防护域名	5分钟
waf_http_2xx	WAF返回码 (2XX)	该指标用于统计测量对象近5分钟内WAF返回的2XX状态码的数量。 单位：次 采集方式：统计WAF引擎返回的2XX系列状态响应码的数量	≥0 次 值类型： Float	防护域名	5分钟
waf_http_3xx	WAF返回码 (3XX)	该指标用于统计测量对象近5分钟内WAF返回的3XX状态码的数量。 单位：次 采集方式：统计WAF引擎返回的3XX系列状态响应码的数量	≥0 次 值类型： Float	防护域名	5分钟
waf_http_4xx	WAF返回码 (4XX)	该指标用于统计测量对象近5分钟内WAF返回的4XX状态码的数量。 单位：次 采集方式：统计WAF引擎返回的4XX系列状态响应码的数量	≥0 次 值类型： Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
waf_http_5xx	WAF返回码 (5XX)	该指标用于统计测量对象近5分钟内WAF返回的5XX状态码的数量。 单位: 次 采集方式: 统计WAF引擎返回的5XX系列状态响应码的数量	≥0 次 值类型: Float	防护域名	5分钟
waf_fused_counts	WAF熔断量	该指标用于统计测量对象近5分钟内被WAF熔断保护的请求数量。 单位: 次 采集方式: 统计防护域名被熔断保护的请求数量	≥0 次 值类型: Float	防护域名	5分钟
inbound_traffic	入网总流量	该指标用于统计测量对象近5分钟内总入带宽的大小。 单位: Mbit 采集方式: 统计近5分钟内总入带宽的大小	≥0 Mbit 值类型: Float	防护域名	5分钟
outbound_traffic	出网总流量	该指标用于统计测量对象近5分钟内总出带宽的大小。 单位: Mbit 采集方式: 统计近5分钟内总出带宽的大小	≥0 Mbit 值类型: Float	防护域名	5分钟
waf_process_time_0	WAF处理时延-区间 [0-10ms)	该指标用于统计测量对象近5分钟内WAF处理时延在区间[0-10ms)内的总数量。 单位: 次 采集方式: 统计近5分钟内WAF处理时延在区间[0-10ms)内的总数量	≥0 次 值类型: Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
waf_proc ess_time_ 10	WAF处理时 延-区间 [10-20ms)	该指标用于统计测量对象近5分钟内WAF处理时延在区间[10-20ms)内的总数量。 单位: 次 采集方式: 统计近5分钟内WAF处理时延在区间[10-20ms)内的总数量	≥0 次 值类型: Float	防护域 名	5分钟
waf_proc ess_time_ 20	WAF处理时 延-区间 [20-50ms)	该指标用于统计测量对象近5分钟内WAF处理时延在区间[20-50ms)内的总数量。 单位: 次 采集方式: 统计近5分钟内WAF处理时延在区间[20-50ms)内的总数量	≥0 次 值类型: Float	防护域 名	5分钟
waf_proc ess_time_ 50	WAF处理时 延-区间 [50-100ms)	该指标用于统计测量对象近5分钟内WAF处理时延在区间[50-100ms)内的总数量。 单位: 次 采集方式: 统计近5分钟内WAF处理时延在区间[50-100ms)内的总数量	≥0 次 值类型: Float	防护域 名	5分钟
waf_proc ess_time_ 100	WAF处理时 延-区间 [100-1000 ms)	该指标用于统计测量对象近5分钟内WAF处理时延在区间[100-1000ms)内的总数量。 单位: 次 采集方式: 统计近5分钟内WAF处理时延在区间[100-1000ms)内的总数量	≥0 次 值类型: Float	防护域 名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
waf_proc ess_time_ 1000	WAF处理时 延-区间 [1000+ms)	该指标用于统计测量对象近5分钟内WAF处理时延在区间[1000+ms)内的总数量。 单位: 次 采集方式: 统计近5分钟内WAF处理时延在区间[1000+ms)内的总数量	≥0 次 值类型: Float	防护域 名	5分钟
qps_peak	QPS峰值	该指标用于统计近5分钟内防护域名的QPS峰值。 单位: 次 采集方式: 统计近5分钟内防护域名的QPS峰值	≥0 次 值类型: Float	防护域 名	5分钟
qps_mea n	QPS均值	该指标用于统计近5分钟内防护域名的QPS均值。 单位: 次 采集方式: 统计近5分钟内防护域名的QPS均值	≥0 次 值类型: Float	防护域 名	5分钟
waf_http_ 0	无返回的 WAF状态码	该指标用于统计测量对象近5分钟内WAF无返回的状态响应码的数量。 单位: 次 采集方式: 统计近5分钟内WAF无返回的状态响应码的数量	≥0 次 值类型: Float	防护域 名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
upstream_code_2xx	业务返回码 (2XX)	该指标用于统计测量对象近5分钟内业务返回的2XX系列状态响应码的数量。 单位: 次 采集方式: 统计近5分钟内业务返回的2XX系列状态响应码的数量	≥0 次 值类型: Float	防护域名	5分钟
upstream_code_3xx	业务返回码 (3XX)	该指标用于统计测量对象近5分钟内业务返回的3XX系列状态响应码的数量。 单位: 次 采集方式: 统计近5分钟内业务返回的3XX系列状态响应码的数量	≥0 次 值类型: Float	防护域名	5分钟
upstream_code_4xx	业务返回码 (4XX)	该指标用于统计测量对象近5分钟内业务返回的4XX系列状态响应码的数量。 单位: 次 采集方式: 统计近5分钟内业务返回的4XX系列状态响应码的数量	≥0 次 值类型: Float	防护域名	5分钟
upstream_code_5xx	业务返回码 (5XX)	该指标用于统计近5分钟内业务返回的5XX系列状态响应码的数量。 单位: 次 采集方式: 统计近5分钟内业务返回的5XX系列状态响应码的数量	≥0 次 值类型: Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
upstream_code_0	无返回的业务状态码	该指标用于统计测量对象近5分钟内业务无返回的状态响应码的数量。 单位：次 采集方式：统计近5分钟内业务无返回的状态响应码的数量	≥0 次 值类型： Float	防护域名	5分钟
inbound_traffic_peak	入网流量的峰值	该指标用于统计近5分钟内防护域名入网流量的峰值。 单位：Mbit/s 采集方式：统计近5分钟内防护域名入网流量的峰值	≥0 Mbit/s 值类型： Float	防护域名	5分钟
inbound_traffic_mean	入网流量的均值	该指标用于统计近5分钟内防护域名入网流量的均值。 单位：Mbit/s 采集方式：统计近5分钟内防护域名入网流量的均值	≥0 Mbit/s 值类型： Float	防护域名	5分钟
outbound_traffic_peak	出网流量的峰值	该指标用于统计近5分钟内防护域名出网流量的峰值。 单位：Mbit/s 采集方式：统计近5分钟内防护域名出网流量的峰值	≥0 Mbit/s 值类型： Float	防护域名	5分钟
outbound_traffic_mean	出网流量的均值	该指标用于统计近5分钟内防护域名出网流量的均值。 单位：Mbit/s 采集方式：统计近5分钟内防护域名出网流量的均值	≥0 Mbit/s 值类型： Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
attacks	攻击总次数	该指标用于统计近5分钟内防护域名攻击请求量的总数。 单位: 次 采集方式: 统计近5分钟内防护域名攻击请求量的总数	≥0 次 值类型: Float	防护域名	5分钟
crawlers	爬虫攻击次数	该指标用于统计近5分钟内防护域名爬虫攻击请求量的总数。 单位: 次 采集方式: 统计近5分钟内防护域名爬虫攻击请求量的总数	≥0 次 值类型: Float	防护域名	5分钟
base_protection_counts	web基础防护次数	该指标用于统计近5分钟内由Web基础防护规则防护的攻击数量。 单位: 次 采集方式: 统计近5分钟内由Web基础防护规则防护的攻击数量	≥0 次 值类型: Float	防护域名	5分钟
precise_protection_counts	精准防护次数	该指标用于统计近5分钟内由精准防护规则防护的攻击数量。 单位: 次 采集方式: 统计近5分钟内由精准防护规则防护的攻击数量	≥0 次 值类型: Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
cc_protection_counts	cc防护次数	该指标用于统计近5分钟内由CC防护规则防护的攻击数量。 单位：次 采集方式：统计近5分钟内由CC防护规则防护的攻击数量。	≥0 次 值类型： Float	防护域名	5分钟

独享引擎实例监控指标

表 14-2 WAF 独享引擎实例监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
cpu_util	CPU使用率	该指标用于统计测量对象的CPU利用率。 单位：百分比 采集方式：100%减去空闲CPU占比	0 ~ 100 % 值类型： Float	独享引擎实例	1分钟
mem_util	内存使用率	该指标用于统计测量对象的内存利用率。 单位：百分比 采集方式：100%减去空闲内存占比	0 ~ 100 % 值类型： Float	独享引擎实例	1分钟
disk_util	磁盘使用率	该指标用于统计测量对象的磁盘利用率。 单位：百分比 采集方式：100%减去空闲磁盘占比	0 ~ 100 % 值类型： Float	独享引擎实例	1分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
disk_avail_size	磁盘可用空间	该指标用于统计测量对象的磁盘可用空间。 单位: byte、KB、MB、GB、TB、PB 采集方式: 空闲磁盘空间大小	≥0 byte 值类型: Float	独享引擎实例	1分钟
disk_read_bytes_rate	磁盘读速率	该指标用于统计测量对象每秒从磁盘读取的字节数。 单位: byte/s、KB/s、MB/s、GB/s 采集方式: 每秒从磁盘读取的字节数	≥0 byte/s 值类型: Float	独享引擎实例	1分钟
disk_write_bytes_rate	磁盘写速率	该指标用于统计测量对象每秒写入磁盘的字节数。 单位: byte/s、KB/s、MB/s、GB/s 采集方式: 每秒写入磁盘的字节数	≥0 byte/s 值类型: Float	独享引擎实例	1分钟
disk_read_requests_rate	磁盘读操作速率	该指标用于统计测量对象每秒从磁盘读取的请求数。 单位: 请求/秒 采集方式: 每秒磁盘处理的读取请求数	≥0 request/s 值类型: Float	独享引擎实例	1分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
disk_write_requests_rate	磁盘写操作速率	该指标用于统计测量对象每秒写入数据到磁盘的请求次数。 单位：请求/秒 采集方式：每秒磁盘处理的写入请求数	≥0 request/s 值类型：Float	独享引擎实例	1分钟
network_incoming_bytes_rate	网络流入速率	该指标用于统计测量对象每秒流入测量对象的网络流量。 单位： byte/s、KB/s、MB/s、GB/s 采集方式：每秒从网络适配器输入的流量	≥0 byte/s 值类型：Float	独享引擎实例	1分钟
network_outgoing_bytes_rate	网络流出速率	该指标用于统计测量对象每秒流出测量对象的网络流量。 单位： byte/s、KB/s、MB/s、GB/s 采集方式：每秒从网络适配器输出的流量	≥0 byte/s 值类型：Float	独享引擎实例	1分钟
network_incoming_packets_rate	网络流入包速率	该指标用于统计测量对象每秒流入测量对象的数据包数量。 单位： packet/s 采集方式：每秒从网络适配器流入的数据包数	≥0 packet/s 值类型：Int	独享引擎实例	1分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
network_outgoing_packets_rate	网络流包速率	该指标用于统计测量对象每秒流出测量对象的数据包数量。 单位： packet/s 采集方式：每秒从网络适配器流出的数据包数	≥0 packet/s 值类型： Int	独享引擎实例	1分钟
concurrent_connections	并发连接数	该指标用于统计测量对象当前处理的并发连接数量。 单位：count 采集方式：系统当前的并发连接数量	≥0 count 值类型： Int	独享引擎实例	1分钟
active_connections	活跃连接数	该指标用于统计测量对象当前打开的连接数量。 单位：count 采集方式：系统当前的活跃连接数量	≥0 count 值类型： Int	独享引擎实例	1分钟
latest_policy_sync_time	最近一次策略同步的耗时	该指标用于统计测量对象最近一次同步WAF策略的耗时。 单位：ms 采集方式：最近一次同步WAF策略的耗时	≥0 ms 值类型： Int	独享引擎实例	1分钟

维度

Key	Value
instance_id	WAF独享引擎实例ID
waf_instance_id	WAF防护网站ID

监控指标原始数据格式样例

```
[
  {
    "metric": {
      // 命名空间
      "namespace": "SYS.WAF",
      "dimensions": [
        {
          // 维度名称, 例如防护网站
          "name": "waf_instance_id",
          // 该维度下的监控对象ID, 例如防护网站ID
          "value": "082db2f542e0438aa520035b3e99cd99"
        }
      ],
      // 指标ID
      "metric_name": "waf_http_2xx"
    },
    // 生存时间, 指标预定义
    "ttl": 172800,
    // 指标值
    "value": 0.0,
    // 指标单位
    "unit": "Count",
    // 指标值类型
    "type": "float",
    // 指标采集时间
    "collect_time": 1637677359778
  }
]
```

14.1.2 设置监控告警规则


通过设置WAF告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解WAF防护状况，从而起到预警作用。


前提条件

[防护网站已接入WAF](#)

设置监控告警规则

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“管理与监管 > 云监控服务 CES”。

步骤4 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤6 配置相关参数。

- 名称：自定义规则名称。
- 告警类型：选择“指标”。
- 云产品：选择“Web应用防火墙-独享实例”或“Web应用防火墙-防护域名”。
 - 独享实例监控指标选择“Web应用防火墙-独享实例”。

- 防护域名监控指标选择“Web应用防火墙-防护域名”。
- 监控范围：全部资源。
- 触发规则：选择“关联模板”，或者自定义创建模板。
- 发送通知：如果希望实时收到告警信息，开启该选项，并选择通知方式。
- 其他参数：根据实际情况配置。

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”，告警规则创建成功。

----结束

14.1.3 查看监控指标


您可以通过CES管理控制台，查看WAF的相关指标，及时了解WAF防护状况，并通过指标设置防护策略。


前提条件

WAF已对接云监控，即已在云监控页面设置监控告警规则。有关设置监控告警规则的详细操作，请参见[设置监控告警规则](#)。

查看监控指标

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务 CES”。

步骤4 在左侧导航树栏，选择“云服务监控”，进入“云服务监控”页面。

步骤5 在搜索框中搜索“看板名称：Web应用防火墙 WAF”，在“看板名称”列，单击“Web应用防火墙 WAF”，进入“云服务监控详情”页面。

步骤6 在“云服务概览”页签，可查看资源概况、告警统计的相关指标。

步骤7 选择“资源详情”页签，在实例列表的“操作”列中，单击“查看监控指标”，查看对象的指标详情。

说明

在“网站设置”列表中，目标域名所在行的“操作”列，单击“云监控”，可直接查看单个网站的监控信息。

----结束

14.2 使用 CTS 审计 WAF

14.2.1 云审计服务支持的 WAF 操作列表

云审计服务（Cloud Trace Service, CTS）记录了Web应用防火墙相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见云审计服务用户指南。

表 14-3 云审计服务支持的 WAF 操作列表

操作名称	资源类型	事件名称
创建云模式域名	instance	createInstance
删除云模式域名	instance	deleteInstance
修改云模式域名的防护状态	instance	modifyProtectStatus
修改云模式域名的接入状态	instance	modifyAccessStatus
修改云模式域名	instance	modifyInstance
修改DNS解析, 快速接入WAF	instance	quickAccessInstance
服务器线路设置	instance	modifyInstanceRoute
创建域名 (独享/elb)	host	createHost
修改域名 (独享/elb)	host	modifyHost
删除域名 (独享/elb)	host	deleteHost
修改防护状态 (独享/elb)	host	modifyProtectStatus
修改接入状态 (独享/elb)	host	modifyAccessStatus
修改接入配置 (独享/elb)	host	modifyAccessProgress
域名迁移	migrate-host	migrateHosts
添加证书	certificate	createCertificate
修改证书	certificate	updateCertificate
删除证书	certificate	deleteCertificate
应用证书 (将证书添加到域名)	certificate	applyCertificate
共享证书	certificate-sharing	createCertificateSharing
关闭证书共享	certificate-sharing	deleteCertificateSharing
创建Web应用防火墙防护策略	policy	createPolicy
应用Web应用防火墙防护策略	policy	applyToHost

操作名称	资源类型	事件名称
更新Web应用防火墙防护策略	policy	modifyPolicy
删除Web应用防火墙防护策略	policy	deletePolicy
创建CC规则	policy	createCc
修改CC规则	policy	modifyCc
删除CC规则	policy	deleteCc
创建精准防护规则	policy	createCustom
修改精准防护规则	policy	modifyCustom
删除精准防护规则	policy	deleteCustom
创建IP黑白名单规则	policy	createWhiteblackip
修改IP黑白名单规则	policy	modifyWhiteblackip
删除IP黑白名单规则	policy	deleteWhiteblackip
创建/刷新网页防篡改规则	policy	createAntitamper
开启/关闭网页防篡改规则	policy	modifyAntitamper
删除网页防篡改规则	policy	deleteAntitamper
创建全局白名单规则	policy	createIgnore
修改全局白名单规则	policy	modifyIgnore
删除全局白名单规则	policy	deleteIgnore
创建隐私屏蔽规则	policy	createPrivacy
修改隐私屏蔽规则	policy	modifyPrivacy
删除隐私屏蔽规则	policy	deletePrivacy
创建攻击惩罚规则	policy	createPunishment
修改攻击惩罚规则	policy	modifyPunishment
删除攻击惩罚规则	policy	deletePunishment
创建地理位置访问控制规则	policy	createGeoip
修改地理位置访问控制规则	policy	modifyGeoip
删除地理位置访问控制规则	policy	deleteGeoip

操作名称	资源类型	事件名称
创建威胁情报访问控制规则	policy	createlp-reputation
修改威胁情报访问控制规则	policy	modifylp-reputation
删除威胁情报访问控制规则	policy	deletelp-reputation
创建反爬虫规则	policy	createAnticrawler
修改反爬虫规则	policy	modifyAnticrawler
删除反爬虫规则	policy	deleteAnticrawler
创建防敏感信息泄露规则	policy	createAntileakage
修改防敏感信息泄露规则	policy	modifyAntileakage
删除防敏感信息泄露规则	policy	deleteAntileakage
批量创建CC规则	policy	batchCreateCc
批量修改CC规则	policy	batchUpdateCc
批量删除CC规则	policy	batchDeleteCc
批量创建精准防护规则	policy	batchCreateCustom
批量修改精准防护规则	policy	batchUpdateCustom
批量删除精准防护规则	policy	batchDeleteCustom
批量创建IP黑白名单规则	policy	batchCreateWhiteblackip
批量修改IP黑白名单规则	policy	batchUpdateWhiteblackip
批量删除IP黑白名单规则	policy	batchDeleteWhiteblackip
批量创建地理位置访问控制规则	policy	batchCreateGeoip
批量修改地理位置访问控制规则	policy	batchUpdateGeoip
批量删除地理位置访问控制规则	policy	batchDeleteGeoip

操作名称	资源类型	事件名称
批量创建威胁情报访问控制规则	policy	batchCreatelp-reputation
批量修改威胁情报访问控制规则	policy	batchUpdatelp-reputation
批量删除威胁情报访问控制规则	policy	batchDeletelp-reputation
批量创建/刷新网页防篡改规则	policy	batchCreateAntitamper
批量开启/关闭网页防篡改规则	policy	batchUpdateAntitamper
批量删除网页防篡改规则	policy	batchDeleteAntitamper
批量创建防敏感信息泄露规则	policy	batchCreateAntileakage
批量修改防敏感信息泄露规则	policy	batchUpdateAntileakage
批量删除防敏感信息泄露规则	policy	batchDeleteAntileakage
批量创建全局白名单规则	policy	batchCreatelgnore
批量修改全局白名单	policy	batchUpdatelgnore
批量删除全局白名单	policy	batchDeletelgnore
批量创建隐私屏蔽规则	policy	batchCreatePrivacy
批量修改隐私屏蔽规则	policy	batchUpdatePrivacy
批量删除隐私屏蔽规则	policy	batchDeletePrivacy
创建告警通知	alertNoticeConfig	createAlertNoticeConfig
修改告警通知	alertNoticeConfig	modifyAlertNoticeConfig
删除告警通知	alertNoticeConfig	deleteAlertNoticeConfig
批量删除告警通知	alertNoticeConfig	batchDeleteAlertNoticeConfig
删除独享实例	instance	deleteInstance
创建独享实例	instance	createInstance
更新独享实例	instance	upgradeInstance

操作名称	资源类型	事件名称
修改实例名	instance	alterInstanceName
添加地址组	ip-group	createIPGroup
修改地址组	ip-group	modifyIPGroup
删除地址组	ip-group	deleteIPGroup
创建引用表	valueList	createValueList
修改引用表	valueList	modifyValueList
删除引用表	valueList	deleteValueList
创建安全报告模板	SecurityReport	createSecurityReportSubscription
修改安全报告模板	SecurityReport	updateSecurityReportSubscription
删除安全报告模板	SecurityReport	deleteSecurityReportSubscription
购买内容安全检测	content_security	openPostpaidContentSecurity
批量购买内容安全检测	content_security	batchCreateContentSecurityTask

14.2.2 在 CTS 事件列表查看云审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。


- [在新版事件列表查看审计事件](#)
- [在旧版事件列表查看审计事件](#)

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)或云日志服务(LTS)，才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。


- CTS新版事件列表不显示数据类审计事件，您需要在旧版事件列表查看数据类审计事件。
- 云审计控制台对用户的操作事件日志保留7天，过期自动删除，不支持人工删除。



在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
 - 事件名称：输入事件的名称。
 - 事件ID：输入事件ID。
 - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
 - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
 - 云服务：在下拉框中选择对应的云服务名称。
 - 资源类型：在下拉框中选择对应的资源类型。
 - 操作用户：在下拉框中选择一个或多个具体的操作用户。
 - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
 - normal：表示操作成功。
 - warning：表示操作失败。
 - incident：表示比操作失败更严重的情况，例如引起其他故障等。
 - 企业项目ID：输入企业项目ID。
 - 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
 - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。


说明

您可以参考[云审计服务应用示例](#)，来学习如何查询具体的事件。

5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
 - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
 - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击  按钮，可以获取到事件操作记录的最新信息。



- 单击  按钮，可以自定义事件列表的展示信息。启用表格内容折行开关 ，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见[事件结构](#)和[事件样例](#)。
 7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
 - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
 - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
 - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
 - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
 - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
 - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
 - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

说明

您可以参考[云审计服务应用示例](#)，来学习如何查询具体的事件。

6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
 - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击  按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击  展开该记录的详细信息。

事件名称	资源类型	云服务	资源ID	资源名称	事件级别	操作用户	操作时间	操作
createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	normal		2023/11/16 10:54:04 GMT+08:00	查看详情

request	trace_id	code	trace_name	resource_type	trace_rsting	api_version	message	source_ip	domain_id	trace_type
		200	createDockerConfig	dockerlogincmd	normal		createDockerConfig, Method: POST Uri=/v2/manager/units/secret, Reason:			ApiCall

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。

查看事件 ×

```
{
  "request": "",
  "trace_id": "676d4ae3-842b-11ee-9299-9159eee6a3ac",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:",
  "source_ip": " ",
  "domain_id": " ",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": " ",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "2023/11/16 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": " ",
      "id": " "
    }
  }
}
```

10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的[事件结构](#)和[事件样例](#)。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。