# 边缘安全

# 最佳实践

**文档版本** 03

**发布日期** 2024-07-19

**华为云计算技术有限公司**

## 商标声明


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 Web 基础防护功能

本文介绍了如何通过边缘安全服务开启Web攻击防护。

## 前提条件

已在CDN（Content Delivery Network，内容分发网络）服务的“域名管理”中，添加了域名，CDN的域名管理请参见**域名管理**。

## 应用场景

通过边缘安全服务对域名开启Web防护。

## 添加防护网站

**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 > 边缘安全”。

**步骤3** 在左侧导航栏选择“安全防护 > 网站设置”，进入“安全防护”的“网站设置”页面。

**步骤4** 在列表左上角，单击“添加防护网站”，参数说明如**表 添加防护网站参数说明**所示。

**图 1-1** 添加防护网站

**表 1-1** 添加防护网站参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 网站名称 | 网站的名称。命名规则如下：<br>● 不可重名。<br>● 须以字母开头。<br>● 长度不能超过128个字符。<br>● 支持英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_:）。 |
| 防护域名 | 选择防护域名，仅支持选择在CDN服务中“域名管理”页面“业务类型”为“网站加速”的域名。 |
| 网站备注 | 网站补充信息。 |
| 策略配置 | 选择已创建的防护策略，默认为“系统自动生成策略”。 |

**步骤5** 单击“确定”，完成防护网站的添加。

**----结束**

## 防护策略

**步骤1** 在左侧导航栏选择“安全防护 > 网站设置”，进入“安全防护”的“网站设置”页面。

**步骤2** 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

**图 1-2** 网站列表


**步骤3** 在“Web基础防护”配置框中，用户可根据自己的需要参照**表1-2**更改Web基础防护的“状态”和“模式”。

**图 1-3** Web 基础防护配置框

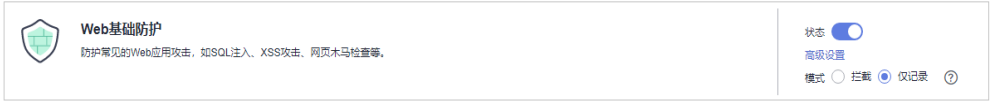


**表 1-2** 防护动作参数说明

| 参数 | 说明 |
| --- | --- |
| 状态 | Web应用防护攻击的状态。<br>•  ：开启状态。<br>•  ：关闭状态。 |
| 模式 | • 拦截：发现攻击行为后立即阻断并记录。<br>• 仅记录：发现攻击行为后只记录不阻断攻击。 |

**步骤4** 在“Web基础防护”配置框中，单击“高级设置”，进入“Web基础防护”界面。

**步骤5** 在“防护配置”页签，根据您的业务场景，开启合适的防护功能，检测项说明如**表1-4**所示。

**图 1-4** Web 基础防护


**须知**

当“模式”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**。

1. 防护等级设置。

   在页面右上角，选择防护等级，Web基础防护设置了三种防护等级：“宽松”、“中等”、“严格”，默认情况下，选择“中等”。

**表 1-3** 防护等级说明

| 防护等级 | 说明 |
| --- | --- |
| 宽松 | 防护粒度较粗，只拦截攻击特征比较明显的请求。<br>当误报情况较多的场景下，建议选择“宽松”模式。 |
| 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。 |
| 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。<br>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。 |

2. 防护检测类型设置。

> **须知**
>
> 默认开启“常规检测”防护检测，用户可根据业务需要，参照表1-4开启其他需要防护的检测类型。

**表 1-4** 检测项说明

| 检测项 | 说明 |
| --- | --- |
| 常规检测 | 防护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。其中，SQL注入攻击主要基于语义进行检测。<br>**说明**<br>开启“常规检测”后，边缘安全将根据内置规则对常规检测项进行检测。 |
| Webshell检测 | 防护通过上传接口植入网页木马。<br>**说明**<br>开启“Webshell检测”后，边缘安全将对通过上传接口植入的网页木马进行检测。 |

**----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（原误报屏蔽）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、JAVA SCRIPT代码。
  - 正常业务的URL尽量不要使用一些特殊的关键字（UPDATE、SET等）作为路径，例如：“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

开启Web基础防护功能后，在浏览器中输入模拟SQL注入攻击的测试域名，边缘WAF将拦截此条攻击。您可以在“安全总览”页面，查看攻击的拦截详情，如图1-6所示。

**图 1-5** SQL 攻击拦截

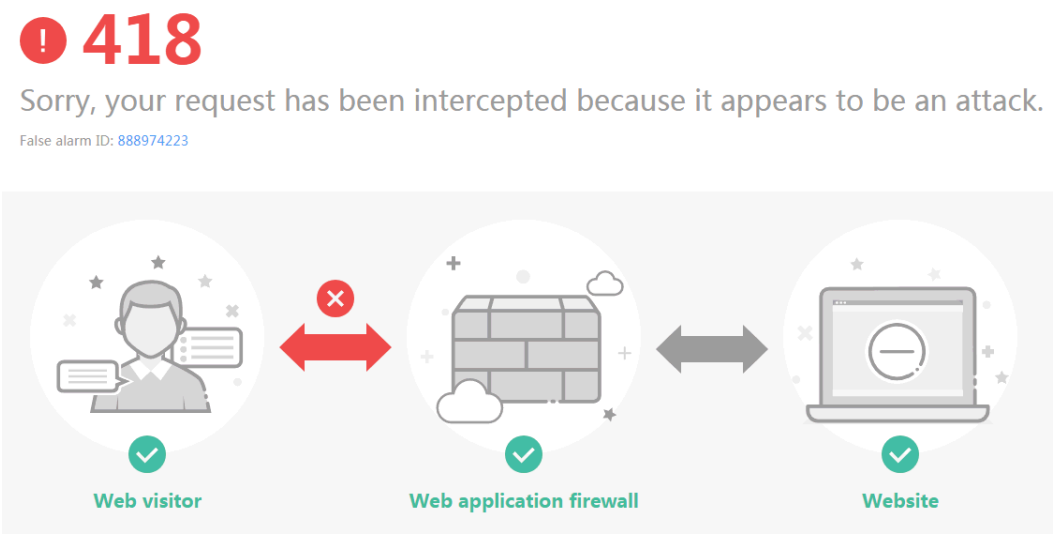
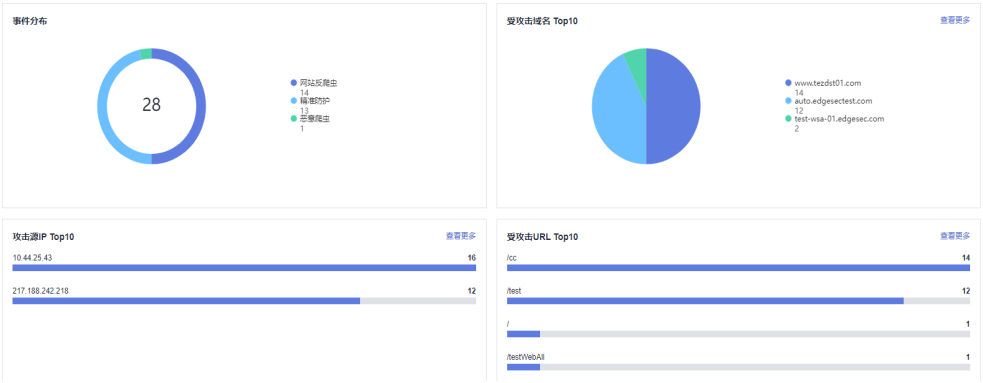



**图 1-6** 安全统计




在“防护事件”页面，您可查看“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。同时，单击“详情”，可以查看具体的攻击信息，如图1-7所示。

**图 1-7** 防护事件列表

# 2 CC 攻击防御

## 2.1 简介

本文指导您在受到CC（Challenge Collapsar）攻击时，完成基于IP限速识别的防护规则的配置。

### 如何判断是否遭受 CC 攻击?

当您发现网站处理速度下降，网络带宽占用过高时，很有可能已经遭受CC攻击，此时可查看Web服务器的访问日志或网络连接数量，如果访问日志或网络连接数量显著增加，则可确定遭受CC攻击，可以按照以下策略进行配置，利用边缘WAF阻断CC攻击，保障网站业务的正常运行。

**说明**

边缘WAF防护应用层流量的拒绝服务攻击，适合防御HTTP Get攻击等。

### 前提条件

您的网站已成功接入边缘安全。关于域名接入的具体操作请参见**添加防护网站**。

## 2.2 基于 IP 限速的配置

当边缘WAF与访问者之间并无代理设备时，通过源IP来检测攻击行为较为精确，建议直接使用IP限速的方式进行访问频率限制。

### 攻击案例

竞争对手控制数台主机，持续向网站“www.example.com”发起HTTP Post请求，网站并无较大的负载能力，网站连接数、带宽等资源均被该攻击者大量占用，正常用户无法访问网站，最终竞争力急剧下降。

### 防护措施

1. 根据服务访问请求统计，判断网站是否有大量单IP请求发生，如果有则说明网站很有可能遭受了CC攻击。

2. **登录管理控制台**。
3. 单击页面左上方的 ，选择“安全与合规 > 边缘安全”。
4. 在左侧导航栏选择“安全防护 > 网站设置”，进入“安全防护”的“网站设置”页面。
5. 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面，确认“CC攻击防护”的“状态”为“开启” ，单击“自定义CC攻击防护规则”，进入CC防护规则配置页面。

**图 2-1** CC 防护规则配置框


6. 在CC防护规则配置页面左上角，单击“添加规则”，配置对指定路径下的请求进行基于IP限速的检测，针对业务特性，设置限速频率，并配置人机验证，防止误拦截正常用户，针对网站所有url进行防护。
   - 限速模式：选择“源限速”、“IP限速”，根据IP区分单个Web访问者。
   - 限速频率：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，边缘安全将暂停该Web访问者的访问。
   - 防护动作：防止误拦截正常用户，选择“人机验证”。
     - 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。
     - 仅记录：表示超过“限速频率”将只记录不阻断。

   当用户访问超过限制后需要输入验证码才能继续访问。
7. 进入防护事件页面，可以查看攻击事件详情，操作方法请参见**查看防护事件**。

# A 修订记录

| 发布日期 | 修改记录 |
| --- | --- |
| 2024-07-18 | 第三次正式发布。<br>删除：<br>基于Cookie字段的配置章节。<br>通过配置业务Cookie和System ID限制恶意抢购章节。 |
| 2024-05-27 | 第二次正式发布。<br>优化全文。 |
| 2023-08-04 | 第一次正式发布。 |