# Web应用防火墙(ngwaf)

## 产品文档

腾讯云TCE

# 文档目录

# 操作指南
# 概览

最近更新时间: 2024-06-12 15:06:00

## 概览

概览页面可浏览当前账户下 WAF 实例信息，攻击概览，安全分析等模块。

## 安全概览

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**概览**，进入概览页面。

2. 在概览页面，左上角选择对应实例或域名，即可查看该实例或域名的概览信息。

## 攻击总览

**全部域名**

1. 当安全概览为全部域名时，攻击总览统计数据为全局攻击数，统计周期可以通过筛选显示。

2. 同时，在页面下方可以查看域名 Web 攻击次数 TOP5(次)、攻击来源 IP TOP5(次) 、域名 CC 攻击次数 TOP5(次)等信息。

字段说明：

- 域名 Web 攻击次数 TOP5(次)：展示全部实例中受到攻击最多的5个域名。

- 攻击来源 IP TOP5(次) ：展示全部实例中受到攻击最多的5个 IP。
- 域名 CC 攻击次数 TOP5(次) ：展示全部实例中受到攻击最多的5个域名。
- 请求来源 IP TOP5(次) ：展示全部实例中访问最多的5个 IP。
- 攻击来源区域分布(次)：展示全部实例中攻击来源分布的地区。
- 攻击类型占比：展示全部实例中攻击类型的分布。
- 浏览器类型占比：展示全部实例中浏览器类型的分布。

**单个域名**

1. 当安全概览为单个域名时，攻击总览统计数据为单个域名收到攻击数，统计周期可以通过筛选显示。

2. 同时，在页面下方可以查看攻击来源 IP TOP5(次)、请求来源 IP TOP5(次) 、攻击来源区域分布(次)等信息。

**字段说明：**

- 攻击来源 IP TOP5(次) ：展示全部实例中受到攻击最多的5个 IP。
- 请求来源 IP TOP5(次) ：展示全部实例中访问最多的5个 IP。
- 攻击来源区域分布(次)：展示全部实例中攻击来源分布的地区。
- 攻击类型占比：展示全部实例中攻击类型的分布。
- 浏览器类型占比：展示全部实例中浏览器类型的分布。

# 概览安全分析

- 基础安全：分析描述了当前选择的域名在统计周期内所受到的 Web 攻击次数。
- 业务运营：分析描述了当前选择的域名在统计周期内的 QPS 及带宽详情，右侧统计了该域名统计周期内的响应及访问次数的 Top 值。
- BOT 与业务安全：描述了当前域名在统计周期内的 BOT 信息，单击前往 BOT流量分析 即可查看 BOT 与业务安全的流量信息。
- API 流量分析：描述了当前域名在统计周期内的 API 资产、API 风险数详情及趋势，右侧展示了不同等级的 API 风险事件占比，单击**查看 API 流量分析**即可前往查看 API 安全流量的统计报表。

概览

概览页面可浏览当前账户下 WAF 实例信息，攻击概览，安全分析等模块。

快速上手指南

本视频为您介绍如何快速上手 Web 应用防火墙。

安全概览

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择概览，进入概览页面。
2. 在概览页面，左上角选择对应实例或域名，即可查看该实例或域名的概览信息。

实例概览 在概览页面，左上角选择对应域名，单击包含x个实例，即可查看当前账户下已购实例过期信息。

规则更新动态 在概览页面的规则更新动态模块，单击右上角的查看更多规则动态，即可查看当前 WAF 支持的 Web 规则库。

攻击总览 全部域名

1. 当安全概览为全部域名时，攻击总览统计数据为全局攻击数，统计周期可以通过筛选显示。
2. 同时，在页面下方可以查看域名 Web 攻击次数 TOP5(次)、攻击来源 IP TOP5(次) 、域名 CC 攻击次数 TOP5(次) 等信息。

字段说明： 域名 Web 攻击次数 TOP5(次)：展示全部实例中受到攻击最多的5个域名。 攻击来源 IP TOP5(次) ：展示全部实例中受到攻击最多的5个 IP。 域名 CC 攻击次数 TOP5(次) ：展示全部实例中受到攻击最多的5个域名。 请求来源 IP TOP5(次) ：展示全部实例中访问最多的5个 IP。 攻击来源区域分布(次)：展示全部实例中攻击来源分布的

地区。 攻击类型占比：展示全部实例中攻击类型的分布。 浏览器类型占比：展示全部实例中浏览器类型的分布。 单个域名

1. 当安全概览为单个域名时，攻击总览统计数据为单个域名收到攻击数，统计周期可以通过筛选显示。

2. 同时，在页面下方可以查看攻击来源 IP TOP5(次)、请求来源 IP TOP5(次) 、攻击来源区域分布(次)等信息。

字段说明： 攻击来源 IP TOP5(次) ：展示全部实例中受到攻击最多的5个 IP。 请求来源 IP TOP5(次) ：展示全部实例中访问最多的5个 IP。 攻击来源区域分布(次)：展示全部实例中攻击来源分布的地区。 攻击类型占比：展示全部实例中攻击类型的分布。 浏览器类型占比：展示全部实例中浏览器类型的分布。 概览安全分析

基础安全：分析描述了当前选择的域名在统计周期内所受到的 Web 攻击次数。

业务运营：分析描述了当前选择的域名在统计周期内的 QPS 及带宽详情，右侧统计了该域名统计周期内的响应及访问次数的 Top 值。

BOT 与业务安全：描述了当前域名在统计周期内的 BOT 信息，单击前往

BOT流量分析 即可查看 BOT 与业务安全的流量信息。

API 流量分析：描述了当前域名在统计周期内的 API 资产、API 风险数详情及趋势，右侧展示了不同等级的 API 风险事件占比，单击 查看 API 流量分析 即可前往查看 API 安全流量的统计报表。

# 域名管理

最近更新时间: 2024-06-12 15:06:00

# 域名管理

## 操作场景

本文档将为您介绍 Web 应用防火墙（WAF）资产中心的域名列表模块，可以查看域名详情，进行新建域名、编辑域名、删除域名等操作。

## 操作步骤

### 添加和查看域名

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**资产中心** > **接入管理**。

2. 在域名列表页面，单击**添加域名**，右侧弹出添加域名页面。

3. 在添加域名页面，根据页面提示配置相关信息，单击**确定**，即可完成添加域名。

4. 在域名列表页面， 单击“域名”，进入域名详情页，可以查看域名的基本信息和域名内容。

### 开启防护开关

1. 在域名列表页面，单击 WAF 开关下的，弹出“确认开启”对话框。

2. 在“确认开启”对话框中，单击**确定**，开启 WAF 开关后，系统会自动根据您的自定义策略和各种攻击设置进行 WAF 防护。

## 编辑域名

1. 在域名列表页面，单击**编辑**，进入编辑域名页面。

2. 在编辑域名页面，可修改服务器配置、代理情况和源站地址等信息，单击确定，即可保存修改。

## 删除域名

1. 在域名列表页面，单击**删除**，弹出“确认删除”对话框。

2. 在“确认删除”对话框中，单击**确定**，即可删除该域名。

> **说明：**
>
> 执行“删除域名”动作后，将会删除域名在后端的配置项。为避免业务受到影响，SaaS-WAF 中删除域名需要您先将 DNS 解析切换至源站或业务相关的记录地址。CLB-WAF 需要您在控制台解绑对应监听器后进行删除动作。

# 接入负载均衡型WAF
# 步骤 1：确认负载均衡配置

最近更新时间: 2024-06-12 15:06:00

# 步骤 1：确认负载均衡配置

如果您的 Web 业务启用了 腾讯云金融专区应用负载均衡（Cloud Load Balancer，简称 CLB），您可以在 Web 应用防火墙实例中接入精准域名防护，以及开启对象默认策略防护。本文档指导您如何开启精准域名的 WAF 防护前，检查确认负载均衡是否配置了对应的 HTTP 及 HTTPS 监听器，监听器是否绑定了有效源站信息。

## 操作步骤

负载均衡型 WAF 通过添加域名的方式与负载均衡的 HTTP 及 HTTPS 监听器进行绑定，实现对经过负载均衡监听器的 HTTP 或 HTTPS 流量进行检测和拦截。在接入负载均衡型 WAF 前，请确保网站业务已在腾讯云金融专区上，并且使用了腾讯云金融专区负载均衡。

为了开启精准域名防护，需要配置负载均衡并且在 HTTP 及HTTPS 监听器配置相应域名，实现业务正常转发。详情请参见 配置 HTTP 监听器 和 配置 HTTPS 监听器。

## 后续步骤

当您确认完成负载均衡配置后，可执行如下步骤：

- 步骤2：域名添加绑定负载均衡
- 步骤3：验证测试

# 步骤 2：添加域名并绑定负载均衡

最近更新时间: 2024-06-12 15:06:00

# 步骤 2：添加域名并绑定负载均衡

如果您的 Web 业务启用了腾讯云金融专区应用负载均衡（Cloud Load Balancer，简称 CLB），您可以在 Web 应用防火墙实例中接入精准域名防护，以及开启对象默认策略防护。本文档将指导您如何在 Web 应用防火墙控制台中，添加精准域名防护并绑定负载均衡。

## 操作步骤

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**资产中心** > **接入管理** > **域名接入**。

2. 在域名接入页面，单击添加域名，配置相关参数，单击确定即可。

**字段说明**

- **所属实例**：选择负载均衡型和实例名称。
- **域名**：在域名输入框中添加需要防护的域名如 `clb.technicalsupport.cn` 。
- **代理情况**：根据实际情况选择是否已使用了高防、CDN、云加速等代理。

  > **说明：**
  >
  > 选择“是”，WAF 将通过 XFF 字段获取客户真实 IP 地址作为源地址，可能存在源 IP 被伪造的风险。

- **地域**：根据实际需求选择。
- **选择域名对应的负载均衡监听器**：根据实际需求选择和配置接入域名的监听器信息。

3. 单击确定，即可返回域名接入。在域名接入可以查看到防护域名 clb.technicalsupport.cn 和负载均衡的负载均衡 ID、名称、VIP 和监听器信息等。

# 后续步骤

当您完成添加域名并绑定负载均衡后，可执行 步骤3：验证测试。

# 步骤 3：验证测试

最近更新时间: 2024-06-12 15:06:00

# 步骤 3：验证测试

本文档将指导您如何验证负载均衡型 WAF 是否生效。

## 操作步骤

1. WAF 通过域名和 CLB 对应监听器进行绑定，对经过 CLB 监听器的域名流量进行防护。验证负载均衡型 WAF 是否生效，请先确保本地电脑可以正常访问在负载均衡不同实例下添加的域名。

   > **说明：**
   >
   > 验证添加在负载均衡中域名型访问是否正常，IPv4 域名请求，请参见负载均衡快速入门的 验证负载均衡服务，IPv6 域名请求，请参见 IPv6 负载均衡快速入门的 步骤4：测试 IPv6 负载均衡。

2. 在浏览器中输入网址 `http://imgcache.finance.cloud.tencent.com:80wow.qcloudwaf.com/?test=alert(123)` 并访问，浏览器返回阻断页面，说明 Web 应用防火墙防护功能正常。

   > **注意：**
   >
   > `wow.qcloudwaf.com` 为本案例中域名，此处需要将域名替换为实际添加的域名。

# 实例管理

最近更新时间: 2024-06-12 15:06:00

# 实例管理

## 操作场景

本文档为您介绍 Web 应用防火墙（WAF）资产中心的实例管理模块。

## 操作步骤

### 新建与查看实例

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**资产中心** > **实例管理**，进入实例管理页面。

2. 在实例管理页面，单击**新建实例**，跳转至购买页，按需购买即可。

### 搜索已有实例

如果有多个实例，需要检索或搜索，则可使用本功能，已有实例支持按地域、类型检索、按关键字搜索。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**资产中心** > **实例管理**，进入实例管理页面。

2. 在实例管理页面，可按类型、地域对已有实例进行筛选，或搜索框通过"实例 ID、实例名称"关键字查找已有实例。

### 管理实例域名

搜索到所需实例并查看后，需要配置实例的域名。

1. 在 实例管理页面，单击管理域名，跳转至域名接入管理页面，搜索和查看当前实例下的域名列表。

2. 在 域名接入页面，可以进行新建域名、编辑域名和删除域名等操作，详情请参见 域名管理。

# 黑白名单防护设置
# 功能简介

最近更新时间: 2024-06-12 15:06:00

## 功能简介

腾讯云金融专区 Web 应用防火墙的黑白名单功能，指的是对经过 Web 应用防火墙防护域名的访问源 IP 进行黑白名单设置，以及对多个 HTTP 特征进行精准白名单设置，主要功能包括： IP 黑白名单设置和精准白名单设置。

- IP 黑白名单设置，支持设置基于域名或全局的 IP 黑白名单规则，支持网段设置。
- 精准白名单设置，支持从 HTTP 报文的请求路径、GET 参数、 POST 参数、 Referer 和 User-Agent 等多个特征进行组合，通过特征匹配来对特定的访问进行加白。

同时，可以添加基于域名的黑白名单或基于全局的黑白名单，生效优先级说明如下所示：

- 黑白名单的优先级仅低于 Web 应用防火墙精准白名单策略，高于其他检测逻辑。
- 黑白名单优先级从高到低顺序：精准白名单策略 > 全局白名单 > 域名白名单 > 域名黑名单 > 全局黑名单 > WAF 其他模块。

# IP黑名单

最近更新时间: 2024-06-12 15:06:00

# IP 黑名单

## 添加 IP 黑名单

**手动添加**

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心** > **黑白名单**。

2. 在黑白名单页面，左上角选择需要防护的域名，单击 IP 黑名单。

3. 在 IP 黑名单页面，单击**添加地址**，进入添加黑名单页面。

4. 在添加黑名单页面，配置相关参数，单击确定。

**字段说明：**

- **IP 地址：**支持任意 IP 地址，例如10.0.0.10或 FF05::B5；支持 CIDR 格式地址，例如10.0.0.0/16或 FF05:B5::/60，使用换行符进行分隔，一次最多添加20个。
  - 选择域名为**全局**时，添加的 IP 地址或 IP 段为全局的黑白名单。

**导入数据**

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 黑名单**。

2. 在 IP 黑名单页面，单击导入数据 > 导入，解析成功后，单击确认导入即可。

# 编辑 IP 黑名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 黑名单**。

2. 在 IP 黑名单页面，选择所需 IP 地址，单击操作列的编辑，修改截止时间和备注，单击确定保存。

# 删除 IP 黑名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 黑名单**。

2. 在 IP 黑名单页面，支持删除单个、部分、全部地址，具体操作如下：

- 单个：选择单个 IP 地址，单击**删除地址**或操作列的**删除**，弹出“确认删除”弹窗。

  > **说明：**
  >
  > 删除后将无法恢复，重新添加才能生效。

- 部分：选择多个 IP 地址，单击**删除地址**，弹出“确认删除”弹窗。

  > **说明：**
  >
  > 删除后将无法恢复，重新添加才能生效。

- 全部：单击**全部删除**，弹出“确认删除”弹窗。

  > **注意：**
  >
  > 将清除当前域名下所有的 IP 黑白名单信息，请谨慎操作！删除后将无法恢复，重新添加才能生效。

3. 在“确认删除”弹窗中，单击**确定**，即可删除地址。

## 导出全部筛选结果

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 黑名单**。

2. 在 IP 黑名单页面，单击搜索框通过 IP 地址对 IP 进行筛选，或单击来源根据来源分类对 IP 进行筛选。

3. 筛选完所需 IP 后，单击导出全部筛选结果，即可导出所需的 IP 筛选结果。

# IP白名单

最近更新时间: 2024-06-12 15:06:00

# IP 白名单

## 添加 IP 白名单

**手动添加**

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击**配置中心** > **黑白名单**，进入黑白名单页面。

2. 在黑白名单页面，左上角选择需要防护的域名，单击 IP 白名单，进入 IP 白名单页面。

3. 在 IP 白名单页面，单击**添加地址**，进入添加白名单页面。

4. 在添加白名单页面，配置相关参数，单击确定。

**参数说明**

- **IP 地址：**支持任意 IP 地址，例如10.0.0.10或 FF05::B5；支持 CIDR 格式地址，例如10.0.0.0/16或 FF05:B5::/60，使用换行符进行分隔，一次最多添加20个。
  - 选择域名为**全局**时，添加的 IP 地址或 IP 段为全局的白名单。
- **截止时间：**永久生效或限定日期。
- **备注：**自定义，50个字符以内。

**导入数据**

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。

2. 在 IP 白名单页面，单击导入数据 > 导入，解析成功后，单击确认导入即可。

## 编辑 IP 白名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。

2. 在 IP 白名单页面，选择所需 IP 地址，单击操作列的编辑，修改截止时间和备注，单击确定保存。

## 删除 IP 白名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。

2. 在 IP 白名单页面，支持删除单个、部分、全部地址，具体操作如下：

- 单个：选择单个 IP 地址，单击**删除地址**或操作列的**删除**，弹出“确认删除”弹窗。

> **说明：**
>
> 删除后将无法恢复，重新添加才能生效。

- 部分：选择多个 IP 地址，单击**删除地址**，弹出“确认删除”弹窗。

> **说明：**
>
> 删除后将无法恢复，重新添加才能生效。

- 全部：单击**全部删除**，弹出“确认删除”弹窗。

> **说明：**
>
> 将清除当前域名下所有的 IP 黑白名单信息，请谨慎操作！删除后将无法恢复，重新添加才能生效。

3. 在“确认删除”弹窗中，单击**确定**，即可删除地址。

## 导出全部筛选结果

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。

2. 在 IP 白名单页面，单击搜索框通过 IP 地址对 IP 进行筛选，或单击来源根据来源分类对 IP 进行筛选。

3. 筛选完所需 IP 后，单击导出全部筛选结果，即可导出所需的 IP 筛选结果。

# 规则引擎

最近更新时间: 2024-06-12 15:06:00

# 规则引擎

本文档为您介绍如何通过 Web 应用防火墙（WAF）设置防护规则，以防护 Web 攻击。

## 背景信息

腾讯云金融专区 Web 应用防火墙（WAF）使用基于正则的规则防护引擎和基于机器学习的 AI 防护引擎，进行 Web 漏洞和未知威胁防护。

腾讯云金融专区 WAF 规则防护引擎，提供基于安全 Web 威胁和情报积累的专家规则集，自动防护 OWASP TOP10 攻击。目前防护 Web 攻击包括：SQL 注入、XSS 攻击、恶意扫描、命令注入攻击、Web 应用漏洞、WebShell 上传、不合规协议、木马后门等17类通用的 Web 攻击。

WAF 规则防护引擎，支持规则等级划分，用户可根据实际业务需要进行规则防护等级设置，并支持对规则集规则或单条规则进行开关设置，可以对 WAF 预设的规则进行禁用操作，同时提供基于指定域名 URL 和规则 ID 白名单处置策略，进行误报处理。

## 操作步骤

### 查看规则分类

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**服务管理** > **Web 规则库**，进入 Web 规则库页面。

在 Web 规则库页面的“防护规则”标签内，可查看当前 WAF 支持防护的攻击分类描述和规则更新动态信息。

当前 WAF 支持防护的攻击分类如下：

| 攻击分类 | 攻击描述 |
| --- | --- |
| SQL 注入攻击 | 在网站实现上，对于输入参数过滤不严，导致 SQL 数据库的内容被非法获取。 |

| 攻击分类 | 攻击描述 |
| --- | --- |
| XSS 攻击 | 当应用程序的新网页中包含不受信任的、未经恰当验证或转义的数据，或者使用可以创建 HTML 或 JavaScript 的浏览器 API 更新现有的网页时，会出现 XSS 缺陷。XSS 让攻击者能够在受害者的浏览器中执行脚本，并劫持用户会话、破坏网站或将用户重定向到恶意站点。 |
| 恶意扫描 | 检测网站是否被恶意扫描。 |
| 核心文件非法访问 | 检测某些配置文件、数据库文件及参数数据，是否被随意下载。 |
| 开源组件漏洞攻击 | 常见 Web 开源组件漏洞产生的攻击行为。 |
| 命令注入攻击 | 注入攻击的一种，包含 Shell 命令注入，PHP 代码注入，Java 代码注入等，若被攻击者成功利用，可导致网站执行攻击者注入的代码。 |
| WEB 应用漏洞攻击 | Web 应用程序的安全性（在 Web 服务器上运行的 Java、 ActiveX、PHP、ASP 代码的安全）。 |
| XXE 攻击 | 由于 XML 处理器在 XML 文件中存在外部实体引用。攻击者可利用外部实体窃取使用 URI 文件处理器的内部文件和共享文件、监听内部扫描端口、执行远程代码和实施拒绝服务攻击。 |
| 木马后门攻击 | 检测木马传播过程或木马上传后与控制端通信行为。 |
| 文件上传攻击 | 当上传文件伪装成正常后缀的恶意脚本时，攻击者可借助本地文件包含漏洞执行该文件。 |
| 其他漏洞攻击 | 由于Web 服务器本身安全和其他软件配置安全或漏洞引起的攻击。 |
| 不合规协议 | HTTP 协议参数，头部请求参数异常。 |

2. 通过**防护规则**标签右侧的规则更新动态，可查看规则更新信息。

## 规则管理

1. 登录Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心** > **基础安全**，进入基础安全页面。

在基础安全页面，单击 **WEB 安全**，在“规则引擎”页签内，可基于域名实现对单条规则的开通设置，决定在规则引擎中是否启用该规则，**所有规则默认开启。**

2. 用户可以通过“规则等级”、“防护等级”或输入“规则 ID、攻击类型、CVE编号”搜索规则集，查看特定规则并进行操作。

> **说明：**
>
> 严格规则等级包含正常和宽松规则，正常规则等级包含宽松规则。

## 规则白名单或误报处理

1. 登录Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心** > **基础安全**，进入基础安全页面。

2. 在基础安全页面，单击 **WEB 安全**，在**规则引擎**页签内，可以实现基于域名 URL 和规则 ID 的加白名单及误报处理。

3. 在“规则引擎”页签，选择所需规则，单击加白名单，弹出添加自定义规则弹窗。

4. 在添加自定义规则弹窗中，配置相关参数，单击确定。

### 字段说明

- **添加规则 ID**：填写需要加白的规则 ID，一条策略可添加1个规则 ID。
- **匹配方式**：加白 URL 路径的匹配方式，支持完全匹配（默认）、前缀匹配和后缀匹配。
- **URL 路径**：需要加白的 URL 路径，同一个域名下 URL 不可重复添加。
- **白名单开关**：白名单策略生效开关，默认为开启。

5. 白名单添加完成后，单击查看白名单，查看该白名单规则，并进行相关操作。

**字段说明：**

- **匹配路径**：需要加白的 URL 路径，同一个域名下 URL 不可重复添加。
- **匹配方式**：加白 URL 路径的匹配方式，支持完全匹配（默认）、前缀匹配和后缀匹配。
- **加白规则 ID**：所设置的加白规则 ID，可以通过攻击日志或规则管理获取。
- **开关**：白名单策略生效开关。
- **修改时间**：最近一次创建或修改策略的时间。
- **操作**：对策略进行编辑或删除操作。
  - 单击**编辑**，修改相关参数，单击**确认**，即可以对规则参数进行修改。
  - 单击**删除**，经过二次确认后，可删除该策略。