

天翼云 • Web 应用防火墙 用户使用指南

中国电信股份有限公司云计算分公司

目 录

| | |
|----------------------|---|
| 1 简介 | 1 |
| 1.1 概念 | 1 |
| 1.1.1 Web 应用防火墙..... | 1 |
| 1.1.2 跨站脚本攻击..... | 1 |
| 1.1.3 SQL 注入攻击 | 1 |
| 1.1.4 命令注入攻击..... | 1 |
| 1.1.5 代码注入攻击..... | 1 |
| 1.1.6 敏感文件访问..... | 1 |
| 1.2 使用场景 | 2 |
| 1.3 计费标准 | 2 |
| 1.4 功能介绍 | 2 |
| 1.5 访问和使用 | 3 |
| 1.5.1 如何访问..... | 3 |
| 1.5.2 如何使用..... | 3 |
| 1.5.3 与其他云服务的关系..... | 3 |

| | |
|------------------------|-----------|
| 2 管理 | 5 |
| 2.1 创建 WAF 实例 | 5 |
| 2.2 配置 WAF 实例 | 6 |
| 2.2.1 接入域名或 IP | 7 |
| 2.2.2 配置策略 | 8 |
| 2.2.2.1 配置全局防护策略 | 8 |
| 2.2.2.2 配置白名单规则 | 11 |
| 2.2.2.3 配置隐私屏蔽规则 | 12 |
| 2.2.2.4 配置误报屏蔽规则 | 14 |
| 2.3 开启防护 | 16 |
| 2.4 管理 WAF 实例 | 16 |
| 2.4.1 查看 WAF 实例 | 16 |
| 2.4.2 停止防护 | 17 |
| 2.4.3 删除 WAF 实例 | 18 |
| 2.5 查看事件日志 | 18 |
| 2.6 开启消息通知 | 22 |
| 3 常见问题 | 26 |

| | |
|-----------------------------------|----|
| 3.1 WEB 应用防火墙支持哪些操作系统？ | 26 |
| 3.2 WEB 应用防火墙支持哪些 WEB 服务框架？ | 26 |
| 3.3 WEB 应用防火墙如何收费？ | 26 |
| 3.4 如何对误报进行处理？ | 26 |
| 3.5 是否可以防护 HTTPS 业务？ | 28 |

1 简介

1.1 概念

1.1.1 Web 应用防火墙

Web 应用防火墙 (Web Application Firewall, WAF), 通过对 HTTP(s) 请求进行检测, 识别并阻断 SQL 注入、XSS 跨站脚本攻击、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击等攻击, 保护 Web 服务安全稳定。

1.1.2 跨站脚本攻击

跨站脚本攻击是一种网站应用程序的安全漏洞攻击, 攻击者将恶意代码注入到网页上, 用户在浏览网页时恶意代码会被执行, 从而达到恶意盗取用户信息的目的。

1.1.3 SQL 注入攻击

SQL (Structured Query Language) 注入攻击是一种常见的 Web 攻击方法, 攻击者通过把 SQL 命令注入到数据库的查询字符串中, 最终达到欺骗服务器执行恶意 SQL 命令的目的。例如可以从数据库获取敏感信息, 或者利用数据库的特性执行添加用户、导出文件等一系列恶意操作, 甚至有可能获取数据库乃至系统用户最高权限。

1.1.4 命令注入攻击

命令注入攻击是通过命令拼接、绕过黑名单等方式在服务端形成对业务攻击的系统命令, 利用各种系统命令调用 Web 应用接口, 从而实现对业务的攻击。

1.1.5 代码注入攻击

代码注入攻击是利用 Web 应用在输入校验上的逻辑缺陷, 或者部分脚本函数本身存在的代码执行漏洞, 而实现的攻击手法。

1.1.6 敏感文件访问

敏感文件访问是指一些涉及操作系统和应用服务框架的配置文件、权限管理文件等作为业务核心敏感的文件被 Internet 上的请求所访问。敏感文件被访问会对业务造成安全风险。

1.2 使用场景

- 常规防护场景

帮助用户防范常见的 Web 安全问题，比如命令注入、敏感文件访问等高危攻击。

用户还可以设置开启、停用 IP 信誉库检测或者扫描器爬虫检测，防范恶意 IP、恶意爬虫扫描器等威胁。

- 0day 漏洞爆发防范场景

当第三方 Web 框架、插件爆出高危漏洞，业务无法快速升级修复，Web 应用防火墙会第一时间升级预置防护规则，保障业务安全稳定。

1.3 计费标准

Web 应用防火墙公测期间免费。

1.4 功能介绍

Web 应用防火墙支持以下功能：

- Web 威胁检测

具有检测各类应用层攻击行为的能力，如 SQL 注入、XSS 攻击、远程溢出攻击、漏洞扫描、Bash 漏洞攻击、远程命令执行、敏感文件访问。

- IP 白名单设置

支持基于 IP（IP 地址、IP 地址+掩码）的白名单设置，符合白名单策略的请求一律放行。

- 扫描器爬虫检测

对恶意的扫描器及爬虫进行检查，防止页面被恶意扫描或恶意抓取。

- 隐私过滤

避免在防护事件日志中，出现用户名或者密码等敏感信息。

- 误报屏蔽

对于误报情况可以加白名单消除，白名单支持通过 URL 的全匹配或前缀匹配，对某些规则 ID 进行忽略设置（比如，某 URL 不进行 XSS 的检查，但其他类型的威胁还可以检测）。

- 非标准端口

防护“80”、“8080”、“443”、“8443”以外的端口。

- 策略管理

在 Web 管理端对相关策略进行开启关闭或相关设置。

- 事件管理

在 Web 管理端查看攻击事件日志、事件通知设置

1.5 访问和使用

1.5.1 如何访问

请使用管理控制台访问 Web 应用防火墙。如果用户已注册天翼云，可直接登录管理控制台，从主页选择“安全 > Web 应用防火墙”。

1.5.2 如何使用

Web 应用防火墙为 Web 服务提供安全防护。由于黑客技术泛滥，导致互联网安全事件频发，Web 服务面临黑客入侵威胁，Web 应用防火墙为 Web 服务提供基础安全防护措施。

用户可以通过开启“IP 信誉库检测”、“扫描器爬虫检测”阻断内置信誉库中的恶意 IP 访问，以及内置的扫描器、爬虫库，阻断非授权的扫描和网页爬取行为。

同时，可以配置防护策略检测 SQL 注入、XSS 跨站脚本攻击、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击等攻击，保护 Web 服务安全稳定。

用户可以查看 Web 服务防护事件日志及统计报告，并可对误报事件进行屏蔽处理，及时了解 Web 服务的安全情况。

1.5.3 与其他云服务的关系

与弹性云主机的关系

Web 应用防火墙为弹性云主机提供 Web 安全防护服务。

与云审计服务的关系

云审计服务记录了 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1-1 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 |
|------------------|--------------|-----------------|
| 开启 Web 应用防火墙防护 | WAF Instance | openWaf |
| 停止 Web 应用防火墙防护 | WAF Instance | stopWaf |
| 更新 Web 应用防火墙防护策略 | Policy | updateWafConfig |

与弹性负载均衡的关系

Web 应用防火墙与弹性负载均衡（以下简称 ELB）绑定，WAF 实例对经过 ELB 的七层负载均衡的流量进行防护。

2 管理

2.1 创建 WAF 实例

操作场景

Web 应用防火墙支持对使用弹性负载均衡产品的 Web 流量进行防护。

在启用 Web 应用防火墙前，请确保域名或 IP 对应的 Web 服务器开通了弹性负载均衡服务。

公测期间单个用户最多 10 个防护对象。

该任务指导用户通过 Web 应用防火墙服务创建 WAF 实例。

前提条件

- 已获取管理控制台的帐号和密码。
- 防护对象对应的 Web 服务器已开通弹性负载均衡服务。
- 域名或者 IP 的流量经过弹性负载均衡（公网）的 HTTP 或 HTTPS 协议监听器。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 单击页面右上角“创建 WAF 实例”。

步骤 4 在弹出的创建 WAF 实例页面，设置“基本信息”，如图 2-1 所示，相关参数说明如表 2-1 所示。

图2-1 创建 WAF 实例

创建WAF实例 ?

Web应用防火墙支持对使用弹性负载均衡产品的Web流量进行防护。
在启用Web应用防火墙前，请确保域名或IP对应的Web服务器开通了负载均衡7层服务。



浏览器/App → 弹性负载均衡 (公网) → Web应用防火墙 → Web服务器

基本信息

* 实例名称：

* 防护对象： 防护对象的输入格式如：www.domain.com 或 192.168.0.1

表2-1 基本信息参数说明

| 参数 | 参数说明 | 取值样例 |
|------|---|-------------------------------------|
| 实例名称 | WAF 实例名称。 <ul style="list-style-type: none">实例名称长度为 1~50 个字符。实例名称由中文、字母、数字、中划线或者下划线组成，但不能只包含中划线和下划线。 | WAF-44df |
| 防护对象 | 用户可设置 WAF 防护的域名或者 IP 地址。 | www.domain.com 或者 192.168.1.1 |

步骤 5 单击“立即创建”，弹出“创建 WAF 实例任务提交成功”页面。

步骤 6 用户可单击“立即刷新，请点击这里”或者等待 15 秒进入 WAF 实例列表。

在 WAF 实例列表中，可以查看申请的 WAF 实例信息，包括“WAF 实例”、“防护对象”、“状态”。

- 防护对象为域名的 WAF 实例，默认状态为“尚未接入”。
- 防护对象为 IP 地址的 WAF 实例，默认状态为“开启（未检测到业务流量）”。

----结束

2.2 配置 WAF 实例

用户需要对已申请的 WAF 实例进行域名接入、配置防护策略，WAF 实例配置完成后才能正常启用。

2.2.1 接入域名或 IP

操作场景

该任务指导用户通过 Web 应用防火墙对申请的 WAF 实例进行域名或者 IP 接入。

- 若用户创建 WAF 实例时设置的防护对象是域名，则需要到 DNS 服务商进行域名接入。
- 若用户创建 WAF 实例时设置的防护对象是弹性负载均衡的公网 IP，则 Web 应用防火墙自动获取当前用户开通了弹性负载均衡的 IP 地址。

WAF 实例创建完成后，WAF 实例立即开启防护，处于“开启（未检测到业务流量）”状态，不需要用户再进行其他操作。

前提条件

- 已获取管理控制台的帐号和密码。
- 已申请 WAF 实例。
- 用户拥有域名的所有权，具有修改域名的 DNS 记录的权限。

操作步骤

创建 WAF 实例后，接入 IP 是 Web 应用防火墙自动获取当前用户开通了弹性负载均衡的 IP 地址，并立即开启防护，不需要用户再进行其他操作。以下是接入域名的操作步骤：

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 单击待接入域名（例如：www.domain.com）的 WAF 实例所在行的“域名接入”，如图 2-2 所示。

图2-2 域名接入

域名接入

请到DNS服务商处，将防护的域名www.domin.com的txt记录修改为

94ae6e2deb20416b8b140b1ca6121700

确定

取消

步骤 4 在弹出的对话框中，查看生成的 txt 记录并执行域名接入的操作步骤。

请前往您的 DNS 服务商处，将防护域名（例如：www.domain.com）的“TXT”记录修改为生成的随机字符串（TXT 记录），例如“94ae6e2deb20416b8b140b1ca6121700”。

步骤 5 TXT 记录修改完成后，单击“确定”，界面右上角弹出“域名接入成功，您可以继续设置防护”，则表示域名接入成功。

用户可在 WAF 实例列表上查看已完成域名接入的 WAF 实例。

----结束

2.2.2 配置策略

2.2.2.1 配置全局防护策略

操作场景

该任务指导用户通过 Web 应用防火墙服务配置全局防护策略，一个 WAF 实例对应一个全局防护策略，对域名进行全局防护。

前提条件

- 已获取管理控制台的帐号和密码。
- 已创建 WAF 实例。
- 已完成域名或者 IP 接入。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 在目标 WAF 实例所在行的操作栏中，单击“修改策略”，进入防护策略配置页面，如图 2-3 所示。

图2-3 全局防护策略

[保存策略](#)

基本设置

检测动作 仅记录

拦截：检测到攻击，立即拦截。
仅记录：检测到攻击，仅记录。

IP信誉库检测 开启

内置的IP信誉库，用于阻断库中的恶意IP访问，放行库中合法的IP访问

扫描器爬虫检测 开启

内置的扫描器、爬虫库，用于阻断非授权的扫描和网页爬取行为

高级设置

白名单 开启

添加放行访问的IP [配置](#)

隐私屏蔽 开启

屏蔽事件日志中的特定敏感信息 [配置](#)

误报屏蔽 开启

忽略某些内置检测规则，用于处理误报事... [配置](#)

步骤 4 按照表 2-2 配置“基本设置”的参数，如图 2-4 所示。

图2-4 基本设置

[保存策略](#)

基本设置

检测动作 仅记录

拦截：检测到攻击，立即拦截。
仅记录：检测到攻击，仅记录。






IP信誉库检测 开启




内置的IP信誉库，用于阻断库中的恶意IP访问，放行库中合法的IP访问

扫描器爬虫检测 开启

内置的扫描器、爬虫库，用于阻断非授权的扫描和网页爬取行为

表2-2 基本设置参数说明

| 参数 | 参数说明 | 设置 |
|----------|--|---|
| 检测动作 | 可选择“拦截”和“仅记录”方式。 <ul style="list-style-type: none"> 拦截：弹性云主机遭受攻击时，Web 应用防火墙发出告警并拦截攻击，用户可通过查看日志了解详情。 仅记录：仅记录遭受的攻击，用户可通过查看日志了解详情。 | 仅记录 |
| IP 信誉库检测 | 内置的 IP 信誉库，用于阻断库中的恶意 IP 访问，放行库中合法的访问。  ：开启状态，默认  。  ：关闭状态。 |  |
| 扫描器爬虫检测 | 内置的扫描器、爬虫库，用于阻断非授权的扫描和网页爬取行为。 |  |

| 参数 | 参数说明 | 设置 |
|----|---|----|
| |  ：开启状态，默认  。  ：关闭状态。 | |

步骤 5 按照表 2-3 设置“高级设置”的参数，如图 2-5 所示。

图2-5 高级设置

高级设置

白名单
添加放行访问的IP

配置













隐私屏蔽
屏蔽事件日志中的特定敏感信息

配置

误报屏蔽
忽略某些内置检测规则，用于处理误报事...

配置

表2-3 高级设置参数说明

| 参 数 | 参数说明 | 设置 |
|------------------|---|---|
| 白 名 单 | 添加放行访问的 IP 地址。  ：开启状态，默认  。  ：关闭状态。 单击“配置”，可以查看 2.2.2.2 配置白名单规则详细配置。 |  |
| 隐 私 屏 蔽 | 隐私信息屏蔽，屏蔽事件日志中的特定敏感信息。  ：开启状态，默认  。  ：关闭状态。 单击“配置”，可以查看 2.2.2.3 配置隐私屏蔽规则详细配置。 |  |
| 误 报 屏 蔽 | 添加内置检测屏蔽规则。忽略内置检测规则，用于处理误报事件。  ：开启状态，默认  。  ：关闭状态。 |  |

| 参数 | 参数说明 | 设置 |
|----|-----------------------------------|----|
| | 单击“配置”，可以查看 2.2.2.4 配置误报屏蔽规则详细配置。 | |

步骤 6 单击“保存策略”，页面右上角弹出“策略保存成功”，防护策略配置生效，如图 2-6 所示。

图2-6 保存策略



----结束

2.2.2.2 配置白名单规则

操作场景

该任务指导用户通过 Web 应用防火墙服务配置白名单规则，符合设置的白名单 IP 或者 IP/Mask 规则，Web 应用防火墙一律放行。

当前版本最多可添加 10 条规则。

前提条件

- 已获取管理控制台的帐号和密码。
- 已创建 WAF 实例。
- 已完成域名或者 IP 接入。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 在目标 WAF 实例所在行的操作栏中，单击“修改策略”，进入防护策略配置页面。

步骤 4 单击“白名单”配置框中的“配置”，进入白名单规则配置页面，如图 2-7 所示。

图2-7 配置白名单规则



步骤 5 单击页面右上角“添加规则”，添加白名单规则，如图 2-8 所示。

图2-8 添加白名单规则



步骤 6 在“IP 地址或 IP 地址段”中输入需要添加的白名单“IP 地址”或者“IP 地址段”。

- IP 地址：添加白名单的 IP 地址，例如，192.168.1.1。
- IP 地址段：IP 地址与子网掩码，例如，192.168.1.1/24。

步骤 7 单击“确认添加”，在页面右上角弹出“添加成功”，则表示添加白名单规则成功。



说明

当您需要修改添加的白名单规则时，可单击待修改的白名单 IP 规则所在行的“修改”，修改白名单规则。

当您需要删除添加的白名单规则时，可单击待删除的白名单规则所在行的“删除”，删除白名单规则。

----结束

2.2.2.3 配置隐私屏蔽规则

操作场景

隐私信息屏蔽，避免用户的密码等信息出现在事件日志中，当前版本最多可添加 10 条规则。

该任务指导用户通过 Web 应用防火墙服务配置隐私屏蔽规则。

前提条件

- 已获取管理控制台的帐号和密码。
- 已创建 WAF 实例。
- 已完成域名或者 IP 接入。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 在目标 WAF 实例所在行的操作栏中，单击“修改策略”，进入防护策略配置页面。

步骤 4 单击“隐私屏蔽”配置框中的“配置”，进入隐私屏蔽规则配置页面，如图 2-9 所示。

图2-9 配置隐私设置规则

高级设置

| | | |
|---|---|--|
| <p>白名单</p> <p>添加放行访问的IP</p> <p><input checked="" type="checkbox"/> 配置</p> | <p>隐私屏蔽</p> <p>屏蔽事件日志中的特定敏感信息</p> <p><input checked="" type="checkbox"/> 配置</p> | <p>误报屏蔽</p> <p>忽略某些内置检测规则，用于处理误报事...</p> <p><input checked="" type="checkbox"/> 配置</p> |
|---|---|--|

步骤 5 单击页面右上角“添加规则”，添加隐私屏蔽规则，如图 2-10 所示，根据表 2-4 配置参数。

图2-10 添加隐私屏蔽规则

×

添加隐私屏蔽规则

* 路径

?

* 正则

?

确认添加

取消

表2-4 添加隐私屏蔽规则参数说明

| 参数 | 参数说明 | 取值样例 |
|----|-------------------|------------------|
| 路径 | 完整的 URL 链接，不包含域名。 | /Admin/login.php |
| 正则 | 密码等敏感信息的正则表达式。 | password:(.*?) |

步骤 6 单击“确认添加”，在页面右上角弹出“添加成功”，则表示添加隐私屏蔽规则成功。

说明

当您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。

当您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。

----结束

2.2.2.4 配置误报屏蔽规则

操作场景

该任务指导用户通过 Web 应用防火墙服务配置误报屏蔽规则，对于误报情况可以添加白名单对误报进行清除，对某些规则 ID 进行忽略设置（比如，某 URL 不进行 XSS 的检查，但其他类型的威胁还可以检测）。

前提条件

- 已获取管理控制台的帐号和密码。
- 已创建 WAF 实例。
- 已完成域名或者 IP 接入。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 在目标 WAF 实例所在行的操作栏中，单击“修改策略”，进入防护策略配置页面。

步骤 4 单击“误报屏蔽”配置框中的“配置”，进入误报屏蔽规则配置页面，如图 2-11 所示。

图2-11 配置误报屏蔽规则

高级设置

| | | |
|---|---|--|
| <p>白名单</p> <p>添加放行访问的IP</p> <p><input checked="" type="checkbox"/> 配置</p> | <p>隐私屏蔽</p> <p>屏蔽事件日志中的特定敏感信息</p> <p><input checked="" type="checkbox"/> 配置</p> | <p>误报屏蔽</p> <p>忽略某些内置检测规则，用于处理误报事...</p> <p><input checked="" type="checkbox"/> 配置</p> |
|---|---|--|

步骤 5 单击页面右上角“添加规则”，添加误报屏蔽规则，如图 2-12 所示。

图2-12 添加误报屏蔽规则

添加误报屏蔽规则

* 路径（完全匹配）

* 规则编号

表2-5 添加误报屏蔽规则说明

| 参数 | 参数说明 | 取值样例 |
|----------|---|------------|
| 路径（完全匹配） | 误报路径，完整的 URL 链接，不包含域名。 | /admin/xxx |
| 规则编号 | “安全总览”下“事件详情”列表出现的误报对应的规则 ID 编号，由 6 位数字组成，不能为空。 | 010001 |

步骤 6 单击“确认添加”，在页面右上角弹出“添加成功”，则表示添加误报屏蔽规则成功。

说明

当您需要删除添加的误报屏蔽规则时，可单击待删除的误报屏蔽规则所在行的“删除”，删除误报屏蔽规则。

----结束

2.3 开启防护

操作场景

该任务指导用户通过 Web 应用防火墙服务开启 WAF 实例的防护操作。

前提条件

- 已获取管理控制台的帐号和密码。
- WAF 实例已完成域名或 IP 接入。
- WAF 实例的“状态”为“关闭”或者“关闭（未检测到业务流量）”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 在目标 WAF 实例所在行的操作列，单击“开启防护”。

步骤 4 在弹出的“开启防护”对话框中，单击“确定”，页面右上方弹出“设置成功”，启用防护操作成功。

在 WAF 实例列表中，WAF 实例的状态切换为“开启”。

说明

如果 WAF 实例的防护对象是 IP 地址，创建 WAF 实例时默认状态为“开启（未检测到业务流量）”。

----结束

2.4 管理 WAF 实例

2.4.1 查看 WAF 实例

操作场景

该任务指导用户通过 Web 应用防火墙服务可查看 WAF 实例名称、防护对象、状态等信息，并可通过选择“防护状态”或者输入“域名/IP”的方式查询 WAF 实例。

前提条件

已获取管理控制台的帐号和密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 查看 WAF 实例信息，如图 2-13 所示。



说明

用户可以通过选择“所有防护状态”、“关闭”、“开启”或者“尚未接入”的方式筛选结果，或者通过输入域名/IP，搜索结果。

图2-13 查看实例

公测期间单个用户最多10个防护对象。

| 所有防护状态 | 请输入域名/IP | Q | 🔄 |
|----------|----------------|------|---|
| WAF实例 | 防护对象 | 状态 | 操作 |
| WAF-44df | www.domin.com | 尚未接入 | 域名接入 修改策略 开启防护 删除 |
| WAF-a187 | www.domin1.com | 尚未接入 | 域名接入 修改策略 开启防护 删除 |

表2-6 参数说明

| 参数 | 参数说明 |
|--------|--|
| WAF 实例 | WAF 实例的名称。 |
| 防护对象 | WAF 实例防护的对象，用户需要防护的域名。 |
| 状态 | WAF 实例的状态，包含： <ul style="list-style-type: none"> • 开启 • 关闭 • 尚未接入 |

----结束

2.4.2 停止防护

操作场景

该任务指导用户通过 Web 应用防火墙服务停止 WAF 实例的防护操作。

前提条件

- 已获取管理控制台的帐号和密码。
- WAF 实例的“状态”为“开启”或者“开启（未检测到业务流量）”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 在目标 WAF 实例所在行的操作列中，单击“停止防护”。

步骤 4 在弹出的对话框中单击“确定”，页面右上方弹出“设置成功”，停止防护操作成功。

在 WAF 实例列表中，WAF 实例的状态切换为“关闭”。

----结束

2.4.3 删除 WAF 实例

操作场景

该任务指导用户通过 Web 应用防火墙服务界面对不再使用的 WAF 实例执行删除操作。WAF 实例删除后，不可恢复。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙”，在左侧导航树选择“WAF 实例”，进入“WAF 实例”页面。

步骤 3 在目标 WAF 实例所在行的操作列中，选择“删除”。

步骤 4 在弹出的对话框中单击“确定”，页面右上角弹出“删除成功”，则说明删除 WAF 实例操作成功。

----结束

2.5 查看事件日志

操作场景

该任务指导用户通过 Web 应用防火墙服务查看事件日志，可查看到一个月内的访问与攻击统计次数、攻击分布以及攻击事件列表。

前提条件

已获取管理控制台的帐号和密码。

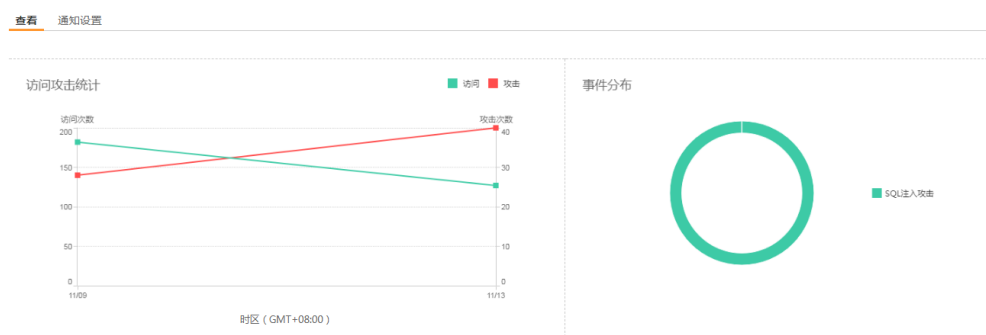
操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙 > 安全总览”，进入 Web 应用防火墙“安全总览”页面。

步骤 3 查看事件日志，如图 2-14 所示。

图2-14 查看事件日志



步骤 4 查看“访问攻击统计”，默认展示一个月内的访问和攻击统计次数，如果数据不满一个月，根据实际天数展示数据，如图 2-15 所示。



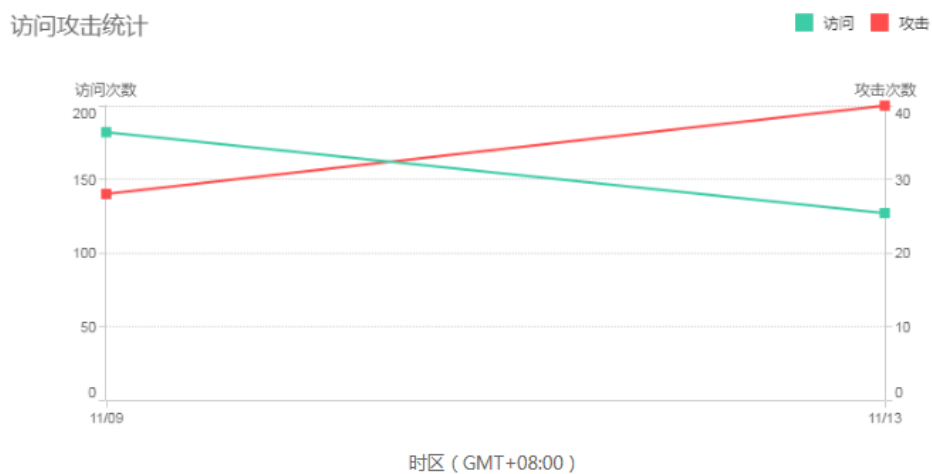
- 仅展示攻击次数统计：可单击  访问。
- 仅展示访问次数统计：可单击  攻击。

图2-15 查看访问攻击统计



步骤 5 查看“攻击分布”，如所图 2-16 示。

图2-16 查看攻击分布

事件分布



- 单击“攻击分布”中的其中一个颜色区域，可查看主机被攻击的类型、攻击的次数、以及占整个攻击分布的比例。
- 当不需要展示某种类型的攻击时，单击右侧对应类型攻击前面的颜色方块，取消在攻击分布的圆环展示。

步骤 6 查看攻击事件详情，可选择显示“最近三天”、“最近一周”或者“最近一个月”的攻击事件详情，如图 2-17 所示。

图2-17 事件详情列表

| 事件详情 | | | | | | | |
|--------------------------|---|-------------|-----|---------|--------|---------------|----------------------|
| | | 最近三天 | | 最近一周 | | 最近一月 | |
| | | | | | | 请输入域名或IP | |
| | | | | | | Q | |
| | | | | | | C | |
| 时间 | 源IP | 防护对象 | URL | 事件类型 | 规则ID | 恶意负载 | 操作 |
| 2017/11/13 11:07:29 G... |  | www.abc.com | / | SQL注入攻击 | 020000 | id=1 or 22=22 | 误报处理 |
| 2017/11/13 11:07:28 G... |  | www.abc.com | / | SQL注入攻击 | 020000 | id=1 or 22=22 | 误报处理 |
| 2017/11/13 11:07:28 G... |  | www.abc.com | / | SQL注入攻击 | 020000 | id=1 or 22=22 | 误报处理 |
| 2017/11/13 11:06:42 G... |  | www.abc.com | / | SQL注入攻击 | 020000 | id=1 or 2=2 | 误报处理 |

攻击事件详情参数说明如表 2-7 所示。

表2-7 事件详情参数说明

| 参数 | 参数说明 |
|-------|------------------------------|
| 时间 | 发生本次攻击的时间。 |
| 源 IP | Web 访问者的公网 IP 地址（攻击者 IP 地址）。 |
| 防护对象 | 发生攻击事件的域名。 |
| URL | 攻击的 URL。 |
| 事件类型 | 发生攻击的类型。 |
| 规则 ID | 自动读取的规则 ID。 |
| 恶意负载 | 发生的恶意负载详情。 |

步骤 7 当攻击事件属于误报时，可单击该攻击事件所在行的“误报处理”添加误报屏蔽策略，如图 2-18 所示。

图2-18 误报处理

×

误报处理

* 防护对象

a.com

* 路径

/login

* 规则ID

20001

确认添加

取消

误报处理参数说明，如表 2-8 所示。

表2-8 误报处理参数说明

| 参数 | 参数说明 | 取值样例 |
|-------|-------------------|--------|
| 防护对象 | 发生攻击事件的域名，系统自动获取。 | - |
| 路径 | 误报事件的 URL 路径。 | /login |
| 规则 ID | 自动读取的内置规则的 ID。 | - |

步骤 8 单击“确认添加”，处理误报，攻击事件详情列表中不再出现此误报。

说明

用户可进入 WAF 实例页面，在发生攻击事件的“防护对象”所对应的“修改策略 > 高级设置 > 误报屏蔽”中，单击“配置”，进入误报屏蔽列表，查看添加的误报屏蔽。

----结束

2.6 开启消息通知

操作场景

该任务指导用户通过 Web 应用防火墙服务对攻击日志进行通知设置。Web 应用防火墙可将拦截的攻击

日志通知发送到用户设置的邮箱或者短信。

开启通知设置后，Web 应用防火墙每 5 分钟发送一次消息通知。

前提条件

- 已获取管理控制台的帐号和密码。
- 已开通消息通知服务。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙 > 安全总览”，进入 Web 应用防火墙“安全总览”页面。

步骤 3 单击“通知设置”，配置消息通知，“通知状态”中选择“开启”，如图 2-19 所示。

图2-19 通知设置

[查看](#)
[通知设置](#)

* 通知状态：☒ 开启 ☐ 关闭

* 通知群组：

| 名称 | 描述 | 操作 |
|-----|-----|---------------------------------------|
| aaa | aaa | 删除 修改 |

步骤 4 单击“新建群组”，创建通知群组，如图 2-20 所示，根据表 2-9 配置参数。

图2-20 新建群组

新建群组

* 名称：

描述：

为了避免用户接受垃圾信息，只有确认后可以成功发送通知。点击确定按钮可以发送验证邮件（短信）。

* 通知列表：

邮箱

+ 添加 您还可以增加29项。

确定

取消

表2-9 新建群组参数说明

| 参数 | 参数说明 | 设置 |
|------|---|-----------|
| 名称 | 通知群组的名称。 名称以字母或者数字开头，由字母、数字、下划线或者连字符组成，且不能为空，长度不能超过256个字符。 | waf |
| 描述 | 新建群组的描述信息。 | test |
| 通知列表 | 可选择输入邮箱地址或者电话号码。 | 根据实际情况配置。 |

步骤 5 单击“确定”，页面右上角弹出“设置成功”，则说明添加群组成功。

步骤 6 在“通知群组”下拉列表中选择已创建的通知群组，例如“waf”。如图 2-21 所示。

图2-21 选择群组

查看 **通知设置**

* 通知状态：☒ 开启 ☐ 关闭

* 通知群组： 

步骤 7 配置完成后，单击“确定”，开启通知设置完成。

----结束

3 常见问题

3.1 Web 应用防火墙支持哪些操作系统？

Web 应用防火墙嵌入在弹性负载均衡服务中，与防护的 Web 服务没有耦合。Web 应用防火墙支持任意操作系统。

3.2 Web 应用防火墙支持哪些 Web 服务框架？

Web 应用防火墙嵌入在弹性负载均衡服务中，与防护的 Web 服务没有耦合。Web 应用防火墙支持任意框架的 Web 服务。

3.3 Web 应用防火墙如何收费？

Web 应用防火墙公测期间免费。

3.4 如何对误报进行处理？

当某种业务频繁误报时，可以在事件日志中，进行误报处理。通过设置 URL 和规则 ID 的忽略，以后该 URL 再次命中设置的规则时，不再告警或者阻断。

步骤 1 登录管理控制台。

步骤 2 选择“安全 > Web 应用防火墙 > 安全总览”，进入 Web 应用防火墙“安全总览”页面。

步骤 3 查看攻击事件详情，可选择显示“最近三天”、“最近一周”或者“最近一个月”的攻击事件详情，如图 3-1 所示。

图3-1 事件详情列表

事件详情

最近三天

最近一周

最近一月

请输入域名或IP

Q

C

| 时间 | 源IP | 防护对象 | URL | 事件类型 | 规则ID | 恶意负载 | 操作 |
|--------------------------|-------------|-------------|-----|---------|--------|---------------|----------------------|
| 2017/11/13 11:07:29 G... | 192.168.1.1 | www.abc.com | / | SQL注入攻击 | 020000 | id=1 or 22=22 | 误报处理 |
| 2017/11/13 11:07:28 G... | 192.168.1.1 | www.abc.com | / | SQL注入攻击 | 020000 | id=1 or 22=22 | 误报处理 |
| 2017/11/13 11:07:28 G... | 192.168.1.1 | www.abc.com | / | SQL注入攻击 | 020000 | id=1 or 22=22 | 误报处理 |
| 2017/11/13 11:06:42 G... | 192.168.1.1 | www.abc.com | / | SQL注入攻击 | 020000 | id=1 or 2=2 | 误报处理 |

表3-2 误报处理参数说明

| 参数 | 参数说明 | 取值样例 |
|-------|-------------------|--------|
| 防护对象 | 发生攻击事件的域名，系统自动获取。 | - |
| 路径 | 误报事件的 URL 路径。 | /login |
| 规则 ID | 自动读取的内置规则的 ID。 | - |

步骤 5 单击“确认添加”，添加误报屏蔽策略，攻击列表中不再出现此误报。

----结束

3.5 是否可以防护 HTTPS 业务？

支持。

用户托管 SSL 证书（在弹性负载均衡服务中进行配置）之后，Web 应用防火墙可以防护 HTTPS 的流量。