

# Web 应用防火墙

## 快速入门



腾讯云

## 【 版权声明 】

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

## 【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

---

## 文档目录

快速入门

  入门概述

  新手常见问题

# 快速入门

## 入门概述

最近更新时间：2023-08-14 14:16:41

本文将指导您快速部署和使用腾讯云 Web 应用防火墙（Web Application Firewall）。首先，您需要购买 WAF 实例；其次，梳理网站域名信息，并完成网站域名接入和防护配置；最后，您可以通过总览报表查看业务和安全概况，及时掌握业务的安全状态；从攻击日志查看详细的流量处置详情，方便调整防护配置以适应业务的特殊需求，并支持通过配置腾讯云可观测平台（TCOP）自定义配置各类告警和告警通知方式，提升业务和安全运维效率。

### 步骤1：实例购买

腾讯云 WAF 支持多实例购买，通过多实例管理，即可适应您对业务本身划分和管理，您也可通过多实例实现异地多活的业务统一就近接入防护。

- 实例采购详情请参见 [购买方式](#)。
- 实例管理和续费详情请参见 [实例管理](#)。

[观看视频](#)

### 步骤2：网站接入

腾讯云 WAF 提供两种产品形态，SaaS 型 WAF 和负载均衡型 WAF。

#### ⓘ 说明：

接入域名需要保证合法，且已完成相关备案，详情请参见 [接入域名相关](#)。

### SaaS 型 WAF 域名接入指南

SaaS 型 WAF 通过为防护域名分配 CNAME，修改网站的 DNS 解析记录，将网站收到的 Web 请求转发给 WAF，从而对网站进行安全防护。配合安全组使用，可以避免攻击者绕过 WAF 直接攻击网站源站。实现上述功能，您需要完成以下步骤：

- [步骤1：域名添加](#)
- [步骤2：本地验证测试](#)
- [步骤3：修改 DNS 解析并验证](#)
- [步骤4：设置安全组](#)
- [步骤5：验证测试](#)

### 负载均衡型 WAF 域名接入指南

负载均衡型 WAF 通过配置域名与腾讯云七层负载均衡（监听器）集群进行联动，对经过负载均衡的 HTTP 或 HTTPS 流量进行旁路威胁检测和清洗，实现业务转发和安全防护分离。实现上述功能，您需要完成以下步骤：

- [步骤1：确认负载均衡配置](#)
- [步骤2：域名添加绑定负载均衡](#)
- [步骤3：验证测试](#)

## 步骤3：防护配置

完成接入的网站访问流量将经过 WAF 保护，WAF 包含多种防护检测模块，帮助网站应对不同类型的安全威胁。其中，规则引擎为默认开启，主要用于防御常见的 Web 应用攻击（例如，SQL 注入、XSS 跨站、WebShell 上传等），其他防护模块需要您手动开启和配置防护规则。

## 步骤4：日志分析

Web 应用防火墙默认只记录攻击日志，在用户购买和开通日志服务后，支持记录基于域名级别的全量访问日志。

### 攻击日志

详细记录攻击产生的时间、攻击源 IP、攻击类型及攻击详情等信息，有助您实时查看和分析威胁攻击，适当调整防护策略，有效满足日常安全运维和业务自身需求。

目前攻击默认为聚类展示，同一请求源 IP 上的同一类型在指定时间内的日志自动聚合一条日志，减少您运维的工作量，提升工作效率。此外，攻击日志也支持全文搜索、模糊搜索和组合条件搜索等检索方式。详情请参见 [攻击日志](#)。

### 访问日志

用于记录 Web 应用防火墙防护域名的访问日志信息，提供开启访问日志开关的域名在用户自定义的日志保存天数内（最大180天）的访问日志记录、查询和下载功能，助力客户等保合规合法。详情参见 [访问日志](#)。

## 步骤5：安全报表

网站业务接入 WAF 防护后，您可以通过 WAF 总览页面，查询当前域名总数、已接入的网站情况、实例情况、最近30天内的网站业务和攻击流量分析数据、最近发布的规则动态，WAF 总览页面帮助您了解网站业务的整体安全状态。详情参见 [访问日志](#)。

## 步骤6：TCOP 配置

网站接入 WAF 防护后，您可以在腾讯云可观测平台（TCOP）配置告警，当 WAF 在网站请求流量中检测到攻击流量异常、业务流量异常时向您发送告警通知，帮助您及时掌握业务的安全动态。方便您快速响应异常情况，及时调整 Web 应用防火墙策略，保证业务稳定性和安全性。详情参见 [TCOP WAF 配置最佳实践](#)。

多实例支持相同域名配置到不同地域的同类型实例中，实现接入配置独立（转发和防护资源），而防护策略配置相同。

# 新手常见问题

最近更新时间：2023-12-27 10:02:02

## 接入相关

### 非腾讯云内的服务器能否使用 WAF?

WAF 支持云外机房用户接入，可以保护任何公网的服务器，包括但不限于腾讯云，包括其他厂商的云，IDC 等。

#### ⚠ 注意：

在中国大陆地区接入的域名必须按照工信部要求进行 ICP 备案。

### WAF 是否支持 HTTPS 防护?

WAF 全面支持 HTTPS 业务。用户只需根据提示将 SSL 证书及私钥上传，或者选择腾讯云托管证书，WAF 即可防护 HTTPS 业务流量。

### WAF 一个防护域名可以设置多少个回源 IP?

WAF 一个防护域名最多可以设置50个回源 IP。

### WAF 是否支持健康检查?

WAF 默认启用健康检查。WAF 会对所有源站 IP 进行接入状态检测，如果某个源站 IP 没有响应，WAF 将不再将请求转发到该源站 IP，直到接入状态恢复正常。

### WAF 是否支持会话保持?

WAF 支持开启会话保持，如需开启，请 [提交工单](#) 联系我们协助您处理。

### 在 WAF 的控制台中，更改配置后大约需要多少时间生效?

一般情况下，更改后的配置在10s内即可生效。

### SaaS 型和负载均衡型 WAF 是否都支持 SSL 双向认证?

SaaS 型 WAF 不支持 SSL 双向认证，负载均衡型 WAF 支持 SSL 双向认证。

## 域名相关

### 如何接入域名?

您可以在 [WAF 控制台](#) 中接入域名，详情请参见 [域名添加](#)。

### 域名回源 IP 地址会变更吗?

WAF 在维护、升级等情况下，可能会变更域名回源 IP 地址。如果变更，我们会提前通过短信、邮件或站内信的方式通知您。具体回源 IP 地址，以控制台 [域名列表](#) 中所查看到的回源 IP 地址为准。

## SaaS 型 WAF 实例域名接入的服务 VIP 地址是否会变化？

为了提供多地以及多地多机房容灾能力，WAF 在维护、升级等情况下，可能会变更服务 VIP 地址。为保障客户业务的稳定性，WAF 只提供 CNAME 方式接入，以支持灵活、弹性的迁移和扩容、缩容能力，不支持直接解析到 VIP 地址或业务应用上直接绑定 WAF 实例的服务 VIP 地址。

## SaaS 型 WAF 实例域名接入的服务 VIP 地址可以申请更新吗？

SaaS 型 WAF 实例不支持申请变更域名的服务 VIP 地址。如果该实例绑定的域名出现服务异常，请先关注是否被 DDoS 攻击；同时可以 [提交工单](#) 联系我们，我们会及时为您处理。

## 域名回源支持哪些方式？

支持域名回源和 IP 回源，您可以根据需要进行选择和配置，详情可参见 [域名添加](#)。

## 域名接入 WAF 之后，如何绑定 CNAME？

您可以参考 CNAME 文档中的 [操作说明](#)，在您的 DNS 服务商处绑定 CNAME。

## 域名列表 WAF 开关关闭后，还会记录日志吗？

WAF 的开关关闭后，WAF 所有的防护功能将会关闭，并进入纯流量转发模式，且不会记录日志。

## 域名删除后重新添加，CNAME 会发生变化吗？

域名删除重新添加，CNAME 不会发生变化，可在 [WAF 控制台域名列表](#) 中，单击域名，在基础设置中查看。

