

ALIBABA CLOUD

阿里云

Web应用防火墙 快速入门

文档版本：20201016

 阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
<code>Courier</code> 字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
<i>斜体</i>	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.快速入门	05
--------	----

1.快速入门

本文将指导您快速部署和使用阿里云Web应用防火墙WAF（Web Application Firewall）。您需要先购买WAF实例，然后完成网站接入和网站防护配置，即可为网站开启WAF防护。开启网站防护后，您可以通过WAF安全报表查看攻击防护记录和访问统计信息，掌握业务的安全状况。

步骤1：购买WAF实例

1. 登录[Web应用防火墙控制台](#)。
2. 在欢迎使用Web应用防火墙页面，单击购买包年包月或者开通按量付费，前往产品购买页面。如果您已经开通Web应用防火墙，则欢迎使用Web应用防火墙页面不会出现，您可以直接在Web应用防火墙控制台使用产品，具体请参见[步骤2：网站接入](#)。

欢迎使用Web应用防火墙

3. 在Web应用防火墙（包月）或者Web应用防火墙（按量计费）页面，选择需要开通的产品版本和规格，并完成购买。具体操作请参见[开通Web应用防火墙](#)。
4. 完成购买后，返回Web应用防火墙控制台。

步骤2：网站接入


网站接入指将需要防护的网站域名接入WAF实例，并修改网站域名的DNS解析到WAF，使访问网站的流量经过WAF，并受到WAF的防护。

 **说明** 请确保在执行网站接入前，您已完成Web应用防火墙访问其他云资源的授权。首次访问[Web应用防火墙控制台](#)的资产识别页面会要求进行授权，具体操作请参见[授权WAF访问云资源](#)。

1. 添加网站。
 - i. 在网站接入页面，单击添加域名。
 - ii. （可选）在域名一键接入页面，选择要添加的网站域名和协议类型，并单击[立即自动添加网站](#)。WAF支持自动添加当前阿里云账号下的网站资产。如果您的阿里云账号下没有检测到网站资产，则域名一键接入页面不会出现，建议您参照下一步手动添加域名。
 - iii. 在添加域名页面，根据配置向导手动添加网站域名信息。具体操作请参见[手动添加网站](#)。

 **说明** 如果您的网站使用了DDoS高防、CDN等代理服务，则WAF前是否有七层代理（高防/CDN等）参数一定要选择是，否则会导致WAF无法获取访问网站的客户端的真实IP。

成功添加网站后，您可以在网站接入页面查看网站域名对应的WAF CNAME地址。

 **注意** 如果您的网站支持HTTPS协议，则在完成网站接入后您必须上传网站域名绑定的SSL证书，保证WAF可以正常处理HTTPS协议流量。具体操作请参见[上传HTTPS证书](#)。

2. 修改网站域名的DNS解析，将网站域名解析到对应的WAF CNAME地址。
 - o 网站未使用WAF以外的代理服务（例如DDoS高防、CDN）：前往域名DNS解析服务商的管理系统（如果您使用阿里云解析DNS，则只需登录[云解析DNS控制台](#)），添加一条CNAME记录，并使用WAF提供的CNAME地址作为CNAME记录值。



具体操作请参见[修改域名DNS](#)。

- 网站使用了其他代理服务（例如DDoS高防、CDN）：前往代理服务的控制台，将代理服务的回源地址修改为WAF提供的CNAME地址，保证WAF可以接收到网站的访问请求。

具体操作请参见[同时部署WAF和DDoS高防](#)、[同时部署WAF和CDN](#)。

步骤3：配置网站防护策略

完成接入流程后，网站访问流量将经过Web应用防火墙保护。Web应用防火墙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，其中正则防护引擎和CC安全防护模块默认开启，分别用于防御常见的Web应用攻击（例如SQL注入、XSS跨站、webshell上传等）和CC攻击，其他防护模块需要您手动开启并配置具体防护规则。更多信息，请参见[网站防护配置概述](#)。

步骤4：查看安全报表

您可以在安全报表页面获取已接入防护的网站的防护记录和访问统计信息，具体操作请参见[查看安全报表](#)。

