Web 应用防火墙

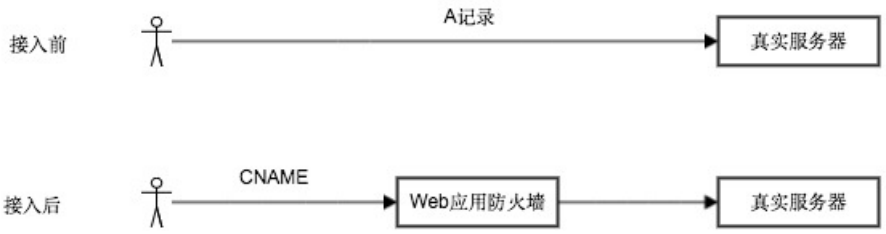
接入指南

阿里云
aliyun.com

接入指南

DNS接入WAF

在WAF控制台配置过域名后，并不代表网站已经被WAF防护了。必须将域名指向WAF，让流量切至WAF，才能受到WAF防护



1.系统检测到未接入WAF时，会在控制台显示：未检测到cname接入且无流量。

判断标准：域名未指向cname，且最近数分钟该域名无流量经过WAF时

2. 已接入的会显示：已接入WAF

3.如果您是CDN/高防 -> WAF 的架构，请确定高防/CDN回源到了WAF的IP或者cname

CDN配置范例：

4.目前cname接入每1小时检测一次，流量每数分钟检测一次，如果确认已正确接入，可以1小时后再次查看状态

操作步骤

1. 获取加速域名

在"Web应用防火墙"找到生成的CNAME

2. 变更DNS解析，接入"Web应用防火墙"（以万网DNS为例）

- 登录万网会员中心
- 点击会员中心左侧导航栏中的【产品管理】-"我的云解析"进入万网云解析列表页。
- 点击要解析的域名，进入解析记录页。
- 进入解析记录页后，点击新增解析按钮，开始设置解析记录。

- 记录类型选择为CNAME，主机记录填写对应的子域名（如www.aliyundemo.cn 的主机记录为：www ）。记录值填写"Web应用防火墙"对应域名的cname

- TTL为域名缓存时间，您可以按照您的需求填写，参考值为3600
- 填写完成后，点击保存按钮，完成解析设置

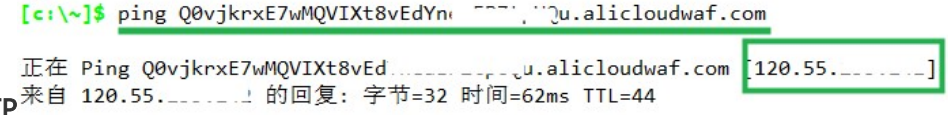
注意事项

同一个主机记录，CNAME解析记录值只能填写一个，您可以修改为"Web应用防火墙"的地址

同一个主机记录，A记录和CNAME记录是互斥的，您可以修改为CNAME类型，并填入CNAME

如果DNS服务商不允许直接从A记录修改为CNAME记录，需要您先删除A记录，增加CNAME记录，注意删除新增过程需要快，如果删除后，长时间没有添加CNAME值，可能导致域名解析不到结果

MX记录和CNAME记录是互斥的，如果您必须保持MX记录，可以将用A记录方式指向WAF的IP，WAF的IP获取可以采取：ping 一下 cname，得到的IP即为WAF IP。直接配置 A 记录，记录值写此IP



Web应用防火墙简介

Web应用防火墙(Web Application Firewall, 简称 WAF)基于云安全大数据能力实现，通过防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，过滤海量恶意访问，避免您的网站资产数据泄露，保障网站的安全与可用性。

Web应用防火墙是针对单个域名提供安全防护的产品，接入前后对比如下图：

接入准备

- 以a.com和b.com为例：

接入域名	源站ip	业务类型	业务端口	源站安全限制检查	是否已经备案
a.com	42.121.192.11,42.121.192.12	http,https	80,443	无安全防护设备	已备案
b.com	42.121.192.11,42.121.192.12	http,htpps	80,443	无安全防护设备	已备案

- 检查需要接入Web应用防火墙的业务域名和服务器IP，同时确认如下几点：
  - 该域名仅提供80,443端口的业务。（如有其他端口如8081、8082，请提前说明，我们会确认是否支持）
  - 该服务器IP未安装相关安全防护软件，如果安装需将Web应用防火墙回源地址加入白名单中防止被误拦截。
  - 该域名是否已经在阿里云完成备案，未备案的域名无法访问会被阿里云备案系统拦截。

接入Web应用防火墙

- 第1-4步不影响实际业务，可以提前完成配置，并且完成Web应用防火墙的配置检查。
- 第5步可能会影响修改dns解析的链路访问，如果有出现问题可以进行操作回滚来恢复，影响范围较小。经过第4步确认出现问题概率较低。

- 第7步可能会影响全部链路访问，如果出现问题可以进行操作回滚来恢复，影响范围大。经过第6步确认出现问题概率低。

详细步骤

登陆云盾控制台-网络安全-Web应用防火墙 控制台地址，如未开通请先开通该服务。

添加防护业务

- 域名：需要接入的域名（支持泛解析，a.com 和 www.a.com 是2个不同的域名）
- 协议类型：业务对外提供的协议类型（如果有https业务，需要在此处勾选https协议，证书在配置完成后上传）
- 源站ip：业务对应的真实服务器地址

上传https证书（如有）

修改电脑的本地hosts文件，让本地的访问经过Web应用防火墙，在不变更业务的情况下，即可进行业务通过Web防火墙墙后的测试，hosts文件修改方式参照 帮助文档

修改dns记录，切换部分链路（移动、海外线路或小流量运营商）流量到Web应用防火墙，并使用17测平台测试对应运营商的业务联通性和访问速度情况。

确认切换的部分业务是否正常。

修改dns记录，切换全部链路流量到Web应用防火墙，并使用 17测平台测试所有运营商的业务联通性和访问速度情况。(DNS配置方式：https://help.aliyun.com/document_detail/35620.html)

确认全部业务是否正常。

如果所有域名都已经切至Web应用防火墙。为了防止直接攻击源站，可以按照如下方式，配置ECS安全组或SLB白名单：https://help.aliyun.com/document_detail/42726.html

常见问题解决

故障切换

Web应用防火墙在企业版、旗舰版中(查看详情)提供多机房冗灾备份的能力，能够在Web应用防火墙单机房故障或者不可用的时候自动切换到备份机房，无需您人工参与，切换生效时间在1-30分钟（视各地DNS缓存为准

）

其他版本或者极端情况所有Web应用防火墙不可用的情况下，我们会直接解析cname地址到您的真实服务器上保证您业务的可用性。切换生效时间在1-30分钟（视各地DNS缓存为准,如果您源站做了访问限制如ecs安全组、防火墙访问控制等，则需要收到我们短信通知后进行限制解除来保证业务的可用。）

504错误

504错误说明该域名未在Web应用防火墙进行配置或者配置未生效，出现此错误后请检查是否遗漏了相关域名的配置，如果确认配置正常且出现504错误，请先修改dns解析到源站ip恢复业务，再与我们联系进行问题排查。

502错误

502错误说明Web应用防火墙访问您源站ip的时候出现了链接错误（连接失败、连接超时等），一般情况刷新业务即可恢复。如果多次刷新仍然出现502错误，请先检查是否源站的安全限制拦截了Web应用防火墙的访问ip，如果没有请先修改dns解析到源站ip恢复业务，再与我们联系进行问题排查。

客户端访问https业务失败

目前Web应用防火墙使用SNI协议对https协议进行支持，部分客户端可能无法支持sni协议。详细信息

源站安全组和白名单配置指南

为了更好的对网站进行防护，防止黑客直接攻击源站IP，建议配置ECS安全组或SLB白名单

配置前，请确保该ECS或SLB实例上，所有域名都已经切至WAF

配置指南：

1. 首先在Web应用防火墙（WAF）控制台，拿到WAF所有回源IP段：

2. 配置只允许WAF回源IP进行访问：

- **源站是ECS**：
  - 配置安全组，公网入方向：80-443允许Web应用防火墙回源IP访问，优先级1
  - 配置安全组，公网入方向：80-443拒绝0.0.0.0/0的访问，优先级100
  - 安全组配置手册：https://help.aliyun.com/document_detail/25833.html
- **源站是SLB**：
  - 配置白名单，只监听Web应用防火墙回源IP访问
  - 白名单配置手册：https://help.aliyun.com/document_detail/27673.html