Web 应用防火墙

接入指南







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 Million Con Million · 正常 BAAKAD Million · Mill

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:



<	× cdn.aliyundemo.cn *返回域名列表						
基本信息	CNAME绑定						
防盗链 CNAME: cdn.aliyundemo.cn.w.kunlunca.com							
鉴权配置	域名信息						
缓存配置	域名: cdn.aliyundemo.cn						
设置HTTP头	源站: Q0vjknxE7wMQVIXt8vEdYneaEPZtpUQu.alicloudwaf.com:80 源站写Web应用防火墙生成的cname						
安全防护	业务类型: 图片小文件加速						
	基础配置						
	页面优化 🕢 :						
	range回源 📀 :						
	协议跟随回源@: 使用HTTPS的用户需要打开						
	回源host②:						

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

83	E0050812	//高与服务 *		Q	8次 日手初版	Accesskeys	工448895 ♥ 19466 1	800与又归。 00.	**@allyun-test.com	×
- 7*	品与服务 ◇	Web/EHINO XAR(MB000)		续费						
=	云服装器 ECS	您购买的服务到期时间是: 2018-07-14,							×	
4	负载均衡	一周攻击状况 * 云雪先知可有	地发现安全扁周,从根源上降低被攻击概题	5、洋情壶署。		防护规则更新				
•	对象存储 OSS					[2016-07-08] XSSB5	护规则(POST)			
•	云楯	* Web应用攻击 348 次	※C C 校击 62 次	(B), 访问控制事件 0次		[2016-07-07] HTTP	Header SQLi主入即的中规则			
×	CON					[2016-07-04] Kesion	iCMS SQL注入0day防护			
0	Web应用防火编	应用配置								
ŵ.	DDoS的验	在配置完成名后,若需要防护生效、必须在您	的DNS服务圈处添加城省对应的Chame,保	征网站流量正常经过Web应用防火墙。						
•	城名	城名 🔻 www.aliyundemo.cn	接線				SE	原加18个城名,还可以3	States ^ States	
	云数据库 RDS 版	城名	业员可用性	安全状态	安全开关				操作	
	反戰詐服得	14 N		in the second second	Waff53P : 155	A		and a	_	
۵	动间控制	www.aliyundemo.cn	http: ● 正常	最近同天内无攻击	CC防护:正常 精准访问控制:	开启		防护管理	「「「「」」」」	
	CA证书服务	Cname Q0vjkrxE7wMQVDtt8vEdYneaEPZtpU0	Qu.alicloudwaf.com							
• 用	ምቀፅ ወ	ABB PERMINANCE								
2	账号管理						共有1条,每	页显示:10条 «	< 1 > >	F

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。



hichina.com

点击这里开始设置解析记录							
新增解	新劃除		首系	浙记录日志	🔓 导出解析记录		
	记录类型會	主机记录(RR) ≜	解析线路會	记录值	MX优先级 會		

- 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

hichina.com

81221624F #359	记录米利法塔CNAME	約 4	Q新记录日志	6 导出解析记录	Q	按索
- i28,82 *	主机记录(RR) ★	解析线路會	记录值	MX优先 會 级	TTL	操作[何时生效?]
CNAME .	.hichina.com	默认 •		10	分钟 💌	<i>87</i> 87 2 •
	填写域名前缀,如	www	在此	真写指向的另-	一个域名	

- 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

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 [c:\~]\$ ping Q0vjkrxE7wMQVIXt8vEdYn(________u.alicloudwaf.com

正在 Ping Q0vjkrxE7wMQVIXt8vEd......u.alicloudwaf.com [120.55.....] 写此IP ^{来自} 120.55......」的回复: 字节=32 时间=62ms TTL=44



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:





- 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. 11,42.121.1 92.12	http,https	80,443	无安全防护 设备	已备案
b.com	42.121.192. 11,42.121.1 92.12	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,防止黑客直接攻击通站ID,建议配置ICC安全组式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:



æ	管理控制台	产品与服务 ▼	Q 搜索	🛛 手机版
	Ш	Web应用防火墙(旗舰版) 应用配置 安全报表 业务分析		
→ ₹	*品与服务 🗘			
	云服务器 ECS	忽闷头的服势到期时间是:2018-07-14。		
4	负载均衡	一周攻击状况 ▼ 云首先和可常您发现安全漏洞,从根源上降低级攻击制率,详慎重着。		
a	对象存储 OSS	Web应用攻击 。 ····································	事件	
٥	云盾	→ 5612 次 ² ² 662 次 ^(の) , 0次		
×		应用配置		
۲	Web应用防火墙		火槽	
łŏį;	DDoS防护	帮助中心: 快速工单入口 即时沟通入口 WAF回源IP段 如何更好的保护网站?	X-H0	
₿	域名	域名 ▼ 请输入关键字进行域名模糊查询 搜索		
*	云数据库 RDS 版	域名 业务可用性 接入状态 安全状态	5	

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