# 解决方案实践

# Web 网站基础安全防护

文档版本1.0.0发布日期2023-08-15





### 版权所有 © 华为技术有限公司 2024。 保留一切权利。

非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部,并不得以任何形式传播。

### 商标声明

### 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束,本文档中描述的全部或部分产品、服务或 特性可能不在您的购买或使用范围之内。除非合同另有约定,华为公司对本文档内容不做任何明示或暗示的声 明或保证。

由于产品版本升级或其他原因,本文档内容会不定期进行更新。除非另有约定,本文档仅作为使用指导,本文 档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 安全声明

### 漏洞处理流程

华为公司对产品漏洞管理的规定以"漏洞处理流程"为准,该流程的详细内容请参见如下网址: https://www.huawei.com/cn/psirt/vul-response-process 如企业客户须获取漏洞信息,请参见如下网址: https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目录

1 方案概述	1
2 资源和成本规划	
3 实施步骤	4
3.1 准备工作	4
3.2 快速部署	8
3.3 开始使用	
3.4 快速卸载	
4 附录	
5 修订记录	16



## 应用场景

该解决方案基于华为云Web应用防火墙 WAF构建,可以帮助企业网站业务流量进行多 维度检测和防护,全面避免网站被黑客恶意攻击和入侵。适用于如下场景:

- 银行系统/金融机构、政府/事业单位、医疗、高校、科研领域网站防御场景;
- 满足Web应用系统,等保合规、保障网站业务安全的场景;
- 防应用层攻击导致业务中断、数据泄密等场景;
- 有效应对活动特殊时期激增的业务流量和恶意流量攻击的场景。

### 方案架构

该解决方案基于华为云Web应用防火墙 WAF构建,可以帮助企业网站业务流量进行多维度检测和防护,全面避免网站被黑客恶意攻击和入侵。

### **图 1-1** 方案架构图



该解决方案部署如下资源:

- 创建一台云模式入门版Web应用防火墙 WAF,用于对HTTP请求进行检测,保证 Web服务安全稳定。
- 在Web应用防火墙WAF上一键添加防御域名,提高配置域名的便利性,构建风险 全面可控的网站安全架构,保障网站业务连续可用。

## 方案优势

- 防御全面

   一键添加WAF防御域名,WAF预置丰富的攻击特征签名库,可检测数十类通用
   Web攻击特征,轻松阻断多种Web攻击。
- 精准高效
   采用规则和AI双引擎架构,默认集成华为最新防护规则和优秀实践;企业级用户 策略定制,支持拦截页面自定义、多条件的CC防护策略配置、海量IP黑名单等, 防护更精准。
- 一键部署
   该解决方案提供一键启动部署,5分钟即可自动化完成环境的部署。

## 约束与限制

- 该解决方案部署前,需注册华为账号并开通华为云,完成实名认证,且账号不能 处于欠费或冻结状态。如果计费模式选择"包年包月",请确保账户余额充足以 便一键部署资源的时候可以自动支付;或者在一键部署的过程进入费用中心,找 到"待支付订单"并手动完成支付。
- 同一账号在同一个大区域(例如华北区域)只能选择一个Web应用防火墙服务版本。
- 如果涉及WAF的退订与重新购买,请确保重新购买的WAF与原WAF在同一区域, 如果不在同一区域,原WAF中配置的数据将不能保存。此时,您需要在购买WAF 后,将防护域名重新接入WAF,并根据防护需求为域名配置相应的防护规则,详 细说明请参见Web防火墙官方帮助文档。
- 使用中国大陆节点服务器部署的Web网站,您需要注册域名,并在开通网站前按照工信部要求办理网站备案,以确保您的网站可以通过域名正常访问。华为云支持一站式完成域名注册、实名认证、网站备案和网站解析等操作,详细操作请参考域名注册服务 Domains流程指引。



该解决方案主要部署如下资源,各项花费如<mark>表2-1</mark>所示,具体收费标准请参考华为云官 网<mark>价格详情</mark>,实际收费以账单为准。

表 2-1 资源和成本规划(仅供参考)

华为云服务	计费说明	每月花费
Web应用防火墙服务	• 入门版: 99元/月	99元
合计:	-	99元



- 3.1 准备工作3.2 快速部署3.3 开始使用
- 3.4 快速卸载

# 3.1 准备工作

# 创建 rf\_admin\_trust 委托(可选)

**步骤1** 进入华为云官网,打开<mark>控制台管理</mark>界面,鼠标移动至个人账号处,打开"统一身份认证"菜单。

图 3-1 控制台管理界面



#### 图 3-2 统一身份认证菜单

简	体中文	EDMENMEDMED MEMMEN
	基本信息	已实名认证
	安全设置	
ţ,	我的凭证	
ŝ	统一身份认	人证
	切换角色	
2	标签管理	
	操作日志	
2		退出

### **图 3-3** 委托列表

委托 ③						创建委托
删除 您还可以创建49个委托。				全部类型	▼ 请输入委托名称进行搜索	Q
● 委托名称ID 1Ξ	委托对象 ↓Ξ	要托时长 ↓Ξ	创建时间 15	描述 ↓Ξ	操作	
rt_admin_trust	云服务 RFS	永久	2023/05/31 11:07:56 GMT+08:00	-	接权 修改 翻除	

- 如果委托存在,则不用执行接下来的创建委托的步骤
- 如果委托不存在时执行接下来的步骤创建委托
- **步骤3** 单击步骤2界面中的"创建委托"按钮,在委托名称中输入"rf\_admin\_trust",委托 类型选择"云服务",输入"RFS",单击"下一步"。

步骤2 进入"委托"菜单,搜索"rf\_admin\_trust"委托。

### **图 3-4** 创建委托

* 委托名称	rf_admin_trust	
★ 受托类型	<ul> <li>普通帐号</li> <li>将帐号内资源的操作权限委托给制</li> <li>云服务</li> <li>将帐号内资源的操作权限委托给纸</li> </ul>	其他华为云帐号。 《为云服务。
* 云服务	RFS	•
★ 持续时间	永久	•
描述	靖输入委托信息。	
		0/255

步骤4 在搜索框中输入"Tenant Administrator"权限,并勾选搜索结果,单击"下一步"。

### **图 3-5** 选择策略

2020 2020 2020 2020 3 max		RHE
委托"ff_admin_trust2"将拥有所法策维格		制行政部分的新任
查看已迭(1) 从其他区域项目复制的7页	金部树型 • 所有云服务	Tenant Administrator X Q
✓ 名称	英型	
Terant Administrator 全部互張的管理员(約404/M管理研究)	系统角色	

步骤5选择"所有资源",并单击"下一步"完成配置。

### 图 3-6 设置授权范围

() 2494 () Add () Add	田別日版
① 有黑黑色的市田和沙漠地、其供用学以下接仅包围方象、更使于影响小以提供、可由行道师、了新动动物集团的运用转属包括中省部的核心国内客	×
选择硬权范围方案	
<ul> <li>所有更原</li> </ul>	
授权后,IAM用小可以据属存预使用新有中新有资源。包括企业项目、区域项目和企用最多资源。	
里轩我也为金	

步骤6 "委托"列表中出现"rf\_admin\_trust"委托则创建成功。

### **图 3-7** 委托列表

委托 ①						创建委托
制除 想还可以创建49个委托。				全部类型	<ul> <li>■ 清縮入委托名称进行搜索</li> </ul>	Q
委托名称/ID 1Ξ	委托对象 ↓Ξ	委托时长 ↓Ξ	创建时间 15	揺迷 1Ξ	操作	
rf_sdmin_trust	云服务 RFS	永久	2023/05/31 11:07:56 GMT+08:00	-	授权 停改 勤除	

### ----结束

## 检查源站

步骤1 登录华为云控制台,选择源站所在的区域.。

### 图 3-8 选择 Region

HUAWEI 4	約云 🗌 🞧 🗄	謝台 ♀ 北京四		×		搜索	(	<b>)</b> 费用与成本	资源 企业	开发工具	备案	支持与服务
Ξ	总览	资源管理	运维管	管理 安全管理	里 自定义控	制台 ③						
۵ ۵	请输入关键词	夏家服务										Q
6	快捷导航										€	)添加
AXA	弾性云服务器	& ECS	云耀云	服务器 HECS	裸金属服务器 BI	ΛS	弹性伸缩 AS		云硬盘 EVS			
Б	云备份 CBR		对象存	储服务 OBS	虚拟私有云 VPC		弹性负载均衡 ELB		弹性公网IP	EIP		
~	云数据库 RD	IS	城名注	册 Domains	NAT网关 NAT							
6 6	<b>最近访问</b> 裸金属服务器 B	MS 弹性公网IP EIP										
Ð	<b>我的资源</b> [全局 部分资源可能会)	] 由于未接入服务,而无法在此	/模块中展/	示。 已支持的服务和区域							查看更多	る源
⇔	<b>云服务器</b> 弹性云服务器	ECS	249	<b>实例</b> 云数据库 RDS	5	弹性伸缩组 弹性伸缩 AS	:	2 磁盘 云硬盘 EV	ſS		266	
Ð	带宽 虚拟私有云 V	PC	270	安全组 虚拟私有云 VPC	165	虚拟私有云 虚拟私有云 VPC	11	7 弹性公网。 虚拟私有法	IP E VPC		276	
	<b>监听器</b> 弹性负载均衡	ELB	7	负载均衡器 弹性负载均衡 ELB	5	桶 対象存储服务 OBS	6	0 集群 云容照引導	≌ CCE		2	

# **步骤2** 查看源站服务器的弹性公网IP。在左侧导航栏,选择"弹性云服务器ECS",在华为云控制台查看源站服务器的弹性公网IP地址。

### 图 3-9 查看源站服务器的弹性公网 IP

=	忠派		弹性云服务器 ②						() 评	() アー建設新	A 最新均态   B	使用指南 购买种性云服务器
6	弹性云服务器		我的ECS: 非北-北京四 (40)   移用・デ	州 (34)   中国-香港 (4	)   亚太·新加坡 (4)   华北·乌言	i棄布一 (2)   豆太·長谷 (	1)					с
۲	大陸大阪务線 NEW	do.	开机 关机 重置出码	●1 天政信								C 🛞 🗂 🏭 🗏
w	裸金屬服务器		SR: 1177195 🔘 20102259.41									× 0 @ Q
•	云硬盘		_ 各称/ID ↓Ξ	重控	可用区 🏹	No V	规称·统级	IP地址	计表模式 🏹	企业项目	标签	操作
0	专属分布式存储	•		Ø	可用区1	😏 运行中		4 ( 6	投票计费	) default	-	远程破录   更多 ▼
6	現象服务											
٢	建性中国	٠		•	可用区7	③ 运行中			按照计算	default	-	這程登录 ● 更多 ▼
4	密码对	ø										
۲	云服务瞬间	. '	4									
&	云黄份	d0										
0	云服务器备份	d <sup>o</sup>										

步骤3 在浏览器栏输入"http://EIP:端口"访问预置页面,验证源站能否正常访问。

### ----结束

# 3.2 快速部署

本章节主要帮助用户快速部署Web网站基础安全防护解决方案。

参数名称	类型	是否可选	参数解释	默认值
domain	string	必填	指定要保护的 域名。	空
address	string	必填	客户端访问的 Web 服务器的 IP 地址或域 名。	空
web_port	string	必填	Web 服务器使 用的端口号。 取值范围为 0 到 65535。	80

**步骤1** 登录**华为云解决方案实践**,选择"Web网站基础安全防护"解决方案。数据中心下拉 菜单可以选择需要部署的区域,单击"一键部署",跳转至解决方案创建堆栈界面。

图 3-10 解决方案实施库



步骤2 在选择模板界面中,单击"下一步"。

### **图 3-11** 选择模板

< 立即创建资源	機	
1 选择模板 ———	— ② R显参数 ———— ③ 安排线设置 ———— ④ R置体A	
* 创建方式	已有補穀 在可说化读唱器创建	
* 模板来源	我论她被 URL 上传模板	
	每个资源线能是基于银灰台运的,银版中必须要有 带 <u>带代码文件</u> ()扩展各为时间fifon)。	
★ 横板 URL	https://documentation-samples.obs.cn-north-4.myhu.	
	能统内至少需要有需需代码文件,文件不能超过1MB。	
	● 进源编排服务不会在管理进源之外的场景使用些上传的数据,我们不会对容的模板进行加密,对于参数中的敏感数据,推荐使用KMS成DEW托管进行加密,目前控制台中支持自动使用KMS加密印的敏感参数。	
		0
		0
		R
		<del>य</del> —न

步骤3 在配置参数界面中,参考表3-1完成自定义参数填写,单击"下一步"。

### **图 3-12** 配置参数

< 立即创建资	源栈					
① 选择模板 ——	—— 2 <b>記</b> 書参数 ——	- ③ 资源线设置 ④ 配置	确认			
★ 资源栈名称	website-security 资源线名称以中文或英文开始	;,支持中文、大小写英文、数字、下划线、;	中划线,128个字符之内 <b>,资源线名称不能</b>	( <b>1</b> 4.		
描述	Web网站基础安全防护	2 11/255				
<b>配置参数</b> 请输入关键的	搜索参数名称	Q				
参数名称		值	类型	描述		
* domain			string	指定要保护的城名。		
* address			string	客户确访问的Web服务器的IP地址或域名。		G
* web_port		80	number	Web服务器使用的端口号,取值范围为0-65535,默认为80		0
						0
					Ŀ	5 <b>T-5</b>

步骤4 在资源栈设置页面中,权限委托选择 "rf\_admin\_trust"(可选),单击"下一步"。

### **图 3-13** 资源栈设置

< 立即创建资源相	1
(1) 选择模板 ————	② EE98 ③ 此限和28 ④ EE984.
* 权限委托	Numericland         ・         C           合作ら用品を行可能能主义が振動を全部団化上可能行的活作相関作(modella, 動物:回動物句), MR電子もの用下型, 有可能导致活動物集 生成的行け加強操作生成。 動物AMADMMASHE
回渡设置	开台回点来示操作失败时, 台台边回点至系统所保留的上一个低处的密度状态, 创编括可在密度附近常情页面传发,
删除保护	防止股票款最多外额份。他就结节在股票款转载责置你表。

步骤5 在配置确认页面中,单击"创建执行计划"。

**图 3-14** 配置确认

< 立即创建资源栈							
① 选择模板 ——— ② 百		配置确认					
1 22%##8585@85.	8、但资源栈内包含的资源可能需要付费。日前暂不支持4	E当前页查询价格,您可通过 创建执行计划 (免费	i) 后获取预估器用。				
<b>选择模板</b> 资源线名称	website-security		1865	Web网络	星融安全防护		
配置参数 🖉							
参数名称	(n	类型	描述 11:10万元(Dhobled)				
address		string	指定實驗的的Web服务器的IP地址或域名。				
web_port	80	number	Web服务器使用的跳口号,取值范围为0-65535,默认	为80			
资源栈设置							0
IAM权限跟托 (Provide	r) huaweicloud, (銀托)rf_admin_trust	開滾	未开启	删除保护	未开启		E
					上一步	创业执行计划	直接部署资源线

步骤6 在弹出的创建执行计划框中,自定义填写执行计划名称,单击"确定"。

×

**图 3-15** 创建执行计划

创建执行计划	
<ul> <li>在部署资源栈之 检查各项配置,</li> <li>该创建免费,值 执行计划详情势</li> </ul>	2前,您可以通过创建执行计划提前浏览您准备部署的资源栈信息、 以此评估对正在运行资源的影响。 <b>2会占用资源栈配额。</b> 创建后会生成一个未开通资源的资源栈,并在 最示预计费用。
★执行计划名称	executionPlan_20230209_0959_i81q
描述	请输入对执行计划的描述
	》 0/255 确定 取消

**步骤7** 待执行计划状态为"创建成功,待部署"后,单击"执行",并且在弹出的执行计划 确认框中单击"部署"。

**图 3-16**执行计划

< website-security				删除资源线 更新资源线	创建执行计划
基本信息 资源 事件 轴	出 模板 执行计划				
执行计划				请输入关键字	QC
执行计划名称/ID	状态	费用预估 ③	创建时间	描述	操作
executionPlan_20221028_0959_s8ew f2d4bd5d-a8eb-4a9b-b4ff-fe5bd35c3dbb	创建成功,待部署	臺署縣用明細	2022/10/28 10:02:19 GMT+08:00	-	删除 执行

**图 3-17**执行计划确认

执行计划			>
您确定要执行该计划吗?			
执行计划名称	状态	创建时间	
executionPlan_20221025_105	创建成功,	2022/10/25 10:54:34 GMT+08	
确定执行后,资源栈会按照该 费要求,可能会产生费用。	30年44,91, … 計划更新, 并且 <del>≤</del>	会开通模板内的资源,根据资源付	
	<b>执行</b> 取消	Se contractor de la con	

- **步骤8** (可选)如果计费模式选择"包年包月",在余额不充足的情况下(所需总费用请参考表2-1)请及时登录费用中心,手动完成待支付订单的费用支付。
- **步骤9** 等待解决方案自动部署。部署成功后,单击"事件",回显结果如下:

### **图 3-18** 资源创建成功

< website-security 基本信息 资源 事件	+ 輸出 模板 执行计划		制度金融	\$ 更新资源线 创建执行计划 C
			調査人	(D) [D]
资源名称/类型	关联资源ID	资源状态	状态描述	创建时间 1三
		LOG	Apply required resource success.	2022/10/28 10:29:13 GMT+08:00
-	-	-	Apply completel Resources: 1 added, 0 changed, 0 destroyed.	2022/10/28 10:29:11 GMT+08:00
domain huaweicloud_waf_domain	2274511993944#66830b3116500a5c11	生成完成	huaweicloud_waf_domain.domain.Creation complete after 8s [id=2274511993944666830b3116500a5c11]	2022/10/28 10:29:11 GMT+08:00
domain huaweicloud_waf_domain	-	正在生成	huaweicloud_waf_domain.domain.Creating	2022/10/28 10:29:02 GMT+08:00
	-	LOG	Creating required resource now	2022/10/28 10:29:00 GMT+08:00

----结束

# 3.3 开始使用

## 配置 WAF

**步骤1** 登录"Web应用防火墙WAF"控制台,进入"网站设置"页面,单击回源IP加白,按照操作步骤完成配置。

### **图 3-19** 网站设置

Web应用防火墙		M	站设置 ⑦ 🔍 海程引导	٢	评价 🔍 入门版 (原松	则版,在原检测版基	云模式 <b>踹上增加拦截能</b> 力)(30天后	到期) 变更 (续费	'〒创建WAF实例
资息全受			如何使网站流量接入Web应用防火墙? 如何在本圳	b测试/Veb应用防火槽?	删除防护城名时,应该注	意哪些事項?  仅证	3录模式如何切换到拦截模式?	Web应用防火槽的回源IP网段 更多常	见问题
防护事件									
防护策略			企业项目 default 👻	C					
网站设置									
对象管理	*		添加防护网站 Bypass 云模式: 独享模式	您在本项目中已添加2个 : 您已经添加了0个城名	·城名,其它项目已添加0个制 ,当前还可以添加0个城名	统名,还可以再添加 (当前版本仅支持04	8个城名(当前版本仅支持1个- 、一级城名)。	—级城名)。	CĽ
系统管理	*		默认按城名搜索						Q
DDoS防护	P	٩	□ 城名 (目	部署模式 7 近:	3天威胁	工作模式	防护兼路	域名接入进度"状态 7	操作
数据安全中心	P		-invicedialde.com	云模式 📀	未发现攻击	开启防护 🔻	已开启 2 项防护	下—步:回测P加白 C ●—●—●—●	删除

### 步骤2 域名接入进度变为已接入,说明配置成功。

Web应用防火墙		网站设置 ⑦ ※ 流程引导			(3) 评价	○入门板 (原检测板, 在原料	云様式 全則板基础上増加拦戦能力)(30天信到期) 変更   楽	(2) 使用指電
安全总规		如何使网站流量接入Web应用防火槽?   如何在本地测试W	96应用防火增?   删除防护域;	5时,应该注意感些事项?   仅记录镜。	Chol词taik是H兰教教堂?   Web应用	防火增的回避中风险 更多常见问	E	
防护事件								
防护策略		企业项目 default • C						
网站设置								
网站设置 对象管理	÷	潮加防护网站 Bypass 云镜式:您在本功 被事情式:您已能	夏目中已溃加1个城名,其它项目 3添加了0个城名,当前还可以滞	1日漆加0个城名,还可以再添加9个城名 500个城名(当前版本仅支持0个一级5	5(当前版本仅支持1个一级城名)。 \$名)。			c
网站设置 对象管理 系统管理	•	添加約計開始 Bypass 芸様式: 歩在本町 発電構式: 学行制 取入決除系统法	8日中已添加1个城名,其它项目 3添加了0个城名,当前还可以将	9已添加0个城名,还可以再添加9个城名 3000个城名(当前版本仅支持0个一级9	5(当航版本仅支持1个一级城名)。 6名)。			С
同就设置 対象管理 系统管理 DDoS防护	• • •		8日中已添加1个体名,其它项目 8项加了0个体名,当前还可以将 部器模式 🍞	已添加0个线名,还可以周添加9个线名 500个线名(当前版本仪支持0个一级5 近3天城物	5 (当前版本汉支持1个一级域名)。 \$8)。 <b>工作根式</b>	防护策路	城名接入进度"状态" 🏹	C 骤作

#### ----结束

## 访问测试

- 步骤1 清理浏览器缓存。
- 步骤2 在本地电脑的浏览器中输入防护域名,测试网站域名是否能正常访问。
- 步骤3 如果网站防护域名能够正常打开,说明通过Web网站基础安全防护访问Web源站的线路连通性正常。

----结束

# 3.4 快速卸载

### 一键卸载

步骤1 解决方案部署成功后,单击该方案堆栈后的"删除"。

图 3-21 ·	一键卸载					
资源编排	資源機 ⑦				Ø 使用指面	立即创建的现代
已況 例源地				服认检察的理论名称激素		QC
1 comes	突进线名称	¥ā 7	6002031A 1F	重整时间 1Ξ	操作	
	build-a-WAF-based-on-modsecurity e0d71621-80df-432e-b597-fatb49a455e3	部署成功	2022/10/25 11:02:07 GMT+08:00	2022/10/25 11:02:31 GMT+08:00	動除   更新	

### 步骤2 在弹出的删除堆栈确认框中,输入Delete,单击"确定",即可卸载解决方案。

### **图 3-22** 删除堆栈确认

资源栈名称	状态	创建时间
build-a-WAF-based-on-mods	部署成功	2022/10/25 11:02:07 GMT+08:00
1您确认要删除资源栈及资源,请输	入Delete	

----结束



## 名词解释

基本概念、云服务简介、专有名词解释:

- 弹性云服务器ECS:是一种可随时自助获取、可弹性伸缩的云服务器,可帮助您打造可靠、安全、灵活、高效的应用环境,确保服务持久稳定运行,提升运维效率。
- 弹性公网IP:提供独立的公网IP资源,包括公网IP地址与公网出口带宽服务。可以 与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活 地绑定及解绑。
- 域名注册(Domains):是用户付费获取Internet上某一域名一段时间使用权的过程。华为云域名注册服务与新网合作,提供域名的注册、购买、实名认证以及管理功能。通过华为云注册的域名其注册商为新网,由华为云提供域名管理服务。
- 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、跨站脚本攻击、网页木马上传、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、CC攻击、恶意爬虫扫描、跨站请 求伪造等攻击,保护Web服务安全稳定。



### **表 5-1** 修订记录

发布日期	修订记录
2022-03-30	第一次正式发布。
2023-02-28	修订实施步骤。