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 |

华为技术有限公司

## 商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 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

## 应用场景

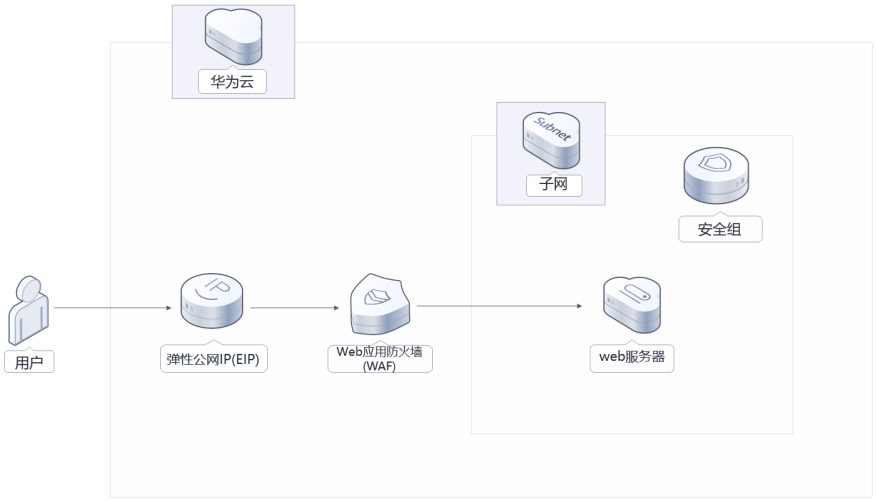
该解决方案基于华为云Web应用防火墙 WAF构建，可以帮助企业网站业务流量进行多维度检测和防护，全面避免网站被黑客恶意攻击和入侵。适用于如下场景：

- 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**。

# 2 资源和成本规划

该解决方案主要部署如下资源，各项花费如**表2-1**所示，具体收费标准请参考华为云官网**价格详情**，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 实施步骤



## 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**控制台管理**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


**步骤2** 进入“委托”菜单，搜索“rf_admin_trust”委托。

**图 3-3** 委托列表


- 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”。

**图 3-4** 创建委托


**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

**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

**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

**----结束**

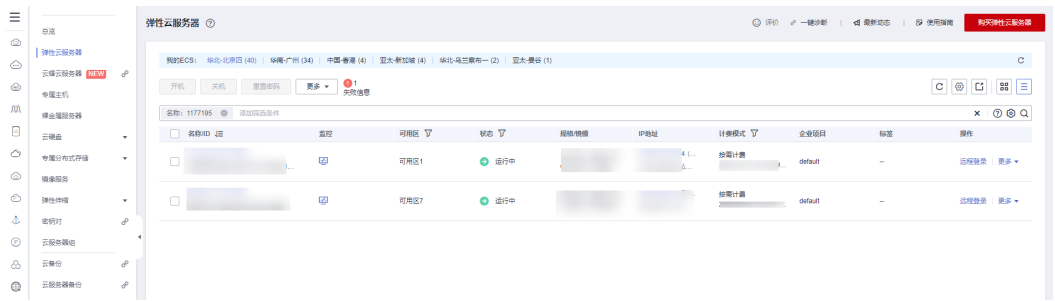
## 检查源站

**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

**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



**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。

**表 3-1** 参数填写说明

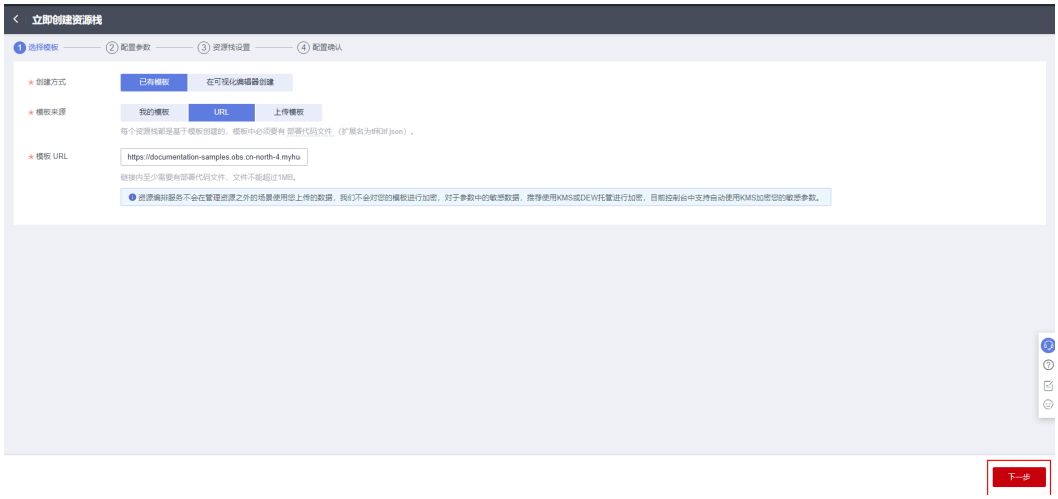
| 参数名称 | 类型 | 是否可选 | 参数解释 | 默认值 |
| --- | --- | --- | --- | --- |
| domain | string | 必填 | 指定要保护的域名。 | 空 |
| address | string | 必填 | 客户端访问的 Web 服务器的 IP 地址或域名。 | 空 |
| web_port | string | 必填 | Web 服务器使用的端口号。取值范围为 0 到 65535。 | 80 |

**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

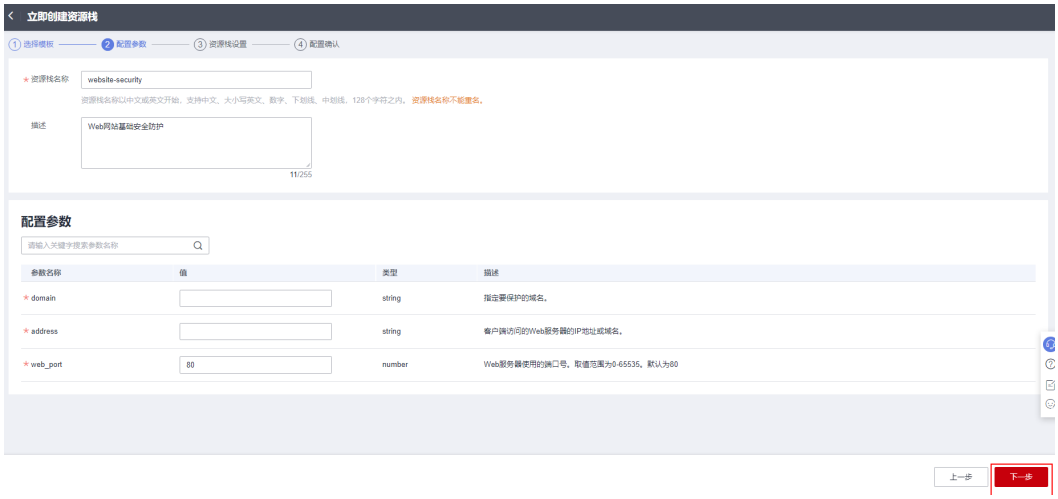

**步骤2** 在选择模板界面中，单击“下一步”。

**图 3-11** 选择模板



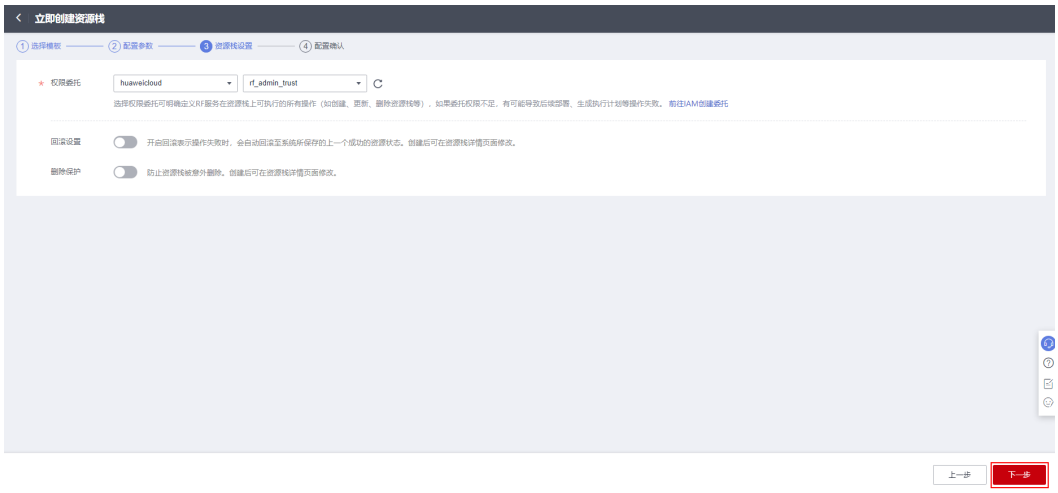

**步骤3** 在配置参数界面中，参考**表3-1**完成自定义参数填写，单击“下一步”。

**图 3-12** 配置参数



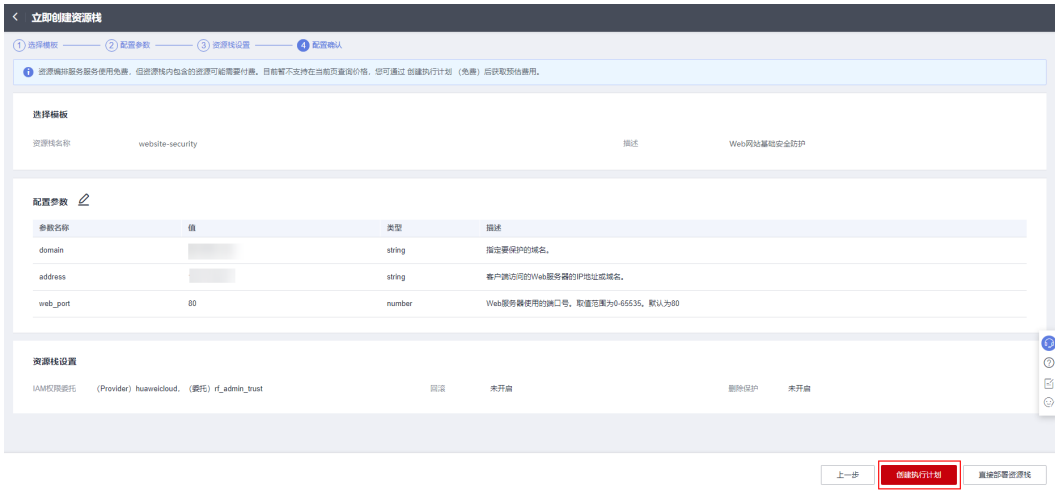

**步骤4** 在资源栈设置页面中，权限委托选择“rf_admin_trust”(可选），单击“下一步”。

**图 3-13** 资源栈设置




**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




**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


**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

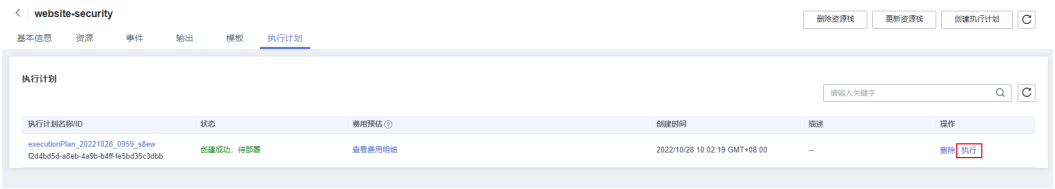


**图 3-17** 执行计划确认


**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


**----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


**步骤2** 域名接入进度变为已接入，说明配置成功。

**图 3-20** 配置成功


**----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


**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


**----结束**

# 4 附录

## 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。

# 5 修订记录

**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。 |