Web 应用防火墙

快速入门

文档版本 01

发布日期 2024-05-14

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 入门指引

Web应用防火墙（Web Application Firewall，WAF），通过对HTTP(S)请求进行检测，识别并阻断各种恶意流量，保障业务核心数据安全，避免您的服务器因恶意攻击导致性能异常等问题。本文介绍如何快速使用WAF为您的业务提供安全防护。

背景信息

您可以通过如下文档，快速了解WAF：

- **什么是Web应用防火墙?**
- **支持的服务版本及服务版本之间的差异**
- **功能特性**
- **如何计费**
- **支持哪些防护规则?**

步骤一：购买 WAF 实例

1. **登录华为云管理控制台**。在控制台页面中选择“安全与合规 > Web应用防火墙 WAF”。
2. 在页面右上角，单击“购买WAF实例”，进入购买页面，选择“WAF模式”，完成WAF实例的购买。

   我们为您提供了三种不同的WAF接入模式，云模式-CNAME接入、云模式-ELB接入和独享模式，三种接入模式之间的差别，请参见**服务版本差异**。

   - **购买WAF云模式**

     说明

     - 云模式的ELB接入方式需要**提交工单**申请开通后才能使用，支持使用的Region请参考**功能总览**。
     - 购买了云模式标准版、专业版或铂金版后，才支持使用ELB接入方式，域名、QPS、规则扩展包的配额与云模式的CNAME接入方式共用，且ELB接入方式的业务规格与购买的云模式版本的对应规格一致。
   - **购买WAF独享模式**

步骤二：网站接入 WAF

根据不同的模式完成网站接入WAF，网站接入WAF后，WAF才能对HTTP(S)请求进行检测。

接入方式	参考文档
云模式-CNAME接入	将网站接入WAF防护（云模式-CNAME接入）
云模式-ELB接入	将网站接入WAF防护（云模式-ELB接入）
独享模式	将网站接入WAF防护（独享模式）

步骤三：配置防护策略

网站接入WAF后，WAF会自动为该网站绑定一个防护策略，并开启“Web基础防护”中的“常规检测”（拦截模式为“仅记录”，“防护等级”为“中等”）和“网站反爬虫”的“扫描器”检测（防护动作为“仅记录”）。

- 如果您没有特殊的安全防护要求，您可以保持默认配置，随时通过“防护事件”查看WAF防护日志。具体操作，请参见**查看防护日志**。
- 如果您的网站遭遇Web攻击，您可以根据“总览”和“防护事件”的攻击详情，配置对应的防护策略。具体操作，请参见**为策略添加防护规则**。

步骤四：查看防护日志

在“防护事件”页面，查看已配置的防护策略的防护详情，处置源IP。

- 在防护事件列表的“操作”列，单击“误报处理”，通过**全局白名单规则**配置误报策略，快速加白源IP。
- 通过将源IP添加到黑白名单，快速拦截或放行源IP。

具体操作，请参见**处理误报事件**。

2 通过 CC 攻击防护规则实现 CC 防护

CC（Challenge Collapsar，以下简称CC）防护对单Web应用访问者IP或者Cookie键值进行访问频率限制，超过限制时通过人机识别或阻断访问，阻断页面可自定义内容和类型，满足业务多样化需要。

CC攻击防护规则根据IP或Cookie字段名设置灵活的限速策略，精准识别CC攻击以及有效缓解CC攻击。

本指南引导您通过Web应用防火墙服务快速配置CC攻击防护策略。

操作流程

操作步骤	说明
准备工作	注册华为账号、开通华为云，并为账户充值、赋予WAF权限。
步骤一：购买WAF	购买WAF，选择业务防护区域、WAF模式等信息。
步骤二：将防护网站添加到WAF	将防护网站添加到WAF防护，实现WAF流量检测并转发。
步骤三：开通CC攻击防护	配置并开启CC攻击防护规则，助力网站有效缓解CC攻击。

准备工作

1. 在购买Web应用防火墙之前，请先注册华为账号并开通华为云。具体操作详见**注册华为账号并开通华为云**、**实名认证**。

   如果您已开通华为云并进行实名认证，请忽略此步骤。
2. 请保证账户有足够的资金，以免购买Web应用防火墙失败。
3. 请确保已为账号赋予相关WAF权限。具体操作请参见**创建用户组并授权使用WAF**。

表 2-1 WAF 系统角色

系统角色/策略名称	描述	类别	依赖关系
WAF Administrator	Web应用防火墙服务的管理员权限。	系统角色	依赖Tenant Guest和Server Administrator角色。 • Tenant Guest：全局级角色，在全局项目中勾选。 • Server Administrator：项目级角色，在同项目中勾选。
WAF FullAccess	Web应用防火墙服务的所有权限。	系统策略	无。
WAF ReadOnlyAccess	Web应用防火墙的只读访问权限。	系统策略	

步骤一：购买 WAF

WAF提供了三种不同的WAF接入模式，云模式-CNAME接入、云模式-ELB接入和独享模式，三种接入模式之间的差别，请参见**服务版本差异**。

本节以购买WAF云模式，通过云模式-CNAME接入方式实现CC防护为例进行介绍。如需使用独享模式，请参考**购买WAF独享模式**。

1. **登录华为云管理控制台**。
2. 在控制台页面中选择“安全与合规 > Web应用防火墙 WAF”，进入Web应用防火墙控制台。
3. 在页面右上角，单击“购买WAF实例”，进入购买页面，选择“WAF模式”，完成WAF实例的购买。
   - “区域”：根据防护业务的所在区域就近选择购买的WAF区域。
   - “版本规格”：建议选择“标准版”及以上版本。
   - “扩展包”及“购买时长”：根据具体情况进行选择。
4. 确认参数配置无误后，在页面右下角单击“立即购买”。
5. 确认订单详情无误后，阅读并勾选《华为云Web应用防火墙免责声明》，单击“去支付”，完成购买操作。
6. 进入“付款”页面，选择付款方式进行付款。

步骤二：将防护网站添加到 WAF

添加防护网站前收集防护网站的配置信息：

表 2-2 准备防护域名相关信息

获取信息	参数	说明	示例
域名是否使用代理	是否已使用代理	• **七层代理**：使用了DDoS高防（七层代理）、CDN、云加速等Web代理产品。 • **四层代理**：使用了DDoS高防（四层转发）等Web代理产品。 • **无代理**：未使用任何代理产品。	无代理
配置参数	防护域名	由一串用点分隔的英文字母组成（以字符串的形式来表示服务器IP），用户通过域名来访问网站。	www.example.com
	防护域名端口	需要防护的域名对应的业务端口。 • 标准端口 – 80：HTTP对外协议默认使用端口 – 443：HTTPS对外协议默认使用端口 • 非标准端口 80/443以外的端口	80
	对外协议	客户端（例如浏览器）请求访问网站的协议类型。WAF支持“HTTP”、“HTTPS”两种协议类型。	HTTP
	源站协议	WAF转发客户端（例如浏览器）请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。	HTTP
	源站地址	客户端（例如浏览器）访问网站所在源站服务器的**公网IP地址**（一般对应该域名在DNS服务商处配置的A记录）或者域名（一般对应该域名在DNS服务商处配置的CNAME）。	XXX.XXX.1.1
（可选）证书	证书名称	对外协议选择“HTTPS”时，需要在WAF上配置证书，将证书绑定到防护域名。 **须知** WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考**如何将非PEM格式的证书转换为PEM格式?** 转化证书格式。	-

具体操作请参见**将网站接入WAF防护（云模式-CNAME接入）**。

步骤三：开通 CC 攻击防护

1. 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。
2. 单击目标策略名称，进入目标策略的防护配置页面。
3. 选择“CC攻击防护”配置框，开启CC攻击防护策略。

    ：开启状态。

    ：关闭状态。
4. 在“CC攻击防护”规则配置列表左上方，单击“添加规则”，在弹出的对话框中，配置CC防护规则。
   a. 根据具体的场景选择“限速模式”。
      i. 当WAF与访问者之间并无代理设备时，通过源IP来检测攻击行为较为精确，建议直接使用IP限速的方式进行访问频率限制。

         选择“源限速 > IP限速”，根据IP区分单个Web访问者。
      ii. 对于有些网站，源IP无法精准获取。例如：存在未在header中插入“X-Forwarded-For”字段的Proxy或其他原因，建议使用配置Cookie字段实现用户标识。

         选择“源限速 > 用户限速”：根据Cookie键值或者Header区分单个Web访问者。
   b. 配置“限速条件”：至少配置一项条件，多个条件同时满足时，本条规则才生效。
   c. 其他参数根据具体情况选择配置。
5. 确认参数配置无误后，单击“确认”。

相关信息

关于CC攻击防护更多详细的操作，请参见**配置CC攻击防护规则防御CC攻击**。

3 通过精准访问防护规则拦截字段为空的请求

精准访问防护规则可对常见的HTTP字段（如IP、路径、Referer、User Agent、Params等）进行条件组合，用来筛选访问请求，并对命中条件的请求设置仅记录、放行或阻断操作。同时支持“JS挑战”验证，即WAF向客户端返回一段正常浏览器可以自动执行的JavaScript代码。如果客户端正常执行了JavaScript代码，则WAF在一段时间（默认30分钟）内放行该客户端的所有请求（不需要重复验证），否则拦截请求。

本场景以拦截字段为空值的请求为例进行介绍。

操作流程

操作步骤	说明
准备工作	注册华为账号、开通华为云，并为账户充值、赋予WAF权限。
步骤一：购买WAF	购买WAF，选择业务防护区域、WAF模式等信息。
步骤二：将防护网站添加到WAF	将防护网站添加到WAF防护，实现WAF流量检测并转发。
步骤四：配置精准访问防护规则	通过精准访问防护规则的Referer字段实现拦截字段为空值的请求。

准备工作

1. 在购买Web应用防火墙之前，请先注册华为账号并开通华为云。具体操作详见**注册华为账号并开通华为云**、**实名认证**。

   如果您已开通华为云并进行实名认证，请忽略此步骤。
2. 请保证账户有足够的资金，以免购买Web应用防火墙失败。
3. 请确保已为账号赋予相关WAF权限。具体操作请参见**创建用户组并授权使用WAF**。

表 3-1 WAF 系统角色

系统角色/策略名称	描述	类别	依赖关系
WAF Administrator	Web应用防火墙服务的管理员权限。	系统角色	依赖Tenant Guest和Server Administrator角色。 • Tenant Guest：全局级角色，在全局项目中勾选。 • Server Administrator：项目级角色，在同项目中勾选。
WAF FullAccess	Web应用防火墙服务的所有权限。	系统策略	无。
WAF ReadOnlyAccess	Web应用防火墙的只读访问权限。	系统策略	

步骤一：购买 WAF

WAF提供了三种不同的WAF接入模式，云模式-CNAME接入、云模式-ELB接入和独享模式，三种接入模式之间的差别，请参见**服务版本差异**。

本节以购买WAF云模式，通过云模式-CNAME接入方式实现精准访问防护为例进行介绍。如需使用独享模式，请参考**购买WAF独享模式**。

1. **登录华为云管理控制台**。
2. 在控制台页面中选择“安全与合规 > Web应用防火墙 WAF”，进入Web应用防火墙控制台。
3. 在页面右上角，单击“购买WAF实例”，进入购买页面，选择“WAF模式”，完成WAF实例的购买。
   - “区域”：根据防护业务的所在区域就近选择购买的WAF区域。
   - “版本规格”：建议选择“标准版”及以上版本。
   - “扩展包”及“购买时长”：根据具体情况进行选择。
4. 确认参数配置无误后，在页面右下角单击“立即购买”。
5. 确认订单详情无误后，阅读并勾选《华为云Web应用防火墙免责声明》，单击“去支付”，完成购买操作。
6. 进入“付款”页面，选择付款方式进行付款。

步骤二：将防护网站添加到 WAF

添加防护网站前收集防护网站的配置信息：

表 3-2 准备防护域名相关信息

获取信息	参数	说明	示例
域名是否使用代理	是否已使用代理	• **七层代理**：使用了DDoS高防（七层代理）、CDN、云加速等Web代理产品。 • **四层代理**：使用了DDoS高防（四层转发）等Web代理产品。 • **无代理**：未使用任何代理产品。	无代理
配置参数	防护域名	由一串用点分隔的英文字母组成（以字符串的形式来表示服务器IP），用户通过域名来访问网站。	www.example.com
	防护域名端口	需要防护的域名对应的业务端口。 • 标准端口 – 80：HTTP对外协议默认使用端口 – 443：HTTPS对外协议默认使用端口 • 非标准端口 80/443以外的端口	80
	对外协议	客户端（例如浏览器）请求访问网站的协议类型。WAF支持“HTTP”、“HTTPS”两种协议类型。	HTTP
	源站协议	WAF转发客户端（例如浏览器）请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。	HTTP
	源站地址	客户端（例如浏览器）访问网站所在源站服务器的**公网IP地址**（一般对应该域名在DNS服务商处配置的A记录）或者域名（一般对应该域名在DNS服务商处配置的CNAME）。	XXX.XXX.1.1
（可选）证书	证书名称	对外协议选择“HTTPS”时，需要在WAF上配置证书，将证书绑定到防护域名。 **须知** WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考**如何将非PEM格式的证书转换为PEM格式?** 转化证书格式。	-

具体操作请参见**将网站接入WAF防护（云模式-CNAME接入）**。

步骤四：配置精准访问防护规则

步骤1 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤2 单击目标策略名称，进入目标策略的防护配置页面。

步骤3 选择“精准访问防护”配置框，开启精准访问防护策略。

-  ：开启状态。
-  ：关闭状态。

步骤4 在“精准访问防护”规则配置列表上方，单击“添加规则”，按照如图3-1所示进行配置。

图 3-1 拦截 referer 空值

步骤5 单击“确认”，完成配置。

----结束

相关信息

关于精准访问防护更多详细的操作，请参见**配置精准访问防护规则定制化防护策略**。

4 入门实践

当您将防护网站接入Web应用防火墙（WAF）后，可以根据自身业务场景使用WAF的一系列常用实践。

表 4-1 常用最佳实践

实践		描述
域名接入	单独使用WAF配置指导	网站没有接入WAF前，DNS直接解析到源站的IP。网站接入WAF后，需要把DNS解析到WAF的CNAME，这样流量才会先经过WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。 本文介绍通过DNS配置模式接入WAF时，如何在已添加网站配置后，配置域名解析，实现业务接入。
	使用CDN和WAF提升网站防护能力和访问速度	“CDN+WAF”组合可以对华为云、非华为云或云下的域名进行联动防护，同时提升网站的响应速度和网站防护能力
	使用独享WAF和7层ELB以防护任意非标端口	如果您需要防护WAF支持的端口以外的非标端口，可参考本章节配置WAF的独享模式和7层ELB联动，实现任意端口业务的防护。
策略防护	CC攻击防御最佳实践	基于Web应用防火墙实践编写，指导您在遭遇CC（Challenge Collapsar）攻击时，完成基于IP限速和基于Cookie字段识别的防护规则配置。
	使用WAF阻止爬虫攻击	Web应用防火墙可以通过Robot检测（识别User-Agent）、网站反爬虫（检查浏览器合法性）和CC攻击防护（限制访问频率）三种反爬虫策略，帮您解决业务网站遭受的爬虫问题。
	使用Postman工具模拟业务验证全局白名单规则	当防护网站成功接入WAF后，您可以使用接口测试工具模拟用户发起各类HTTP(S)请求，验证配置的WAF防护规则是否生效，检验防护效果。 本实践以Postman工具为例，说明如何验证全局白名单（原误报屏蔽）规则。

实践		描述
	使用WAF和HSS提升网页防篡改能力	主机安全HSS网页防篡改功能和Web应用防火墙“双剑合璧”，杜绝网页篡改事件发生。
Web漏洞防护	Java Spring框架远程代码执行高危漏洞	Spring是一款主流的Java EE轻量级开源框架，面向服务器端开发设计。Spring框架被曝出可导致RCE远程代码执行的漏洞，该漏洞攻击面较广，潜在危害严重，对JDK 9及以上版本皆有影响。
	Apache Dubbo反序列化漏洞	2020年02月10日，华为云安全团队监测到Apache Dubbo官方发布了CVE-2019-17564漏洞通告，漏洞等级中危。当用户选择http协议进行通信时，攻击者可以通过发送POST请求的时候来执行一个反序列化的操作，由于没有任何安全校验，该漏洞可以造成反序列化执行任意代码。目前，华为云Web应用防火墙（Web Application Firewall，WAF）提供了对该漏洞的防护。
	开源组件Fastjson拒绝服务漏洞	2019年09月03日，华为云安全团队检测到应用较广的开源组件Fastjson的多个版本出现拒绝服务漏洞。攻击者利用该漏洞，可构造恶意请求发给使用了Fastjson的服务器，使其内存和CPU耗尽，最终崩溃，造成用户业务瘫痪。目前，华为云Web应用防火墙（Web Application Firewall，WAF）提供了对该漏洞的防护。
	开源组件Fastjson远程代码执行漏洞	2019年07月12日，华为云应急响应中心检测到开源组件Fastjson存在远程代码执行漏洞，此漏洞为2017年Fastjson 1.2.24版本反序列化漏洞的延伸利用，可直接获取服务器权限，危害严重。
	Oracle WebLogic wls9-async反序列化远程命令执行漏洞（CNVD-C-2019-48814）	2019年04月17日，华为云应急响应中心检测到国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）发布的Oracle WebLogic wls9-async组件安全公告。Oracle WebLogic wls9-async组件在反序列化处理输入信息时存在缺陷，攻击者可以发送精心构造的恶意HTTP请求获取目标服务器权限，在未授权的情况下远程执行命令，CNVD对该漏洞的综合评级为“高危”。
LTS日志分析	通过LTS查询分析WAF访问日志	开启WAF全量日志功能后，您可以将攻击日志、访问日志记录到云日志服务（Log Tank Service，简称LTS）中。通过LTS记录的WAF日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。
	通过LTS分析Spring core RCE漏洞的拦截情况	对WAF攻击日志开启LTS快速分析功能，通过Spring规则ID快速查询、分析被拦截的Spring core RCE漏洞日志。

实践		描述
	通过LTS配置WAF规则的拦截告警	本实践对WAF攻击日志开启LTS快速分析功能，再配置告警规则，实现WAF规则拦截日志的分析及告警，实时洞察您的业务在WAF中的防护情况并作出决策分析。
TLS加密配置	**通过配置TLS最低版本和加密套件提升客户端访问域名的通道安全**	HTTPS协议是由“TLS（Transport Layer Security，传输层安全性协议）+HTTP协议”构建的可进行加密传输、身份认证的网络协议。 当**域名接入WAF**时，如果客户端采用HTTPS协议请求访问服务器（即防护域名的“对外协议”配置为“HTTPS”），您可以通过为域名配置最低TLS版本和加密套件来确保网站安全。
源站安全保护实践	**通过配置ECS/ELB访问控制策略保护源站安全**	介绍源站服务器部署在华为云弹性云服务器（以下简称ECS）、或华为云弹性负载均衡（以下简称ELB）时： ● 如何判断源站是否存在泄漏风险? ● 如何配置访问控制策略保护源站安全?
获取客户端真实IP	**获取客户端真实IP**	介绍通过WAF直接获取真实IP的方法，以及不同类型的Web应用服务器（包括Tomcat、Apache、Nginx、IIS 6和IIS 7）如何进行相关设置，以获取客户端的真实IP。
安全与治理	**基于开源Modsecurity构建WAF**	ModSecurity是一个开源的、跨平台的Web应用防火墙（WAF）。它可以通过检查Web服务接收到的数据，以及发送出去的数据来对网站进行安全防护。 该解决方案帮助您在华为云弹性云服务器上基于开源ModSecurity软件，一键部署实现Web应用防火墙（WAF）功能；配合Nginx的灵活与高效，有效的增强Web安全性。