Web 应用防火墙

产品介绍

文档版本 83

发布日期 2024-07-17

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 什么是 Web 应用防火墙

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。

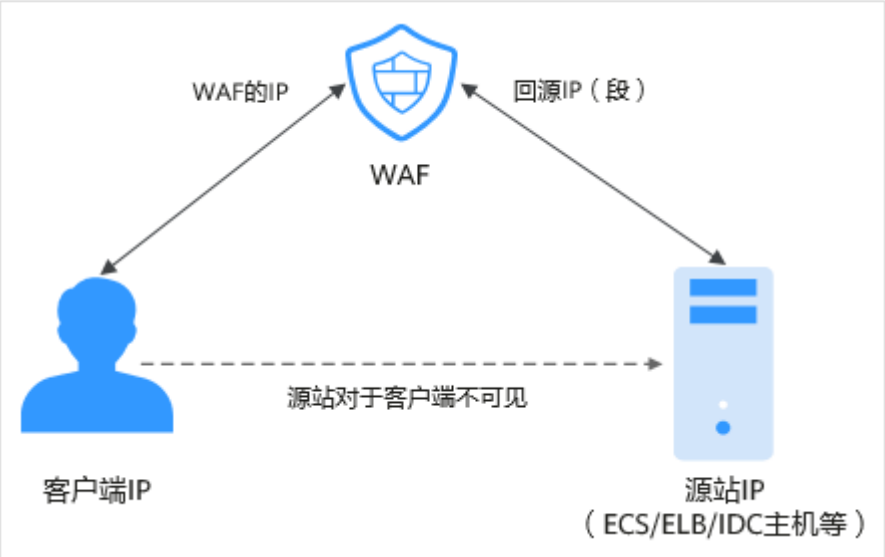
防护原理（云模式-CNAME 接入、独享模式接入）

通过WAF云模式-CNAME接入或者独享模式将网站添加并接入WAF后，网站所有访问请求将先流转到WAF，WAF检测过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。

图 1-1 防护原理

流量经WAF返回源站的过程称为回源。WAF通过回源IP代替客户端发送请求到源站服务器，接入WAF后，在客户端看来，所有的目标IP都是WAF的IP，从而隐藏源站IP。

图 1-2 回源 IP

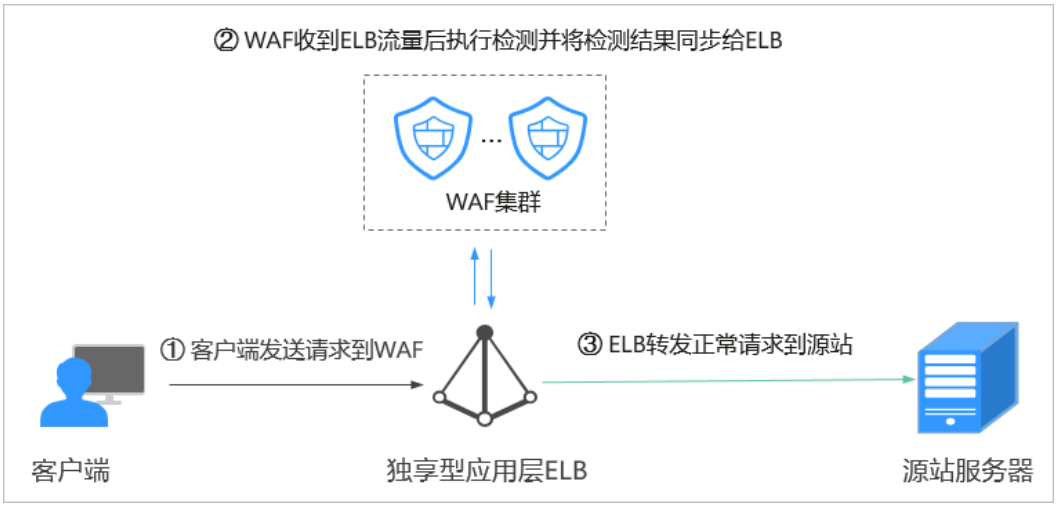


防护原理（云模式-ELB 接入）

通过云模式-ELB接入的方式将网站接入WAF防护，其原理如下：

- 通过SDK模块化的方式将WAF集成在ELB的网关中，WAF通过内嵌在网关中的SDK提取流量并进行检测和防护。
- WAF将检测结果同步给ELB，由ELB根据WAF的检测结果决定是否将客户端请求转发到源站。
- 该过程中，WAF不参与流量转发，避免因额外引入一层转发而带来各种兼容性和稳定性问题。

图 1-3 ELB 接入防护原理



防护对象

WAF支持云模式-CNAME接入、云模式-ELB接入和独享模式三种部署模式，各部署模式支持防护的对象说明如下：

- 云模式-CNAME接入：域名，华为云、非华为云或云下的Web业务
- 云模式-ELB接入：域名或IP，华为云的Web业务
- 独享模式：域名或IP，华为云的Web业务

2 内容安全检测

内容安全检测服务，基于丰富的违规样例库和内容审核专家经验，通过机器审核加人工审核结合的方式，帮助您准确检测出Web网站和新媒体平台上的关于涉黄、涉赌、涉毒、暴恐、涉政、惊悚、违禁广告等敏感违规内容，并提供文本内容纠错审校（错别字、生僻字、语法表述不当等有违准确性内容）。并提供专业检测报告助您自纠自查，降低内容违规风险。

特性说明

表 2-1 特性说明

特性	说明
检测位置	检测Web网站和新媒体平台发布的内容。
检测范围	内容的合法合规性、准确性。
检测技术	机器检测：基于丰富的违规样例库进行机器初审核。
	人工审核：内容审核专家基于多年经验对机器检测结果进行再审核。
交付形式	Word形式的检测报告。 ● “检测类型”选择“内容安全单次检测（按需）”时，下单后的7个工作日内出报告。 ● “检测类型”选择“文本安全监测（按月/按年）”时，下单后的检测周期（1个月）后的7个工作日内出报告。
计费模式	包年/包月（预付费）和按需计费（后付费）两种计费方式。 ● 文本安全监测（按年） ● 文本安全监测（按月） ● 内容安全单次检测（按需） 按“检测对象”的总个数进行收费。同一个对象再次进行扫描时，需要重新收费。例如：单次配置了10个检测对象（新媒体账号或网站网址），每个检测对象检测一次，则需要进行10次收费。

应用场景

网站/新媒体内容安全检测

- 内容合法合规性检测

  国家政策要求各地方机构要认真落实意识形态工作和网络内容安全工作责任制。为响应国家政策，华为云内容安全检测服务可对网站/新媒体内容进行合法合规检测，主要对文本、图片、视频、语音进行检测和识别是否包含色情、涉政、暴力、惊悚、不宜广告、垃圾信息、不良内容等，有效帮助您降低内容风险。

- 内容准确性检测

  对网站/主流新媒体平台的内容进行准确性检测，主要对文本、图片、视频、语音进行表述规范审核，如对错别字、生僻字、词法表述、语法表述等内容进行检测审核。

相关操作

- **购买并执行内容检测任务**
- **下载报告**
- **购买内容安全检测服务后，什么时候扣费?**

3 服务版本差异

Web应用防火墙支持云模式-CNAME接入、云模式-ELB接入和独享模式三种部署方式，部署模式的差异说明如**云模式和独享模式使用说明**。

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。

云模式和独享模式使用说明

请您根据业务需求选择使用云模式-CNAME接入、云模式-ELB接入或独享模式，三种模式的部署架构如**图3-1**所示，主要差异说明如**表3-1**所示。

图 3-1 部署架构

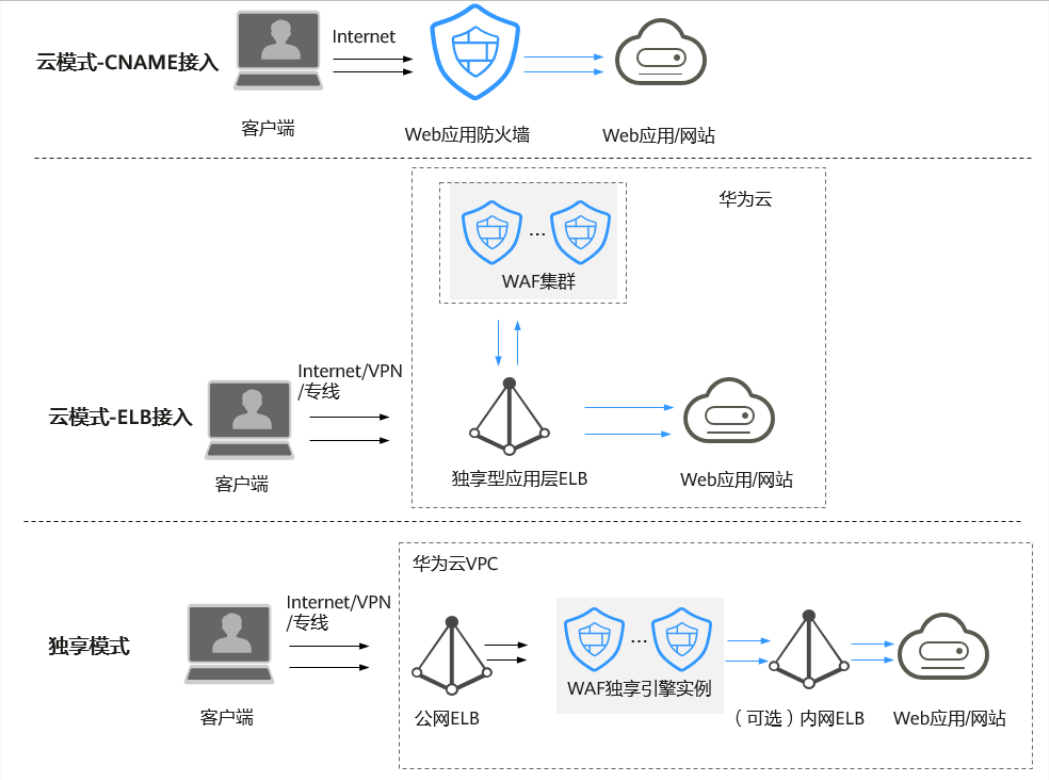


表 3-1 各模式使用说明

项目	云模式		独享模式
	CNAME接入	ELB接入	
计费方式	包周期（包年/包月）	购买了云模式标准版、专业版或铂金版后，支持使用ELB接入，域名、QPS、规则扩展包的配额与云模式的CNAME接入方式共用。	按需计费
服务版本	• 入门版 • 标准版 • 专业版 • 铂金版	-	-

项目	云模式		独享模式
	CNAME接入	ELB接入	
使用场景	业务服务器部署在华为云、非华为云或线下。 各服务版本推荐使用的场景说明如下： • 入门版 个人网站防护 • 标准版 中小型网站，对业务没有特殊的安全需求 • 专业版 中型企业级网站或服务对互联网公众开放，关注数据安全且具有高标准的安全需求 • 铂金版 中大型企业网站，具备较大的业务规模，或是具有制定个性化防护的安全需求	业务服务器部署在华为云。 大型企业网站，对业务稳定性有较高要求的安全防护需求。	业务服务器部署在华为云。 大型企业网站，具备较大的业务规模且基于业务特性具有制定个性化防护规则的安全需求。
防护对象	域名	• 域名 • IP地址	• 域名 • IP地址
优势	• 弹性扩容能力强，通过升级规格可以扩容防护能力 • 可以防护华为云、非华为云和云下的Web业务 • 支持IPv6防护	• 不改变业务架构，水平扩展防护能力 • 旁路部署，业务零影响 • 可靠性高 当WAF发生故障时，流量将直接通过ELB发送给后端，不影响客户正常业务。	• 部署灵活 • 独享引擎实例资源由用户独享 • 可以满足大规模流量攻击场景防护需求 • 独享引擎实例部署在VPC内，网络链路时延低

各版本支持的业务规格

WAF各个模式适用的业务规格如**表3-2**所示。其中，购买云模式时您可以选择购买域名扩展包、QPS扩展包和规则扩展包，以满足更多域名、更大流量的防护需求，也可以购买额外的扩展包或者通过**变更WAF云模式版本和规格**从较低版本升级到任一更高版本。

须知

购买了云模式标准版、专业版或铂金版，才支持使用ELB接入的方式，其业务规格与购买的云模式版本的对应规格一致。

扩展包限制和规格说明如下：

- 一个域名包支持10个域名，限制仅支持1个一级域名和与一级域名相关的子域名或泛域名。
- 一个QPS扩展包的QPS限制和带宽限制：
  - 对于部署在华为云的Web应用

    业务带宽：50Mbit/s

    每秒钟的请求量：1000QPS（Queries Per Second，例如一个HTTP GET请求就是一个Query）
  - 对于未部署在华为云的Web应用

    业务带宽：20Mbit/s

    每秒钟的请求量：1000QPS（Queries Per Second，例如一个HTTP GET请求就是一个Query）
- 一个规则扩展包包含10条IP黑白名单防护规则。

须知

- 域名个数为一级域名（例如，example.com）、单域名/二级域名等子域名（例如，www.example.com）和泛域名（例如，*.example.com）的总数。例如，标准版支持防护10个域名，可以添加1个一级域名和9个与其相关的子域名或泛域名。
- 同一个域名对应不同端口视为不同的域名，例如www.example.com:8080和www.example.com:8081视为两个不同的域名，将占用两个不同的域名防护额度。
- WAF支持上传的证书套数和WAF支持防护的域名的个数相同。例如，购买了标准版WAF（支持防护10个域名）、1个独享版WAF（支持防护2,000个域名）和域名扩展包（20个域名），WAF可以防护2,030个域名，则WAF支持上传2,030套证书。

表 3-2 适用的业务规格

业务规格	入门版	标准版	专业版	铂金版	独享模式
正常业务请求峰值	• 100 QPS业务请求 • 6,000 回源长连接（每域名）	• 2,000 QPS业务请求 • 6,000回源长连接（每域名）	• 5,000 QPS业务请求 • 6,000回源长连接（每域名）	• 10,000 QPS业务请求 • 6,000 回源长连接（每域名）	以下数据为单实例规格： • WAF实例规格选择WI-500，参考性能： – HTTP业务：建议QPS 5,000；极限QPS 10,000 – HTTPS业务：建议QPS 4,000；极限QPS 8,000 – Websocket业务：支持最大并发连接5,000 – 最大回源长连接：60,000 • WAF实例规格选择WI-100，参考性能： – HTTP业务：建议QPS 1,000；极限QPS 2,000 – HTTPS业务：建议QPS 800；极限QPS 1,600 – Websocket业务：支持最大

业务规格	入门版	标准版	专业版	铂金版	独享模式
					并发连接1,000 – 最大回源长连接：60,000 **须知** 极限值为实验室测试值，高敏感业务请以实际业务测试数据为准。实际QPS与业务请求数据大小、自定义防护规则种类及数量相关
业务带宽阈值（源站服务器部署在华为云）	10Mbit/s	100Mbit/s	200Mbit/s	300Mbit/s	● WAF实例规格选择WI-500，参考性能：吞吐量：500 Mbps ● WAF实例规格选择WI-100，参考性能：吞吐量：100 Mbps
业务带宽阈值（源站服务器未部署在华为云）	10Mbit/s	30Mbit/s	50Mbit/s	100Mbit/s	-
域名个数	10个（支持1个一级域名）	10个（支持1个一级域名）	50个（支持5个一级域名）	80个（支持8个一级域名）	2,000个（支持2,000个一级域名）
回源IP（单个防护域名支持的回源服务器IP个数）	10个	20个	50个	80个	-

业务规格	入门版	标准版	专业版	铂金版	独享模式
支持的端口个数 **说明** 云模式的专业版和铂金版支持定制非标准端口，您可以**提交工单**申请开通定制的非标准端口。	标准端口：2个（80，443）	• 标准端口：2个（80，443） • 非标准端口：可任意使用**WAF支持的端口列表**中的端口，不限制数量。	• 标准端口：2个（80，443） • 非标准端口：可任意使用**WAF支持的端口列表**中的端口，不限制数量。	• 标准端口：2个（80，443） • 非标准端口：可任意使用**WAF支持的端口列表**中的端口，不限制数量。	• 标准端口：2个（80，443） • 非标准端口：可任意使用**WAF支持的端口列表**中的端口，不限制数量。
CC攻击防护峰值	-	100,000QPS	200,000 QPS	1,000,000 QPS	• WAF实例规格选择WI-500，参考性能：防护峰值：20,000QPS • WAF实例规格选择WI-100，参考性能：防护峰值：4,000QPS
CC攻击防护规则	-	20条	50条	100条	100条
精准访问防护规则	-	20条	50条	100条	100条
引用表规则	-	-	50条	100条	100条
IP黑白名单规则	-	1000条	2000条	5000条	1000条
地理位置封禁规则	-	-	50条	100条	100条

业务规格	入门版	标准版	专业版	铂金版	独享模式
网页防篡改规则	-	20条	50条	100条	100条
网站反爬虫规则	-	-	50条	100条	100条
防敏感信息泄露	-	-	50条	100条	100条
全局白名单规则	1000条	1000条	1000条	1000条	1000条
隐私屏蔽规则	-	20条	50条	100条	100条
安全报告模板	5个	5个	10个	20个	20个

各版本支持的功能特性

云模式各个版本、独享模式适用的安全功能特性如**表3-3**所示，请您根据业务需求选择对应的服务版本。其中，云模式支持入门版、标准版、专业版和铂金版，您可以通过**变更WAF云模式版本和规格**从较低版本升级到任一更高版本，以满足更多防护功能需求。

须知

云模式的专业版和铂金版支持定制非标准端口，您可以**提交工单**申请开通定制的非标准端口。

标识说明：

- √：表示在当前版本中支持。
- ×：表示在当前版本中不支持。
- -：表示不涉及，通过ELB实现。ELB支持的功能特性详见**弹性负载均衡功能特性对比**。

表 3-3 安全功能特性

功能模板	云模式-CNAME接入				云模式-ELB接入	独享模式
	入门版	标准版	专业版	铂金版		
域名/QPS/规则扩展包	×	√	√	√	√（与CNAME接入共用配额）	×
域名备案检查	√	√	√	√	×	×

功能模板	云模式-CNAME接入				云模式-ELB接入	独享模式
	入门版	标准版	专业版	铂金版		
支持添加泛域名	×	√	√	√	√	√
非80、443标准端口防护	×	√	√	√	-	√
非80、443标准端口定制	×	×	√	√	-	×
批量灵活配置防护策略	√（仅支持批量配置全局白名单规则）	×	√	√	√	√
为防护策略批量配置适用的防护域名	×	×	√	√	√	√
支持IPv6防护 **须知** 支持IPv6防护的版本，请参考**哪些版本支持IPv6防护?**	×	×	√	√	-	×
常见的Web应用攻击防护，包括SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等	√	√	√	√	√	√
云端自动更新最新0Day漏洞防护规则，及时下发0Day漏洞虚拟补丁	√	√	√	√	√	√
Webshell检测	√	√	√	√	√	√
深度检测，同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等深度反逃逸检测	√	√	√	√	√	√

功能模板	云模式-CNAME接入				云模式-ELB接入	独享模式
	入门版	标准版	专业版	铂金版		
header全检测，对请求里header中所有字段进行攻击检测	√	√	√	√	√	√
CC攻击防护	×	√	√	√	√	√
精准访问防护	×	√（不支持全检测）	√	√	√	√
引用表管理	×	×	√	√	√	√
IP黑白名单设置，支持批量导入IP地址/IP地址段	×	√	√	√	√	√
支持对指定国家、省份的IP自定义访问控制	×	×	√	√	√	√
网页防篡改	×	√	√	√	×	√
检测并拦截搜索引擎、扫描器、脚本工具、其它爬虫等爬虫行为	×	×	√	√	√	√
检测并拦截JS脚本反爬虫检测行为	×	×	√	√	×	√
防敏感信息泄露	×	×	√	√	×	√
全局白名单规则	√	√	√	√	√	√
隐私屏蔽	×	√	√	√	√	√

功能模板	云模式-CNAME接入				云模式-ELB接入	独享模式
	入门版	标准版	专业版	铂金版		
资源建议	-	-	-	-	-	使用独享实例时，建议在云监控（CES）服务配置资源监控及告警：建议CPU使用率不超过70%，内存使用率不超过80%

功能模板	云模式-CNAME接入				云模式-ELB接入	独享模式
	入门版	标准版	专业版	铂金版		
						说明 当业务请求较大或自定义防护策略复杂时，会增加对CPU、内存的消耗；极端情况下，性能指标会有较大波动。建议根据业务模型压测后，做好性能规格的评估。

4 相关概念

本文为您介绍Web应用防火墙相关名词的主要含义。

CC 攻击

CC攻击是针对Web服务器或应用程序的攻击，利用获取信息的标准的GET/POST请求，如请求涉及数据库操作的URI（Universal Resource Identifier）或其他消耗系统资源的URI，造成服务器资源耗尽，无法响应正常请求。

跨站请求伪造

跨站请求伪造攻击是一种常见的WEB攻击手法。攻击者通过伪造非受害者意愿的请求数据，诱导受害者访问，如果受害者浏览器保持目标站点的认证会话，则受害者在访问攻击者构造的页面或URL的同时，携带自己的认证身份向目标站点发起了攻击者伪造的请求。

扫描器

扫描器是一类自动检测本地或远程主机安全弱点的程序，它能够快速的准确的发现扫描目标存在的漏洞并提供给使用者扫描结果。

网页防篡改

网页防篡改为用户的文件提供保护功能，避免指定目录中的网页、电子文档、图片、数据库等类型的文件被黑客、病毒等非法篡改和破坏。

跨站脚本攻击

一种网站应用程序的安全漏洞攻击，攻击者将恶意代码注入到网页上，用户在浏览网页时恶意代码会被执行，从而达到恶意盗取用户信息的目的。

SQL 注入

SQL注入攻击是一种常见的Web攻击方法，攻击者通过把SQL命令注入到Web后台数据库的查询字符串中，最终达到欺骗服务器执行恶意SQL命令的目的。例如可以从数据库获取敏感信息，或者利用数据库的特性执行添加用户、导出文件等一系列恶意操作，甚至有可能获取数据库乃至系统用户最高权限。

命令注入

利用各种调用系统命令的Web应用接口，通过命令拼接、绕过黑名单等方式在服务端形成对业务服务攻击的系统命令，从而实现对业务服务的攻击。

代码注入

利用Web应用在输入校验上的逻辑缺陷，或者部分脚本函数本身存在的代码执行漏洞，而实现的攻击手法。

敏感文件访问

一些涉及操作系统、应用服务框架的配置文件、权限管理文件等作为业务核心敏感的文件不应该被Internet上的请求所访问，否则会影响业务的安全。

服务端请求伪造

一种由攻击者构造形成由服务端发起请求的一个安全漏洞。一般情况下，SSRF攻击的目标是从外网无法访问的内部系统。SSRF形成的原因是服务端提供了从其他服务器应用获取数据的功能，在用户可控的情况下，未对目标地址进行过滤与限制，导致此漏洞的产生。

网站后门

Webshell是一种Web入侵的脚本攻击工具，攻击者在入侵了一个网站后，将asp、php、jsp或者cgi等脚本文件与正常的网页文件混在一起，然后使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。因此也有人称之为网站的后门工具。

盗链

盗链是指对方网站直接链接您网站上的文件，而不是将其置于自己的服务器上。一般而言，盗链的对象大多为耗带宽的大体积文件，如图片、视频等。从某种意义上说，造成了让您为其访问流量买单，不仅您的服务器带宽被无任何回报地占用，而且往往会在很大程度上影响您网站的访问速度。

多模匹配

利用高效的多模匹配算法，对请求流量进行特征检测，极大提升了检测引擎的性能。

精准访问防护

支持对HTTP请求的多个常用字段（URL、IP、Params、Cookie、Referer、User-Agent、Header）的自定义检测策略，并且支持多逻辑检测策略。

黑白名单

IP黑白名单包括IP白名单和IP黑名单配置，其中IP白名单即指定IP为可信IP，源IP为可信IP的流量不进行攻击检测。IP黑名单即指定IP为恶意IP，源IP为恶意IP的流量需要根据检测策略执行相应的动作。

智能解码

智能识别请求中的多种编码无限次多层混淆，对其进行深度解码，从而获取攻击者原始的攻击意图。

基于语义分析检测

基于语义上下文构建语法树，分析并判断是否为攻击载荷。

访问频率控制

通过访问控制策略，限制接口的访问的频率。

反爬虫

丰富的爬虫特征库，检测各种类别的爬虫（引擎爬虫，脚本爬虫，扫描工具）。

A 记录

A（Address）记录是地址记录，用来指定主机名（或域名）对应的IP地址记录，通过A记录，可以设置不同域名指向不同的IP。

SQL 注入攻击

通过输入域或页面请求的查询字符串，欺骗服务器执行恶意的SQL命令。

非标准端口

除“80”、“443”以外的端口。

5 功能特性

通过Web应用防火墙，轻松应对各种Web安全风险，Web应用防火墙支持功能如下表。

功能类别		功能说明
业务配置	域名（泛域名、一级域名、二级域名等各级域名）/IP防护 **说明** WAF云模式支持域名备案检查，添加防护域名时，WAF会检查域名备案情况，未备案域名将无法添加到WAF。	WAF支持云模式-CNAME接入、云模式-ELB接入和独享模式三种部署模式，各部署模式支持防护的对象说明如下： • 云模式-CNAME接入：域名，华为云、非华为云或云下的Web业务 • 云模式-ELB接入：域名或IP，华为云的Web业务 • 独享模式：域名或IP，华为云的Web业务
	HTTP/HTTPS业务防护	支持对网站的HTTP、HTTPS流量进行安全防护。
	支持WebSocket/WebSockets协议	WAF支持WebSocket/WebSockets协议，且默认为开启状态。
	非标端口防护 **说明** 云模式的专业版和铂金版支持定制非标准端口，您可以**提交工单**申请开通定制的非标准端口。	Web应用防火墙除了可以防护标准的80，443端口外，还支持非标准端口的防护。

功能类别		功能说明
Web应用安全防护	Web基础防护 **说明** 防护动作为“拦截”时，可使用攻击惩罚标准功能，即当恶意请求被拦截时，可自动封禁访问者一段时间。	覆盖OWASP（Open Web Application Security Project，简称OWASP）TOP 10中常见安全威胁，通过预置丰富的信誉库，对漏洞攻击、网页木马等威胁进行检测和拦截。 ● 常规检测 防护SQL注入、XSS跨站脚本、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击。 ● Webshell检测 防护通过上传接口植入网页木马。 ● 识别精准 – 内置语义分析+正则双引擎，黑白名单配置，误报率更低。 – 支持防逃逸，自动还原常见编码，识别变形攻击能力更强。 默认支持的编码还原类型：url_encode、Unicode、xml、OCT（八进制）、HEX（十六进制）、html转义、base64、大小写混淆、javascript/shell/php等拼接混淆。 ● 深度检测 深度反逃逸识别（支持同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等的防护）。 ● header全检测 支持对请求里header中所有字段进行攻击检测。 ● Shiro解密检测 支持对Cookie中的rememberMe内容做AES，Base64解密后再检测。
	CC攻击防护规则	限制单个IP/Cookie/Referer访问者对您的网站上特定路径（URL）的访问频率，WAF会根据您配置的规则，精准识别CC攻击以及有效缓解CC攻击。
	精准访问防护规则 **说明** 防护动作为“阻断”时，可使用攻击惩罚标准功能，即当恶意请求被拦截时，可自动封禁访问者一段时间。	对常见的HTTP字段（如IP、路径、Referer、User Agent、Params等）进行条件组合，配置强大的精准访问控制策略；支持盗链防护、空字段拦截等防护场景。

功能类别		功能说明
	黑白名单规则 **说明** 防护动作为“拦截”时，可使用攻击惩罚标准功能，即当恶意请求被拦截时，可自动封禁访问者一段时间。	配置黑白名单规则，阻断、仅记录或放行指定IP的访问请求，即设置IP黑/白名单。
	地理位置访问控制规则	针对指定国家、地区的来源IP自定义访问控制。
	网页防篡改规则	当用户需要防护静态页面被篡改时，可配置网页防篡改规则。
	网站反爬虫规则	动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别700+种爬虫行为。 ● 特征反爬虫 自定义扫描器与爬虫规则，用于阻断网页爬取行为，添加定制的恶意爬虫、扫描器特征，使爬虫防护更精准。 ● JS脚本反爬虫 通过自定义规则识别并阻断JS脚本爬虫行为。
	防敏感信息泄露规则	该规则可添加两种类型的防敏感信息泄露规则： ● 敏感信息过滤。配置后可对返回页面中包含的敏感信息做屏蔽处理，防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露。 ● 响应码拦截。配置后可拦截指定的HTTP响应码页面。
	全局白名单规则	针对特定请求忽略某些攻击检测规则，用于处理误报事件。
	隐私屏蔽规则	隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。
高级配置	PCI DSS/PCI 3DS合规认证和TLS	● TLS支持TLS v1.0、TLS v1.1、TLS v1.2三个版本和七种加密套件，可以满足各种行业客户的安全需求。 ● WAF支持PCI DSS和PCI 3DS合规认证功能。

功能类别		功能说明
	IPv6防护	● Web应用防火墙支持IPv6/IPv4双栈，针对同一域名可以同时提供IPv6和IPv4的流量防护。 ● 针对仍然使用IPv4协议栈的Web业务，Web应用防火墙支持NAT64机制（NAT64是一种通过网络地址转换（NAT）形式促成IPv6与IPv4主机间通信的IPv6转换机制），即WAF可以将IPv4源站转化成IPv6网站，将外部IPv6访问流量转化成对内的IPv4流量。
	熔断保护	当502/504请求数量或读等待URL请求数量以及占比阈值达到您设置的值时，将触发WAF熔断功能开关，实现宕机保护和读等待URL请求保护。
	配置攻击惩罚的流量标识	WAF根据配置的流量标识识别客户端IP、Session或User标记，以分别实现IP、Cookie或Params恶意请求的攻击惩罚功能。
	手动设置网站连接超时时间	● 浏览器到WAF引擎的连接超时时长默认是120秒，该值取决于浏览器的配置，该值在WAF界面不可以手动设置。 ● WAF到客户源站的连接超时时长默认为30秒，该值可以在WAF界面手动设置，但仅“独享模式”和“云模式”的专业版、铂金版支持手动设置连接超时时长。
高阶功能	内容安全检测服务	基于丰富的违规样例库和内容审核专家经验，通过机器审核加人工审核结合的方式，帮助您准确检测出Web网站和新媒体平台上的关于涉黄、涉赌、涉毒、暴恐、违禁等敏感违规内容，并提供文本内容纠错审校，助您降低内容违规风险
防护事件管理		● 当Web应用防火墙拦截或者仅记录的攻击事件为误报时，用户可通过Web应用防火墙处理误报事件、查看事件详情。 ● 用户可以通过Web应用防火墙服务下载5天内的全量防护事件数据。 ● WAF支持全量日志功能，您可以将攻击日志、访问日志记录到华为云的云日志服务（Log Tank Service，简称LTS）。

功能类别	功能说明
告警通知	通过对攻击日志进行通知设置，WAF可将仅记录和拦截的攻击日志通过用户设置的接收通知方式（例如邮件或短信）发送给用户。 同时，您也可以配置证书到期通知，证书即将到期时，WAF将通过用户设置的接收通知方式（例如邮件或短信）通知用户。
安全可视化	提供简洁友好的控制界面，实时查看攻击信息和事件日志。 ● 策略事件集中配置 在Web应用防火墙服务的控制台集中配置适用于多个防护域名的策略，快速下发，快速生效。 ● 流量及事件统计信息 实时查看访问次数、安全事件的数量与类型、详细的日志信息。
灵活性、可靠性	多区域多集群部署，支持负载均衡，可在线平滑扩容，没有单点故障，最大限度保护业务运行稳定。

6 产品优势

Web应用防火墙对网站业务流量进行多维度检测和防护，降低数据被篡改、失窃的风险。

精准高效的威胁检测

- 采用规则和AI双引擎架构，默认集成最新的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，使网站防护更精准。

0day 漏洞快速修复

专业安全团队7*24小时运营，实现紧急0day漏洞2小时内修复完成，帮助用户快速抵御最新威胁。

保护用户数据隐私

- 支持用户对攻击日志中的账号、密码等敏感信息进行脱敏。
- 支持PCI-DSS标准的SSL安全配置。
- 支持TLS协议版本和加密套件的配置。

助力企业安全合规

帮助企业满足等保测评、PCI-DSS等安全标准的技术要求。

7 应用场景

常规防护

帮助用户防护常见的Web安全问题，比如命令注入、敏感文件访问等高危攻击。

电商抢购秒杀防护

当业务举办定时抢购秒杀活动时，业务接口可能在短时间承担大量的恶意请求。Web应用防火墙可以灵活设置CC攻击防护的限速策略，能够保证业务服务不会因大量的并发访问而崩溃，同时尽可能地给正常用户提供业务服务。

0Day 漏洞爆发防范

当第三方Web框架、插件爆出高危漏洞，业务无法快速升级修复，Web应用防火墙确认后会第一时间升级预置防护规则，保障业务安全稳定。WAF相当于第三方网络架构加了一层保护膜，和直接修复第三方架构的漏洞相比，WAF创建的规则能更快的遏制住风险。

防数据泄露

恶意访问者通过SQL注入，网页木马等攻击手段，入侵网站数据库，窃取业务数据或其他敏感信息。用户可通过Web应用防火墙配置防数据泄露规则，以实现：

- 精准识别

  采用语义分析+正则表达式双引擎，对流量进行多维度精确检测，精准识别攻击流量。
- 变形攻击检测

  支持7种编码还原，可识别更多变形攻击，降低Web应用防火墙被绕过的风险。

防网页篡改

攻击者利用黑客技术，在网站服务器上留下后门或篡改网页内容，造成经济损失或带来负面影响。用户可通过Web应用防火墙配置网页防篡改规则，以实现：

- 挂马检测

  检测恶意攻击者在网站服务器注入的恶意代码，保护网站访问者安全。
- 页面不被篡改

保护页面内容安全，避免攻击者恶意篡改页面，修改页面信息或在网页上发布不良信息，影响网站品牌形象。

内容安全检测

网站/新媒体内容安全检测

- 内容合法合规性检测

  国家政策要求各地方机构要认真落实意识形态工作和网络内容安全工作责任制。为响应国家政策，华为云内容安全检测服务可对网站/新媒体内容进行合法合规检测，主要对文本、图片、视频、语音进行检测和识别是否包含色情、涉政、暴力、惊悚、不宜广告、垃圾信息、不良内容等，有效帮助您降低内容风险。

- 内容准确性检测

  对网站/主流新媒体平台的内容进行准确性检测，主要对文本、图片、视频、语音进行表述规范审核，如对错别字、生僻字、词法表述、语法表述等内容进行检测审核。

8 项目和企业项目

项目

IAM中的项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。用户拥有的资源必须挂载在项目下，项目可以是一个部门或者项目组。一个账户中可以创建多个项目。

企业项目

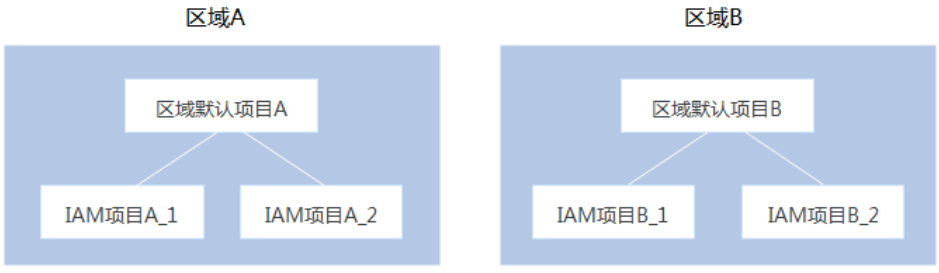
企业管理中的企业项目是对多个资源进行分组和管理，在目标区域中同一类型的资源可以划分到一个企业项目中，且主机安全服务的使用不受企业项目的划分影响。

企业可以根据不同的部门或项目组，将相关的资源放置在相同的企业项目内进行管理，并支持资源在企业项目之间迁移。

项目与企业项目的区别

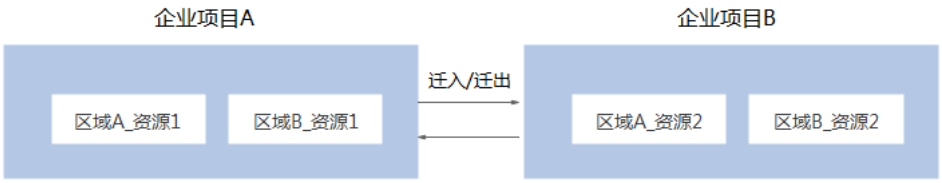
- IAM项目

  IAM项目是针对同一个区域内的资源进行分组和隔离，是物理隔离。在IAM项目中的资源不能转移，只能删除后重建。



- 企业项目

  企业项目是IAM项目的升级版，是针对企业不同项目间资源的分组和管理。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。如果您开通了企业管理，将不能创建新的IAM项目（只能管理已有项目）。未来IAM项目将逐渐被企业项目所替代，推荐使用更为灵活的企业项目。



项目和企业项目都可以授权给一个或者多个用户组进行管理，管理企业项目的用户归属于用户组。通过给用户组授予策略，用户组中的用户就能在所属项目/企业项目中获得策略中定义的权限。

有关创建项目、企业项目，以及授权的详细操作，请参见**管理项目和企业项目**。

9 个人数据保护机制

为了确保网站访问者的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，WAF通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

对于触发攻击告警的请求，WAF在事件日志中会记录相关请求记录，收集及产生的个人数据如表9-1所示。

表 9-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
请求源IP	攻击防护域名时，被WAF拦截或者记录的攻击者IP。	否	是
URL	攻击的防护域名的URL，被WAF拦截或者记录的防护域名的URL。	否	是
HTTP/HTTPS Header信息（包括Cookie）	用户在配置CC攻击、精准访问防护规则时，在配置界面输入的Cookie值和Header值。	否	否 如果配置的Cookie和Header信息不含有用户的个人信息，则WAF记录的相关请求中不会收集及产生用户的个人数据。
请求参数（Get、Post）	防护日志里，WAF记录的请求详情。	否	否 如果请求参数里不含有用户的个人信息，则WAF记录的相关请求中不会收集及产生用户的个人数据。

存储方式

对敏感字段提供了脱敏配置，其他字段在日志中明文保存。

访问权限控制

用户只能查看自己业务的相关日志。

10 安全

10.1 责任共担

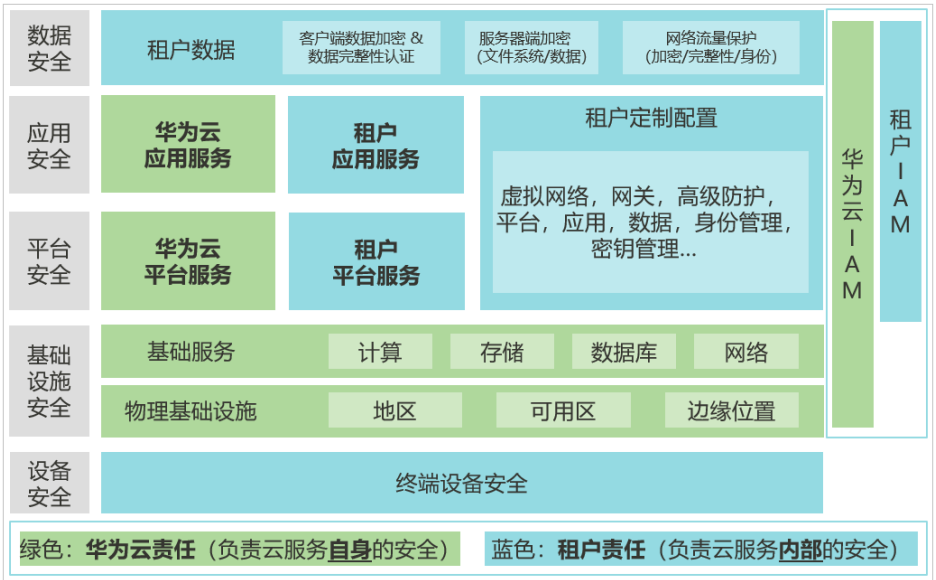
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图10-1**所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 10-1 华为云安全责任共担模型



10.2 身份认证与访问控制

WAF对接了统一身份认证服务（Identity and Access Management，IAM）服务。WAF租户身份认证与访问控制通过IAM权限控制。

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助WAF服务安全地控制访问权限。通过IAM，可以将用户加入到一个用户组中，并用策略来控制他们对WAF资源的访问范围。IAM权限可以通过细粒度定义允许和拒绝的访问操作，以此实现WAF资源的权限访问控制。关于对WAF资源的访问权限，详细请参考**WAF权限管理**。

10.3 数据保护技术

WAF通过多种数据保护手段和特性，保证通过WAF的数据安全可靠。

表 10-1 WAF 的数据保护手段和特性

数据保护手段	简要说明
静态数据保护	WAF通过敏感数据加密保证用户流量中敏感数据的安全性。
传输中的数据保护	微服务间数据传输进行加密，防止数据在传输过程中泄露或被篡改。 用户的配置数据传输采用安全协议HTTPS，防止数据被窃取。
数据完整性校验	WAF进程启动时，配置数据从配置中心获取而非直接读取本地文件。
数据隔离机制	租户区与管理面隔离，租户的所有操作权限隔离，不同租户间的策略、日志等数据隔离。

数据保护手段	简要说明
数据销毁机制	考虑到残留数据导致的信息泄露问题，华为云根据客户等级设定了不同的保留期时长，保留期到期仍未续订或充值，存储在云服务中的数据将被删除，云服务资源将被释放。WAF对云服务自动感知并在保留期到期后释放资源。

同时，WAF服务充分尊重用户隐私，遵循法律法规。以入侵防护功能为例，WAF仅会对流量进行**威胁签名匹配检测**和**异常行为检测**，不会采集和存储任何用户隐私数据。更多隐私数据使用和保护问题，请参考**隐私政策声明**。

10.4 审计与日志

- 审计

  云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

  用户开通云审计服务并创建和配置追踪器后，CTS可记录WAF的管理事件和数据事件用于审计。

  CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

  CTS支持追踪的WAF操作列表，请参见**标签管理服务支持的WAF操作列表**。

- 日志

  出于分析或审计等目的，用户开启了云审计服务后，系统开始记录WAF资源的操作。云审计服务管理控制台保存最近7天的操作记录。

  关于WAF云审计日志的查看，请参见**查看审计日志**。

10.5 服务韧性

华为云WAF按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减小由硬件故障、自然灾害或其他灾难带来的服务中断，华为云WAF提供灾难恢复计划。

当发生故障时，WAF的五级可靠性架构支持不同层级的可靠性，因此具有更高的可用性、容错性和可扩展性。

华为云WAF已面向全球用户服务，并在多个分区部署，同时WAF的所有管理面、引擎等组件均采用主备或集群方式部署。分区部署详情参见**可用分区**。

10.6 监控安全风险

WAF已对接云监控服务（Cloud Eye，CES），可以通过管理控制台，查看WAF的相关指标，及时了解WAF防护状况，并通过指标设置防护策略。CES服务是华为云为用户提供一个针对各种云上资源的立体化监控平台，用户通过云监控服务可以全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

用户通过设置WAF告警规则，可自定义监控目标与通知策略，告警规则包含名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助用户及时了解WAF防护状况，从而起到预警作用。

如何使用CES对WAF进行监控，请参见：

- **WAF监控指标说明**
- **设置监控告警规则**
- **查看监控指标**

10.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 10-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 10-3 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 10-4 销售许可证&软件著作权证书

11 WAF 权限管理

如果您需要对华为云购买的WAF资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为账号中给员工创建IAM用户，并授权控制员工对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这些员工拥有WAF的使用权限，但是不希望这些员工拥有删除WAF等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用WAF，但是不允许删除WAF的权限，控制员工对WAF资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用WAF的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

WAF 权限

默认情况下，创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

WAF部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问WAF时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对WAF服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，WAF支持的API授权项请参见**WAF权限及授权项**。

如表11-1所示，包括了WAF的所有系统角色。

表 11-1 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	

相关链接

- IAM产品介绍
- 创建用户组、用户并授予WAF权限
- WAF自定义策略
- WAF权限及授权项

WAF FullAccess 策略内容

```
{    "Version": "1.1",
     "Statement": [
         {
            "Action": [
              "waf:*:*",
              "lts:groups:get",
              "lts:groups:list",
              "lts:topics:get",
              "lts:topics:list",
              "smn:*:list*",
              "vpc:*:get*",
              "vpc:*:list*",
              "ecs:*:get*",
              "ecs:*:list*",
              "elb:*:get*",
              "elb:*:list*"
            ],
              "Effect": "Allow"
        }
             ]
}
```

WAF ReadOnlyAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "waf:*:get*",
            "waf:*:list*",
            "lts:groups:get",
            "lts:groups:list",
            "lts:topics:get",
            "lts:topics:list",
            "smn:*:list*",
            "vpc:*:get*",
            "vpc:*:list*",
            "ecs:*:get*",
            "ecs:*:list*",
            "elb:*:get*",
            "elb:*:list*"
       ],
            "Effect": "Allow"
      }
   ]
}
```

12 约束与限制

本节介绍Web应用防火墙WAF服务在使用过程中的约束和限制。

防护对象限制

表 12-1 防护对象限制

接入方式	防护对象
云模式-CNAME接入	• 仅支持防护域名 • 支持防护华为云、非华为云或云下的Web业务
云模式-ELB接入	• 支持防护域名 • 支持防护IP • 仅支持防护华为云的Web业务
独享模式	• 支持防护域名 • 支持防护IP • 仅支持防护华为云的Web业务

服务版本限制

- 同一账号在同一个大区域只能选择一个服务版本。

  以“华东区域”为例，同一账号在华东-上海一、华东-上海二只能选购一个WAF版本。

  说明

  原则上，在任何一个区域购买的WAF支持防护所有区域的Web业务。但是为了提高WAF的转发效率，建议您在购买WAF时，根据防护业务的所在区域就近选择购买的WAF区域。

- 服务版本选择：
  - 购买了云模式标准版、专业版或铂金版后，才支持使用“云模式-ELB接入”方式。

- 使用独享模式WAF时，建议WAF独享引擎实例与源站在同一个VPC中，如果WAF独享引擎实例与源站不在同一个VPC中，可通过**对等连接**打通两个VPC之间网络。

防护域名限制

- 通过云模式-CNAME接入方式接入的域名，请确保域名已经过ICP备案，WAF会检查域名备案情况，未备案域名将无法添加。
- 同一防护对象不能重复添加到WAF。

  同一个域名对应不同非标准端口视为不同的防护对象，例如www.example.com:8080和www.example.com:8081为两个不同的防护对象，且占用两个域名防护配额。如果您需要防护同一域名的多个端口，您需要将该域名和端口逐一添加到WAF。

证书限制

- WAF当前仅支持PEM格式证书。
- 目前华为云SCM证书只能推送到“default”企业项目下。如果您使用其他企业项目，则不能选择使用SCM推送的SSL证书。
- 拥有“SCM Administrator”和“SCM FullAccess”权限的账号才能选择SCM证书。

ELB 限制

- 将网站以独享模式接入WAF时，仅支持与独享型ELB配置使用。有关ELB类型的详细介绍，请参见**共享型弹性负载均衡与独享型负载均衡的功能区别**。

  说明

  2023年4月之前的独享引擎版本，不支持与独享ELB网络型配合使用。因此，如果您使用了独享ELB网络型（TCP/UDP）负载均衡，请确认独享WAF实例已升级到最新版本（2023年4月及之后的版本）。
- 将网站以云模式-ELB接入WAF时，仅支持与独享型ELB配套使用，且ELB“规格”必须为“应用型（HTTP/HTTPS）”，不支持“网络型（TCP/UDP）”的独享型的ELB。

规格限制

- WAF各版本支持的业务规格限制，详见**各版本支持的业务规格**。
- 将网站接入WAF后，网站的文件上传请求限制为10GB。

13 与其他云服务的关系

本章节介绍Web应用防火墙与其他云服务的关系。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录了Web应用防火墙相关的操作事件，方便用户日后的查询、审计和回溯。

与云监控服务的关系

云监控服务可以监控Web应用防火墙的相关指标，用户可以通过指标及时了解Web应用防火墙防护状况，并通过这些指标设置防护策略。具体请参见《云监控服务用户指南》。

有关WAF监控指标的详细介绍，请参见**WAF监控指标说明**。

与弹性负载均衡的关系

Web应用防火墙通过绑定**弹性负载均衡**（Elastic Load Balance，以下简称ELB），使流量通过ELB后先发送给WAF检测，再发送给应用端，以提升防护性能和确保业务稳定运行。

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为Web应用防火墙服务提供了权限管理的功能。需要拥有WAF Administrator权限的用户才能使用WAF服务。如需开通该权限，请联系拥有Security Administrator权限的用户。

与云日志服务的关系

云日志服务（Log Tank Service，简称LTS）用于收集来自主机和云服务的日志数据。Web应用防火墙可以设置将攻击日志、访问日志记录到LTS中，为您提供一个实时、高效、安全的日志处理功能。

与消息通知服务的关系

消息通知服务（Simple Message Notification，简称SMN）提供消息通知功能。Web应用防火墙开启通知设置后，如果防护的域名受到事件攻击时，告警信息会通过用户设置的接收通知方式发送给用户。

与企业管理的关系

企业中有多个项目，多个项目的资源需要分开结算，且分属不同人员进行管理。同时项目可以单独启动或停止，对其他项目没有影响。**企业管理**可以针对企业中的每个项目，分别建立企业项目，管理各自的资源，并且针对不同的企业项目，设置不同的人员进行管理。

Web应用防火墙支持企业管理，您可以将Web应用防火墙上的资源按照企业项目进行管理，并设置每个企业项目的用户权限。

须知

目前华北-乌兰察布一区域不支持企业管理功能。