Web 应用防火墙

常见问题

文档版本 153

发布日期 2025-01-17

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。

目 录

1 产品咨询

1.1 WAF 基础知识

本章节为您罗列了WAF入门级的常见问题。

Web 应用防火墙是硬防火墙还是软防火墙?

Web应用防火墙是软防火墙。当您购买WAF后，只需要将域名接入WAF，就可以使用WAF防护功能。

有关域名接入WAF的详细操作，请参见**添加防护域名**。

接入 WAF 对现有业务和服务器运行有影响吗?

接入WAF不需要中断现有业务，不会影响源站服务器的运行状态，即不需要对源站服务器进行任何操作（例如关机或重启）。

须知

以云模式的CNAME接入方式接入WAF时，您需要修改DNS解析使流量经过WAF进行转发。修改DNS解析可能会影响网站访问业务，建议您在业务量少时进行修改。有关网站接入WAF的详细操作，请参见**域名接入配置**。

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（公网IP/私网IP），华为云的Web业务
- 独享模式：域名或IP（公网IP/私网IP），华为云的Web业务

Web 应用防护墙可以部署在 VPC 内网吗?

可以。独享版WAF的独享引擎实例部署在VPC内。

独享版 WAF 是否支持跨 VPC 防护?

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，但受限于网络的不稳定性，建议WAF独享引擎实例与源站在同一个VPC中。

Web 应用防火墙是否支持防护非华为云和云下服务器?

WAF云模式可以跨云使用，支持防护非华为云和云下服务器，但是该服务器必须已连接互联网。

WAF云模式是基于域名进行防护的，只要有域名就能防护，不区分云上云下服务器，也不受Region、Project和账户的影响。

Web 应用防火墙支持哪些操作系统?

Web应用防火墙部署在云端，即与操作系统没有关系。故Web应用防火墙支持任意操作系统，任意操作系统上的域名服务器都可以接入WAF做防护。

Web 应用防火墙提供的是几层防护?

Web应用防火墙提供的是七层（物理层、数据链路层、网络层、传输层、会话层、表示层和应用层）防护。

Web 应用防火墙如何拦截请求内容?

WAF对请求的首部和body体都会进行检测。例如body的表单、xml、json等数据都会被WAF检测，WAF通过检测对不符合防护规则的请求内容进行拦截。

有关WAF防护流程的详细介绍，请参见**配置引导**。

Web 应用防火墙是否支持文件缓存?

WAF只缓存配置了网页防篡改的静态网页，用于将缓存的未被篡改的网页返回给Web访问者，以达到防篡改的目的。

如果您需要缓存所有的网站内容，可以选择部署CDN，WAF部署在CDN和源站之间，具体的配置方式请参见**同时部署CDN和WAF的配置指导**。

WAF 会缓存网站数据吗?

WAF的网页防篡改功能，可以为用户提供应用层的防护，只对网站的静态网页进行缓存，当用户访问网站时返回给用户缓存的正常页面，并随机检测网页是否被篡改。

WAF不会缓存网站数据。如果您需要缓存网站内容，可以使用**CDN**，或者同时部署WAF和CDN。

有关同时部署CDN和WAF的详细介绍，请参见**“CDN+WAF”联动提升网站防护能力和访问速度**。

Web 应用防火墙是否支持健康检查?

WAF目前暂不支持健康检查的功能，如果您希望服务器有健康性检查的功能，建议您将弹性负载均衡（ELB）和WAF搭配使用，ELB配置完成后，再将ELB的EIP作为服务器的IP地址，接入WAF，实现健康检查。

Web 应用防火墙是否支持 SSL 双向认证?

不支持。您可以在WAF上配置单向的SSL证书。

说明

添加防护网站时，如果“对外协议”使用了HTTPS协议，您需要上传证书使证书绑定到防护网站。

Web 应用防火墙支持基于应用层协议和内容的访问控制吗?

WAF支持应用层协议和内容的访问控制，应用层协议支持HTTP和HTTPS。

Web 应用防火墙是否可以对用户添加的 Post 的 body 进行检查?

WAF的内置检测会检查Post数据，webshell是Post提交的文件。Post类型提交的表单、json等数据，都会被WAF的默认策略检查。

您可以通过配置精准访问防护规则，对添加的Post的body进行检查。有关配置精准访问防护规则的详细操作，请参见**配置精准访问防护规则**。

Web 应用防火墙可以限制域名访问速度吗?

不支持。WAF支持通过自定义CC防护规则，限制单个IP/Cookie/Referer访问者对防护网站上特定路径（URL）的访问频率，精准识别CC攻击以及有效缓解CC攻击。

有关CC防护规则的详细介绍，请参见**配置CC攻击防护规则**。

Web 应用防火墙支持拦截包含特殊字符的 URL 请求吗?

WAF不支持将拦截请求URL中含有特殊字符作为拦截条件，即URL请求中有特殊字符，WAF不会拦截。WAF可以对来源IP进行检测和限制。

Web 应用防火墙可以防止垃圾注册和恶意注册吗?

WAF不能防止垃圾注册和恶意注册等业务层面攻击行为。建议您在网站配置注册验证机制，以防止垃圾注册和恶意注册。

WAF通过对HTTP(S)请求进行检测，可以识别并阻断Web服务的网络攻击（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）。

Web 应用防火墙可以拦截 Web 页面调用其他接口的请求数据吗?

当Web页面调用其他接口的请求数据在WAF防护域名内时，该请求数据将经过WAF，WAF会检测并阻断该请求数据。

如果Web页面调用其他接口的请求数据不在WAF防护域名内，则该请求数据不经过WAF，WAF不会拦截该请求数据。

Web 应用防火墙可以设置域名限制访问吗?

WAF不能直接通过域名限制访问。WAF支持配置黑白名单规则（即设置IP黑/白名单），阻断、仅记录或放行指定IP或IP段的访问请求。

您可以通过配置黑白名单规则，阻断、仅记录或放行域名对应的IP或IP段的访问请求。

Web 应用防火墙有 IPS 入侵防御系统模块吗?

Web应用防火墙没有传统防火墙的IPS模块，不支持IPS入侵防御，仅支持对HTTP/HTTPS协议的入侵检测。

WAF 支持弹性伸缩功能吗?

WAF暂不支持弹性伸缩功能。

WAF支持云模式和独享模式，请根据您的业务需求和资源，选择WAF模式。

HTTP 2.0 业务接入 WAF 防护是否会对源站有影响?

HTTP 2.0业务接入WAF防护对源站有影响。HTTP 2.0业务接入WAF防护表示WAF可以处理客户端的HTTP 2.0请求，而WAF目前仅支持以HTTP 1.0/1.1协议转发回源请求，即WAF与源站间暂不支持HTTP 2.0。因此，如果您将HTTP 2.0业务接入WAF防护，则源站的HTTP 2.0特性将会受到影响，例如，源站HTTP 2.0的多路复用特性可能失效，造成源站业务请求量上升。

WAF 中的防 SQL 注入攻击和 DBSS 中的 SQL 注入的区别?

WAF支持对SQL注入攻击进行防护，防止恶意SQL命令的执行。具体的防护检测原理参见**WAF针对SQL注入攻击的检测原理**。

数据库安全审计(DBSS)提供SQL注入库，可以基于SQL命令特征或风险等级，发现数据库异常行为立即告警。

使用 Web 应用防火墙对邮件收发和邮件端口有影响吗?

WAF是对Web应用网页进行防护，当您的网站接入WAF后，对邮件收发和邮件端口不会产生影响。

在安全组中配置 WAF 白名单，需要开放所有端口吗?

可以开放所有端口。为了降低网络安全风险，建议只开放80和443端口。

什么是并发数?

并发数指系统能够同时处理请求的数目。对于网站而言，并发数即网站并发用户数，指同时提交请求的用户数目。

WAF对QPS有限制，各版本支持的QPS和业务带宽说明，请参见**服务版本差异**。

如果证书挂载在 ELB 上，WAF 可以根据请求内容进行拦截吗?

如果证书挂载在ELB上，通过WAF的请求都是加密的。对于HTTPS的业务，您必须将证书上传到WAF上，WAF才能根据解密之后的请求判断是否进行拦截。

源站 IP 地址服务器更换安全组后，在 WAF 中需要做更改吗?

添加到WAF的网站的源站IP地址服务器更换安全组后，在WAF中不需要做任何操作，但是需要在源站放行WAF的回源IP或者实例IP。

不同WAF模式的操作方法如下：

- 云模式：**放行WAF回源IP**。
- 独享模式：**放行独享引擎回源IP**。

WAF 配置多个源站时如何负载?

如果您配置了多个源站IP地址，WAF默认使用加权轮询的方式对访问请求进行负载均衡。您也可以根据需要自定义负载均衡算法。更多信息，请参见**修改负载均衡算法**。

源站开启 gzip 对 WAF 有影响吗?

如果源站开启gzip，WAF可能误拦截源站正常访问请求。如果确认拦截的为正常访问请求，您可以参照**处理误报事件**将该事件处理为误报事件。处理后，WAF将不再拦截该事件，即“防护事件”页面中将不再显示该攻击事件，您也不会收到该攻击事件的告警通知。

使用 WAF 是否影响内网向外发送数据?

使用WAF不会影响内网机器向外发送数据。以云模式的CNAME方式或独享模式将网站成功接入WAF后，WAF对网站的HTTP(S)请求进行检测，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。

多个域名对应同一源站，Web 应用防火墙可以防护这些域名吗?

可以。不同域名对应同一个源站时，您可以将这些域名都接入WAF进行防护。

WAF的防护对象是域名或IP，如果是多个域名使用了同一个EIP对外提供服务，必须将多个域名都接入WAF才能对所有域名进行防护。

什么是防护 IP?

防护IP是指需要保护的网站的IP地址。

云模式 WAF 提供的解析地址是固定 IP 吗?

将域名通过云模式添加到WAF后，WAF会随机分配一个CNAME值给域名，用作域名解析，该CNAME值是WAF IP池内随机分配的，不是固定的。

源站 IP 更改后是否会改变 CNAME 值?

通过云模式WAF接入网站，源站IP更改后，不会改变WAF分配给该网站的CNAME值。

更换 IP 后，需要重新将域名添加到 WAF 吗?

如果网站所在的IP没有发生变化则无需重新在WAF中重新配置，如果网站解析到了新IP则需要重新配置。

WAF 需要绑定 EIP 吗?

WAF云模式无需绑定EIP，独享WAF需要和七层的独享型ELB进行联动，ELB需要有公网IP地址作为业务地址。详细的操作请参见**为弹性负载均衡绑定弹性公网IP**.。

Web 应用防火墙支持漏洞检测吗?

WAF的网站反爬虫防护功能可以对第三方漏洞攻击等威胁进行检测和拦截。在配置网站反爬虫防护规则时，如果您开启了扫描器，WAF将对扫描器爬虫，如OpenVAS、Nmap等进行检测。

有关网站反爬虫防护规则的详细操作，请参见**配置网站反爬虫防护规则**。

Web 应用防火墙是否支持 Exchange 里的相关协议?

WAF支持exchange里登录网页webmail时的http和https协议；WAF不支持exchange里的SMTP 、POP3 、IMAP 等邮件相关的协议。

Web 应用防火墙是否支持防御 XOR 注入攻击?

Web应用防火墙支持防御XOR注入。

为什么域名接入 WAF 后，有的攻击场景还是触发不了拦截呢?

大概率是因为客户没有开启Web基础防护的header全检测。在header自定义字段中携带攻击载荷，“header全检测”必须开启拦截模式，才可以拦截此类攻击。具体的操作请参见**配置Web基础防护规则**。

如何理解 WAF 日志里的 bind_ip 参数?

网站接入WAF后，WAF作为反向代理存在客户端与源站服务器之间，检测过滤恶意攻击流量，用bind_ip（WAF的回源IP）将正常的流量转发传输到源站。参考**如何放行云模式WAF的回源IP段?** 查看WAF的回源IP并放行回源IP。

通过 IP 接入 WAF 后，WAF 可以防护映射到这个 IP 的所有域名吗?

不支持。

WAF的独享模式支持源站IP接入WAF防护，且该IP支持私网IP或者内网IP，但WAF仅防护通过IP访问的流量，不能防护映射到这个IP的域名，如需防护域名，需要单独将域名接入WAF进行防护。

如果业务超时数据较多，如何处理?

云模式WAF为多租共享，随着其他客户业务的增长，可能会影响业务转发的时延，如果您对时延要求严格，建议您使用WAF的独享模式，该模式不会因其他客户业务增长而受到影响。

WAF 是否支持 HTTP/3 协议吗?

目前WAF最高支持HTTP/2协议，还不支持HTTP/3协议。

WAF 是否支持防护 CS 架构的网站?

如果该网站的CS架构是七层HTTP/HTTPS协议，则WAF可以防护，否则不支持防护。

WAF 云模式是否能防护其他账号下的域名?

可以。WAF云模式的防护对象是域名，只需要将该域名在当前账号下添加到WAF云模式中进行防护即可。

如何查看当前 WAF 业务 QPS 的使用情况和流入的流量?

您可以在源站上，查看源站IP地址的带宽/QPS使用情况流入的流量。

Web 应用防火墙可以拦截 multipart/form-data 格式的数据包吗?

WAF支持拦截multipart/form-data格式的数据包。

Multipart/form-data是浏览器使用表单上传文件的方式。例如，在写邮件时，如果邮件添加了附件，附件通常使用multipart/form-data格式上传到服务器。

Web 应用防火墙支持跨域禁止访问功能吗?

WAF不支持配置跨域禁止访问功能。有关WAF功能的详细介绍，请参见**功能特性**。

WAF 支持防御哪些 CVE 漏洞?

WAF支持防御的CVE漏洞：CVE-2017-7525、CVE-2019-17571、CVE-2018-1270、CVE-2016-1000027、CVE-2022-22965、CVE-2022-22968、CVE-2018-20318。

网站部署了反向代理服务器，如何配置 WAF?

如果网站部署了反向代理服务器，网站接入WAF后不会影响反向代理服务器。以云模式的CNAME接入将网站接入WAF后，WAF作为一个反向代理部署在客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址。

域名添加到 WAF 后，域名是否可以修改?

防护域名添加到WAF后，您不能修改防护域名的名称。如果您需要修改防护域名的名称，建议您删除原域名后再重新添加待防护的域名。

一个独享 WAF 实例可以接入多个 ELB 吗?

多个ELB可以共用一个WAF独享引擎实例，将独享WAF实例添加到对应的ELB后端服务器组即可。

将网站以独享模式接入WAF的具体操作请参见**网站接入WAF（独享模式）**。

1.2 Web 应用防火墙是否能防护 IP?

WAF可以对IP进行防护。

云模式-CNAME 接入

WAF不能防护IP，只能基于域名进行防护。

在WAF中配置的源站IP只支持公网IP，不支持私网IP或者内网IP。

如果您需要减少公网IP的数量，可以购买ELB（Elastic Load Balance，简称ELB）搭建负载均衡，代理后端私网IP，并将EIP（公网IP）设置为源站地址。

独享模式/云模式-ELB 接入

WAF可以对IP或域名进行防护。

在WAF中配置的源站IP支持私网IP或者内网IP。

有关域名接入WAF的流程说明，请参见**网站接入WAF**。

1.3 Web 应用防火墙支持对哪些对象进行防护?

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。

WAF支持对域名或IP进行防护，相关说明如下：

- 云模式的CNAME接入只能基于域名进行防护

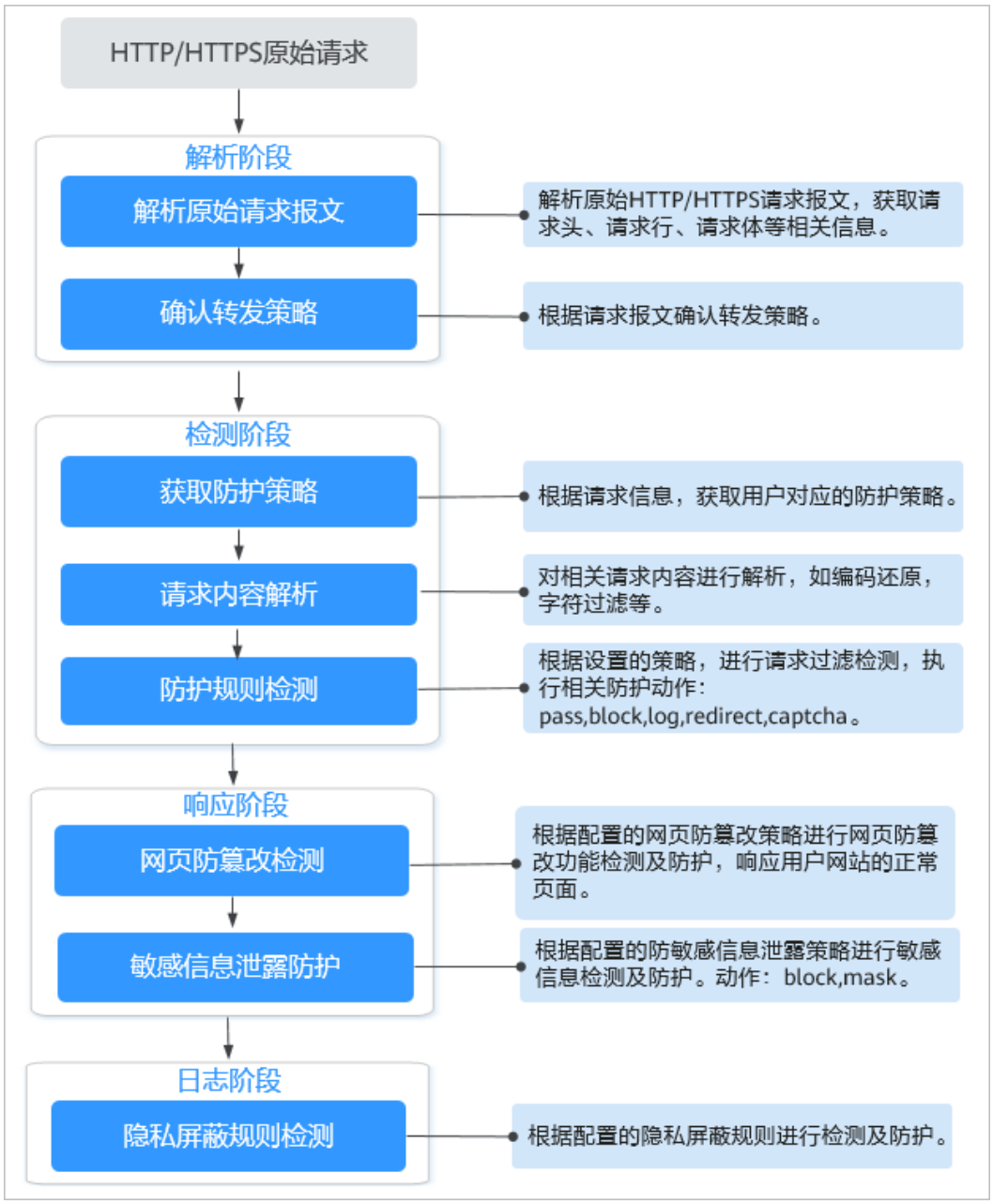
  在WAF中配置的源站IP只支持公网IP。例如，源站服务器部署了华为云弹性负载均衡（Elastic Load Balance，简称ELB）时，只要ELB（经典型、共享型或独享型）有公网IP，云模式就可以对域名进行防护。
- 独享模式和云模式的ELB接入可以对域名或IP进行防护

1.4 Web 应用防火墙支持自定义 POST 拦截吗?

WAF不支持自定义POST拦截。

针对HTTP/HTTPS原始请求，WAF引擎内置防护规则的检测流程如**图1-1**所示。

图 1-1 WAF 引擎检测图



有关WAF防护流程的详细介绍，请参见**配置引导**。

1.5 Web 应用防火墙是否支持 IPv4 和 IPv6 共存?

WAF支持IPv4和IPv6共存，针对同一域名可以同时提供IPv6和IPv4的流量防护。

- 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可以将外部IPv6访问流量转化成对内的IPv4流量。

- 哪些Region支持IPv6防护请参考**功能总览**。

须知

仅云模式专业版和铂金版支持IPv6防护。

1.6 WAF 和 HSS 的网页防篡改有什么区别?

HSS网页防篡改版是专业的锁定文件不被修改，实时监控网站目录，并可以通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，是政府、院校及企业等组织必备的安全服务。

WAF网页防篡改为用户提供应用层的防护，对网站的静态网页进行缓存，当用户访问网站时返回给用户缓存的正常页面，并随机检测网页是否被篡改。

网页防篡改的区别

HSS与WAF网页防篡改的区别，如**表1-1**所示。

表 1-1 HSS 和 WAF 网页防篡改的区别

类别	HSS	WAF
静态网页	锁定驱动级文件目录、Web文件目录下的文件，禁止攻击者修改。	缓存服务端静态网页
动态网页	• 动态数据防篡改 提供tomcat应用运行时自我保护，能够检测针对数据库等动态数据的篡改行为。 • 特权进程管理 配置特权进程白名单后，网页防篡改功能将主动放行可信任的进程，确保正常业务进程的运行。	不支持
备份恢复	• 主动备份恢复 若检测到防护目录下的文件被篡改时，将立即使用本地主机备份文件自动恢复被非法篡改的文件。 • 远端备份恢复 若本地主机上的文件目录和备份目录失效，可通过远端备份服务恢复被篡改的网页。	不支持
防护对象	网站防护要求高，手动恢复篡改能力差	网站防护要求低，仅需要对应用层进行防护

如何选择网页防篡改

防护对象	选择网页防篡改
普通网站	WAF网页防篡改+HSS企业版
网站防护+高要求网页防篡改	WAF网页防篡改+HSS网页防篡改

1.7 Web 应用防火墙支持哪些 Web 服务框架/协议?

Web应用防火墙部署在云端，与Web服务框架没有关系。

WAF通过对HTTP/HTTPS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。

WAF支持防护的协议类型说明如下：

- WebSocket/WebSockets协议，且默认为开启状态
  - “对外协议”选择“HTTP”时，默认支持WebSocket
  - “对外协议”选择“HTTPS”时，默认支持WebSockets
- HTTP/HTTPS协议

1.8 WAF 可以防护使用 HSTS 策略/NTLM 代理认证访问的网站吗?

可以。WAF支持防护HTTP/HTTPS协议业务。

- 网站选择使用HSTS（HTTP Strict Transport Security，HTTP严格传输安全协议）策略后，会强制要求客户端（如浏览器）使用HTTPS协议与网站进行通信，以减少会话劫持风险。配置HSTS策略的网站使用的是HTTPS协议，WAF可以防护。
- NTLM（New Technology LAN Manager，Windows NT LAN管理器）代理是Windows平台下HTTP代理的一种认证方式，其认证方式与Windows远程登录的认证方式是一样的，客户端（如浏览器）和代理之前需要三次握手才开始传递信息。

  对于客户端（如浏览器）和代理之前使用NTLM认证的业务，WAF可以防护。

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（公网IP/私网IP），华为云的Web业务
- 独享模式：域名或IP（公网IP/私网IP），华为云的Web业务

1.9 WAF 转发和 Nginx 转发有什么区别?

WAF转发和Nginx转发的主要区别为Nginx是直接转发访问请求到源站服务器，而WAF会先检测并过滤恶意流量，再将过滤后的访问请求转发到源站服务器，详细说明如下：

- WAF转发

  网站接入WAF后，所有访问请求将先经过WAF，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流量后，将正常流量返回给源站，从而确保Web应用安全、稳定、可用。

  图 1-2 防护原理

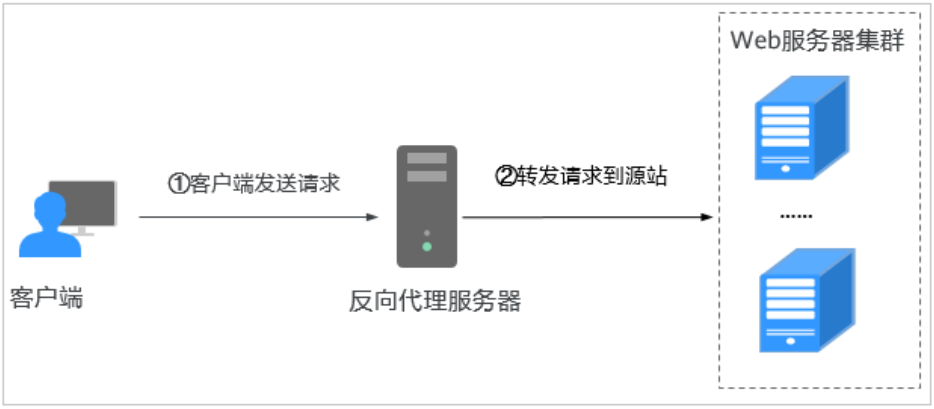
  

- Nginx转发

  即反向代理（Reverse Proxy）方式转发。反向代理服务器接受客户端访问请求后，直接将访问请求转发给Web服务器，并将从Web服务器上获取的结果返回给客户端。反向代理服务器安装在网站机房，代理Web服务器接收访问请求，并对访问请求进行转发。

  反向代理可以防止外网对内网服务器的恶性攻击，缓存以减少内网服务器压力，还可以实现访问安全控制和负载均衡。

  图 1-3 Nginx 转发原理

1.10 Web 应用防火墙和云防火墙有什么区别?

Web应用防火墙和云防火墙是华为云推出的两款不同的产品，分别针对您的Web服务，互联网边界和VPC边界的流量进行防护。

WAF和CFW的主要区别说明如表1-2所示。

表 1-2 WAF 和 CFW 的主要区别说明

类别	Web应用防火墙	云防火墙
定义	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。	云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。
防护机制	网站成功接入WAF后，WAF作为一个反向代理存在于客户端和服务器之间，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。	CFW可对全流量进行精细化管控，包括互联网边界防护，跨VPC，NAT流量防护，防止外部入侵、内部渗透攻击和从内到外的非法访问。

类别	Web应用防火墙	云防火墙
部署模式	WAF支持云模式、独享模式和ELB模式。 ● **云模式**-CNAME接入：业务服务器部署在华为云、非华为云或线下，且防护对象为域名。 各服务版本推荐使用的场景说明如下： – 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，或是具有特殊定制的安全需求 ● **云模式**-ELB接入：业务服务器部署在华为云，防护对象为域名或IP。大型企业网站，对业务稳定性有较高要求的安全防护需求。 ● **独享模式**：业务服务器部署在华为云，防护对象为域名或IP。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。	互联网边界和VPC边界
防护对象	● 云模式-CNAME接入：域名。 ● 独享模式/云模式-ELB接入：域名或IP。	弹性公网IP和VPC
功能特性	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防护。	● **资产管理与入侵防御**：对已开放公网访问的服务资产进行安全盘点，进行实时入侵检测与防御。 ● **访问控制**：支持互联网边界访问流量的访问控制。 ● **流量分析与日志审计**：VPC间流量全局统一访问控制，全流量分析可视化，日志审计与溯源分析。

1.11 Web 应用防火墙可以配置会话 Cookie 吗?

WAF不支持配置会话Cookie。

WAF可以通过配置CC攻击防护规则，限制单个Cookie字段特定路径（URL）的访问频率，精准识别CC攻击以及有效缓解CC攻击。例如，您可以通过配置CC攻击规则，使Cookie标识为name的用户在60秒内访问域名的“/admin*”页面超过10次时，封禁该用户访问域名600秒。

有关配置CC攻击防护规则的详细操作，请参见**配置CC攻击防护规则**。

什么是 Cookie

Cookie是网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），Cookie由Web服务器发送到浏览器，可以用来记录用户个人信息。

Cookie由一个名称（Name）、一个值（Value）和其它几个用于控制Cookie有效期、安全性、使用范围的可选属性组成。Cookie分为会话Cookie和持久性Cookie两种类型，详细说明如下：

- 会话Cookie

  临时的Cookie，不包含到期日期，存储在内存中。当浏览器关闭时，Cookie将被删除。
- 持久性Cookie

  包含到期日期，存储在磁盘中，当到达指定的到期日期时，Cookie将从磁盘中被删除。

1.12 WAF 对 SQL 注入、XSS 跨站脚本和 PHP 注入攻击的检测原理?

SQL（Structured Query Language）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。

XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript，但实际上也可以包括Java、 VBScript、ActiveX、 Flash 或者甚至是普通的HTML。攻击成功后，攻击者可能得到包括但不限于更高的权限（如执行一些操作）、私密网页内容、会话和Cookie等各种内容。

WAF 针对 SQL 注入攻击的检测原理

WAF针对SQL注入攻击的检测原理是检测SQL关键字、特殊符号、运算符、操作符、注释符的相关组合特征，并进行匹配。

- SQL关键字（如 union，Select，from，as，asc，desc，order by，sort，and ，or，load，delete，update，execute，count，top，between，declare，distinct，distinctrow，sleep，waitfor，delay，having，sysdate，when，dba_user，case，delay 等）
- 特殊符号（’ ”,; () ）
- 运算符（±*/%| ）
- 操作符（=，>,<,>=,<=,!=,+=,-= ）

- 注释符（–，/**/）

WAF 针对 XSS 攻击的检测原理

WAF对XSS跨站脚本攻击的检测原理主要是针对HTML脚本标签、事件处理器、脚本协议、样式等进行检测，防止恶意用户通过客户端请求注入恶意XSS语句。

- XSS关键字（javascript 、script、object、style、iframe、body、input、form、onerror、alert等）；
- 特殊字符（<、>、’ 、” ）；
- 外部链接（href=“http：//xxx/”，src="http：//xxx/attack.js"）。

说明

如果业务需要上传富文本，可以用multipart方式上传，不用body方式上传，放在表单里，即使base64编码也会解码。分析业务场景，建议限制引号、尖括号输入。

WAF 针对 PHP 攻击的检测原理

如果请求中包含类似于system(xx) 关键字，该关键字具有PHP注入攻击风险，因此，WAF会拦截了该类请求。

1.13 WAF 是否可以防护 Apache Struts2 远程代码执行漏洞（CVE-2021-31805）？

WAF的Web基础防护规则可以防护Apache Struts2远程代码执行漏洞（CVE-2021-31805）。

参考以下配置方法完成配置。

配置方法

步骤1 购买WAF。

步骤2 将网站域名添加到WAF中并完成域名接入，详细操作请参见添加防护域名。

步骤3 将Web基础防护动作设置为“拦截”模式，详细操作请参见配置Web基础防护规则。

----结束

1.14 接入 WAF 后为什么漏洞扫描工具扫描出未开通的非标准端口?

问题现象

域名接入WAF通过第三方漏洞扫描工具扫描后，扫描结果显示了域名的标准端口（例如443）和非标准端口（例如8000、8443等）。

可能原因

由于WAF的非标准端口引擎是所有用户间共享的，即通过第三方漏洞扫描工具可以检测到所有已在WAF中使用的非标准端口。域名的端口检测，应以源站IP开通的端口为

准，即引擎的端口检测并不影响源站的使用安全，且WAF保证客户解析CNAME返回的引擎IP的安全性。

处理建议

无需处理

1.15 多 Project 下使用 Web 应用防火墙的限制条件?

各Project是相互独立的，创建的策略、证书都不可互用。

- 策略不可互用，例如，主Project创建的policy A，则子Project创建的规则都不能属于policy A，只能单独创建策略。
- 证书不可互用，主Project和子Project创建的证书无法相互推送，则只能使用各自Project创建的证书。

1.16 本地文件包含和远程文件包含是指什么?

您可以在WAF的防护事件中查看文件包含等安全事件，快速定位攻击源或对攻击事件进行分析。

文件包含是指程序开发人员一般会把重复使用的函数写到单个文件中，需要使用某个函数时直接调用此文件，而无需再次编写，这种文件调用的过程一般被称为文件包含。文件包含分为本地文件包含和远程文件包含，说明如下：

- 当被包含的文件在服务器本地时，称为本地文件包含。
- 当被包含的文件在第三方服务器时，称为远程文件包含。

文件包含漏洞是指通过函数包含文件时，由于没有对包含的文件名进行有效的过滤处理，被攻击者利用从而导致了包含了Web根目录以外的文件进来，导致文件信息的泄露甚至注入了恶意代码。

有关查看防护日志的详细操作，请参见**查看防护日志**。

1.17 QPS 和请求次数有什么区别?

QPS（Queries Per Second）即每秒钟的请求量，例如一个HTTP GET请求就是一个Query。请求次数是间隔时间内请求的总量。

QPS是单个进程每秒请求服务器的成功次数。

说明

QPS = 请求数/秒（req/sec ）

“安全总览”页面中QPS的计算方式说明如**表1-3**所示。

表 1-3 QPS 取值说明

时间段	QPS平均取值说明	QPS峰值取值说明
“昨天”、“今天”	间隔1分钟，取1分钟内的平均值	间隔1分钟，取1分钟内的最大值
“3天”	间隔5分钟，取5分钟内的平均值	间隔5分钟，取5分钟内的最大值
“7天”	间隔10分钟，取每5分钟内平均值的最大值	间隔10分钟，取10分钟内最大值
“30天”	间隔1小时，取每5分钟内平均值的最大值	间隔1小时，取1小时内最大值

WAF各版本支持的QPS指标说明，请参见**服务版本差异**。

1.18 Web 应用防火墙支持自定义授权策略吗?

WAF支持自定义授权策略，通过IAM，您可以：

- 根据企业的业务组织，在您的华为账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用WAF资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将WAF资源委托给更专业、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

有关创建WAF权限策略的详细介绍，请参见**创建用户组并授权使用WAF**。

1.19 为什么 Cookie 中有 HWWAFSESID 或 HWWAFSESTIME 字段?

HWWAFSESID：会话ID；HWWAFSESTIME：会话时间戳，这两个字段用于标记请求，如CC防护规则中用户计数。

防护域名/IP接入WAF后，WAF会在客户请求Cookie中插入HWWAFSESID（会话ID），HWWAFSESTIME（会话时间戳）等字段，这些字段服务于WAF统计安全特性，不插入这些字段将会影响CC人机验证、攻击惩罚、动态反爬虫的功能使用。

说明

以下配置中，WAF不会在客户请求Cookie中插入HWWAFSESID（会话ID），HWWAFSESTIME（会话时间戳）字段：

- 防护动作配置为“放行”的规则。
- 全局白名单规则中“不检测模块”选择了“所有检测模块”。
- 防护模式为“暂停防护”。
- 未开启Web基础防护。

1.20 云模式、独享模式可以互相切换吗?

不能直接切换。添加防护域名/IP时，您需要根据业务实际情况，选择部署模式：云模式-CNAME接入、云模式-ELB接入或独享模式。防护域名添加到WAF后，部署模式不能切换。

如果您需要更换防护域名/IP的部署模式，请确保业务已部署到对应模式。在WAF的网站配置列中删除添加的防护域名/IP后，再以对应的部署方式重新添加该防护域名/IP，完成部署模式切换。例如，“www.example.com”防护域名以云模式添加到WAF，如果您希望“www.example.com”切换到独享模式，请先确保当前业务支持独享模式部署方式，申请独享模式后，您需要先删除“www.example.com”防护域名，然后再重新以独享模式方式重新添加“www.example.com”防护域名。

1.21 同一防护域名/IP 可以添加到不同的账号进行防护吗?

当防护域名以云模式添加到WAF时，不能再重复添加该防护域名进行防护。因此，同一防护域名不能添加到不同的账号进行防护。

当防护域名/IP以独享模式或云模式的ELB接入添加到WAF时，可以添加到不同的账号进行防护。

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（公网IP/私网IP），华为云的Web业务
- 独享模式：域名或IP（公网IP/私网IP），华为云的Web业务

须知

同一个域名/IP对应不同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，且占用两个防护配额。如果您需要防护同一域名/IP的多个端口，您需要将该域名/IP和端口逐一添加到WAF。

1.22 什么是区域和可用区?

什么是区域、可用区?

通常使用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。

一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图1-4阐明了区域和可用区之间的关系。

图 1-4 区域和可用区

目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。
- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

1.23 Web 应用防火墙可以跨区域使用吗?

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。

例如，如果买一个WAF能同时覆盖不同地域的业务（如北京和上海），但是如果购买北京region的WAF，对于客户在上海的业务，可能转发时长相比于北京的业务会更长。为了提高转发效率，建议您购买2个WAF（北京region的WAF和上海region的WAF），分别防护北京和上海的业务。

1.24 Web 应用防火墙支持防护哪些区域?

Web应用防火墙支持防护所有区域。

须知

- 购买WAF后，区域不能修改。如果您需要修改购买WAF的区域，您可以退订后重新购买。
- 同一账号在同一个大区域（例如，华东区域（华东-上海一、华东-上海二））只能购买一个服务版本。

购买 WAF 时如何选择区域

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。

例如，如果您只购买了北京region的WAF，需要同时覆盖不同地域的业务（如北京和上海），对于客户在上海的业务，可能转发时长相比于北京的业务会更长。为了提高转发效率，建议您购买2个WAF（北京region的WAF和上海region的WAF），分别防护北京和上海的业务。

1.25 WAF 可以跨企业项目使用吗?

不同的WAF模式，是否支持跨企业项目使用，详情如下：

- 云模式
  - 云模式-CNAME接入：支持跨企业项目使用。
  - 云模式-ELB接入：通过WAF防护的ELB与购买的ELB实例组必须在同一个VPC内，才支持跨企业项目使用。
- 独享模式

  通过WAF购买的独享引擎实例到源站的VPC网络是互通的，则支持跨企业项目使用。否则，在某个企业项目下购买的WAF独享引擎实例， 在其他企业项目下不能使用。

说明

如果独享引擎实例到源站的VPC网络不互通，且您又想跨企业项目使用WAF实例的话，您可以在“企业项目管理”页面将购买的WAF迁入目标企业项目，使目标企业项目可以使用购买或升级的WAF。

1.26 购买或升级 WAF 时选择了企业项目，其他企业项目可以使用该企业项目的 WAF 吗?

开通企业管理功能后，WAF可以按企业项目分配管理。

- 云模式（CNAME接入和ELB接入）

  购买或升级WAF时如果您选中了某一个企业项目，其他企业项目可以使用该企业项目的WAF。

- 独享模式

  通过WAF购买的独享引擎实例到源站的VPC网络是互通的，则支持跨企业项目使用。否则，在某个企业项目下购买的WAF独享引擎实例， 在其他企业项目下不能使用。

  说明

  如果独享引擎实例到源站的VPC网络不互通，且您又想跨企业项目使用WAF实例的话，您可以在“企业项目管理”页面将购买的WAF迁入目标企业项目，使目标企业项目可以使用购买或升级的WAF。

2 购买和变更规格

2.1 同一账号可以购买多个 Web 应用防火墙吗?

购买云模式时，同一账号在同一个大区域（例如华东区域）只能选择一个服务版本。

购买云模式后，您可以升级云模式版本和规格。

2.2 主账号与子账号的权限有哪些区别?

企业为了方便管理，在IAM注册账号时，提供多个账号之间形成企业主子关系的能力，如果多个账号属于同一组织架构，可以将多个账号创建关联关系。

主账号可以给子账号划拨费用，并由子账号独立进行资源管理，子账号的作用是方便主账号进行费用管理以及成本核算。

主账号与子账号中都可以再创建更小层级的IAM用户，这些IAM用户分别属于对应的账号，可以帮助账号管理资源。企业主账号只能管理企业主账号创建的IAM用户，无法管理子账号创建的IAM用户。

主账号与子账号的权限区别取决于企业授予了该账号什么权限，账号本身并无权限区别。

关于WAF账号权限的详细介绍，请参见**WAF权限管理**。

2.3 Web 应用防火墙是否支持多个账号共享使用?

WAF不支持多个账号共享使用，每个账号需要单独购买WAF进行部署。但是支持多个IAM用户共享使用。

多个 IAM 用户共享使用

例如，您通过注册华为云创建了1个账号（“domain1”），且由“domain1”账号在IAM中创建了2个IAM用户（“sub-user1a”和“sub-user1b”），如果您授权了“sub-user1b”用户WAF的权限策略，则“sub-user1b”用户可以使用“sub-user1a”用户的WAF。

有关WAF权限管理的详细操作，请参见**创建用户组并授权使用WAF**。

2.4 WAF 是如何计算域名个数的?

WAF支持的防护域名个数计算方式说明如下:

- 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。
- 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。

有关WAF各版本支持防护的域名个数的详细说明，请参见**服务版本差异**。

2.5 防护规则条数不够用时，如何处理?

Web应用防火墙云模式提供了标准版、专业版和铂金版三种服务版本。各服务版本针对各种规则的配置条数请参见**服务版本差异**。如果您所购买的服务版本支持的规则条数不能满足您业务的需要，您可以升级服务版本。

2.6 如果流量超过 Web 应用防火墙的业务请求限制，该如何处理?

如果您的正常业务流量超过您已购买的WAF版本的业务请求限制，您在WAF中配置的全部业务的流量转发将可能受到影响。

超出业务请求限制后，可能出现限流、随机丢包、自动Bypass等现象，导致您的正常业务在一定时间内不可用、卡顿、延迟等。

说明

超出业务请求限制后，WAF不会发告警通知，当QPS超过版本支持的峰值且受到攻击时，WAF会发送告警通知。有关告警通知的详细介绍，请参见**开启告警通知**。

如果出现这种情况，您需要升级WAF版本或者扩展业务QPS，避免正常业务流量超出业务带宽限制所产生的影响。

有关升级版本的详细介绍，请参见**变更WAF云模式版本和规格**。

2.7 QPS 超过当前 WAF 版本支持的峰值时有什么影响?

如果您选择的QPS规格不足以支撑网站/应用业务每天的流量峰值，对超出当前WAF版本支持峰值的QPS，WAF将不再防护网站，可能出现限流、随机丢包、自动Bypass等现象，导致您的正常业务在一定时间内不可用、卡顿、延迟等。

WAF各版本支持的QPS规格说明如**表2-1**所示。

表 2-1 WAF 支持的 QPS 规格说明

服务版本	正常业务请求峰值	CC攻击防护峰值
标准版	2,000QPS	100,000QPS
专业版	5,000QPS	200,000QPS
铂金版	10,000QPS	1,000,000QPS
独享版	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5,000QPS – HTTPS业务：建议4,000QPS – 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1,000QPS – HTTPS业务：建议800QPS – Websocket业务：支持最大并发连接1,000 – 最大回源长连接：60,000	• WAF实例规格选择WI-500，参考性能：吞吐量：500Mbps • WAF实例规格选择WI-100，参考性能：吞吐量：100Mbps

有关WAF各版本规格的详细介绍，请参见**服务版本差异**。

2.8 续费时如何变更 Web 应用防火墙的规格?

您只能为当前的WAF云模式进行续费，续费时不能直接变更WAF的规格。即WAF会按照当前WAF的版本、购买的域名/QPS/规则扩展包的数量进行续费。如果您需要在续费时变更WAF的规格，可参见**变更云模式版本和规格**先进行操作后再进行续费操作。

如果您需要在续费时变更WAF的规格，请您根据以下说明先升级或降低WAF规格：

- 升级WAF规格
  - 从较低版本升级到任一更高版本
  - 增加域名扩展包、QPS扩展包或规则扩展包的数量

  有关升级WAF规格的详细操作，请参见**变更云模式版本和规格**。
- 降低WAF规格
  - 从较高版本降低到任一更低版本
  - 减少域名扩展包、QPS扩展包带宽扩展包或规则扩展包的数量

须知

如果重购的WAF与原WAF不在同一区域，原WAF配置数据将不能保存。当您重新购买WAF后，您需要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**退订后重购WAF，原配置数据可以保存吗？**。

2.9 如何购买域名扩展包/QPS 扩展包/规则扩展包？

购买WAF云模式的标准版、专业版和铂金版时，您可以选择购买域名扩展包、QPS扩展包或规则扩展包。同时也可以在产品信息页面单独购买扩展包。

有关扩展包的详细介绍，请参见**扩展包说明**。

须知

WAF独享模式不支持购买扩展包，因此，如果您需要扩展QPS，只能购买多个WAF独享引擎实例。

购买云模式时同时购买扩展包

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在界面右上角，单击“购买WAF实例 ”。

步骤5 在“购买Web应用防火墙”界面，选择“云模式”。

步骤6 在“购买Web应用防火墙”界面，选择“区域”和服务版本。

步骤7 可以选择“域名扩展包”、“QPS扩展包”和“规则扩展包”的数量。

步骤8 选择“购买时长”后，按界面提示付款。

说明

扩展包购买时长和购买WAF时长一致。

----结束

单独购买扩展包

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 WAF”。

步骤4 在左侧导航栏中，选择“系统管理 > 产品信息”，进入产品信息页面。

步骤5 分别在“域名扩展包”、“QPS扩展包”和“规则扩展包”列，单击“购买扩展包”。

步骤6 在“变更详情”列，增加扩展包数量。

说明

扩展包购买时长和购买WAF时长一致。

步骤7 在页面右下角，单击“下一步”。

步骤8 确认订单详情无误并阅读《Web应用防火墙免责声明》后，勾选“我已阅读并同意《Web应用防火墙免责声明》”，单击“去支付”，完成购买操作。

步骤9 进入“付款”页面，选择付款方式进行付款。

----结束

2.10 购买 WAF 时如何选择业务 QPS?

WAF对防护带宽/共享带宽没有限制，对业务带宽和业务QPS请求数有限制。WAF各版本支持的业务QPS请求数规格请参见**服务版本差异**。

什么是 QPS?

WAF的业务QPS是指所有该WAF防护的域名、站点中正常业务流量的大小，单位为QPS。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（Query 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（Query Per Second，例如一个HTTP GET请求就是一个Query）

须知

- 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。
- 带宽限制仅对云模式-CNAME接入的网站有限制，通过ELB接入方式接入的网站，没有带宽限制，仅有QPS限制。

有关QPS扩展包的详细介绍，请参见**扩展包说明**。

购买WAF时，您需要提前考虑准备通过WAF配置防护的所有站点的日常入方向和出方向总流量的峰值，确保您选购的WAF所对应的业务带宽限制大于入、出方向总流量峰值中较大的值。

什么是流量?

流量指的是业务去掉攻击流量后的正常流量。例如，您需要将所有站点对外访问的流量都接入WAF进行防护，在正常访问（未遭受攻击）时，WAF将这些正常访问流量回源到源站ECS实例；而当站点遭受攻击（CC攻击或DDoS攻击）时，WAF将异常流量拦截、过滤后，将正常流量回源到源站ECS实例。因此，您在云服务器（ECS）管理控制台中查看您源站ECS实例的入方向及出方向的流量就是正常的业务流量。如果存在多个源站ECS实例，则需要统计所有源站ECS实例流量的总和。例如：假设您需要通过WAF配置防护六个站点，每个站点的出方向的正常业务流量峰值都不超过2,000QPS，流量总和不超过12,000QPS。这种情况下，您只需选择购买Web应用防火墙铂金版套餐即可。

说明

一般情况下，出方向的流量会比较大。

超过业务带宽限制和请求限制会有什么影响

如果您的正常业务流量超过您已购买的WAF版本的业务带宽和请求限制，您在WAF中配置的全部业务的流量转发将可能受到影响。

超出业务请求限制后，可能出现限流、随机丢包等现象，导致您的正常业务在一定时间内不可用、卡顿、延迟等。

如果出现这种情况，您需要升级WAF版本或者扩展业务请求，避免正常业务流量超出业务请求限制所产生的影响。

2.11 选择业务 QPS 时是按照入流量计算还是出流量计算?

WAF的业务QPS是指所有该WAF防护的域名、站点中正常业务流量的大小，单位为QPS。

购买WAF时，您需要提前考虑准备通过WAF配置防护的所有站点的日常入方向和出方向总流量的峰值，确保您选购的WAF所对应的业务带宽限制大于入、出方向总流量峰值中较大的值。

流量指的是业务去掉攻击流量后的正常流量。例如，您需要将所有站点对外访问的流量都接入WAF进行防护，在正常访问（未遭受攻击）时，WAF将这些正常访问流量回源到源站ECS实例；而当站点遭受攻击（CC攻击或DDoS攻击）时，WAF将异常流量拦截、过滤后，将正常流量回源到源站ECS实例。因此，您在云服务器（ECS）管理控制台中查看您源站ECS实例的入方向及出方向的流量就是正常的业务流量。如果存在多个源站ECS实例，则需要统计所有源站ECS实例流量的总和。例如：假设您需要通过WAF配置防护六个站点，每个站点的出方向的正常业务流量峰值都不超过2,000QPS，流量总和不超过12,000QPS。这种情况下，您只需选择购买Web应用防火墙铂金版套餐即可。

说明

一般情况下，出方向的流量会比较大。

有关QPS的详细介绍，请参见**QPS扩展包说明**。

2.12 WAF 对防护带宽/共享带宽有限制吗?

WAF对防护带宽/共享带宽没有限制，WAF对业务带宽和QPS有限制。

WAF的业务QPS是指所有该WAF防护的域名、站点中正常业务流量的大小，单位为QPS。

购买WAF时，您需要提前考虑准备通过WAF配置防护的所有站点的日常入方向和出方向总流量的峰值，确保您选购的WAF所对应的业务带宽限制大于入、出方向总流量峰值中较大的值。

有关WAF各版本防护规格的详细介绍，请参见**服务版本差异**。

2.13 如何查看防护网站的入带宽和出带宽信息?

在安全总览页面，您可以查看防护网站或实例的带宽信息，操作步骤如下。

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的  ，选择区域或项目。

步骤3 单击页面左上方的  ，选择“安全与合规 > Web应用防火墙 WAF”，进入“总览”页面。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目的安全总览信息。

步骤4 在网站或实例下拉列表中，选择要查看的网站或实例，并选择查看的时间段（昨天、今天、3天、7天、30天）。

步骤5 在“安全统计”区域框中，选择“发送/接收字节数”页签，可以查看防护网站或实例的入带宽和出带宽信息。

----结束

3 网站接入

3.1 如何在添加域名中配置防护域名?

在使用WAF防护前，您需要根据您的Web业务防护需求，在WAF中添加防护域名，WAF支持添加单域名和泛域名。本章节为您介绍如何配置防护域名。

相关概念

- 泛域名

  泛域名是指带1个通配符“*”且以“*.”号开头的域名。

  例如：“*.example.com”是正确的泛域名，但“*.*.example.com”则是不正确的。

  说明

  一个泛域名算一个域名。

- 单域名

  单域名又称普通域名，是相对泛域名来说的，是一个具体的域名或者说不是通配符域名。

  例如：“www.example.com”或“example.com”都算一个单域名。

  说明

  如“www.example.com”或“a.www.example.com”各个明细子域名都算一个域名。

如何选择域名类型

WAF支持防护单域名和泛域名。

在DNS服务商处购买的域名为单域名（example.com），WAF中添加的域名形式可以为example.com、子域名（例如：a.example.com）、泛域名（*.example.com），可根据以下场景选择配置域名的类型：

- 如果防护的域名业务相同：输入单域名。例如：防护www.example.com的业务都是8080端口的业务，则“防护域名”直接配置为单域名“www.example.com”。

- 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：a.example.com、b.example.com和c.example.com对应的服务器IP地址相同，则“防护域名”可配置为泛域名“*.example.com”。
- 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。

说明

建议添加的“防护域名”与在DNS服务商处设置的域名保持一致。

同时在 WAF 中添加单域名和泛域名，WAF 会优先检测哪个域名?

WAF会先检测精准度高的域名。例如，www.example.com、*.a.example.com、*.example.com都添加到WAF，WAF的检测顺序为：www.example.com > *.a.example.com > *.example.com。

3.2 添加域名时，防护网站端口需要和源站端口配置一样吗?

端口为实际防护网站的端口，源站端口是WAF转发客户端请求到服务器的业务端口。两者不用配置为一样，端口配置说明如下：

- “对外协议”选择“HTTP”时，WAF默认防护“80”标准端口的业务；“对外协议”选择“HTTPS”时，WAF默认防护“443”标准端口的业务。
- 如需配置除“80”/“443”以外的端口，在防护端口下拉列表中选择非标准端口。

Web应用防火墙支持的非标准端口请参见**Web应用防火墙支持哪些非标准端口?** 。

3.3 如何放行云模式 WAF 的回源 IP 段?

网站以“云模式-CNAME”方式成功接入WAF后，建议您在源站服务器上配置只放行WAF回源IP的访问控制策略，防止黑客获取源站IP后绕过WAF直接攻击源站，以确保源站安全、稳定、可用。

须知

网站成功接入WAF后，如果访问网站频繁出现502/504错误，建议您检查并确保源站服务器已配置了放行WAF回源IP的访问控制策略。

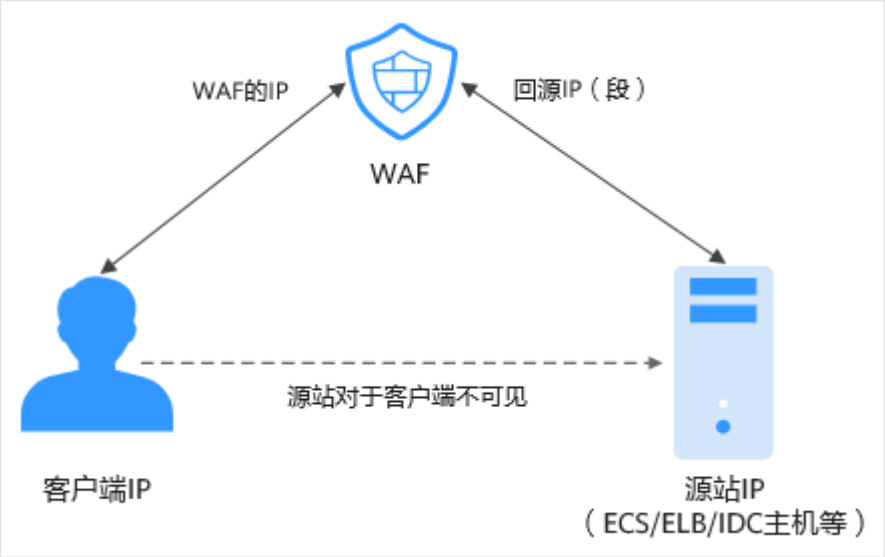
什么是回源 IP?

回源IP是WAF用来代理客户端请求服务器时用的源IP，在服务器看来，接入WAF后所有源IP都会变成WAF的回源IP，而真实的客户端地址会被加在HTTP头部的XFF字段中。

说明

- WAF的回源IP会因为扩容/新建集群而增加，对于一个客户的存量域名，一般回源IP会固定在2~4个集群的几个C类IP地址（192.0.0.0~223.255.255.255）上。
- 一般情况下，在没有灾备切换或其他调度切换集群的场景下，回源IP不会变。且WAF后台做集群切换时，会探测源站安全组配置，确保不会因为安全组配置导致业务整体故障。

图 3-1 回源 IP



回源 IP 检测机制

回源IP（该IP在回源IP段中）是随机分配的。回源时WAF会监控回源IP的状态，如果该IP异常，WAF将剔除该异常IP并随机分配正常的回源IP接收/转发访问请求。

为什么需要放行回源 IP 段?

WAF实例的IP数量有限，且源站服务器收到的所有请求都来自这些IP。在源站服务器上的安全软件很容易认为这些IP是恶意IP，有可能触发屏蔽WAF回源IP的操作。一旦WAF的回源IP被屏蔽，WAF的请求将无法得到源站的正常响应，因此，在接入WAF防护后，您需要在源站服务器的安全软件上设置放行所有WAF回源IP，不然可能会出现网站打不开或打开极其缓慢等情况。

说明

网站接入WAF后，建议您卸载源站服务器上的其他安全软件，或者配置只允许来自WAF的访问请求访问您的源站，这样既可保证访问不受影响，又能防止源站IP暴露后被黑客直接攻击。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在网站列表上方，单击“Web应用防火墙回源IP网段”，查看Web应用防火墙所有回源IP段。

图 3-2 回源 IP 网段

步骤6 在“Web应用防火墙的回源IP网段”对话框，单击“复制IP段”，复制所有回源IP。

图 3-3 Web 应用防火墙的回源 IP 网段

步骤7 打开源站服务器上的安全软件，将复制的IP段添加到白名单。

- 源站服务器部署在华为云ECS上，请参考**源站服务器部署在ECS上，放行WAF回源IP**进行操作。
- 源站服务器部署在华为云ELB上，请参考**源站服务器部署在华为云ELB上，放行WAF回源IP**进行操作。

- 如果您同时使用了华为云云防火墙（CFW），请参考**添加防护规则**放行WAF的回源IP。
- 如果后端资源在其他云厂商，请在对应安全组、访问控制等中添加信任WAF的回源IP。
- 如果源站服务器只安装了个人版杀毒软件，通常这些软件没有配置加白IP的界面。如果是对外提供Web业务的服务器，建议您安装服务器版本的企业安全软件，或华为云主机安全服务产品，这些产品会识别一些请求量较大的IP的socket，并偶发断开连接，一般情况下不会拦截WAF的回源IP。

----结束

源站服务器部署在 ECS 上，放行 WAF 回源 IP

如果您的源站服务器直接部署在华为云ECS上，请参考以下操作步骤设置安全组规则，只放行WAF回源IP段。

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“计算 > 弹性云服务器 ECS”。

步骤4 在目标ECS所在行的“名称/ID”列中，单击目标ECS实例名称，进入ECS实例的详情页面。

步骤5 选择“安全组”页签，单击“更改安全组”。

步骤6 单击安全组名称，进入安全组基本信息页面。

步骤7 选择“入方向规则”页签，单击“添加规则”，进入“添加入方向规则”页面，如**图3-4**所示，参数配置说明如**表3-1**所示。

图 3-4 添加入方向规则

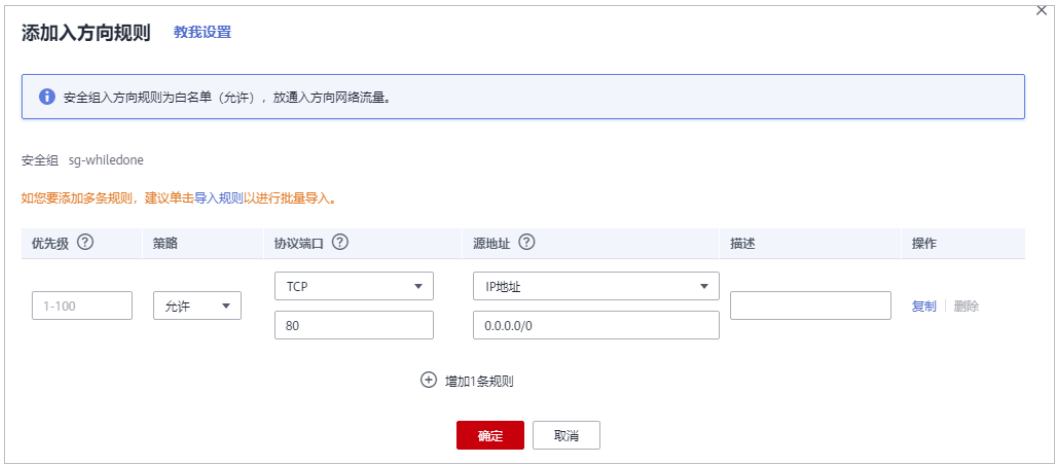


表 3-1 入方向规则参数配置说明

参数	配置说明
协议端口	安全组规则作用的协议和端口。选择“自定义TCP”后，在TCP框下方输入源站的端口。
源地址	逐一添加**步骤6**中复制的所有WAF回源IP段。 **说明** 一条规则配置一个IP。单击“增加1条规则”，可配置多条规则，最多支持添加10条规则。

步骤8 单击“确定”，安全组规则添加完成。

成功添加安全组规则后，安全组规则将允许WAF回源IP段的所有入方向流量。

----结束

源站服务器部署在华为云 ELB 上，放行 WAF 回源 IP

如果您的源站服务器直接部署在华为云ELB上，请参考以下操作步骤设置访问控制（白名单）策略，只放行WAF回源IP段。

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“网络 > 弹性负载均衡 ELB”。

步骤4 在目标ELB所在行的“监听器”列中，单击监听器名称，进入监听器的详情页面。

步骤5 在目标监听器所在行的“访问控制”列，单击“设置”。

图 3-5 监听器列表

步骤6 在弹出的对话框中，“访问控制”选择“白名单”。

1. 单击“创建IP地址组”，将**步骤6**中复制的WAF回源IP地址添加到“IP地址组”。
2. 在“IP地址组”的下拉框中选择**步骤6.1**中创建的IP地址组。

步骤7 单击“确定”，白名单访问控制策略添加完成。

----结束

3.4 删除防护域名后 CNAME 记录会保留多久?

删除防护域名时，如果您没有勾选“强制删除WAF的接入CNAME”，WAF会将该域名的CNAME保留约30天后再删除该CNAME。

但是如果您在删除防护域名时，勾选了“强制删除WAF的接入CNAME”，WAF不再检测业务域名解析配置，立即删除WAF的CNAME，如果业务域名解析未做修改，可能会导致业务异常。

3.5 后端服务器配置多个源站地址时的注意事项?

- 同一个域名在后端配置多个源站地址时，请注意：
  - 域名对应的业务端口为非标准端口

    对外协议、源站协议和源站端口必须都相同
  - 域名对应的业务端口为标准端口

    对外协议、源站协议和源站端口可不相同
- 添加域名时，WAF支持添加多个服务器IP，多个服务器之间，WAF采用轮询的方式回源，这样有助于减少服务器的压力，起到保护源站的作用。例如，后端添加了两个服务器IP（IP-A，IP-B），当有10个请求访问该域名时，5个请求会被WAF转发到IP-A，其余5个请求会被WAF转发到IP-B。

3.6 Web 应用防火墙支持配置泛域名吗?

在WAF中添加防护的域名时，您可以根据业务需求配置单域名或泛域名，说明如下：

- 单域名

  配置待防护的单域名。例如：www.example.com。
- 泛域名

  配置泛域名可以使泛域名下的多级域名经过WAF防护。
  - 如果各子域名对应的服务器IP地址相同：配置防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。
  - 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条配置。

有关添加防护域名的详细操作，请参见**添加防护域名**。

3.7 Web 应用防火墙支持防护中文域名吗?

WAF不支持中文域名。防护的域名只能由字母、数字、-、_和.组成，且域名的字符长度不能超过63个字符长度。

WAF支持防护单域名和泛域名。

- 单域名：输入防护的单域名。
- 泛域名：输入防护的泛域名。

3.8 泛域名和单域名都接入 WAF，WAF 如何转发访问请求?

单域名和泛域名都接入WAF后，WAF优先将防护网站的访问请求转发到单域名，如果不能识别单域名，访问请求将转发到泛域名。

例如，单域名a.example.com和泛域名*.example.com接入WAF，访问请求将优先通过单域名a.example.com进行转发。

泛域名配置说明如下：

- 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。
- 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。

3.9 添加域名时提示“非法的源站地址”，如何处理?

故障现象

添加防护域名时，无法添加域名，提示“非法的源站地址”。

可能原因

- “源站地址”配置为内部保留的私网IP地址。
- “防护对象”和“源站地址”配置成了一样。

处理建议

将“源站地址”配置为真实的源站IP地址（公网IP地址）或单独的回源域名（回源域名不能和“防护域名”相同）。

3.10 添加防护域名时，提示“其他人已经添加了该域名，请确认该域名是否属于你”，如何处理?

背景

添加防护域名时，如果不能正常添加域名，而提示：其他人已经添加了该域名，请确认该域名是否属于您，如果是，请联系服务人员帮您解决。

原因

可能是由于您的域名已在其他账号下添加到了WAF。同一个域名不支持重复添加到WAF。

解决办法

如果您想将该域名添加到当前账号下进行使用，需要将该域名在其他账号下的相关配置进行删除，删除后再在当前账号下重新将域名添加到WAF。

3.11 添加域名时，为什么不能选择对外协议?

添加防护域名时，如果配置了非标准端口，当对外协议（HTTP/HTTPS）不支持该非标准端口时，您将不能选择对外协议。建议您在配置非标准端口时，确认对外协议（HTTP/HTTPS）支持该非标准端口。

有关WAF支持的非标准端口的详细介绍，请参见**Web应用防火墙支持哪些非标准端口?** 。

3.12 云模式服务器的源站地址可以配置成 CNAME 吗?

可以。如果服务器的源站地址配置为CNAME，添加域名后会多经历一层DNS解析，即先将CNAME解析为IP地址，DNS解析会增加时延，故推荐您将源站地址配置成公网IP地址。

添加域名的相关配置请参见**添加防护域名**。

3.13 如何在华为云的云解析服务上进行 DNS 验证?

DNS验证一般需要由您的域名管理人员进行相关操作。如果您是在华为云平台管理您的域名，并且您的域名在您的华为账号中，请参见本章节在华为云的云解析服务上进行DNS验证。

须知

如果您是在其他域名管理平台（如万网、新网、DNSPod等）管理您的域名，请在相应的平台上进行DNS验证。例如，域名托管在阿里云，则需要到阿里云的云解析DNS控制台进行相关配置。

以下操作步骤是以申请证书的域名“domain3.com”添加一条DNS记录“2019030700000022ams1xbyevdn4jvahact9xzpicb565k9443mryw2qe99mbzpb”（记录类型为TXT）为例说明，在华为云的云解析服务上进行DNS验证的操作步骤。

前提条件

已获取域名验证所需的配置信息（“主机记录”和“记录值”）。

操作步骤

步骤1 登录管理控制台。

步骤2 选择“网络 > 云解析服务”，进入“云解析”页面。

步骤3 在左侧树状导航栏，选择“公网域名”，进入“公网域名”页面。

步骤4 在“公网域名”页面的域名列表中，单击需要解析的域名“domain3.com”，进入“解析记录”页面。

步骤5 在“解析记录”页面的左上角，单击“添加记录集”，进入“添加记录集”页面。

说明

如果在“解析记录”的域名列表中，已存在域名“domain3.com”的TXT记录值，直接在目标域名的“操作”列，单击“修改”，进入“修改记录集”页面。

- “主机记录”：“域名验证”页面，域名服务商返回的“主机记录”的前缀。

  根据域名服务商不同，返回的“主机记录”不同，以下仅为两个样例。

  举例：

  - 如果域名服务商返回的“主机记录”为“_dnsauth.domain3.com”，则主机记录填写“_dnsauth”。
  - 如果域名服务商返回的“主机记录”为“domain3.com”，则“主机记录”为空，不需要填写。
- “类型”：选择“TXT – 设置文本记录”。
- “线路类型”：全网默认。
- “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
- “值”：“域名验证”页面，域名服务商返回的“记录值”。

  说明

  记录值必须用英文引号引用后粘贴在文本框中。
- 其他的设置保持不变。

图 3-6 添加记录集

步骤6 单击“确定”，记录集添加成功。

当记录集的状态显示为“正常”时，表示记录集添加成功。

说明

- 该DNS配置记录在证书颁发或吊销后才可以删除。
- 请您务必检查是否正确配置了DNS记录，DNS没有配置正确是无法签发证书的。
- 验证完成后，CA机构可能还需要2-3个工作日审核域名信息，请耐心等待，在此期间，证书状态为“待完成域名验证”。CA机构审核通过后，证书审核才可以进入“待完成组织验证”状态。

----结束

3.14 未配置子域名和 TXT 记录的影响?

如果在WAF中添加的域名，已使用了DDoS高防等相关代理产品，但是没有在DNS服务商处配置“子域名”和“TXT记录”，WAF将无法判断域名的所有权。

因此，为了防止其他用户提前将您的域名配置到Web应用防火墙上，干扰WAF对您的域名进行防护，请在DNS服务商处添加一条“子域名”，并为该子域名配置一条“TXT记录”，WAF会据此判断域名的所有权真正属于哪个用户。

如何判断

目标域名在域名列表中被置灰，“接入状态”为“未接入”，且无法切换为“开启防护”模式。如果出现此种现象，则说明您的域名被其他用户占用了。

解决办法

前往您的DNS服务商处，添加一条“子域名”，并为该子域名配置一条“TXT记录”，以下以目标域名“www.example.com”为例，描述如何在华为云的云解析服务DNS进行配置。

步骤1 获取“子域名”和“TXT记录”值。

1. 登录管理控制台。
2. 单击页面左上方的 ☰，在右侧弹框中选择“安全与合规 > Web应用防火墙 WAF”，在左侧导航树中选择“网站设置”，进入“网站设置”页面。
3. 在目标域名“www.example.com”所在行中，单击目标域名，进入域名基本信息页面。
4. 在页面顶部，单击“未接入”旁边的 ⓘ，在弹出的对话框中，复制“子域名”和“TXT记录”。

步骤2 在DNS服务商添加一条WAF的子域名和TXT记录。

1. 在目标域名“www.example.com”的“操作”列，单击“解析”，如图3-7所示。

图 3-7 云解析页面入口

2. 在页面的左上角，单击“添加记录集”，进入“添加记录集”页面，配置模式如图3-8所示。
   - “记录类型”：选择“TXT-设置文本记录”。
   - “主机记录”：将步骤1.4中复制的TXT记录粘贴到文本框中。
   - “线路类型”：全网默认。
   - “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
   - “记录值”：将步骤1.4中复制的TXT记录加上引号后粘贴在对应的文本框，例如，"37c795804124dd4a0dd88defff8941f"。
   - 其他的设置保持不变。

图 3-8 添加记录集

3. 单击“确定”，完成子域名配置。

----结束

3.15 如何查询域名提供商?

用户可以通过查询域名注册信息，确认域名所属的DNS服务器信息，然后再根据域名所属的DNS服务器信息进行DNS验证的相关操作。

有关查询域名提供商的详细操作，请参见**如何查询域名提供商?** 。

3.16 新旧 CNAME 的区别?

背景

为了提高域名解析的可靠性，WAF针对CNAME做了升级。

为了不影响已添加域名的使用，WAF在已添加域名的基本信息页面保留了旧的CNAME，并呈现了新的CNAME。

新旧 CNAME 的区别

新CNAME实现了双活，即双DNS，为异构的两个DNS解析服务。提高了域名解析的可靠性。

建议您在做域名解析时，选择新的CNAME。

3.17 域名接入 Web 应用防火墙后，能通过 IP 访问网站吗?

域名接入到Web应用防火墙后，可以直接在浏览器的地址栏输入源站IP地址进行访问。但是这样容易暴露您的源站IP，使攻击者可以绕过Web应用防火墙直接攻击您的源站。

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。

建议您参照**源站保护最佳实践**配置源站保护。

3.18 如何设置使流量不经过 WAF，直接访问源站?

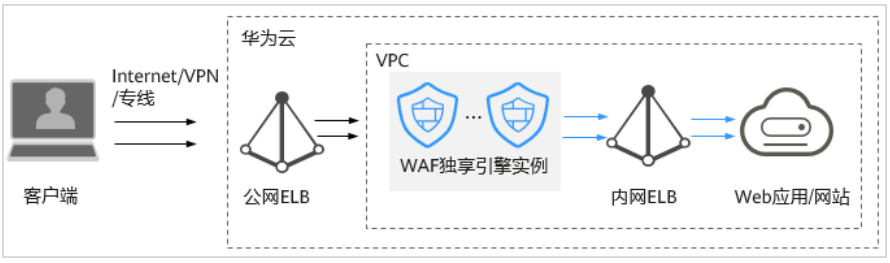
当防护网站的“部署模式”为“云模式-CNAME接入”或“独享模式”时，您可以通过以下方式，使访问防护网站的流量不经过WAF，直接访问源站。

- 云模式-CNAME接入

  到DNS服务商处将域名重新解析，指向源站服务器IP地址。

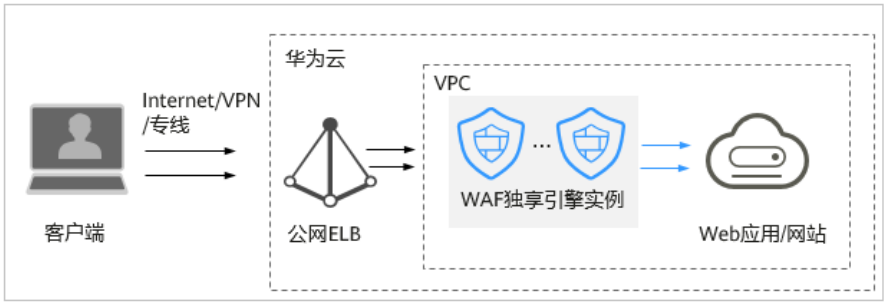
- 独享模式
  - 当网站的部署架构如**图3-9**所示时（即独享引擎实例后端部署了内网ELB），将EIP从公网ELB上解绑，然后再绑定到内网ELB上，使业务请求绕过WAF，直接到达源站。

    图 3-9 独享模式部署架构（独享引擎实例后端部署了内网 ELB）

  - 当网站的部署架构如**图3-10**所示时（即独享引擎实例后端未部署内网ELB），将公网ELB上添加的独享引擎实例移除后，再将源站添加到公网ELB，使业务请求绕过WAF，直接到达源站。

图 3-10 独享模式部署架构（独享引擎实例后端未部署内网 ELB）



独享模式配置操作-独享引擎实例后端部署了内网 ELB

通过将EIP从公网ELB上解绑，然后再绑定到内网ELB上，使访问防护网站的流量不经过WAF，直接访问源站。

步骤1 单击管理控制台左上角的，选择区域或项目。

步骤2 单击页面左上方的，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。

步骤3 在“负载均衡器”页面，目标公网ELB所在行“操作”列，选择“更多 > 解绑IPv4公网IP”，如图3-11所示。

图 3-11 解绑公网 ELB 上绑定的 EIP

步骤4 在弹出的提示框中，单击“是”，将EIP从公网ELB上解绑。

步骤5 在“负载均衡器”页面，内网ELB所在行“操作”列，选择“更多 > 绑定IPv4公网IP”。

步骤6 在弹出的“绑定IPv4公网IP”对话框中，选择步骤3解绑的公网IP后，单击“确定”，将EIP绑定到内网ELB。

----结束

独享模式配置操作-独享引擎实例后端未部署内网 ELB

通过将公网ELB上添加的独享引擎实例移除，再将源站添加到公网ELB，使业务请求绕过WAF，直接到达源站。

步骤1 单击管理控制台左上角的，选择区域或项目。

步骤2 单击页面左上方的，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。

步骤3 在负载均衡器所在行的“名称”列，单击目标负载均衡器名称，进入ELB“基本信息”页面。

图 3-12 负载均衡器列表

步骤4 选择“后端服务器组”页签，勾选待移除的独享引擎实例后，单击“移除”，如**图3-13**所示。

图 3-13 移除公网 ELB 上添加的独享引擎实例

步骤5 在弹出的提示框中，单击“是”，将独享引擎实例从公网ELB移除。

步骤6 单击“添加云服务器”，在弹出的“添加后端服务器”对话框中，选择源站服务器。

步骤7 单击“下一步”，设置业务端口后，单击“完成”，将源站服务器添加到公网ELB。

----结束

3.19 域名接入 WAF 后，为什么无法开启防护模式?

其他用户在WAF配置了同样的域名，导致域名所有权被另外一个用户占有了。此时，您需要前往您的DNS服务商处，添加一条“子域名”，并为该子域名配置一条“TXT记录”。

具体的配置方法请参见**未配置子域名和TXT记录的影响?** 。

4 防护规则

4.1 Web 基础防护支持设置哪几种防护等级?

Web基础防护设置了三种防护等级，默认为“中等”。防护等级相关说明如**表4-1**所示。

表 4-1 防护等级说明

防护等级	说明
默认规则集【宽松】	防护粒度较粗，只拦截攻击特征比较明显的请求。 当误报情况较多的场景下，建议选择“宽松”模式。
默认规则集【中等】	默认为“中等”防护模式，满足大多数场景下的Web防护需求。
默认规则集【严格】	防护粒度最精细，可以拦截具有复杂的绕过特征的攻击请求，例如jolokia网络攻击、探测CGI漏洞、探测 Druid SQL注入攻击。 建议您等待业务运行一段时间后，根据防护效果配置全局白名单规则，再开启“严格”模式，使WAF能有效防护更多攻击。

有关配置Web基础防护规则的详细操作，请参见**配置Web基础防护规则**。

4.2 CC 攻击的防护峰值是多少?

各版本对应的CC攻击防护峰值如**表1 CC攻击的防护峰值**所示。

表 4-2 CC 攻击的防护峰值

服务版本	正常业务请求峰值	CC攻击防护峰值
标准版	• 2,000 QPS • 6,000回源长连接（每域名）	100,000QPS
专业版	• 5,000 QPS业务请求 • 6,000 回源长连接（每域名）	200,000QPS
铂金版	• 10,000 QPS业务请求 • 6,000 回源长连接（每域名）	1,000,000QPS
独享版	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5,000QPS – HTTPS业务：建议 4,000QPS – 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1,000QPS – HTTPS业务：建议800QPS – Websocket业务：支持最大并发连接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	• WAF实例规格选择WI-500，参考性能：吞吐量：500Mbps • WAF实例规格选择WI-100，参考性能：吞吐量：100Mbps

4.3 在什么情况下使用 Cookie 区分用户?

在配置CC防护规则时，当IP无法精确区分用户，例如多个用户共享一个出口IP时，用户可以使用Cookie区分用户。

用户使用Cookie区分用户时，如果Cookie中带有用户相关的“session”等“key”值，直接设置该“key”值作为区分用户的依据。

须知

如果CC防护策略中配置的URL请求是被其他服务调用的API接口，可能不支持Cookie方式。

4.4 CC 规则里“限速频率”和“放行频率”的区别?

“限速频率”是单个Web访问者在限速周期内可以正常访问的次数，如果超过该访问次数，WAF将根据配置的CC攻击防护规则“防护动作”来处理。例如，“限速频率”设置为“10次/60秒”，“防护动作”设置为“阻断”，则表示60秒只能有10次访问请求，一旦在60秒内访问请求超过10次，WAF就直接阻断该Web访问者访问目标URL。

配置CC防护规则时，如果选择了“高级”工作模式，且“防护动作”配置为“动态阻断”，则除了需要配置“限速频率”外，还需要配置“放行频率”。

如果在一个限速周期内，访问的请求频率超过“限速频率”触发了拦截，那么，在下一个限速周期内，拦截阈值将动态调整为“放行频率”。且“放行频率”为0时，表示上个周期发生拦截后，下一个周期所有满足规则条件的请求都会被拦截。

区别

- “放行频率”和“限速频率”的限速周期一致。
- “放行频率”小于等于“限速频率”，且“放行频率”可为0。

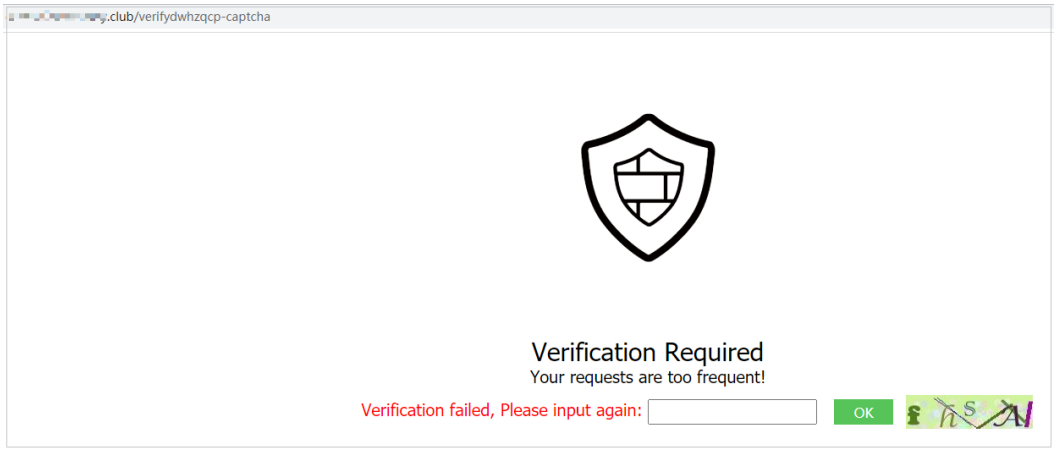
有关配置CC攻击防护规则的详细介绍，请参见**配置CC攻击防护规则**。

4.5 配置“人机验证”CC 防护规则后，验证码不能刷新，验证一直不通过，如何处理?

故障现象

在WAF上开启“CC攻击防护”，添加“防护动作”为“人机验证”的规则后，访问网站，验证码不能刷新，验证一直不通过，如**图4-1**所示。

图 4-1 验证码一直验证不通过



配置“人机验证”后，在配置的指定时间内当用户访问网站超过配置的次数限制后，将弹出验证码进行人机验证，完成验证后，请求将不受访问限制。

有关配置CC攻击防护规则的详细操作，请参见**配置CC攻击防护规则**。

可能原因

域名同时接入WAF和CDN（Content Delivery Network，内容分发网络），CC攻击防护规则的“路径”中包含静态页面，静态页面被CDN缓存，导致验证码不能刷新，验证不能通过。

处理建议

在CDN上，将缓存的静态URL设置为放行，操作步骤如下。

须知

配置完成后，请等待3～5分钟，待配置的缓存策略生效后，再访问网站使用验证码功能。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“CDN与智能边缘 > 内容分发网络 CDN”，进入CDN页面。

步骤4 在左侧导航树中，选择“域名管理”，进入“域名管理”页面。

步骤5 在“域名”列，单击目标域名的名称，进入域名配置页面。

步骤6 选择“缓存配置”页签，单击“编辑”，系统弹出“配置缓存策略”对话框。

步骤7 单击“添加”，添加两条缓存策略规则，如图4-2所示，相关参数说明如表4-3所示。

图 4-2 “配置缓存策略”对话框

表 4-3 配置静态 URL 缓存策略参数说明

参数	配置说明
类型	选择“全路径”。

参数	配置说明
内容	依次添加的两条规则的内容为： • “/verifydwhzqcp-captcha” • “/getdwhzqcp-captcha.jpg”
优先级	将两条规则设置为最高的优先级。
缓存过期时间	设置为“0”，不缓存静态URL。

步骤8 单击“确定”，完成缓存规则配置，如图4-3所示。

图 4-3 完成缓存规则配置

配置完成后，请等待3～5分钟，待配置的缓存策略生效后，再访问网站使用验证码功能。

----结束

4.6 如何不拦截带有.js 的文件?

您可以通过WAF的精准访问防护规则配置放行路径后缀为.js的文件，具体配置如下：

步骤1 登录华为云WAF控制台，参考图4-4进入华为云WAF防护规则配置页面。

图 4-4 防护规则配置页面入口

步骤2 选择“精准访问防护”配置框，单击“添加规则”，配置如图4-5所示的规则。

图 4-5 放行带.js 的文件

步骤3 单击“确定”。

----结束

相关操作

关于更多精准访问防护规则的详细操作请参加**配置精准访问防护规则定制化防护策略**。

4.7 Web 应用防火墙可以批量配置黑白名单吗?

WAF支持批量配置黑白名单。您可以通过添加地址组，批量设置IP/IP段黑白规则，阻断、仅记录或放行指定IP/IP段的访问请求。您也可以为每一个IP/IP段分别配置黑白名单规则。

IP地址组集中管理IP地址或网段，被黑白名单规则引用时可以批量设置IP/IP地址段。

有关配置黑白名单规则的详细操作，请参见**配置黑白名单规则**。

4.8 Web 应用防火墙可以导入/导出黑白名单吗?

WAF支持导入黑白名单，您可以在添加黑白名单规则时选择通过“地址组”方式导入黑白名单。WAF不支持导出黑白名单。

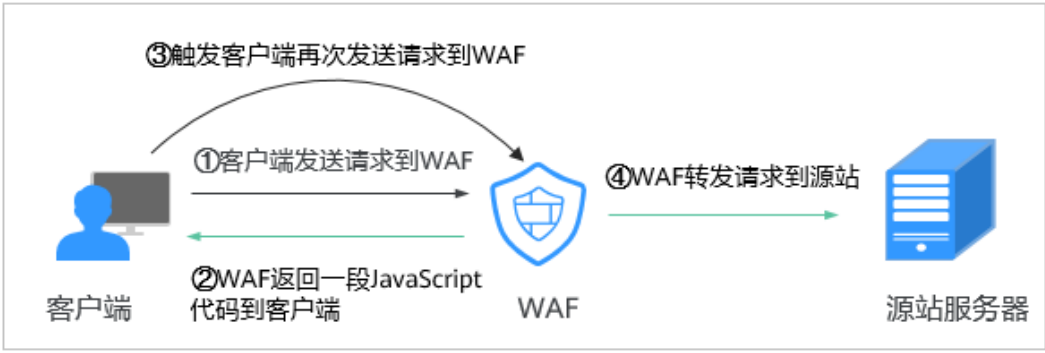
IP地址组集中管理IP地址或网段，被黑白名单规则引用时可以批量设置IP/IP地址段。

有关配置黑白名单的详细操作，请参见**配置黑白名单规则**。

4.9 开启 JS 脚本反爬虫后，为什么客户端请求获取页面失败?

开启JS脚本反爬虫后，当客户端发送请求时，WAF会返回一段JavaScript代码到客户端。如果客户端是正常浏览器访问，就可以触发这段JavaScript代码再发送一次请求到WAF，即WAF完成JS验证，并将该请求转发给源站，如图4-6所示。

图 4-6 JS 脚本反爬虫正常检测流程



- 如果客户端是爬虫访问，就无法触发这段JavaScript代码再发送一次请求到WAF，即WAF无法完成js验证。
- 如果客户端爬虫伪造了WAF的认证请求，发送到WAF时，WAF将拦截该请求，js验证失败。

须知

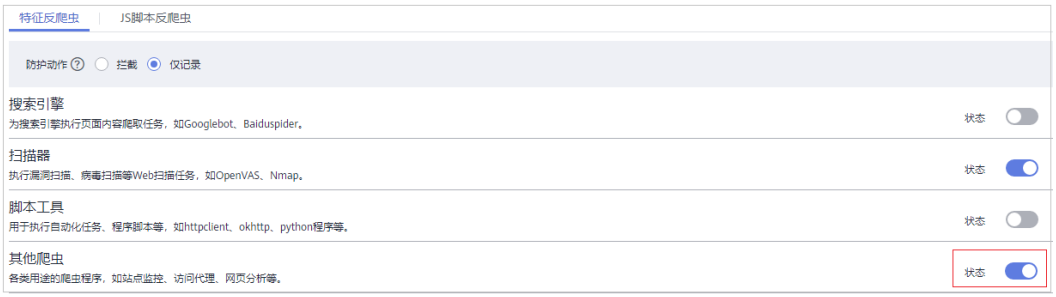
- 开启JS脚本反爬虫，要求客户端浏览器具有JavaScript的解析能力，并开启了Cookie。
- 如果客户端不满足以上要求，则只能完成①和②，此时客户端请求将不能成功获取到页面。

请您排查业务侧是否存在这种场景。如果您的网站有非浏览器访问的场景，建议您关闭JS脚本反爬虫功能。

4.10 开启网站反爬虫中的“其他爬虫”会影响网页的浏览速度吗?

在配置网站反爬虫的“特征反爬虫”时，如果开启了“其他爬虫”，WAF将对各类用途的爬虫程序（例如，站点监控、访问代理、网页分析）进行检测。开启该防护，不影响用户正常访问网页，也不影响用户访问网页的浏览速度。

图 4-7 开启“其他爬虫”

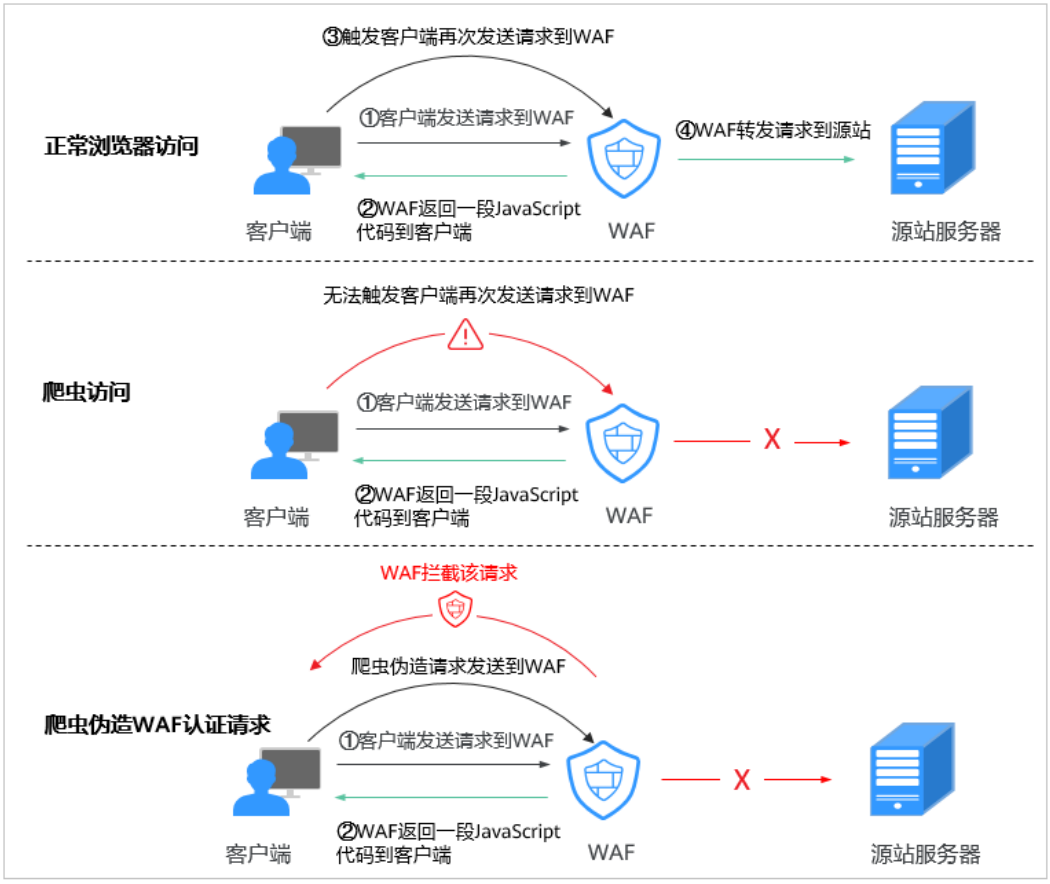


有关配置网站反爬虫的详细操作，请参见**配置网站反爬虫规则**。

4.11 JS 脚本反爬虫的检测机制是怎么样的?

JS脚本检测流程如**图4-8**所示，其中，①和②称为“js挑战”，③称为“js验证”。

图 4-8 JS 脚本检测流程说明



开启JS脚本反爬虫后，当客户端发送请求时，WAF会返回一段JavaScript代码到客户端。

- 如果客户端是正常浏览器访问，就可以触发这段JavaScript代码再发送一次请求到WAF，即WAF完成js验证，并将该请求转发给源站。

- 如果客户端是爬虫访问，就无法触发这段JavaScript代码再发送一次请求到WAF，即WAF无法完成js验证。
- 如果客户端爬虫伪造了WAF的认证请求，发送到WAF时，WAF将拦截该请求，js验证失败。

通过统计“js挑战”和“js验证”，就可以汇总出JS脚本反爬虫防御的请求次数。例如，图4-9中JS脚本反爬虫共记录了18次事件，其中，“js挑战”（WAF返回JS代码）为16次，“js验证”（WAF完成JS验证）为2次，“其他”（即爬虫伪造WAF认证请求）为0次。

图 4-9 JS 脚本反爬虫防护数据

须知

网站反爬虫“js挑战”的防护动作为“仅记录”，“js验证”的防护动作为人机验证（即js验证失败后，弹出验证码提示，输入正确的验证码，请求将不受访问限制）。

4.12 哪些情况会造成 WAF 配置的防护规则不生效?

域名成功接入WAF后，正常情况下，域名的所有访问请求流量都会经过WAF检测并转发到服务器。但是，如果网站在WAF前使用了CDN，对于静态缓存资源的请求，由于CDN直接返回给客户端，请求没有到WAF，所以这些请求的安全策略不会生效。

WAF与CDN的配置请参见**使用CDN和WAF提升网站防护能力和访问速度**。

4.13 如果只允许指定地区的 IP 可以访问，如何设置防护策略?

如果您只允许某一地区的IP访问防护域名，例如，只允许来源“上海”地区的IP可以访问防护域名，请参照以下步骤处理。

说明

由于地理位置访问控制的优先级高于内置规则的检测，配置了该地区IP放行后，WAF将不再检测其他的Web基础防护策略，直接放行。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 在“地理位置访问控制”配置列表的左上方，单击“添加规则”。

步骤7 添加一条地理位置访问控制规则，添加“上海”地区的“放行”防护动作，如图4-10所示。

图 4-10 添加“放行”防护动作

步骤8 在“精准访问防护”规则配置列表左上方，单击“添加规则”。配置一条精准访问防护规则，拦截所有的请求，如图4-11所示。

图 4-11 拦截所有访问请求

----结束

4.14 拦截所有来源 IP 或仅允许指定 IP 访问防护网站，WAF 如何配置?

防护网站接入WAF后，您可以通过配置黑白名单规则或精准访问防护规则，使WAF仅允许指定IP访问防护网站，即WAF拦截除指定IP外的所有来源IP。

通过配置 IP 黑白名单规则拦截除指定 IP 外的所有来源 IP

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 在“黑白名单设置”配置框中，开启防护规则。

图 4-12 黑白名单配置框

步骤7 在黑白名单设置规则页面左上方，单击“添加规则”。

步骤8 在弹出的“添加黑白名单设置规则”对话框中，添加2条黑名单规则，拦截所有来源IP，如图4-13和图4-14所示。

图 4-13 拦截 1.0.0.0/1 IP 地址段

图 4-14 拦截 128.0.0.0/1 IP 地址段

步骤9 单击“添加规则”，在弹出的“添加黑白名单设置规则”对话框中，分别添加放行指定IP或IP地址段的防护规则。

例如，如果您需要放行XXX.XXX.2.3，添加一条如图4-15所示防护规则。

图 4-15 放行指定 IP

----结束

通过配置精准访问防护规则拦截除指定 IP 外的所有来源 IP

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的 ☰，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 在“精准访问防护”配置框中，开启防护规则。

图 4-16 精准访问防护配置框

步骤7 在精准访问防护规则页面左上角，单击“添加规则”。

步骤8 在弹出的“添加精准访问防护规则”对话框中，添加如图4-17所示防护规则，阻断所有请求。

⚠ 注意

因为配置精准防护白名单放行的优先级要高于拦截的优先级且“优先级”值越小优先级越高，因此此处配置的“优先级”值应大于步骤9中“优先级”配置的值。

图 4-17 阻断所有的请求

步骤9 单击“添加规则”，在弹出的“添加精准访问防护规则”对话框中，分别添加放行指定IP的防护规则。

例如，如果您需要放行192.168.2.3，添加一条如**图4-18**所示防护规则。

注意

因为配置精准防护白名单放行的优先级要高于拦截的优先级且“优先级”值越小优先级越高，因此此处配置的“优先级”值应小于**步骤8**中“优先级”配置的值。

图 4-18 放行指定 IP

您也可以参照**步骤9**，在黑白名单中添加防护规则，放行指定IP或IP地址段。

----结束

4.15 系统自动生成策略包括哪些防护规则?

在添加防护网站进行“策略配置”时，您可以选择已创建的防护策略或默认的“系统自动生成策略”，系统自动生成的策略相关说明如**表4-4**所示。

须知

标准版只能选择“系统自动生成策略”。

您也可以在域名接入后根据防护需求配置防护规则。

表 4-4 系统自动生成策略说明

版本	防护策略	策略说明
标准版	Web基础防护（“仅记录”模式、常规检测）	仅记录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/代码注入等攻击行为。
专业版、铂金版/独享模式	Web基础防护（“仅记录”模式、常规检测）	仅记录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/代码注入等攻击行为。
	网站反爬虫（“仅记录”模式、扫描器）	仅记录漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap的爬虫行为。

说明

“仅记录”模式：发现攻击行为后WAF只记录攻击事件不阻断攻击。

4.16 开启网页防篡改后，为什么刷新页面失败?

WAF网页防篡改仅支持对网站的静态网页进行缓存。如果您配置网页防篡改规则后，刷新页面访问的还是未更新的页面，请参考以下步骤处理：

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“网页防篡改”配置框，检查是否已开启网页防篡改。

- ：开启状态，表示已开启，请执行步骤7。
- ：关闭状态，表示已关闭，单击开启网页防篡改，等待几分钟后，刷新页面后重新访问。。

步骤7 查看目标规则配置的域名和路径是否配置正确。

- 如果配置正确，请执行步骤8。

- 如果配置不正确，在目标网页防篡改规则所在行的“操作”列中，单击“删除”，删除该防护规则后，在列表上方单击“添加规则”，重新配置网页防篡改规则。有关配置网页防篡改规则的详细操作，请参见**配置网页防篡改规则**。

  规则添加成功，等待几分钟后，刷新页面后重新访问。

步骤8 在目标网页防篡改规则所在行的“操作”列中，单击“更新缓存”。

当防护页面内容进行了修改，请务必更新缓存，否则WAF将始终返回最近一次缓存的页面内容。

此时，刷新页面后重新访问，如果还是未更新的页面，请联系技术支持。

----结束

4.17 黑白名单规则和精准访问防护规则的拦截指定 IP 访问请求，有什么差异?

黑白名单规则和精准访问防护规则都可以拦截指定IP访问请求，两者的区别说明如**表4-5**所示。

表 4-5 黑白名单规则和精准访问防护规则区别

防护规则	防护功能	WAF检测顺序
黑白名单规则	只能阻断、仅记录或放行指定IP地址/IP地址段的访问请求。	最高 WAF根据配置的防护规则，按照防护规则检测顺序，进行访问请求过滤检测。
精准访问防护规则	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放行或阻断操作。	低于黑白名单规则

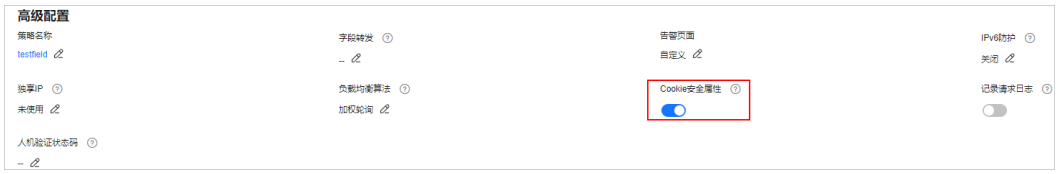
4.18 如何处理 Appscan 等扫描器检测结果为 Cookie 缺失 Secure/HttpOnly?

Cookie是后端Web Server插入的，可以通过框架配置或set-cookie实现，其中，Cookie中配置Secure，HttpOnly有助于防范XSS等攻击获取Cookie，对于Cookie劫持有一定的防御作用。

Appscan扫描器在扫描网站后发现客户站点没有向扫描请求Cookie中插入HttpOnly Secure等安全配置字段将记录为安全威胁。

当“对外协议”配置为HTTPS时，WAF支持在网站基本信息页面，开启“Cookie安全属性”，开启后会将Cookie的HttpOnly和Secure属性设置为true。

图 4-19 开启 Cookie 安全属性



4.19 如何拦截 4 层链接对应的 IP?

可通过精准访问防护规则拦截4层链接对应的IP，具体配置如下：

步骤1 登录华为云WAF控制台，参考图4-20进入华为云WAF防护规则配置页面。

图 4-20 防护规则配置页面入口

步骤2 选择“精准访问防护”配置框，单击“添加规则”，配置如图4-21所示的规则。

图 4-21 添加规则

步骤3 单击“确定”。

----结束

5 IPv6 防护

5.1 哪些版本支持 IPv6 防护?

WAF支持IPv6防护，详细说明如下：

- 云模式的CNAME接入的专业版和铂金版支持IPv6的防护。
- 独享模式/云模式-ELB接入没有公网IP，公网IP绑定在ELB的弹性公网IP上 ，如果独享模式/云模式-ELB接入所在的ELB支持IPv6，那么独享模式/云模式-ELB接入也支持IPv6。

须知

- 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可以将外部IPv6访问流量转化成对内的IPv4流量。
- 哪些Region支持IPv6防护请参考**功能总览**。

5.2 如何测试在 WAF 中配置的源站 IP 是 IPv6 地址?

执行此操作前，请确认已在WAF中添加了域名并完成了域名接入。

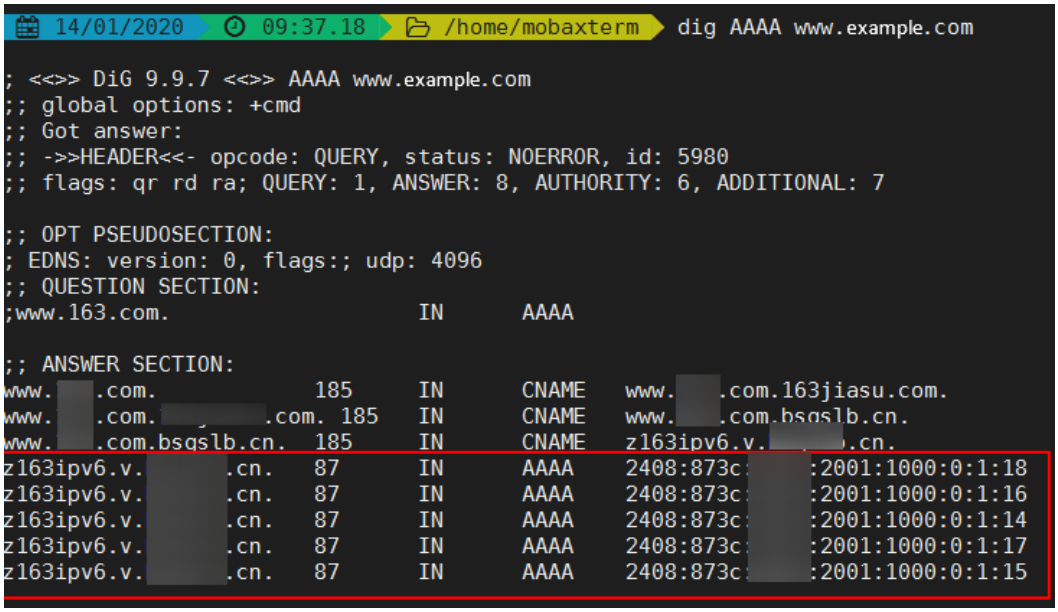
假如已在WAF中添加域名www.example.com。通过以下方法可以测试配置的源站IP是否是IPv6地址：

步骤1 在Windows中打开cmd命令行工具。

步骤2 执行**dig AAAA www.example.com**命令。

如果返回的结果里有IPv6格式的IP地址，如**图5-1**所示，则证明配置的源站IP是IPv6地址。

图 5-1 测试结果



----结束

5.3 业务使用了 IPv6，WAF 中的源站地址如何配置?

如果域名已接入了WAF（源站地址配置为IPv4地址）进行防护，当业务开启了IPv6时，WAF中配置的源站地址可以保持原IPv4地址，也可以修改为IPv6地址。

WAF支持IPv6/IPv4双栈模式和NAT64机制，详细说明如下：

- 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可以将外部IPv6访问流量转化成对内的IPv4流量。
- 哪些Region支持IPv6防护请参考**功能总览**。

须知

仅专业版和铂金版支持IPv6防护。

5.4 WAF 如何解析/访问 IPv6 源站?

当防护网站的源站地址配置为IPv6地址时，WAF直接通过IPv6地址访问源站。WAF默认在CNAME中增加IPv6地址解析，IPv6的所有访问请求将先流转到WAF，WAF检测并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。

WAF支持IPv6/IPv4双栈模式和NAT64机制，详细说明如下：

- 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可以将外部IPv6访问流量转化成对内的IPv4流量。
- 哪些Region支持IPv6防护请参考**功能总览**。

须知

仅专业版和铂金版支持IPv6防护。

6 证书管理

本章节为您罗列了证书使用过程中遇到的一些常见问题。

为什么华为云 SCM 上的 SSL 证书在 WAF 上不能查看?

华为云SCM上的SSL证书签发后或成功上传后，您需要将证书一键推送到WAF中，才能在华为云WAF中使用。

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，则不能使用SCM推送的SSL证书。

有关推送SSL证书的详细操作，请参见**推送证书到云产品**。

为什么非 default 企业项目不能使用华为云 SCM 推送的 SSL 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，则不能使用SCM推送的SSL证书。

有关SCM证书推送的详细介绍，请参见**推送证书到云产品**。

配置泛域名时，如何选择证书?

域名和证书需要一一对应，泛域名只能使用泛域名证书。如果您没有泛域名证书，只有单域名对应的证书，则只能在WAF中按照单域名的方式逐条添加域名进行防护。

ELB 已上传证书，在 Web 应用防火墙上需要重新导入上传吗?

在选择证书时，您可以选择已创建证书或选择导入的新证书。在ELB上已上传的证书，还需要在WAF上导入上传。

如何将非 PEM 格式的证书转换为 PEM 格式?

WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考**表6-1**在本地将证书转换为PEM格式，再上传。

表 6-1 证书转换命令

格式类型	转换方式
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	• 提取私钥命令，以“cert.pfx”转换为“key.pem”为例。 **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** • 提取证书命令，以“cert.pfx”转换为“cert.pem”为例。 **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	• 提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** • 提取证书命令，以“cert.cer”转换为“cert.pem”为例。 **openssl x509 -inform der -in cert.cer -out cert.pem**

说明

- 执行openssl命令前，请确保本地已安装**openssl**。
- 如果本地为Windows操作系统，请进入“命令提示符”对话框后，再执行证书转换命令。

7 防护日志

7.1 Web 应用防火墙支持记录防护日志吗?

在WAF管理控制台，您可以免费查看最近30天的防护日志。

如果您需要长期保存防护日志，您可以将WAF的防护日志记录到单独收费的云日志服务（Log Tank Service，简称LTS）上。LTS默认存储日志的时间为7天，存储时间可以在1～30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）或者数据接入服务（DIS）中长期保存。

- 有关查看防护日志的详细操作，请参见**查看防护日志**。
- 有关下载防护日志的详细操作，请参见**下载防护事件数据**。
- 有关WAF日志配置到LTS的详细操作，请参见**开启全量日志**。

7.2 Web 应用防火墙的日志是否可以通过 API 的方式获取?

您可以通过API的方式查看WAF的防护日志。

您也可以通过LTS服务的控制台分析、查看并下载防护事件，具体您可参考**下载防护事件数据**章节。

7.3 如何获取拦截的数据?

在“安全总览”页面，您可以查看昨天、今天、3天、7天、30天或自定义30天任意时间段内所有防护网站或所有实例以及指定防护网站或实例的防护日志。包括请求与各攻击类型统计次数，QPS、带宽、响应码信息，以及事件分布、受攻击域名 Top5、攻击源IP Top5、受攻击URL Top5、攻击来源区域 Top5和业务异常监控 Top5等防护数据。在“BOT防护统计”页面，可以查看BOT防护的流量分布、流量趋势和TOP事件源统计的相关数据。

7.4 防护事件列表中，防护动作为“不匹配”是什么意思呢?

配置网页防篡改、防敏感信息泄露、隐私屏蔽防护规则后，如果访问请求命中这些防护规则，则防护日志中记录的防护事件，“防护动作”显示为“不匹配”。

查看防护日志的其他信息请参见**查看防护日志**。

7.5 WAF 获取真实 IP 是从报文中哪个字段获取到的?

根据WAF不同的接入模式判断从报文中的哪个字段来获取客户端的真实IP。

云模式-CNAME 接入、独享模式接入

WAF引擎会根据防护规则确定是否代理转发请求去后端，如果WAF配置了基于IP的规则（比如黑白名单、地理位置、基于IP的精准访问防护规则），那么WAF引擎就会获取真实IP后才能放行或者拦截代理请求。获取真实IP的方法基于以下原则：

- 在WAF中开启了代理，即添加域名时，“是否使用七层代理”选择了“是”，按以下顺序获取源IP：
  a. 优先取“upstream”中配置的源IP头列表，即在域名的基本信息页面配置的“IP标记”，具体的操作请参见**配置攻击惩罚的流量标识**。如果未取到，执行**b**。

     说明

     如果想以TCP连接IP作为客户端IP，“IP标记”应配置为“remote_addr”。
  b. 取config中配置的源IP头列表“cdn-src-ip”字段对应的值，未取到，执行**c**。
  c. 取“x-real-ip”字段的值，未取到，执行**d**。
  d. 取“x-forwarded-for”字段左边开始第一个公网IP，未取到，执行**e**。
  e. 取WAF看到的TCP连接IP，“remote_addr”字段对应的值。
- 在WAF中未开启代理，即添加域名时，“是否使用七层代理”选择了“否”，直接取“remote_ip”字段的值为真实IP。

云模式-ELB 接入

1. 优先取“upstream”中配置的源IP头列表，即在域名的基本信息页面配置的“IP标记”，具体的操作请参见**配置攻击惩罚的流量标识**。如果未取到，执行**2**。

   说明

   如果想以TCP连接IP作为客户端IP，“IP标记”应配置为“remote_addr”。
2. 取config中配置的源IP头列表“cdn-src-ip”字段对应的值，未取到，执行**3**。
3. 取“x-real-ip”字段的值，未取到，执行**4**。
4. 取“x-forwarded-for”字段左边开始第一个公网IP，未取到，执行**5**。
5. 取ELB看到的TCP连接IP，“remote_addr”字段对应的值。

7.6 Web 应用防火墙的日志可以转储到 OBS 吗?

您可以先将日志配置到LTS，然后在LTS上将WAF转储到OBS。

- 有关WAF日志配置到LTS的详细操作，请参见**防护日志记录到LTS**。
- 有关LTS日志转储至OBS的详细操作，请参见**LTS日志转储至OBS**。

7.7 Web 应用防火墙的防护日志可以存储多久?

在WAF管理控制台，您可以免费查看最近30天的防护日志。

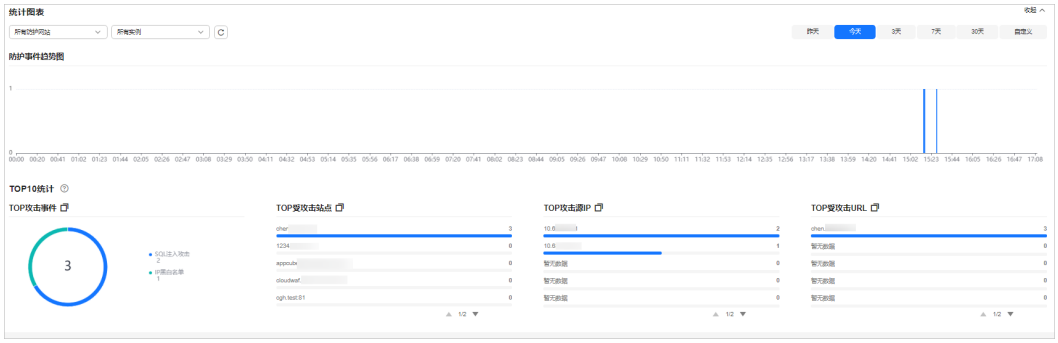
您可以将WAF的防护日志记录到单独收费的云日志服务（Log Tank Service，简称LTS），LTS默认存储日志的时间为7天，存储时间可以在1～30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）或者数据接入服务（DIS）中长期保存。

- 有关WAF日志配置到LTS的详细操作，请参见**防护日志记录到LTS**。
- 有关LTS日志转储至OBS的详细操作，请参见**LTS日志转储至OBS**。

7.8 Web 应用防火墙可以同时查询多个指定 IP 的防护事件吗?

WAF不支持同时查询多个指定IP的防护事件。您可以在“防护事件”页面，通过“事件类型”、“防护动作”、“源IP”、“URL”、“事件ID”组合条件，查看防护域名相应的防护事件。

图 7-1 防护事件



有关查看防护事件的详细操作，请参见**查看防护日志**。

7.9 Web 应用防火墙会记录未拦截的事件吗?

WAF根据配置的防护规则拦截攻击事件，并将拦截或者仅记录攻击的事件记录在防护日志中，不会记录未拦截的事件。

有关查看防护日志的详细操作，请参见**查看防护日志**。

7.10 为什么 WAF 显示的流量大小与源站上显示的不一致?

WAF“安全总览”页面显示的流量大小与源站上显示的不同，主要原因说明如下：

- 网页压缩

  WAF默认开启压缩，客户端（如浏览器）与WAF之间进行通信的网页可能被压缩（依赖浏览器压缩选项），而源站服务器可能不支持压缩。

- 连接复用

  WAF与源站服务器之间会复用socket连接，这样会降低源站服务器与WAF之间的带宽消耗。

- 攻击请求

  攻击请求被WAF拦截，而这种请求不会消耗源站服务器的带宽。

- 其他异常请求

  如果源站服务器存在超时，无法连接等情况，这种情况不会消耗源站务器的带宽。

- TCP层的重传等

  WAF统计的带宽是7层的数据，而源站服务器网卡统计的是4层的数据。当网络通信质量差时，会出现TCP重传，网卡统计的带宽会重复计算，而7层传输的数据不会重复计算。在这种情况下，WAF上显示的带宽会低于源站上显示的带宽。

7.11 为什么“安全总览”和全量日志统计的日志个数不一致?

当攻击源、匹配规则、负载位置、URL等信息一致时，全量日志只记录一条日志。因此，全量日志显示的日志个数可能会低于“安全总览”显示的日志个数。

有关查看防护日志的详细操作，请参见**查看防护日志**。

7.12 如何处理导出的防护事件数据乱码?

如果您需要将防护事件导出到本地，可在“防护事件”页面，单击“导出”。如果导出的防护事件数据，用Excel工具打开时，有乱码情况，可参照本章节处理。

原因

导出的防护事件数据为CSV格式，如果使用Excel工具打开该文件，可能会出现中文乱码的情况。这是因为通过WAF控制台导出的CSV文件使用了UTF-8编码格式，而Excel是以ANSI格式打开的，没有做编码识别。

图 7-2 导出防护事件数据

解决方案

方案一:

1. 打开csv文件时，对Excel进行如下设置：
   a. 新建Excel。
   b. 选择“数据 > 自文本”。
   c. 选择导出的防护事件数据CSV文件，单击“导入”，进入“文本导入向导”页面。
   d. 选择“分隔符号”，单击“下一步”。
   e. 去勾选“Tab键”，勾选“逗号”，单击“下一步”。
   f. 单击“完成”。
   g. 在“导入数据”对话框里，单击“确定”。
2. 完成1后，使用记事本等文本编译器直接打开，或使用WPS打开。

方案二:

1. 使用记事本文本编译器打开导出的防护事件数据CSV文件。
2. 选择“文件 > 另存为” 。
3. “编码”选择“ANSI”，修改文件名（后缀依然是.csv），避免覆盖原文件，单击“保存”。
   使用Excel打开修改后CSV文件，一般中文就可以正常显示了。