

# Web 应用防火墙

## 快速入门

文档版本 01  
发布日期 2025-02-19



版权所有 © 华为云计算技术有限公司 2025。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



HUAWEI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.....	1
2 通过 CC 攻击防护规则拦截大流量高频攻击.....	3
3 通过黑白名单设置拦截网站恶意 IP 流量.....	13
4 入门实践.....	18

# 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](#)。

独享模式在部分区域已经停售，详见[独享模式停售通知](#)。

### - [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。

## 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	防护场景	参考文档
云模式-CNAME接入	<ul style="list-style-type: none"><li>业务服务器部署在华为云、非华为云或线下</li><li>防护对象：域名</li></ul>	<a href="#">将网站接入WAF防护（云模式-CNAME接入）</a>
云模式-ELB接入	<ul style="list-style-type: none"><li>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。</li><li>防护对象：域名/IP</li></ul>	<a href="#">将网站接入WAF防护（云模式-ELB接入）</a>
独享模式	<ul style="list-style-type: none"><li>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。</li><li>防护对象：域名/IP</li></ul>	<a href="#">将网站接入WAF防护（独享模式）</a>

## 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 攻击防护规则拦截大流量高频攻击

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。

在大规模CC攻击中, 单台傀儡机发包的速率往往远超过正常用户的请求频率。针对这种场景, 直接对请求源IP设置限速规则是最有效的办法。

本文以如下配置为例, 介绍如何通过CC攻击防护规则基于IP限速拦截大流量高频攻击。

- 接入方式: 云模式-CNAME接入
- 防护对象: 域名
- 计费模式: 包年/包月
- 版本规格: 标准版
- 防护策略: CC攻击防护

## 操作流程

操作步骤	说明
<a href="#">准备工作</a>	注册华为账号、开通华为云, 并为账户充值、赋予WAF权限。
<a href="#">步骤一: 购买WAF</a>	购买WAF, 选择业务防护区域、WAF模式等信息。
<a href="#">步骤二: 将防护网站添加到WAF</a>	将防护网站添加到WAF防护, 实现WAF流量检测并转发。
<a href="#">步骤三: 配置CC攻击防护拦截大流量高频攻击</a>	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。 <ul style="list-style-type: none"><li>• Tenant Guest: 全局级角色，在全局项目中勾选。</li><li>• Server Administrator: 项目级角色，在同项目中勾选。</li></ul>
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 云模式标准版

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，参考[表2-2](#)配置，完成WAF实例的购买。

表 2-2 购买参数说明

参数	示例	说明
WAF模式	云模式	支持使用云模式-CNAME接入，可防护部署在华为云、非华为云上或云下的Web业务，防护对象为域名。
计费模式	包年/包月	预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。
区域	中国-香港	根据防护业务的所在区域就近选择购买的WAF区域。

参数	示例	说明
版本规格	标准版	可防护中小型网站。

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《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

1. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
2. 在网站列表左上角，单击“添加防护网站”。
3. 选择“云模式-CNAME接入”，并单击“开始配置”。
4. 在“添加防护网站”页面，完成如下必要参数配置，其余参数保持默认值即可。参数说明请参见表2-3。

图 2-1 添加域名

基础信息

防护域名 ①  
 [快速添加云内域名](#)  
请确保域名已经过ICP备案 (https://beian.xinnet.com)，WAF会检查域名备案情况，未备案域名将无法添加。

网站名称(可选)

网站备注(可选)

防护端口 ②  
 [查看可添加端口](#)  
标准端口为HTTP对外协议80和HTTPS对外协议443

服务器配置 ③

对外协议	源站协议	源站地址	源站端口	权重	操作	
HTTP	HTTP	IPv4	公网IP地址或者域名	80	1	删除

④ [添加地址](#) 您还可以添加59个源站地址

是否使用七层代理 ⑤  
 是  否

表 2-3 必要参数说明

参数	示例	说明
防护域名	www.example.com	需要添加到WAF进行防护的域名。
防护端口	标准端口	需要防护的域名对应的业务端口。 配置80/443端口，在下拉框中选择“标准端口”。



参数	示例	说明
服务器配置	<b>对外协议: HTTP</b> <b>源站协议: HTTP</b> <b>源站地址: IPv4</b> <b>XXX.XXX.1.1</b> <b>源站端口: 80</b>	<p>服务器地址的配置。包括对外协议、源站协议、源站地址、源站端口和权重。</p> <ul style="list-style-type: none"> <li>● 对外协议: 客户端请求访问服务器的协议类型。包括“HTTP”、“HTTPS”两种协议类型。</li> <li>● 源站协议: Web应用防火墙转发客户端请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。</li> <li>● 源站地址: 客户端访问的网站服务器的公网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）。支持以下两种IP格式: <ul style="list-style-type: none"> <li>- IPv4, 例如: XXX.XXX.1.1</li> <li>- IPv6, 例如: fe80:0000:0000:0000:0000:0000:0000:0000</li> </ul> </li> <li>● 源站端口: WAF转发客户端请求到服务器的业务端口。</li> <li>● 权重: 负载均衡算法将按权重将请求分配给源站。</li> </ul>
是否使用七层代理	否	<ul style="list-style-type: none"> <li>● 是: 使用了DDoS高防（七层代理）、CDN、云加速等Web代理产品。</li> <li>● 否: 没有使用七层代理。此处以“否”为例。</li> </ul>

5. 单击“下一步”，域名的基础信息配置完成。


图 2-2 基础信息配置完成



6. 根据界面提示，完成“放行回源IP”和“本地验证”。
7. 完成“DNS解析”。

到该域名的DNS服务商处，配置防护域名的别名解析，具体操作请咨询您的域名服务提供商。


以下为华为云DNS的CNAME绑定方法，仅供参考。如与实际配置不符，请以各自域名服务商的信息为准。


- a. 在图2-2中复制WAF提供的CNAME值。
- b. 单击页面左上方的 ，选择“网络 > 云解析服务 DNS”。
- c. 在左侧导航栏中，选择“公网域名”，进入“公网域名”页面。
- d. 在目标域名所在行的“操作”列，单击“管理解析”，进入“解析记录”页面。
- e. 在目标记录集的所在行“操作”列，单击“修改”。
- f. 在弹出的“修改记录集”对话框中修改记录值。
  - “主机记录”：在WAF中配置的域名。
  - “类型”：选择“CNAME-将域名指向另外一个域名”。
  - “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”：修改为7.a中已复制的WAF CNAME地址。
  - 其他的设置保持不变。
- g. 单击“确定”，完成DNS配置，等待DNS解析记录生效。

### 步骤三：配置 CC 攻击防护拦截大流量高频攻击

**配置示例：**您可以配置以下CC规则，当一个IP在30秒内访问当前域名下任意路径的次数超过1000次，则封禁该IP的请求10个小时。该规则可以作为一般中小型站点的预防性配置。

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，参考如图2-3所示进行配置。

示例中仅解释必要参数，其余大多数配置可保留默认值。必要参数说明请参见表2-4。

图 2-3 配置 CC 防护规则



添加CC防护规则

限速类型 <sup>1</sup>

IP限速  用户限速  其他

域名聚合统计 <sup>2</sup>

当开启时，如配置的泛域名为“\*.a.com”，会将所有子域名（b.a.com，c.a.com）的请求一起聚合统计。

限速条件

字段	子字段	逻辑	内容	操作
路径	-	前缀为	/login.php	删除

+ 添加条件 您还可以添加29项条件。（多个条件同时成立才生效） 添加引用表

限速频率 <sup>3</sup>

次  秒

全局计数 <sup>4</sup>

采取防护措施

防护动作 <sup>4</sup>

阻断  动态阻断  人机验证  仅记录  JS挑战

阻断时长 <sup>5</sup>

阻断页面

默认设置  自定义

生效模式 <sup>6</sup>

表 2-4 必要参数说明

参数	示例	参数说明
限速模式	“源限速 > IP限速”	<ul style="list-style-type: none"> <li>“源限速”：对源端限速，如某IP（或用户）的访问频率超过限速频率，就会对该IP（或用户）的访问限速。                             <ul style="list-style-type: none"> <li>“IP限速”：根据IP区分单个Web访问者。</li> <li>“用户限速”：根据Cookie键值或者Header区分单个Web访问者。</li> <li>“其他”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。</li> </ul> </li> </ul> <p><b>说明</b> 选择“其他”时，“Referer”对应的“内容”填写为包含域名的完整URL链接，仅支持前缀匹配和精准匹配的逻辑，“内容”里不能含有连续的多条斜线的配置，如“///admin”，WAF引擎会将“///”转为“/”。</p> <p>例如：如果用户不希望访问者从“www.test.com”访问网站，则“Referer”对应的“内容”设置为“http://www.test.com”。</p> <ul style="list-style-type: none"> <li>“目的限速”：选择该参数时，可选择以下限速类型进行配置：                             <ul style="list-style-type: none"> <li>“策略限速”：当多个域名共用一个策略时，该策略下对应的所有域名请求次数合并限速(不区分访问IP)；泛域名防护场景时，该泛域名对应的所有子域名的请求次数合并限速(不区分访问IP)。</li> <li>“域名限速”：每个域名单独统计总请求次数，超过设定值则触发防护动作(不区分访问IP)。</li> <li>“URL限速”：每个URL请求单独统计请求次数，超过设定值则触发防护动作(不区分访问IP)。</li> </ul> </li> </ul>

参数	示例	参数说明
限速条件	<ul style="list-style-type: none"> <li>“字段”：路径</li> <li>“逻辑”：前缀为</li> <li>“内容”：/login.php</li> </ul>	<p>单击“添加条件”增加新的条件，至少配置一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。</p> <ul style="list-style-type: none"> <li>字段</li> <li>子字段：当“字段”选择IPv4、IPv6、Cookie、Header、Params时，请根据实际需求配置子字段。</li> </ul> <p><b>须知</b> 子字段的长度不能超过2048字节。</p> <ul style="list-style-type: none"> <li>逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。</li> <li>内容：输入或者选择条件匹配的内容。</li> </ul>
限速频率	<b>1,000次30秒全局计数</b>	<p>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，Web应用防火墙服务将根据配置的“防护动作”来处理。</p> <p>“全局计数”：根据不同的限速模式，将已经标识的请求在一个或多个WAF节点上的计数聚合。默认为每WAF节点单独计数，开启后本区域所有节点合并计数。“IP限速”不能满足针对某个用户进行限速，需要选择“用户限速”或“其他”的Referer限速，此时标识的请求可能会访问到不同的WAF节点，开启全局计数后，将请求访问的一个或多个WAF节点访问量聚合，达到全局统计的目的。</p>

参数	示例	参数说明
防护动作	阻断	<p>当访问的请求频率超过“限速频率”时，可设置以下防护动作：</p> <ul style="list-style-type: none"><li>● 人机验证：表示超过“限速频率”后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。人机验证目前支持英文。</li><li>● 阻断：表示超过“限速频率”将直接阻断。</li><li>● 动态阻断：上一个限速周期内，请求频率超过“限速频率”将被阻断，那么在下一个限速周期内，请求频率超过“放行频率”将被阻断。</li><li>● 仅记录：表示超过“限速频率”将只记录不阻断。</li><li>● JS挑战：表示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。</li></ul> <p><b>说明</b> 请求的Referer跟当前的Host不一致时，JS挑战不生效。</p>
阻断时长	36,000秒	当“防护动作”选择“阻断”时，可设置阻断后恢复正常访问页面的时间。

5. 确认参数配置无误后，单击“确定”。

## 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](#)。
- 如果您的业务部署在华为云上，规模为大型企业网站，且对业务稳定性有较高的安全防护需求，需要防护对象为域名/IP，您可以采用“云模式-ELB接入”的接入方式，具体操作可参考如下方法：
  - a. [购买WAF云模式标准版](#)。  
购买实例后，[提交工单](#)申请开通“云模式-ELB接入”。
  - b. [将网站接入WAF防护（云模式-ELB接入）](#)。
  - c. [配置CC攻击防护拦截大流量高频攻击](#)。
- 如果您的业务部署在华为云上，规模为大型企业网站，且基于业务特性具有制定个性化防护规则的安全需求，需要防护对象为域名/IP，您可以采用“独享模式”的接入方式，具体操作可参考如下方法：
  - a. 独享模式在部分区域已经停售，详见[独享模式停售通知](#)。如果您已购买独享模式的WAF，可跳过该步骤继续使用。
  - b. [将网站接入WAF防护（独享模式）](#)。

- c. [配置CC攻击防护拦截大流量高频攻击。](#)

# 3 通过黑白名单设置拦截网站恶意 IP 流量

WAF默认放行所有的IP地址，如果您发现您的网站存在恶意IP访问，可通过WAF的黑白名单设置规则拦截恶意IP。

本场景以WAF云模式-ELB接入方式为例，介绍如何通过黑白名单设置规则拦截恶意IP流量。

- 接入方式：云模式-ELB接入
- 防护对象：域名/IP
- 计费模式：包年/包月
- 版本规格：标准版
- 防护策略：黑白名单设置

## 操作流程

操作步骤	说明
<a href="#">准备工作</a>	注册华为账号、开通华为云，并为账户充值、赋予WAF权限。
<a href="#">步骤一：购买WAF云模式标准版</a>	购买WAF，选择业务防护区域、WAF模式等信息。
<a href="#">步骤二：将防护网站通过ELB接入方式添加到WAF</a>	将防护网站添加到WAF防护，实现WAF流量检测。
<a href="#">步骤三：配置黑白名单设置规则拦截恶意IP</a>	通过黑白名单设置规则拦截恶意IP。

## 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。 <ul style="list-style-type: none"><li>• Tenant Guest: 全局级角色, 在全局项目中勾选。</li><li>• Server Administrator: 项目级角色, 在同项目中勾选。</li></ul>
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 云模式标准版

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。本节以购买WAF云模式标准版本为例进行介绍。

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，参考如下配置，完成WAF实例的购买。

表 3-2 购买参数说明

参数	示例	说明
WAF模式	云模式	购买WAF后，可 <a href="#">提交工单</a> ，开通云模式-ELB接入，可防护部署在华为云上的Web业务，防护对象为域名/IP。
计费模式	包年/包月	预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。
区域	中国-香港	根据防护业务的所在区域就近选择购买的WAF区域。

参数	示例	说明
版本规格	标准版	可防护中小型网站。

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《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。

#### 说明

购买完成后，[提交工单](#)申请开通云模式的ELB接入。

## 步骤二：将防护网站通过 ELB 接入方式添加到 WAF

### 步骤1 创建独享型负载均衡器。

- “规格”选择“应用型（HTTP/HTTPS）”
- 其他参数根据业务需要进行配置。

### 步骤2 为步骤1中创建的负载均衡添加监听器，详细操作请参见[添加HTTP监听器](#)或[添加HTTPS监听器](#)。

### 步骤3 创建后端服务器组。

- “所属负载均衡器”：选择“关联已有”，并在下拉框中选择步骤1中创建的负载均衡器。
- 后端服务器配置为步骤8中需要添加到WAF中的网站对应的服务器地址。

### 步骤4 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

### 步骤5 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

### 步骤6 在网站列表左上角，单击“添加防护网站”。

### 步骤7 选择“云模式-ELB接入”，并单击“开始配置”。

### 步骤8 在“添加防护网站”页面，配置信息如[图3-1](#)所示。

- ELB（负载均衡器）：选择的ELB，需要确认防护网站对应的服务器地址已添加到该ELB。
- ELB监听器：“所有监听器”。
- 防护域名：需要通过WAF防护的域名或IP，此处以“www.example.com”为例。
- 策略配置：系统自动生成策略。

图 3-1 域名配置信息

The screenshot shows a configuration form with the following fields and options:

- \* ELB (负载均衡器)**: A dropdown menu with the value "waf-xyf-elb" and a search icon.
- \* ELB监听器**: Two buttons, "所有监听器" (All Listeners) in blue and "指定监听器" (Specify Listener) in grey.
- 网站名称**: A text input field with the placeholder text "您可以为域名自定义名称".
- \* 防护域名**: A text input field with the value "www.example.com".
- 网站备注**: An empty text input field.
- \* 策略配置**: A dropdown menu with the value "系统自动生成策略" and a help icon.

步骤9 单击“确定”。

----结束

### 步骤三：配置黑白名单设置规则拦截恶意 IP

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“黑白名单设置”配置框，开启黑白名单设置策略。

-  : 开启状态。
-  : 关闭状态。

步骤4 在“黑白名单设置”规则配置列表上方，单击“添加规则”，按照如图3-2所示进行配置。

- **IP/IP段或地址组**：IP/IP段。如果您需要拦截多个IP，可选择“地址组”。
- **IP/IP段**：根据实际情况配置需要拦截的IP或IP段，示例：192.168.2.1。
- **防护动作**：拦截。

图 3-2 拦截指定 IP

添加黑白名单设置规则

\* 规则名称

\* IP/IP段或地址组  IP/IP段  地址组

\* IP/IP段

\* 防护动作

攻击惩罚  [添加攻击惩罚](#)

\* 生效模式  立即生效  自定义

规则描述

步骤5 单击“确定”，完成配置。

----结束

## 相关信息

- 关于黑白名单设置更多详细的操作，请参见[配置IP黑白名单规则拦截/放行指定IP](#)。
- 如果您的业务部署在华为云、非华为云上或云下，需要防护对象为域名，您可以需要采用“云模式-CNAME接入”的接入方式，具体操作可参考如下方法：
  - a. [购买WAF云模式标准版](#)。
  - b. [将网站接入WAF防护（云模式-CNAME接入）](#)。
  - c. [步骤三：配置黑白名单设置规则拦截恶意IP](#)。
- 如果您的业务部署在华为云上，规模为大型企业网站，且基于业务特性具有制定个性化防护规则的安全需求，需要防护对象为域名/IP，您可以采用“独享模式”的接入方式，具体操作可参考如下方法：
  - a. 独享模式在部分区域已经停售，详见[独享模式停售通知](#)。如果您已购买独享模式的WAF，可跳过该步骤继续使用。
  - b. [将网站接入WAF防护（独享模式）](#)。
  - c. [步骤三：配置黑白名单设置规则拦截恶意IP](#)。

# 4 入门实践

当您防护网站接入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	<p><b>未使用代理的网站通过CNAME方式接入WAF</b></p> <p>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。</p>
	<p><b>使用DDoS高防和WAF提升网站全面防护能力</b></p> <p>“DDoS高防+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，同时防御DDoS攻击和Web应用攻击，确保业务持续可靠运行。</p> <ul style="list-style-type: none"><li>• 防御DDoS攻击：NTP Flood攻击、SYN Flood攻击、ACK Flood攻击、ICMP Flood攻击、HTTP Get Flood攻击等。</li><li>• 防御Web应用攻击：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。</li></ul>
	<p><b>使用CDN和WAF提升网站防护能力和访问速度</b></p> <p>“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</p>
	<p><b>使用独享WAF和7层ELB以防护任意非标端口</b></p> <p>如果您需要防护<b>WAF支持的端口</b>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。</p>

实践	描述
	<p><b>使用WAF、ELB和NAT网关防护云下业务</b></p> <p>WAF云模式-ELB接入默认只支持云上业务，当您的源站服务器在云下时，需要通过NAT网关进行流量转发，将您的流量由华为云内网回源到源站的公网IP，再通过云模式-ELB接入方式将网站接入WAF，实现流量检测。</p>
策略配置	<p><b>网站防护配置建议</b></p> <p>从不同场景、角色的视角介绍Web应用防火墙（Web Application Firewall，简称WAF）的防护规则，帮助您从自己最关心的需求入手，了解WAF的防护逻辑。</p>
	<p><b>使用WAF防护CC攻击</b></p> <p>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。</p>
	<p><b>使用WAF阻止爬虫攻击</b></p> <p>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。</p>
	<p><b>使用Postman工具模拟业务验证全局白名单规则</b></p> <p>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。</p>
	<p><b>通过WAF和HSS提升网页防篡改能力</b></p> <p>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。</p>
LTS日志分析	<p><b>通过LTS查询并分析WAF访问日志</b></p> <p>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<b>云日志服务</b>（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。</p>
	<p><b>通过LTS分析Spring core RCE漏洞的拦截情况</b></p> <p>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。</p>
	<p><b>通过LTS配置WAF规则的拦截告警</b></p> <p>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中的防护情况并做出决策分析。</p>
TLS加密配置	<p><b>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</b></p> <p>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<b>域名接入WAF</b>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。</p>

实践		描述
源站安全 保护实践	<a href="#">通过WAF提升客户端访问域名的通道安全</a>	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”时，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。
	<a href="#">通过ECS/ELB访问控制策略保护源站安全</a>	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： <ul style="list-style-type: none"> <li>• 如何判断源站是否存在泄漏风险？</li> <li>• 如何配置访问控制策略保护源站安全？</li> </ul>
获取客户端真实IP	<a href="#">获取客户端真实IP</a>	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。
通过CES配置WAF指标异常告警	<a href="#">通过CES配置WAF指标异常告警</a>	介绍如何在华为云云监控服务（CES）对WAF指标配置异常告警，当Web应用防火墙（WAF）的监控指标出现异常情况，及时了解WAF防护状况，从而起到预警作用。