Web 应用防火墙（原生版）

用户使用指南

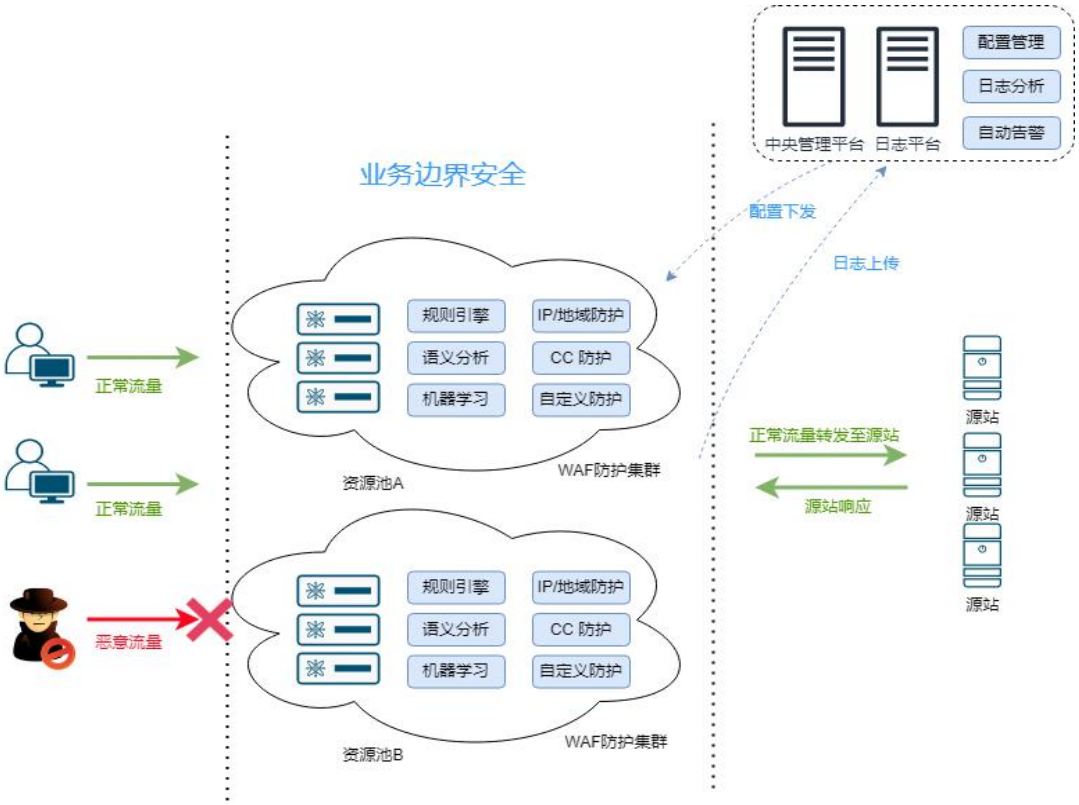
天翼云科技有限公司

目 录

1. 产品简介

1.1. 产品定义

Web 应用防火墙（原生版）（CT-WAF，Web Application Firewall，简称云 WAF）为用户 Web 应用提供一站式安全防护，对 Web 业务流量进行智能全方位检测，有效识别恶意请求特征并防御，避免源站服务器被恶意入侵，保护网站核心业务安全和数据安全。



Web 应用防火墙（原生版）产品整体架构主要包括 3 个部分，分别为 WAF 防护集群、中央管理平台、日志平台。

- **WAF 防护集群**：依托规则引擎实现流量过滤，并通过管控 Agent 与管理平台通信，接收防护策略的下发，上报执行节点运行状态。
- **中央管理平台**：提供多维策略规则的编辑和下发能力，并监控执行节点运行状态。

- **日志平台**：存放访问日志及防护日志，并提供自动告警能力。

1.2. 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，产品优势如下：

- **先进的检测技术**

集成机器学习检测引擎，支持专家经验特征与语义特征，有效检测 SQL 注入、XSS 等基于形式语言的攻击类型，准确率与召回率可以达到 99.9%。

- **高质量的规则集**

持续优化的高质量攻击检测规则集，兼顾性能与效果且配置简单，对 OWASP 常见攻击类型进行了良好覆盖。

- **精细化的策略配置**

支持自定义防护规则，基于会话特征灵活配置攻击识别、对抗策略，精准拦截，降低误报。

- **稳定可靠**

营商级云资源池架构，可支持高并发业务接入防护；采用集群+冗余高可用模式，消除单点故障。

- **等保合规**

满足等保测评要求，助力企业安全合规建设。

1.3. 功能特性

通过 Web 应用防火墙（原生版）服务，可以轻松应对各种 Web 安全风险。功能特性如下：

- **HTTP/HTTPS 业务防护**

支持防护 HTTP/HTTPS 业务，通过对 HTTP/HTTPS 请求进行检测，识别并阻断恶意攻击，保护 Web 服务安全稳定。

- **Ipv4/Ipv6 防护**

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。

- **Web 基础防护**

覆盖 OWASP 常见安全威胁，支持 SQL 注入、XSS、文件包含、远程命令执行、目录穿越、文件上传、CSRF、SSRF、命令注入、模板注入、XML 实体注入等攻击检测和拦截。

- **CC 攻击防护**

支持默认防护策略及灵活的自定义防护策略。自定义策略支持依托精准访问控制规则进行特征识别，并根据访问源 IP/ SESSION 控制访问频率，恶意流量通过阻断、人机验证等处置手段有效缓解 CC 攻击。

- **BOT 防护**

提供公开类型、协议特征、自定义会话特征等多种判定维度的防护策略，支持根据 BOT 会话行为特征设置 BOT 对抗策略，对 BOT 行为进行处理，有效防护搜索引擎、扫描器、脚本工具等爬虫攻击。

- **精准访问控制**

支持基于 IP、URL、Referer、User-Agent 等请求特征进行多维度组合，定义访问匹配条件过滤访问请求，实现针对性的攻击阻断。

- **IP 黑白名单**

支持添加始终拦截与始终放行的黑白名单 IP/IP 地址段，增强防御准确性。

- **地域访问控制**

支持针对地理位置的黑名单封禁，可指定需要封禁的国家、地区，阻断该区域的来源 IP 的访问。

- **告警通知**

支持基于攻击防护事件设置告警通知策略，通过对选定攻击类型范围的事件设置告警阈值，当大于阈值时发送通知给用户群组。

- **安全概览**

提供统一可视化界面展示网页业务的整体安全状态，包括防护统计数据、网站流量分析数据等。

- **攻击事件报表**

支持通过控制台界面，实时查看攻击信息和事件详情。

1.4. 相关术语解释

- **SSL 证书**：指一种安全协议，目的是为互联网通信提供安全及数据完整性保障。SSL 证书遵循 SSL 协议，可安装在服务器上，实现数据传输加密。
- **域名解析**：互联网上的机器相互间通过 IP 地址来建立通信，但是人们大多数习惯记忆域名，将 IP 地址与域名之间建立一对多的关系，而它们之间转换工作的过程称为域名解析。
- **QPS**：每秒查询率（Query Per Second QPS） 是对一个特定的查询服务器，在规定时间内所处理流量多少的衡量标准，在因特网上，作为域名系统服务器的机器性能经常用每秒查询率来衡量，对应 fetches/sec（每秒响应请求数，即是最大吞吐能力）。
- **回源 IP 地址**：回源 IP 指云 WAF 用来与源站服务器建立网络连接的 IP 地址。客户添加域名成功后，由 WAF 自动分配多个回源 IP 地址，WAF 使用特定的回源 IP 段将经过防护引擎检测后的正常流量转发到网站域名的源站服务器。
- **CC 攻击**：攻击者借助代理服务器生成指向受害主机的合法请求，实现 DDOS 和伪装称为 CC(Challenge Collapsar)。攻击将导致被攻击服务器资源耗尽，一直到宕机崩溃，无法正常对外提供服务。
- **爬虫攻击**：攻击者利用通过自动化的机器人程序批量获取源站页面数据或者利用业务逻辑缺陷获得非法业务收益，当爬虫抓取数据量逐渐增大时，会对被访问的服务器造成很大的压力。

1.5. 应用场景

场景一：Web 应用基础安全防护

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。

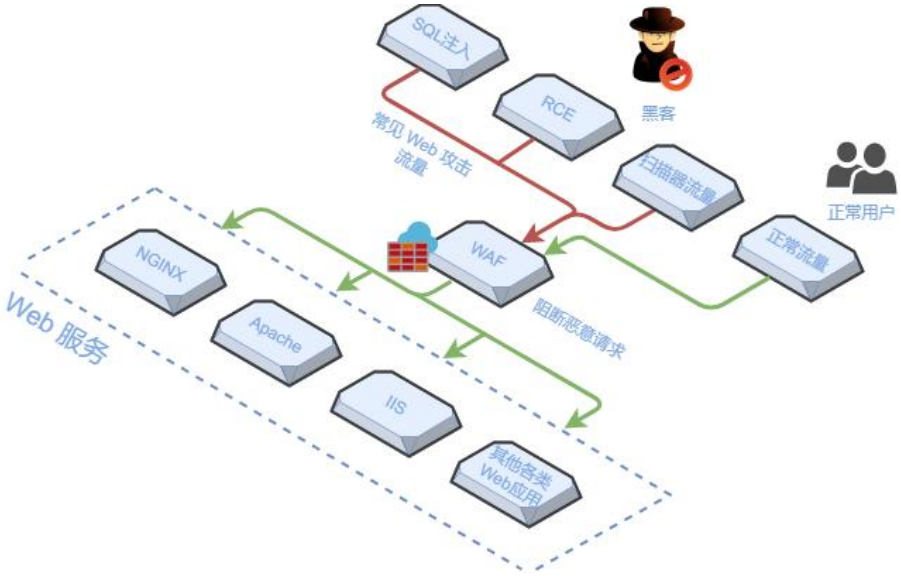
方案优势

- 精准识别恶意流量，全面防护 SQL 注入、XSS、Webshell 上传、目录遍历、后门隔离等各类常见 Web 攻击。
- 根据会话特征有效识别恶意爬虫，防止数据泄露。

目标用户

- 支撑互联网 + 企业 Web 服务、电商 O2O 站点、金融政务网站

场景示意图



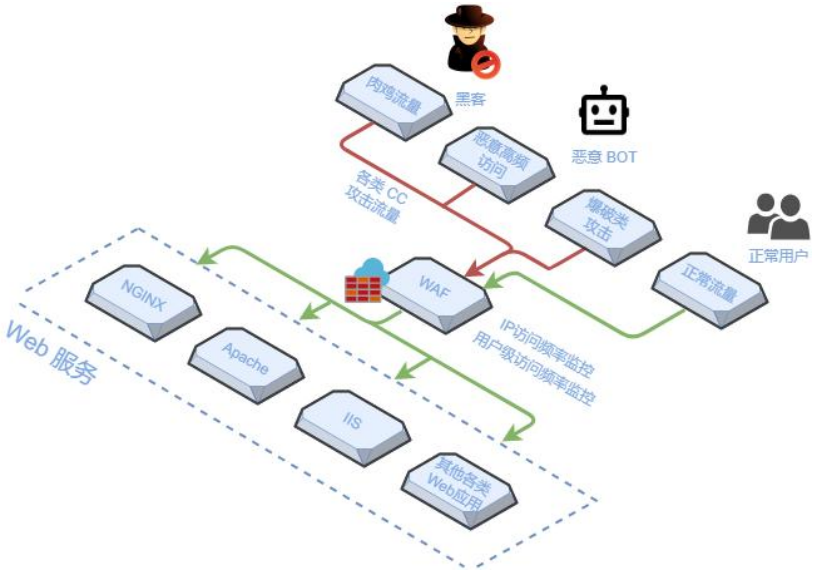
场景二：CC 攻击防护

网站被发起大量的恶意 CC 请求，长时间占用核心资源，导致网站业务响应缓慢或无法正常提供服务。

方案优势

- 可根据 IP 或者会话 Session 设置灵活的限速策略，精准识别 CC 攻击，保障业务稳定运行。
- 用户可根据业务需要，自主控制访问频率，并配置期望的处置动作，满足业务定制化需要。

场景示意图



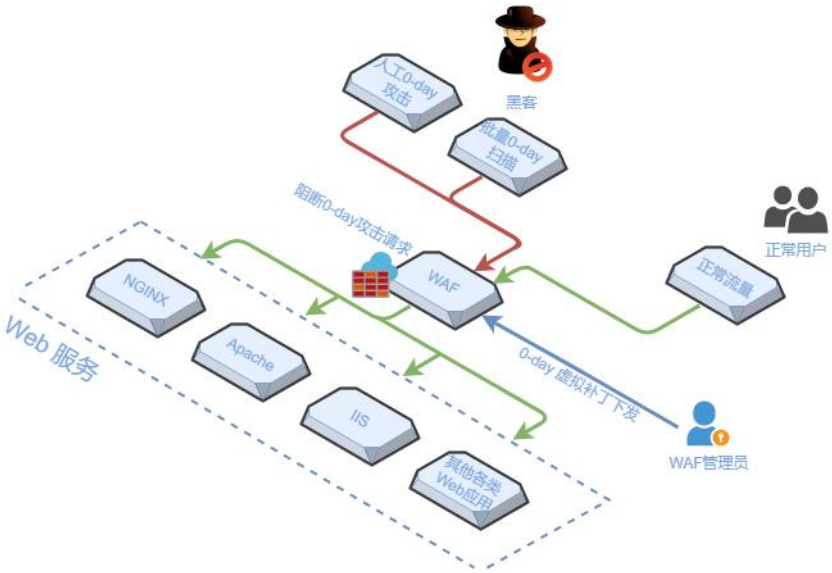
场景三：0Day 漏洞修复

第三方框架或插件爆发 0Day 漏洞时，需要通过下发虚拟补丁，第一时间防护由漏洞引发的攻击

方案优势

- 主动发现并响应，及时下发虚拟补丁，更新防御规则，实现漏洞防护。
- 用户无需任何操作即可获取紧急漏洞防御能力，降低维护成本。

场景示意图



1.6. 产品规格

Web 应用防火墙（原生版）根据支持防护的业务规模以及提供的防护功能不同，产品实例主套餐具体分为基础版、标准版、企业版、旗舰版四个版本。各版本详细规格描述见下方表 1 所示。

另外，标准版、企业版、旗舰版主套餐支持选择购买资源扩展包，用户可以通过升级实例版本或购买额外的资源扩展包，以满足更多域名、更大流量的防护需求。

资源扩展包规格说明

- **域名扩展包**：1 个域名扩展包支持 10 个域名，其中支持添加 1 个一级域名。
- **业务扩展包**：1 个业务扩展包包含 1000QPS，最多支持 30 个业务扩展包。
- **规则扩展包**：1 个规则扩展包包含 50 条防护规则/域名，当前仅适用 IP 黑白名单防护模块。

资源限制规则说明

- **域名个数统计**：套餐内的域名个数为一级域名和与其相关的子域名/泛域名的总数。例如，基础版支持防护 10 个域名，则可以添加 10 个子域名或泛域名，也可以添加 1 个一级域名和 9 个与其相关的子域名或泛域名。同时套餐内有一级域名的限制，以基础版仅支持 1 个一级域名为例，若用户已经添加 example.com 或其子域名进行防护，当添加 test.com（另一个主域名）或其子域名进行防护时，则会提示数量限制，用户需要购买域名扩展包，才能添加其他的主域名或其子域名。
- **业务 QPS 峰值统计**：业务 QPS 峰值指云 WAF 实例支持处理的网站正常业务流量的峰值大小。云 WAF 实例的业务 QPS 峰值=产品主套餐规格默认支持的业务 QPS+业务扩展包扩展的 QPS。

  如果用户将多个网站业务接入云 WAF 实例进行保护，则必须保证所有网站业务的正常 QPS 峰值之和不超出 WAF 实例的业务 QPS 峰值。超出 WAF 实例的业务 QPS 峰值限制，云 WAF 会触发限流、随机丢包等动作，导致用户的网站业务在一定时间内出现卡顿、延迟，甚至不可用等，云 WAF 的 SLA 无法得到保障。

版本规格说明

分类	功能点	基础版	标准版	企业版	旗舰版
套餐基础信息	适用场景	适合个人网站用户	适用于中小型网站的标准防护	适用中大型网站防护	适用于大型及超大型复杂业务网站防护
	业务 QPS 峰值	100QPS/实例	3000QPS/实例	5000QPS/实例	10000QPS/实例
	支持一级域名个数	1 个/实例	2 个/实例	5 个/实例	8 个/实例

分类	功能点	基础版	标准版	企业版	旗舰版
	支持所有防护域名个数	10 个/实例	20 个/实例	50 个/实例	80 个/实例
	泛域名防护	×	√	√	√
	IPv6 防护	×	×	√	√
	HTTP/HTTPS 非标准端口防护	不支持 仅支持 80、443	√	√	√
	支持防护端口数量	2 个/实例	20 个/实例	30 个/实例	60 个/实例
	域名接入方式	CNAME	CNAME	CNAME	CNAME
基础安全防护	规则白名单	×	√，20 条/域名	√，50 条/域名	√，100 条/域名
	Web 基础规则防护引擎	√，仅支持默认规则组的防护	√，支持自定义	√，支持自定义	√，支持自定义
	自定义防护规则组个数	×	10 个/实例	20 个/实例	30 个/实例
	0Day 漏洞虚拟补丁	√	√	√	√
	IP 黑白名单	×	200 条/实例	500 条/实例	1000 条/实例
	地域封禁	×	×	√，50 条/实例	√，100 条/实例
	自定义精准防护策略	×	√，100 条/实例	√，200 条/实例	√，500 条/实例
	CC 防护（包括紧急模式）	×	√	√	√
	自定义 CC 防护规则	×	100 条/实例	200 条/实例	500 条/实例
高级安全防护	公开 BOT 类	×	√	√	√

分类	功能点	基础版	标准版	企业版	旗舰版
	型防护				
	BOT 协议特征防护	×	√	√	√
	BOT 自定义会话特征防护	×	√，100 条/实例	√，200 条/实例	√，500 条/实例
	数据统计分析	√	√	√	√
	敏感信息保护	×	×	√，50 个/实例	√，50 个/实例
	网页防篡改	×	√，20 条/域名	√，50 条/域名	√，100 条/域名
	Cookie 防篡改	×	×	√，50 个/实例	√，50 个/实例
	隐私屏蔽	×	√，20 条/域名	√，50 条/域名	√，100 条/域名

2. 计费说明

2.1. 计费模式

Web 应用防火墙（原生版）支持包年包月付费模式。

标准资费

Web 应用防火墙（原生版）根据开通实例时选购的主套餐版本、资源扩展包个数、购买时长生成预付费账单。

计费项		基础版	标准版	企业版	旗舰版
主套餐		99 元/月	3880 元/月	9800 元/月	29800 元/月
资源扩展包	域名扩展包	-	600 元/个/月	1000 元/个/月	2000 元/个/月
	业务扩展包	-	1000 元/个/月	2000 元/个/月	2000 元/个/月
	规则扩展包	-	70 元/个/月	70 元/个/月	70 元/个/月

关于不同主套餐版本的规格参数，请参见产品规格。

针对一次性包年付费，标准价格如下：

一次性付费 1 年	一次性付费 2 年	一次性付费 3 年
包月标准价格×12×85%	包月标准价格×24×70%	包月标准价格×36×50%

须知：
1、一个账号支持购买一个包周期实例，实例必须绑定一个主套餐版本，可叠加购买资源扩展包；
2、基础版最多支持一次性付费 1 年，不支持一次性付费 2 年、3 年。

资源扩展包规格说明

- **域名扩展包**：1 个域名扩展包支持 10 个域名，其中支持添加 1 个一级域名。

- **业务扩展包**：一个业务扩展包包含 1000QPS/个，最多支持 30 个业务扩展包。
- **规则扩展包**：一个规则扩展包包含 50 条防护规则/域名，当前仅适用 IP 黑白名单防护模块。

须知：

1、基础版不支持购买资源扩展包，可升级到标准版或更高版本才能购买；

2、资源扩展包不支持独立购买，必须在购买主套餐的基础上进行叠加购买；

3、资源扩展包购买后与主套餐绑定，资源到期时间与主套餐一致，不支持单独退订或单独续订。

2.2. 购买云 WAF 实例

Web 应用防火墙（原生版）支持包年/包月计费方式，同时提供四个主套餐版本：基础版、标准版、企业版、旗舰版，三种资源扩展包：域名扩展包、带宽扩展包、规则扩展包。您可以根据业务规模选择云 WAF 规格。

前提条件

- 已经注册天翼云账号。

规格限制

- 基础版不支持购买资源扩展包，可升级到标准版或更高版本才能购买；
- 1 个域名扩展包支持 10 个域名，其中支持添加 1 个一级域名；
- 一个业务扩展包包含：1000QPS/个，最多支持 30 个业务扩展包。
- 一个规则扩展包包含 50 条防护规则/域名，当前仅适用 IP 黑白名单防护模块。

约束条件

- 云 WAF 实例生效期间，支持升级购买的服务版本以及扩增资源扩展包数量，但不支持降级。
- 开通云 WAF 实例，必须购买主套餐，可以在主套餐基础上叠加购买资源扩展包，扩展包与主套餐绑定，到期时间与主套餐一致，不支持单独续订、退订。

适用场景

用户 Web 业务服务器部署在天翼云上、非天翼云或线下，防护对象为域名。

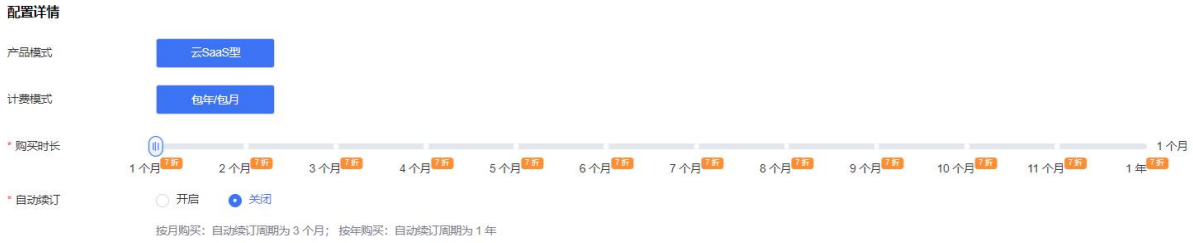
各服务版本推荐适用的场景说明如下：

服务版本	适用场景说明
基础版	适用个人网站防护。
标准版	适用中小型网站，对业务没有特殊的安全需求。
企业版	适用中型企业级网站或服务对互联网公众开放的网站，关注数据安全且具有高标准的安全需求。
旗舰版	适用中大型企业网站，具备较大的业务规模，或是具有特殊定制的安全需求。

操作步骤

1. 登录天翼云控制中心。
2. 在天翼云控制台左上方选择地域。
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”。
4. 在“欢迎使用 Web 应用防火墙”页面，点击“立即购买”。

5. 进入产品订购页面，选择“购买时长”，拖动时间轴设置购买时长。



须知：

1. 支持勾选 “自动续费”，当服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费；
2. 基础版最多支持一次性付费 1 年，不支持一次性付费 2 年、3 年。

6. 选择“主套餐版本”。

须知：

1. 一个账号支持购买一个包周期实例，实例必须绑定一个主套餐版本。
2. 关于产品规格信息对比，详见产品规格。

7. 选择标准版、企业版、旗舰版时，支持叠加购买“域名扩展包”、“业务扩展包”、“规则扩展包”，可以设置购买数量。

8. 确认参数配置无误后，阅读《天翼云 Web 应用防火墙（原生版）服务协议》，并勾选“我已阅读，理解并接受《天翼云 Web 应用防火墙（原生版）服务协议》“，点击“立即购买”。

2.3. 升级扩容

开通了云 WAF 实例后，支持从较低版本的主套餐升级至任一更高版本，可支持根据实际使用需求购买域名扩展包、业务扩展包和规则扩展包。

前提条件

- 已开通 Web 应用防火墙（原生版）实例。

规格限制

- 基础版不支持购买资源扩展包，可升级到标准版或更高版本才能购买。
- 1 个域名扩展包支持 10 个域名，其中支持添加 1 个一级域名。
- 一个业务扩展包包含：1000QPS/个，最多支持 30 个业务扩展包。
- 一个规则扩展包包含 50 条防护规则/域名，当前仅适用 IP 黑白名单防护模块；

约束条件

- 已到期的服务版本，不支持直接升级，需先完成续费再升级；
- 主套餐版本升级后，已购买的资源扩展包也将同步升级至对应的版本；
- 对实例进行升级扩容时，资源到期时间不变；
- 资源扩展包不支持独立购买，必须在购买主套餐的基础上进行叠加购买；

- 资源扩展包购买后与主套餐绑定，资源到期时间与主套餐一致，不支持单独退订或单独续订。

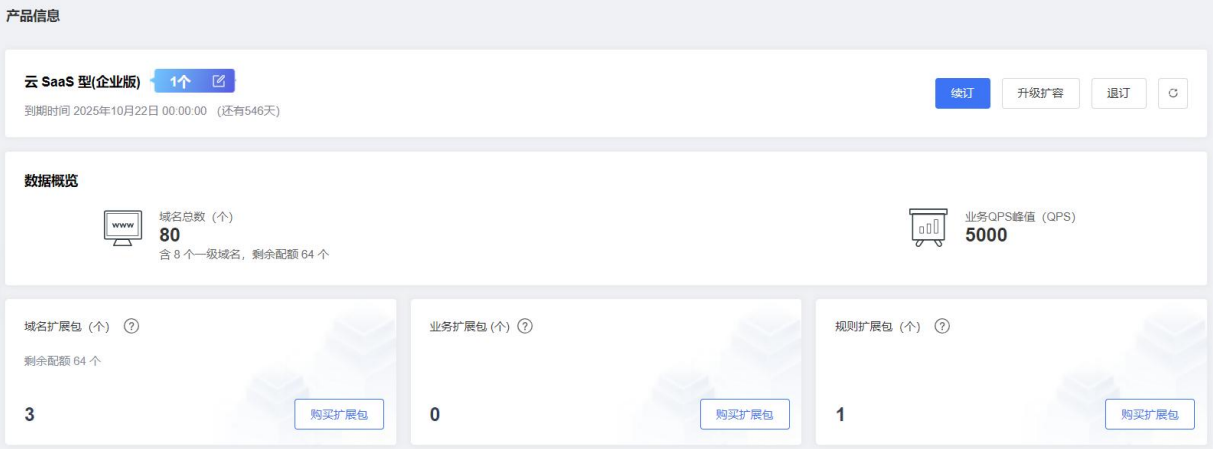
系统影响

升级服务版本和购买资源扩展包时，原已启用的防护服务不会暂停，对已防护的网站业务无任何影响。

升级实例规格

升级实例规格支持主套餐版本升级，以及当前已开通资源扩展包的数量扩增。

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择地域。
3. 在控制台列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“产品信息”。
5. 产品信息页显示当前已生效的实例版本以及相关规格使用情况。



6. 点击“升级扩容”，在页面下方“升级扩容”区域进行升级扩容配置。
7. 升级规格版本：“规格选择”默认为当前实例版本，可以对当前实例版本进行升级。

8. 升级资源扩展包：若当前实例已购买某类资源扩展包，可在实例规格升级界面，通过扩增资源扩展包数量，数量设置需高于当前已购买数量。

9. 升级规格设置完成后，在页面下方确认支付费用，阅读《天翼云 Web 应用防火墙（原生版）服务协议》，并勾选“我已阅读，理解并接受《天翼云 Web 应用防火墙（原生版）服务协议》“，点击“立即下单”。
10. 在订单页完成订单确认并支付，付费成功后，购买的版本和扩展包规格将生效。

新增购买资源扩展包

若当前实例还未购买某类资源扩展包，则需单独购买。

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择地域。
3. 在控制台列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“产品信息”。
5. 在当前实例信息展示界面，点击“购买 XX 扩展包”。

6. 设置资源扩展包数量。

   下图以“域名扩展包”为例。

7. 在页面下方确认支付费用，并阅读《天翼云 Web 应用防火墙（原生版）服务协议》，勾选“我已阅读，理解并接受《天翼云 Web 应用防火墙（原生版）服务协议》“，点击“立即下单”。

8. 在订单页完成订单确认并支付，付费成功后，购买资源扩展包规格生效。

2.4. 续订

为避免 Web 应用防火墙（原生版）实例到期后，防护服务自动停止，需要在实例到期前为实例手动续费，或设置到期自动续费。

到期说明

服务即将到期前，系统会以短信或邮件的形式提醒服务即将到期，并提醒用户续费。

服务到期后，如果没有按时续费，平台会冻结服务，但用户配置信息会提供 15 天的保留期。

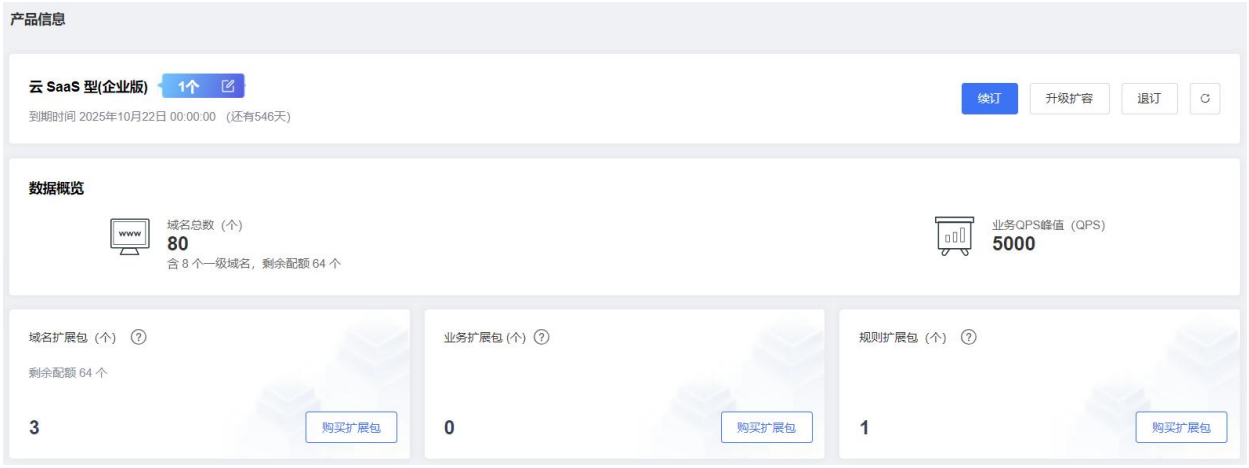
- 保留期内，平台会冻结 WAF 服务，用户配置的各类防护策略将不再生效，云 WAF 只转发流量。
- 保留期满，用户若仍未续费，平台会清除实例资源，用户所添加域名的所有配置将会被删除，同时云 WAF 将不再转发业务流量，若用户未及时将 DNS 指回服务器源站 IP，否则网站业务流量将无法正常转发。

续订说明

- 在购买云 WAF 时，支持勾选并同意“自动续订”，则在服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费；
- 若购买云 WAF 时勾选了“自动续订”，系统将会默认设置续费周期：按月购买，自动续费周期默认为 3 个月；按年购买，自动续费周期默认为 1 年。如需要修改自动续费周期，可进入天翼云“管理中心”，进入“产品中心>产品续订”页面，在资源页面找到待修改自动续订的资源，单击操作列的“修改自动续订”，拖动“续订周期”可修改自动续订周期，当自动续订周期达 1 年或以上时，将可享受包年折扣。

手动续订

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择地域。
3. 在控制台列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“产品信息”。



5. 在当前实例信息展示界面，点击“续订”。

6. 在“续订”操作界面，根据使用需要调整续订周期后，提交续订订单。

自动续费

方法一：云 WAF 支持在购买实例时，同步开通“自动续订”。详细操作请参见购买云 WAF 实例。

方法二：若开通实例时未开启自动续订，用户也可在开通后，通过天翼云“费用中心 > 订单管理 > 续订管理”页面，开通自动续订。详细操作请参见开通自动续订。

2.5. 退订

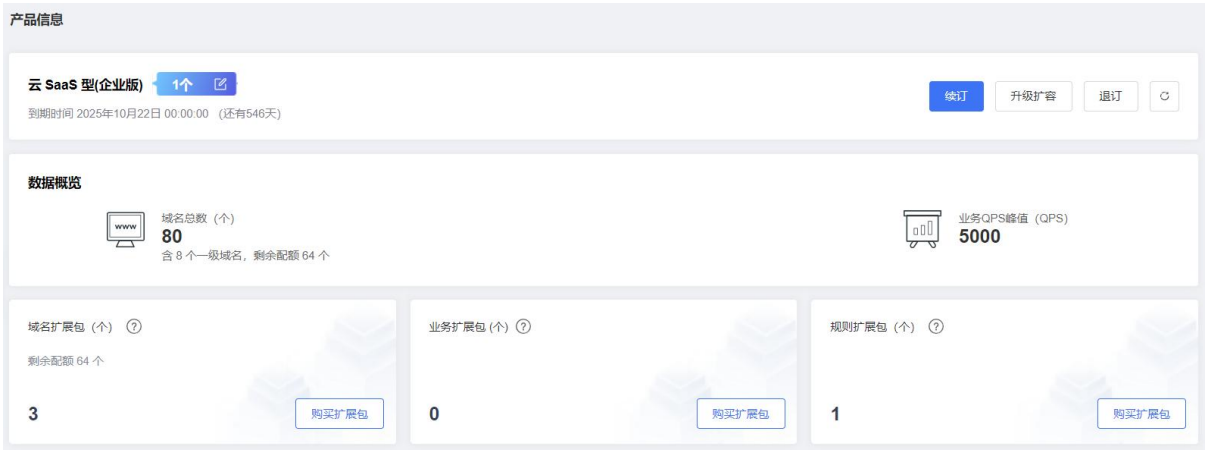
Web 应用防火墙（原生版）支持退订，可通过 Web 应用防火墙（原生版）控制台界面、天翼云管理中心发起并完成退订操作。

退订说明

- 云 WAF 实例退订后，主套餐及资源扩展包将一同退订；资源扩展包不支持单独退订。
- 成功发起退订后，实例资源将转入冻结状态，冻结期 15 天。冻结期间，用户配置数据会保留 15 天，WAF 仍可以转发流量，同时 WAF 保留用户的配置数据，15 天后资源被释放，释放后无法恢复。

操作步骤

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择地域。
3. 在控制台列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“产品信息”。



5. 在当前实例信息展示界面，点击“退订”。
6. 进入退订申请页面，确认退订信息，信息确认无误后选择退订原因，勾选“我已确认本次退订金额和相关费用”后，点击“退订”后即可进行退订。

7. 系统提示退订申请提交成功，可前往订单详情查看退订进度。

2.6. 查看账单

客户可以在费用中心按月查看在天翼云的消费概况，详情请参见账单概览。

账单说明

WAF 产品为包年包月计费产品，包年包月产品采用预付费模式，即先付费再使用，一般为包年包月的购买形式，支付成功后，云资源将被系统分配给用户使用，直到超过保留期后被系统回收。

说明：

- 当月最终账单将在次月 3 日生成，在次月 4 日 10 点后可查看和导出。
- WAF 属于按月结算的产品，当月消费可在次月 3 日查看账单。

操作步骤

1. 登录天翼云控制中心。
2. 在页面右上角用户名称处，选择“费用中心”。

3. 在左侧菜单栏选择“账单管理”，进入“账单概览页面”，可按产品类型汇总查看产品账单。

4. 在左侧菜单栏选择“账单详情”页面，统计维度选择“产品”，统计周期选择“按账期”，计费模式选择“包周期”，账期选择需要查看的账单时间，即可查看到产品的账单详情。


费用中心
总览
订单管理
资金管理
撤单管理
账单管理
账单概览
流水账单
账单详情
导出记录
产品视图
发票管理
总计 4,982.46 0.00 0.00 4,982.46
汇总图表和表格
收起
按产品类型汇总
按企业项目汇总
按计费模式汇总
¥4,982.46
云下一代防火墙 ¥60.00
弹性云主机 ¥98.93
SSL VPN ¥80.00
云硬盘 ¥10.00
导出

3. 快速入门

3.1. 注册天翼云账号

在购买和使用 Web 应用防火墙（原生版）之前，您需要先注册天翼云门户的账号。本节将介绍如何进行账号注册，如果您拥有天翼云的账号，请跳转至开启 WAF 防护。

1. 登录天翼云门户 http://www.ctyun.cn，点击**注册**；

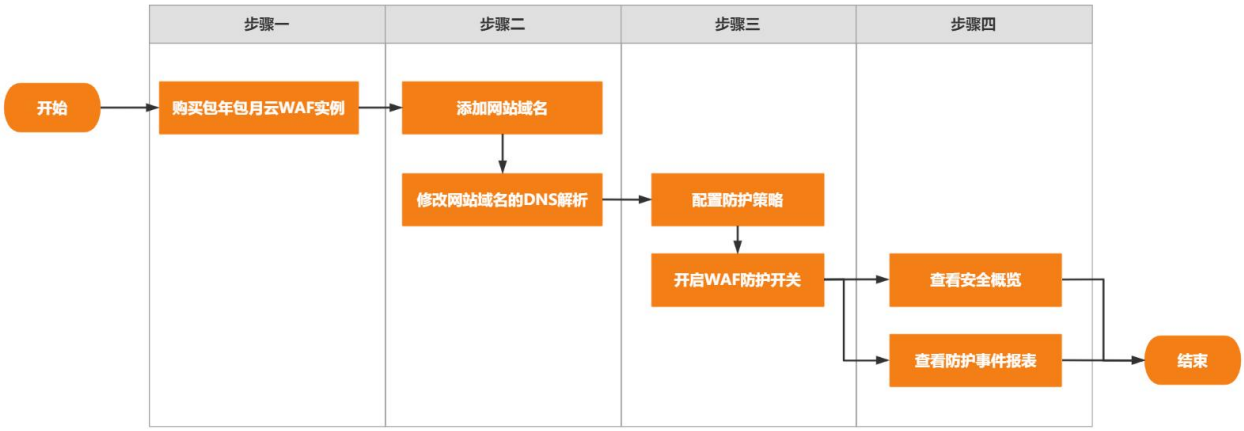
2. 在注册页面，请填写“邮箱地址”、“登录密码”、“手机号码”，并点击**同意协议并提交**，如 1 分钟内手机未收到验证码，请再次点击**免费获取短信验证码**；

3. 注册成功后，可到邮箱激活您的账号或立即体验天翼云。

3.2. 开启 WAF 防护

为快速实现 Web 应用防护，您需要购买云 WAF 实例、完成域名接入并配置防护策略。防护开启后，剋通过安全总览、防护时间报表查看访问统计信息和攻击防护记录，掌握业务的安全状况。

使用流程



步骤一 购买云 WAF 实例

操作流程

1. 登录天翼云控制台，在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
2. 首次使用 Web 应用防火墙（原生版），需点击“立即购买”，选择服务版本、扩展包以及购买时长；
3. 确认支付费用，点击“立即开通”，进入支付页面完成支付即可开通。

说明

1. Web 应用防火墙（原生版）提供了基础版、标准版、企业版、旗舰版四个版本，规格详情请参见产品规格；
2. 勾选“自动续费”后，当服务器满时，系统将会按照默认续费周期续费。按月购买，自动续费周期默认为 3 个月；按年购买，自动续费周期默认为 1 年。如需要修改自动续费周期，可进入天翼云“管理中心>产品中心>产品续订”页面，找到对应的资源进行修改。

步骤二 网站接入

1. 进入云 WAF 产品控制台，在左侧导航栏点击“域名接入”，在域名列表上方点击“添加域名”；
2. 根据页面提示配置域名、服务器协议、源站地址、代理情况、负载均衡策略等相关信息；
3. **放行 WAF 回源 IP 段**：WAF 使用特定的回源 IP 段将经过防护引擎检测后的正常流量转发回网站域名的源站服务器。网站接入 WAF 进行防护时，您需要设置源站服务器的安全软件或访问控制策略，放行 WAF 回源 IP 段的入方向流量。
4. **本地验证**：添加域名后，在本地电脑上搭建简易的模拟环境，验证网站流量转发设置已经生效，避免转发设置未生效时修改域名的 DNS 解析设置，导致业务访问异常。
5. **修改域名 DNS**：若域名在接入 WAF 前未使用代理，则需要到该域名的 DNS 服务商处，修改域名的 DNS 解析配置，将网站的流量解析到 WAF；若域名在接入 WAF 前使用了代理（DDoS 高防、CDN 等），则需要将使用的代理类服务（DDoS 高防、CDN 等）的回源地址修改为的目标域名的“CNAME”值。

说明

1. 系统默认防护 80 和 443 端口，如需配置 80 和 443 以外的端口，请额外选择；
2. 服务器配置若勾选了 HTTPS 协议，需要导入 HTTPS 证书。

步骤三 配置网站防护策略

网站域名接入 WAF 后，WAF 默认开启 Web 基础防护的规则防护引擎，可防御常见的 Web 应用攻击，如 SQL 注入、XSS、目录穿越、代码执行、文件包含、文件上传、命令注入、信息泄露、XML 实体注入等等。如需要开启其他防护模块，可按如下步骤配置：

1. 在 WAF 控制台左侧导航栏点击“防护配置”，在防护配置页面可以定位需要开启的防护模块，将“状态”切换为开启；
2. 开启后，可点击对应防护模块的“前去配置”，配置具体的防护策略或添加自定义防护策略。

步骤四 查看防护事件报表

网站开启正常防护后，WAF 会记录防护事件信息，包括域名、事件类型、处置动作、攻击 URL、攻击 IP、攻击时间等。

1. 在 WAF 控制台左侧导航栏点击“防护事件”；

2. 在防护事件列表可以查看网站的防护记录。

3.3. 配置 CC 攻击防护策略

网站域名接入云 WAF 后，您可以选择开启 CC 防护功能，为网站拦截针对页面请求的 CC 攻击。您也可以根据实际需求自定义 CC 安全防护的防护策略。

前提条件

- 已开通 Web 应用防火墙（原生版）实例；
- 已完成网站域名接入。

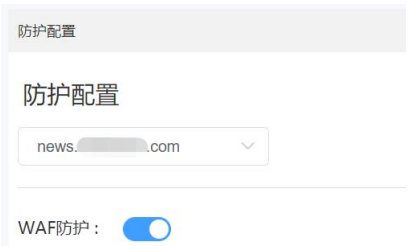
使用限制

基础版不支持 CC 防护，请升级到更高版本使用。

操作步骤-CC 防护模式配置

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。



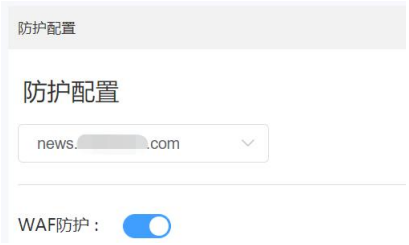
6. 在“防护配置”页面定位到 CC 防护区域，可以选择开启/关闭防护状态；同时可以直接选择防护模式，配置信息如下。

配置项	说明
状态	开启或关闭 CC 安全防护功能。
模式	要应用的防护模式。可选值： • **常规**：只针对特别异常的请求进行拦截，误杀较少。建议您在网站无明显流量异常时应用此模式，避免误杀。 • **紧急**：高效拦截 CC 攻击，可能造成较多误杀。当您发现有防护模式无法拦截的 CC 攻击，并出现网站响应缓慢，流量、CPU、内存等指标异常时，可以应用此模式。 • **自定义**：自定义 CC 防护可以通过精确匹配条件过滤访问请求的基础上，基于用户访问源 IP 或者 SESSION 频率定义访问频率限制条件，对于超过频率限制的访问进行处置，处置措施包括人机识别、JS 验证、阻断等。 策略配置方法，请参见设置自定义 CC 防护策略。 说明： ✓ 防护模式只能选择一种，不能同时开启。

操作步骤-自定义 CC 防护策略

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

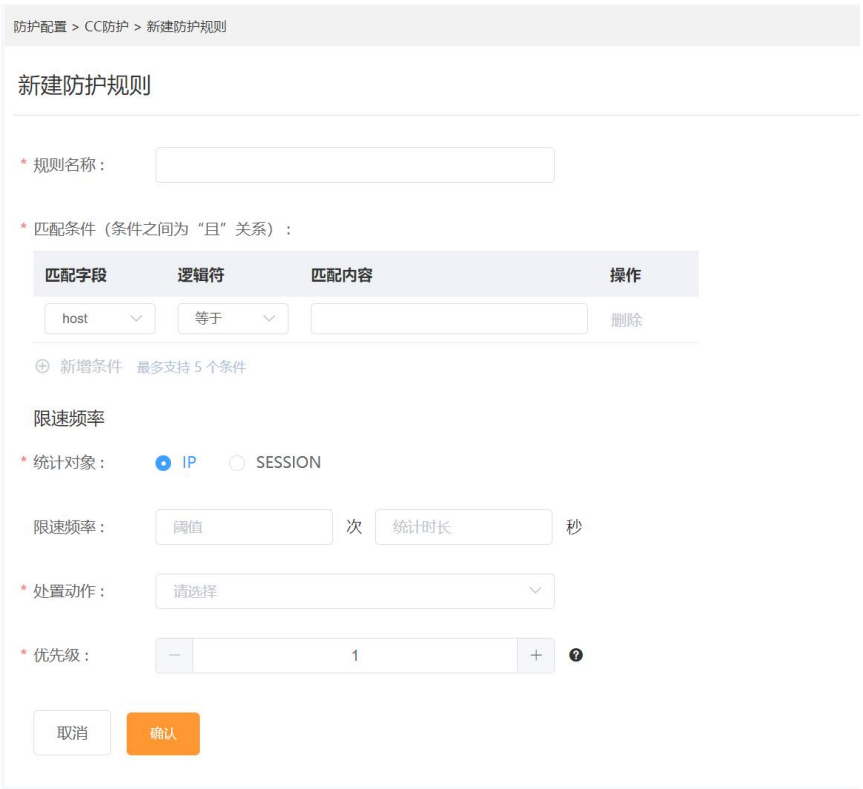
，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。



6. 在“防护配置”页面定位到 CC 防护区域，在自定义防护模式后方点击“前去配置”；

7. 进入 CC 防护自定义规则列表页，列表会展示已创建规则的相关信息，包括规则 ID/名称、匹配条件、限速频率、处置动作、优先级、规则状态、更新时间等；

8. 点击列表上方“新建防护规则”，进入规则配置页面，完成以下信息配置；



配置项	说明
规则名称	设置规则的名称。 规则名称用于标识当前防护规则，建议您使用有明确含义的名称。
匹配条件	设置访问请求需要匹配的条件（即特征）。单击新增条件可以设置最多 5 个条件。存在多个条件时，多个条件必须同时满足才算命中。 关于匹配条件的配置描述，请参见匹配条件字段说明。
频率设置	频率统计在匹配条件检测后生效，需要配置统计对象及限速频率。 统计对象为统计请求数量的依据，可选值如下： • IP：根据 IP 区分单个访问者。 • SESSION：根据会话区分单个访问者。对于 SESSION 模式，需要进一步设置 SESSION 信息。 SESSION 设置： • SESSION 位置：可选则 GET、POST、COOKIE • SEESION 标识：取值标识，通过配置唯一可识别 Web 访问者的某属性变量名（Key），系统讲根据此标识匹配到的内容识别访问者 限速频率为单个访问者在限速周期内最大可以正常访问的次数，如果超过该访问次数，WAF 则将根据配置的处置动作处理。配置项如下： • 统计时长（秒）：统计周期。 • 阈值（次）：统计时长内统计对象的允许数量，超过阈值，则触发频率限制。
处置动作	定义触发规则后执行的动作，可选值： • 观察 • 拦截 • 放行 • 验证码 • js 挑战 • 重定向 • 重置链接
优先级	代表该规则在 CC 防护模块儿中执行的优先级。 可输入 1～100 的整数，数字越大，代表这条规则的优先级越高。相同的优先级下，创建/更新时间越晚，优先级越高。

9. 点击“确认”，规则创建成功，成功后规则默认启用。您可以在规则列表中查看该规则。

10. 其他相关操作，对于已创建的规则，您可以执行以下操作：

    1）编辑：编辑自定义防护规则的名称、匹配条件、频率限制、处置动作、优先级等；

    2）删除：若不再使用某条规则，可对该规则进行删除；

    3）状态变更：可对每一条规则单独设置启用状态，若临时无须启用某条规则，可禁用该规则。

4. 用户指南

4.1. 接入 WAF

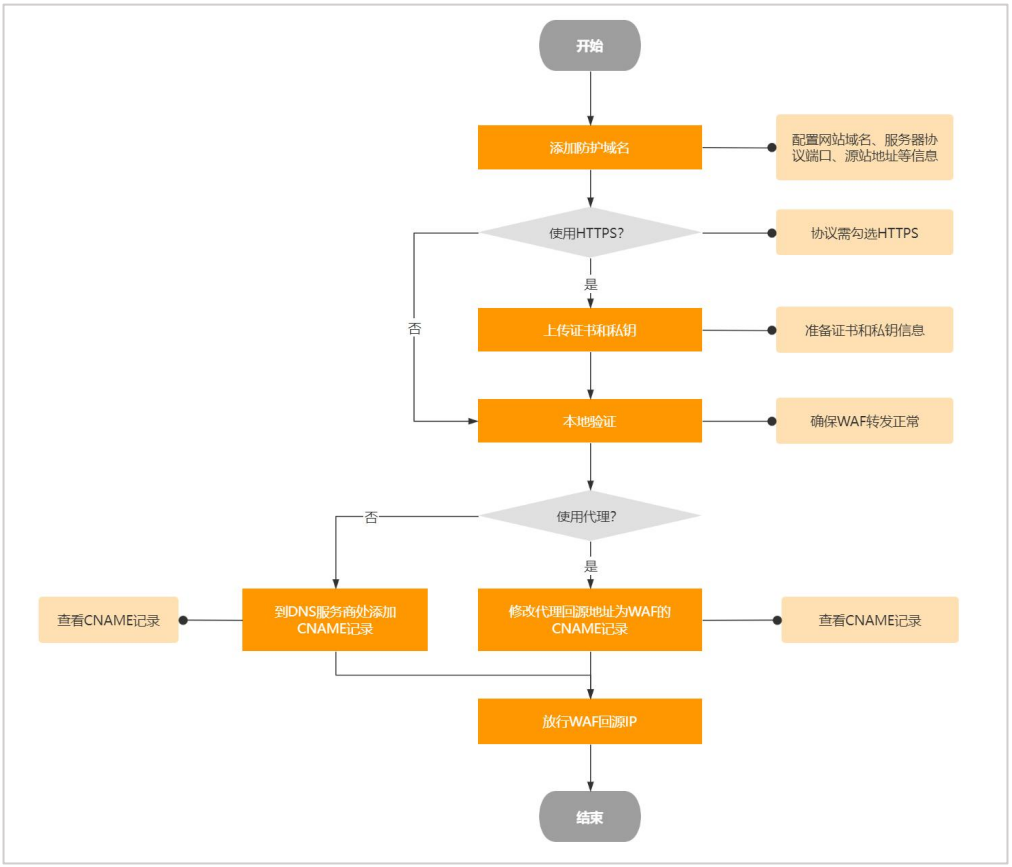
开通云 WAF 实例后，需要将您需要防护的网站域名接入 WAF，使网站的访问流量全部流转到 WAF 进行检测并转发，实现恶意流量的拦截。

域名接入 WAF 后，WAF 作为一个反向代理存在于客户端和服务器之间，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。

当前云 WAF 提供 CNAME 接入模式，可以防护通过域名访问的 Web 应用/网站，包括 Web 业务服务器部署在天翼云上、非天翼云或线下的域名。

CNAME 接入流程

在 WAF 控制台添加需要防护的网站域名后，通过修改域名的 DNS 解析设置，将网站流量解析到 WAF，使访问网站的流量经过 WAF 并受到 WAF 的防护。WAF 将过滤和处理后的请求转发回该域名的源站服务器。接入流程如下：



1. **添加域名**：配置域名、协议、源站等相关信息；
2. **放行 WAF 回源 IP 段**：WAF 使用特定的回源 IP 段将经过防护引擎检测后的正常流量转发回网站域名的源站服务器。网站接入 WAF 进行防护时，您需要设置源站服务器的安全软件或访问控制策略，放行 WAF 回源 IP 段的入方向流量。
3. **本地验证**：添加域名后，在本地电脑上搭建简易的模拟环境，验证网站流量转发设置已经生效，避免转发设置未生效时修改域名的 DNS 解析设置，导致业务访问异常。
4. **修改域名 DNS**：若域名在接入 WAF 前未使用代理，则需要到该域名的 DNS 服务商处，修改域名的 DNS 解析配置，将网站的流量解析到 WAF；若域名在接入 WAF 前使用了代理（DDoS 高防、CDN 等），则需要将使用的代理类服务（DDoS 高防、CDN 等）的回源地址修改为的目标域名的“CNAME”值。

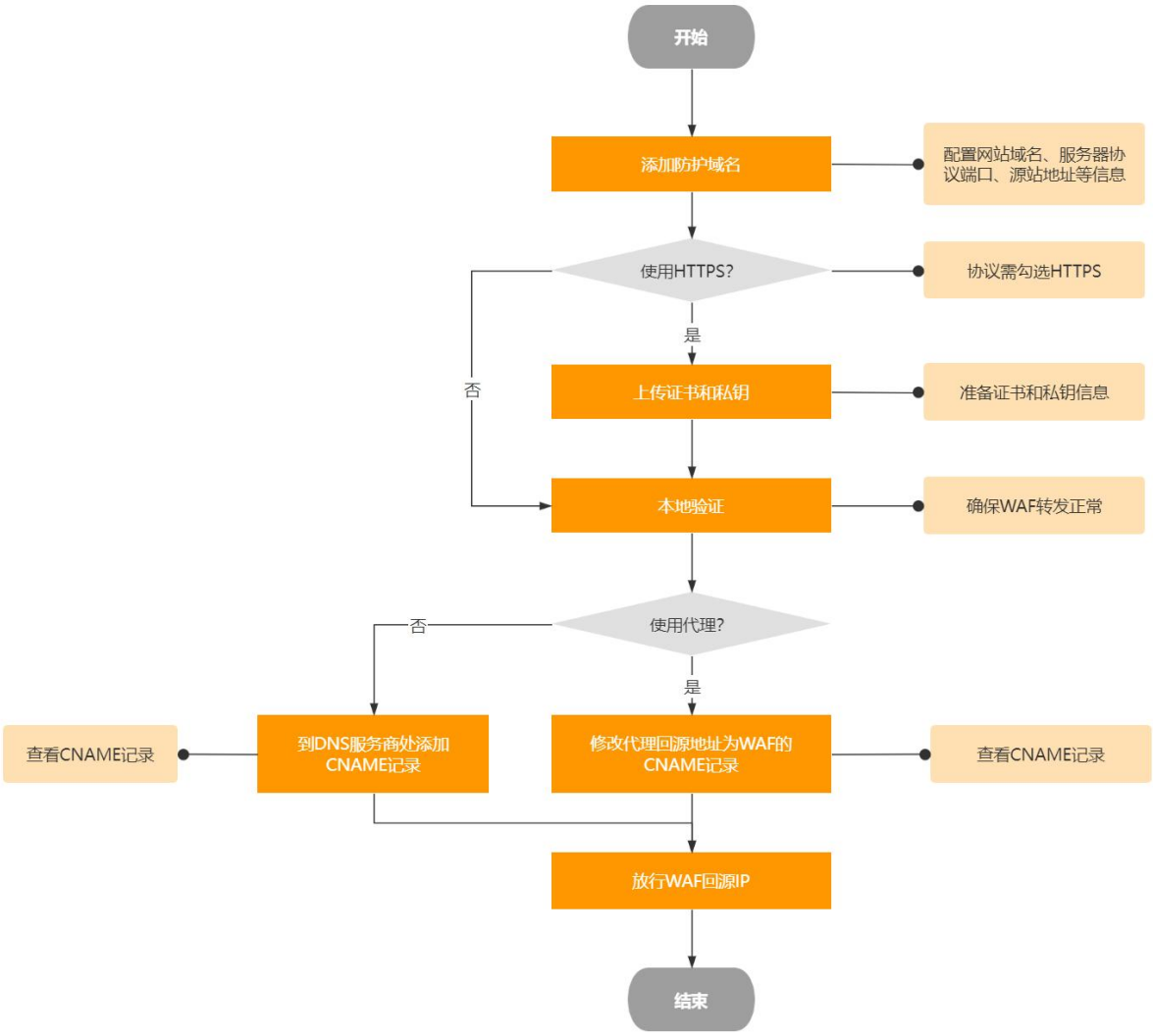
完成接入流程后，网站访问流量将经过 WAF 转发检测。WAF 包含多种防护检测模块，帮助网站应对不同类型的安全威胁，其中 Web 基础防护模块默认开启，用于防御常见的 Web 应用攻击（例如 SQL 注入、XSS 跨站、webshell 上传等），其他防护模块需要您手动开启并配置具体防护规则。

4.1.1. 概述

开通云 WAF 实例后，需要将您需要防护的网站域名接入 WAF，使网站的访问流量全部流转到 WAF 进行检测并转发，实现恶意流量的拦截。域名接入 WAF 后，WAF 作为一个反向代理存在于客户端和服务器之间，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。当前云 WAF 提供 CNAME 接入模式，可以防护通过域名访问的 Web 应用/网站，包括 Web 业务服务器部署在天翼云上、非天翼云或线下的域名。

CNAME 接入流程

在 WAF 控制台添加需要防护的网站域名后，通过修改域名的 DNS 解析设置，将网站流量解析到 WAF，使访问网站的流量经过 WAF 并受到 WAF 的防护。WAF 将过滤和处理后的请求转发回该域名的源站服务器。接入流程如下：



1. 添加域名： 配置域名、协议、源站等相关信息，详情请参见添加域名。
2. 放行 WAF 回源 IP 段： WAF 使用特定的回源 IP 段将经过防护引擎检测后的正常流量转发回网站域名的源站服务器。网站接入 WAF 进行防护时，您需要设置源站服务器的安全软件或访问控制策略，放行 WAF 回源 IP 段的入方向流量，详情请参见放行 WAF 回源 IP 段。
3. 本地验证： 添加域名后，在本地电脑上搭建简易的模拟环境，验证网站流量转发设置已经生效，避免转发设置未生效时修改域名的 DNS 解析设置，导致业务访问异常，详情请参见本地验证。
4. 修改域名 DNS： 若域名在接入 WAF 前未使用代理，则需要到该域名的 DNS 服务商处，修改域名的 DNS 解析配置，将网站的流量解析到 WAF；若域名在接入 WAF 前使用了代理（DDoS 高防、CDN

等），则需要将使用的代理类服务（DDoS 高防、CDN 等）的回源地址修改为的目标域名的“CNAME”值，详情请参见修改域名 DNS。

说明：

完成接入流程后，网站访问流量将经过 WAF 转发检测。WAF 包含多种防护检测模块，帮助网站应对不同类型的安全威胁，其中 Web 基础防护模块默认开启，用于防御常见的 Web 应用攻击（例如 SQL 注入、XSS 跨站、webshell 上传等），其他防护模块需要您手动开启并配置具体防护规则。

4.1.2. 添加域名

使用 CNAME 接入方式接入云 WAF 前，先要添加需要防护的域名。本文介绍如何将要防护的域名添加到云 WAF。

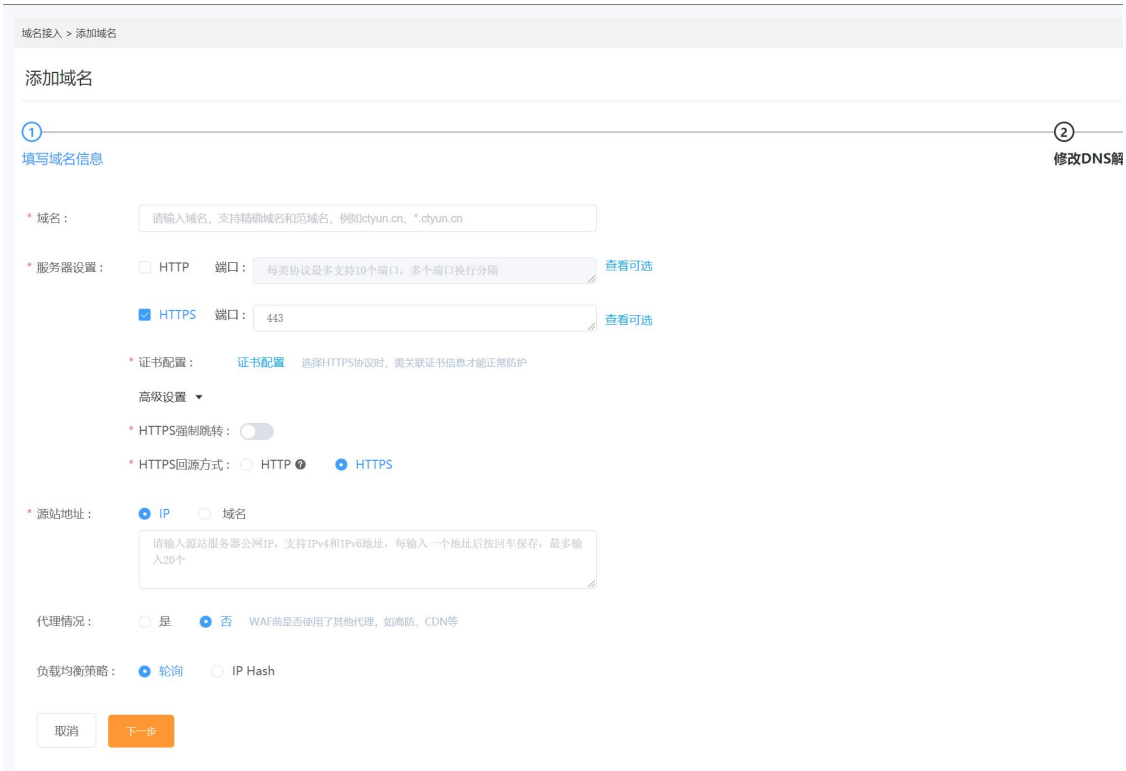
前提条件

- 已购买 WAF 实例，且当前实例支持接入的域名数量未超过限制。
- 如果您已购买云 WAF 实例，您必须先为域名完成 ICP 备案，才可以将网站接入云 WAF。

操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 南京3 ，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 进入到云 WAF 控制台，点击“域名接入”进入域名列表页，点击“添加域名”；

5. 进入域名接入信息配置页，依次配置“防护域名”、“服务器配置”、“源站配置”、“源站地址”、“代理情况”、“负载均衡策略”信息：



配置项说明如下：

配置项	说明
域名	填写网站域名。支持添加精确域名和泛域名： • 支持多级别精确域名，例如一级域名 ctyun.cn、二级域名 www.ctyun.cn 等； • 支持使用泛域名格式，例如*.ctyun.cn 可以比配 www.ctyun.cn、test.ctyun.cn； 说明： ✓ 使用泛域名后，WAF 将自动匹配该泛域名对应的所有子域名，例如，*.ctyun.cn 能够匹配 www.ctyun.cn、test.ctyun.cn 等； ✓ 泛域名不支持匹配对应的主域名，例如*.ctyun.cn 不能匹配 ctyun.cn； ✓ 如果同时存在精确域名和泛域名，则精确域名的转发规则和防护策略优先生效。 • 添加的域名必须通过工信部 ICP 备案，若未备案则无法添加。
服务器配置	选择网站使用的协议类型以及对应的转发服务端口。 协议类型可选项： • HTTP • HTTPS 选中协议后，系统会对应设置默认端口，HTTP 协议默认为 80 端口，HTTPS 协议默认为

443 端口。用户也可自定义选择其他端口，可选类型：

- 标准端口：80、8080；443、8443；
- 非标端口：除以上标准端口意外的端口

说明：

✓ 如果防护域名使用非标准端口，请查看 WAF 支持的端口；

✓ WAF 通过此处添加的端口为网站提供流量的接入与转发服务，网站域名的业务流量只通过已添加的服务端口进行转发。对于未添加的端口，WAF 不会转发任何该端口的访问请求流量到源站服务器，因此这些端口的启用不会对源站服务器造成任何安全威胁。

选择 HTTPS 后，还支持启用以下功能：

- （高级设置）开启 HTTPS 的强制跳转

  HTTPS 强制跳转表示将客户端的 HTTP 请求强制转换为 HTTPS 请求，默认跳转到 443 端口。如果您需要强制客户端使用 HTTPS 请求访问网站以提高安全性，则开启该设置。

  说明：

  ✓ 只有在未选中 HTTP 协议时，支持开启该设置。

  ✓ 请确保网站支持 HTTPS 业务再开启该设置。开启该设置后，部分浏览器将被强制设置为使用 HTTPS 请求访问网站。

- （高级设置）选择 HTTPS 回源方式

  HTTP 回源表示 WAF 使用 HTTP 协议向源站转发回源请求，默认回源端口是 80。开启 HTTP 回源可以在无需改动源站服务器的前提下，通过 WAF 实现 HTTPS 访问，帮助您降低网站的负载损耗。

  说明：

  ✓ 如果您的网站不支持 HTTPS 回源，请务必开启该设置。

若选择 HTTPS 协议，还需要上传证书，且证书必须正确、有效，才能保证 WAF 正常防护网站的 HTTPS 协议访问请求。

上传证书支持以下方式：

- 手动填写：填写**证书名称**，并将与域名关联的**证书文件**和**私钥文件**的文本内容的 PEM 编码分别复制粘贴到证书文件和私钥文件。
- 文件上传：填写**证书名称**，并将与域名关联的**证书文件**和**私钥文件**上传至平台中。

  说明：

	✓ 手动填写需要将证书和私钥的 PEM 编码内容填入； ✓ 上传证书时，需要如果证书是.PEM/.CER/.CRT 的后缀，可以直接上传；私钥文件若为.KEY/.PEM 的后缀，请确保内容格式为 PME 编码，即可上传。
源站地址	设置网站的源站服务器地址，支持 IP 地址格式和域名（如 CNAME）格式。完成接入后，WAF 将过滤后的访问请求转发到此处设置的服务器地址。设置说明： • IP 地址格式：填写源站的公网 IP 地址。需要为公网可达的 IP 地址。支持填写多个 IP 地址，每填写一个 IP 地址，按回车进行确认。最多支持添加 20 个源站 IP 或 20 个服务器域名。 支持同时配置 IPv4 和 IPv6 地址。 • 域名格式：一般对应该域名在 DNS 服务商处配置的 CNAME。 使用域名格式时， WAF 会将客户端请求转发到回源域名解析出来的 IP 地址
代理情况	选择网站业务在接入 WAF 前是否开启了其他代理服务（例如 DDoS 高防、CDN 等），按实际情况选择： • **否**：表示 WAF 收到的业务请求来自发起请求的客户端。WAF 直接获取与 WAF 建立连接的 IP 作为客户端 IP； • **是**：表示 WAF 收到的业务请求来自其他代理服务转发，而非直接来自发起请求的客户端。为了保证 WAF 可以获取真实的客户端 IP 进行安全分析，需要进一步设置客户端 IP 判定方式。 客户端 IP 判定方式：系统默认设置为“从 Socket 连接中获取”，您也可按实际情况，创建一个有序的判定列表，系统将从列表的第一项开始查找，若不存在或者是非法的 IP 格式，则尝试下一条。其中检测末项固定为“从 Socket 连接中获取”。 获取方式列表最多可添加 5 条规则，可选项如下： ✓ 从 Socket 连接中获取 ✓ 从 X-Fowarded-For 连接中获取倒数第___层代理 ✓ 从 HTTP 头_____中获取

	
负载均衡策略	当设置了多个源站服务器地址时，需设置多源站服务器间的负载均衡算法。可选项如下： • 轮询：将所有请求轮流分配给源站服务器。 • IP Hash：将某个 IP 的请求定向到同一个源站服务器。 设置生效后，WAF 将根据设置的负载均衡算法向多个源站地址分发回源请求，实现负载均衡。

6. 修改 DNS 解析。

   根据根据页面提示修改域名的 *DNS* 解析，将网站域名解析到 *WAF* 进行防护，完成后单击**下一步**。

   更多信息，请参见修改域名 *DNS*。

7. 添加完成。

   根据页面提示设置放行 WAF 回源 IP 段，完成后单击完成，返回网站列表，返回网站接入页面。更多信息，请参见放行 WAF 回源 IP 段。

8. 域名添加完成后，该域名 WAF 防护开关默认开启。

后续配置

完成域名接入流程后，网站访问流量将经过 *WAF* 保护，您还需要完善以下防护配置，才能实现针对性的网站防护。

配置	说明	相关文档
Web 基础防护	覆盖 OWASP 常见安全威胁，支持 SQL 注入、XSS、文	Web 基础防护

	件包含、远程命令执行、目录穿越、文件上传、CSRF、SSRF、命令注入、模板注入、XML 实体注入等攻击检测和拦截。	
CC 防护	CC 防护支持默认防护策略及灵活的自定义防护策略。自定义策略支持依托精准访问控制规则进行特征识别，并根据访问源 IP/ SESSION 控制访问频率，恶意流量通过阻断、人机验证等处置手段有效缓解 CC 攻击。	CC 防护
BOT 防护	提供公开类型、协议特征、自定义会话特征等多种判定维度的防护策略，支持根据 BOT 会话行为特征设置 BOT 对抗策略，对 BOT 行为进行处理，有效防护搜索引擎、扫描器、脚本工具等爬虫攻击。	BOT 防护
精准访问控制	支持基于 IP、URL、Referer、User-Agent 等请求特征进行多维度组合，定义访问匹配条件过滤访问请求，实现针对性的攻击阻断。	精准访问控制
IP 黑白名单	支持添加始终拦截与始终放行的黑白名单 IP/IP 地址段，增强防御准确性。	IP 黑白名单
地域访问控制	支持针对地理位置的黑名单封禁，可指定需要封禁的国家、地区，阻断该区域的来源 IP 的访问。	地域访问控制

4.1.3. 放行 WAF 回源 IP 段

WAF 使用特定的回源 IP 段，将经过防护引擎检测后的正常流量转发回网站域名的源站服务器。网站接入 WAF 进行防护后，您需要将回源 IP 段添加到源站安全软件的白名单中，放行该回源 IP 段。本文介绍如何放行 WAF 回源 IP 段。

为什么要放行回源 IP 段

网站接入 WAF 后，由于访问来源 IP 变得更加集中，访问频率变得更高，服务器上的防火墙或安全软件很容易认为这些 IP 在发起攻击，从而将 WAF 回源 IP 段拉黑。如果 WAF 的回源 IP 段被拉黑，WAF 的请求将无法得到源站的正常响应。因此，在网站接入 WAF 后，您应确保源站服务器已将 WAF 的全部回源 IP 放行（即加入白名单），否则可能会出现网站无法打开或打开极其缓慢等情况。

操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 ，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在域名列表中，定位到已添加的域名，点击进入“域名详情”页；
5. 在“域名详情”页 Web 应用防火墙信息栏中，可以复制 WAF 回源 IP 地址；
6. 将 WAF 回源 IP 地址添加到源站安全软件的白名单中。

4.1.4. 本地验证

已在 Web 应用防火墙（WAF）中添加域名，但还未修改域名的 DNS 解析（将网站域名解析到 WAF）时，建议您通过修改本地计算机的 DNS 解析，在本地计算机上验证 WAF 的域名接入设置正确有效。本文以 Windows 操作系统为例，介绍了在本地计算机验证域名接入设置的操作步骤。

前提条件

已通过 CNAME 接入模式手动添加网站域名。

背景信息

通过修改本地计算机的 hosts 文件，可以设置本地计算机的域名寻址映射，即仅对本地计算机生效的 DNS 解析记录。本地验证需要您在本地计算机上将网站域名的解析指向 WAF 的 IP 地址。这样就可以通过本地计算机访问被防护的域名，验证 WAF 中添加的域名接入设置是否正确有效，避免域名接入配置异常导致网站访问异常。

操作步骤

以下操作以本地计算机使用 Windows 操作系统为例进行描述。

1. 打开本地计算机的文件资源管理器。

2. 在地址栏输入 C:\Windows\System32\drivers\etc\hosts，并选择使用文本编辑器打开 hosts 文件。

3. 在 hosts 文件最后一行添加以下记录：

```
<WAF IP 地址> <被防护域名>
```

其中<被防护域名>表示已在 WAF 添加的域名，<WAF IP 地址>表示域名对应的 WAF IP 地址。<WAF IP 地址>和<域名>之间使用空格分隔。

获取 WAF IP 地址的操作步骤如下：

1) 登录天翼云控制中心；

2) 单机管理控制台右上方的 南京3 ，选择地域；

3) 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；

4) 在域名列表中，定位到已添加的域名，点击进入“域名详情”页；

5) 在“域名详情”页 Web 应用防火墙信息栏中，可以复制该域名对应的 WAF Cname 地址；

6) 在 Windows 操作系统中，打开 cmd 命令行工具。

7) 执行以下命令：

```
ping <已复制的 WAF Cname 地址>
```

8) 在 ping 命令的返回结果中，记录域名对应的 WAF IP 地址。

4. 保存修改后的 hosts 文件，并执行 ping <被防护域名>命令，验证 hosts 修改已生效。

预期 ping 命令解析到的 IP 地址是域名对应的 WAF IP 地址，表示 hosts 修改已经生效。

如果解析到了源站 IP 地址，请刷新本地的 DNS 缓存（可以执行.\ipconfig /flushdns 命令）并重新执行 ping 命令，直到验证 hosts 修改已经生效。

5. 打开本地计算机的浏览器，在地址栏输入被防护域名进行访问。

- 如果网站能够正常访问，说明 WAF 中添加的域名设置正确有效。您可以在将 hosts 文件复原后，放心修改域名的 DNS 解析，将网站流量解析到 WAF 进行防护。更多信息，请参见修改域名 DNS。
- 如果网站访问不正常，说明 WAF 中添加的域名设置可能有问题，建议您检查 WAF 中的域名接入设置，修复问题后重新进行本地验证。更多信息，请参见添加域名。

6. 完成本地验证后，重新修改 hosts 文件，删除步骤 3 中添加的记录。

4.1.5. 修改域名 DNS

在添加网站域名后，您必须使用 WAF 的 CNAME 地址（或 IP 地址）修改域名的 DNS 解析设置，将网站的 Web 请求解析到 WAF 进行安全防护。本文介绍了修改域名 DNS 的相关内容。

前提条件

- 已通过 CNAME 接入模式手动添加网站域名；
- 可选：已在源站服务器上放行 WAF 回源 IP 地址；
- 可选：已通过本地验证确保转发配置生效。通过本地验证确保 WAF 的网站转发配置正常，防止因配置错误导致业务中断；
- 拥有在域名的 DNS 服务商处修改域名解析设置的权限。

> 注意：如果在 WAF 的网站转发配置未生效时修改域名 DNS，可能导致业务中断。

操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 ，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在域名列表中，定位到已添加的域名，点击进入“域名详情”页；
5. 在“域名详情”页 Web 应用防火墙信息栏中，可以复制该域名对应的 WAF Cname 地址；

6. 若用户网站前未使用代理类服务（高防、CDN 服务等），则应到该域名的 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。

   以下以天翼云云解析产品为例，价绍修改域名解析记录的方法，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。

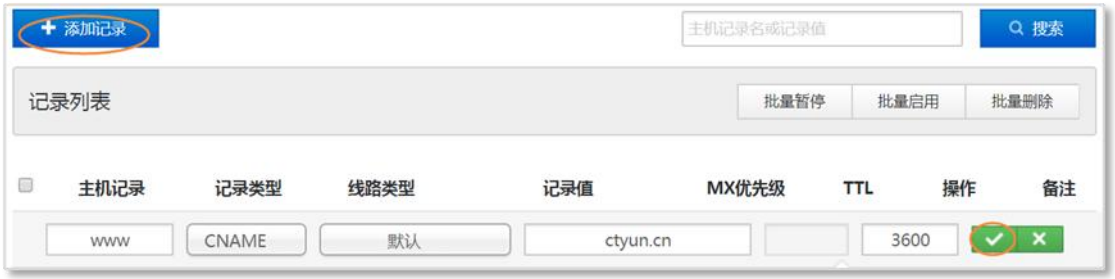
   1） 登录天翼云控制中心；

   2） 进入云解析产品控制台，点击“解析管理”进入域名维护页面；

   3） 在域名维护页面，点击要修改的域名进入记录管理页；

   4） 单击页面上方的“添加记录”按钮，系统将自动生成一条空白记录。

   5） 填写以下信息：



   - 主机记录：一般是指子域名的前缀。（如需实现 www.ctyun.cn，主机记录输入“ www”；如需实现 ctyun.cn，主机记录输入“@”）
   - 记录类型：选 CNAME 记录
   - 线路类型：通常选择默认（默认为必填项，否则会导致部分用户无法解析）
   - 记录值：填写刚获取的 WAF Cname 地址
   - TTL：缓存时间，默认为 3600 秒

   6） 单击“√”完成记录添加。

7. DNS 解析修改完成之后，待 DNS 记录生效，云 WAF 即可对访问网站的流量进行防护了。

8. 若用户网站前使用了代理类服务（高防、CDN 服务等），则需要将代理类服务的回源地址修改为该域名对应的 WAF Cname 地址。

注意：为保证 WAF 的安全策略能够对真实的源 IP 生效，请确保网站接入时的“是否已使用代理”参数已配置“是”。

4.1.6. WAF 支持的端口

WEB 应用防火墙除了可以防护标准端口外，还支持非标准端口的防护。不同版本的云 WAF 实例支持添加的端口数量不同，具体可见下表所示。

服务版本	端口分类	HTTP 协议端口范围	HTTPS 协议端口范围	端口防护限制数
基础版	标准端口	80、8080	443、8443	4 个
标准版	标准端口	80、8080	443、8443	20 个
	非标准端口	81、82、83、84、86、87、88、89、97、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7070、7071、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、	4443、5443、6443、7443、8553、8663、9443、9553、9663、18980	

		9916、9918、9919、9928、9929、9939、9999、10000、10001、10080、12601、28080、33702、48800		
企业版	标准端口	80、8080	443、8443	30 个
	非标准端口	81、82、83、84、86、87、88、89、97、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7070、7071、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、9999、10000、10001、10080、12601、28080、33702、48800	4443、5443、6443、7443、8553、8663、9443、9553、9663、18980	
旗舰版	标准端口	80、8080	443、8443	60 个
	非标准端口	81、82、83、84、86、87、88、89、97、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、	4443、5443、6443、7443、8553、8663、9443、9553、9663、18980	

		7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7070、7071、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、9999、10000、10001、10080、12601、28080、33702、48800		

4.1.7. WAF 支持的加密套件

在使用过程中，需要 Web 业务管理员将 Web 服务的证书及对应的私钥导入到 Web 应用防火墙中，从而实现客户对 Web 业务的安全访问。证书加密的方式主要通过加密套件对所传输的信息进行加密，Web 应用防火墙支持的加密算法套件及协议如下表：

OpenSSL 名称	RFC 名称	TLS 支持的版本
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS1.2
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS1.2
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS1.2
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS1.2

OpenSSL 名称	RFC 名称	TLS 支持的版本
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS1.2
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS1.2
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS1.2
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS1.2
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS1.2
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS1.2
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS1.2
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS1.2
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS1.0, TLS1.1, TLS1.2
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS1.0, TLS1.1, TLS1.2
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS1.0, TLS1.1, TLS1.2
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS1.0, TLS1.1, TLS1.2
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA	TLS1.0, TLS1.1, TLS1.2
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA	TLS1.0, TLS1.1, TLS1.2
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS1.0, TLS1.1, TLS1.2
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	TLS1.3
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	TLS1.3
TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	TLS1.3

注意：

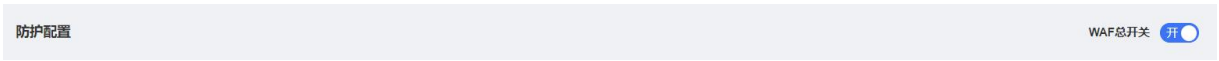
证书指主要指 https 访问请求所使用的证书，通过使用 https 的证书能够保证用户请求的安全性。证书的主要原理是通过对用户请求通过第三方颁发的可信证书中的公钥对会话进行加密和签名从而保证用户本身的信息以及用户所访问服务器的安全性。服务器端接受到用户通过公钥加密发送的请求和签名后，再通过私钥进行解密，从而验证用户本身的安全性，而 Web 应用防火墙通过导入所防护域名的证书和私钥，是需要作为一个中间人对用户的会话进行安全验证，同时还需要将用户请求通过安全的方式发送回服务端从而保证整个访问业务链路的安全。

4.2. 防护配置

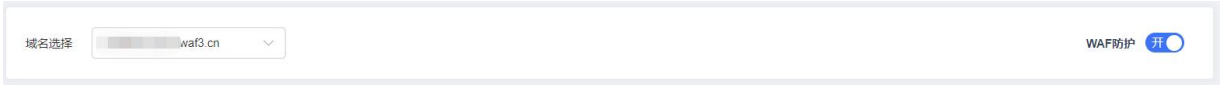
4.2.1. WAF 防护概述

WAF 提供各级防护开关，支持通过开关一键控制 WAF 实例防护状态、某个域名的防护状态、域名的某个防护模块的防护状态以及某条防护规则的防护状态。

- WAF 总开关：可以控制当前 WAF 实例的防护状态。关闭 WAF 总开关后，所有域名的防护状态均关闭。WAF 将只进行流量转发，不会拦截攻击行为也不会记录攻击日志。



- 域名防护开关：可以控制某个域名的防护状态。闭 WAF 总开关后，该域名的所有的防护功能关闭，WAF 进入流量转发模式，不会拦截攻击行为也不会记录攻击日志。



- 防护模块开关：可以控制域名的某个防护模块的防护状态。用户可以根据防护需要选择开启或关闭某个防护模块，防护模块包括 Web 基础防护、BOT 防护、精准访问控制、CC 防护、IP 黑白名单、地域访问控制。

- 防护规则开关：可以控制某条具体的防护规则的防护状态。用户可以根据防护需要选择开启或关闭规则的防护状态。例如，关闭某条 CC 自定义防护规则的防护状态。

4.2.2. Web 基础防护

Web 基础防护基于内置的防护规则集，自动为网站防御 SQL 注入、XSS、文件包含、远程命令执行、目录穿越、文件上传、CSRF、SSRF、命令注入、模板注入、XML 实体注入攻击等通用的 Web 攻击。

前提条件

- 已开通 Web 应用防火墙（原生版）实例；
- 已完成网站域名接入。

背景信息

云 WAF 的 Web 基础防护规则引擎默认开启，所有接入云 WAF 防护的网站业务，默认都受到 Web 基础防护规则引擎的检测和防护。

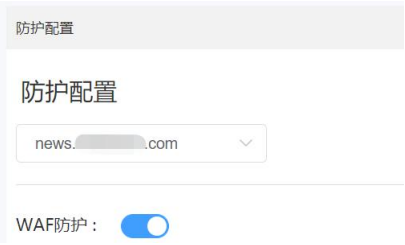
Web 基础防护规则引擎基于天翼云持续优化的高质量攻击检测规则集，帮助网站防御各种常见的 Web 应用攻击。您可以根据业务防护需要，在防护规则组的维度，设置规则引擎采用哪些防护规则。WAF 按照防护严格程度，内置了三套规则组供选用：

- 中等规则组：默认选用该规则组。
- 宽松规则组：如需减少误拦截，可选用该规则组。
- 严格规则组：如需提高攻击检测命中率，可选用该规则组。

您也可以自定义防护规则组，相关操作，请参见自定义防护规则组。

操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的  ，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置”页面上方，切换到要设置的域名。



6. 在“防护配置”定位到 Web 基础防护区域，完成以下功能配置。

配置项	说明
状态	开启或关闭 Web 基础防护规则引擎。防护规则引擎默认开启，为所有接入 WAF 防护的网站防御常见的 Web 应用攻击。
防护规则组	选择要应用的防护规则组。支持应用内置规则组和自定义规则组。内置规则组包括： • 中等规则组：按照标准防护程度去检测常见的 Web 应用攻击。默认应用该规则组。 • 严格规则组：按照严格防护程度去检测路径穿越、SQL 注入、命令执行等 Web 应用攻击。 • 宽松规则组：按照宽松防护程度去检测常见 Web 应用攻击。当您发现中等规则下存在较多误拦截，或者业务存在较多不可控的用户输入（例如，富文本编辑器、技术论坛等），建议您选择该规则组。 • 自定义防护规则组：用户可根据业务情况自定义防护规则组。 单击“前去配置”，将跳转到防护规则组配置页面，您可以根据业务需要自定义防护规则组及要应用的防护规则。具体操作，请参见自定义防护规则组。

处置动作	检测发现攻击请求时，对攻击请求执行的操作。可选值： • 拦截：检测到攻击行为后，直接阻断攻击请求，并记录攻击日志； • 观察：检测到攻击行为后，不阻断攻击，仅记录攻击日志。
规则白名单	开启 Web 基础防护后对正常网站请求造成误拦截，可以通过设置规则白名单，让满足条件的请求不经过指定规则的检测。建议您在设置 Web 入侵防护白名单规则时，结合实际业务需求，确保放行的都是预期的访问请求。 单击“前去配置”，将跳转到规则白名单列表页面，您可以根据业务需要创建白名单规则。具体操作，请参见配置规则白名单。

4.2.2.1. 设置防护规则引擎

Web 基础防护基于内置的防护规则集，自动为网站防御 SQL 注入、XSS、文件包含、远程命令执行、目录穿越、文件上传、CSRF、SSRF、命令注入、模板注入、XML 实体注入攻击等通用的 Web 攻击。

前提条件

- 已开通 Web 应用防火墙（原生版）实例。
- 已完成网站域名接入。

背景信息

云 WAF 的 Web 基础防护规则引擎默认开启，所有接入云 WAF 防护的网站业务，默认都受到 Web 基础防护规则引擎的检测和防护。

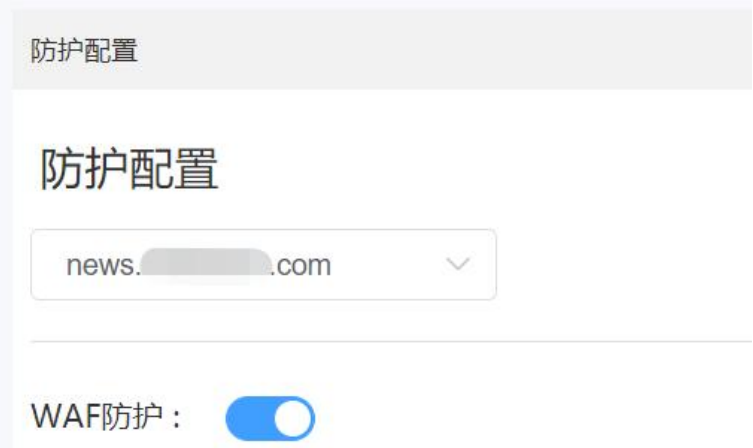
Web 基础防护规则引擎基于天翼云持续优化的高质量攻击检测规则集，帮助网站防御各种常见的 Web 应用攻击。您可以根据业务防护需要，在防护规则组的维度，设置规则引擎采用哪些防护规则。WAF 按照防护严格程度，内置了三套规则组供选用：

- 正常规则组：默认选用该规则组。
- 宽松规则组：如需减少误拦截，可选用该规则组。
- 严格规则组：如需提高攻击检测命中率，可选用该规则组。

您也可以自定义防护规则组，相关操作，请参见自定义防护规则组。

操作步骤

1. 登录天翼云控制中心。
2. 单机管理控制台右上方的，选择地域。
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”。
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面。
5. 在“防护配置“页面上方，切换到要设置的域名。



6. 在“防护配置”定位到 Web 基础防护区域，完成以下功能配置。

配置项	说明
状态	开启或关闭 Web 基础防护规则引擎。防护规则引擎默认开启，为所有接入 WAF 防护的网站防御常见的 Web 应用攻击。
防护规则组	选择要应用的防护规则组。支持应用内置规则组和自定义规则组。内置规则组包括： ● 正常规则组：按照标准防护程度去检测常见的 Web 应用攻击。默认应用该规则组。 ● 严格规则组：按照严格防护程度去检测路径穿越、SQL 注入、命令执行等 Web 应用攻击。 ● 宽松规则组：按照宽松防护程度去检测常见 Web 应用攻击。当您发现中等规则下存在较多误拦截，或者业务存在较多不可控的用户输入（例如，富文本编辑器、技术论坛等），建议您选择该规则组。 ● 自定义规则组：用户可根据业务情况自定义防护规则组。 单击“前去配置”，将跳转到防护规则组配置页面，您可以根据业务需要自定义防护规

配置项	说明
	则组及要应用的防护规则。具体操作，请参见自定义防护规则组。
处置动作	检测发现攻击请求时，对攻击请求执行的操作。可选值： ● 拦截：检测到攻击行为后，直接阻断攻击请求，并记录攻击日志； ● 观察：检测到攻击行为后，不阻断攻击，仅记录攻击日志。
规则白名单	开启 Web 基础防护后对正常网站请求造成误拦截，可以通过设置规则白名单，让满足条件的请求不经过指定规则的检测。建议您在设置 Web 入侵防护白名单规则时，结合实际业务需求，确保放行的都是预期的访问请求。 单击“前去配置”，将跳转到规则白名单列表页面，您可以根据业务需要创建白名单规则。 具体操作，请参见配置规则白名单。

4.2.2.2. 自定义防护规则组

云 WAF 的防护规则引擎支持用户自定义搭建防护规则组，为具体的防护场景创建有针对性的防护策略。在设置网站防护功能时，如果默认的防护规则组不能满足您的需求，建议您自定义防护规则组。

前提条件

- 已开通了 Web 应用防火墙，且实例版本为标准版及以上版本；
- 已完成网站接入。具体操作，请参见添加域名。

使用限制

基础版不支持自定义防护规则组，请升级到更高版本使用。

使用流程

防护规则组应用流程如下：

1. 新建规则组：为具体防护功能创建自定义防护规则组，形成有针对性的防护策略。
2. 应用规则组：已添加自定义防护规则组后，您可以为网站域名应用自定义防护规则组。

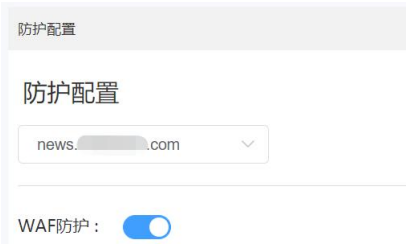
操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；

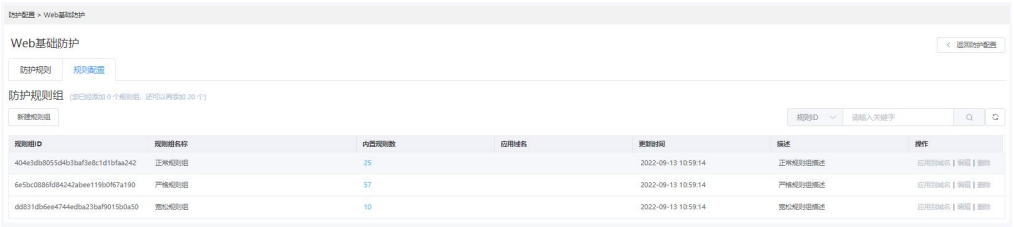
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；

5. 在“防护配置“页面上方，切换到要设置的域名。

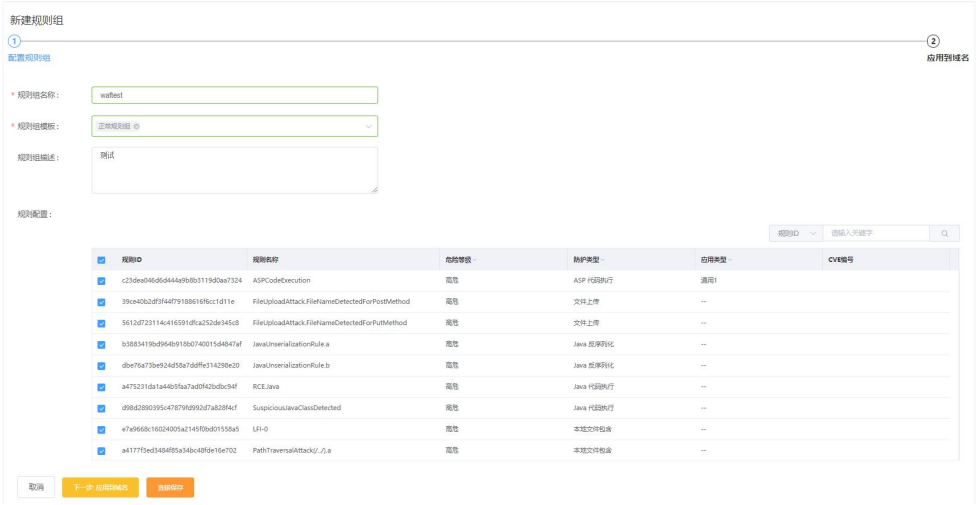


6. 在“防护配置”页面定位到 Web 基础防护区域，在防护规则组项点击“前去配置”；

7. 进入“规则配置”页面，可以看到当前的规则组列表。规则组列表展示了系统默认防护规则组及自定义防护规则组；



8. 在规则组列表上方，点击“新建规则组”，进入新建规则组页面，完成以下信息配置；



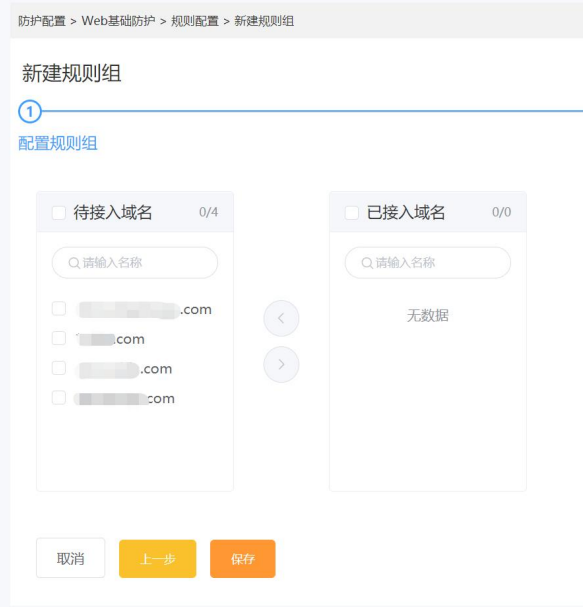
配置项	说明
规则组名称	设置规则组的名称。 规则组名称用于标识当前规则组，建议您使用有明确含义的名称。
规则组模板	选择要应用的规则组模板。可选项： • 严格规则组 • 中等规则组 • 宽松规则组 • 其他自定义规则组 规则组模板可以多选，系统会将所选的规则组最大集作为模板，下一步基于该集合规则配置。
规则组描述	输入规则组的描述信息。
规则配置	选择当前规则组要应用的防护规则。 当前规则列表默认展示您所选的规则组模板集合中的所有规则，您需要从中勾选适用的规则，将不适用或者可能造成误拦截的规则取消勾选。 您可以使用筛选和搜索功能查询规则，例如通过危险等级、防护类型、应用类型筛选规则，或者输入规则名称、CVE 编号、ID 搜索规则。 • **危险等级**：表示规则防御的 Web 攻击的危险等级，包括高危、中危、低危。 • **防护类型**：表示规则防御的 Web 攻击类型，包括 SQL 注入、XSS、机器人请求、目录穿越、Java 代码执行、PHP 代码执行、ASP 代码执行、通用代码执行、Java 反序列化、PHP 反序列化、本地文件包含、远程文

	件包含、文件上传、CSRF、SSRF、命令注入、信息泄露、模板注入、XML 实体注入、未知攻击。 • **应用类型**：表示规则防护的 Web 应用类型，包括通用、Dedecms、Wordpress、其他。

9. 如您暂时无需应用新建的规则组，可以在完成以上配置后，点击“直接保存”，完成配置向导。后续需要应用该规则组的时候再配置即可；

10. （可选）将规则组应用到域名防护。从“待接入域名”列表中选择要应用当前规则组的域名，添加到“已接入域名”列表，点击“保存”。

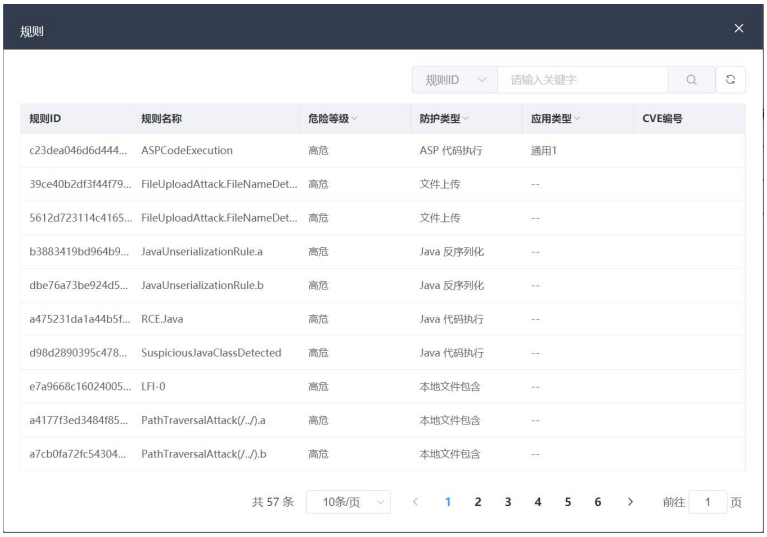
注意：每个网站域名只能应用一个防护规则组。



11. 完成操作后，您可以在规则组列表中查看新建的规则组，包括规则组的更新时间以及应用域名的情；

12. 您可以根据需要调整应用防护规则组的域名，通过点击“应用到域名”进行操作即可。

13. 创建规则组后，您可以在防护规则组列表中查看规则组内置规则情况，点击“内置规则数”进入规则列表。



14. 其他相关操作，对于已创建的规则组，您可以执行以下操作：

1）编辑：编辑自定义防护规则组的名称、描述和规则配置。系统默认规则组不支持编辑。

2）删除：删除自定义防护规则组。系统默认规则组不支持删除。

注意：在删除自定义防护规则组时，请确保当前防护组未被应用到网站域名上，否则将会影响 WAF 对网站无法正常防护。

4.2.2.3. 配置规则白名单

网站接入云 WAF 后，您可以通过设置 Web 基础防护模块中的规则白名单，让满足指定特征的请求不经过规则防护引擎的检测。Web 入侵防护白名单一般用于放行因触发 Web 基础防护相关规则被误拦截的特殊业务请求。

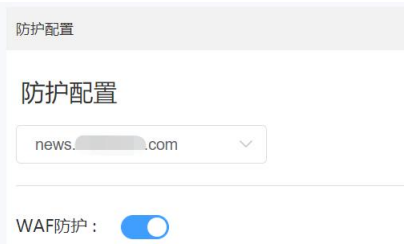
前提条件

- 已开通了 Web 应用防火墙，且实例版本为标准版及以上版本；
- 已完成网站接入。具体操作，请参见添加域名。

操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。



6. 在“防护配置”页面定位到 Web 基础防护区域，在规则白名单项点击“前去配置”；

7. 进入“白名单配置”列表页，可以查看当前已创建的白名单列表，可以查看白名单相关配置内容，如白名单匹配规则条件、不检测项、更新时间、白名单生效状态等；

8. 点击列表上方“新建白名单”，进入白名单配置页面，并完成以下规则配置；

配置项	说明
规则适用域名	在页面上方下拉列表中，可指定白名单适用的域名。 
规则名称	设置规则的名称。 规则名称用于标识当前规则组，建议您使用有明确含义的名称。

匹配条件	设置白名单请求需要匹配的条件（即特征）。单击新增条件可以设置最多 5 个条件。存在多个条件时，多个条件必须同时满足才算命中。  关于匹配条件的配置描述，请参见匹配条件字段说明。
不检测项	设置不检测的规则，可选项： • 全部规则：规则防护引擎包含的全部规则； • 特定规则 ID：只忽略检测指定的规则，选中“特定规则 ID”，并输入不检测的规则 ID；  说明： ✓ 您可以在“防护规则组”配置页面，通过“防护规则”选项卡查看云 WAF 所包含的所有防护规则，并获取相关规则的 ID。 ✓ 每输入一个规则 ID，需要按回车进行确认。最多支持输入 50 个规则 ID。 • 特性规则类型：只忽略检测指定的规则类型，选中“特定规则类型”，并选中不检测的规则类型。 

9. 成功添加 Web 入侵防护白名单规则后，规则自动启用。您可以在规则列表中查看新建的规则，并根据需要禁用、编辑或删除规则。

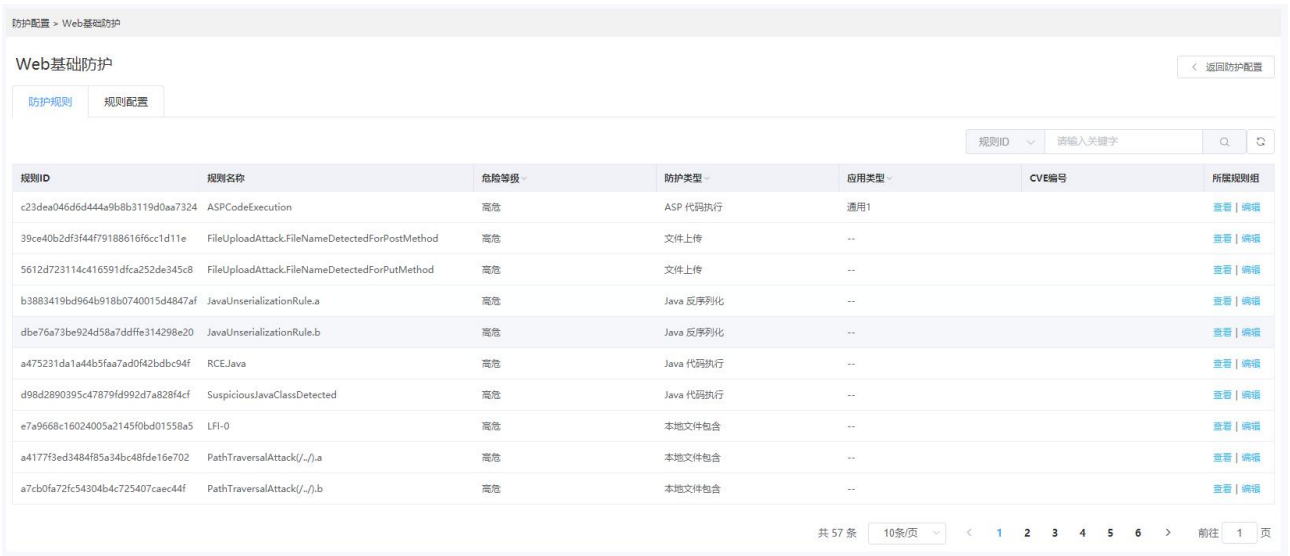
4.2.2.4. 查看内置防护规则

您可以在 Web 基础防护>防护规则页面，查询规则防护引擎中目前包含的所有防护规则。

操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 南京3 ，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置”页面定位到 Web 基础防护区域，在防护规则组项点击“前去配置”；

6. 进入“防护规则”页面，可以看到当前的规则引擎包含的规则列表；



规则列表中包含的参数如下：

配置项	说明
规则 ID	WAF 防护引擎中可唯一标识该规则的 ID。

规则名称	防护规则的描述信息。
危险等级	防护规则防护漏洞的危险等级，包括： • 高危 • 中危 • 低危
防护类型	表示规则防御的 Web 攻击类型。 包括 SQL 注入、XSS、机器人请求、目录穿越、Java 代码执行、PHP 代码执行、ASP 代码执行、通用代码执行、Java 反序列化、PHP 反序列化、本地文件包含、远程文件包含、文件上传、CSRF、SSRF、命令注入、信息泄露、模板注入、XML 实体注入、未知攻击。
应用类型	表示规则防护的 Web 应用类型。 包括通用、Dedecms、Wordpress、其他。
CVE 编号	防护规则对应的 CVE（Common Vulnerabilities & Exposures，通用漏洞披露）编号。对于非 CVE 漏洞，显示为空。

7. 其他相关操作，对于某条特定规则，您可以执行以下操作：

   1）查看：查看当前规则所属的规则组。

   2）编辑：将当前规则添加至某个自定义规则组。

4.2.3. CC 防护

网站域名接入云 WAF 后，您可以选择开启 CC 防护功能，为网站拦截针对页面请求的 CC 攻击。您也可以根据实际需求自定义 CC 安全防护的防护策略。

前提条件

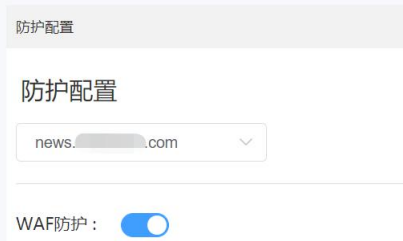
- 已开通 Web 应用防火墙（原生版）实例；
- 已完成网站域名接入。

使用限制

基础版不支持 CC 防护，请升级到更高版本使用。

操作步骤-CC 防护模式配置

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的  ，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。



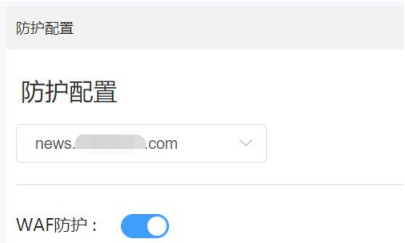
6. 在“防护配置”页面定位到 CC 防护区域，可以选择开启/关闭防护状态；同时可以直接选择防护模式，配置信息如下。

配置项	说明
状态	开启或关闭 CC 安全防护功能。
模式	要应用的防护模式。可选值： • **常规**：只针对特别异常的请求进行拦截，误杀较少。建议您在网站无明显流量异常时应用此模式，避免误杀。 • **紧急**：高效拦截 CC 攻击，可能造成较多误杀。当您发现有防护模式无法拦截的 CC 攻击，并出现网站响应缓慢，流量、CPU、内存等指标异常时，可以应用此模式。 • **自定义**：自定义 CC 防护可以通过精确匹配条件过滤访问请求的基础上，基于用户访问源 IP 或者 SESSION 频率定义访问频率限制条件，对于超过频率限制的访问进行处置，处置措施包括人机识别、JS 验证、阻断等。 策略配置方法，请参见设置自定义 CC 防护策略。 说明： ✓ 防护模式只能选择一种，不能同时开启。

操作步骤-自定义 CC 防护策略

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

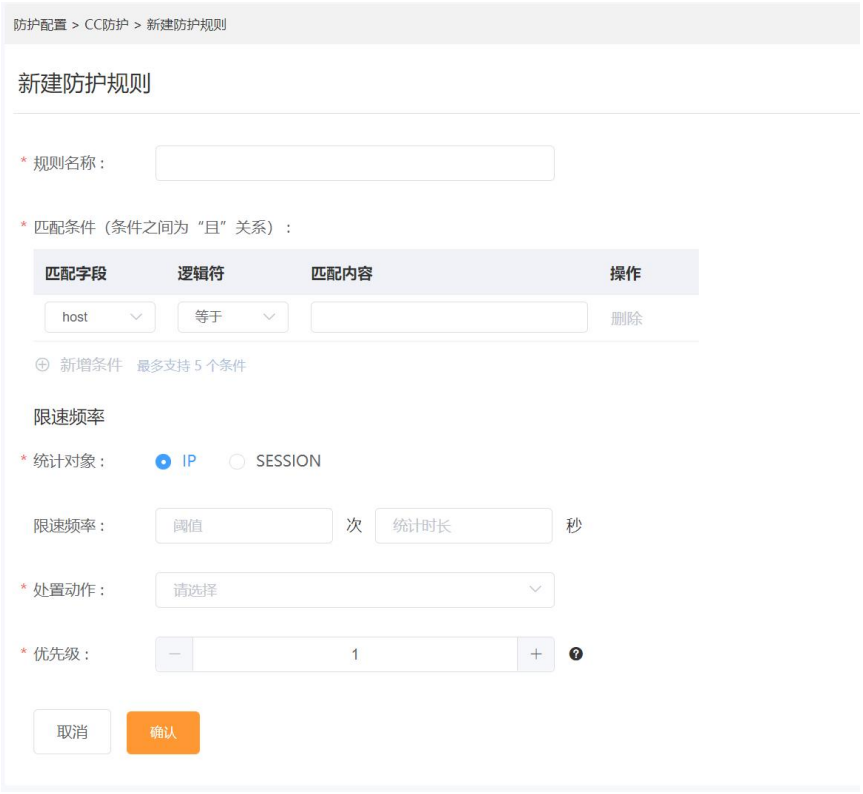
，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。



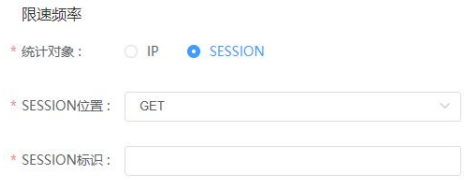
6. 在“防护配置”页面定位到 CC 防护区域，在自定义防护模式后方点击“前去配置”；

7. 进入 CC 防护自定义规则列表页，列表会展示已创建规则的相关信息，包括规则 ID/名称、匹配条件、限速频率、处置动作、优先级、规则状态、更新时间等；

8. 点击列表上方“新建防护规则”，进入规则配置页面，完成以下信息配置；



配置项	说明
规则名称	设置规则的名称。 规则名称用于标识当前防护规则，建议您使用有明确含义的名称。
匹配条件	设置访问请求需要匹配的条件（即特征）。单击新增条件可以设置最多 5 个条件。存在多个条件时，多个条件必须同时满足才算命中。 关于匹配条件的配置描述，请参见匹配条件字段说明。
频率设置	频率统计在匹配条件检测后生效，需要配置统计对象及限速频率。 统计对象为统计请求数量的依据，可选值如下： • IP：根据 IP 区分单个访问者。 • SESSION：根据会话区分单个访问者。对于 SESSION 模式，需要进一步设置 SESSION 信息。

	 SESSION 设置： • SESSION 位置：可选则 GET、POST、COOKIE • SEESION 标识：取值标识，通过配置唯一可识别 Web 访问者的某属性变量名（Key），系统讲根据此标识匹配到的内容识别访问者 限速频率为单个访问者在限速周期内最大可以正常访问的次数，如果超过该访问次数，WAF 则将根据配置的处置动作处理。配置项如下： • 统计时长（秒）：统计周期。 • 阈值（次）：统计时长内统计对象的允许数量，超过阈值，则触发频率限制。
处置动作	定义触发规则后执行的动作，可选值： • 观察 • 拦截 • 放行 • 验证码 • js 挑战 • 重定向 • 重置链接
优先级	代表该规则在 CC 防护模块儿中执行的优先级。 可输入 1～100 的整数，数字越大，代表这条规则的优先级越高。相同的优先级下，创建/更新时间越晚，优先级越高。

9. 点击“确认”，规则创建成功，成功后规则默认启用。您可以在规则列表中查看该规则。

10. 其他相关操作，对于已创建的规则，您可以执行以下操作：

    1）编辑：编辑自定义防护规则的名称、匹配条件、频率限制、处置动作、优先级等；

    2）删除：若不再使用某条规则，可对该规则进行删除；

    3）状态变更：可对每一条规则单独设置启用状态，若临时无须启用某条规则，可禁用该规则。

4.2.4. BOT 防护

网站域名接入云 WAF 后，您可以选择开启 BOT 防护功能。通过 BOT 防护配置，用户可以根据 BOT 会话行为特征设置 BOT 对抗策略，对 BOT 行为动作处理，保护网站核心业务安全。BOT 防护设置支持公开类型、自定义会话策略两大类防护策略。

- **公开类型**：云 WAF 提供已知公开的 BOT 大类，包括 Web 爬虫、扫描器、语言库等爬虫类型，用户可以根据自身需求对公开 BOT 类型设置防护状态及防护动作，WAF 将对命中公开类型的 BOT 请求进行相应处理。
- **自定义会话策略**：提供自定义协议特征、自定义会话特征两类防护策略，每种类型特征包含多个判定维度，用户可以根据实际业务情况设置协议特征规则状态、自定义会话策略，WAF 将根据命中防护策略的请求进行处理。

前提条件

- 已开通 Web 应用防火墙（原生版）实例；
- 已完成网站域名接入。

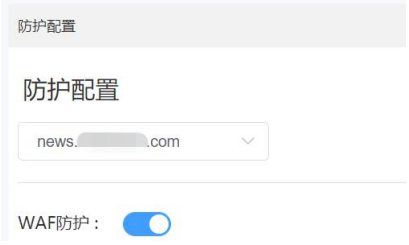
使用限制

基础版不支持 BOT 防护，请升级到更高版本使用。

操作步骤-BOT 防护模式配置

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。



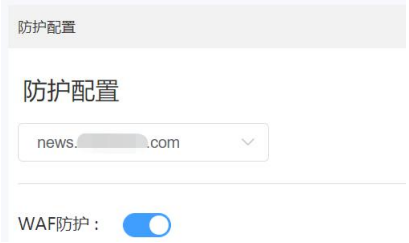
6. 在“防护配置”页面定位到 BOT 防护区域，可以选择开启/关闭防护状态。

配置项	说明
状态	开启或关闭 BOT 防护。
防护策略	BOT 支持三类防护策略设置。可选值： • **公开类型** • **自定义协议特征** • **自定义会话策略** 点击“前去配置”，可以进入到对应的策略配置页面进行配置。

操作步骤-策略配置

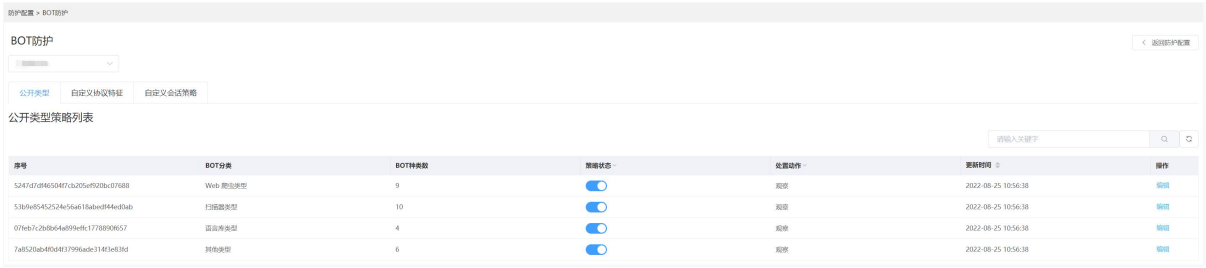
1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。



6. 在“防护配置”页面定位到 BOT 防护区域，在对应防护策略后方点击“前去配置”；
7. 进入 BOT 防护策略配置页面，通过切换防护类型选项卡，进入不同的策略配置页面进行配置。

1）**公开类型策略**：页面列表会展示系统已有规则的相关信息，包括 BOT 分类、BOT 种类数、处置动作、策略状态、更新时间等；用户可以选择开启或关闭某个分类策略的防护状态，并可以点击编辑，修改该规则的处置动作。



2）**自定义协议特征**：协议特征规则列表展示当前系统支持的防护规则，包括规则类型、规则名称/ID、处置动作、优先级、规则状态、更新时间等；用户可以选择开启或关闭某个规则的防护状态，并可以点击编辑，设置该规则的处置动作和优先级；

3）自定义会话策略：自定义会话特征规则列表展示当前用户已创建的规则，包括规则名称/ID、匹配条件、处置动作、优先级、规则状态、更新时间等；

4）用户点击“新建防护规则”，在规则配置页面，完成以下信息配置；

配置项	说明
规则名称	设置规则的名称。 规则名称用于标识当前防护规则，建议您使用有明确含义的名称。
匹配条件	设置访问请求需要匹配的条件（即特征）。单击新增条件可以设置最多 5 个条件。存在多个条件时，多个条件必须同时满足才算命中。 关于匹配条件的配置描述，请参见匹配条件字段说明。
处置动作	定义触发规则后执行的动作，可选值： • 观察 • 拦截 • 放行 • 验证码 • js 挑战 • 重定向 • 重置链接
优先级	代表该规则在 CC 防护模块儿中执行的优先级。 可输入 1～100 的整数，数字越大，代表这条规则的优先级越高。相同的优先级下，创建/更新时间越晚，优先级越高。

8. 对于已创建的自定义会话规则，可以在规则列表执行以下操作：

1）编辑：编辑自定义防护规则的名称、匹配条件、频率限制、处置动作、优先级等；

2）删除：若不再使用某条规则，可对该规则进行删除；

3）状态变更：可对每一条规则单独设置启用状态，若临时无须启用某条规则，可禁用该规则。

4.2.5. 精准访问控制

精准访问控制允许自定义访问控制规则，通过对请求路径、请求 URI、Cookie、请求参数、Header、referer、User-Agent 等多个特征进行条件组合，对访问请求进行特征匹配实现管控，有针对性的阻断各类攻击行为。

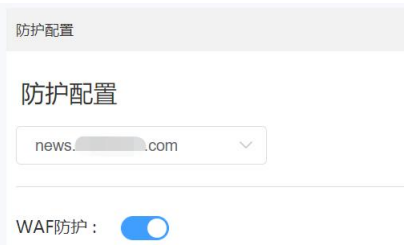
前提条件

- 已开通 Web 应用防火墙（原生版）实例；
- 已完成网站域名接入。

操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。



6. 在“防护配置”页面定位到精准访问控制区域，可以选择开启/关闭防护状态。点击“前去配置”；

7. 进入精准访问控制规则列表页，列表会展示已创建规则的相关信息，包括规则 ID/名称、匹配条件、处置动作、优先级、规则状态、过期时间、更新时间等；

8. 点击列表上方“新建防护规则”，进入规则配置页面，完成以下信息配置；

配置项	说明
规则名称	设置规则的名称。 规则名称用于标识当前防护规则，建议您使用有明确含义的名称。
匹配条件	设置访问请求需要匹配的条件（即特征）。单击新增条件可以设置最多 5 个条件。存在多个条件时，多个条件必须同时满足才算命中。 关于匹配条件的配置描述，请参见匹配条件字段说明。

处置动作	定义触发规则后执行的动作，可选值： • 观察 • 拦截 • 放行 • 验证码 • js 挑战 • 重定向 • 重置链接
过期时间	规则配置后，规则状态开启即生效。可通过设置过期时间，为该规则定义生效时间段。 过期时间可选： • 永久生效 • 限定日期：自定义设置失效日期
优先级	代表该规则在 CC 防护模块儿中执行的优先级。 可输入 1～100 的整数，数字越大，代表这条规则的优先级越高。相同的优先级下，创建/更新时间越晚，优先级越高。

9. 点击“确认”，规则创建成功，成功后规则默认启用。您可以在规则列表中查看该规则。

10. 其他相关操作，对于已创建的规则，您可以执行以下操作：

    1）编辑：编辑自定义防护规则的名称、匹配条件、处置动作、优先级、过期时间等；

    2）删除：若不再使用某条规则，可对该规则进行删除；

    3）状态变更：可对每一条规则单独设置启用状态，若临时无须启用某条规则，可禁用该规则。

4.2.6. IP 黑白名单

IP 黑白名单支持对经过云 WAF 防护域名的访问源 IP 进行黑白名单设置，来自该 IP 地址/IP 地址段的访问，云 WAF 将不会做任何检测，直接拦截/放行。

- IP 黑白名单设置，支持基于域名创建 IP 黑白名单规则；
- 支持添加 IPv4、IPv6 地址，支持添加 IP 地址段；
- IP 黑白名单模块的防护检测逻辑优先级高于其他防护模块；IP 黑白名单内部检测逻辑，白名单高于黑名单。

前提条件

- 已开通 Web 应用防火墙（原生版）实例；
- 已完成网站域名接入。

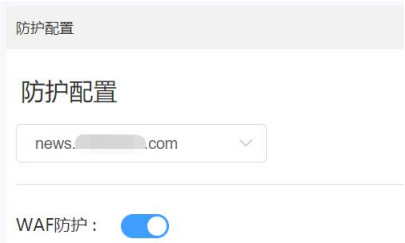
规格限制

- 不同实例版本支持添加的 IP 黑白名单规则数量不同，有关个版本规格的详细介绍，请参见产品规格。
- 若当前版本的 IP 黑白名单防护规则条数无法满足业务需求时，您可以通过购买规则扩展包或升级版本，以实现规则条数的扩容。一个规则扩展包包含 50 条 IP 黑白名单防护规则。

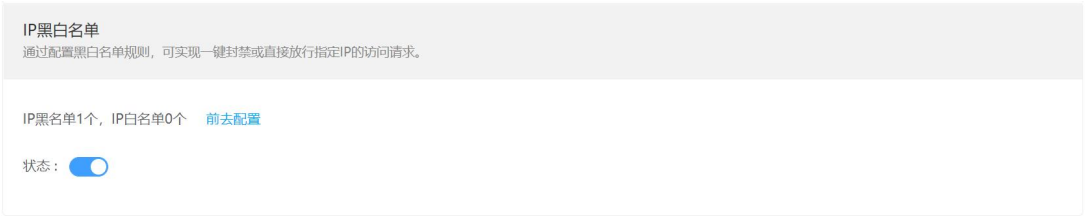
操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。

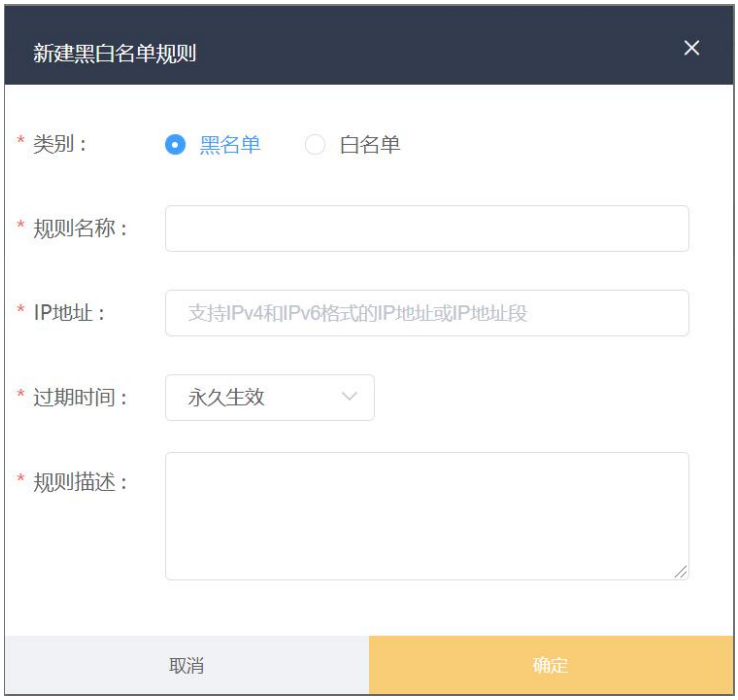


6. 在“防护配置”页面定位到 IP 黑白名单区域，可以选择开启/关闭防护状态。点击“前去配置”；



7. 进入精准访问控制规则列表页，列表会展示已创建规则的相关信息，包括规则 ID/名称、IP 地址、类别、规则状态、过期时间、更新时间、规则描述等；

8. 点击列表上方“新建黑白名单”，进入规则配置页面，完成以下信息配置；



配置项	说明
规则名称	设置规则的名称。 规则名称用于标识当前防护规则，建议您使用有明确含义的名称。
类别	定义该规则类型是黑名单或白名单。
IP 地址	添加 IP 地址/地址段，支持 IPv4 和 IPv6 格式的 IP 地址/地址段
过期时间	规则配置后，规则状态开启即生效。可通过设置过期时间，为该规则定义生效时间段。 过期时间可选： • 永久生效 • 限定日期：自定义设置失效日期
规则描述	可选参数，设置该规则的备注信息

9. 点击“确认”，规则创建成功，成功后规则默认启用。您可以在规则列表中查看该规则。

10. 其他相关操作，对于已创建的规则，您可以执行以下操作：

    1）编辑：编辑黑白名单规则的名称、名单类别、IP 地址/地址段、过期时间、规则描述等；

    2）删除：若不再使用某条规则，可对该规则进行删除；

    3）状态变更：可对每一条规则单独设置启用状态，若临时无须启用某条规则，可禁用该规则。

4.2.7. 地域访问控制

地域访问控制支持针对地理位置的黑名单封禁，可指定需要封禁的国家、地区，阻断该区域的来源 IP 的访问。

前提条件

- 已开通 Web 应用防火墙（原生版）实例；
- 已完成网站域名接入。

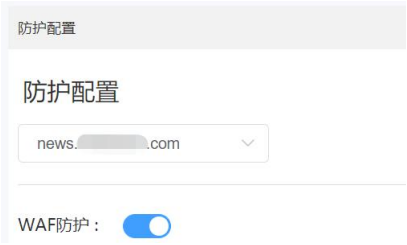
使用限制

基础版、标准版不支持自定义防护规则组，请升级到更高版本使用。

操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面；
5. 在“防护配置“页面上方，切换到要设置的域名。



6. 在“防护配置”页面定位到地域访问控制区域，可以选择开启/关闭防护状态，并查看当前已封禁的地域。点击“前去配置”；

7. 进入地域访问控制规则列表页，列表会展示已创建规则的相关信息，包括规则 ID/名称、封禁地域、规则状态、过期时间、更新时间、规则描述等；

8. 点击列表上方“新建防护规则”，进入规则配置页面，完成以下信息配置；

配置项	说明

规则名称	设置规则的名称。 规则名称用于标识当前防护规则，建议您使用有明确含义的名称。
地理位置	IP 访问来源的地理范围，可以选择“中国境内”和“境外”区域。支持多选。
过期时间	规则配置后，规则状态开启即生效。可通过设置过期时间，为该规则定义生效时间段。 过期时间可选： • 永久生效 • 限定日期：自定义设置失效日期
规则描述	可选参数，设置该规则的备注信息

9. 点击“确认”，规则创建成功，成功后规则默认启用。您可以在规则列表中查看该规则。

10. 其他相关操作，对于已创建的规则，您可以执行以下操作：

    1）编辑：编辑地域封禁规则的名称、封禁地理范围、过期时间、规则描述等；

    2）删除：若不再使用某条规则，可对该规则进行删除；

    3）状态变更：可对每一条规则单独设置启用状态，若临时无须启用某条规则，可禁用该规则。

支持封禁的地域

地域访问控制支持封禁的地域如下：

- **中国境内地区**

区域	省市自治区
华东地区	山东、江苏、安徽、浙江、福建、江西、上海
华南地区	广东、广西、海南
华中地区	湖北、湖南、河南
华北地区	北京、天津、河北、山西、内蒙古
西北地区	宁夏、新疆、青海、陕西、甘肃

西南地区	四川、云南、贵州、西藏、重庆
东北地区	辽宁、吉林、黑龙江
港澳台地区	台湾、香港、澳门

- **中国境外地区**

区域	国家（按英文首字母区分）
境外国家	A:安哥拉、阿富汗、阿尔巴尼亚、阿尔及利亚、安道尔共和国、安圭拉岛、安提瓜和巴布达、阿根廷、亚美尼亚、阿森松、澳大利亚、奥地利、阿塞拜疆 B：巴哈马、巴林、孟加拉国、巴巴多斯、白俄罗斯、比利时、伯利兹、贝宁、百慕大群岛、玻利维亚、博茨瓦纳、巴西、文莱、保加利亚、布基纳法索、缅甸、布隆迪 C：喀麦隆、加拿大、开曼群岛、中非共和国、乍得、智利、哥伦比亚、刚果、库克群岛、哥斯达黎加、古巴、塞浦路斯、捷克 D：丹麦、吉布提、多米尼加共和国 E：厄瓜多尔、埃及、萨尔瓦多、爱沙尼亚、埃塞俄比亚 F：斐济、芬兰、法国、法属圭亚那 G：加蓬、冈比亚、格鲁吉亚、德国、加纳、直布罗陀、希腊、格林纳达、关岛、危地马拉、几内亚、圭亚那 H：海地、洪都拉斯、匈牙利 I：冰岛、印度、印度尼西亚、伊朗、伊拉克、爱尔兰、以色列、意大利、科特迪瓦

	J：牙买加、日本、约旦 K：柬埔寨、哈萨克斯坦、肯尼亚、韩国、科威特、吉尔吉斯坦 L：老挝、拉脱维亚、黎巴嫩、莱索托、利比里亚、利比亚、列支敦士登、立陶宛、卢森堡 M：马达加斯加、马拉维、马来西亚、马尔代夫、马里、马耳他、马里亚那群岛、马提尼克、毛里求斯、墨西哥、摩尔多瓦、摩纳哥、蒙古、蒙特塞拉特岛、摩洛哥、莫桑比克 N：纳米比亚、瑙鲁、尼泊尔、荷属安的列斯、荷兰、新西兰、尼加拉瓜、尼日尔、尼日利亚、朝鲜、挪威 O：阿曼 P：巴基斯坦、巴拿马、巴布亚新几内亚、巴拉圭、秘鲁、菲律宾、波兰、法属玻利尼西亚、葡萄牙、波多黎各 Q：卡塔尔 R：留尼旺、罗马尼亚、俄罗斯 S：圣卢西亚、圣文森特岛、东萨摩亚(美)、西萨摩亚、圣马力诺、圣多美和普林西比、沙特阿拉伯、塞内加尔、塞舌尔、塞拉利昂、新加坡、斯洛伐克、斯洛文尼亚、所罗门群岛、索马里、南非、西班牙、斯里兰卡、圣卢西亚、圣文森特、苏丹、苏里南、斯威士兰、瑞典、瑞士、叙利亚 T：塔吉克斯坦、坦桑尼亚、泰国、多哥、汤加、特立尼达和多巴哥、突尼斯、土耳其、土库曼斯坦 U：乌干达、乌克兰、阿拉伯联合酋长国、英国、美国、乌拉圭、乌兹别克斯坦

	V：委内瑞拉、越南 Y：也门、南斯拉夫 Z：津巴布韦、扎伊尔、赞比亚

4.2.8. 防敏感信息泄露

网站域名接入 Web 应用防火墙后，您可以选择开启防敏感信息泄露功能，并配置防敏感信息泄露规则，可对网页中的敏感信息或指定的 HTTP 响应码页面进行过滤或拦截。

前提条件

- 已开通 Web 应用防火墙（原生版）实例。
- 已完成网站域名接入。

使用限制

基础版和标准版不支持防敏感信息泄露功能，请升级到更高版本使用。

操作步骤

1. 登录天翼云控制中心。
2. 单击控制中心顶部的，选择区域。
3. 单击控制中心左上角的“服务列表”，选择“安全>Web 应用防火墙（原生版）”。
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面。

5. 在“防护配置”页面上方的“域名选择”下拉框，切换到要设置的域名。

6. 在“防护配置”页面定位到“防敏感信息泄露”模块，可以选择开启/关闭防护状态。

7. 点击防护规则右侧的“前去配置”，进入防敏感信息泄露规则页面。

8. 单击“新建防护规则”，在弹出的对话框中，配置防敏感信息泄露规则。

参数说明如下：

配置项	说明
规则名称	设置规则的名称。 规则名称用于标识当前防护规则，建议您使用有明确含义的名称。
匹配条件	选择需要在响应信息中检测的敏感信息类型，包括敏感信息、响应码、关键字。 ● 敏感信息：用户的个人身份信息，包括身份证号、电话号码、电子邮箱等。 ● 响应码：指定的 HTTP 响应码，比如 401、402、403 等。 ● 关键字：自定义需要检测关键字。
匹配内容	根据所选匹配条件，对应不同的内容。 ● 敏感信息：包括身份证号、电话号码、电子邮箱等。

	● 响应码：选择特定的 HTTP 请求状态码。 ● 关键字：需要手动输入匹配的关键字。
防护路径	需要防护的 URL 的路径。
执行动作	选择在响应信息中检测到敏感信息后系统执行的动作。 ● 观察：仅通过日志记录匹配到的页面和内容，不进行拦截。 ● 信息脱敏-全部屏蔽：对匹配到的内容，将被全部进行脱敏展示。 ● 信息脱敏-自定义范围：选择该项，还需要配置“显示”或“屏蔽”具体的范围。 ● 拦截：拦截匹配到的页面和内容，并向发起请求的客户端返回拦截响应页面。
规则描述	可选项。设置规则的描述信息。

9. 单击“确定”，规则创建成功，成功后规则默认启用。您可以在规则列表中查看该规则。

相关操作

对于已创建的防敏感信息泄露规则，您可以执行以下操作：

- 状态变更：可对每一条规则单独设置状态，若临时无须启用某条规则，可禁用该规则。
- 编辑：可根据需要单击规则所在行的“编辑”，编辑自定义防护规则的所有参数。
- 删除：若不再使用某条规则，可对该规则进行“删除”。

4.2.9. 网页防篡改

网站域名接入 Web 应用防火墙后，您可以选择开启网页防篡改功能，通过设置网页防篡改规则，锁定需要保护的网站页面。当被锁定的页面在收到请求时，返回已设置的缓存页面，预防源站页面内容被恶意篡改。

前提条件

- 已开通 Web 应用防火墙（原生版）实例。
- 已完成网站域名接入。

使用限制

基础版不支持网页防篡改功能，请升级到更高版本使用。

操作步骤

1. 登录天翼云控制中心。
2. 单击控制中心顶部的，选择区域。
3. 单击控制中心左上角的“服务列表”，选择“安全>Web 应用防火墙（原生版）”。
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“域名选择”下拉框，切换到要设置的域名。

6. 在“防护配置”页面定位到“网页防篡改”模块，可以选择开启/关闭防护状态。

7. 点击防护规则右侧的“前去配置”，进入网页防篡改防护规则页面。
8. 单击“新建防护规则”，在弹出的对话框中，配置网页防篡改防护规则。

参数说明如下：

配置项	说明
域名	此处不可修改。可返回防护规则页面，在页面右上角进行域名切换。
规则名称	设置规则的名称。 规则名称用于标识当前防护规则，建议您使用有明确含义的名称。
网页地址	输入需要防篡改的网站静态页面的路径。 格式为“协议名://域名或 IP 地址[:端口号]/[路径名/.../文件名]”，例如“https://www.example.com:5443/index.html”。

	路径不支持通配符或参数，支持输入端口。
规则描述	可选项。设置规则的描述信息。

9. 单击“确定”，规则创建成功，成功后规则默认启用。您可以在规则列表中查看该规则。

相关操作

对于已创建的防敏感信息泄露规则，您可以执行以下操作：

- 状态变更：可对每一条规则单独设置状态，若临时无须启用某条规则，可禁用该规则。
- 编辑：可根据需要单击规则所在行的“编辑”，编辑自定义防护规则的所有参数。
- 删除：若不再使用某条规则，可对该规则进行“删除”。

4.2.10. Cookie 防篡改

网站域名接入 Web 应用防火墙后，您可以选择开启 Cookie 防篡改功能，开启后，WAF 可通过 Cookie 中的字段对网页进行完整性校验保护。

前提条件

- 已开通 Web 应用防火墙（原生版）实例。
- 已完成网站域名接入。

使用限制

基础版和标准版不支持 Cookie 防篡改功能，请升级到更高版本使用。

操作步骤

1. 登录天翼云控制中心。
2. 单击控制中心顶部的  ，选择区域。
3. 单击控制中心左上角的“服务列表”，选择“安全>Web 应用防火墙（原生版）”。
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面。

5. 在“防护配置”页面上方的“域名选择”下拉框，切换到要设置的域名。

6. 在“防护配置”页面定位到“Cookie 防篡改”模块，可以选择开启/关闭防护状态。

7. 单击配置详情右侧的“前去配置”，进入 Cookie 防篡改配置页面，配置相关参数。

参数说明如下：

配置项	说明
防护模式	默认为“Cookie 签名”，且不支持修改。 新增 Cookie 字段，字段值为待防护 Cookie 字段的签名，请求会对签名值进行完整性校验，若发生篡改则进行处置。
Cookie 密钥	用于生成防篡改签名值的密钥（AES256），您可以自定义或者“快速生成密钥”。
Cookie 兼容时间	生成配置后为了兼容之前未带 Cookie 签名的请求，可以设置生效时间。默认为当前时间。
IP 校验	默认为“是”，表示除了对于防护 Cookie 值校验，同时也会对访问 IP 进行校验，同一 Cookie 值更换 IP 后无法通过校验。 修改为“否”，将仅对 Cookie 值进行校验。
Cookie 字段名称	单击“新增 Cookie 字段”，新增一个 Cookie 字段。 ● HttpOnly：Cookie 属性字段，用于避免客户端脚本访问该 Cookie，勾选后可防止客户端脚本读取 Cookie，防范 XSS 攻击。

	• Secure：Cookie 属性字段，勾选后仅支持通过 Https 发送 Cooike，防范采用 Http 协议发起的政击。
处置动作	选择 WAF 检测到篡改行为后，系统执行的动作。 • 拦截：拦截请求。 • 观察（仅记录）：仅通过日志记录请求，不进行拦截。

8. 单击“确认”，完成配置。

4.2.11. 隐私屏蔽

网站域名接入 Web 应用防火墙后，您可以选择开启隐私屏蔽功能。通过配置隐私屏蔽规则，可以避免用户的密码等隐私信息出现在事件日志中。

前提条件

- 已开通 Web 应用防火墙（原生版）实例。
- 已完成网站域名接入。

使用限制

基础版不支持隐私屏蔽功能，请升级到更高版本使用。

操作步骤

1. 登录天翼云控制中心。
2. 单击控制中心顶部的  ，选择区域。
3. 单击控制中心左上角的“服务列表”，选择“安全>Web 应用防火墙（原生版）”。
4. 在左侧导航栏中，选择“防护配置”，进入防护配置页面。

5. 在“防护配置”页面上方的“域名选择”下拉框，切换到要设置的域名。

6. 在“防护配置”页面定位到“隐私屏蔽”模块，可以选择开启/关闭防护状态。

7. 点击防护规则右侧的“前去配置”，进入隐私屏蔽规则页面。

8. 单击“新建防护规则”，在弹出的对话框中，配置隐私屏蔽规则。

参数说明如下：

配置项	说明
域名	此处不可修改。可返回防护规则页面，在页面右上角进行域名切换。

规则名称	设置规则的名称。 规则名称用于标识当前防护规则，建议您使用有明确含义的名称。
网页地址	输入网站静态页面路径。 路径格式为： 协议名://域名或 IP 地址[:端口号]/[路径名/.../文件名]。 例如“https://www.example.com/index.html”。 路径不支持通配符或参数，支持输入端口。
字段范围	设置屏蔽的字段。 ● Cookie：根据 Cookie 区分的 Web 访问者。 ● Header：自定义 HTTP 首部。 ● Body：请求体参数。 ● URI：URI 参数。
屏蔽关键词	根据字段范围设置屏蔽关键词，被屏蔽的关键词将不会出现在日志中。 默认已勾选银行卡、手机、身份证等关键词，也可以单击“自定义屏蔽关键词正则表达式”手动输入正则表达式，根据正则表达式对匹配的数据进行隐私屏蔽。
规则描述	可选项。设置规则的描述信息。

9. 单击“确定”，规则创建成功，成功后规则默认启用。您可以在规则列表中查看该规则。

相关操作

对于已创建的防敏感信息泄露规则，您可以执行以下操作：

- 状态变更：可对每一条规则单独设置状态，若临时无须启用某条规则，可禁用该规则。
- 编辑：可根据需要单击规则所在行的“编辑”，编辑自定义防护规则的所有参数。
- 删除：若不再使用某条规则，可对该规则进行“删除”。

4.2.12. 匹配条件字段说明

在进行云 WAF 的防护配置时，其中 Web 基础防护白名单、CC 防护、BOT 防护、精准访问控制均涉及定义规则匹配条件。本文具体描述了规则匹配条件中支持使用的字段及其释义。

什么是匹配条件、匹配动作

在进行云 WAF 的防护配置时，您可以自定义 Web 基础防护白名单、自定义 CC 防护规则、自定义 BOT 防护会话策略、自定义精准访问策略，自定义规则由匹配条件与匹配动作构成。在创建规则时，通过设置匹配字段、罗基夫和响应的匹配内容定义匹配条件，并针对符合匹配条件的访问请求设置相应的动作。

- **匹配条件**

匹配条件包含匹配字段、逻辑符、匹配内容。每一条自定义规则中最多允许设置 5 个匹配条件组合，且各个条件间是“与”的逻辑关系，即访问请求必须同时满足所有匹配条件才算命中该规则，并执行相应的匹配动作。

- **匹配动作**

防护白名单中的匹配动作表示不检测模块，其他自定义防护策略的匹配动作表示处置动作，具体配置方式请参见各防护模块配置说明。

支持匹配的字段

匹配字段	适用的逻辑符	字段描述
请求参数值	包含、等于、正则匹配	请求的参数 value，包括 query 和 form，如 /?p=123 中的 123
请求参数名	包含、等于、正则匹配	请求的参数 key，包括 query 和 form，如 /?p=123 中的 p
Cookie	包含、等于、正则匹配	请求的 Cookie 值
请求路径	包含、等于、正则匹配	请求的路径，不包含域名和参数，未解码
请求 URI	包含、等于、正则匹配	请求的 URI，带参数
请求头值	包含、等于、正则匹配	请求 header 的值

请求头名	包含、等于、正则匹配	请求 header 的名字
请求方法	包含、等于、正则匹配	请求方法
请求大小	大于等于、小于等于	请求的大小
请求 Host	包含、等于、正则匹配	请求 Host 头的值
请求 referer 头	包含、等于、正则匹配	请求 referer 头的值
请求 User-Agent	包含、等于、正则匹配	请求 User-Agent
请求体	包含、等于、正则匹配	请求体

4.3. 安全总览

Web 应用防火墙（原生版）安全总览页面向您展示当前 WAF 实例中所有域名的防护统计记录、请求趋势图表以及攻击事件的分布状态等，帮助您了解网站业务的整体安全状态。

前提条件

- 已开通 Web 应用防火墙（原生版）实例;
- 已完成网站域名接入并正常防护。

查询条件

在总览页面上方，设置要查询的域名和查询时间，查询总览数据。查询设置说明：

- 域名：默认展示全部已接入 WAF 防护的域名相关的数据。您可以选择只查询某个域名的数据。
- 时间：系统支持展近 7 天的数据。查询时间支持选择昨天、今天、近 3 天、近 7 天或自定义时间（近 7 天内的时间范围）。

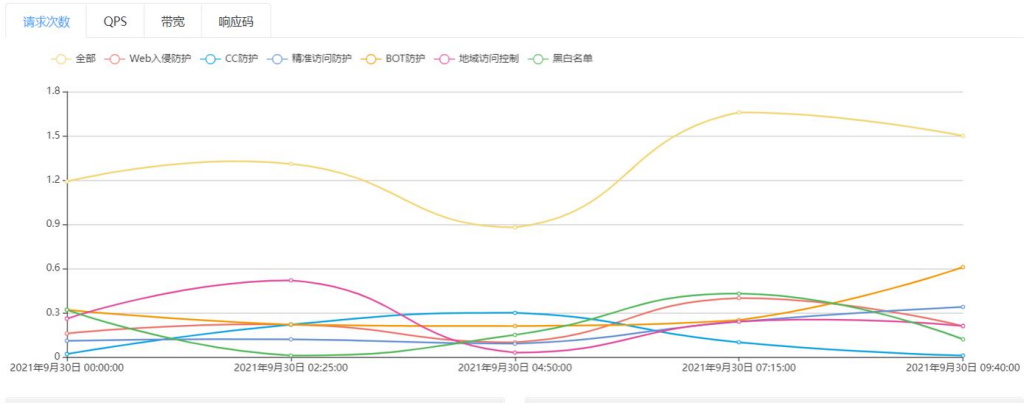
防护统计数据

防护统计数据展示了网站域名收到的全部请求次数、全部攻击次数和触发了不同防护模块的防护次数，防护模块包括 Web 入侵防护、CC 防护、精准访问防护、BOT 防护、地域访问控制、IP 黑白名单。

单击全部攻击次数，可以跳转至防护事件列表页，查看统计数据对应的详细攻击事件记录。

请求分析图表

请求分析图表展示请求趋势图，包含请求次数、QPS、带宽、响应码随时间变化的趋势。



不同趋势数据的说明如下：

- **请求次数**：包含全部请求次数、全部攻击次数、Web 入侵防护次数、CC 安全防护次数、精准访问防护次数、地域访问控制防护次数、Bot 防护次数、黑白名单防护次数随时间的变化趋势。
- **QPS**：包含全部请求 QPS、全部攻击 QPS、Web 入侵防护 QPS、CC 安全防护 QPS、精准访问防护 QPS、地域访问控制 QPS、Bot 防护 QPS、黑白名单 QPS 随时间的变化趋势。单击趋势图右上角的均值图/峰值图，可以选择显示 QPS 均值或 QPS 峰值数据。
- **带宽**：包含入方向带宽和出方向带宽（单位：bps）随时间的变化趋势。
- **响应码**：包含 WAF 返回给客户端、源站返回给 WAF 的 5XX、405、499、302、444 等异常响应码的数量随时间的变化趋势。

攻击事件分布

攻击事件分布可以展示域名受到攻击的分布、以及各类排行分析图。

各图表具体含义如下：

- **事件分布**：可查看指定域名被攻击的类型的数量占比

- **受攻击域名 TOP10**：受攻击统计次数 Top 10 的域名以及各域名收到攻击次数的占比
- **攻击源 IP TOP10**：攻击统计次数 Top 10 的攻击源 IP 以及各源 IP 发出攻击次数的占比
- **受攻击 URL TOP10**：受攻击统计次数 Top 10 的 URL 以及各 URL 受攻击次数的占比
- **攻击来源区域 TOP10**：攻击次数 Top 10 的地区以及来源各地区发起攻击次数的占比
- **业务异常监控**：业务异常的 Top 10 防护网站。可以查看业务异常为“404”、“500”、“502”的防护网站

4.4. 管理防护事件

云 WAF 将将攻击防护的事件详情记录在事件报表中，用户可在事件列表中查看攻击时间、攻击 IP、攻击类型、攻击 URL、地理位置、处置动作、命中规则 ID、攻击详情等。具体功能如下：

- 支持查看近 7 天内的防护事件，查询时间支持选择昨天、今天、近 3 天、近 7 天或自定义时间（近 7 天内的时间范围）。
- 提供防护事件多级查询，筛选条件包括域名、事件类型、攻击 IP、处置动作、攻击 URL、规则 ID、请求 UUID。
- 支持将列表数据下载到本地。

前提条件

- 已开通 Web 应用防火墙（原生版）实例；
- 已完成网站域名接入并正常防护。

操作步骤

1. 登录天翼云控制中心；
2. 单机管理控制台右上方的 

，选择地域；
3. 在控制台列表页，选择“安全>Web 应用防火墙（原生版）”；
4. 在左侧导航栏中，选择“防护事件”，进入防护事件页面；

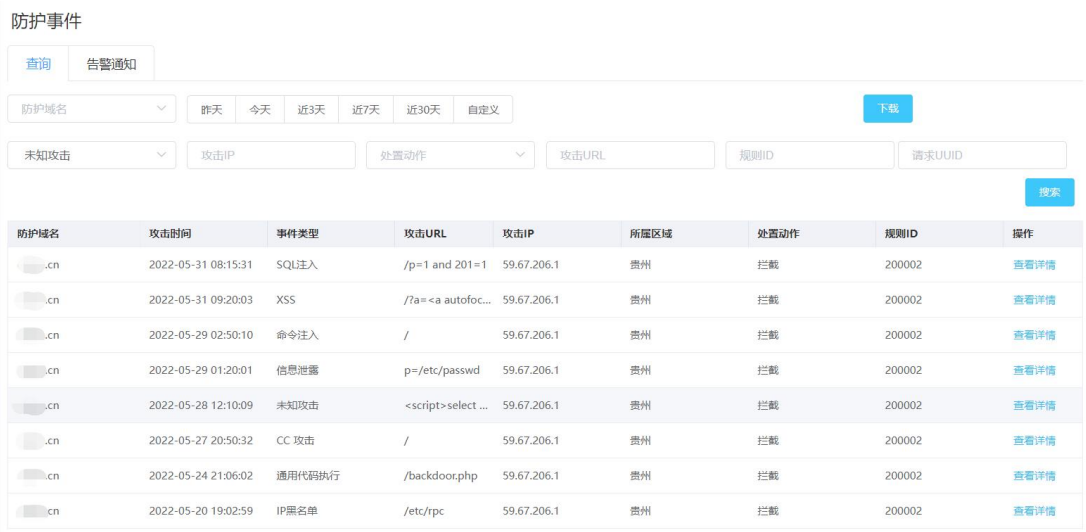
5. 在防护事件列表上方，可以对事件进行筛选条件设置，支持设置多项匹配条件；

条件字段参数说明：

参数名称	参数说明
域名	选择想要查看的域名，支持全部域名或某个域名
时间范围	可查看“昨天”、“今天”、“近 3 天”、“近 7 天”或者近 7 天内自定义时间范围内的防护日志
事件类型	发生的攻击类型。默认为全部攻击类型，也可以根据需要，选择攻击类型查看攻击日志信息
攻击 IP	Web 访问者的公网 IP 地址，默认为全部，也可以根据需要输入攻击者 IP 地址查看攻击日志信息
处置动作	防护配置中设置的防护动作，包含：观察、拦截、放行、验证码、js 挑战、重定向、重置链接
攻击 URL	攻击的防护域名的 URL
规则 ID	攻击触发的防护规则 ID
请求 UUID	请求对应的唯一标识

6. 筛选条件设置完成后，点击“搜索”，筛选后的结果将在列表中展示；可以点击“查看详情”，查看完整日志。

注意：单次查询控制台最多支持返回 1000 条事件数据。当筛选条件范围过大时，可能存在返回数据不全问题，建议查询时缩小时间范围。



攻击日志字段说明:

参数名称	参数说明
http_host	请求头中的 host 字段值，即域名；
action	规则动作，包括观察、拦截、验证码、JS 挑战、重定向等
attack_type	发生的攻击类型，包括 SQL 注入、XSS、BOT、目录穿越、命令注入、模板注入、CC 攻击、IP 黑名单、自定义精准攻击、信息泄露、文件上传等等
request_uri	攻击的防护域名的 URL
remote_addr	客户端 IP 地址，即攻击 IP
attack_area	客户端攻击 IP 所属地区
time_local	服务器时间，即攻击时间
rule_id	攻击触发的防护规则 ID
unique_id	请求对应的唯一标识

4.5. 报表管理

Web 应用防火墙（原生版）支持生成日报、周报、月报，并支持订阅报表，订阅后系统会在报表生成后将报表发送至您的邮箱。

前提条件

- 已购买 Web 应用防火墙（原生版）实例。
- 已完成网站域名接入并开启防护。

配置报表

1. 登录天翼云控制中心。
2. 单击控制中心顶部的  ，选择区域。
3. 单击控制中心左上角的“服务列表”图标，选择“安全>Web 应用防火墙（原生版）”。
4. 在左侧导航栏中，选择“报表管理”，进入报表管理页面。

5. 在“报表管理”页面右上角，单击“报表配置”，进入报表配置页面。

配置如下参数：

参数名称	说明
报表生成	WAF 支持生成日报、周报、月报。根据需要进行开启，可多选。 ● 日报：每天 00:00:00 生成前一日的报表。 ● 周报：每周一 00:00:00 生成前一周的报表。 ● 月报：每月 1 日 00:00:00 生成前一月的报表。

参数名称	说明
报表订阅	该页面自动列出当前账号及其全部子账号。 勾选需要订阅报表的账号，报表生成后，系统会自动发送报表至订阅账号的邮箱。

6. 单击“确认”，完成报表配置。

查看及下载报表

报表保留周期如下表所示，建议您定期下载报表，以满足等保测评以及审计的需要。

报表类型	保留周期
日报	报表保存 180 天，约半年
周报	报表保存 52 周，约一年
月报	报表保存 24 个月，约两年

请参考如下步骤查看及下载报表：

1. 登录天翼云控制中心。
2. 单击控制中心顶部的  ，选择区域。
3. 单击控制中心左上角的“服务列表”，选择“安全>Web 应用防火墙（原生版）”。
4. 在左侧导航栏中，选择“报表管理”，进入报表管理页面。
5. 在目标报表所在行的“操作”列，单击“预览”即可查看报表内容，单击“下载”即可将报表下载到本地。

报表中主要包含如下信息：

- 防护基本信息：包括使用的 WAF 版本、配额信息、用户账号、报表生成时间、防护范围、报表统计范围等。

- 数据统计信息：包括防护域名、请求次数和已发现的攻击次数。
- 攻击防护统计：按防护类型统计各防护事件的次数以及防护事件的详细信息。
- 防护 Top 统计：包括攻击类型、受攻击域名 TOP10、攻击源 IP TOP10、受攻击 URL TOP10、攻击来源区域 TOP10 等。

5. 最佳实践

5.1. WAF 接入配置最佳实践

将网站域名接入 Web 应用防火墙（原生版），能够帮助您的网站防御 OWASP 常见 Web 攻击和恶意 CC 攻击流量等，避免网站遭到入侵导致数据泄露，全面保障您网站的安全性和可用性。您可以参考本文中的接入配置最佳实践，在各类场景中使用 WAF 更好地保护您的网站。

说明：

域名接入 WAF 后，WAF 作为一个反向代理存在于客户端和服务器之间，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。当前云 WAF 提供 CNAME 接入模式，可以防护通过域名访问的 Web 应用/网站，包括 Web 业务服务器部署在天翼云上、非天翼云或线下的域名。

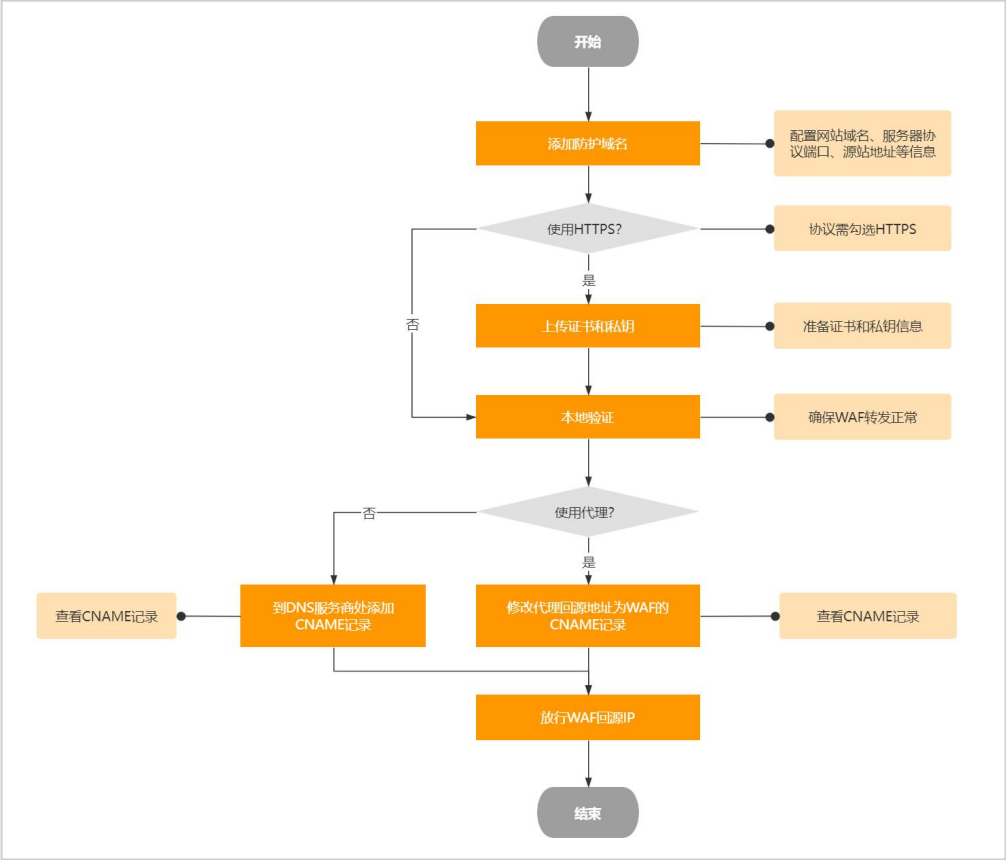
网站接入 WAF 准备工作

在将网站业务接入 WAF 前，您需要完成以下准备工作：

- 所需接入的网站域名清单，包含网站的源站服务器 IP、端口信息等。
- 所接入的网站域名必须已完成备案。
- 如果您的网站支持 HTTPS 协议访问，您需要准备相应的证书和私钥信息，一般包含扩展名为 PEM/CRT/CER 的证书文件、扩展名为 PEM/KEY 的私钥文件，文件内容均需为 PEM 编码格式。
- 具有网站 DNS 域名解析管理员的账号，用于修改 DNS 解析记录将网站流量切换至 WAF。
- 推荐在将网站业务接入前，完成压力测试。
- 检查网站业务是否已有信任的访问客户端（例如，监控系统、通过内部固定 IP 或 IP 段调用的 API 接口、固定的程序客户端请求等）。在将业务接入后，需要将这些信任的客户端 IP 加入白名单。

接入配置流程

在 WAF 控制台添加需要防护的网站域名后，通过修改域名的 DNS 解析设置，将网站流量解析到 WAF，使访问网站的流量经过 WAF 并受到 WAF 的防护。WAF 将过滤和处理后的请求转发回该域名的源站服务器。



1. 添加域名：配置域名、协议、源站等相关信息，配置流程详见添加域名。

2. 放行 WAF 回源 IP 段：WAF 使用特定的回源 IP 段将经过防护引擎检测后的正常流量转发回网站域名的源站服务器。网站接入 WAF 进行防护时，您需要设置源站服务器的安全软件或访问控制策略，放行 WAF 回源 IP 段的入方向流量。配置流程详见放行 WAF 回源 IP 段。

3. 本地验证：添加域名后，在本地电脑上搭建简易的模拟环境，验证网站流量转发设置已经生效，避免转发设置未生效时修改域名的 DNS 解析设置，导致业务访问异常。配置流程详见本地验证。

4. 修改域名 DNS：若域名在接入 WAF 前未使用代理，则需要到该域名的 DNS 服务商处，修改域名的 DNS 解析配置，将网站的流量解析到 WAF；若域名在接入 WAF 前使用了代理（DDoS 高防、CDN 等），

则需要将使用的代理类服务（DDoS 高防、CDN 等）的回源地址修改为的目标域名的“CNAME”值。配置流程详见修改域名 DNS 解析。

> **注意**：如果在添加域名配置时，提示添加域名重复无法添加，建议您检查是否已在当前账号或其他账号的 WAF 实例中添加过相同的域名，如果确实存在，您需要删除造成冲突的域名配置记录后再进行添加。

5.2. 防护配置最佳实践

网站接入 WAF 实例后，您可以按照以下推荐防护配置对已接入的网站域名进行防护。

Web 基础防护

一般情况下，建议选用**拦截**模式，并选用**正常规则组**防护策略。

> **说明**：业务接入 WAF 防护一段时间后（一般为 2~3 天），如果出现网站业务的正常请求被 WAF 误拦截的情况，您可以通过设置自定义规则组的方式提升 Web 防护效果。相关操作，请参见自定义防护规则组，提升 Web 攻击防护效果。

CC 防护

业务正常运行时，建议采用**常规**防护模式。

由于 CC 防护的防护-紧急模式可能产生一定量的误拦截，如果您的业务为 App 业务或 Web API 服务，不建议您开启防护-紧急模式。如果使用 CC 安全防护的正常模式仍发现误拦截现象，建议您使用精准访问控制功能放行特定类型请求。

说明：业务接入 WAF 防护一段时间后（一般为 2-3 天），可以通过分析业务日志数据（例如，访问 URL、单个 IP 访问 QPS 情况等）评估单个 IP 的请求 QPS 峰值，提前通过自定义 CC 攻击防护配置限速策略，避免遭受攻击后的被动响应和临时策略配置。

BOT 防护

当您的业务经常受到爬虫骚扰或面临数据泄露、被篡改的风险，针对防护需求，建议您为网站开启 BOT 防护功能。BOT 防护设置支持公开类型、自定义会话策略两大类防护策略。

- **公开类型**：云 WAF 提供已知公开的 BOT 大类，包括 Web 爬虫、扫描器、语言库等爬虫类型，用户可以根据自身需求对公开 BOT 类型设置防护状态及防护动作，WAF 将对命中公开类型的 BOT 请求进行相应处理。
- **自定义会话策略**：提供自定义协议特征、自定义会话特征两类防护策略，每种类型特征包含多个判定维度，用户可以根据实际业务情况设置协议特征规则状态、自定义会话策略，WAF 将根据命中防护策略的请求进行处理。

精准访问控制

当攻击源 IP 比较分散时，可以通过分析防护事件日志，使用精准访问控制提供的丰富字段和逻辑条件组合，灵活配置访问控制策略实现精准防护，有效降低误拦截。

- 支持 URL、Cookie、Referer、User Agent、Params、Header 等 HTTP 常见参数和字段的条件组合。

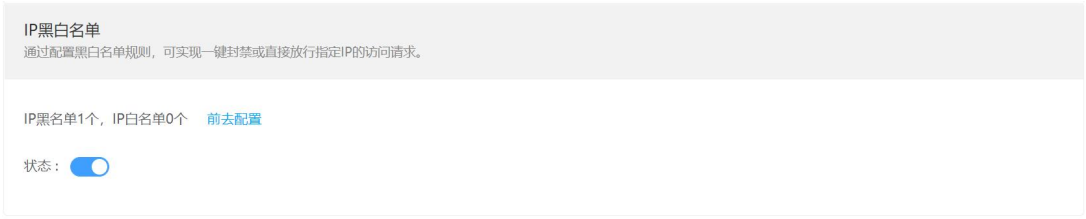
- 支持包含、等于、大于等于、小于等于、正则匹配等逻辑条件，设置阻断或放行等策略。

说明：

- 当您配置了自定义 CC 防护，其可能会产生误拦截，建议您通过防护事件日志分析找出攻击特征，配合使用精准访问防护策略实现精准拦截；
- 支持对创建的规则设置失效时间及优先级。

IP 黑白名单

您可以将网站业务已有信任的访问客户端（例如，监控系统、通过内部固定 IP 或 IP 段调用的 API 接口、固定的程序客户端请求等），设置成 IP 白名单；同时可封禁与业务不相关的 IP 地址和地址段。



说明：

- 支持添加 IPv4、IPv6 地址，支持添加 IP 地址段； 支持对创建的规则设置失效时间；
- IP 黑白名单模块的防护检测逻辑优先级高于其他防护模块；IP 黑白名单内部检测逻辑，白名单高于黑名单。

说明：

- 支持添加 IPv4、IPv6 地址，支持添加 IP 地址段； 支持对创建的规则设置失效时间；
- IP 黑白名单模块的防护检测逻辑优先级高于其他防护模块；IP 黑白名单内部检测逻辑，白名单高于黑名单。

地域访问控制

地域访问控制支持针对地理位置的黑名单封禁，可指定需要封禁的国家、地区，阻断该区域的来源 IP 的访问。

说明：

- 支持封禁境内、境外的地域；
- 支持针对创建的防护规则定义失效时间。

以上配置完成后，建议您进行配置准确性检查和验证测试，检查项包括域名是否填写正确、是否备案、接入配置协议/端口是否与实际一致、WAF 前是否有配置其他代理、源站填写的 IP 是否是真是的服务器 IP、回源算法是否与预期一致、证书信息是否准确上传、证书是否合法完整等等。

所有的检测测试均通过后，再进行逐个域名修改 DNS 解析记录，将网站业务流量切换至 WAF，避免业务异常。

5.3. Web 基础防护规则引擎配置最佳实践

Web 基础防护基于内置的防护规则集，自动为网站防御 SQL 注入、XSS、文件包含、远程命令执行、目录穿越、文件上传、CSRF、SSRF、命令注入、模板注入、XML 实体注入攻击等通用的 Web 攻击。

规则防护引擎

云 WAF 的 Web 基础防护规则引擎默认开启，所有接入云 WAF 防护的网站业务，默认都受到 Web 基础防护规则引擎的检测和防护。

Web 基础防护规则引擎基于天翼云持续优化的高质量攻击检测规则集，帮助网站防御各种常见的 Web 应用攻击。您可以根据业务防护需要，在防护规则组的维度，设置规则引擎采用哪些防护规则。WAF 按照防护严格程度，内置了三套规则组供选用：

- 中等规则组：默认选用该规则组。

- 宽松规则组：如需减少误拦截，可选用该规则组。
- 严格规则组：如需提高攻击检测命中率，可选用该规则组。

您也可以自定义防护规则组，相关操作，请参见自定义防护规则组。

防护模式

检测发现攻击请求时，对攻击请求执行的操作。可选以下两种模式：

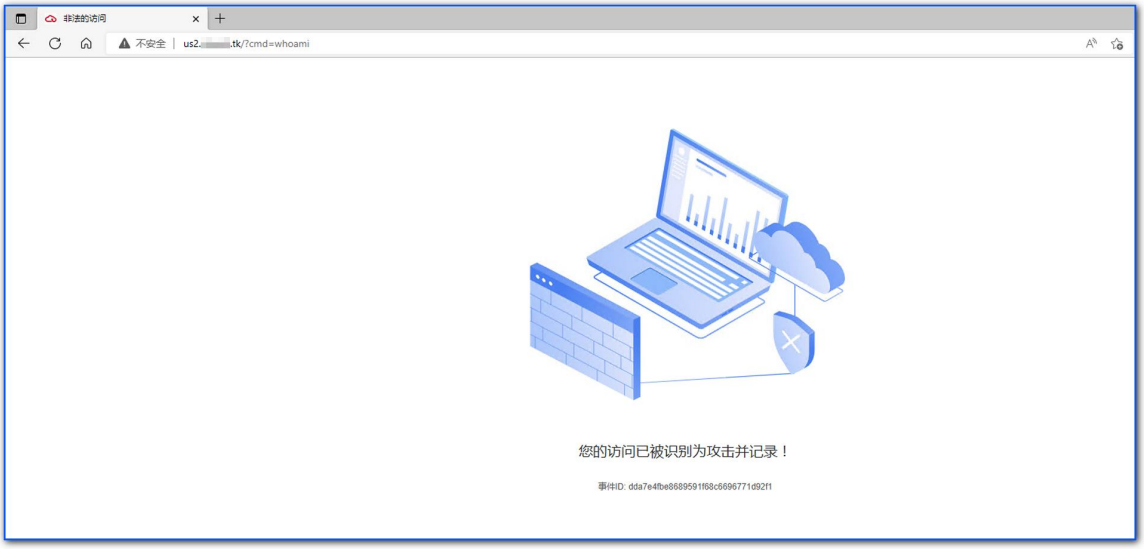
- 拦截：检测到攻击行为后，直接阻断攻击请求，并记录攻击日志；
- 观察：检测到攻击行为后，不阻断攻击，仅记录攻击日志。

配置建议

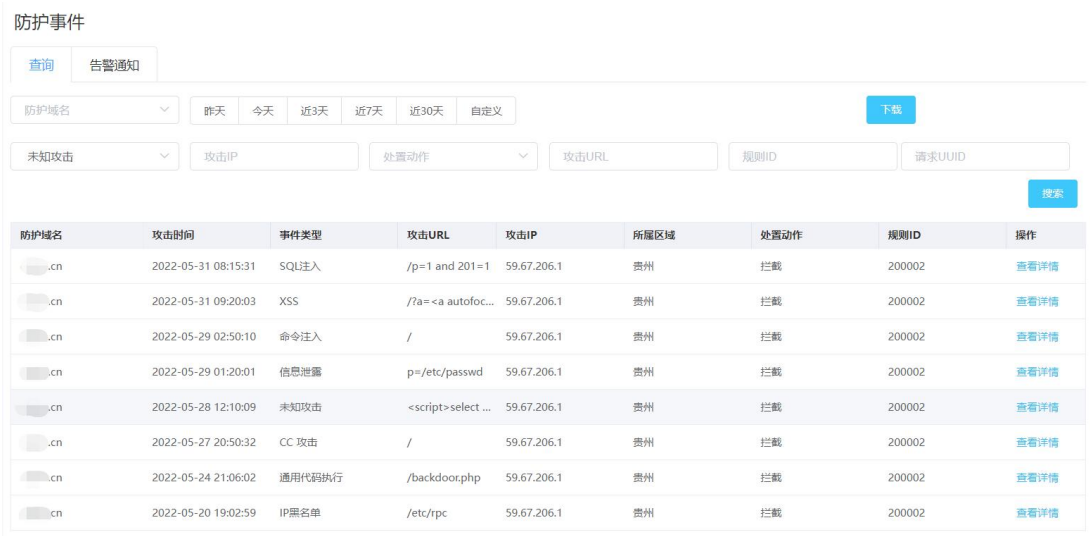
- 如果您对自己的业务流量特征还不完全清楚，建议先切换到“观察”模式。一般情况下，建议您观察一至两周，然后根据攻击日志分析网站访问情况。
  - ✓ 如果没有发现任何正常业务流量被拦截的记录，则可以切换到“拦截”模式启用正常防护。
  - ✓ 如果发现攻击日志中存在正常业务流量被拦截的记录，建议调整防护等级或者设置规则白名单来避免正常业务的误拦截。配置流程详见规则白名单。
- 业务操作方面应注意以下问题：
  - ✓ 正常业务的 HTTP 请求中尽量不要直接传递原始的 SQL 语句、JAVA SCRIPT 代码。
  - ✓ 正常业务的 URL 尽量不要使用一些特殊的关键字（UPDATE、SET 等）作为路径，例如：“www.example.com/abc/update/mod.php?set=1”。
  - ✓ 如果业务中需要上传文件，不建议直接通过 Web 方式上传超过 50M 的文件，建议使用对象存储服务或者其他方式上传。

防护效果

开启 Web 基础防护功能后，模拟常见命令注入攻击测试域名，WAF 拦截了此条攻击，拦截效果如下：



同时，您可以在防护事件页面，查看攻击的防护日志。



5.4. CC 攻击防护最佳实践

当客户发现网站处理速度下降，网络带宽占用过高时，很有可能已经遭受 CC 攻击，此时可查看 Web 服务器的访问日志或网络连接数量，如果访问日志或网络连接数量显著增加，则可确定遭受 CC 攻击，可以利用 WAF 阻断 CC 攻击，保障网站业务的正常运行。

CC 攻击防护策略

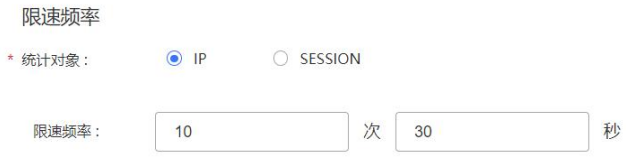
在大规模 CC 攻击中，单台傀儡机发包的速率往往远超过正常用户的请求频率。针对这种场景，直接对请求源设置限速规则是最有效的办法。推荐您自定义 CC 防护策略，对具体的访问源配置限速策略，具体操作，请参见 CC 防护。

在实际场景中，您需要根据自身业务需求调整防护路径和触发防护的阈值，并选择合适的处置动作，以达到更有针对性、更精细化的防护效果。例如，为了预防登录接口受到恶意高频撞库攻击的影响，您可以配置登录接口的地址（示例：使用 path 字段作为匹配条件，将匹配内容设置为/login.php），并设置 30 秒内超过 10 次请求则进行拦截。

限速配置

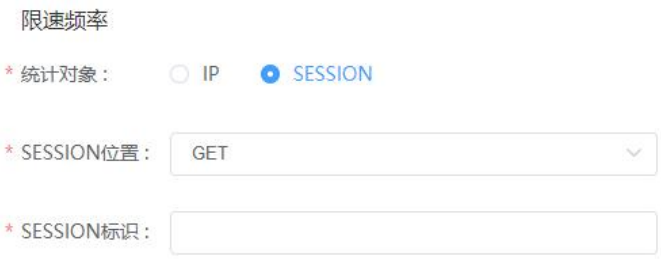
- **基于 IP 的限速配置**

当 WAF 与客户端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。



- **基于 session 的频率限制**

当黑客控制多台肉鸡，模仿普通访问者，共用同一 IP，或通过代理频繁更换源 IP 持续向站点发起请求，通过 IP 进行频率限制无法准确识别恶意访问源。因此建议通过配置 session，通过会话区分单个访问者，实现更细粒度的限速。



SESSION 配置项：

- SESSION 位置：可选则 GET、POST、COOKIE；

- SEESION 标识：取值标识，通过配置唯一可识别 Web 访问者的某属性变量名（Key），系统讲根据此标识匹配到的内容识别访问者。

6. 常见问题

6.1. 计费购买类

6.1.1. 计费常见问题

Q：同一个账号可以购买多个 WAF 原生版实例吗？

A：天翼云 Web 应用防火墙（原生版）是全球级服务，从产品防护原理上来说，一个 WAF 实例就可以防护所有区域的 Web 业务，但是考虑不同地域之间的网络转发效率，选择业务就近区域的 Web 防护实例对业务进行防护，能够显著的提升 Web 业务的可用性，例如北京的 Web 业务选择北京地区资源池防护实例进行防护，会比选择上海资源池的防护实例拥有更快的业务访问速度，故建议用户选择就近地域的资源实例进行购买，同一个账号在同一个区域只能购买一个 WAF 实例，同一个账号下可以在不同地域购买多个实例，每一个实例对应一个主套餐版本。

在同一个地域购买 WAF 实例后，如果该地域的 Web 业务防护需求因业务发展超出所购买实例的性能上线，您可以在业务需要的时候，按需升级版本或购买资源扩展包对实例的防护性能进行扩展，从而满足业务发展的需求。

Q：WAF 实例到期后，还能防护域名吗？

A：购买的 WAF 实例到期后如未按时续费，公有云平台会提供一定的保留期。

- 保留期内，平台会冻结 WAF 服务，用户配置的各类防护策略将不再生效，云 WAF 只转发流量。
- 保留期满，用户若仍未续费，平台会清除实例资源，用户所添加域名的所有配置将会被删除，同时云 WAF 将不再转发业务流量，若用户未及时将 DNS 指回服务器源站 IP，否则网站业务流量将无法正常转发。

Q：WAF 原生版实例可以降低版本和规格吗？

A：WAF 原生版实例不支持降级，同时已绑定的资源扩展包也不支持单独退订。如您需要降低当前规格，你可以先退订当前的 WAF 实例，再重新购买较低版本的 WAF。

Q：Web 应用防火墙是否支持自动续订?

A：支持。您可以在购买套餐的同时勾选自动续订，也支持在使用过程中，在订单中心中设置自动续订。

Q：不同版本的 WAF 规格差异是什么?

A：Web 应用防火墙（原生版）根据支持防护的业务规模以及提供的防护功能不同，产品实例主套餐具体分为基础版、标准版、企业版、旗舰版四个版本。各版本详细规格描述见下方表格所示。

分类	功能点	基础版	标准版	企业版	旗舰版
套餐基础信息	适用场景	适合个人网站用户	适用于中小型网站的标准防护	适用中大型网站防护	适用于大型及超大型复杂业务网站防护
	业务 QPS 峰值	100QPS/实例	3000QPS/实例	5000QPS/实例	10000QPS/实例
	支持一级域名个数	1 个/实例	2 个/实例	5 个/实例	8 个/实例
	支持所有防护域名个数	10 个/实例	20 个/实例	50 个/实例	80 个/实例
	泛域名防护	×	√	√	√
	IPv6 防护	×	×	√	√
	HTTP/HTTPS 非标准端口防护	不支持 仅支持 80、443	√	√	√
	支持防护端口数量	2 个/实例	20 个/实例	30 个/实例	60 个/实例
	域名接入方式	CNAME	CNAME	CNAME	CNAME
基础安全防护	规则白名单	×	√，20 条/域名	√，50 条/域名	√，100 条/域名

分类	功能点	基础版	标准版	企业版	旗舰版
	Web 基础规则防护引擎	√，仅支持默认规则组的防护	√，支持自定义	√，支持自定义	√，支持自定义
	自定义防护规则组个数	×	10 个/实例	20 个/实例	30 个/实例
	0Day 漏洞虚拟补丁	√	√	√	√
	IP 黑白名单	×	200 条/实例	500 条/实例	1000 条/实例
	地域封禁	×	×	√，50 条/实例	√，100 条/实例
	自定义精准防护策略	×	√，100 条/实例	√，200 条/实例	√，500 条/实例
	CC 防护（包括紧急模式）	×	√	√	√
	自定义 CC 防护规则	×	100 条/实例	200 条/实例	500 条/实例
高级安全防护	公开 BOT 类型防护	×	√	√	√
	BOT 协议特征防护	×	√	√	√
	BOT 自定义会话特征防护	×	√，100 条/实例	√，200 条/实例	√，500 条/实例
	数据统计分析	√	√	√	√
	敏感信息保护	×	×	√，50 个/实例	√，50 个/实例
	网页防篡改	×	√，20 条/域名	√，50 条/域名	√，100 条/域名
	Cookie 防篡改	×	×	√，50 个/实例	√，50 个/实例
	隐私屏蔽	×	√，20 条/域名	√，50 条/域名	√，100 条/域名

Q：Web 应用防火墙是如何计算并限制域名个数的？

A：域名数量有两项限制，一是域名总数限制，二是支持的所属一级域名的个数限制。

- 域名总数为一级/二级/三级等单域名和泛域名的总数。例如，基础版支持防护 10 个域名，则可以添加 10 个子域名或泛域名，也可以添加 1 个一级域名和 9 个与其相关的子域名或泛域名。
- 同时主套餐版本及域名扩展包还有所属一级域名个数的限制，以基础版仅支持 1 个一级域名为例，若用户已经添加 example.com（或其子域名 a.example.com）进行防护，此时系统已识别 1 个所属的一级域名（即 example.com）。当添加 test.com（或其子域名 a.test.com）进行防护时，则会提示数量限制，用户需要购买域名扩展包，才能添加其他的主域名或其子域名。

Q：若当前版本包含的域名个数不够用时，如何处理？

A：若当前版本包含的域名个数不够用时，您可以购买域名扩展包，或者直接升级当前实例版本。

1 个域名扩展包支持 10 个域名，其中支持添加 1 个新的一级域名。

Q：续费时是否可同时变更 Web 应用防火墙版本或规格？

A：续费时您只能为当前的 WAF 实例版本规格进行续费，增加使用时长。续费时不能同时变更 WAF 的规格。您可以在续费完成后，对 WAF 实例版本进行升级。

Q：资源扩展包购买上限是什么？

A：为了保证用户的账户安全，避免出现恶意购买等情况，WAF 服务为每个用户设置了资源扩展包的购买上限。请您根据业务需要按需订购。

当前 Web 应用防火墙提供域名扩展包、业务扩展包及规则拓展包三类扩展包：

- 域名扩展包：1 个域名扩展包支持 10 个域名，其中支持添加 1 个一级域名。域名扩展包订购上限为 500 个。
- 业务扩展包：1 个业务扩展包包含 1000QPS。业务扩展包订购上限是 30 个。

- 规则扩展包：1 个规则扩展包包含 50 条防护规则/域名，当前仅适用 IP 黑白名单防护模块。规则扩展包订购上限是 1000 个。

Q：Web 应用防火墙（原生版）是否支持按需计费？

A：当前 Web 应用防火墙（原生版）不支持按需计费。

Q：Web 应用防火墙（原生版）有促销折扣吗？

A：当前 Web 应用防火墙（原生版）可以享受 8 折优惠。

注意：促销折扣与包年折扣不同享，取低者进行计费。若您一次性下单 1 年的标准版套餐，常规情况下可享受包年折扣 85 折，但促销期间将按照 8 折计费。若您一次性下单 3 年的标准版套餐，则会按照常规的包年折扣 5 折计费。

Q：基础版是否支持购买资源扩展包？

A：不支持，基础版仅面向个人网站用户使用，基础版中默认支持 10 个防护域名、100QPS/实例、2 个防护端口以及默认规则组的防护，相关配置已能够满足个人网站用户使用，若存在需要购买资源扩展包的场景，建议用户购买标准版及以上的版本，以便为用户的 Web 业务提供更完善的安全防护。用户可在产品信息中将所使用的版本升级到更高版本，标准版、企业版、旗舰版都可支持购买资源扩展包。

Q：在使用期间购买了资源扩展包，资源到期时间是何时？

A：资源扩展包购买后与主套餐绑定，资源到期时间与主套餐一致。

Q：购买的资源扩展包，支持单独退订吗？

A：不支持。资源扩展包购买后与主套餐绑定，不支持单独退订。

Q：退订重购后，原实例的配置数据可以保留吗？

A：用户退订后在 15 天内重新购买实例时，仅当新实例版本等于或高于旧实例时，可恢复原有配置。当重新购买时距离退订已超过 15 天，原资源已释放且配置数据已删除，则无法恢复。

Q：如何选择带宽扩展包?

A：购买业务扩展包时，您需要测算接入 WAF 的所有站点的日常入方向和出方向流量的峰值，确保您选购的 WAF 所对应的业务 QPS 峰值限制大于入、出方向总流量峰值中较大的值。你可通过防火墙、交换机等流量设备对 Web 业务中的 80、443、8443 等常见 Web 端口流量进行统计，将相关业务端口的流量进行累加，从而得出访问 WAF 站点的流量。

注意：

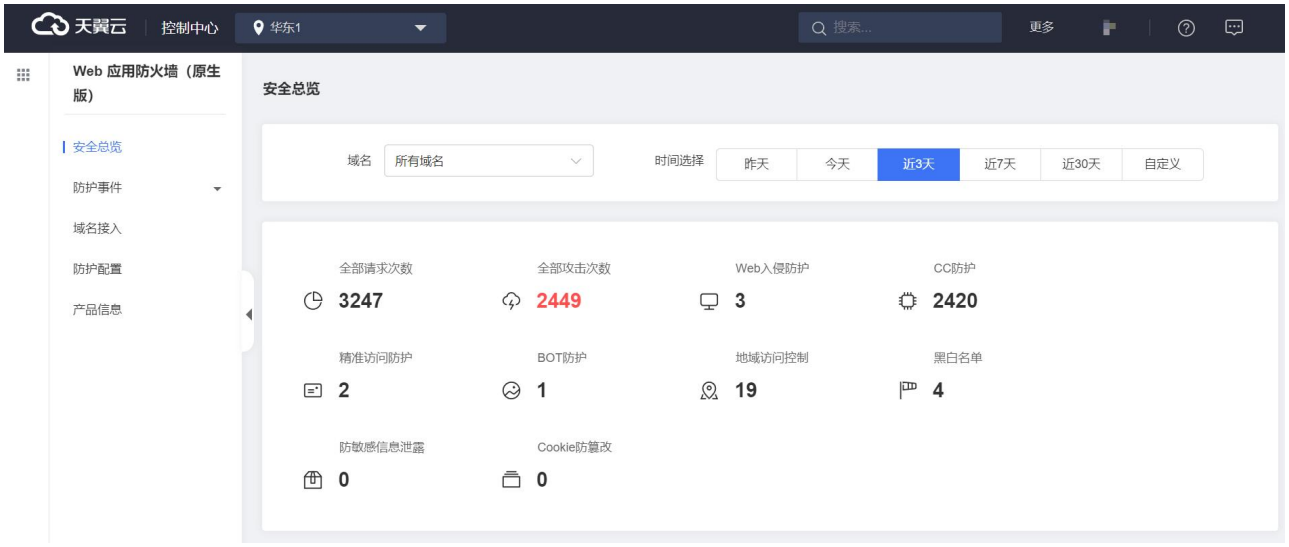
因流量存在波动性，在不同时间访问 Web 应用的流量会出现不同的峰值，您在购买业务扩展包时，需要统计一天中入方向流量及出方向流量的最大值，从而确定你所需要购买的业务扩展包。通常在业务访问量较大时，易出现流量峰值。

6.1.2. 如何查看当前购买产品的产品规格

购买、续订、升级扩容后可以通过产品信息页面查看所购买产品的规格，同时个人消息中心以及用户绑定的手机也能够收到相关的购买成功提示短信。

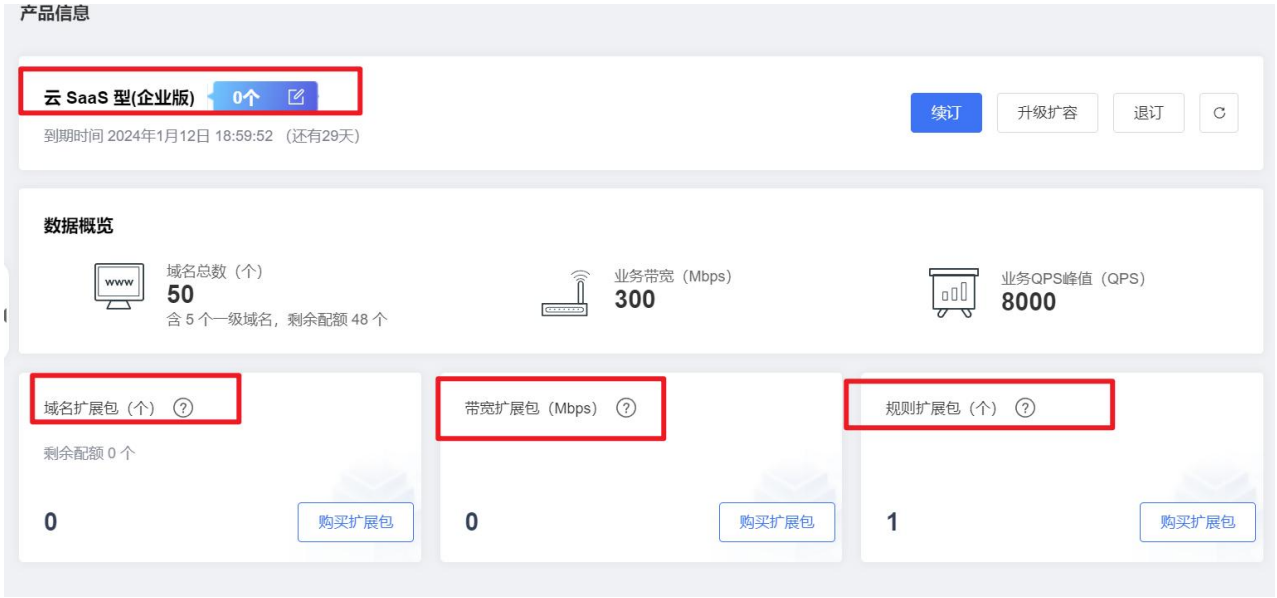
查看购买后的 WAF 规格方式如下：

1. 登录 WAF 控制台页面。



2. 选择左侧“产品信息”菜单栏。

3. 查看当前产品购买规格信息。


产品信息
云 SaaS 型(企业版)
0个
到期时间 2024年1月12日 18:59:52 （还有29天）
续订
升级扩容
退订
数据概览
域名总数（个）
50
含 5 个一级域名，剩余配额 48 个
业务带宽（Mbps）
300
业务QPS峰值（QPS）
8000
域名扩展包（个）
剩余配额 0 个
0
购买扩展包
带宽扩展包（Mbps）
0
购买扩展包
规则扩展包（个）
1
购买扩展包

注意：

购买成功后需要等待一段时间相关规格才能刷新，预计等到 1-2 分钟左右。

6.2. 网站接入类

6.2.1. 域名/端口相关

Q：为什么要进行域名备案？

A：为了规范互联网信息服务活动，促进互联网信息服务健康有序发展，根据国务院令第 292 号《互联网信息服务管理办法》和工信部令第 33 号《非经营性互联网信息服务备案管理办法》规定，国家对经营性互联网信息服务实行许可制度，对非经营性互联网信息服务实行备案制度。未取得许可或者未履行备案手续的，不得从事互联网信息服务，否则就属于违法行为。详细法规如下：

根据 《非经营性互联网信息服务备案管理办法》第五条规定：在中华人民共和国境内提供非经营性互联网信息服务，应当依法履行备案手续。未经备案，不得在中华人民共和国境内从事非经营性互联网信息服务。本办法所称在中华人民共和国境内提供非经营性互联网信息服务，是指在中华人民共和国境内的组织或个人利用通过互联网域名访问的网站或者利用仅能通过互联网 IP 地址访问的网站，提供非经营性互联网信息服务。第十九条规定：互联网接入服务提供者应当记录其接入的非经营性互联网信息服务提供者的备案信息。

详情见工信部备案管理系统《非经营性互联网信息服务备案管理办法》（信息产业部令第 33 号）。

Q：Web 应用防火墙（原生版）对于用户添加的防护端口个数有限制吗？

A：根据订购的版本不同，防护端口数量有上限。基础版、标准版、企业版、旗舰版的端口上限分别是 4 个、20 个、30 个、60 个。

Q：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？

A：WAF 的防护对象是域名，如果多个域名使用了同一个源站对外提供服务，需要将多个域名都接入 WAF 实现所有域名的防护。

Q：多个端口的服务器，如果某个端口不需要 WAF 防护，如何处理？

A：防护网站是通过域名+端口方式接入 WAF 进行防护的。在添加防护域名时，您只需要配置域名+需要防护的端口即可。防护网站接入 WAF 后，流量不会通过其他端口转发到 WAF。

Q：Web 应用防火墙支持配置泛域名吗？

A：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。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。

Q：域名添加到 WAF 后，是否可以修改？

A：防护域名添加到 WAF 后，不能修改，建议您删除原域名后再重新添加待防护的域名。

Q：Web 应用防火墙支持哪些非标准端口

A： WEB 应用防火墙除了可以防护标准端口外，还支持非标准端口的防护。不同版本的云 WAF 实例支持添加的端口数量不同，具体可见下表所示。

服务版本	端口分类	HTTP 协议端口范围	HTTPS 协议端口范围
基础版	标准端口	80、8080	443、8443
标准版	标准端口	80、8080	443、8443
	非标准端口	81、82、83、84、86、87、88、89、97、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7070、7071、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8686、8800、8888、8889、8999、	4443、5443、6443、7443、8553、8663、9443、9553、9663、18980

		9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、9999、10000、10001、10080、12601、28080、33702、48800	
企业版	标准端口	80、8080	443、8443
	非标准端口	81、82、83、84、86、87、88、89、97、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7070、7071、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、9999、10000、10001、10080、12601、28080、33702、48800	4443、5443、6443、7443、8553、8663、9443、9553、9663、18980
旗舰版	标准端口	80、8080	443、8443
	非标准端口	81、82、83、84、86、87、88、89、97、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、	4443、5443、6443、7443、8553、8663、9443、9553、9663、18980

		7022、7023、7024、7025、7026、7070、7071、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、9999、10000、10001、10080、12601、28080、33702、48800	

6.2.2. 证书配置相关

Q：为什么需要导入证书？

A：证书指主要指 Https 访问请求所使用的证书，通过使用 https 的证书能够保证用户请求的安全性，证书的主要原理是通过对用户请求通过第三方颁发的可信证书中的公钥对会话进行加密和签名从而保证用户本身的信息以及用户所访问服务器的可信性，服务器端接受到用户通过公钥加密发送的请求和签名后，再通过私钥进行解密，从而验证用户本身的可信性，而 WAF 需要导入所防护域名的证书和私钥，从而完成对客户请求的认证，以及通过 https 的安全请求方式将用户的请求转发回源站。故在使用过程中，需要 Web 业务管理员将 Web 服务的证书及对应的私钥导入到 WAF 中，从而实现客户对 Web 业务的安全访问。

Q：配置泛域名时，如何选择证书？

A：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。

并且泛域名与证书必须是同级匹配，例如您的泛域名是*.b.example.com，则泛域名证书必须为*.b.example.com，不能是*.example.com 或*.a.b.example.com。

Q：如何更新已绑定域名的证书？

A：登录 Web 应用防火墙管理控制台，在左侧导航栏选择“域名接入”，进入域名列表页。定位到需要更新证书的域名，点击“详情”进入网站详情信息页，点击“协议及端口”后的“设置”，在弹出的对话框中点击“证书更新”，即可重新填写证书内容或上传新的证书文件。

Q：如何将非 PEM 编码格式的证书转换为 PEM 编码格式？

A：当前 WAF 仅支持 PEM 编码格式的证书，如果证书为非 PEM 编码格式，请参考下表将本地证书转换为 PEM 格式，再上传。

格式类型	转换方式
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

6.2.3. 服务器配置相关

Q：当配置多个源站时，如何负载？

A：如果您配置了多个源站 IP 地址，WAF 支持使用轮询、IP Hash 的方式对访问请求进行负载均衡。您可以根据需要自定义负载均衡算法。

Q：如何通过 WAF 实现 HTTPS 访问？

A：在添加网站域名时，需选择 HTTPS 协议及端口，这样用户即可通过 HTTPS 协议发送访问请求。当您的网站不支持 HTTPS 回源时，您务必要开启 HTTP 回源选项，这样 WAF 将会通过 HTTP 80 端口将请求转发给源站。这样您可在无须改动源站服务器的前提下，通过 WAF 实现 HTTPS 访问，帮助您降低网站的负载损耗。

Q：如何强制客户端使用 HTTPS 请求访问网站？

A：当您想要提高网站访问的安全性，可以开启 HTTPS 强制跳转功能，此时所有客户端的 HTTP 请求都将强制转换为 HTTPS 请求，并默认跳转至 443 端口。

Q：WAF 原生版是否支持 HTTP 2.0 协议？

A：WAF 原生版暂不支持 HTTP 2.0 协议。

Q：域名接入时，源站 IP 可以填写云主机的内网 IP 吗？

A：不可以。当前 WAF 原生版通过公网进行回源，不支持直接填写内网 IP。

Q：WAF 原生版是否支持配置多个源站 IP？

A：支持。当前 1 个域名支持最多配置 20 个源站 IP。

Q：WAF 原生版是否支持添加 IPv6 的源站地址？

A：支持。当前 WAF 原生版支持 IPv4/IPv6 双栈防护，针对同一域名可以同时提供 Ipv6 和 Ipv4 的流量防护。

Q：若防护网站在 WAF 前开启了其他代理服务，WAF 原生版是否支持自定义配置客户端 IP 的判定方式？

A：支持。当防护网站 WAF 前开启了代理服务，说明 WAF 收到的业务请求来自其他代理服务转发，而非客户端直接发起，WAF 支持进一步配置自定义客户端 IP 判定策略，保证获取到真实的客户端 IP。

6.3. 防护配置类

6.3.1. 防护配置常见问题

Q：Web 基础防护支持哪几种防护等级？

A：Web 基础防护默认可以选择三个等级的防护规则组，分别为正常、宽松和严格。用户也可根据业务需求，自定义创建防护规则组，移除经常误报的防护规则。配置详情请参见设置防护规则引擎。

- 正常：中等宽松规则组，该组规则综合考虑误报和漏报策略检测情况，选择均衡的规则策略进行匹配，一般情况下，该种策略为默认推荐规则，建议用户选择正常策略。
- 宽松：宽松规则组，该规则组更关注精准攻击拦截度，对于疑似攻击行为的访问请求将会认定为安全从而放行，如需减少误拦截，可选用该规则组。

- 严格：严格规则组，该规则组关注攻击拦截的覆盖程度，会全面拦截攻击和疑似攻击行为，如需尽可能保证业务的安全性，可选用该规则组。

Q：CC 防护中，什么情况下使用 Session 识别访问者？

A：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，您可以使用 Session 区分单个访问者。CC 攻击（Challenge Collapsar）是 DDOS 的一种，攻击者通过代理服务器向受害主机不停发送大量数据包，造成 Web 业务服务器的资源耗尽，从而无法响应其他正常访问请求的一种攻击行为。因 CC 攻击采用周期和频率判断业务是否遭受到攻击，而当多个用户共用一个出口 IP 时，若采用 IP 识别访问者，则会造成系统将多个用户识别为一个，从而将来源于同一个出口 IP 的正常业务访问请求识别为 CC 攻击，进而导致用户的正常访问被拦截或阻断掉。而采用 Session 识别访问者，则可以避免将来源于同一个 IP 的多个用户访问识别的 CC 攻击。故当多个用户共享一个出口 IP 时，建议用户采用 Session 区分单个访问者。

Q：什么情况下，可以选择紧急模式的 CC 防护？

A：CC 攻击防护可以通过对 web 业务请求的安全验证防护网络攻击者对业务服务器发起的 CC 攻击。默认情况下，CC 攻击的防护模式是正常模式，帮助您拦截常规的 CC 攻击。当您发现在使用正常 CC 攻击防护模式状态下，依然出现源站 CPU 利用率飙升、数据库或者应用丢包时，此时说明常规的 CC 防护模式由于阈值设定的原因，已无法防护该 CC 攻击，为了缓解服务器的紧急状态，您可以选用攻击紧急模式。攻击紧急模式会降低判定 CC 攻击频率和周期的阈值，此时 CC 攻击的防护策略会非常敏感，对于所有超过阈值的访问请求都会拦截，从而保证在极端情况下依然能够对用户的 web 业务进行防护。

注意：

由于紧急模式下，防护策略阈值较低，敏感度较高，可能导致对正常请求的误拦截。所以建议您在服务器紧急情况缓解后，排查清楚出具体出现紧急情况的原因并解决后，在正常状态下依然启用正常模式的 CC 防护。配置方式请参见 CC 防护。

Q：IP 黑名单支持批量添加 IP 地址吗？

A：不可以，当前 WAF 暂不支持批量添加 IP 地址，您可以通过创建 IP 黑名单规则，添加单个 IP 地址或 IP 地址段。IP 黑白名单支持配置的策略如下：

- 支持基于域名创建 IP 黑白名单规则。
- 支持添加 IPv4、IPv6 地址，支持添加 IP 地址段。
- IP 黑白名单模块的防护检测逻辑优先级高于其他防护模块；IP 黑白名单内部检测逻辑，白名单高于黑名单。

注意：

- 不同实例版本支持添加的 IP 黑白名单规则数量不同，有关个版本规格的详细介绍，请参见产品规格。
- 若当前版本的 IP 黑白名单防护规则条数无法满足业务需求时，您可以通过购买规则扩展包或升级版本，以实现规则条数的扩容。一个规则扩展包包含 50 条 IP 黑白名单防护规则，详情请参见升级扩容。

Q：WAF 原生版是否支持 HTTPS 双向认证？

A：HTTPS 双向认证是相较于 HTTPS 单向认证而言的，HTTPS 单向认证是指客户端在请求服务器数据时，需要验证服务器的身份。而双向认证是在此基础上，服务器端验证客户端的身份，从而实现双向认证。双向认证主要应用场景是部分重要业务需要验证客户端身份时，需要使用双向验证。而使用 WAF 防护的业务，一般为对公众提供的 web 服务，其原始业务不会有双向验证的要求，故当前 WAF 原生版不支持 HTTPS 双向认证。

Q：WAF 原生版是否支持 WebSocket 协议？

A：WebSocket 是 HTML5 引入的一项技术，用于在 Web 应用程序中实现实时双向通信。与传统的 HTTP 请求-响应模型不同，WebSocket 允许服务器主动向客户端推送数据，而不需要客户端发起请求。WebSocket 连接保持打开状态，允许客户端和服务器之间进行双向通信，这为实时应用程序提供了更高效和实时的通信方式。当前 WAF 支持 WebSocket 进行用户业务的转发，实现 WebSocket 通信。

Q：若一个 IP 同时配置了白名单和黑名单，优先级是什么？

A：IP 白名单的优先级高于黑名单，若同时配置了白名单和黑名单，则优先以白名单为准，详情请参见 IP 黑白名单。

Q：WAF 原生版支持设置单条防护规则的防护状态吗？

A：支持。WAF 原生版提供具体防护规则的防护开关。您可以根据业务需要选择开启或关闭规则的防护。

Q：WAF 原生版支持针对地理位置配置禁止访问策略吗？

A：支持。地域访问控制支持针对地理位置的黑名单封禁，可指定需要封禁的国家、地区，阻断该区域的来源 IP 的访问。通过地域访问控制模块，可以满足针对地理位置的黑名单封禁。支持封禁的地域请参见地域访问控制。

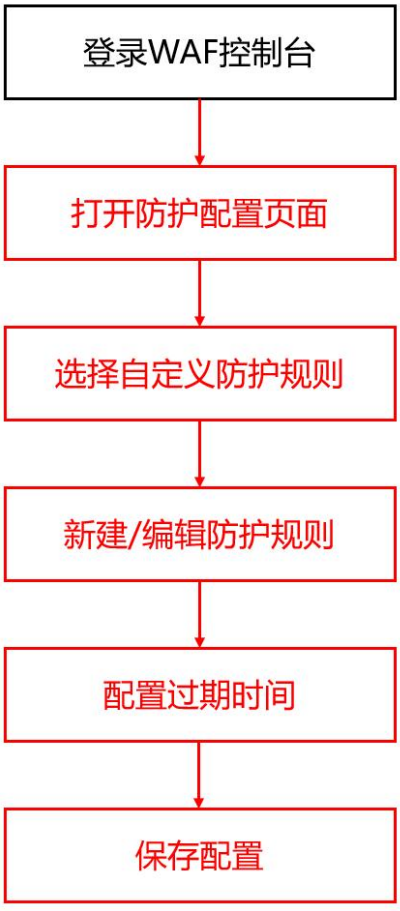
注意：

基础版、标准版不支持自定义防护规则组，请升级到更高版本使用。

6.3.2. 精准访问控制如何设置生效时间

精准访问控制允许自定义访问控制规则，通过对请求路径、请求 URI、Cookie、请求参数、Header、referer、User-Agent 等多个特征进行条件组合，对访问请求进行特征匹配实现管控，有针对性的阻断各类攻击行为。为了保证用户业务使用的灵活性，例如部分敏感地址仅允许在系统维护时间范围内短暂的访问等，从而对业务的访问策略能够进行精细化的防护和控制，系统允许创建精准访问控制规则时，可以选择让该规则永久生效，或定义失效时间。可以通过规则列表控制规则是否开启，自定义控制规则生效的时间段。

设置精准访问控制策略步骤如下：



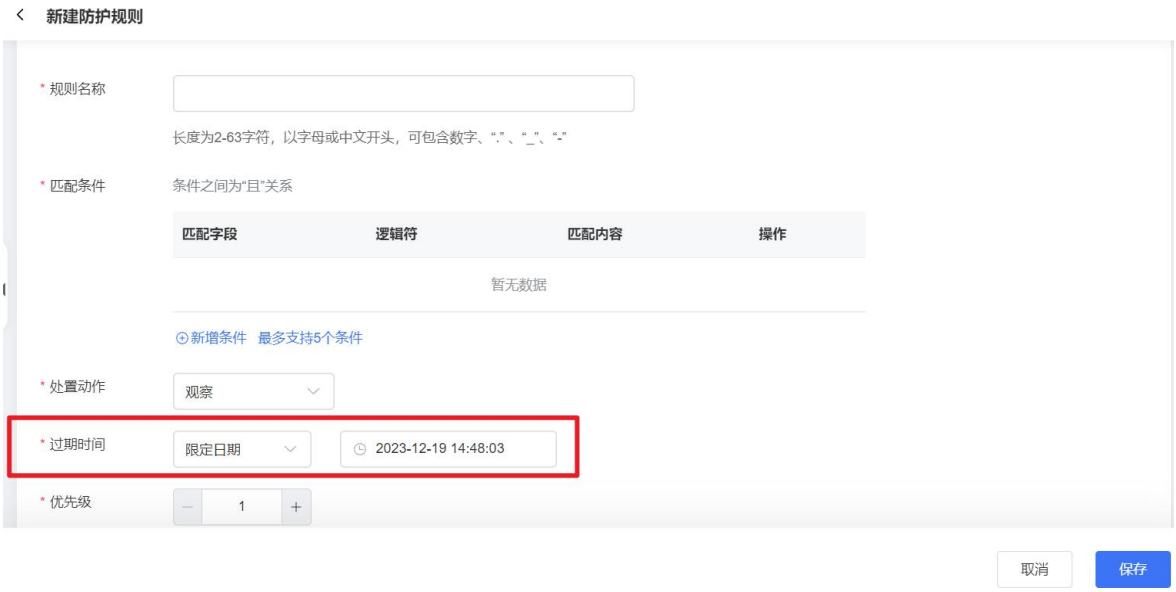
1. 登录 WAF 控制台。

2. 选择防护配置。

3. 选择自定义防护规则。

4. 新建/编辑防护规则。

5. 设置过期时间。



6. 保存配置，即可完成设置精准访问控制的生效时间。

6.3.3. WAF 如何设置白名单

WAF 支持 IP 黑白名单和规则白名单两种白名单策略，其中 IP 黑白名单功能用于对会话中的 IP 地址设置黑白名单规则，设置了 IP 白名单后，该 IP 的访问请求将不会被检测，直接可以访问业务服务器，配置详情请参见 IP 黑白名单。规则白名单是提供精细化的规则白名单策略，作用于 web 基础防护，您可以自定义具体的匹配特征，使命中匹配条件的请求不经过特定的检测项。检测项可以是全部规则、特定的规则类型或特定的规则 ID。通过设置规则白名单，您可以精细化的控制 web 基础防护规则的生效对象和生效策略，详情请参见配置规则白名单。综上所述，您即可以使用 IP 黑白名单进行白名单策略设置，也可以使用规则白名单对白名单进行设置。

注意：

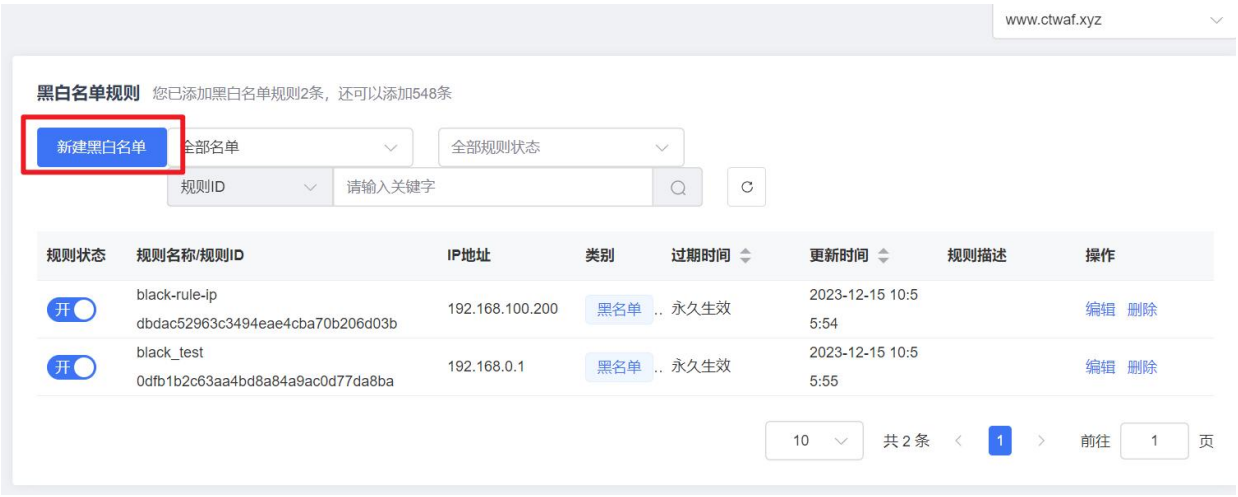
其中 IP 黑白名单的作用范围大于规则白名单的作用范围，IP 黑白名单作用于所有会话，属于 IP 白名单的 IP 会话会被直接放行，不再进行后续检测。规则白名单作用于 web 基础防护，当会话经过 web 基础防护后，还会被后续的其他防护模块检测。

IP 白名单设置方法

1. 登录管理控制台。

2. 选择 IP 黑白名单。

3. 新建黑白名单规则。



4. 设置 IP 白名单地址。

5. 点击确定，完成设置。

规则白名单设置方法

1. 登录管理控制台。

2. 选择防护配置。

3. 选择 Web 基础防护的规则白名单。

4. 新建白名单。

5. 进行白名单配置。

6. 点击确定，完成配置。

6.3.4. 防护策略如何设置优先级

WAF 中的部分模块支持针对防护策略设置优先级，包含 CC 防护、BOT 防护、精准访问控制三个模块，优先级数值越高，该条规则优先级越高。高优先级的策略在命中后将会执行阻断或防护动作，从而不再会进行低优先级的规则检测。

> 说明：
>
> 这三个防护模块中 CC 安全防护的优先级>精准访问控制优先级>BOT 防护优先级。

配置示例

例如精准访问控制规则 1 中出现放行自于 HOST=192.168.12.3，方法=POST 的请求，其优先级为 1，如下图。

同时规则 2 要求拦截所有请求方法=POST 的请求，优先级为 2，如下图。

那此时系统会优先执行优先级为 1 的策略，放行来自于 HOST=192.168.12.3 的请求，之后，拦截所有其他方法=POST 的请求。

但，反之，如果将规则 2 的优先级设置为 1，即拦截所有 POST 请求。规则 1 的优先级设置为 2，放行来自于 HOST=192.168.12.3 请求。那系统会拦截掉所有 POST 请求，包含来自于 HOST=192.168.12.3 请求。此时，HOST=192.168.12.3 的用户就无法访问相关的页面。

配置方法

1. 登录 WAF 管理控制台。

2. 选择防护配置。

3. 选择需要**设置**优先级的防护模块。

4. 新建/**编辑**规则。

5. 设置优先级，**点击**确定，完成设置。

6.4. 管理类

6.4.1. 管理类常见问题

Q：若流量超过当前 WAF 实例版本支持的带宽峰值时有什么影响？

A：如果用户将多个网站业务接入 WAF 实例进行保护，则必须保证所有网站业务的正常峰值带宽之和不超出 WAF 实例的业务带宽。超出业务带宽限制，WAF 会触发限流、随机丢包等动作，导致用户的网站业务在一定时间内出现卡顿、延迟，甚至不可用等，WAF 的服务防护性能无法得到保障。

Q：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？

A：WAF 的防护对象是域名，如果多个域名使用了同一个源站对外提供服务，需要将多个域名都接入 WAF 实现所有域名的防护。

Q：WAF 支持防护 IPv6 地址吗？

A：支持，WAF 支持添加 IPv6 的源站地址。

Q：接入 WAF 的域名需要备案吗？

A：使用 WAF 前，请确保域名已在工信部备案，未备案域名将无法正常使用 WAF。

Q：接入 WAF 对现有业务和服务器运行有影响吗？

A：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站进行任何操作（例如关机或重启）。

以 CNAME 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。

Q：WAF 原生版的防护日志可以存储多久？

A：当前 WAF 原生版可为您保存近 30 天的防护日志，支持下载至本地，您可以在防护事件中查看。

Q：WAF 回源是否需要放行所有客户端 IP？

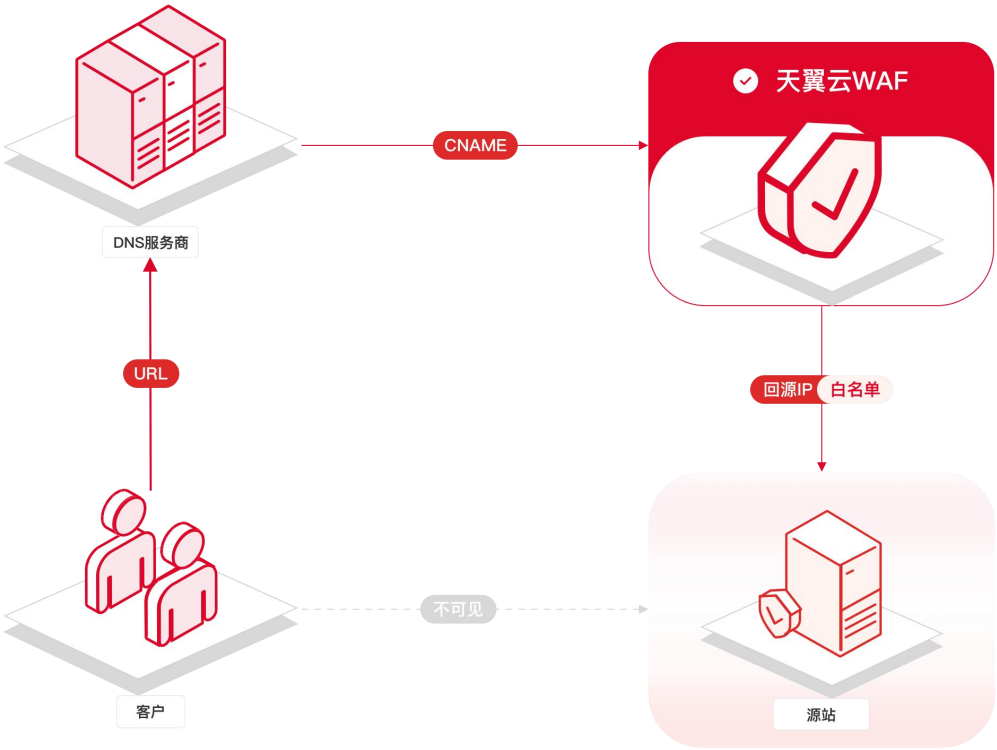
A：根据您的业务情况，您可以只放行 WAF 回源 IP 段，也可以放行所有客户端 IP。对于 Web 业务，建议您只放行 WAF 回源 IP，实现源站保护。

6.4.2. 如何删除 WAF 接入域名

如果要删除的防护域名没有完全接入 WAF，可直接在域名列表删除防护域名；

域名接入防护后，用户请求链路如下：

防护后



如果要删除的防护域名已经接入 WAF，请先到 DNS 服务商处，将该域名重新解析，指向源站服务器地址，然后再删除 WAF 上接入的域名，从而保证用户业务不中断，否则，如果直接删除 WAF 上接入的域名，将会导致用户业务不可用。