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

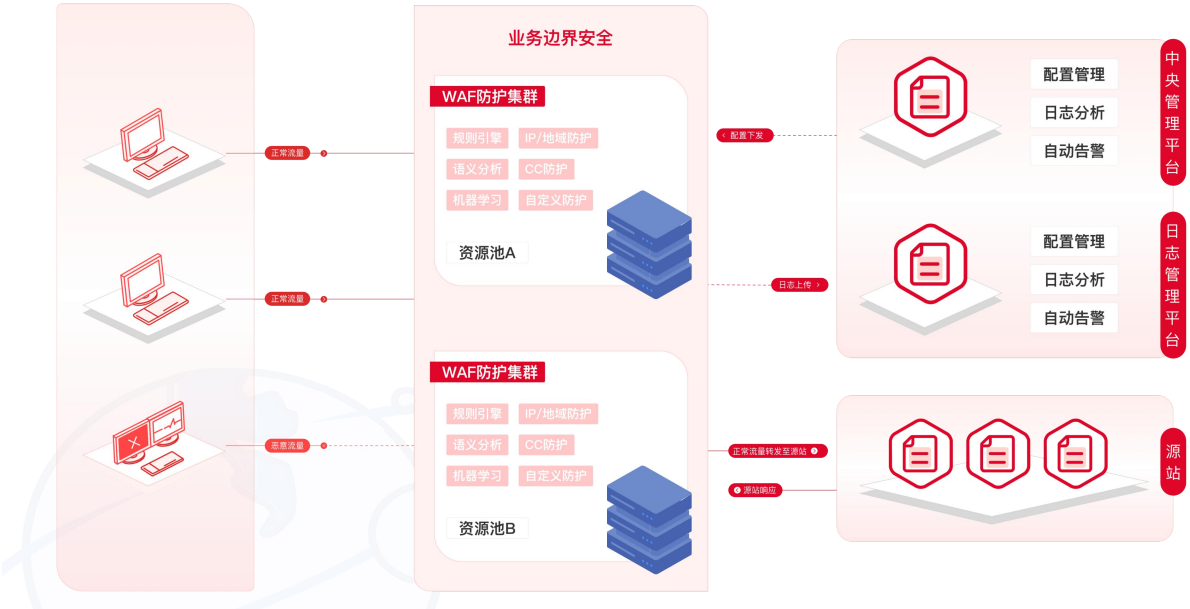
1. 产品简介

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。

产品架构

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。

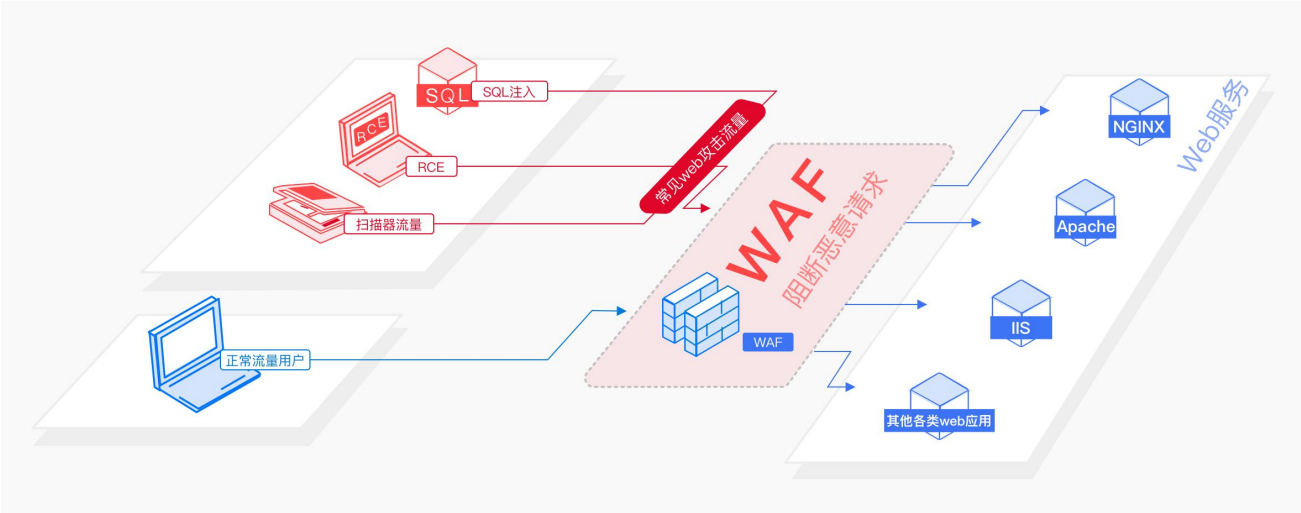
方案优势

- 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



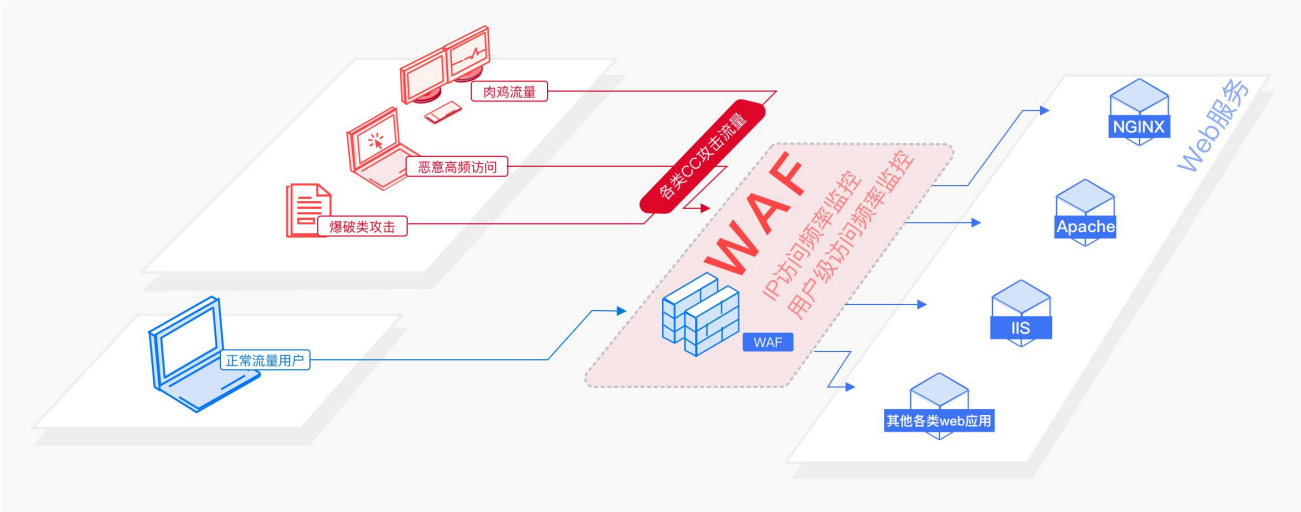
场景二：CC 攻击防护

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



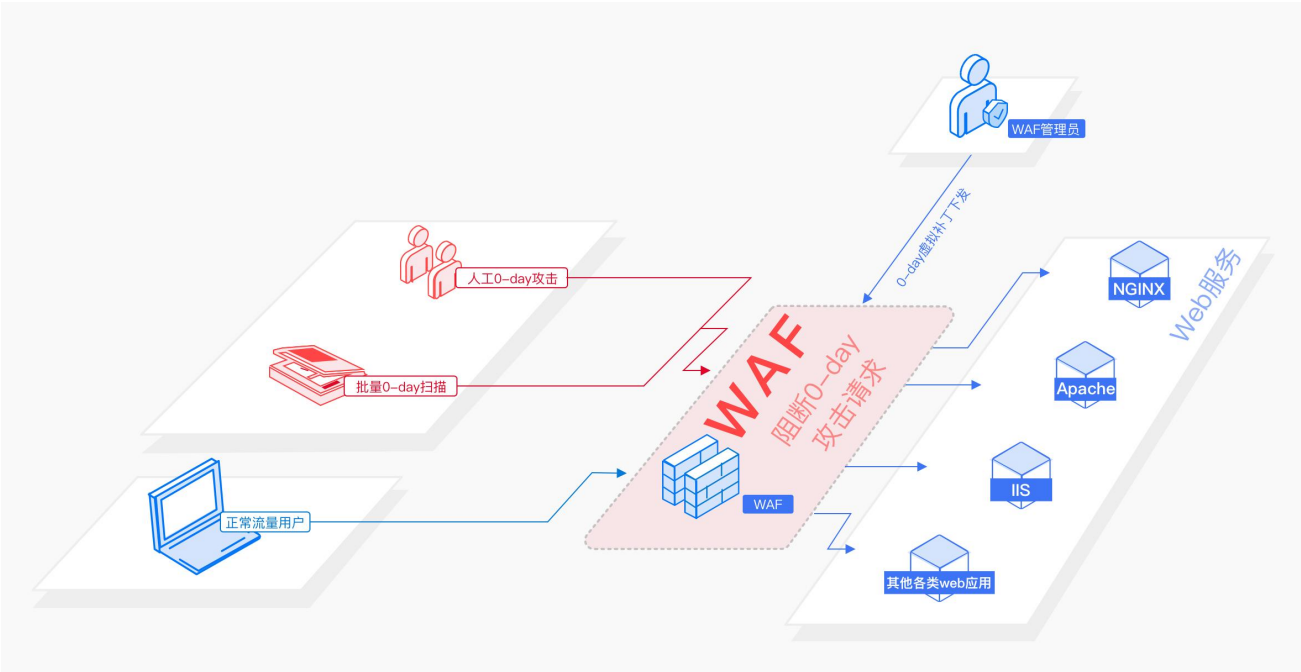
场景三：0Day 漏洞修复

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

产品版本说明

Web 应用防火墙（原生版）提供两种版本：**WAF SaaS 版**和 **WAF 独享版。**

- **WAF SaaS 版**根据支持防护的业务规模以及提供的防护功能不同，提供基础版、标准版、企业版、旗舰版四个版本供用户选择。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。
- **WAF 独享版**提供单机版、集群版供用户选择，且支持选择购买域名扩展包和带宽扩展包。

分类	WAF SaaS 版				WAF 独享版	
	基础版	标准版	企业版	旗舰版	单机版	集群版
适用场景	适合个人网站、小型网站等只需要满足基础安全需求，对业务没有特殊安全需求的用户，不适合企业用户使用	适用于对少量用户提供业务服务，没有大量高频访问中小型网站，没有特殊安全需求，仅需要满足基础防护能力	适用中大型企业或服务对互联网公众开放，有较高访问频率，并有较高数据安全与网络安全防护需求的网站防护	适用于大型及超大型复杂业务网站防护或有特殊定制安全需求的用户（支持定制需求，定制需求需要和客户经理联系）	适用于资源在天翼云上的 0-1Gbps 的 IP 防护场景	适用于资源在天翼云上的 1-10Gbps，需要集群高可用的防护场景
防护对象	域名				域名、IP	
接入指导	1. 购买 WAF SaaS 版实例 2. 网站接入 WAF 防护（域名接入）				1. 购买 WAF 独享版实例 2. 网站接入 WAF 防护（独享型接入）	

版本规格说明

分类	功能点	WAF SaaS 版				WAF 独享版	
		基础版	标准版	企业版	旗舰版	单机版（1 节点/实例）	集群版（4~12 节点/实例）
套餐基础信息	业务 QPS 峰值	100QPS/实例	3000QPS/实例	5000QPS/实例	10000QPS/实例	3000QPS/实例	20000QPS/实例
	支持主域名	1 个/实例	2 个/实例	5 个/实例	8 个/实例	100 个/实例	10000 个/实例

分类	功能点	WAF SaaS 版				WAF 独享版	
		基础版	标准版	企业版	旗舰版	单机版 (1 节点/实例)	集群版 (4~12 节点/实例)
	个数						
	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	100 个/实例	10000 个/实例
	支持防护的 ELB 监听器个数	×	600 个/实例	2500 个/实例	10000 个/实例	×	×
	泛域名防护	×	√	√	√	√	√
	IPv6 防护	×	√	√	√	√	√
	HTTP/HTTPS 非标准端口防护	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	不限制，最大 65535 个	不限制，最大 65535 个
	带宽弹性上限	10Mbps 超过 10Mbps 即丢包	200Mbps，超过弹性带宽上限不超过带宽保护上限的流量将直接转发，可通过扩展业务扩展包的形式增加弹性上限	300Mbps，超过弹性带宽上限不超过带宽保护上限的流量将直接转发，可通过扩展业务扩展包的形式增加弹性上限	400Mbps，超过弹性带宽上限不超过带宽保护上限的流量将直接转发，可通过扩展业务扩展包的形式增加弹性上限	200Mbps 超过 200Mbps 即丢包	1000Mbps 超过 1000Mbps 即丢包
	带宽保护上限	-	400Mbps，超过带宽保护上限的流量将会被直接丢弃，可通过购买业务扩展包的形式增加保护上限	600Mbps，超过带宽保护上限的流量将会被直接丢弃，可通过购买业务扩展包的形式增加保护上限	800Mbps，超过带宽保护上限的流量将会被直接丢弃，可通过购买业务扩展包的形式增加保护上限	-	-
基础安全防护	规则白名单	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	√，最大 1000 条	√，最大 1000 条
	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	√，支持自定义	√

分类	功能点	WAF SaaS 版				WAF 独享版	
		基础版	标准版	企业版	旗舰版	单机版 (1 节点/实例)	集群版 (4~12 节点/实例)
	自定义防护规则组	×	√，10 个/实例	√，20 个/实例	√，30 个/实例	最大 100 个	最大 100 个
	0Day 漏洞虚拟补丁	√	√	√	√	√	√
	IP 黑白名单	×	√，200 条/实例	√，500 条/实例	√，1000 条/实例	√，1000 条/实例	√，1000 条/实例
	地域封禁	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	√，1000 条/实例	√，1000 条/实例
	自定义精准防护策略	×	√，100 条/实例	√，200 条/实例	√，500 条/实例	√，1000 条/实例	√，1000 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	1000 条/实例	1000 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	√，1000 条/实例	√，1000 条/实例
	动态防护	×	√，与 BOT 防护共享规则	√，与 BOT 防护共享规则	√，与 BOT 防护共享规则	√，与 BOT 防护共享规则	√，与 BOT 防护共享规则
	BOT 攻击惩罚策略上限	×	1000 个/实例	1000 个/实例	1000 个/实例	10000 条/实例	10000 条/实例
	攻击惩罚防护策略上限	×	1000 个/实例	1000 个/实例	1000 个/实例	10000 条/实例	10000 条/实例
	数据统计分析	√	√	√	√	√	√
	敏感信息保护	×	×	√，50 个/实例	√，50 个/实例	√，1000 条/实例	√，1000 条/实例

分类	功能点	WAF SaaS 版				WAF 独享版	
		基础版	标准版	企业版	旗舰版	单机版 (1 节点/实例)	集群版 (4~12 节点/实例)
	网页防篡改	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	√，1000 条/实例	√，1000 条/实例
	Cookie 防篡改	×	×	√	√	√	√
	隐私屏蔽	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	√，1000 条/实例	√，1000 条/实例
	重保防护场景	×	√	√	√	×	×
	全局防护白名单	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	×	×
	全局精准访问控制	×	√，100 条/实例	√，200 条/实例	√，500 条/实例	×	×

资源扩展包规格说明

模式	扩展包	规格	数量限制
云 SaaS 模式	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 个主域名（备案的域名）。	最多支持 500 个域名扩展包。
	业务扩展包	1 个业务扩展包包含 1000QPS 业务请求峰值。 每增加一个业务扩展包，可增加 50Mbps 带宽弹性上限，100Mbps 带宽保护上限。	最多支持 30 个业务扩展包。
	规则扩展包	规则扩展包用于提升防护规则配额，支持以下两种扩展方式（二选一）： ● IP 黑白名单：每个扩展包包含 **50 条防护规则/域名。** ● 重保防护场景：每个扩展包包含 **1000 个 IP/实例。**	最多支持 1000 个规则扩展包。
独享模式	域名扩展包	1 个域名扩展包支持 10 个域名或 IP。	最多支持 1000 个域名扩展包。
	带宽扩展包	1 个带宽扩展包包含 1000QPS 业务请求峰值、50Mbps 业务带宽。	单机版：最多支持 16 个带宽扩展包。 集群版：带宽扩展包的数量上限与节点数量相关联，每增加一个节点，带宽扩展包的上限数量增加 20 个。 例如，当集群包含 4 个节点时，最多支持配置 20 个带宽扩展包；而节点数量最多 12

模式	扩展包	规格	数量限制
			个，则最多支持配置 180 个带宽扩展包。

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。

2. 计费说明

2.1. 计费模式

适用场景

Web 应用防火墙（原生版）支持包年包月付费模式。用户根据需要，一次性支付一个月/多个月/一年/多年的费用，支付成功后，WAF 将被系统分配给用户使用，直到超过保留期后被系统回收。

WAF SaaS 版

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
适用范围	适合个人网站、小型网站等只需要满足基础安全需求对业务没有特殊安全需求用户，不适用于商业用户	适用于对少量用户提供业务服务，没有大量高频访问中小型网站，没有特殊安全需求，仅需要满足基础防护能力	适用中大型企业或服务对互联网公众开放，有较高访问频率，并有较高数据安全与网络安全防护需求的网站防护	适用于大型及超大型复杂业务网站防护或有特殊定制安全需求的用户（支持定制需求，定制需求需要和客户经理联系）
主套餐	99 元/月	3880 元/月	9800 元/月	29800 元/月
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%

说明：

- 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。
- 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 个主域名（备案的域名）。
- 业务扩展包：1 个业务扩展包包含 1000QPS/个，最多支持 30 个业务扩展包，每增加一个业务扩展包，可增加 50Mbps 带宽弹性上限，100Mbps 带宽保护上限。
- 规则扩展包用于提升防护规则配额，支持以下两种扩展方式（二选一）。
  - IP 黑白名单：每个扩展包包含 **50 条防护规则/域名。**
  - 重保防护场景：每个扩展包包含 **1000 个 IP/实例。**

说明：

- 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。
- 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。

优惠活动

Web 应用防火墙（原生版）产品订购享受 8 折优惠。

包年订购折扣与本次活动不能同享，取低者计算（如包 1 年折扣为 85 折的，按照包一年 8 折计算；包 3 年折扣为 5 折的，按照 5 折计算）。

WAF 独享版

标准资费

根据开通实例时选购的版本、节点数量、购买时长生成预付费账单。

说明：

- 如下费用仅为 WAF 独享版实例的费用。
- 在“二类节点”区域（WAF 独享版支持的区域请参见支持的区域）购买 WAF 独享版实例时，还需要同时购买实例所依赖的基础资源（包括弹性云主机、弹性 IP 等），基础资源与实例一起计费，统一下单。相关基础资源的价格请以对应产品的实际定价为准，详细说明请参见“云主机计费说明”、“弹性 IP 计费说明”。

计费项	标准资费	计费单位
独享模式-单机版（200M）	2837	元/月
独享模式-集群版（1G）	11348	元/月
独享模式-集群版扩展节点	2837	元/节点/月
独享模式-带宽扩展包	500	元/50M/月
独享模式-域名扩展包	500	元/个/月

关于不同版本的规格参数，请参见“产品规格”。

资源扩展包规格说明

扩展包	规格	数量限制
域名扩展包	1 个域名扩展包支持 10 个域名或 IP。	最大支持 1000 个域名扩展包。
带宽扩展包	1 个带宽扩展包包含 1000QPS 业务请求峰值、50Mbps 业务带宽。	• 单机版：最多支持 16 个带宽扩展包。 • 集群版：带宽扩展包的数量上限与节点数量相关联，每增加一个节点，带宽扩展包的上限数量增加 20 个。 例如，当集群包含 4 个节点时，最多支持配置 20 个带宽扩展包；而

扩展包	规格	数量限制
		节点数量最多 12 个，则最多支持配置 180 个带宽扩展包。

计费组成

Web 应用防火墙（原生版）计费项由主套餐（必选）和资源扩展包（可选）组成，费用计算公式如下：

用户费用=（主套餐费用-月费用+资源扩展包费用-月费用）* 购买包年/包月时长 *购买折扣（包年折扣与促销优惠活动无法同享）

如何选购适合的版本

Web 应用防火墙（原生版）提供 **WAF 云 SaaS 模式**和 **WAF 独享模式**供用户选择，两种模式的基本功能保持一致，根据用户需求侧重点，有如下建议：

- 对于需要**满足基础防护、计划短期使用**的用户，鼓励**购买独享模式。**购买 1 年及以内，独享模式价格更便宜能满足基本防护需求。
- 对于**有高可用需求、需要长期进行 Web 防护**的用户，鼓励**购买 SaaS 模式。**SaaS 模式产品可用性更强，且购买 2 年及以上，SaaS 模式能够享受更优惠的价格。

如何选购适合的规格

WAF 是以域名为防护对象进行防护的产品，所以 WAF 的防护性能受到用户需要防护的所有域名总访问量的影响，如何选购合适的规格对需要防护的域名进行防护，有如下几种建议的方法：

1. 通过百度站长统计或其他带有统计功能的统计应用，统计所需要防护站点一天的访问量，计算平均访问请求数，从而选择出合适的产品规格。
2. 通过 Nginx 内置状态模块和相关工具查看 Nginx 每秒处理的请求数，从而了解到所需要防护站点总的访问请求数量，若只防护了该站点下部分域名，可以购买小于总请求数量的产品规格，即可满足需求。
3. 通过访问站点处理流量大小估算访问请求数量大小，根据经验值，推荐每个 HTTP 请求访问大小约为 3KB 左右，可通过站点实时带宽除以 3KB 推测出站点访问量大小。

注意：

- 如下费用仅为 WAF 独享版实例的费用。
- 在“二类节点”区域（WAF 独享版支持的区域请参见支持的区域）购买 WAF 独享版实例时，还需要同时购买实例所依赖的基础资源（包括弹性云主机、弹性 IP 等），基础资源与实例一起计费，统一下单。相关基础资源的价格请以对应产品的实际定价为准，详细说明请参见“云主机计费说明”、“弹性 IP 计费说明”。

实例到期说明

WAF 实例到期后，您所购买的防护服务会自动停止，保留期为 15 天，为了保证您能够持续为 Web 业务提供防护，所购买服务到期前后，WAF 会给您发送通知，通知的具体规则如下：

- 提醒及通知方式：邮件、短信、站内信。
- 充值成功通知：当用户充值成功后，会发送 1 次充值成功通知。
- 资源到期通知：WAF 到期前 7 天、3 天以及到期当天，会分别发送到期提醒。
- 资源释放通知：WAF 到期后 3 天、7 天，会分别发送释放提醒。
- 资源销毁通知：当用户的 WAF 销毁后，会向用户发送 1 次销毁通知。

2.2. 购买 WAF 实例

2.2.1. 购买 WAF 云 SaaS 型实例

Web 应用防火墙（原生版）SaaS 版支持包年/包月计费方式，同时提供四个规格：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 WAF SaaS 版规格。

前提条件

已经注册天翼云账号并完成实名认证。

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 个主域名（备案的域名）。
- 一个业务扩展包包含：1000QPS/个，最多支持 30 个业务扩展包。
- 规则扩展包用于提升防护规则配额，支持以下两种扩展方式（二选一）：
  - IP 黑白名单：每个扩展包包含 **50 条防护规则/域名。**
  - 重保防护场景：每个扩展包包含 **1000 个 IP/实例。**

约束条件

- WAF SaaS 版实例生效期间，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 WAF SaaS 版实例，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. 在左侧导航栏，选择“系统管理 > 查看产品信息”，默认进入“云 SAAS 型”页签。在实例列表上方，单击“立即购买”。

   首次使用 WAF 时，进入如下欢迎页面，单击“立即购买”。

5. 进入产品订购页面，选择版本、规格和购买数量。

参数说明如下：

参数	说明

参数	说明
版本选择	此处选择“WAF 云 SaaS 模式”。
规格选择	提供四个规格：基础版、标准版、企业版、旗舰版，关于产品规格信息对比，请参见“产品规格”。
购买数量	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。

6. 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。

7. （可选）填写交付联系方式。

> 说明：
>
> 为保障产品顺利交付，天翼云提供免费交付服务，请提供交付联系方式，订购完成后，天翼云安全专家会与您取得联系。

8. 选择购买时长。

说明：

- 支持勾选 “自动续订”，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。
- 基础版最多支持一次性付费 1 年。

9. 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”。
10. 进入“付款”页面，完成付款。

2.2.2. 购买 WAF 独享型实例

Web 应用防火墙（原生版）独享版支持包年/包月计费方式，同时提供两个规格：单机版、集群版，两种资源扩展包：带宽扩展包、域名扩展包。您可以根据业务规模选择 WAF 独享版规格。

根据所选购买区域，购买步骤略有不同，WAF 独享版支持的区域请参见“支持的区域”。

- 购买步骤（一类节点区域）
- 购买步骤（二类节点区域）

支持的区域

支持购买 WAF 独享版的区域如下：

区域	一类节点	二类节点
华东地区	上海 7/华东 1/南昌 5/上海 36/杭州 2/杭州 7/芜湖 4/南京 3/南京 4/南京 5/九江	芜湖/南昌/上海 4/杭州/苏州
华南地区	华南 2/郴州 2/长沙 42/福州 25/佛山 3/南宁 23/武汉 41/海口 2/福州 4/厦门 3/广州 6/南宁 2/武汉 3/武汉 4/长沙 3	福州 1/深圳/广州 4/南宁/武汉 2/长沙 2/海口
西北地区	乌鲁木齐 27/乌鲁木齐 7/兰州 2/庆阳 2/中卫 5/西宁 2/西安 3/西安 5//西安 7	兰州/西宁/西安 2/乌鲁木齐
西南地区	西南 1/拉萨 3/西南 2-贵州/昆明 2/成都 4/重庆 2/贵州 3	重庆/贵州 1/成都 3/昆明
北方地区	北京 5/晋中/郑州 5/华北 2/青岛 20/太原 4/呼和浩特 3/石家庄 20/辽阳 1/内蒙 6	郑州/华北/内蒙 3/青岛/太原

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，防护对象为域名或 IP。

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
单机版	适用于资源在天翼云上的 0-1Gbps 的 IP 防护场景。
集群版	适用于资源在天翼云上的 1-10Gbps，需要集群高可用的防护场景。

约束条件

- WAF 独享版实例生效期间，支持扩增资源扩展包数量。
- 开通 WAF 独享版实例，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。

前提条件

已经注册天翼云账号并完成实名认证。

购买步骤（一类节点区域）

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 管理独享引擎”；或选择“系统管理 > 查看产品信息”，选择“独享型”页签。在实例列表上方，单击“立即购买”。

   首次使用 WAF 时，进入如下欢迎页面，单击“立即购买”。

5. 在产品订购页面，版本选择“WAF 独享模式”，配置区域、可用区、虚拟私有云、子网等信息。

> 说明：
>
> 若需要开启 IPv6，请确保所选子网已开启 IPv6 功能。

6. 选择规格和购买数量。

参数说明如下：

参数	说明
规格选择	支持“单机版”和“集群版”。
购买数量	● 一个单机版实例只需购买 1 个节点。 ● 一个集群版实例至少购买 4 个节点（2 个反向代理节点，2 个检测引擎节点），最多购买 12 个节点。
云主机配置	“集群版”支持多 AZ 部署，选择“集群版”时，可以为各个节点选择不同的可用区。

7. 购买“带宽扩展包”、“域名扩展包”，可以设置购买数量。

扩展包	规格	数量限制
带宽扩展包	1 个带宽扩展包包含 1000QPS 业务请求峰值、50Mbps 业务带宽。	● 单机版：最多支持 16 个带宽扩展包。 ● 集群版：带宽扩展包的数量上限与节点数量相关联，每增加一个节点，带宽扩展包的上限数量可增加 20 个。例如，当集群包含 4 个节点时，最多支持配置 20 个带宽扩展包；而当节点数量增至 12 个时，最多支持配置 180 个带宽扩展包。

扩展包	规格	数量限制
域名扩展包	1 个域名扩展包支持 10 个域名或 IP。	最多支持 1000 个域名扩展包。

8. （可选）填写交付联系方式。

> 说明：
>
> 为保障产品顺利交付，天翼云提供免费交付服务，请提供交付联系方式，订购完成后，天翼云安全专家会与您取得联系。

9. 选择“购买时长”，拖动时间轴设置购买时长。

> 说明：
>
> 支持开启“自动续订”，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。

10. 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”。
11. 进入“付款”页面，完成付款。

购买步骤（二类节点区域）

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 管理独享引擎”；或选择“系统管理 > 查看产品信息”，选择“独享型”页签。在实例列表上方，单击“立即购买”。

   首次使用 WAF 时，进入如下欢迎页面，单击“立即购买”。

5. 在产品订购页面，版本选择“WAF 独享模式”，配置区域、可用区、虚拟私有云、子网、弹性 IP 等信息。

说明：

- 若需要开启 IPv6，请确保所选子网已开启 IPv6 功能。
- 仅“二类节点”区域需要在此处配置弹性 IP。

6. 选择规格和购买数量。

参数说明如下：

参数	说明
规格选择	二类节点区域暂时只支持选择“单机版”。
购买数量	单机版实例只需购买 1 个节点。

7. 配置承载 WAF 独享版实例的云主机规格。

说明：

- 云主机的 CPU 和内存为系统默认选择，不支持修改。
- 主机规格、系统盘类型、数据盘类型请根据实际情况进行选择，系统盘和数据盘大小不能低于系统限制的最小值，具体限制请在购买时以购买页面的信息为准。

8. 购买“带宽扩展包”、“域名扩展包”，可以设置购买数量。

扩展包	规格	数量限制
带宽扩展包	1 个带宽扩展包包含 1000QPS 业务请求峰值、50Mbps 业务带宽。	单机版最多支持 16 个带宽扩展包。
域名扩展包	1 个域名扩展包支持 10 个域名或 IP。	最多支持 1000 个域名扩展包。

9. （可选）填写交付联系方式。

> 说明：
>
> 为保障产品顺利交付，天翼云提供免费交付服务，请提供交付联系方式，订购完成后，天翼云安全专家会与您取得联系。

10. 选择“购买时长”，拖动时间轴设置购买时长。

> 说明：
>
> 支持开启“自动续订”，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。

11. 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”。

12. 进入“付款”页面，完成付款。

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。

到期说明

升级扩容时，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。

计费说明

计费场景

某用户于 2024/04/30 购买一套 1 个月的 WAF 云 SaaS 模式标准版，默认规格配置如下：

- 防护域名数：20 个（含 2 个 1 级域名）
- 业务 QPS 峰值：3000QPS

使用一段时间后，用户发现当前规格无法满足业务需要，于 2024/5/15 进行升级，升级后规格配置如下：

- 防护域名数：30 个（含 3 个 1 级域名），购买了 1 个域名扩展包
- 防护带宽：6000QPS，购买了 3 个业务扩展包

那么在 4~5 月份，共计花费了多少钱呢？5~6 月份，预计会花费多少钱呢？

计费构成

4~5 月实际费用

- Web 应用防火墙标准版本费用：3880 元/月，实际费用为 3880 元。
- 域名扩展包费用：600 元/月，因购买时间为 5 月 15 日，实际费用为 15/30 * 600=300 元。
- 业务扩展费用：1000 元/月*3 个，因购买时间为 5 月 15 日，实际费用为 15/30 * 3000=1500 元。
- 本月实际总计费用为：3880+300+1500=5680 元。

5~6 月预期费用

- Web 应用防火墙标准版本费用：3880 元/月，实际费用为 3880 元。
- 域名扩展包费用：600 元/月，因购买时间为 5 月 15 日，实际费用为 600 元。
- 业务扩展费用：1000 元/月*3 个，因购买时间为 5 月 15 日，实际费用为 3000 元。

- 本月实际总计费用为：3880+600+3000=7480 元。

注意：

- 因资源扩展包需要在主套餐的基础上进行购买，当主套餐停止使用后，资源扩展包也无法使用，故资源扩展包计费时间与主套餐计费时间保持一致。
- 示例中计算的价格为按月购买的价格，当按年购买时，实际价格以购买详情页具体的折扣价格为准。
- 因扩容、升配等业务具体购买价格与所购买规格的时长和使用时间有相关性，不同的购买时长和使用时长涉及不同的折扣，故以上示例不完全等同于实际计算价格，详细价格以购买页面显示价格为准。

升级实例规格

具体操作请参见：

- 升级云 SAAS 型实例规格
- 增加独享版实例的节点数量

新增购买资源扩展包

具体操作请参见：

- 扩增云 SAAS 型实例资源扩展包
- 扩增独享型实例资源扩展包

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

- 服务支持手动续订，需要在服务到期前进入控制台操作。
- 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“费用中心 > 订单管理 > 续订管理”页面，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

具体操作请参见：

- 续订云 SAAS 型实例
- 续订独享型实例

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”。

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。

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

您（天翼云客户）可根据需要，在符合天翼云退订规则的前提下，灵活退订配额。目前退订包含七天无理由全额退订和非七天无理由退订以及其他退订。

退订完成后，退款金额会退回账户余额，客户可根据需要进行提现。

- 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

具体操作请参见：

- 退订云 SAAS 型实例
- 退订独享型实例

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。

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“账单管理 > 账单详情”，进入账单详情页面。按如下筛选条件，即可查看到产品的账单详情。

- 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。

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**；

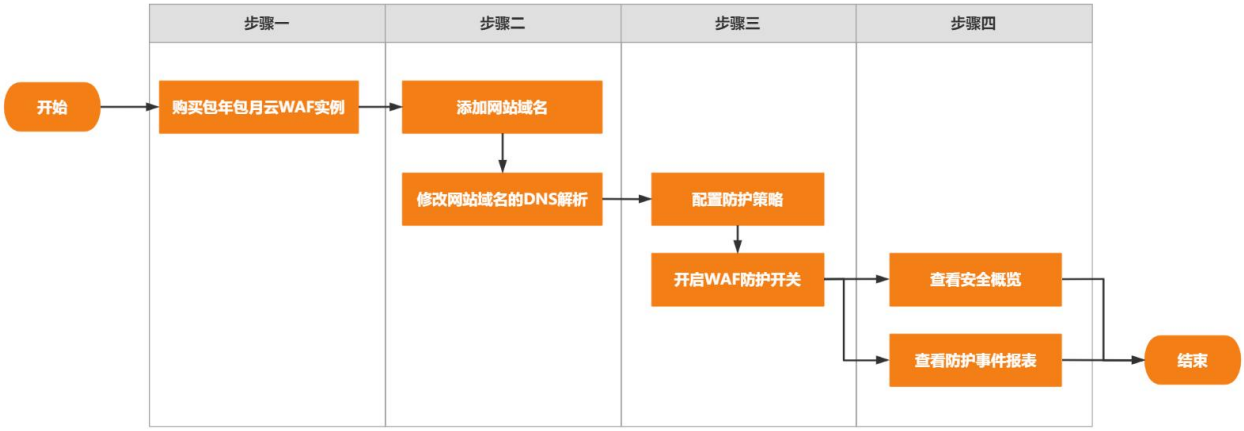
2. 在注册页面，请填写“邮箱地址”、“登录密码”、“手机号码”，并点击**同意协议并提交**，如 1 分钟内手机未收到验证码，请再次点击**免费获取短信验证码**；

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. 登录天翼云控制中心，在产品服务列表页，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“立即购买”，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）提供的规格详情请参见产品规格。
2. 勾选“自动续订”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“费用中心 > 订单管理 > 续订管理”页面，找到对应的资源进行修改。

步骤二 网站接入

网站接入 WAF 后，WAF 才能对访问网站的请求进行检测。

产品版本	接入方式	接入步骤
WAF SAAS 版	域名接入	1. 进入云 WAF 产品控制台，在左侧导航栏选择“接入管理”，在接入管理页面选择“域名接入”页签。 2. 添加防护对象：在列表上方点击“添加防护对象”，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。
WAF 独享版	独享型接入	1. 进入云 WAF 产品控制台，在左侧导航栏选择“接入管理”，在接入管理页面选择“独享型接入”页签。 2. 添加防护对象：在列表上方点击“添加防护对象”，根据页面提示配置域名或 IP、服务器协议、源站地址、代理情况、负载均衡策略等相关信息。

说明：

- 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。
- 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。

- 在 WAF 控制台左侧导航栏点击“防护事件”。
- 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。

CC 防护模式配置

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“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。 说明： 防护模式只能选择一种，不能同时开启。

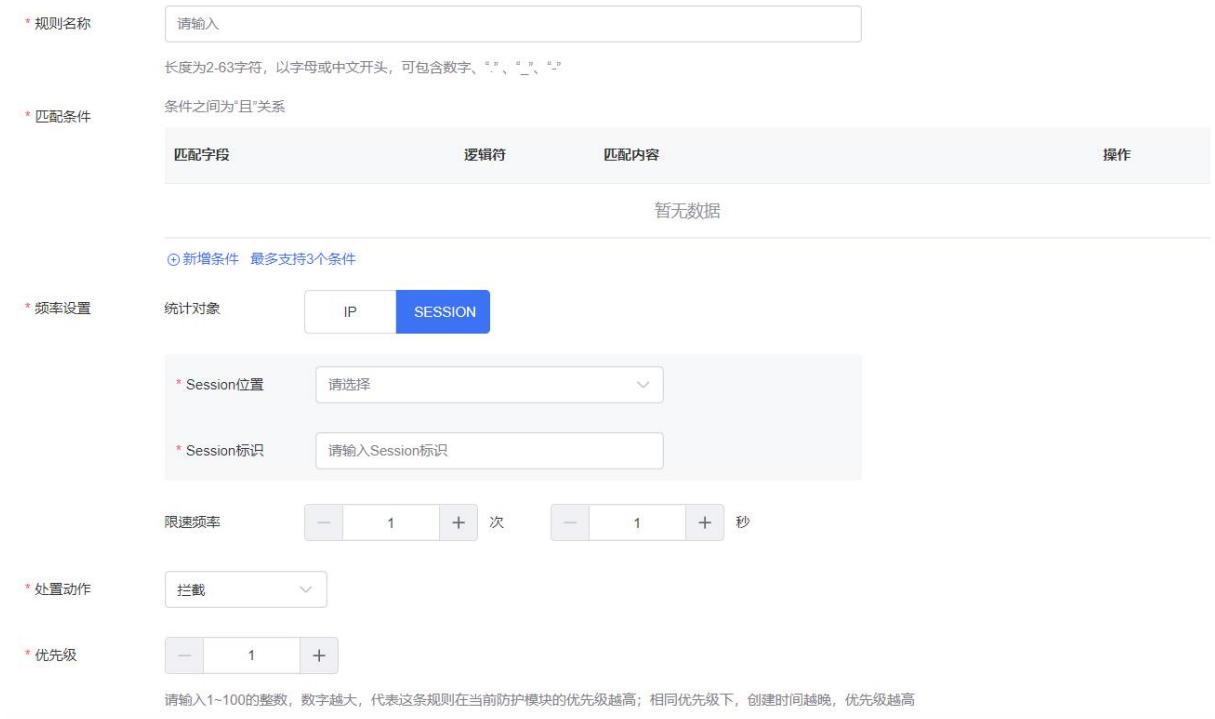
自定义 CC 防护策略

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“CC 防护”模块，在防护模式后方点击“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 3 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 位置：可选择 GET、POST、COOKIE、HEADER。 ◆ 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），系统将根据此标识匹配到的内容识别访问者。

配置项	说明
	● 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 将根据配置的处置动作处理。配置项如下： ■ 阈值（次）：统计时长内统计对象的允许访问的次数，超过阈值，则触发频率限制。 ■ 统计时长（秒）：统计周期。
处置动作	定义触发规则后执行的动作，支持“拦截”。
优先级	代表该规则在 CC 防护模块中执行的优先级。 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。

相关操作

对于已创建的规则，您可以执行以下操作：

- 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。
- 删除：若不再使用某条规则，可对该规则进行删除。
- 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

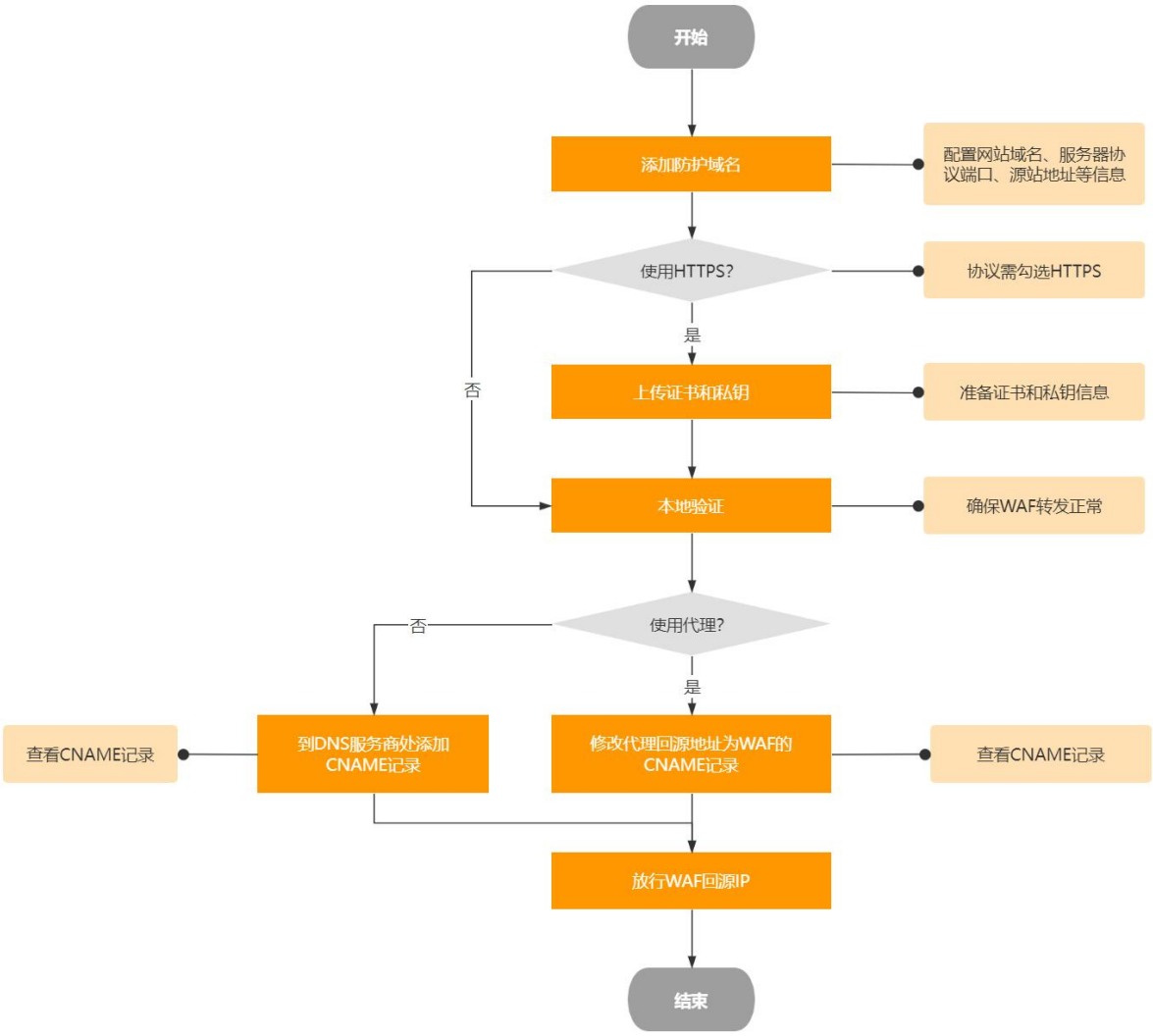
4.1.1. 网站接入 WAF 防护（域名接入）

4.1.1.1. 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。

4.1.1.2. 添加防护对象

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

说明：

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。

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，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 进入到云 WAF 控制台，在左侧导航栏选择“接入管理”，默认进入“域名接入”页签。

5. 点击“添加防护对象”进入域名接入信息配置页，依次配置“防护对象”、“服务器配置”、“代理情况”、“负载均衡策略”等信息。

   配置项说明如下：

配置项	说明
防护对象	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。
防护对象名称	自定义防护网站的显示名称。

配置项	说明
服务器配置	单击“添加一个服务器端口组”，弹出新增服务器端口组窗口。 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。 ● 端口：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。 ● 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。设置说明如下： ● 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。 ● 权重：当负载均衡算法为“加权轮询”时生效，所有请求将此处配置的权重轮流分配给源站服务器，权重越大，回源到该源站的几率越高。

配置项	说明
	■ 不输入则视同为最低权重 1。 ■ 当输入值为 0 时，业务不会回源到该站点。 ■ 取值范围：0~100 的正整数。 说明： 当健康检查发现站点出现问题时，剩余站点将按照剩余配置权重进行动态比例变化后的结果进行回源转发。
证书配置	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。 1. 点击“上传证书”，进入服务器端证书配置页面。 2. 选择证书类型，支持“通用证书”和“国密证书”。 3. 配置证书。支持证书选择、手动填写、文件上传方式： ● 证书选择：如您使用了证书管理服务，可通过下拉框选择已有证书。 ● 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，点击“上传”，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。
高级设置	● 选择 HTTPS 后，还支持启用以下功能： ● 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。

配置项	说明
	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。 ● SSL 解析方式：支持“单向认证”。
健康检查	开启健康检查将自动移除对失效源站的转发策略，当失效源站恢复健康后将重新加入转发列表。 开启后，还需配置健康检查策略。
IPv6	WAF 默认只处理 IPv4 请求流量。如果需要支持 IPv6 请求，请开启该功能。 ●  ：开启 IPv6 功能，支持将 IPv6 请求流量接入 WAF 进行防护。 注意 功能开启并完成域名接入后无法修改，如需关闭 IPv6 请求防护，需要重新接入域名。 ● ：不开启 IPv6 功能，仅防护 IPv4 请求流量。
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，需要进一步设置源 IP 获取方式。 **源 IP 获取方式**：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

配置项	说明
	下： ■ 从 Socket 连接中获取 ■ 从 X-Fowarded-For 连接中获取倒数第 1 层代理 ■ 从 HTTP 头 X-Client-IP 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。 • 加权轮询：根据同一组回源地址内配置的权重进行加权回源，权重越大，回源到该源站的几率越高。 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。
流量标记	开启流量标记功能，WAF 在转发客户端请求到源站服务器时，通过在回源请求头部添加标记字段，标记该请求经过 WAF 转发，可以帮助源站判断请求来源。 如果请求中存在指定标记字段，则为 WAF 检测后的正常请求，放行该请求；如果请求中不存在指定标记字段，则为攻击者请求，拦截该请求。 单击“添加一个标记”，添加流量标记。最多支持添加 5 个标记字段。 支持如下标记类型： ● 自定义 Header，配置自定义 Header 名、Header 值。 ● 客户端真实源 IP，配置客户端真实源 IP 所在的 HTTP Header 名。 ● 客户端真实源端口，配置客户端真是源端口所在的 HTTP Header 名。 注意： 请勿填写标准的 HTTP 头部字段，否则会导致标准头部字段内容被自定义的字段值覆盖。
回源长连接	● 功能开启后，支持回源长连接功能，最大支持 1000 个回源长连接。

配置项	说明
	开启“回源长连接”后，还需配置“空闲连接超时时间”，默认值为 10 秒，最多支持 60 秒。 ● 功能关闭后，将不支持 WebSocket。
超时配置	开启超时配置，可以配置如下超时时间： ● 连接超时时间：WAF 转发客户端请求时，与源站建立连接的超时时间。 ● 读连接超时时间：WAF 等待源站响应的超时时间。 ● 写连接超时时间：WAF 向源站发送请求的超时时间。 以上默认值均为 60 秒，最短支持 10 秒，最长支持 1200 秒。

6. 本地验证。

   根据页面提示，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。

7. 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。

8. 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。

9. 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。

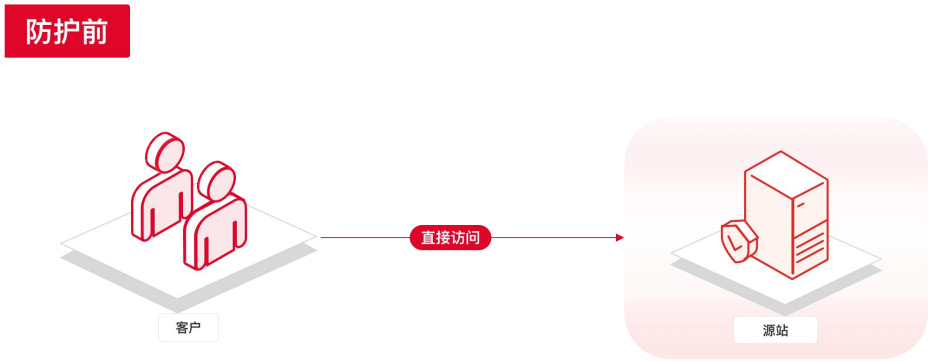
配置	说明	相关文档
Web 基础防护	覆盖 OWASP 常见安全威胁，支持 SQL 注入、XSS、	Web 基础防护

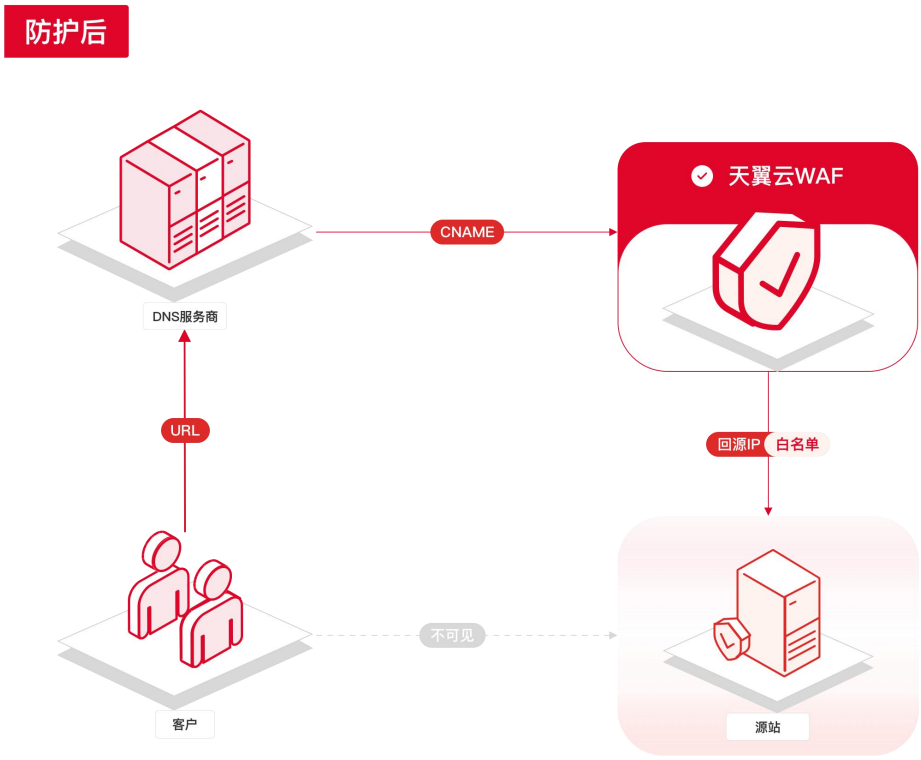
配置	说明	相关文档
	文件包含、远程命令执行、目录穿越、文件上传、CSRF、SSRF、命令注入、模板注入、XML 实体注入等攻击检测和拦截。	
CC 防护	CC 防护支持默认防护策略及灵活的自定义防护策略。自定义策略支持依托精准访问控制规则进行特征识别，并根据访问源 IP/ SESSION 控制访问频率，恶意流量通过阻断、人机验证等处置手段有效缓解 CC 攻击。	CC 防护
BOT 防护	提供公开类型、协议特征、自定义会话特征等多种判定维度的防护策略，支持根据 BOT 会话行为特征设置 BOT 对抗策略，对 BOT 行为进行处理，有效防护搜索引擎、扫描器、脚本工具等爬虫攻击。	BOT 防护
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
防敏感信息泄露	支持对网站返回的内容进行过滤（拦截、脱敏展示），过滤内容包括敏感信息、关键字和响应码。	防敏感信息泄露
网页防篡改	通过缓存页面和锁定访问请求，可避免页面被恶意篡改而带来的负面影响，对重点静态页面进行保护。	网页防篡改
Cookie 防篡改	通过对 Cookie 中的字段增加完整性校验保护，WAF 会新增一个 Cookie 字段用于篡改校验。	Cookie 防篡改
隐私屏蔽	通过设置隐私屏蔽规则，可屏蔽用户隐私信息，避免用户隐私信息出现在系统记录的日志中。	隐私屏蔽

4.1.1.3. 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





WAF 采用 CNAME 的方式将原本去向网站的请求转向到 WAF，从而实现对网站访问的安全防护，这些用户请求将在 WAF 进行安全检测和过滤后，发送回源站。此时由于网站接入 WAF，访问网站的 IP 实际上变成了 WAF 的回源 IP 段，从网站的角度来看，访问其的来源 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。

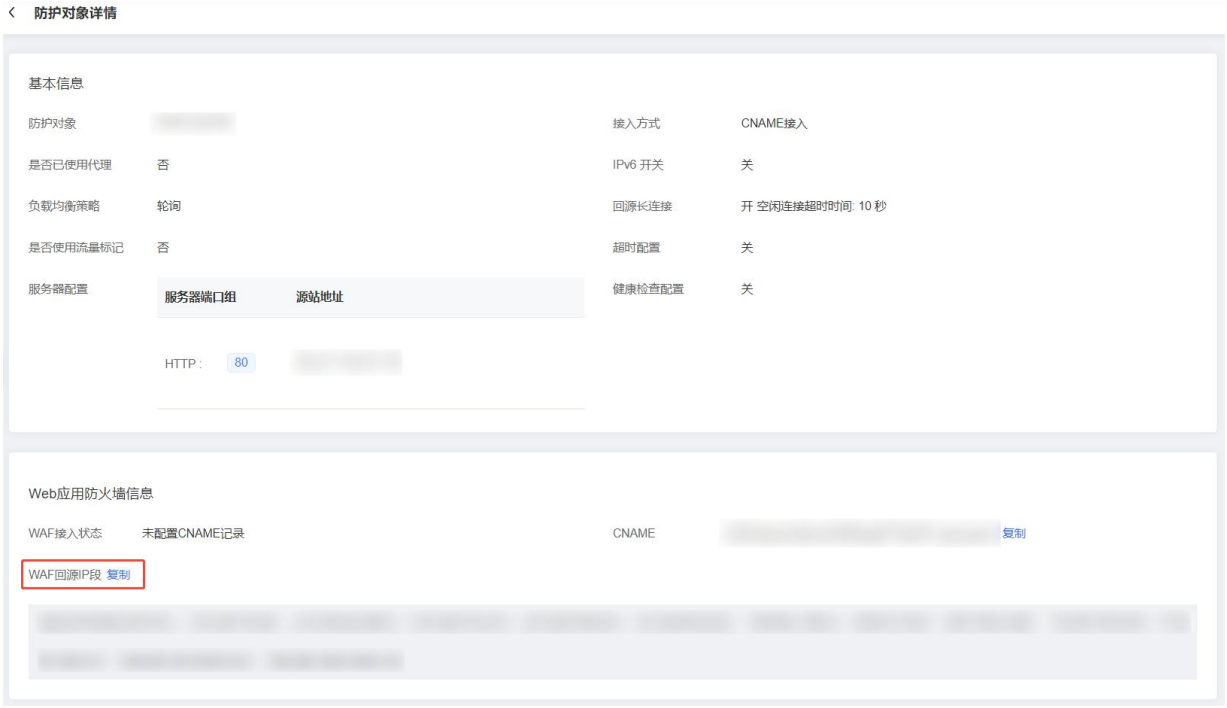
注意：

将源站加入白名单的操作需要将源站的回源 IP 加入到业务整个访问链路上所有安全设备的白名单，例如边界防火墙白名单、IPS 设备白名单、源站服务器中的安全组白名单以及服务器上具备访问控制能力的安全软件的白名单等。

获取 WAF 回源 IP 段

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏选择“接入管理”，默认进入“域名接入”页签。
5. 定位到已添加的防护对象，在操作列点击进入“详情”进入防护对象详情页。

6. 在“域名详情”页 Web 应用防火墙信息栏中，复制 WAF 回源 IP 地址。



放行 WAF 回源 IP 段

将获取到的 WAF 回源 IP 地址添加到源站安全软件的白名单中。

注意：

- 为了保证您的业务安全性，建议您在放行回源 IP 段时，仅配置入方向的放行策略，将回源 IP 段加入白名单，这样能够保证出方向的数据依然能够被 WAF 检测，从而避免攻击者绕过 WAF 直接对源站进行攻击。
- 请注意，如果没有将回源 IP 段添加到白名单列表，将会导致通过 WAF 回源的正常业务请求被拦截，导致业务无法正常提供服务。

4.1.1.4. 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。

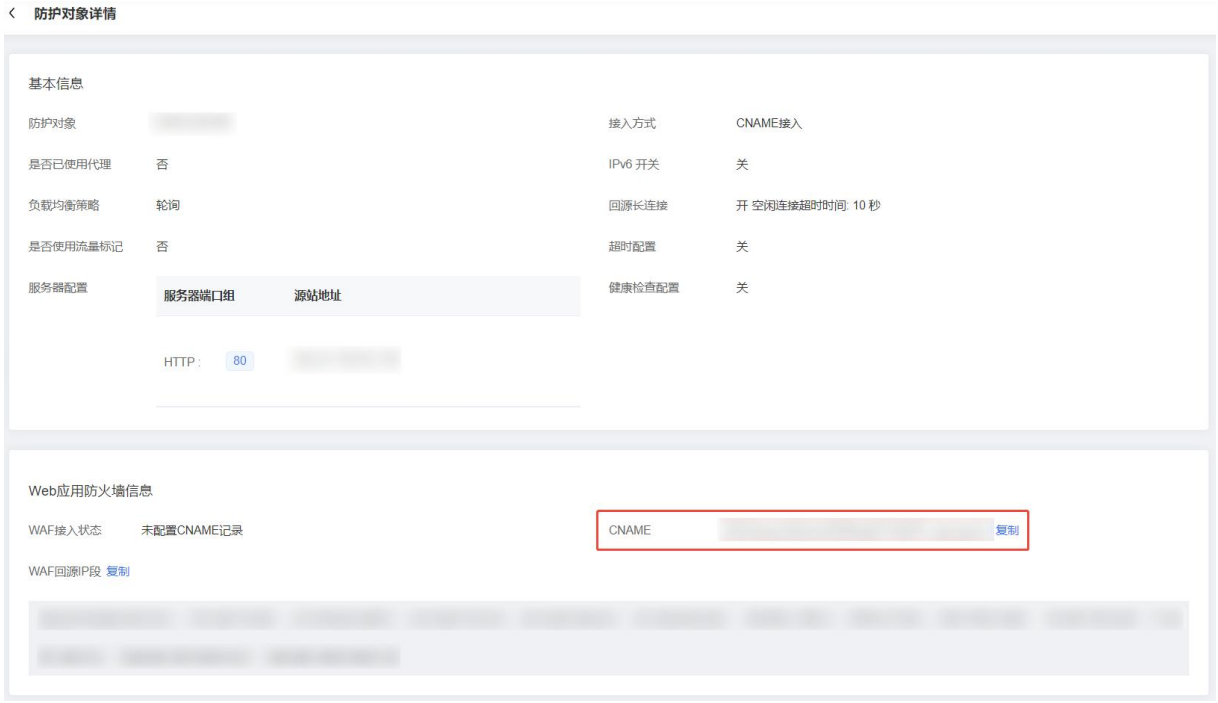
背景信息

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。

获取 WAF IP

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏选择“接入管理”，默认进入“域名接入”页签。
5. 定位到已添加的防护对象，在操作列点击进入“详情”进入防护对象详情页。

6. 在“防护对象详情”页中，复制该域名对应的 WAF CNAME 地址。



7. 在 Windows 操作系统中，打开 cmd 命令行工具。

8. 执行命令：**ping *已复制的 WAF CNAME 地址***。

9. 在 ping 命令的返回结果中，记录域名对应的 WAF IP 地址。

本地验证

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。

> 说明：
>
> 通过修改本机的 HOSTS 信息可以将本机对源站的域名请求强制修改至 WAF，从而实现通过本地对源站的访问经过 WAF 防护的业务流程验证。
>
> 改本地文件 HOSTS 信息的方式仅对本机生效，在此期间不会影响其他用户对源站的访问。

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。

4.1.1.5. 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。

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；

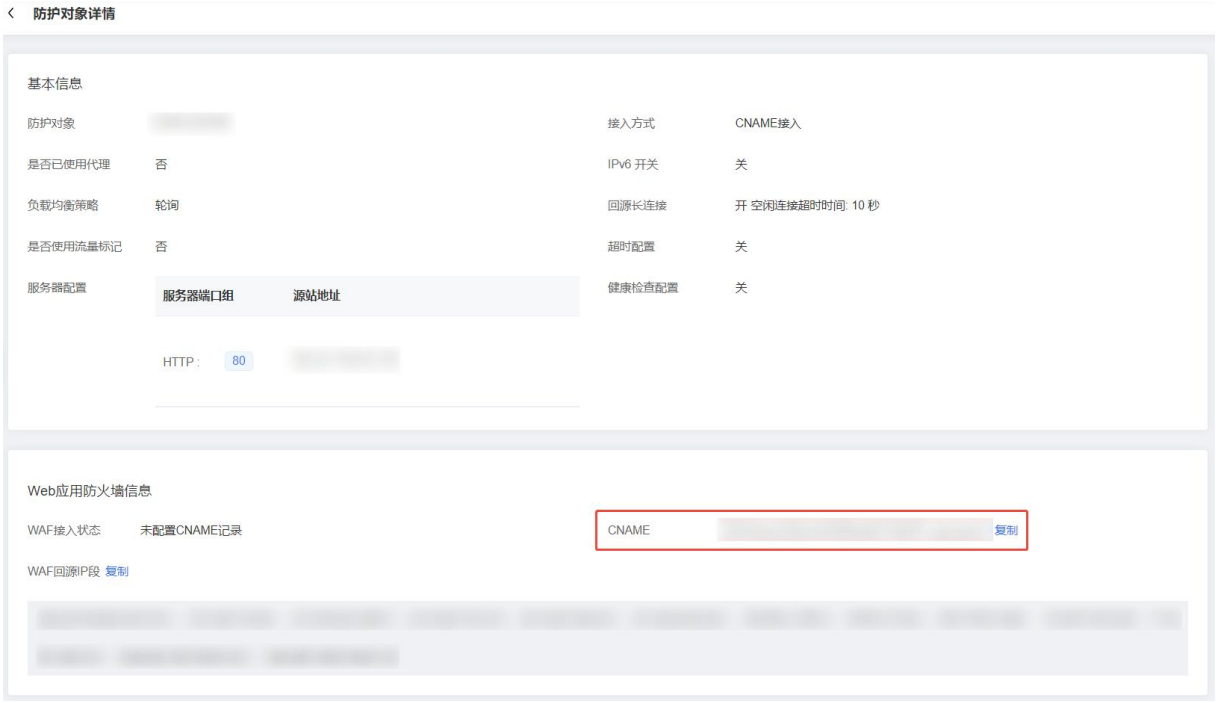
> 注意：
>
> 如果在 WAF 网站转发配置未生效时修改域名 DNS，可能导致业务中断。建议先通过本地验证，再修改域名 DNS。

- 拥有在域名的 DNS 服务商处修改域名解析设置的权限。

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，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏选择“接入管理”，默认进入“域名接入”页签。
5. 定位到已添加的防护对象，在操作列点击进入“详情”进入防护对象详情页。

6. 在“防护对象详情”页中，复制该域名对应的 WAF CNAME 地址。



修改域名 DNS 解析

- 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：

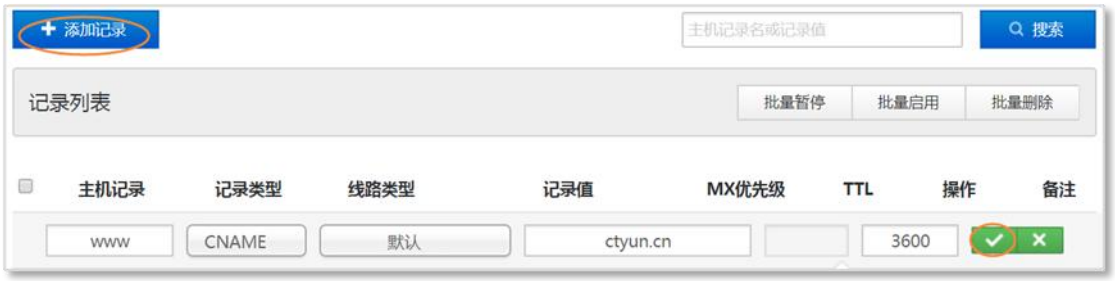
  为保证 WAF 的安全策略能够对真实的源 IP 生效，请确保网站接入时的“是否已使用代理”参数已配置“是”。

- 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，介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. 进入云解析产品控制台。
  2. 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。

4.1.1.6. 开启 IPv6 防护

如果需要对网站的 IPv6 请求流量进行防护，可以在域名接入 WAF 时开启 IPv6 功能。开启 IPv6 功能后，所有 IPv6 请求将先流转到 WAF，WAF 检测并过滤恶意攻击流量后，将正常流量转发给源站，实现恶意流量的拦截。

约束限制

- IPv6 功能仅支持在添加域名时配置，完成域名接入后 IPv6 配置无法修改，若需要修改，需要先删除已接入的域名，然后再重新接入域名。
  - 若您的域名接入时未开启 IPv6 功能，后续需要开启 IPv6 请求防护时，需要重新接入域名。

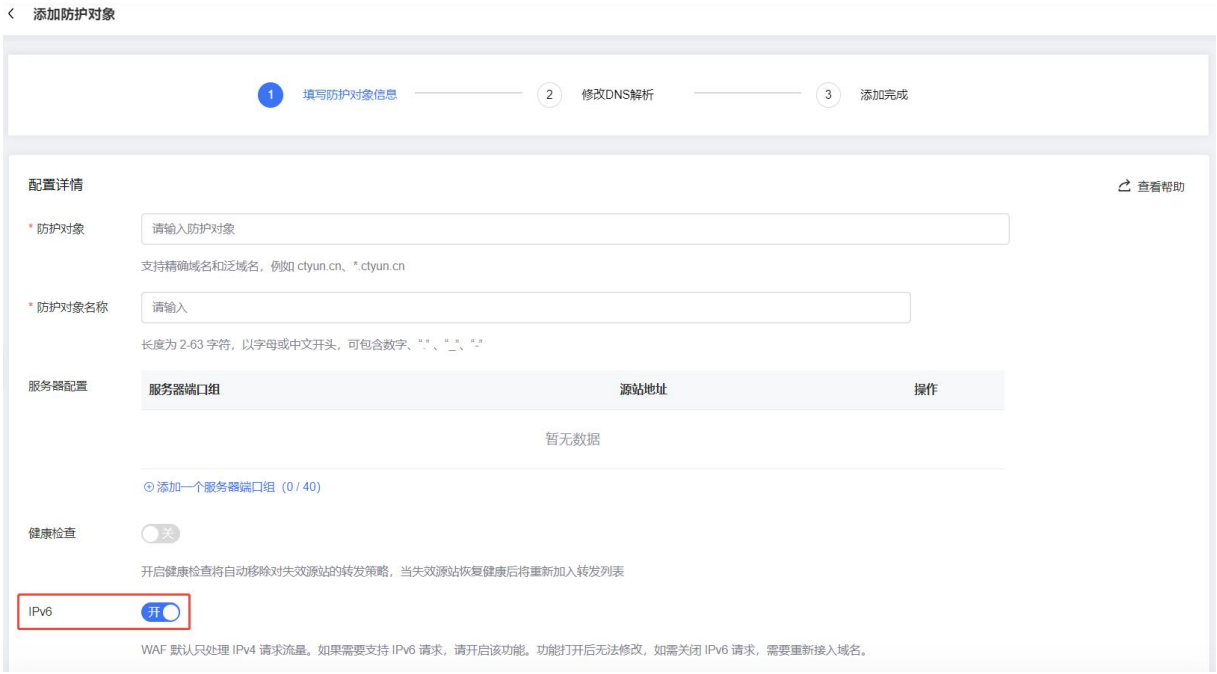
- 若您的域名接入时开启了 IPv6 功能，如需关闭 IPv6 请求防护，需要重新接入域名。

- 基础版不支持开启 IPv6 功能，若需要防护 IPv6 流量，请购买标准版、企业版或旗舰版。

开启 IPv6 防护

域名首次接入 WAF 防护

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏选择“接入管理”，默认进入“域名接入”页签。
5. 点击“添加防护对象”进入域名接入信息配置页，打开 IPv6 开关，其余参数说明及操作请参见“添加防护对象”。



域名已通过 IPv4 方式接入 WAF 防护

此时若需要开启 IPv6 防护，需要先删除已接入的域名，然后重新以 IPv6 方式接入防护。

1. 删除已接入 WAF 的域名。

   (1) 先到 DNS 服务商处，将该域名重新解析，指向源站服务器地址。

(2) 在“域名接入”页面，删除已接入的域名。

2. 重新以 IPv6 方式接入防护。详细操作请参见“域名首次接入 WAF 防护”。

4.1.2. 网站接入 WAF 防护（ELB 接入）

Web 应用防火墙（原生版）支持接入负载均衡（ELB）实例，您可以为使用 HTTP 或 HTTPS 监听协议的 ELB 监听器开启 WAF 防护。WAF 对进入监听器的应用层流量进行检测（不参与流量转发），您可根据自身应用需求设置相应的防护规则。

前提条件

- 该功能当前处于试用阶段，如需试用请通过天翼云控制台提工单进行申请。
- 已购买 WAF 云 SaaS 型实例，且实例版本为标准版及以上版本
- 实例支持防护的 ELB 监听器个数未超过配额限制。各个版本支持的配额请参见“产品规格”。

约束限制

- 目前仅支持防护**性能保障型**的负载均衡实例，不支持经典型实例。
- 目前仅支持为 HTTP/HTTPS 监听器开启安全防护。
- 目前仅支持防护“武汉 41”区域的 ELB 监听器。

在 WAF 控制台开启防护

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 进入到 WAF 控制台，在左侧导航栏选择“接入管理”，选择“云产品接入”页签。
5. 单击“添加防护对象”进入添加防护对象页面，配置防护对象参数。

配置项	说明
ELB（负载均衡	单击“选择 ELB（负载均衡器）”，弹出当前所在区域的 ELB 实例列表，找到目标

配置项	说明
器）	ELB，单击操作列的“选择”。
监听器	单击“选择监听器”，弹出所选 ELB 实例下的监听器列表，找到目标监听器，单击操作列的“选择”。 说明： 仅支持选择监听协议为 HTTP、HTTPS 的监听器。
防护对象名称	防护对象的名称，默认为“ELB 名称:监听器名称”，支持自定义。
域名	（可选）填写所选监听器下的域名，可添加精确域名和泛域名： 精确域名：支持多级别精确域名，例如主域名 ctyun.cn、子域名 www.ctyun.cn 等。 泛域名：支持使用泛域名格式，例如*.ctyun.cn 可以匹配 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。
备注	（可选）防护对象的描述信息，可以自定义。

6. 配置完成后单击“确定”，返回云产品接入页面。

说明：

ELB 监听器接入 WAF 后，**WAF 防护开关**默认“开启”，暂不支持在 WAF 控制台关闭防护。

在 ELB 控制台开启防护

请参见 HTTP/HTTPS 监听器开启安全防护（WAF 防护）。

配置防护规则

ELB 监听器接入 WAF 后，网站访问流量将经过 WAF 保护，**默认开启 Web 基础防护规则，防护规则组默认选择“正常规则组”，防护动作默认选择“观察”。**

监听器防护对象支持以下防护配置，您可以根据需要进行选择，实现有针对性的网站防护。

> 说明：
>
> 监听器防护对象的防护动作只支持“观察”、“拦截”。

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。	Web 基础防护
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
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
隐私屏蔽	通过设置隐私屏蔽规则，可屏蔽用户隐私信息，避免用户隐私信息出现在系统记录的日志中。	隐私屏蔽

4.1.3. 网站接入 WAF 防护（独享型接入）

4.1.3.1. 添加防护对象

使用独享型接入方式接入 WAF 前，需要先添加防护对象。

前提条件

已购买 WAF 独享型实例，且当前实例支持接入的防护对象数量未超过限制。

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，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 进入到云 WAF 控制台，在左侧导航栏选择“接入管理”，选择“独享型接入”页签。

5. 点击“添加防护对象”进入信息配置页，依次配置“防护对象”、“服务器配置”、“代理情况”、“负载均衡策略”等信息。

   配置项说明如下：

配置项	说明
选择实例	单击“选择实例”，通过下拉框选择可用的独享型实例。
防护对象	填写防护网站的域名或 IP。 ● 域名：支持添加精确域名和泛域名。 ■ 精确域名：支持多级别精确域名，例如主域名 ctyun.cn、子域名 www.ctyun.cn 等。

配置项	说明
	■ 泛域名：支持使用泛域名格式，例如*.ctyun.cn 可以匹配 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。 ● IP：支持防护公网 IP、私网 IP。 说明 如果此处配置私网 IP，请确保 WAF 到源站的网络路径是可访问的，以便于 WAF 能够对流量进行监控。
防护对象名称	自定义防护网站的显示名称。
服务器配置	单击“添加一个服务器端口组”，弹出新增服务器端口组窗口。 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：HTTP/HTTPS。 ● 端口：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：除以上标准端口以外的端口。 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

配置项	说明
	任何安全威胁。 ● 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。设置说明如下： ■ IP 地址格式：填写源站的私网 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 40 个源站 IP 或 40 个服务器域名。 ◆ 支持同时配置 IPv4 和 IPv6 地址。 说明 如果此处配置私网 IP，请确保 WAF 到源站的网络路径是可访问的，以便于 WAF 能够对流量进行监控。 ■ 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。 ● 权重：当负载均衡算法为“加权轮询”时生效，所有请求将此处配置的权重轮流分配给源站服务器，权重越大，回源到该源站的几率越高。 ■ 不输入则视同为最低权重 1。 ■ 当输入值为 0 时，业务不会回源到该站点。 ■ 取值范围：0~100 的正整数。 说明： 当健康检查发现站点出现问题时，剩余站点将按照剩余配置权重进行动态比例变化后的结果进行回源转发。
证书配置	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。 1. 点击“上传证书”，进入服务器端证书配置页面。 2. 选择证书类型，支持“通用证书”和“国密证书”。 3. 配置证书。支持证书选择、手动填写、文件上传方式： ● 证书选择：如您使用了证书管理服务，可通过下拉框选择已有证书。

配置项	说明
	● 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证书私钥中。 ● 文件上传：填写证书名称，点击“上传”，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，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。
高级设置	选择 HTTPS 后，还支持启用高级设置功能。 ● HTTPS 强制跳转：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。 ● TLS 协议版本：支持 TLS1.0、TLS1.1、TLS1.2。 ● SSL 解析方式：支持“单向认证”和“双向认证”。 说明 国密证书暂不支持双向认证。
健康检查	开启健康检查将自动移除对失效源站的转发策略，当失效源站恢复健康后将重新加入转发列表。 开启后，还需配置健康检查策略。
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：

配置项	说明
	● 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“源 IP 获取方式”。 **源 IP 获取方式**：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 x 层代理 ■ 从 HTTP 头 X-Client-IP 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不同的源站服务器。 ● IP Hash：将来自同一个 IP 的请求定向分配给同一个源站服务器。 ● 加权轮询：根据同一组回源地址内配置的权重进行加权回源，权重越大，回源到该源站的几率越高。 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。
流量标记	开启流量标记功能，WAF 在转发客户端请求到源站服务器时，通过在回源请求头部添加标记字段，标记该请求经过 WAF 转发，可以帮助源站判断请求来源。 如果请求中存在指定标记字段，则为 WAF 检测后的正常请求，放行该请求；如果请求中不存在指定标记字段，则为攻击者请求，拦截该请求。 单击“添加一个标记”，添加流量标记。最多支持添加 5 个标记字段。

配置项	说明
	支持如下标记类型： ● 自定义 Header，配置自定义 Header 名、Header 值。 ● 客户端真实源 IP，配置客户端真实源 IP 所在的 HTTP Header 名。 ● 客户端真实源端口，配置客户端真是源端口所在的 HTTP Header 名。 注意 请勿填写标准的 HTTP 头部字段，否则会导致标准头部字段内容被自定义的字段值覆盖。
回源长连接	● 功能开启后，支持回源长连接功能，最大支持 1000 个回源长连接。 开启“回源长连接”后，还需配置“空闲连接超时时间”，默认值为 10 秒，最多支持 60 秒。 ● 功能关闭后，将不支持 WebSocket。
超时配置	开启超时配置，可以配置如下超时时间： ● 连接超时时间：WAF 转发客户端请求时，与源站建立连接的超时时间。 ● 读连接超时时间：WAF 等待源站响应的超时时间。 ● 写连接超时时间：WAF 向源站发送请求的超时时间。 以上默认值均为 60 秒，最短支持 10 秒，最长支持 1200 秒。
备注	防护对象的描述信息，可以自定义。

6. 配置完成后单击“保存”，返回独享型接入页面。该网站的 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

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。	Web 基础防护
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
防敏感信息泄露	支持对网站返回的内容进行过滤（拦截、脱敏展示），过滤内容包括敏感信息、关键字和响应码。	防敏感信息泄露
网页防篡改	通过缓存页面和锁定访问请求，可避免页面被恶意篡改而带来的负面影响，对重点静态页面进行保护。	网页防篡改
Cookie 防篡改	通过对 Cookie 中的字段增加完整性校验保护，WAF 会新增一个 Cookie 字段用于篡改校验。	Cookie 防篡改
隐私屏蔽	通过设置隐私屏蔽规则，可屏蔽用户隐私信息，避免用户隐私信息出现在系统记录的日志中。	隐私屏蔽

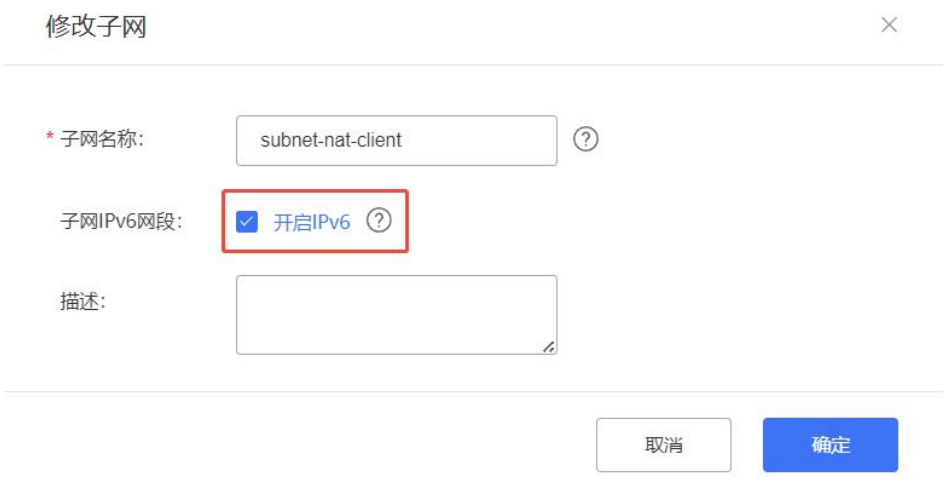
4.1.3.2. 开启 IPv6 防护

如果需要对网站的 IPv6 请求流量进行防护，需要**在购买 WAF 独享版实例时，选择已开启 IPv6 功能的 VPC 和子网。**

开启 IPv6 功能后，所有 IPv6 请求将先流转到 WAF，WAF 检测并过滤恶意攻击流量后，将正常流量转发给源站，实现恶意流量的拦截。

步骤一：子网开启 IPv6

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“网络 > 虚拟私有云”。
4. 选择对应的虚拟私有云，选择对应子网，点击子网后的“修改”进入修改子网页面，勾选“开启 IPv6”，单击“确定”。



步骤二：购买 WAF 独享版实例

在产品订购页面，选择已开启 IPv6 功能的子网，其他参数配置请参见**购买 WAF 独享版实例**。

步骤三：接入 WAF 防护

网站通过独享型接入方式接入 WAF 防护时，选择上述支持 IPv6 功能的实例，网站将自动开启 IPv6 防护。

详细操作请参见网站接入 WAF 防护（独享型接入）。

4.1.4. 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。

注意

非标端口可提工单申请开通，预计需要 3 个工作日。

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	443	2 个
标准版	标准端口	80、8080	443、8443	20 个
	非标准端口	1936, 1937, 1985, 2001, 3333, 3501, 3601, 4050, 5000, 5100, 5106, 5107, 5110, 5222, 5601, 5666, 5667, 5668, 5901, 6001, 6640, 6666, 6868, 7000, 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, 7744, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8012, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8095, 8096, 8097, 8098, 8099, 8106, 8181, 8334, 8336, 8443, 8686, 8765, 8780, 8800, 8880, 8888, 8889, 8980, 9000, 9001, 9002, 9003, 9011, 9021, 9023, 9027, 9037, 9040, 9080, 9081, 9082, 9100, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9999, 10000, 10001, 10040, 10080, 11033, 12601, 13201, 15080, 18080, 19090, 20080, 20202, 20203, 20204, 20205, 20443, 28080, 33702, 48800, 50751, 50761, 50776, 50780, 51654	4443, 5000, 5100, 5443, 5601, 5680, 6443, 6646, 6648, 6649, 6918, 7201, 7443, 7741, 7745, 7746, 7748, 7749, 7753, 7763, 7786, 8000, 8002, 8020, 8081, 8082, 8096, 8100, 8445, 8553, 8663, 8860, 8868, 8883, 8887, 8999, 9000, 9010, 9020, 9060, 9070, 9090, 9180, 9181, 9182, 9443, 9553, 9663, 10002, 10101, 10211, 10443, 10809, 12000, 12002, 12004, 12006, 13000, 13001, 13202, 13203, 18072, 18073, 18702, 18703, 18980, 30080, 30223, 30443, 33005	
企业版	标准端口	80、8080	443、8443	30 个
	非标准端口	1936, 1937, 1985, 2001, 3333, 3501, 3601, 4050, 5000, 5100, 5106, 5107, 5110, 5222, 5601, 5666, 5667, 5668, 5901, 6001, 6640, 6666, 6868, 7000, 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, 7744, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8012, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8095, 8096, 8097, 8098, 8099, 8106, 8181, 8334, 8336, 8443, 8686, 8765, 8780, 8800, 8880, 8888, 8889, 8980, 9000, 9001, 9002, 9003, 9011, 9021, 9023, 9027, 9037, 9040, 9080, 9081, 9082, 9100, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9999, 10000, 10001, 10040, 10080, 11033, 12601, 13201, 15080, 18080, 19090, 20080, 20202, 20203, 20204, 20205, 20443, 28080, 33702, 48800, 50751, 50761, 50776, 50780, 51654	4443, 5000, 5100, 5443, 5601, 5680, 6443, 6646, 6648, 6649, 6918, 7201, 7443, 7741, 7745, 7746, 7748, 7749, 7753, 7763, 7786, 8000, 8002, 8020, 8081, 8082, 8096, 8100, 8445, 8553, 8663, 8860, 8868, 8883, 8887, 8999, 9000, 9010, 9020, 9060, 9070, 9090, 9180, 9181, 9182, 9443, 9553, 9663, 10002, 10101, 10211, 10443, 10809, 12000, 12002, 12004, 12006, 13000, 13001, 13202, 13203, 18072, 18073, 18702, 18703, 18980, 30080, 30223, 30443, 33005	
旗舰版	标准端口	80、8080	443、8443	60 个
	非标准端口	1936, 1937, 1985, 2001, 3333, 3501, 3601, 4050, 5000, 5100, 5106, 5107, 5110, 5222, 5601, 5666, 5667, 5668, 5901, 6001, 6640, 6666, 6868, 7000, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020,	4443, 5000, 5100, 5443, 5601, 5680, 6443, 6646, 6648, 6649, 6918, 7201, 7443, 7741, 7745, 7746, 7748, 7749, 7753, 7763,	

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
		7021, 7022, 7023, 7024, 7025, 7026, 7070, 7071, 7081, 7082, 7083, 7088, 7097, 7510, 7744, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8012, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8095, 8096, 8097, 8098, 8099, 8106, 8181, 8334, 8336, 8443, 8686, 8765, 8780, 8800, 8880, 8888, 8889, 8980, 9000, 9001, 9002, 9003, 9011, 9021, 9023, 9027, 9037, 9040, 9080, 9081, 9082, 9100, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9999, 10000, 10001, 10040, 10080, 11033, 12601, 13201, 15080, 18080, 19090, 20080, 20202, 20203, 20204, 20205, 20443, 28080, 33702, 48800, 50751, 50761, 50776, 50780, 51654	7786, 8000, 8002, 8020, 8081, 8082, 8096, 8100, 8445, 8553, 8663, 8860, 8868, 8883, 8887, 8999, 9000, 9010, 9020, 9060, 9070, 9090, 9180, 9181, 9182, 9443, 9553, 9663, 10002, 10101, 10211, 10443, 10809, 12000, 12002, 12004, 12006, 13000, 13001, 13202, 13203, 18072, 18073, 18702, 18703, 18980, 30080, 30223, 30443, 33005	

4.1.5. 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
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

OpenSSL 名称	RFC 名称	TLS 支持的版本
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
ECDHE-SM2-SM4-GCM-SM3	ECDHE_SM4_GCM_SM3	TLS1.1

OpenSSL 名称	RFC 名称	TLS 支持的版本
ECDHE-SM2-SM4-CBC-SM3	ECDHE_SM4_CBC_SM3	TLS1.1
ECC-SM2-SM4-CBC-SM3	ECC_SM4_CBC_SM3	TLS1.1
ECC-SM2-SM4-GCM-SM3	ECC_SM4_GCM_SM3	TLS1.1
RSA-SM4-CBC-SM3	RSA_SM4_CBC_SM3	TLS1.1
RSA-SM4-GCM-SM3	RSA_SM4_GCM_SM3	TLS1.1
RSA-SM4-CBC-SHA256	RSA_SM4_CBC_SHA256	TLS1.1
RSA-SM4-GCM-SHA256	RSA_SM4_GCM_SHA256	TLS1.1

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。

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. 防护对象管理

4.2.1. 自定义网站响应页面

当访问者触发 WAF 拦截时，系统默认会显示 WAF 内置的响应页面。

若您需要自定义响应页面的内容和样式，可以参照本文准备自定义页面的内容，然后提交工单联系技术支持进行配置。

前提条件

网站已接入 WAF 进行防护。

准备工作

您需要准备自定义页面的如下信息：

- 响应码：自定义页面的返回码。
- 页面类型：支持 text/html、text/xml、application/json 类型。
- 页面内容：根据页面类型准备对应的页面内容。

操作步骤

1. 进入提交工单页面。
2. 在工单页面填写已准备好的自定义页面内容，并提交工单。
3. 等待工单审核，工单审核通过后，技术支持会联系您确认并配置自定义响应页面。
4. 配置完成后，您可以参考以下步骤验证修改效果。
   a. 配置 Web 基础防护规则，将处置动作配置为“拦截”。
   b. 模拟攻击者访问防护网站，若攻击被拦截后的返回页面为自定义响应页面的内容，则表示配置成功。

4.3. 防护配置

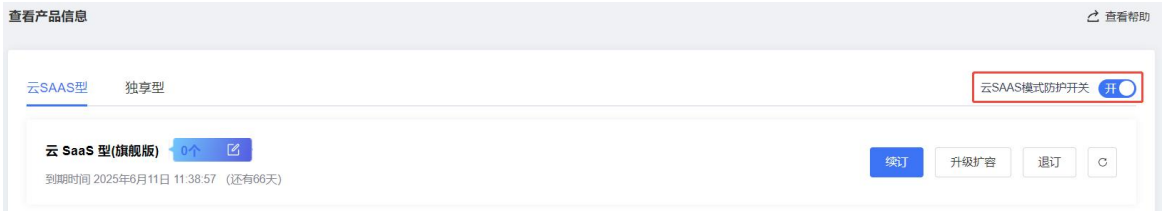
4.3.1. WAF 防护概述

WAF 防护配置是 WAF 防护的核心功能，对不同模块和不同层次的防护策略配置，可以实现灵活多变，适配不同场景的安全防护要求。WAF 支持多层级的防护功能控制，也支持多模块的防护功能控制，通过对防护功能的设置，实现您对 Web 业务的安全防护需求。

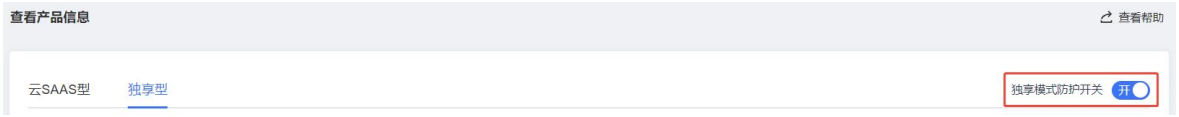
WAF 防护控制层级

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，从而实现对业务网站的灵活防护。

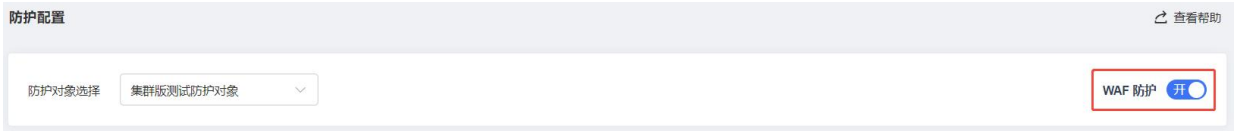
- WAF 总开关：可以控制当前 WAF 实例的防护状态。关闭 WAF 总开关后，所有域名的防护状态均关闭。WAF 将只进行流量转发，不会拦截攻击行为也不会记录攻击日志。
  - 云 SAAS 型实例总开关



  - 独享实例总开关



- 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。
  - 安全防护模块包括 Web 基础防护、CC 防护、精准访问控制、IP 黑白名单、地域访问控制、防敏感信息泄露、网页防篡改、防护白名单、BOT 防护。
  - 系统配置模块包括 Cookie 防篡改、隐私屏蔽、攻击惩罚。

- 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，关闭某条防敏感信息泄露规则的防护状态。

4.3.2. 对象防护配置（安全防护）

4.3.2.1. Web 基础防护

4.3.2.1.1. 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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“Web 基础防护”模块，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

配置项	说明
	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。

4.3.2.1.2. 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。

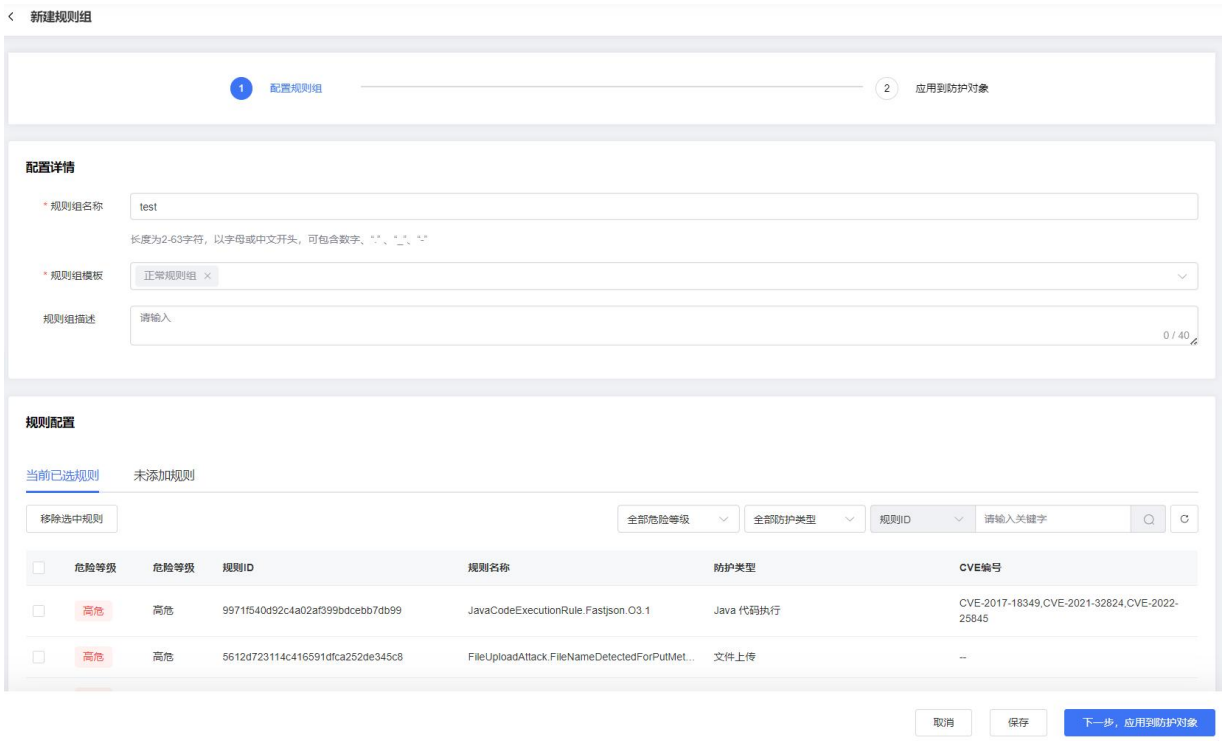
操作步骤

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“Web 基础防护”模块，在防护规则组后方点击“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。



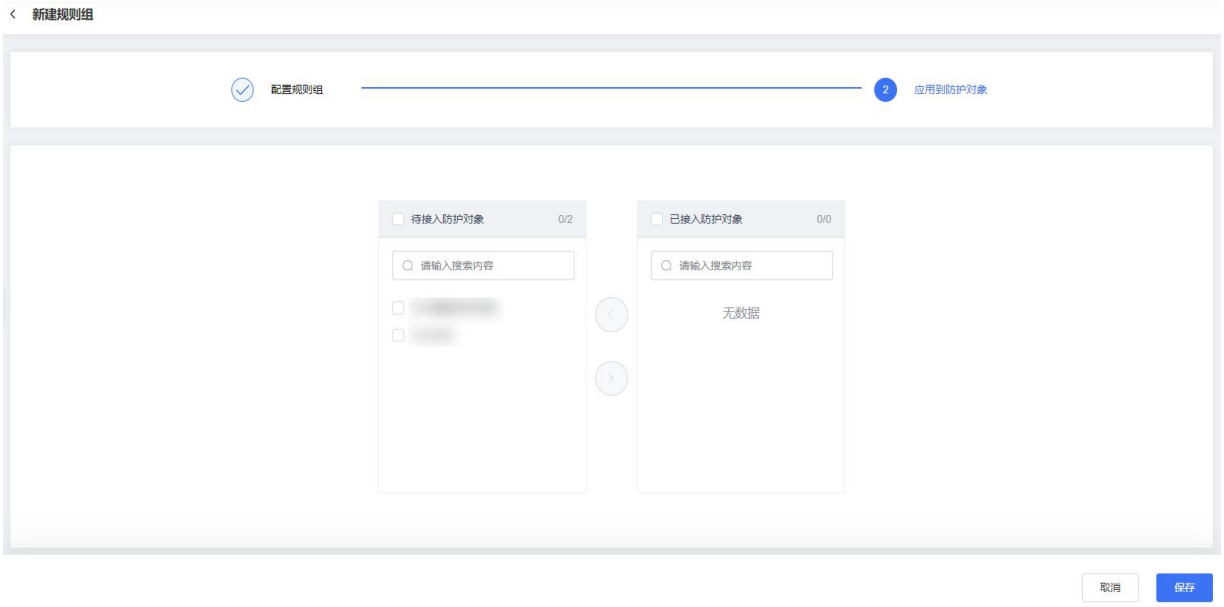
配置项	说明
规则组名称	设置规则组的名称。 规则组名称用于标识当前规则组，建议您使用有明确含义的名称。
规则组模板	选择要应用的规则组模板。可选项： • 严格规则组 • 中等规则组 • 宽松规则组 • 其他自定义规则组 规则组模板可以多选，系统会将所选的规则组最大集作为模板，下一步基于该集合规则配置。

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。

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；

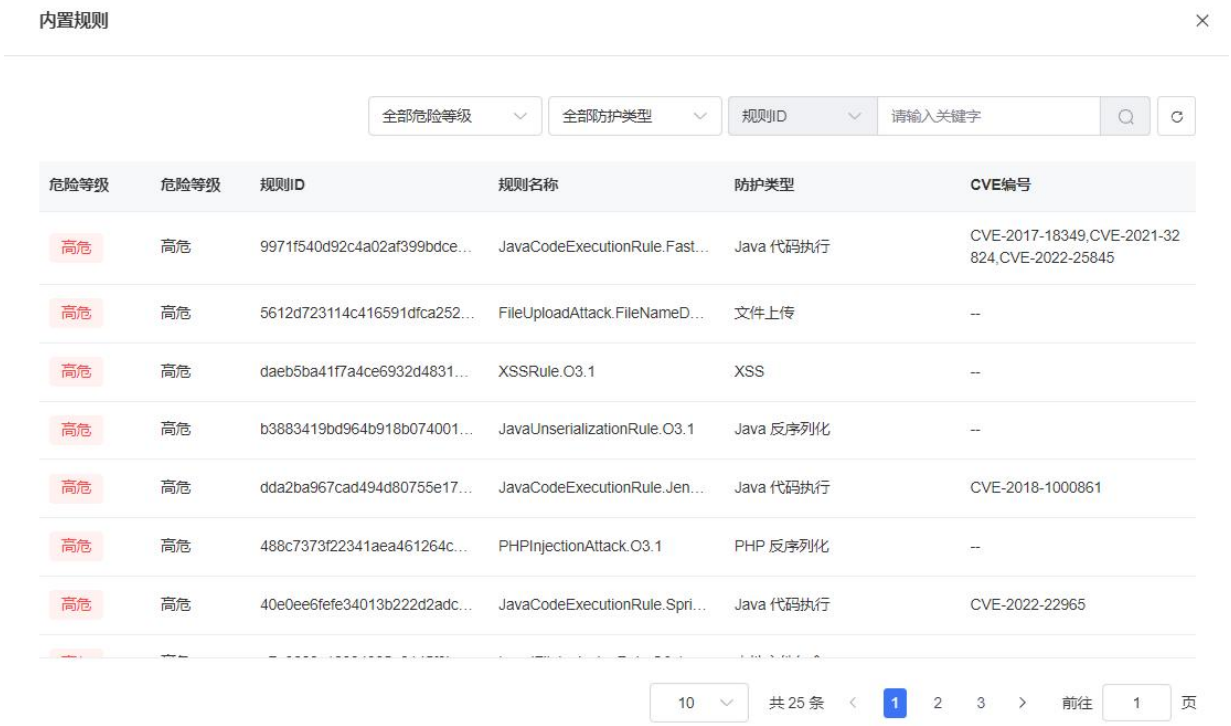
10. （可选）将规则组应用到域名防护。从“待接入域名”列表中选择要应用当前规则组的域名，添加到“已接入域名”列表，点击“保存”。

> 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况。

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。



相关操作

对于已创建的规则组，您可以执行以下操作：

- 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。
- 删除：删除自定义防护规则组。系统默认规则组不支持删除。

4.3.2.1.3. 查看内置防护规则

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

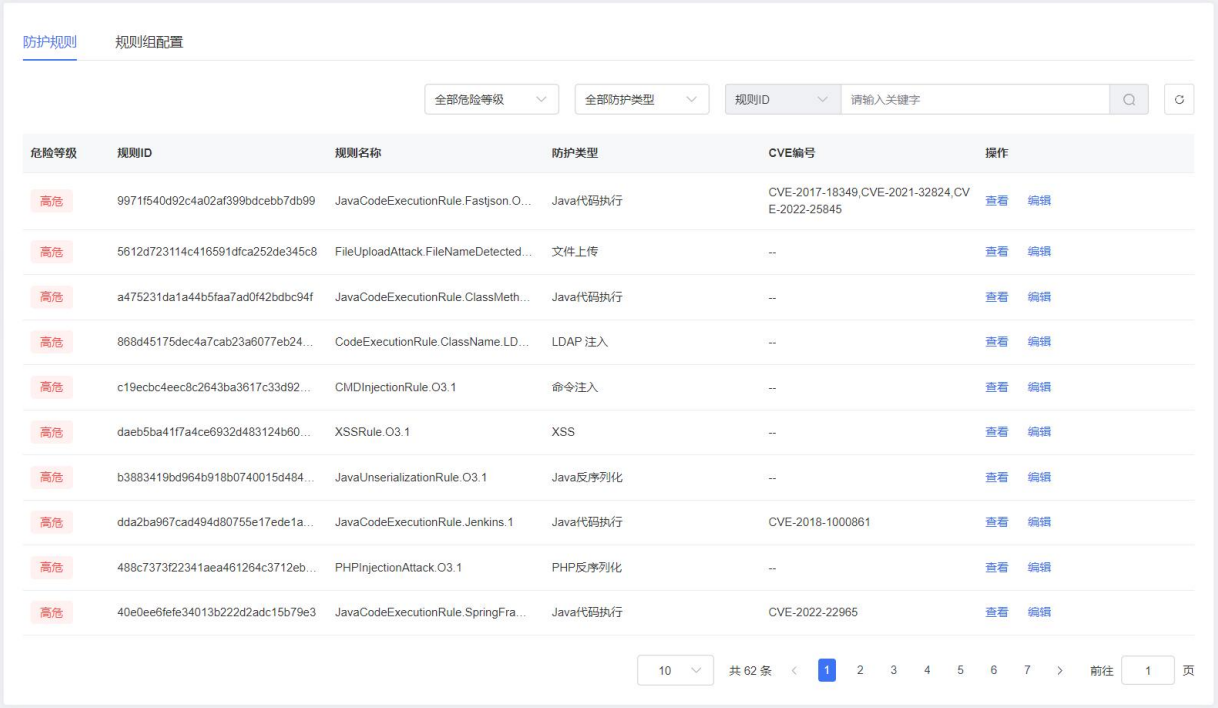
操作步骤

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。

5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“Web 基础防护”模块，在防护规则组后方点击“前去配置”。

7. 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
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
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。
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。
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。

相关操作

对于某条特定规则，您可以执行以下操作：

- 查看：查看当前规则所属的规则组。
- 编辑：将当前规则添加至某个自定义规则组。

4.3.2.1.4. 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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“防护白名单”模块，点击防护规则右侧的“前去配置”。

7. 进入“白名单”页面，可以查看当前已创建的白名单规则列表。

8. 单击“新建白名单”，在弹出的对话框中，配置白名单规则。

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规则组，建议您使用有明确含义的名称。
规则描述	可选项。设置规则的描述信息。
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。
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
生效范围	设置白名单生效范围，表示触发匹配条件的请求不受所选规则的检测，可选项： ● 全部规则：规则防护引擎包含的全部规则。选择该项，表示触发匹配条件的请求不受任何防护模块的检测，将被直接放行到源站服务器。 ● 特定模块：只忽略检测指定的防护模块，支持 BOT 防护和 Web 基础防护。在模块右侧的下拉框，选择不检测的规则类型。 ● 特定规则 ID：只忽略检测指定的规则，在模块右侧的下拉框，选择不检测的规则 ID。

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，并根据需要禁用、编辑或删除规则。

4.3.2.2. 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。

配置 CC 防护模式

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“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。

配置项	说明
状态	开启或关闭 CC 安全防护功能。
防护模式	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拦截。 说明： 防护模式只能选择一种，不能同时开启。

自定义 CC 防护策略

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“CC 防护”模块，在防护模式后方点击“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 3 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

配置项	说明
	SESSION 信息。 ◆ SESSION 位置：可选择 GET、POST、COOKIE、HEADER。 ◆ 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），系统将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 将根据配置的处置动作处理。配置项如下： ■ 阈值（次）：统计时长内统计对象的允许访问的次数，超过阈值，则触发频率限制。 ■ 统计时长（秒）：统计周期。
处置动作	定义触发规则后执行的动作，支持“拦截”。
优先级	代表该规则在 CC 防护模块中执行的优先级。 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。

相关操作

对于已创建的规则，您可以执行以下操作：

- 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；
- 删除：若不再使用某条规则，可对该规则进行删除；
- 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。

4.3.2.3. 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。

使用限制

基础版不支持精准访问控制功能，请升级到更高版本使用。

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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“精准访问控制”模块，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：选择拦截时，支持开启“攻击惩罚”。

配置项	说明
	若需使用攻击惩罚功能，需将 WAF 升级到企业版或旗舰版。 ● 放行 ● 验证码 ● js 挑战 ● 重定向
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“保存”，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

对于已创建的规则，您可以执行以下操作：

- 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；
- 删除：若不再使用某条规则，可对该规则进行删除；
- 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。

4.3.2.4. 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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“IP 黑白名单”模块，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

配置项	说明
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。

相关操作

对于已创建的规则，您可以执行以下操作：

- 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。
- 删除：若不再使用某条规则，可对该规则进行删除。
- 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。

4.3.2.5. 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. 单击页面顶部的区域选择框，选择区域。

3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“地域访问控制”模块，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。

配置项	说明
防护目标	需输入完整防护的网页路径或端口。 例如 https://www.ctyun.cn/index.html，其中 https://为协议类型，www.ctyun.cn 为域名地址，/index.html 为路径地址。 ● 路径不支持通配符(例如 /*)或参数(例如 /abc?xxx=yyy 中，xxx=yyy 为参数部分)。 ● 支持输入端口，如 https://www.ctyun.cn:443 或 https://www.ctyun.cn:443/index.html，当输入端口时，则防护对象为端口地址。
地理位置	IP 访问来源的地理范围，可以选择“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。

相关操作

对于已创建的规则，您可以执行以下操作：

- 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。
- 删除：若不再使用某条规则，可对该规则进行删除。
- 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

区域	省市自治区
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

区域	国家（按英文首字母区分）
	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

区域	国家（按英文首字母区分）
	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

4.3.2.6. 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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“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。

配置项	说明
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”。

4.3.2.7. 防护白名单

网站域名接入 Web 应用防火墙后，您可以选择开启白名单功能，并配置白名单规则。

- 可用于放行具有指定特征的请求，使请求不经过全部或特定防护模块（Web 基础防护、BOT 防护）的检测。
- 也可用于处理误报事件，对于误报的事件可进行规则级别的加白，将单次拦截放通。

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

基础版不支持白名单功能，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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。

4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。

5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到“防护白名单”模块，可以选择开启/关闭防护。

7. 点击防护规则右侧的“前去配置”，进入防护白名单页面。

8. 单击“新建白名单”，在弹出的对话框中，配置白名单规则。

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。
规则描述	可选项。设置规则的描述信息。
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 30 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”。
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
生效范围	设置白名单生效范围，表示触发匹配条件的请求不受所选规则的检测，可选项： ● 全部规则：规则防护引擎包含的全部规则。选择该项，表示触发匹配条件的请求不受任何防护模块的检测，将被直接放行到源站服务器。

配置项	说明
	● 特定模块：只忽略检测指定的防护模块，支持 BOT 防护和 Web 基础防护。在模块右侧的下拉框，选择不检测的规则类型。 ● 特定规则 ID：只忽略检测指定的规则，在模块右侧的下拉框，选择不检测的规则 ID。

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

对于已创建的白名单规则，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”。

4.3.2.8. 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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”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。

配置项	说明
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”。

4.3.2.9. 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 防护模块提供了默认内置的防护规则，用户也可以自定义添加防护规则。

- 系统默认规则

  WAF 提供已知公开的 BOT 大类，包括 Web 爬虫、扫描器爬虫、语言库等爬虫类型，用户可以根据自身需求设置防护状态及处置动作，WAF 将对命中的 BOT 请求进行相应处理。

- 自定义防护规则

  用户可以根据实际业务情况自定义防护规则，WAF 将根据命中防护规则的请求进行处理。

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。

配置 BOT 防护模式

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”页签定位到 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： 点击“前去配置”，可以进入到对应的策略配置页面进行配置。

配置防护策略

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 在“安全防护”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。

查看系统默认规则

系统内置了 BOT 防护规则，该防护规则会和用户自定义防护规则同时生效。

- 规则状态：规则支持开启和关闭，若不需要检测该类爬虫类型，可选择关闭某条规则。
- 修改规则的处置动作：单击操作列的“编辑”，可以修改该规则的处置动作。
- 筛选列表：单击列表右上角的“过滤条件”，可以对列表进行筛选查询。

添加自定义防护规则

自定义防护规则列表展示当前用户已创建的规则，包括规则状态、规则名称/规则 ID、匹配条件、处置动作、优先级、风险等级、更新时间等。

单击“新建防护规则”，在规则配置页面，完成以下信息配置，然后单击“保存”。新建的规则默认状态为开启。

自定义防护规则参数说明如下：

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。
防护目标	需输入完整防护的网页路径或端口。 例如 https://www.ctyun.cn/index.html，其中 https://为协议类型，www.ctyun.cn 为域名地址，/index.html 为路径地址。 ● 路径不支持通配符(例如 /*)或参数(例如 /abc?xxx=yyy 中，xxx=yyy 为参数部分)。 ● 支持输入端口，如 https://www.ctyun.cn:443 或 https://www.ctyun.cn:443/index.html，当输入端口

配置项	说明
	时，则防护对象为端口地址。
会话识别	支持 IP、SESSION、REFERER。 ● 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 位置：可选择 QUERY、HEADER、BODY、COOKIE。 ◆ 选择 QUERY 时，则在整个请求中查找会话标识。 ◆ 选择 HEADER 时，则在 HEADER 中查找会话标识。 ◆ 选择 BODY 时，则在 Form 类型的 BODY 中查找会话标识。 ◆ 选择 COOKIE 时，则在 COOKIE 中查找会话标识。 ■ 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），系统将据此标识匹配到的内容识别访问者。 当输入 test 时，将以 JSON 字符串中 test 参数的值为会话标识；当输入 test1.test2，将以 JSON 字符串中 test1 中包含有 test2 参数的值为会话标识。 ● REFERER：根据 Referer（自定义请求访问的来源）字段区分单个 Web 访问者。
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 30 个条件。存在多个条件时，多个条件必须同时满足才算命中。 当选择统计类的逻辑符（统计次数、统计个数）时，还需设置“统计周期”。 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。 ● 当选择统计类的逻辑符时，处置动作支持： ■ 动态拦截：选择动态拦截时，还需要设置动态拦截的持续时间，表示触发规则后，访问对象被拦截的时长；选择动态拦截时，支持开启“攻击惩罚”。 ■ 限速：选择限速时，还需要配置限速频率，触发规则后，将按照配置的限速频率对访问对象进行限速。 ● 当选择除统计类之外的逻辑符时，处置动作支持：

配置项	说明
	■ 观察 ■ 拦截：选择拦截时，支持开启“攻击惩罚”。 ■ 放行 ■ 验证码 ■ JS 验证 ■ 重定向 说明： 当处置动作选择拦截、动态拦截时，可触发攻击惩罚，攻击惩罚功能可将多次触发自定义规则的会话对象进行自动拉黑封禁。 若需使用攻击惩罚功能，需将 WAF 升级到企业版或旗舰版。
风险等级	包括高危、中危、低危、无威胁。
优先级	代表该规则在 BOT 防护模块中执行的优先级。 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。
规则描述	规则的描述信息，用户可自定义。

相关操作：

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：

- 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；
- 删除：若不再使用某条规则，可对该规则进行删除；
- 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。

添加动态防护规则

动态防护规则列表展示当前用户已创建的规则，包括规则状态、规则名称/规则 ID、处置动作、优先级、防护目标、防护功能、更新时间等。

单击“新建防护规则”，在规则配置页面，完成以下信息配置，然后单击“保存”。新建的规则默认状态为开启。

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。
防护目标	需输入完整防护的网页路径或端口。 例如 https://www.ctyun.cn/index.html，其中 https://为协议类型，www.ctyun.cn 为域名地址，/index.html 为路径地址。 ● 路径不支持通配符(例如 /*)或参数(例如 /abc?xxx=yyy 中，xxx=yyy 为参数部分)。 ● 支持输入端口，如 https://www.ctyun.cn:443 或 https://www.ctyun.cn:443/index.html，当输入端口时，则防护对象为端口地址。
排除目标	通过输入排除条件，排除不需要防护的地址范围，支持多行输入，每一行为一个排除条件地址。最大支持 20 行。
动态令牌	默认对每一次请求数据进行签名验证，验证不通过的请求将被拦截。
客户端环境验证	勾选“客户端指纹检测”，可以对浏览器版本检测、客户端 IP 地址检测。
页面防调试	默认开启，用户可根据实际情况进行选择。开启页面防防调试功能后，能够防止用户对页面的调试。 注意： 由于该功能会对业务的请求和响应进行混淆，所以使用该功能可能导致页面异常，请谨慎使用。建议在需要进行防护的敏感目录下开启此防护功能。
处置动作	支持“观察”、“拦截”。

配置项	说明
优先级	代表该规则在当前防护模块中执行的优先级。 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。
规则描述	规则的描述信息，用户可自定义。

查看拦截列表

当会话触发了自定义防护规则中配置的动态拦截或限速策略，可在动态防护列表中查看已被拦截或限速的对象。用户也可以根据实际情况，手动解除动态拦截/限速状态。

1. 单击拦截列表右侧的“解除拦截”。

2. 进入动态防护列表，可按“动态拦截”、“限速”查看防护对象，可手动解除动态拦截/限速状态。

   对于正在拦截中/限速中的对象，单击操作列的“解除拦截”可放开拦截/限速对象。

4.3.3. 对象防护配置（系统配置）

4.3.3.1. 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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 选择“系统配置”页签，定位到“Cookie 防篡改”模块，可以选择开启/关闭防护。

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。

配置项	说明
	● 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。

4.3.3.2. 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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。

5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 选择“系统配置”页签，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。

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。
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”。

4.3.3.3. 攻击惩罚

网站域名接入 Web 应用防火墙后，您可以选择开启攻击惩罚功能。开启并配置攻击惩罚功能后，当 WAF 检测到访问者的 IP、Cookie 或请求参数中有恶意请求时，WAF 将按配置的攻击惩罚时长来自动封禁访问者。

配置的攻击惩罚标准会提供给 BOT 防护、精准访问控制防护模块使用。当配置 BOT 防护规则、精准访问控制规则时，可使用攻击惩罚标准功能。

- BOT 防护规则：当处置动作选择拦截、动态拦截时，支持勾选“攻击惩罚”。
- 精准访问控制规则：当处置动作选择拦截时，支持勾选“攻击惩罚”。

攻击惩罚对象

攻击惩罚的对象包含 IP 以及 SESSION 会话对象。

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攻击惩罚功能，请升级到更高版本使用。

配置攻击惩罚标准

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 对象防护配置”，进入防护配置页面。
5. 在“防护配置”页面上方的“防护对象选择”下拉框，切换到要设置的域名。

6. 选择“系统配置”页签，定位到“攻击惩罚”模块，可以选择开启/关闭防护。

7. 单击攻击惩罚右侧的“前去配置”，进入攻击惩罚配置页面。

8. 配置攻击惩罚参数。

配置项	说明
拦截周期	配置初次拦截的时长，即第一次惩罚的时长。 单位为“分钟”，可输入 10~60 的整数。 说明：攻击惩罚与动态拦截同时生效，实际拦截时长按照攻击惩罚和动态拦截的最大时间进行拦截。
每次增长时长	配置多次拦截的增长时长，即在上一次惩罚时长的基础上增长对应的时间。 单位为“分钟”，可输入 10~60 的整数，10 代表拦截时长每次增长 10 分钟。
最多拦截次数	配置最多拦截的次数。 可输入 1~5 的数字，1 代表着惩罚目标增长 1 次处罚时间，下一次被永久拦截。5 代表惩罚目标增长 5 次处罚时间后，下一次被永久拦截。
生效范围	默认为全部规则。

9. 单击“确认”，完成攻击惩罚配置。

查看攻击惩罚列表

> 说明：
>
> 需要在相应防护规则配置时勾选“攻击惩罚”，才会对触发规则的对象进行惩罚。

在“攻击惩罚”模块，单击惩罚列表右侧的“前去配置”，进入惩罚列表页面，可查看攻击惩罚拦截对象。

解除惩罚：对于正在惩罚中的拦截对象，单击操作列的“解除惩罚”可放开惩罚对象封禁。

4.3.4. 全局防护配置

4. 3. 4. 1. 防护白名单

防护对象接入 Web 应用防火墙后，您可以选择开启全局白名单功能，并配置白名单规则。

- 可用于放行具有指定特征的请求，使请求不经过全部（包含 Web 基础防护、CC 防护、BOT 防护、精准访问控制）或特定防护模块（Web 基础防护）的检测。
- 也可用于处理误报事件，对于误报的事件可进行规则级别的加白，将单次拦截放通。

前提条件

- 已购买 WAF 云 SaaS 型实例，且实例版本为标准版及以上版本。
- 网站已通过“域名接入”方式接入 WAF 进行防护。

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，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 全局防护配置”，进入全局防护配置页面。
5. 定位到“防护白名单”模块，可以选择开启/关闭防护。

6. 点击防护规则右侧的“前去配置”，进入白名单页面。

7. 单击“新建白名单”，在弹出的对话框中，配置白名单规则。

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。
接入对象	设置白名单作用对象，支持选择“全部防护对象”或选择“特定防护对象”。 说明：全局白名单不支持不支持独享版防护对象和监听器防护对象。
规则描述	可选项。设置规则的描述信息。
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 30 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。

配置项	说明
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
生效范围	设置白名单生效范围，表示触发匹配条件的请求不受所选规则的检测，可选项： ● 全部规则：选择该项，表示触发匹配条件的请求不受 Web 基础防护、CC 防护、BOT 防护、精准访问控制模块的检测，将被直接放行到源站服务器。 ● 特定模块：只忽略检测指定的防护模块，支持 Web 基础防护。在模块右侧的下拉框，选择不检测的规则类型。 ● 特定规则 ID：只忽略检测指定的规则，支持 Web 基础防护。在模块右侧的下拉框，选择不检测的规则 ID。

8. 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

对于已创建的白名单规则，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”。

4.3.4.2. 精准访问控制

防护对象接入 Web 应用防火墙后，您可以选择开启全局精准访问控制功能，并配置精准访问控制规则。

全局精准访问控制支持对全局域名或单个域名生效。

全局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，有针对性地阻断各类攻击行为。

前提条件

- 已购买 WAF 云 SaaS 型实例，且实例版本为标准版及以上版本。
- 网站已通过“域名接入”方式接入 WAF 进行防护。

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，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护配置 > 全局防护配置”，进入全局防护配置页面。
5. 定位到“精准访问控制”模块，可以选择开启/关闭防护。

6. 点击防护规则右侧的“前去配置”，进入全局精准访问控制页面。

7. 单击“新建防护规则”，配置全局精准访问控制规则。

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。
接入对象	设置精准访问控制规则的作用对象，支持选择“全部防护对象”或选择“特定防护对象”。 说明：全局精准访问控制不支持独享版和监听器防护对象。
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

配置项	说明
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。

8. 单击“保存”，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

对于已创建的全局精准访问控制规则，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”。

4.3.5. 重保防护场景

重保防护支持配置全局 IP 黑白名单，对经过云 WAF 防护域名的访问源 IP 进行黑白名单设置，来自黑白名单中的 IP 地址/IP 地址段的访问，WAF 将不会做任何检测，直接拦截/放行。

- 支持添加 IPv4、IPv6 地址，支持添加 IP 地址段。
- 重保防护提供的全局 IP 黑白名单，检测逻辑优先级高于 IP 黑白名单检测；内部检测逻辑，白名单高于黑名单。

前提条件

- 已购买 WAF 云 SaaS 型实例，且实例版本为标准版及以上版本。
- 网站已通过“域名接入”方式接入 WAF 进行防护。

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，选择区域。

3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。

4. 在左侧导航栏，选择“防护配置 > 重保防护场景”，进入重保防护配置页面。

5. 单击“新建黑白名单”，弹出新建黑白名单规则窗口，配置黑白名单规则参数，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。
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。
生效范围	支持选择“全部防护对象”或“特定防护对象”。 ● 全部防护对象：配置的黑白名单规则对所有已接入的域名生效。 ● 特定防护对象：配置的黑白名单规则仅对所选域名生效，可以选择多个域名。 说明：不支持独享版防护对象和监听器防护对象。

6. 配置完成后，单击“确定”。可以在列表中查看已新建的黑白名单规则。

相关操作

对于已创建的规则，您可以执行以下操作：

- 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、生效范围。
- 删除：若不再使用某条规则，可对该规则进行删除。
- 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。

4.3.6. 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、相等、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、相等、正则匹配	请求的参数 key，包括 query 和 form，如 /?p=123 中的 p
Cookie	包含、相等、正则匹配、统计次数、统计个数	请求的 Cookie 值
请求路径	包含、相等、正则匹配、统计次数、统计个数	请求的路径，不包含域名和参数，未解码
请求 URI	包含、相等、正则匹配、统计次数、统计个数	请求的 URI，带参数
请求头值	包含、相等、正则匹配	请求 header 的值
请求头名	包含、相等、正则匹配	请求 header 的名字
请求方法	包含、相等、正则匹配、统计次数、统计个数	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、相等、正则匹配、统计次数、统计个数	请求 Host 头的值
请求 referer 头	包含、相等、正则匹配、统计次数、统计个数	请求 referer 头的值
请求 User-Agent	包含、相等、正则匹配、统计次数、统计个数	请求 User-Agent
请求体	包含、相等、正则匹配、统计次数	请求体
请求端口	相等、统计次数、统计个数	请求的端口
源 IP	属于、不属于	请求来源 IP

4.3.7. 沙箱机制

实例的实际峰值 QPS 超过已购 QPS 流量规格时，实例可能会进入沙箱。本文介绍 WAF 的沙箱机制、如何解除实例的沙箱状态。

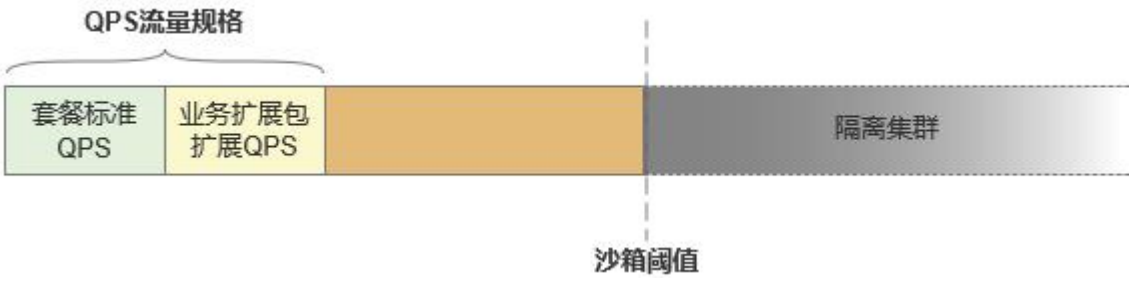
沙箱说明

沙箱机制设有沙箱隔离阈值，是不同 QPS 规格的 WAF 实例可短期服务的最大防护 QPS 阈值。当实际业务 QPS 峰值超过沙箱阈值，或者实际业务 QPS 峰值超过正常业务请求 QPS 峰值，但未达到实例沙箱隔离阈值累计 3 次（含 3 次），实例会进入沙箱隔离状态，进入沙箱的实例将不再保证产品 SLA。

正常业务请求 QPS 峰值=套餐标准 QPS 峰值+业务扩展包扩展 QPS。

沙箱隔离阈值

实例 QPS 沙箱隔离阈值 = 正常业务请求 QPS 峰值 * 2



不同版本的最大流量规格值及沙箱隔离阈值如下：

版本	套餐标准 QPS 峰值	正常业务请求 QPS 峰值	沙箱隔离阈值
基础版	100	100	200
标准版	3000	203000	406000
企业版	5000	205000	410000
旗舰版	10000	210000	420000

上表中，**正常业务请求 QPS 峰值**指购买了 200 个业务扩展包的情况。一个业务扩展包包含：1000QPS/个，最多支持 200 个业务扩展包。基础版不支持购买扩展包。

沙箱隔离条件

- 情况一：实际业务 QPS 峰值超过流量规格值，但未达到实例沙箱隔离阈值

通过超限次数判断：WAF 会实时获取每个时间点的上 5 分钟内的峰值 QPS，峰值 QPS 连续 5 分钟超过当前规格阈值时，被判定为一次超用。一天内最多 3 次 QPS 超用。实例第 4 次超用时，实例进入沙箱隔离状态。

说明：

- 因正常业务流量突增导致的短暂 QPS 超用，并且超用时间未达到 5 分钟时，实例不会统计为一次超用。
- 如果存在超用时间跨天的情况，例如超用时间为 23:58~00:04，WAF 会根据超用起始时间统计为一次超用。

- **情况二：实际业务 QPS 峰值超过 QPS 流量规格值**

通过 QPS 用量判断：实例 QPS 峰值超过当前实例 QPS 沙箱隔离阈值一次，将不再计算当日超量次数，实例直接进入隔离状态。

进入沙箱后如何处理

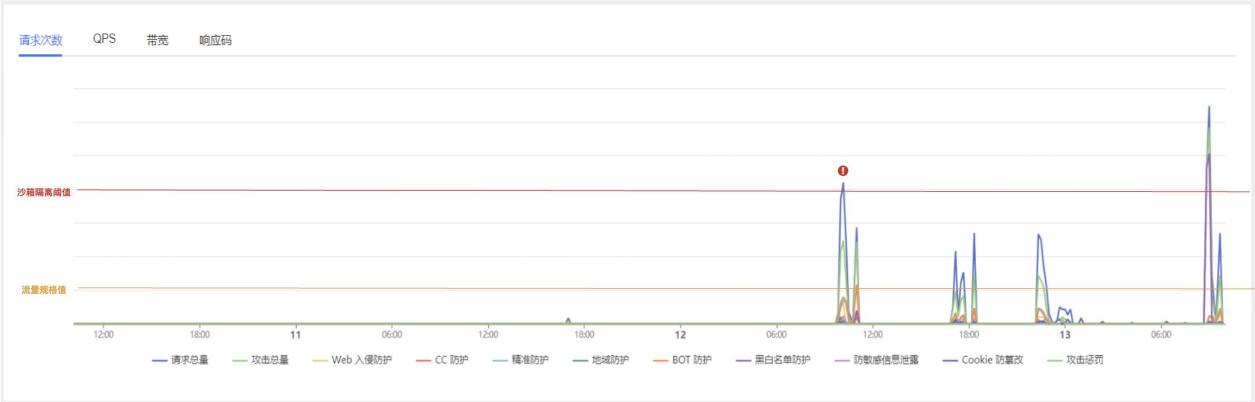
进入沙箱对实例有何影响?

对于进入沙箱的实例，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。

如何获知实例已经为非正常流量状态?

实例进入沙箱后，系统会通过邮件、短信或站内信等方式提示您。同时，您会在控制台页面顶部收到超用信息。

在安全总览页面，您可以通过 QPS 图表查看具体的 QPS 流量情况。



如何解除沙箱隔离状态?

注意：

实例进入隔离状态后，即使实际 QPS 用量已回落至当前规格以内，也不会自动解除。

您需要扩展该实例 QPS 规格值，当扩展后实例 QPS 规格值大于最大业务峰值后，将自动结束隔离，恢复正常防护和产品服务 SLA。

您可以通过购买业务扩展包或者升级 WAF 版本实现该实例 QPS 规格值的扩展。QPS 扩展后，实例的状态将变成正常流量状态，QPS 超用次数统计清零。

4.4. 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。
- 已完成防护对象接入并正常防护。

查询条件

在总览页面上方，选择要查询的防护对象和时间，查询总览数据。

查询条件说明：

- 防护对象：默认展示 SaaS 模式下已接入防护的域名相关数据，也可以查询其他模式下已接入防护的数据，或只查询某个域名的数据。
- 时间：查询时间支持选择昨天、今天、近 3 天、近 7 天、近 30 天或自定义时间范围的防护统计数据。

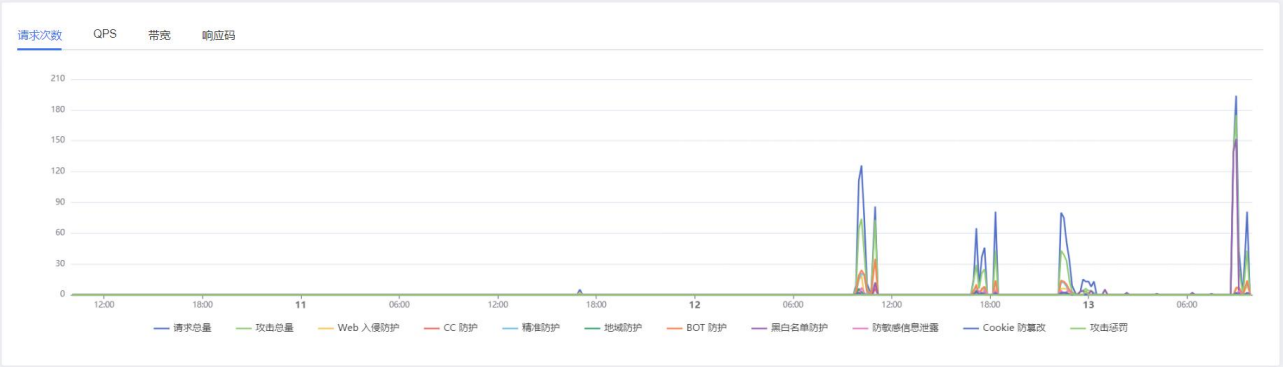
防护统计数据

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。

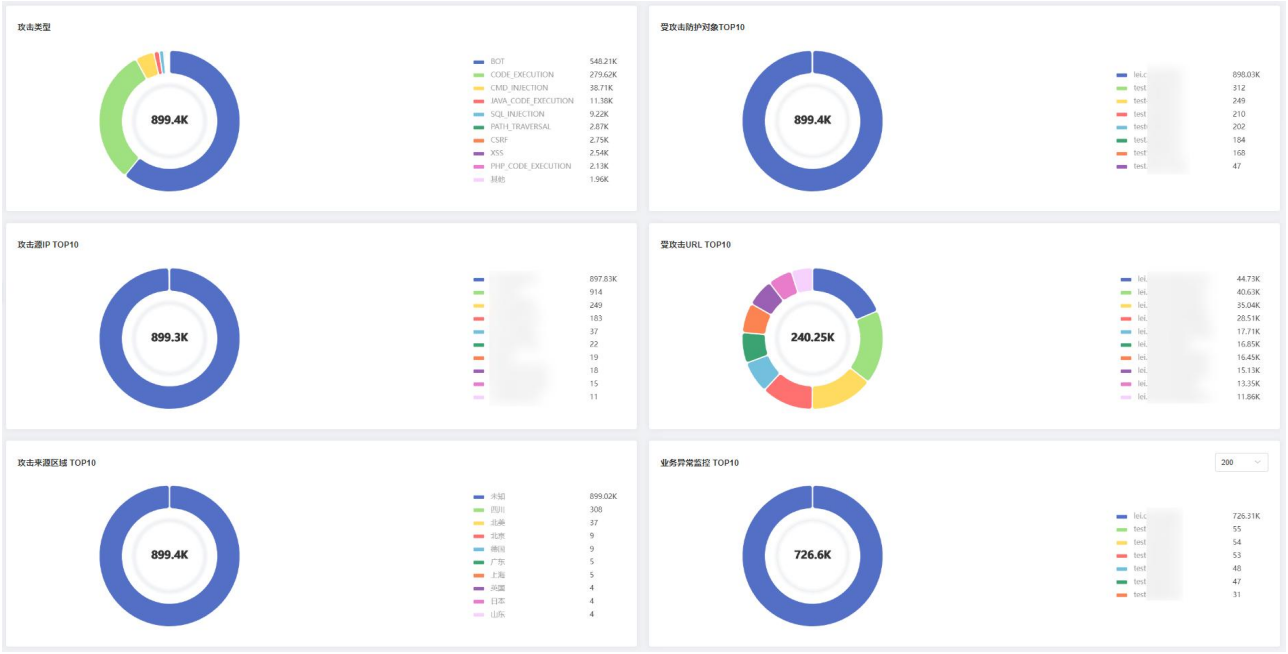


不同趋势数据的说明如下：

- **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：

- **攻击类型**：可查看指定域名被攻击的类型的数量占比。
- **受攻击防护对象 TOP10**：受攻击统计次数 Top 10 的域名以及各域名受到攻击次数的占比。
- **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 的地区以及各地区发起攻击次数的占比。
- **业务异常监控 TOP10**：业务异常的 Top 10 防护网站。可以按响应码查看业务异常的防护网站。

4.5. 防护事件

4.5.1. 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

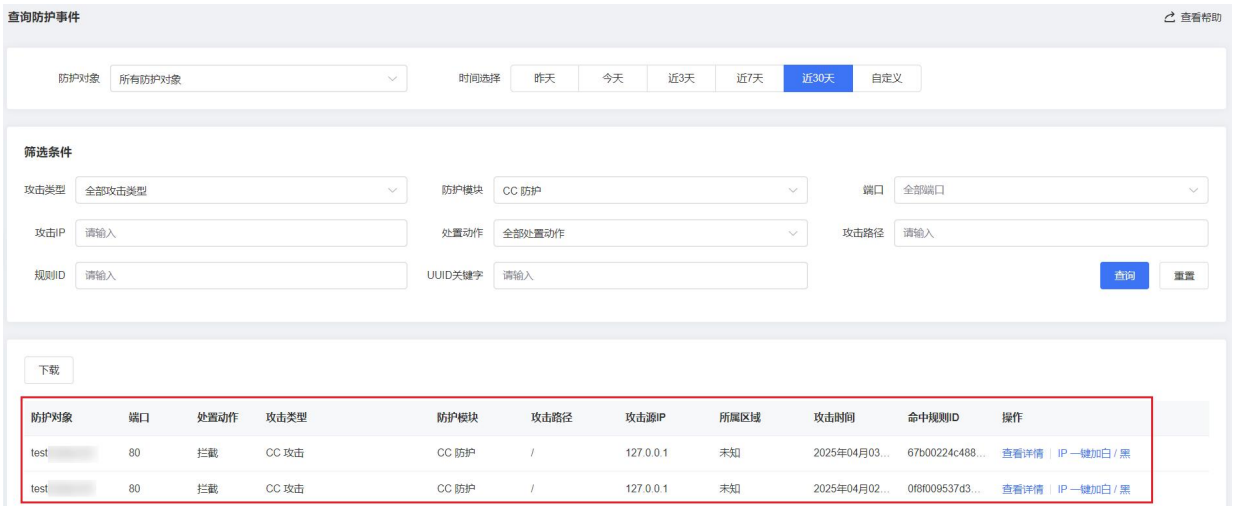
1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护事件 > 查询防护事件”，进入防护事件页面。
5. 在防护事件列表上方，可以设置筛选条件，支持设置多项匹配条件。

查询条件字段参数说明：

参数名称	参数说明
防护对象	选择想要查看的防护对象，支持选择各防护模式下的所有防护对象或某个防护对象。
时间选择	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
攻击类型	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

参数名称	参数说明
	查看攻击日志信息
防护模块	按防护模块进行筛选。
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
规则 ID	攻击触发的防护规则 ID
UUID 关键字	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。



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

参数名称	参数说明
	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

4.5.2. 开启告警通知

通过对攻击日志设置告警通知，WAF 可将仅记录和拦截的攻击日志按用户设置的接收通知渠道（邮件或短信）发送给用户。

使用限制

独享版防护对象暂不支持告警通知功能。

开启告警通知

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“防护事件 > 告警通知”，进入告警通知页面。
5. 单击“新增通知策略”，弹出新建通知策略窗口。

6. 配置告警通知参数。

参数	说明
策略名称	用户可以自定义策略的名称。
通知状态	配置告警通知的状态，默认为关闭。根据需要进行开启。
通知群组	在下拉列表选择需要接收告警通知的群组。 若已有群组无法满足需求，单击“创建群组”创建新的群组，需要为群组中的联系人配置姓名、手机、邮箱等信息。
通知渠道	支持邮件、短信。
事件类型	设置告警的事件类型，系统默认选择“全部”，用户也可以选择“自定义”，勾选需要告警的事件类型。
告警频率阈值	在设置的时间间隔内，当攻击次数大于或等于您设置的阈值时，才会发送告警通知。

7. 配置完成后，单击“确认”，告警通知策略设置成功。

相关操作

- 关闭告警通知：如果需要关闭告警通知，在目标告警通知所在行的“策略状态”列，修改策略状态，将状态置为关闭。
- 修改告警通知：在目标告警策略所在行的“操作”列，单击“编辑”。
- 删除告警通知：在目标告警策略所在行的“操作”列，单击“删除”。

4.6. API 安全

4.6.1. API 总览

API 总览页面展示 API 防护整体情况，包括 API 资产统计、API 风险统计等。

前提条件

已开通 Web 应用防火墙（原生版）实例企业版或旗舰版。

防护对象列表

页面左侧展示所有防护对象信息，统计已接入的对象个数（不包括泛域名、ELB 防护对象）。

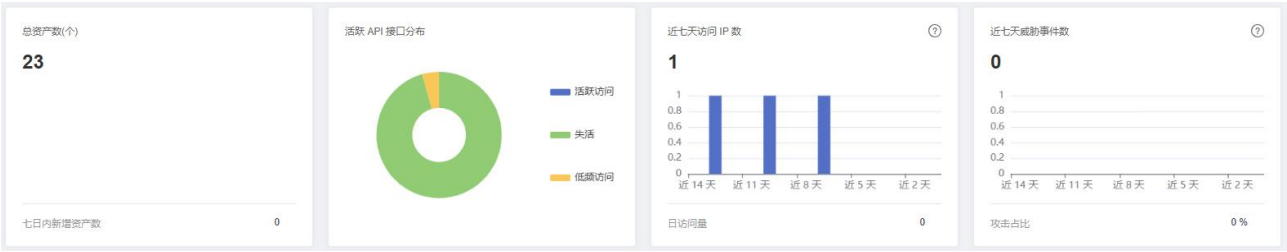
支持选择“所有防护对象”或选择单个域名站点，查看统计信息：

- 选择“所有防护对象”，页面右侧展示全局防护统计信息。
- 选择单个域名站点，页面右侧展示单个域名站点统计信息。

资产统计

统计单个域名/所有域名下的资产统计信息，包含总资产数、活跃 API 接口分布、近七天访问 IP 数、近七天威胁事件数。

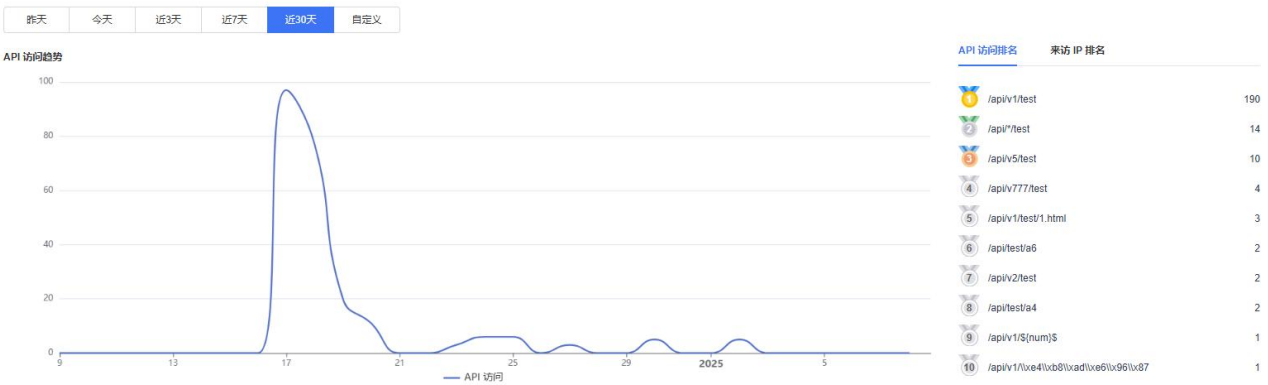
- 总资产数：展示总资产个数和七日内新增资产数。
- 活跃 API 接口分布：展示所选域名下活跃访问、低频访问、失活的 API 资产分布占比情况（饼状图）。
- 近七天访问 IP 数：展示所选域名近 7 天访问 IP 总数和近 14 天的访问趋势（柱状图），并统计日访问量。
- 近七天威胁事件数：统计所选域名下近 7 天威胁涉及 API 的威胁事件数量和近 14 天威胁事件日趋势（柱状图），并统计攻击占比（攻击占比指所有攻击事件数/正常业务事件数，不包含因为带宽原因被屏蔽的部分）。



API 统计

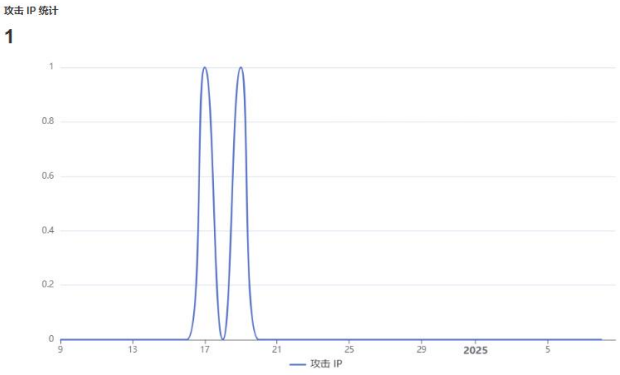
支持按所选时间范围查看 API 统计信息，支持选择昨天、今天、，近 3 天、近 7 天、近 30 天，或自定义时间段。

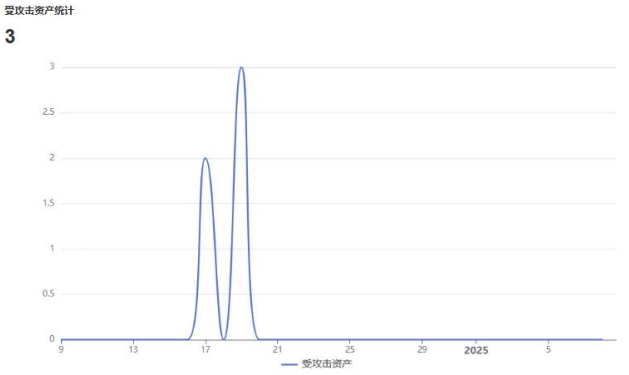
- API 访问趋势：展示 API 的受访趋势。
- API 访问排名：展示受访 TOP10 的 API。
- 来访 IP 排名：展示来访 IP 的 TOP10。



风险情况

- 攻击 IP 统计：展示所选域名下攻击 IP 的个数以及趋势，同时展示 TOP30 攻击 IP 列表。
- 受攻击资产统计：展示所选域名下受攻击的接口数，点击后展示 TOP30 受攻击接口列表。





排名	攻击源 IP	攻击次数
1	127.0.0.1	12

排名	受攻击资产	攻击次数
1	/api/v1/test	8
2	/api/*/test	3
3	/api/v5/test	1

4.6.2. API 管理

4.6.2.1. 手动添加 API 资产

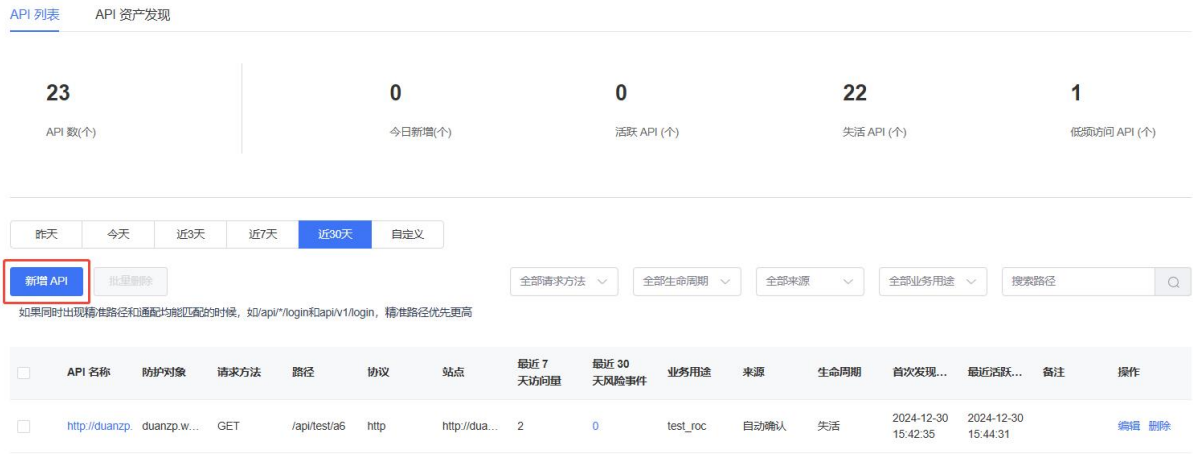
手动添加 API 资产用于添加单个 API 资产。若防护对象的 API 资产规模较大，请配置 API 自动发现任务自动发现防护对象中的 API 资产，具体操作请参见“API 自动发现”。

前提条件

- 已开通 Web 应用防火墙（原生版）实例企业版或旗舰版。
- 已完成防护域名接入，并正常防护。

操作步骤

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“API 安全 > API 管理”，进入 API 管理页面。
5. 在 API 列表上方，单击“新增 API”，弹出新建 API 资产页面。



6. 在新建 API 资产页面中，配置 API 资产参数，配置完成后，单击“确认”。

API 资产参数说明如下：

参数	说明
防护对象	通过下拉框选择已接入防护的防护对象。若下拉框没有目标对象，请参考接入 WAF 接入防护对象。
站点	选择防护对象下的站点，一次只能选择一个站点。
API 名称	自定义 API 的名称。长度为 2-63 字符，以字母或中文开头，可包含数字、“.” 、“_”、“-”、“/”、“%”、“:”、“$”、“{”、“}”。
路径	API 的路径。长度为 1-1000 字符，目前仅支持大小写字母、数字、"/"、"-"、"_"、"."以及通配符"*"，如/api/*/login，可以匹配 api/v1/login、api/v2/login 等。 说明：路径中的每一节支持独立通配符，可对该节进行通配匹配，但不允许连续出现通配符，也不支持正则类型输入。
请求方法	通过下拉框选择请求 API 的方法，支持 GET、POST、HEAD、PUT、DELETE、OPTIONS、PATCH。
业务用途	通过下拉框选择 API 的业务用途。若下拉框没有目标选项，请参考“新增业务用途规则”进行创建。
描述	自定义 API 的描述信息。

4.6.2.2. API 自动发现

API 自动发现主要用于帮助用户自动或半自动发现 API 资产。

- 当 API 资产规模较小时（不超过 100 条），可选择开启“确认为 API 资产”，自动将发现的 API 确认为 API 资产。
- 当 API 资产规模校大时（超过 100 条），API 自动发现任务可发现 API 资产，用户需进行人工识别和确认后，添加为 API 资产。

前提条件

- 已开通 Web 应用防火墙（原生版）实例企业版或旗舰版。
- 已完成防护域名接入，并正常防护。

配置 API 自动发现任务

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“API 安全 > API 管理”，进入 API 管理页面。
5. 选择“API 资产发现”页签，单击“API 自动发现”，进入 API 自动发现任务页面。

6. 在弹出的 API 自动发现任务页面中，配置任务参数。

   任务参数说明如下：

参数	说明
识别范围	通过设置识别范围可限定 API 的发现范围。单次识别 API 资产不超过 10000 个。 支持输入长度为 1-256 字符，支持通配符，最多可输入 10 个条件，多个条件之间是或关系。
排除条件	通过设置排除条件排除在识别范围内不属于 API 的其他路径，从而提升 API 识别的准确性。 支持输入长度为 1-256 字符，支持通配符，最多可输入 10 个条件，多个条件之间是或关系。
执行周期过期时间	通过设置执行周期过期时间可设置单次任务的运行周期，任务运行最长支持 30 天，最短支持 5 分钟。 任务到期或发现 API 接口超过 10000 后将自动结束任务。
业务用途识别	开启“业务用途识别”，可基于 API 接口的路径特征和参数名特征，与自定义的业务用途字段

参数	说明
	进行匹配，自动判断识别到的 API 接口业务用途。自定义业务用途请参见新增业务用途规则。
确认为 API 资产	开启“确认为 API 资产”，在任务执行结束后，会将本次任务发现的 API 自动确认为 API 资产并展示在“API 列表”中。 说明：为保证自动确认的资产不产生大量的冗余数据，单次自动确认的资产不超过 100 条，如果单次自动发现的资产超过 100 条时，将会将本次任务所有发现的 API 资产识别为待确认资产。
识别到待确认 API 资产后	配置 API 自动发现任务识别到待确认 API 资产后，对历史待确认 API 资产的处理方式： ● 在历史待确认 API 列表上新增：将识别到的待确认 API 资产在原有资产上新增。默认选择该方式。 ● 清除历史待确认 API 资产：清除历史所有待确认 API 资产，API 资产发现列表仅展示本次新发现的待确认 API 资产。

7. 参数配置完成后，单击“确认”，系统会自动发现从开始任务之后的 API 接口。

   - 在 API 识别过程中，发现一个 API 待确认资产即显示一个，无需在任务执行完成之后再将所有结果添加至待确认列表。
   - 任务执行过程中，可查看任务执行时间、查看任务详情、手动停止任务。

确认 API 资产

API 自动发现任务识别到待确认 API 资产后，用户手动将其确认为 API 资产，即可展示在“API 列表”中。

说明：

确认 API 时，如果出现相同 API，不会重复添加。

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“API 安全 > API 管理”，进入 API 管理页面，选择“API 资产发现”页签。
5. 搜索待确认的 API。
   a. 在页面左侧，展示了所有防护对象信息（不包括泛域名、ELB 防护对象），支持选择“所有防护对象”或选择单个域名站点，在右侧 API 列表中查看对应防护对象的详细数据列表。
      - 选择“所有防护对象”，页面右侧展示所有待确认的 API 资产。
      - 选择单个域名站点，页面右侧展示选中的域名站点待确认的 API 资产。

b. 可通过发现时间、请求方法、业务用途对待确认资产进行筛选。

- 发现时间：根据 API 资产最近活跃时间对 API 资产进行过滤，支持昨天、今天、近 3 天、近 30 天，或自定义时间范围。默认选中今天。
- 请求方法：支持多选。
- 业务用途：支持多选。
- API 路径：支持模糊匹配。

6. 搜索定位到目标 API 后，单击操作列的“确认为 API”。

或勾选多个 API，单击列表上方的“批量确认”进行批量操作。

7. 在确认为 API 窗口中，确认 API 信息，可对 API 名称、业务用途进行修改。

8. 单击“确认”。

确认为 API 资产后，API 资产将从“API 资产发现”页面移动到“API 列表”页面中。

4.6.2.3. 管理 API 资产

API 列表页面展示通过手动添加的 API 资产，和自动发现任务发现并已确认为 API 的资产，在该页面可以对这些 API 资产进行管理，包括编辑、删除操作。

编辑 API 资产

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“API 安全 > API 管理”，进入 API 管理页面。
5. 在“API 列表”中，单击操作列的“编辑”。

6. 在“编辑 API 资产”窗口中，可对 API 名称、业务用途、描述进行修改。
7. 修改完成后，单击“确认”。

删除 API 资产

- 删除单个 API：在 API 列表中，单击操作列的“删除”。

- 批量删除 API：勾选多个 API，单击列表上方的“批量确认”进行批量操作。

4.6.2.4. 查看 API 列表

在 API 列表页面，可查看已添加的 API 资产。

查看 API 列表

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。

4. 在左侧导航栏，选择“API 安全 > API 管理”，进入 API 管理页面。

5. 在页面左侧，展示了所有防护对象信息（不包括泛域名、ELB 防护对象），支持选择“所有防护对象”或选择单个域名站点，在右侧 API 列表中查看对应防护对象的详细数据列表。

   - 选择“所有防护对象”，页面右侧展示所有的 API 资产。
   - 选择单个域名站点，页面右侧展示选中的域名站点 API 资产。

6. API 列表页面上方展示了所选防护对象的 API 资产统计信息。

   - API 数：统计已识别的 API 资产数量。
   - 今日新增：统计自然时间今日新增的 API 数量。
   - 活跃 API：统计活跃 API 数量。

- 失活 API：统计失活 API 数量。

7. 搜索目标 API 资产：可通过最近活跃时间、请求方法、生命周期、来源、业务用途、API 路径进行搜索。

- 最近活跃时间：根据 API 资产最近活跃时间对 API 资产进行过滤，支持昨天、今天、近 3 天、近 30 天，或自定义时间范围。默认选中今天。
- 请求方法：支持多选。
- 生命周期：支持多选。
- 来源：单选。
- 业务用途：支持多选。

8. 查看 API 列表，列表中字段说明如下。

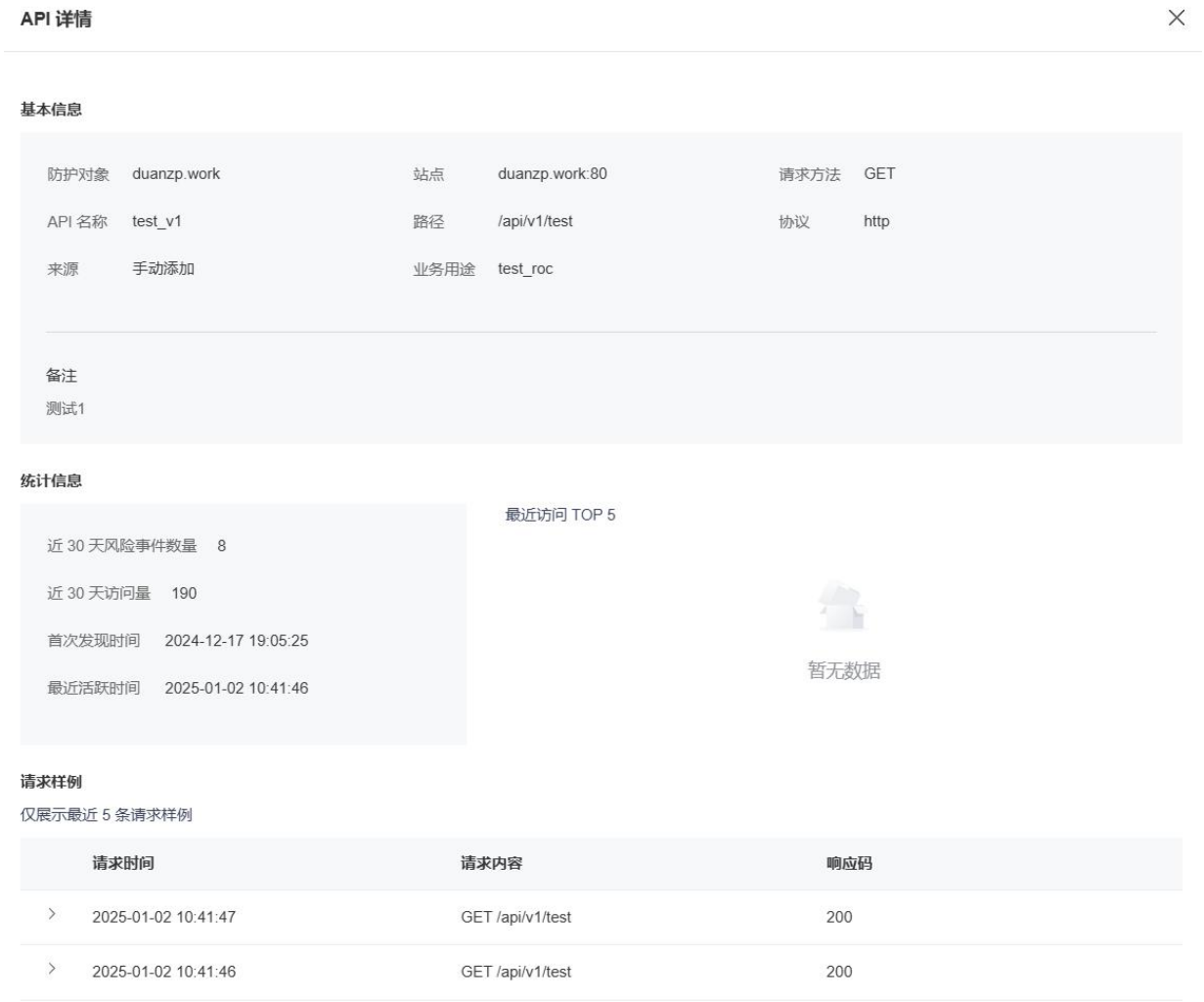
参数	说明
API 名称	API 的自定义名称。单击 API 名称链接，可查看 API 详情。
防护对象	API 所属防护对象。
请求方法	API 所用的请求方法。
路径	API 的路径信息。
协议	HTTP、HTTPS。
站点	API 所属站点。
最近 7 天访问量	统计该 API 最近 7 天访问量。
最近 30 天风险事件	统计该 API 最近 30 天的风险事件数。
业务用途	API 所属业务用途。
来源	• 手动添加：通过手动新增 API 方式添加的 API 自查。

参数	说明
	● 自动识别：通过 API 自动发现任务发现的 API 资产，然后手动确认为 API 资产。 ● 自动确认：通过 API 自动发现任务发现的 API 资产，并开启了“确认为 API 资产”，自动确认为 API 资产。
生命周期	包括失活、低频、活跃。
首次发现时间	● 手动添加的 API 资产为创建时间。 ● 自动发现的 API 资产为自动发现时间。
最近活跃时间	该 API 最近活跃的时间。活跃为产生成功的请求响应。
备注	用户自定义的 API 备注信息。

查看 API 详情

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“API 安全 > API 管理”，进入 API 管理页面。

5. 单击 API 名称链接，进入 API 详情页面。



6. 查看 API 详情。

参数		说明
基本信息	防护对象	API 所属防护对象。
	站点	API 所属站点。
	请求方法	API 所用的请求方法。
	API 名称	API 的自定义名称。
	路径	API 的路径信息。
	协议	HTTP、HTTPS。

参数		说明
	来源	• 手动添加：通过手动新增 API 方式添加的 API 自查。 • 自动识别：通过 API 自动发现任务发现的 API 资产，然后手动确认为 API 资产。 • 自动确认：通过 API 自动发现任务发现的 API 资产，并开启了“确认为 API 资产”，自动确认为 API 资产。
	业务用途	API 所属业务用途。
	备注	用户自定义的 API 备注信息。
统计信息	近 30 天风险事件数量	统计该 API 最近 30 天的风险事件数。
	近 30 天访问量	统计该 API 最近 30 天访问量。
	首次发现时间	发现该 API 的时间。
	最近活跃时间	该 API 最近活跃的时间。
	最近访问 TOP5	最近七天访问 API 的 TOP5 访问 IP。
请求样例	-	展示最近 5 条请求样例，包括请求时间、请求内容、响应码。 默认展开了第一条请求详情，可以看到该请求的请求内容、响应内容，点击 图标可收起详情。

4.6.3. 策略配置

配置业务用途

业务用途用于标识 API 的用途，您可以根据业务需要，创建自定义业务用途，并对策略状态进行管理。

新增业务用途规则

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。

3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。

4. 在左侧导航栏，选择“API 安全 > 策略配置”，进入 API 策略配置页面。

5. 在“业务用途”模块，单击右下角的“配置”，进入业务用途配置页面。

6. 在业务用途配置页面，单击“新增策略配置”，进入新建业务用途规则页面。

7. 在新建业务用途规则页面，配置业务用途规则参数，配置完成后，单击“确定”。

业务用途规则参数说明如下：

参数	说明
业务用途	自定义业务用途的名称，长度为 2-10 字符。名称不允许重复，不允许以“默认”命名。
匹配条件	支持输入匹配条件对特征进行匹配： 匹配字段：支持请求路径、请求参数、请求 HOST、请求方法、响应内容类型五个字段。 逻辑符：支持“正则匹配”。 最多支持 5 个条件，多个条件之间为或关系。
优先级	请输入 1~100 的整数，数字越大，代表这条规则的优先级越高。若配置的优先级数字相同，则创建时间越晚，优先级越高。

管理业务用途规则

规则创建完成后，支持对规则状态进行修改、编辑规则、删除规则。

- 规则状态：业务用途规则创建完成后，规则状态默认为“已启用”。用户可根据需要对规则状态进行修改。
- 编辑规则：单击操作列的“编辑”，对规则进行修改。业务用途规则的所有参数均支持修改。
- 删除规则：单击操作列的“删除”，在弹出的提示框中，单击“确定”，删除对应的规则。

配置生命周期

用户可通过设置监测周期、每天访问次数，来自定义低频访问 API、失活 API 的判断标准。使得 API 检测更符合业务实际情况。

- 失活：在设定的监测周期内，每天的访问次数均小于或等于设置的失活阈值的 API 接口，将被判定为失活 API。通常用来标识该接口不活跃或者无访问的情况。
- 低频访问：在设定的监测周期内，每天访问次数均小于等于设置的低频访问阈值的 API 接口，将被判定为低频访问 API。通常用来标识有一定访问量，但不太活跃的接口，该类接口需要重点关注。

- 活跃：在设定的监测周期内，每天的访问次数大于设置的低频访问阈值的接口。通常用来标识该接口较为活跃。

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，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“API 安全 > 策略配置”，进入 API 策略配置页面。
5. 在“生命周期”模块，单击右下角的“配置”，进入 API 生命周期监测页面。

6. 在 API 生命周期监测页面，配置监测周期、每天访问次数，配置完成后，单击“确定”。

API 生命周期监测参数说明如下：

参数		说明
周期监测	监测周期	请输入 7~30 的数字，默认值为 7 天。
每天访问次数	低频访问	设置低频访问阈值，最小值为 2，默认值为 10。
	失活	设置失活阈值，最小值为 1，默认值为 1。

4.7. 系统管理

4.7.1. 管理云 SaaS 型实例

4.7.1.1. 查看云 SaaS 型实例产品信息

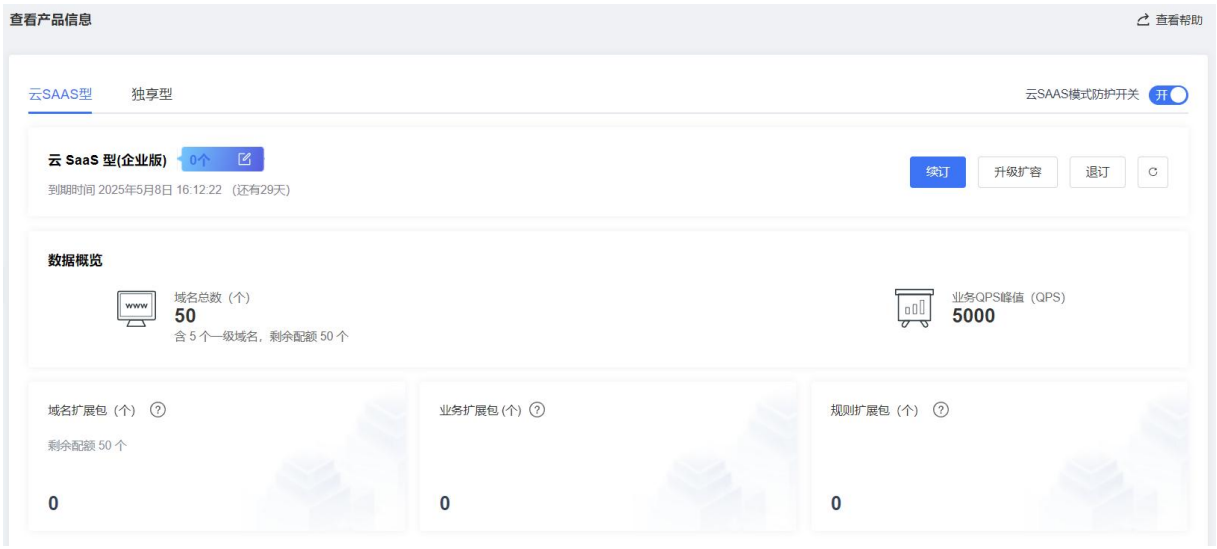
您可以在产品信息页面查看已购买实例的版本、规格等信息。

前提条件

已购买 WAF 云 SaaS 型实例。

查看云 SaaS 型产品信息

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“云 SAAS 型”页签。
5. 在产品信息页面，可以查看实例版本、到期时间、实例规格等信息，并支持对实例进行管理。



相关操作

- 升级实例规格和扩展包
- 续订云 SaaS 型实例
- 退订云 SaaS 型实例

4.7.1.2. 升级实例规格和扩展包

开通了云 SaaS 型实例后，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

已购买 WAF 云 SaaS 型实例。

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 个主域名（备案的域名）。
- 一个业务扩展包包含：1000QPS/个，最多支持 30 个业务扩展包。
- 规则扩展包用于提升防护规则配额，支持以下两种扩展方式（二选一）：
  - IP 黑白名单：每个扩展包包含 **50 条防护规则/域名。**
  - 重保防护场景：每个扩展包包含 **1000 个 IP/实例。**

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。

升级云 SaaS 型实例规格

云 SaaS 型实例支持升级主套餐版本，以及扩增资源扩展包的数量。

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. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“云 SAAS 型”页签。
5. 单击“升级扩容”，进入“升配”页面。
6. “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。

7. 选择升级的规格后，在页面下方确认支付费用，单击“立即购买”。

8. 在订单页完成订单确认并支付，付费成功后，购买的版本将生效。

扩增云 SaaS 型实例资源扩展包

云 SaaS 型实例支持升级主套餐版本，以及扩增资源扩展包的数量。

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. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。

4. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“云 SAAS 型”页签。

5. 单击“升级扩容”，进入升配页面。

6. 在“升配”页面下方，单击“去增项”，进入增项页面。

7. 设置资源扩展包数量，需高于当前已购买数量。

8. 设置完成后，在页面下方确认支付费用，单击“立即购买”。
9. 在订单页完成订单确认并支付，付费成功后，购买扩展包将生效。

4.7.1.3. 续订云 SaaS 型实例

购买云 SaaS 型实例后，在实例到期被删除前，您可以随时在 WAF 控制台为 WAF 续费。

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. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“云 SAAS 型”页签。
5. 单击“续订”，进入续订页面。
6. 在“续订”操作界面，根据使用需要调整续订周期。

7. 续订周期设置完成后，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》 “，单击“立即购买”。

4.7.1.4. 退订云 SaaS 型实例

购买云 SaaS 型实例后，在实例到期被删除前，您可以随时在 WAF 控制台退订实例。

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. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“云 SAAS 型”页签。
5. 单击“退订”，进入退订页面。
6. 确认退订信息后，单击“立即退订”。

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。

4.7.2. 管理独享型实例

4.7.2.1. 查看独享型实例产品信息

您可以在产品信息页面查看已购买实例的版本、规格等信息。

前提条件

已购买 WAF 独享型实例。

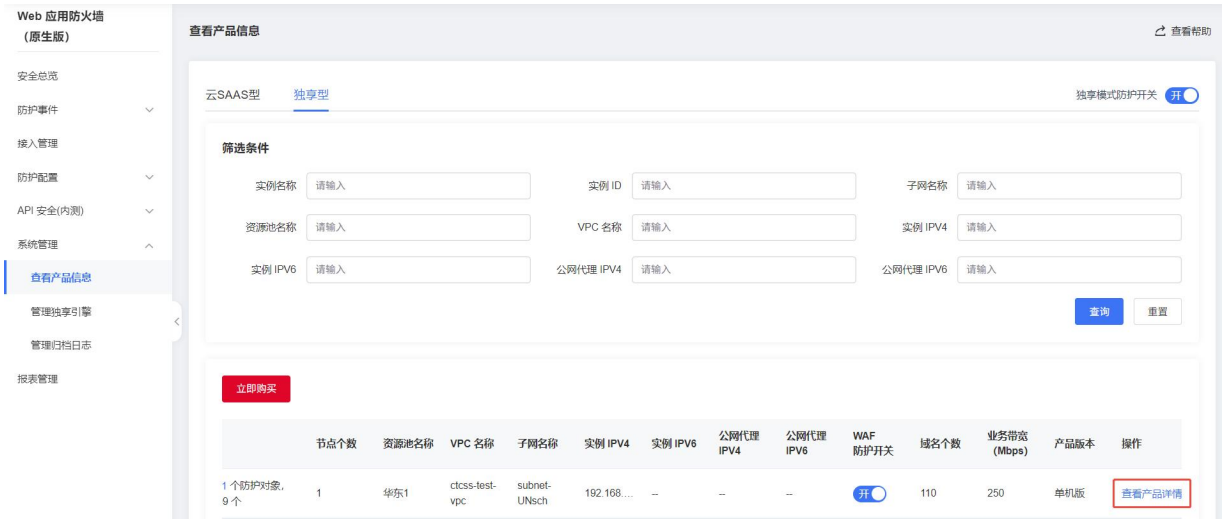
查看独享型产品详情

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“独享型”页签。
5. 查看独享型实例列表。

参数	说明
实例名称	系统默认以“资源池名称+VPC 名称+实例内网 IP”自动生成实例名称。用户可在实例详情页面对其进行修改。
实例 ID	实例的 ID。
运行状态	当前实例的运行状态，包括正常、异常、离线。
防护对象	接入防护对象的个数。在实例详情页点击数字可跳转至对应防护对象列表页。
节点个数	当前实例的节点个数。
资源池名称	当前实例所属资源池。
VPC 名称	当前实例所属 VPC。
子网名称	当前实例所属子网。
实例 IPv4	● 单机版：显示单机节点本身内网 IPV4 地址。 ● 集群版：显示集群 VIP 的 IPV4 地址。
实例 IPv6	● 单机版：显示单机节点本身内网 IPV6 地址。 ● 集群版：显示集群 VIP 的 IPV6 地址。
公网代理 IPv4	绑定在实例上的 IPV4 公网地址，用于互联网 IPV4 通信。在下拉框中选择一个可用的 IPv4 地址，手动进行绑定。
公网代理 IPv6	绑定在实例上的 IPV6 公网地址，用于互联网 IPV6 通信。在下拉框中选择一个可用的 IPv6 地址，手动进行绑定。

参数	说明
WAF 防护开关	可对实例的防护状态进行开启或关闭，关闭后，该实例下所有防护对象都将不受防护。
域名个数	当前实例支持防护的防护对象个数。
业务带宽	当前实例支持防护的业务带宽。
产品版本	实例的规格，单机版或集群版。

6. 单击目标实例操作列的“查看产品详情”。



7. 在产品信息页面，可以查看实例版本、实例名称、实例 ID、到期时间、实例规格等信息，并支持对实例进行管理。

相关操作

- 升级实例规格和扩展包
- 续订独享型实例
- 退订独享型实例

4.7.2.2. 查看独享版实例详情

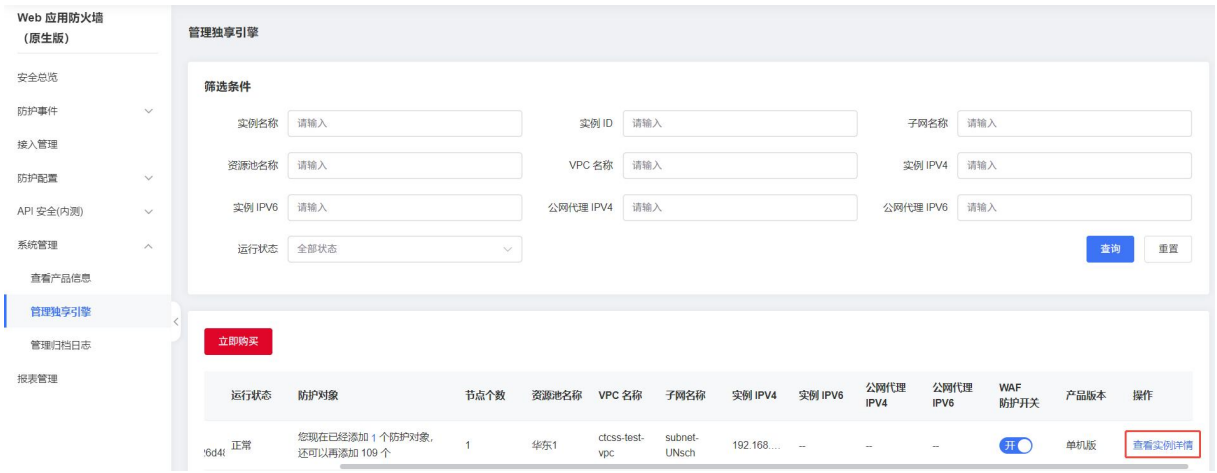
您可以在产品信息页面查看已购买实例的详细信息，包括实例基本信息、实例节点的健康状态。

前提条件

已购买 WAF 独享型实例。

查看独享版实例详情

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 管理独享引擎”，单击目标实例操作列的“查看实例详情”。



5. 在实例详情页面，可以查看实例信息、接入端口，以及实例节点状态。
   - 实例信息

参数	说明

参数	说明
实例名称	系统默认以“资源池名称+VPC 名称+实例内网 IP”自动生成实例名称。用户可在实例详情页面对其进行修改。 修改实例名称： 1. 在实例详情页面，单击  图标。 2. 修改实例名称后，单击“保存”，完成修改。
实例 ID	实例的 ID。
节点个数	当前实例的节点个数。
运行状态	当前实例的运行状态，包括正常、异常、离线。
WAF 防护开关	可对实例的防护状态进行开启或关闭，关闭后，该实例下所有防护对象都将不受防护。
资源池	当前实例所属资源池。
VPC 名称	当前实例所属 VPC。
子网名称	当前实例所属子网。
防护对象	接入防护对象的个数。在实例详情页点击数字可跳转至对应防护对象列表页。
产品版本	实例的规格，单机版或集群版。
实例 IPv4	● 单机版：显示单机节点本身内网 IPV4 地址。 ● 集群版：显示集群 VIP 的 IPV4 地址。
实例 IPv6	● 单机版：显示单机节点本身内网 IPV6 地址。 ● 集群版：显示集群 VIP 的 IPV6 地址。
公网代理 IPv4	绑定在实例上的 IPV4 公网地址，用于互联网 IPV4 通信。在下拉框中选择一个可用的 IPv4 地址，手动进行绑定。
公网代理 IPv6	绑定在实例上的 IPV6 公网地址，用于互联网 IPV6 通信。在下拉框中选择一个可用的

参数	说明
	IPv6 地址，手动进行绑定。

- 节点状态：显示实例节点的健康状态，集群版有多个节点，可以通过趋势图右侧切换节点。
  - 支持按均值、峰值查看资源趋势图。
  - 支持按照最近一小时、最近一天、最近一周进行过滤。
  - 支持查看节点的 IPv4 地址、IPv6 地址、节点属性、可用区。
  - 支持显示节点当前运行的 CPU、内存、存储、网络信息。

参数	说明
CPU	显示当前节点 CPU 利用率统计情况。
内存	显示当前节点内存使用情况，包括使用中、剩余可用、总内存的使用情况。
磁盘	显示当前节点系统盘和数据盘占用情况。
网络	显示当前节点发送和接收数据包情况。

4.7.2.3. 升级实例规格和扩展包

开通了独享型实例后，可支持根据实际使用需求增加集群节点数量，购买域名扩展包、带宽扩展包。

前提条件

已购买 WAF 独享型实例。

规格限制

扩展包	规格	数量限制
域名扩展包	1 个域名扩展包支持 10 个域名或 IP。	最大支持 1000 个域名扩展包。
带宽扩展包	1 个带宽扩展包包含 1000QPS 业务请求	• 单机版：最多支持 16 个带宽扩展包。

扩展包	规格	数量限制
	峰值、50Mbps 业务带宽。	● 集群版：带宽扩展包的数量上限与节点数量相关联，每增加一个节点，带宽扩展包的上限数量增加 20 个。例如，当集群包含 4 个节点时，最多支持配置 20 个带宽扩展包；而节点数量最多 12 个，则最多支持配置 180 个带宽扩展包。

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

升级节点数量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。

增加独享版实例的节点数量

独享版实例暂不支持升级实例规格，可以根据需要增加集群版节点的数量。

1. 登录 Web 应用防火墙（原生版）控制台。
2. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“独享型”页签。
3. 单击目标实例操作列的“查看产品详情”。
4. 单击“升级扩容”，进入“升配”页面。
5. “规格选择”默认为当前实例版本，设置节点数量。

6. 节点数量设置完成后，在页面下方确认支付费用，单击“立即购买”。

7. 在订单页完成订单确认并支付。

扩增独享型实例资源扩展包

1. 登录 Web 应用防火墙（原生版）控制台。

2. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“独享型”页签。

3. 单击目标实例操作列的“查看产品详情”。

4. 单击“升级扩容”，进入升配页面。

5. 在“升配”页面下方，单击“去增项”，进入增项页面。

6. 设置资源扩展包数量，需高于当前已购买数量。

7. 设置完成后，在页面下方确认支付费用，单击“立即购买”。

8. 在订单页完成订单确认并支付。

4.7.2.4. 续订独享型实例

购买独享型实例后，在实例到期被删除前，您可以随时在 WAF 控制台进行续费。

操作步骤

1. 登录 Web 应用防火墙（原生版）控制台。

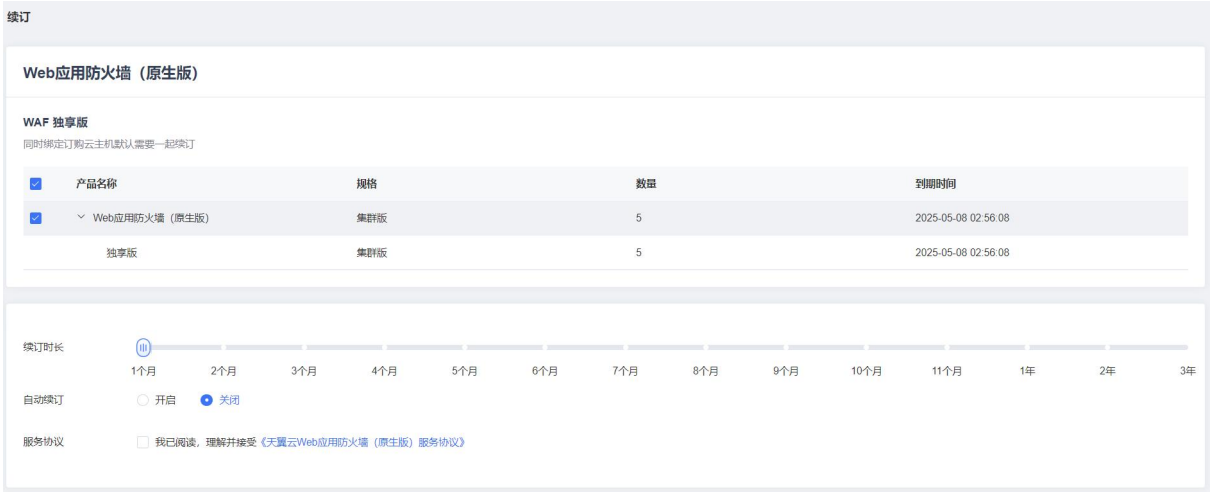
2. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“独享型”页签。

3. 单击目标实例操作列的“查看产品详情”。

4. 单击“续订”，进入续订页面。

5. 在“续订”操作界面，根据使用需要调整续订周期。

   续订“二类节点”区域的独享版实例时，实例绑定的云主机默认需要一起续订。



6. 续订时长设置完成后，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》“，单击“立即购买”。

4.7.2.5. 退订独享型实例

购买独享型实例后，在实例到期被删除前，您可以随时在 WAF 控制台退订实例。

操作步骤

1. 登录 Web 应用防火墙（原生版）控制台。
2. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“独享型”页签。
3. 单击目标实例操作列的“查看产品详情”。
4. 单击“退订”，进入退订页面。
5. 确认退订信息后，单击“立即退订”。

   退订“二类节点”区域的独享版实例时，实例绑定的云主机默认需要一起退订。

6. 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。

4.7.3. 管理归档日志

当日志超过热日志分析上限，将执行自动归档，将超过热日志上限的部分自动归档。

当日志超过热日志分析上限时，系统将自动对超出部分执行归档操作。

- 日志归档周期：每日凌晨 2 点自动归档一次。
- 归档日志存储时间：180 天。

下载归档日志

> 说明：
>
> 文件生成时间与文件中日志起始时间可能存在较大差异，若选择文件时间内未找到目标时间日志，可下载与目标时间相邻的文件。

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 管理归档日志”。
5. 查询日志：
   - 选择模式：支持选择“云 SAAS 模式”、独享版实例。
   - 日志文件名称：支持模糊搜索文件名称。
   - 归档时间：根据选择的时间范围过滤文件归档时间。
6. 查看日志文件列表。

参数	说明
日志文件名称	根据归档文件生成时间命名的文件。
日志时间	显示该归档文件内日志的起止时间。
归档时间	显示文件的归档时间。

参数	说明
文件条数	当前文件内归档的日志条数。
文件大小	显示文件的大小。
文件类型	显示文件的类型，攻击日志或访问日志。

7. 下载日志：单击操作列的“下载”，下载对应日志文件。
   - 选择“云 SAAS 模式”，支持下载对应归档文件。
   - 选择独享版实例，仅支持查看日志归档记录，不支持下载归档文件。

4.8. 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。

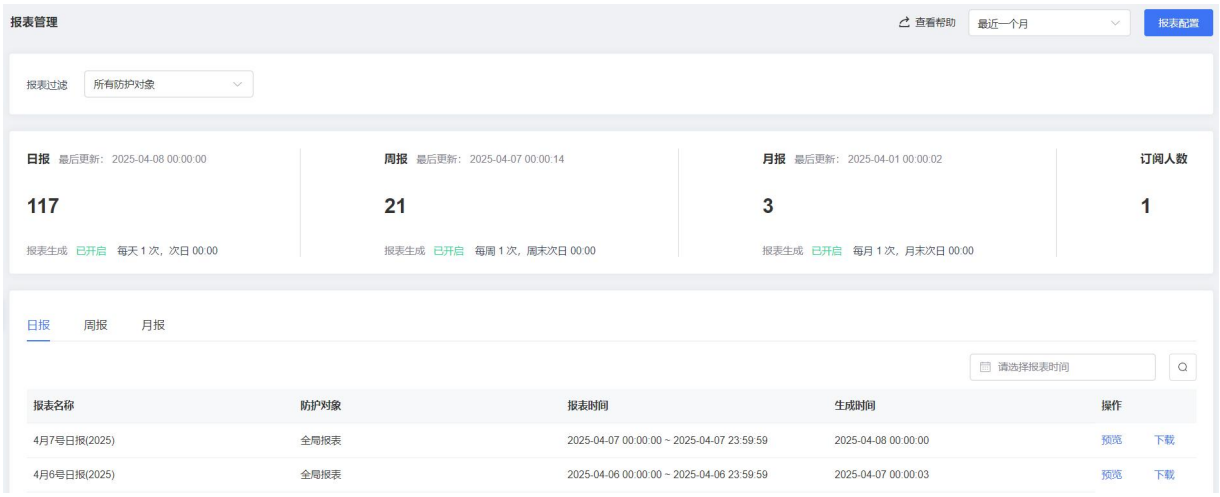
- 日报：每天 00:00:00 生成前一日的报表。
- 周报：每周一 00:00:00 生成前一周的报表。
- 月报：每月 1 日 00:00:00 生成前一月的报表。

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。

订阅报表

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“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。
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。

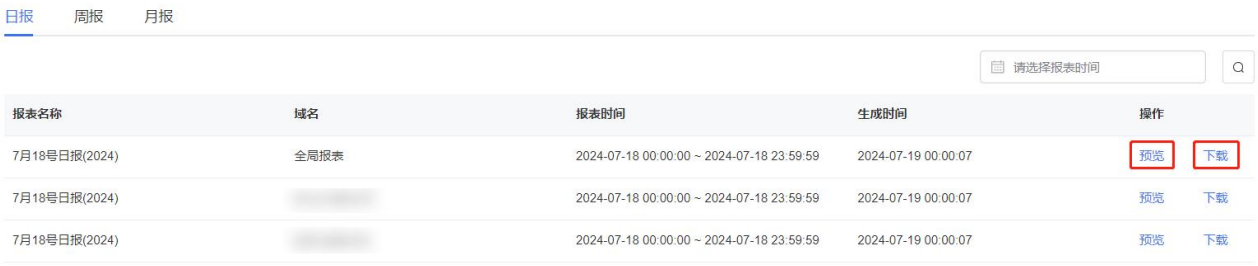
查看及下载报表

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. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“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。

4.9. 权限管理

Web 应用防火墙（原生版）通过 IAM（统一身份认证服务，Identity and Access Management）对用户权限进行管理，IAM 可以帮助用户安全地控制 Web 应用防火墙（原生版）服务的访问及操作权限。

默认情况下，天翼云主账号拥有管理员权限，而主账号创建的 IAM 用户没有任何权限。IAM 用户需要加入用户组，并给用户组授权相应策略后，IAM 用户才能获得策略对应的权限，才可以基于被授予的权限对云服务进行操作。

IAM 应用场景

IAM 策略主要面向同一主账号下，对不同 IAM 用户授权的场景：

- 您可以为不同操作人员或应用程序创建不同 IAM 用户，并授予 IAM 用户刚好能完成工作所需的权限，比如查看权限，进行最小粒度授权管理。
- 新创建的 IAM 用户可以使用自己的登录名和密码登录控制台，实现多用户协同操作时无需分享账号密码的安全要求。

IAM 策略说明

天翼云为 Web 应用防火墙（原生版）提供如下系统策略。如果系统策略不满足授权要求，可以创建自定义策略，自定义策略是对系统策略的扩展和补充。

策略名称	策略描述	类别	授权范围
ctwaf admin	Web 应用防火墙（原生版）管理员，拥有全部操作权限。	系统策略	全局级
ctwaf monitor	Web 应用防火墙（原生版）运营人员，不具备具名接入、产品信息页面功能权限，具备其他页面功能权限。	系统策略	全局级
ctwaf viewer	Web 应用防火墙（原生版）分析人员，只具备查看权限。	系统策略	全局级

通过 IAM 授权使用 Web 应用防火墙（原生版）

以下步骤，以仅授予用户“ctwaf admin”策略为例，实现用户只能访问、使用 Web 应用防火墙（原生版）服务，无法访问其他云服务的权限管理目标。

步骤一：创建用户组并授权

用户组是用户的集合，IAM 通过用户组功能实现用户的授权。

1. 使用主账号登录天翼云控制台，在右上角单击头像选择“账号中心”，在左侧导航中选择“统一身份认证”，或者直接点击 IAM 控制台。
2. 在左侧导航栏，选择“用户组”，单击右上角的“创建用户组”。
3. 在“创建用户组”界面，输入用户组名称和描述。

4. 单击“确定”，完成用户组创建。用户组列表中显示新创建的用户组。

5. 在用户组列表中，单击新建的用户组右侧的“授权”。

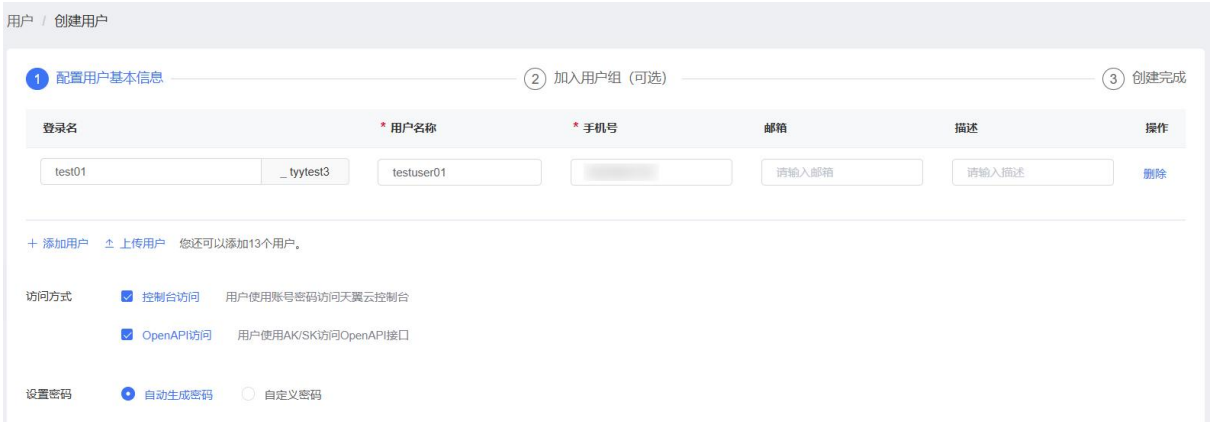
6. 选择策略：以仅授予用户“ctwaf admin”权限为例。在右上角“请输入策略名称进行搜索”框内输入策略名称进行搜索，勾选需要授予用户组的全局策略“ctwaf admin”，单击“下一步”。

7. 设置授权范围：由于上一步选择的系统策略，作用范围为全局，因此在设置授权范围时，默认勾选了“全局”选项，也可以指定企业项目。单击“确定”完成授权。

步骤二：创建 IAM 用户并加入用户组

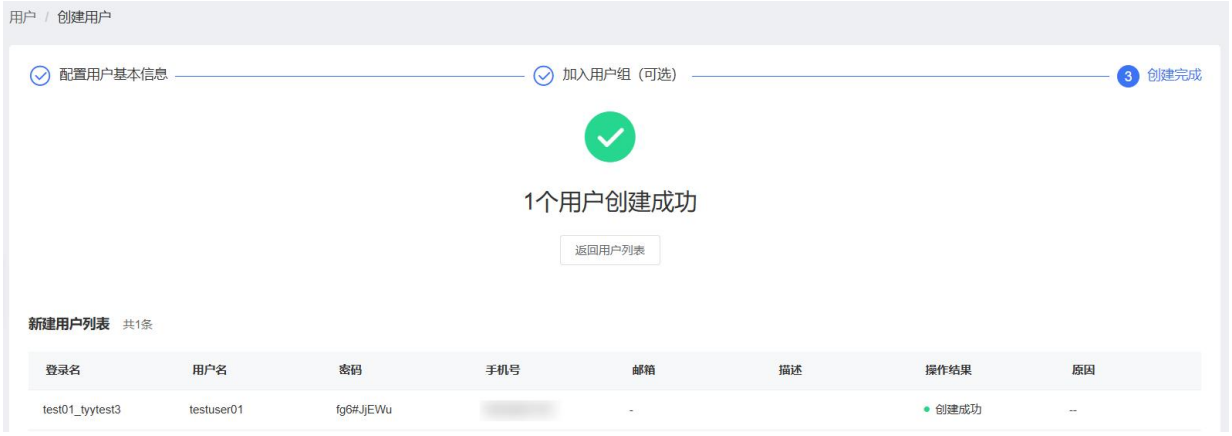
1. 在统一身份认证服务左侧导航栏，选择“用户”，单击右上角“创建用户”。
2. 配置用户基本信息：在“创建用户”界面填写“用户基本信息”，单击“下一步”。

   如需一次创建多个用户，可以单击“添加用户”添加多个用户，或单击“上传用户”进行批量创建。



3. 加入用户组：在左侧可选用户组列表中找到刚创建的用户组，单击操作列的“添加”将用户加入到该用户组。

4. 单击“下一步”，等待 IAM 用户创建完成。记录新建的 IAM 用户的登录名和密码。



步骤三：使用创建的 IAM 用户登录并验证权限

完成 IAM 用户创建后，即可以使用登录名和密码登录天翼云，验证权限（当前用户权限仅包含“ctwaf admin”权限）。

1. 使用新创建的 IAM 用户登录天翼云控制中心。
2. 在登录页面，输入 IAM 用户的登录名及密码。如果登录失败，IAM 用户可以联系主账号重置密码。

3. 执行以下操作，若满足预期结果，表示“ctwaf admin”权限已生效。
   - 在产品服务列表中选择“Web 应用防火墙（原生版）”，成功进入 Web 应用防火墙（原生版）控制台。
   - 在产品服务列表中选择除“Web 应用防火墙（原生版）”之外的其他服务，提示权限不足。

4.10. 查看云审计事件

操作场景

本服务现已对接天翼云云审计服务，云审计服务提供对各种云资源操作的记录和查询功能，用于支撑合规审计、安全分析、操作追踪和问题定位等场景，同时提供事件跟踪功能，将操作日志转储至对象存储实现永久保存。

云审计可提供的功能服务具体如下：

- 记录审计日志：支持用户通过管理控制台或 API 接口发起的操作，以及各服务内部自触发的操作。
- 审计日志查询：支持在管理控制台对 7 天内操作记录按照事件类型、事件来源、资源类型、筛选类型、操作用户和事件级别等多个维度进行组合查询。

使用限制

- 云审计服务本身免费，包括时间记录以及 7 天内时间的存储和检索。
- 用户通过云审计能查询到多久前的操作事件：7 天。
- 用户操作后多久可以通过云审计查询到数据：5 分钟。
- 其它限制请参考使用限制-云审计。

支持审计的关键操作列表

事件名称	读写类型
租户管理-获取 ICP 状态	读类型
租户的所有实例-详情	读类型
独享版租户-节点实时信息	读类型
独享版租户-查询实例列表	读类型
独享版租户-详情	读类型
独享版租户-修改实例信息	读类型

事件名称	读写类型
独享版租户-查询用户可用的 eip 列表	写类型
独享版租户-绑定 eip-ipv4	写类型
独享版租户-解绑 eip-ipv4	写类型
独享版防护对象-新增	写类型
独享版防护对象-更新	写类型
独享版防护对象-查询	读类型
独享版防护对象-详情	读类型
独享型和 saas 型的防护对象-查询	读类型
ELB 防护对象-查询 ELB 防护对象的可用资源池	读类型
安全策略-详情	读类型
安全策略-更新	写类型
规则组-查询	读类型
增强型 bot 规则-查询统计	读类型
增强型 bot 规则-查询	读类型
精准防护-查询统计	读类型
精准防护-查询	读类型
访问规则-新增	写类型
访问规则-查询统计	读类型
访问规则-查询	读类型
访问规则-详情	读类型

事件名称	读写类型
访问规则-查询加密套件	读类型
访问规则-获取可用端口	读类型
访问规则-API 安全获取防护对象	读类型
访问规则-查询 WAF 回源 IP 段	读类型
访问规则-查询域名是否备案	读类型
访问规则-根据资源池 id 获取 cname	读类型
API 列表-查询	读类型
API 安全业务用途-查询	读类型
全局规则表-对应非全局配置的 policy 表-详情	读类型
管理归档日志-查询	读类型
管理归档日志-获取当前实例已使用的归档空间	读类型

查看云审计事件

1. 开通云审计服务。

   参见开通云审计服务-云审计。

2. 查看云审计事件。

   参见查看审计事件-云审计。

3. 在事件列表中，选择事件来源为“安全”，资源类型选择“ctyun_waf”，上方时间选择需要筛选的时间段。点击“查询”即可。

4. 在审计事件右侧点击详情，可以看到更详细的事件信息。

更多云审计相关使用说明和常见问题请参考用户指南、常见问题。

5. 最佳实践

5.1. 网站通过域名接入 WAF 防护最佳实践

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。

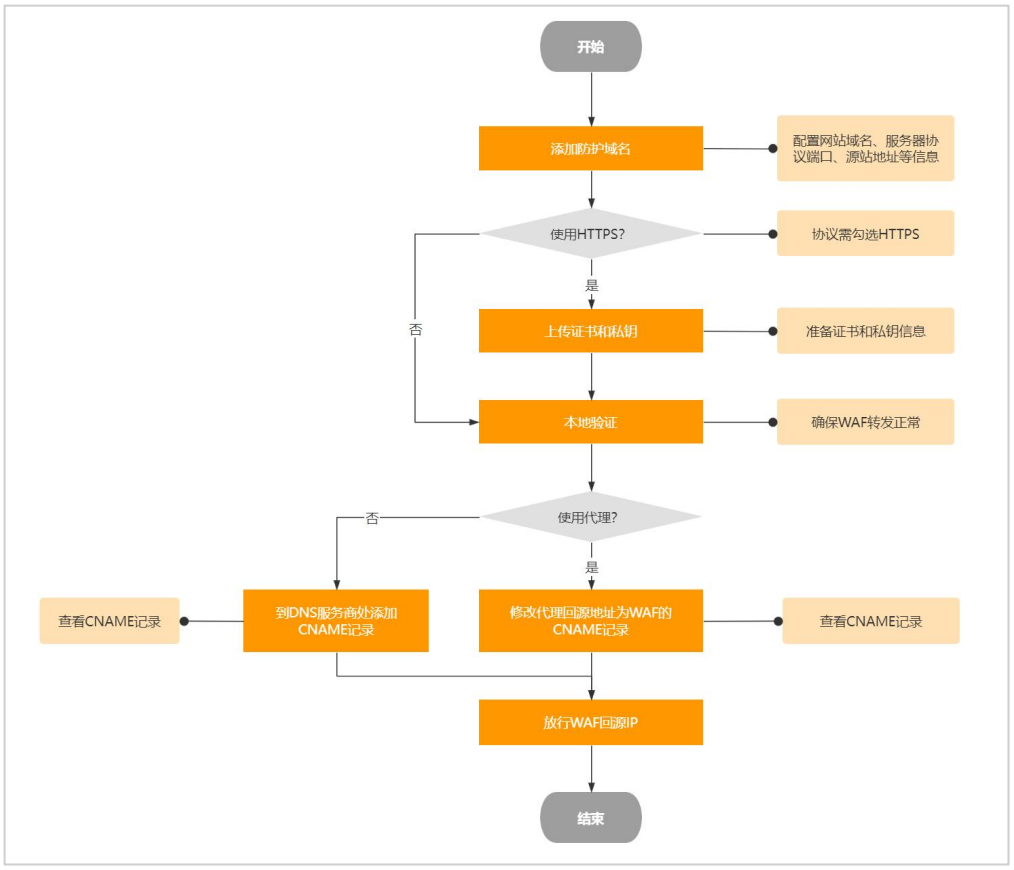
网站接入 WAF 准备工作

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。

> 说明：
>
> 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。

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。

5.2. DeepSeek 安全防护最佳实践

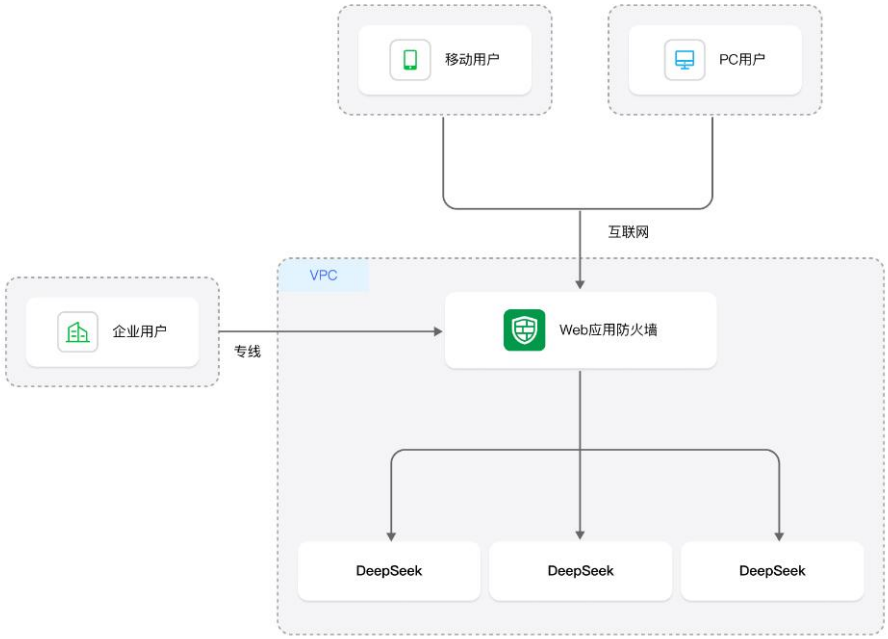
背景介绍

随着人工智能技术的快速发展，很多企业选择在 GPU 云主机或 GPU 裸金属上搭建 DeepSeek 私有化服务，在这个过程中，用户不仅享受到了强大的 AI 算力资源，同时也面临着复杂的网络威胁，如 DDoS 攻击、SQL 注入、跨站脚本（XSS）等。

为了保障 AI 算力资源、训练数据及服务 API 链路的安全性，部署 Web 应用防火墙成了必不可少的安全举措。Web 应用防火墙支持多种定制化的安全防护策略，帮助企业有效应对各种网络威胁，确保 DeepSeek 服务的稳定运行，保障 DeepSeeK 安全性。

DeepSeek 安全防护场景示意图

在 DeepSeek Web 安全防护场景中，用户的 DeepSeeK 服务部署在 GPU 云主机或 GPU 裸金属上，WAF 作为前端的安全网关，负责过滤所有进入的流量。通过 WAF 的定制化规则和先进的内容检测引擎，恶意流量被有效拦截，确保 AI 算力资源和训练数据的安全。



安全风险及应对方案

风险名称	风险描述	WAF 应对方案	相关文档
Web UI 漏洞	Open WebUI 0.1.105 版本存在文件上传漏洞，ComfyUI 多个插件存在安全漏洞。部署大模型过程中，通常会使用大模型自带的 WebUI 组件，开源的 Web UI 组件以及老旧的版本，为大模型的部署和应用带来了巨大的入侵风险。	开启 WAF 的 Web 攻击防护功能，为 Web UI 提供必要的安全防护能力。	Web 基础防护
企业敏感信息泄露	企业利用私有数据进行数据训练时，私有数据可能包含商业敏感信息，存在数据泄露风险。	根据企业机密信息内容，通过 WAF 精准访问控制功能，对敏感信息进行检测拦截，保障企业数据安全。	精准访问控制
大模型输入输出内容违规	私有化大模型输入输出内容可能涉及政治、赌博、色情、违法犯罪等违规内容，影响企业声誉。	通过 WAF 敏感信息防泄漏功能，自动屏蔽违规内容，保障企业声誉安全。	防敏感信息泄露
应用层 CC 攻击	由于多用户同时使用或单用户对大模型 API 接口	采用 WAF 的 CC 防护限速功	CC 防护

风险名称	风险描述	WAF 应对方案	相关文档
及 API 互联网暴露风险	的频繁调度导致大模型 token 被大量占用，服务器繁忙无法为用户提供正常服务；大模型 API 接口的暴露，会为用户的 API 接口带来安全风险。	能，保证大模型连续可用性；建设 API 安全监测与分析能力，降低因 API 漏洞造成的安全风险。	API 安全

方案优势

- 一键接入：无需复杂配置，只需在控制台简单操作几步即可完成网站接入，快速开启安全防护。
- 实时安全补丁：能够及时获取最新的漏洞信息和攻击特征，自动更新防御规则，有效应对新型攻击，确保用户始终处于最新的安全防护状态。
- 敏感内容定制：用户根据自身的业务需求，为敏感信息配置特定的防护规则，精确识别并过滤掉针对敏感信息的恶意请求，有效防止数据泄露和非法访问。
- 个性化 CC 防护：针对 DDoS 攻击，WAF 提供了个性化的 CC 防护策略。用户可以根据 Web 应用的业务特点，灵活调整防护阈值和策略，制定针对性的 CC 防护策略，精准识别和拦截恶意流量，确保在高流量攻击下仍能保持服务的稳定性。

方案总结

在人工智能服务日益普及的今天，WAF 提供的 Web 防护方案为用户 DeepSeek 服务提供了强大的安全保障。WAF 通过先进的内容检测引擎、定制化的敏感内容防护规则、以及个性化的安全防护建议，WAF 能够有效应对各种网络威胁，确保 AI 算力资源和训练数据的安全。无论是面对 DDoS 攻击、数据泄露还是零日漏洞，WAF 都能提供可靠的防护，帮助用户构建安全、稳定的 DeepSeek 环境。

5.3. 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。

- 防护规则组：可选择宽松规则组、正常规则组、严格规则组。
  - 正常规则组：中等宽松规则组，该规则组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。
- 处置动作：可选择拦截、观察两种动作。
  - 拦截：将会拦截掉所有攻击行为，并产生告警拦截日志。
  - 观察：会放行所有攻击行为，但会产生告警日志。

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。

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。

5.4. 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

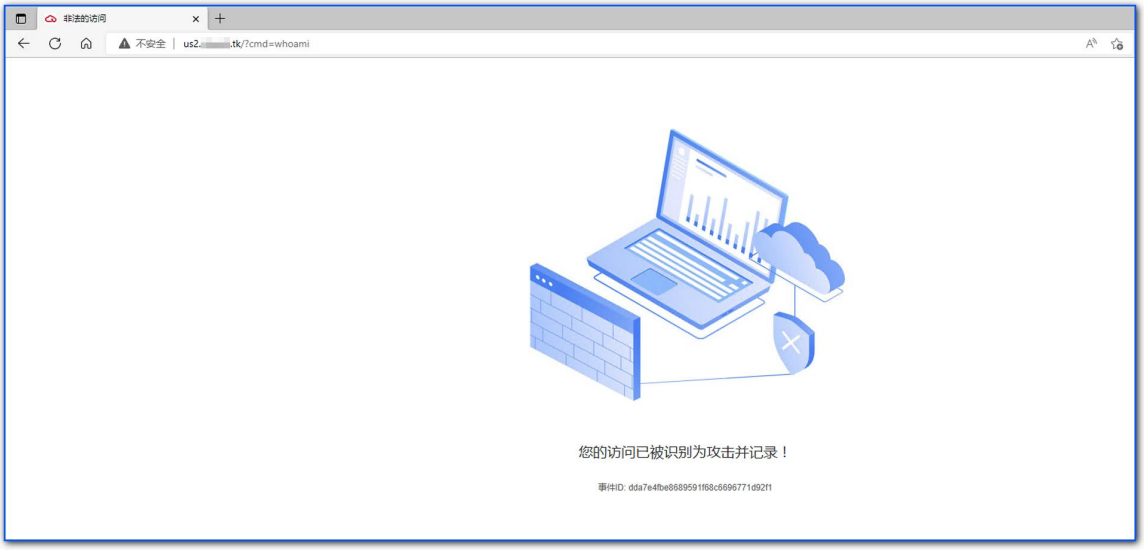
- 如果您对自己的业务流量特征还不完全清楚，建议先切换到“观察”模式。一般情况下，建议您观察一至两周，然后根据攻击日志分析网站访问情况。

- 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。

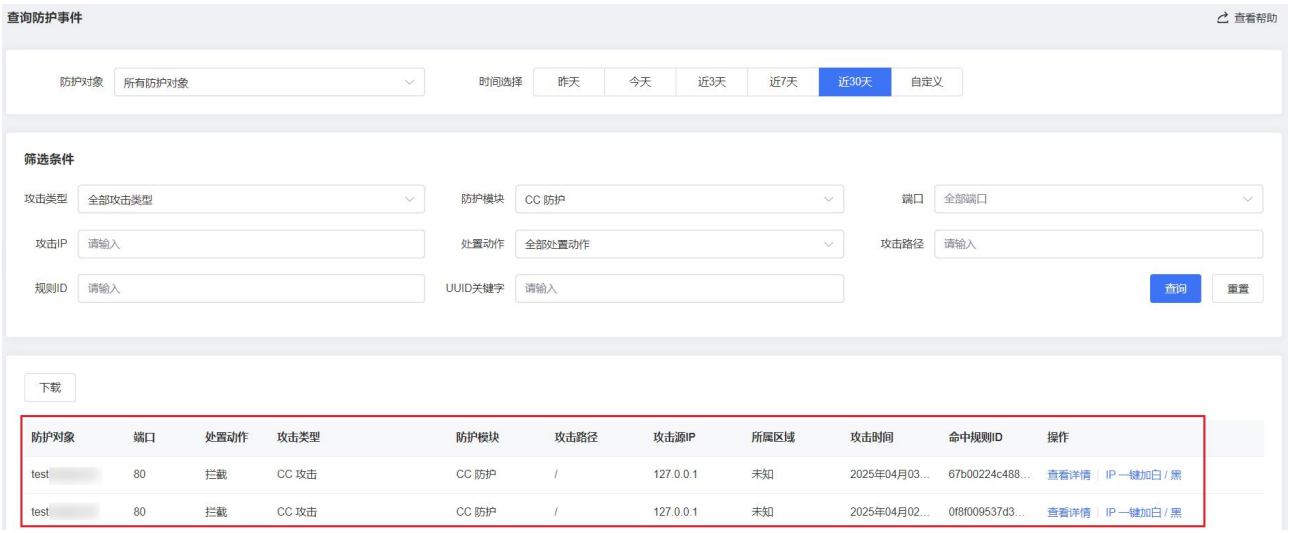
- 业务操作方面应注意以下问题：
  - 正常业务的 HTTP 请求中尽量不要直接传递原始的 SQL 语句、JAVA SCRIPT 代码。
  - 正常业务的 URL 尽量不要使用一些特殊的关键字（UPDATE、SET 等）作为路径，例如：“www.example.com/abc/update/mod.php?set=1”。
  - 如果业务中需要上传文件，不建议直接通过 Web 方式上传超过 50M 的文件，建议使用对象存储服务或者其他方式上传。

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。



5.5. 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、HEADER。
- 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。

5.6. “自动封禁/解封攻击者”配置实践

Web 应用防火墙（原生版）的企业版及以上版本支持自定义 BOT 防护策略，通过智能 BOT 防护+攻击惩罚，帮助用户实现自动化动态拉黑攻击 IP，实现业务的自动化防护。

用户可以结合业务情况进行自定义防护规则的配置，实现自动封禁和自动解禁。

示例场景

- 防护对象：“www.ctyun.cn”。
- 触发条件：来自“xxx.xxx.10.15”的请求中，5 秒内“请求 URI 中包含 password”的请求次数大于等于 10 次。
- 处置措施：自动封禁“xxx.xxx.10.15”30 分钟，30 分钟后解封。

前提条件

- 已购买 WAF SaaS 模式企业版或旗舰版实例。
- 防护域名“www.ctyun.cn”已接入 WAF 并开启防护。

步骤一：配置并开启 BOT 防护

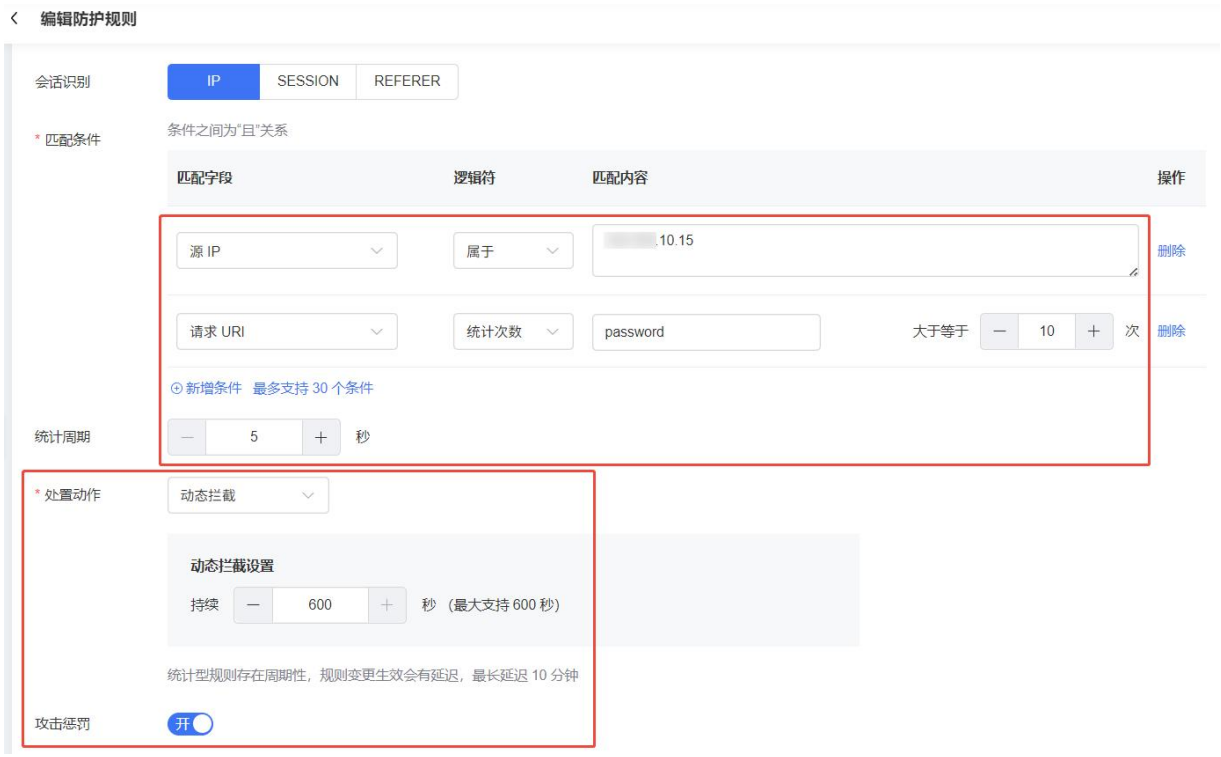
1. 开启 BOT 防护：在“防护配置 > 对象防护配置”页面，选择“安全防护”页签，定位到“BOT 防护”模块，开启 BOT 防护。

2. 单击自定义规则右侧的“前去配置”，进入自定义防护规则页面。

3. 单击“新建防护规则”，添加一条自定义防护规则。

- 匹配条件：来自“xxx.xxx.10.15”的请求中，5 秒内请求 URI 中包含 password 的请求次数大于等于 10 次。
- 处置动作：动态拦截最大支持 600 秒（即 10 分钟）。

- 攻击惩罚：需要拦截超过 10 分钟，可以开启攻击惩罚。攻击惩罚功能可将多次触发自定义规则的会话对象进行自动拉黑封禁。



步骤二：配置并开启攻击惩罚

1. 在“防护配置 > 对象防护配置”页面，选择“系统配置”页签，定位到“攻击惩罚”模块，开启攻击惩罚。

2. 单击攻击惩罚右侧的“前去配置”，进入攻击惩罚配置页面。

3. 配置攻击惩罚标准。

- 首次拦截：触发后封禁 30 分钟，到期自动解除封禁。
- 重复拦截：每新增一次拦截，封禁时长增加 10 分钟（如第二次封禁 40 分钟，第三次 50 分钟，依此类推）。
- 永久拦截：同一 IP 累计触发 5 次拦截后，将被永久封禁。

步骤三：验证拦截效果

当“xxx.xxx.10.15”访问“www.ctyun.cn”页面时，若 WAF 检测到 5 秒内“请求 URI 中包含 password”的请求次数大于等于 10 次，访问请求会被 WAF 拦截，且自动封禁“xxx.xxx.10.15”，时长为 30 分钟。

1. 查看防护事件：在“防护事件 > 查询防护事件”页面，您可以查看该防护事件。

2. 查看 BOT 防护动态拦截列表：在“防护配置 > 对象防护配置”页面，选择“安全防护”页签，定位到“BOT 防护”模块，单击拦截列表右侧的“解除拦截”，进入动态拦截页面，可查看已被拦截的对象及拦截时间。
3. 查看攻击惩罚列表：在“防护配置 > 对象防护配置”页面，选择“系统配置”页签，定位到“攻击惩罚”模块，单击惩罚列表右侧的“前去查看”，进入惩罚列表页面，可查看攻击惩罚拦截对象及惩罚时间。

步骤四：手动为封禁 IP 解封

说明：

当 IP 解封后，访问频率未超过设定阈值时，不会被封禁。

解除 BOT 防护动态拦截

1. 在“防护配置 > 对象防护配置”页面，选择“安全防护”页签，定位到“BOT 防护”模块。
2. 单击拦截列表右侧的“解除拦截”，进入动态拦截页面。
3. 对于正在拦截中的对象，单击操作列的“解除拦截”可放开拦截。

解除攻击惩罚

1. 在“防护配置 > 对象防护配置”页面，选择“系统配置”页签，定位到“攻击惩罚”模块。
2. 单击惩罚列表右侧的“前去查看”，进入惩罚列表页面。
3. 对于正在惩罚中的拦截对象，单击操作列的“解除惩罚”可放开惩罚对象封禁。

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）SaaS 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。

购买 WAF 云 SAAS 型实例后，如果 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 实例支持升配，当用户当前配置不能满足需要时，可以将低规格的产品升级为高规格的产品，例如将 WAF SaaS 版从标准版升级为旗舰版、或将防护域名从 1 个扩展为 5 个。

因产品升级或升配涉及计算资源、存储资源等资源扩充，相关资源无法弹性降低，故产品不能支持降级，同时已绑定的资源扩展包也不支持单独退订。因此，您在规划升级 WAF 产品规格或配置时，建议充分评

估当前需求，以便能够准确地购买到所需的产品规格。如您需要降低当前规格，您可以先退订当前的 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：天翼云 WAF 为您提供了便捷的自动续订功能，通过自动续订可以保证 Web 业务处于持续安全防护状态中，免受来源于网络中的恶意攻击。您可以在购买实例时勾选自动续订功能，也支持在使用过程中，在费用中心设置自动续订功能。

说明：

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“费用中心 > 订单管理 > 续订管理”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，可享受包年折扣。

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：WAF 不同版本支持不同规格的默认域名数量，如云 SaaS 模式基础版默认支持 10 个域名，标准版支持 20 个域名等，详情请参见“产品规格”。

若当前版本包含的域名个数不够用时，您可以通过购买域名扩展包的方式，或者直接升级当前实例版本的方式进行域名规格扩充。域名扩展包购买方式请参见“升级扩容”。

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，不能同时变更 WAF 的规格。您可以在续费完成后，对 WAF 实例进行升级扩容。

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。

服务到期后，若未开通自动续订，则资源将处于冻结状态，只能通过手动续费的方式重新开通服务。

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。

模式	扩展包	规格	数量限制
云 SaaS 模式	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 个主域名（备案的域名）。	最多支持 500 个域名扩展包。
	业务扩展包	1 个业务扩展包包含 1000QPS 业务请求峰值。 每增加一个业务扩展包，可增加 50Mbps 带宽弹性上限，100Mbps 带宽保护上限。	最多支持 30 个业务扩展包。
	规则扩展包	规则扩展包用于提升防护规则配额，支持以下两种扩展方式（二选一）： ● IP 黑白名单：每个扩展包包含 **50 条防护规则/域名。** ● 重保防护场景：每个扩展包包含 **1000 个 IP/实例。**	最多支持 1000 个规则扩展包。

模式	扩展包	规格	数量限制
独享模式	域名扩展包	1 个域名扩展包支持 10 个域名或 IP。	最多支持 1000 个域名扩展包。
	带宽扩展包	1 个带宽扩展包包含 1000QPS 业务请求峰值、50Mbps 业务带宽。	● 单机版：最多支持 16 个带宽扩展包。 ● 集群版：带宽扩展包的数量上限与节点数量相关联，每增加一个节点，带宽扩展包的上限数量增加 20 个。 例如，当集群包含 4 个节点时，最多支持配置 20 个带宽扩展包；而节点数量最多 12 个，则最多支持配置 180 个带宽扩展包。

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：WAF 云 SaaS 型实例在不同活动时期可以通过不同折扣购买。

- 当前优惠活动为 8 折。
- 另外一次性包年付费也可享受包年折扣，具体折扣如下表。

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%

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。

具体折扣价格以购买详情页为准。

Q：WAF 云 SaaS 模式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。

例如您在 2023 年 11 月 1 日 9:00:00 购买了 WAF 的标准版服务一个月，则该服务的到期时间为 2023 年 12 月 1 日 8:59:59，您需要支付的费用为购买标准版产品一个月的价格。在 2023 年 11 月 15 日，您需要购买 1 个域名扩展包满足域名扩展需求，此时您购买的域名扩展包到期时间不是 2023 年 12 月 15 日，而是与主套餐时间一致的 2023 年 12 月 1 日 8:59:59。您需要支付的扩展包费用也为 2023 年 11 月 15 日到 2023 年 12 月 1 日所需要花费的费用，而非扩展包全时段费用。

Q：购买的资源扩展包，支持单独退订吗？

A：不支持。资源扩展包可在主套餐使用期间的任意时间进行购买，其购买时计算的到期时间与主套餐到期时间一致，不单独计算，故资源扩展包购买后将与主套餐绑定，退订时也会随主套餐一同退订，即购买的资源扩展包不支持单独退订。

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：如何选择业务扩展包？

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。

Q：不同版本的 WAF 规格差异是什么？

A：Web 应用防火墙（原生版）提供两种版本：WAF 云 SaaS 模式和 WAF 独享模式。

- WAF 云 SaaS 模式根据支持防护的业务规模以及提供的防护功能不同，提供基础版、标准版、企业版、旗舰版四个版本供用户选择。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。
- WAF 独享模式提供单机版、集群版供用户选择，且支持选择购买域名扩展包和带宽扩展包。

分类	功能点	WAF SaaS 版				WAF 独享版	
		基础版	标准版	企业版	旗舰版	单机版（1 节点/实例）	集群版（4~12 节点/实例）
套餐基础信息	业务 QPS 峰值	100QPS/实例	3000QPS/实例	5000QPS/实例	10000QPS/实例	3000QPS/实例	20000QPS/实例
	支持主域名个数	1 个/实例	2 个/实例	5 个/实例	8 个/实例	100 个/实例	10000 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	100 个/实例	10000 个/实例
	支持防护的 ELB 监听器个数	×	600 个/实例	2500 个/实例	10000 个/实例	×	×
	泛域名防护	×	√	√	√	√	√
	IPv6 防护	×	√	√	√	√	√
	HTTP/HTTPS 非标准端口	仅支持	√	√	√	√	√

分类	功能点	WAF SaaS 版				WAF 独享版	
		基础版	标准版	企业版	旗舰版	单机版 (1 节点/实例)	集群版 (4~12 节点/实例)
	防护	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	不限制，最大 65535 个	不限制，最大 65535 个
	带宽弹性上限	10Mbps 超过 10Mbps 即丢包	200Mbps，超过弹性带宽上限不超过带宽保护上限的流量将直接转发，可通过扩展业务扩展包的形式增加弹性上限	300Mbps，超过弹性带宽上限不超过带宽保护上限的流量将直接转发，可通过扩展业务扩展包的形式增加弹性上限	400Mbps，超过弹性带宽上限不超过带宽保护上限的流量将直接转发，可通过扩展业务扩展包的形式增加弹性上限	200Mbps 超过 200Mbps 即丢包	1000Mbps 超过 1000Mbps 即丢包
	带宽保护上限	-	400Mbps，超过带宽保护上限的流量将会被直接丢弃，可通过购买业务扩展包的形式增加保护上限	600Mbps，超过带宽保护上限的流量将会被直接丢弃，可通过购买业务扩展包的形式增加保护上限	800Mbps，超过带宽保护上限的流量将会被直接丢弃，可通过购买业务扩展包的形式增加保护上限	-	-
基础安全防护	规则白名单	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	√，最大 1000 条	√，最大 1000 条
	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	√，支持自定义	√
	自定义防护规则组	×	√，10 个/实例	√，20 个/实例	√，30 个/实例	最大 100 个	最大 100 个
	0Day 漏洞虚拟补丁	√	√	√	√	√	√
	IP 黑白名单	×	√，200 条/实例	√，500 条/实例	√，1000 条/实例	√，1000 条/实例	√，1000 条/实例
	地域封禁	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	√，1000 条/实例	√，1000 条/实例
	自定义精准	×	√，100 条/实	√，200 条/实	√，500 条/实例	√，1000 条/实	√，1000 条/实例

分类	功能点	WAF SaaS 版				WAF 独享版	
		基础版	标准版	企业版	旗舰版	单机版（1 节点/实例）	集群版（4~12 节点/实例）
	防护策略		例	例		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	1000 条/实例	1000 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	√，1000 条/实例	√，1000 条/实例
	动态防护	×	√，与 BOT 防护共享规则	√，与 BOT 防护共享规则	√，与 BOT 防护共享规则	√，与 BOT 防护共享规则	√，与 BOT 防护共享规则
	BOT 攻击惩罚策略上限	×	1000 个/实例	1000 个/实例	1000 个/实例	10000 条/实例	10000 条/实例
	攻击惩罚防护策略上限	×	1000 个/实例	1000 个/实例	1000 个/实例	10000 条/实例	10000 条/实例
	数据统计分析	√	√	√	√	√	√
	敏感信息保护	×	×	√，50 个/实例	√，50 个/实例	√，1000 条/实例	√，1000 条/实例
	网页防篡改	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	√，1000 条/实例	√，1000 条/实例
	Cookie 防篡改	×	×	√	√	√	√
	隐私屏蔽	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	√，1000 条/实例	√，1000 条/实例
	重保防护场景	×	√	√	√	×	×
	全局防护白	×	√，20 条/实例	√，50 条/实例	√，100 条/实例	×	×

分类	功能点	WAF SaaS 版				WAF 独享版	
		基础版	标准版	企业版	旗舰版	单机版（1 节点/实例）	集群版（4~12 节点/实例）
	名单						
	全局精准访问控制	×	√，100 条/实例	√，200 条/实例	√，500 条/实例	×	×

6.1.2. 如何查看当前购买产品的产品规格

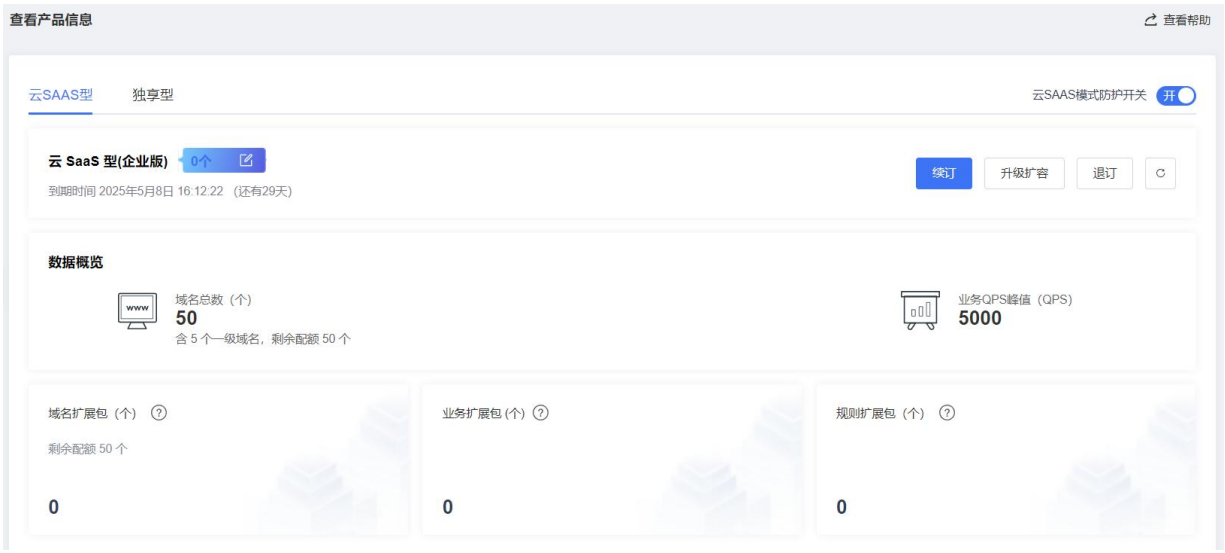
购买、续订、升级扩容后可以通过产品信息页面查看所购买产品的规格，同时个人消息中心以及用户绑定的手机也能够收到相关的购买成功提示短信。

查看购买后的 WAF 规格方式如下：

查看云 SaaS 型产品信息

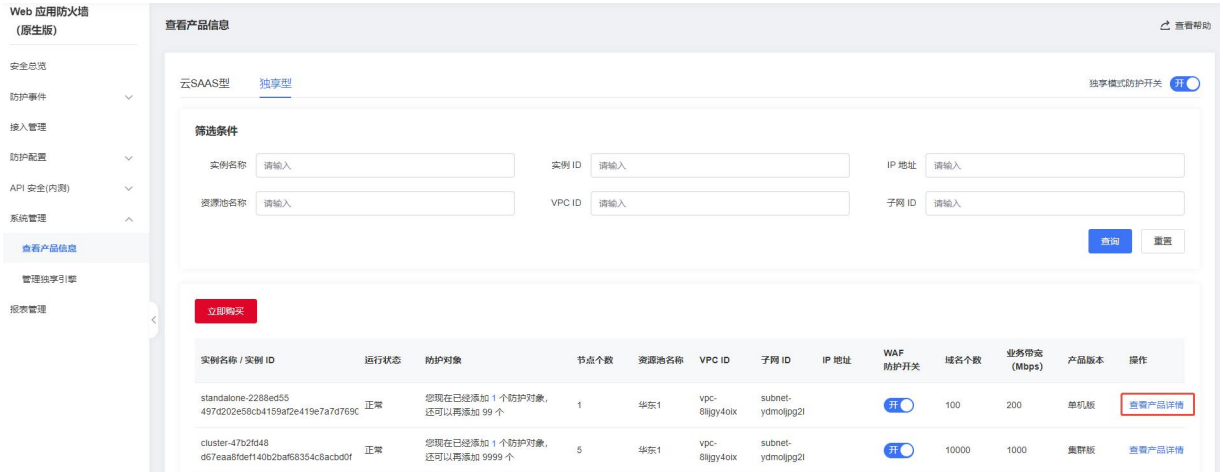
1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“云 SAAS 型”页签。
5. 在产品信息页面，可以查看实例版本、到期时间、实例规格等信息，并支持对实例进行管理。

> 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。



查看独享型产品信息

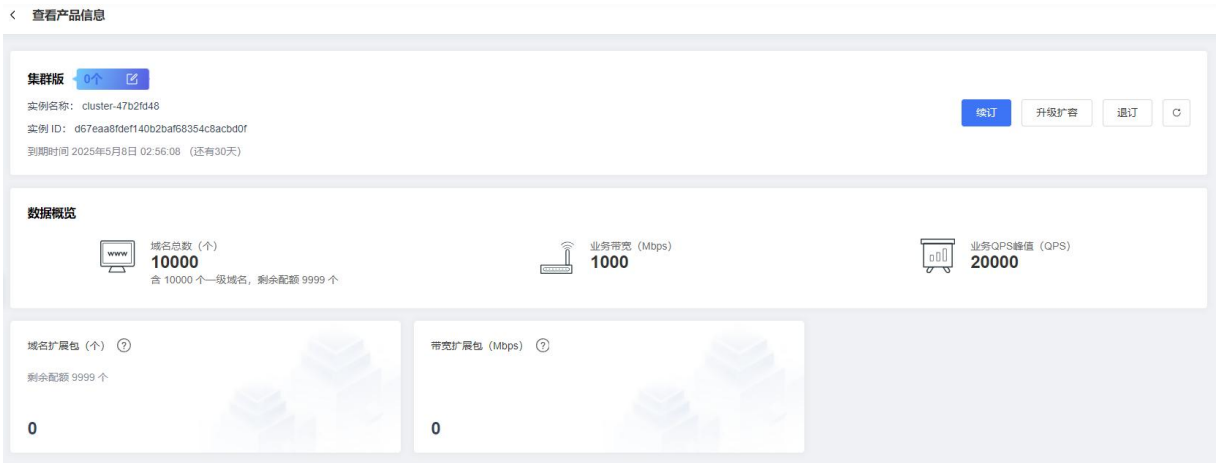
1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > Web 应用防火墙（原生版）”。
4. 在左侧导航栏，选择“系统管理 > 查看产品信息”，选择“独享型”页签。
5. 单击目标实例操作列的“查看产品详情”。



6. 在产品信息页面，可以查看实例版本、实例名称、实例 ID、到期时间、实例规格等信息，并支持对实例进行管理。

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：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，用户通过将需要防护的域名接入到 WAF 中，并将 DNS 服务商处对应域名的解析修改至 Web 应用防火墙所提供的 CNAME，从而实现将需要防护域名的请求转发到 WAF 进行防护，而源站对于 WAF 来说，只是用于转发请求的目标地址，如果多个域名使用了同一个源站对外提供服务，只需要将多个域名都接入 WAF 中即能实现对所有域名的防护。

注意：

在对多个域名接入同一个源站进行防护时，需要购买的防护带宽为所有域名累加的带宽，若购买的带宽小于所需要防护的带宽时，超过防护带宽容量的访问将得不到保护。

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：WAF 防护网站是通过域名+端口方式接入 WAF 进行防护的，即当管理员在接入时配置的 80 端口，那 Web 应用防火墙也只会接收来自于 80 端口的请求，当出现非 80 端口的请求时，例如 443 端口或其他端口，WAF 则会将对应的请求丢弃掉。所以在添加防护域名时，您需要将您所有需要防护的域名以及对应域名下所有需要防护的端口都进行配置，若服务器本身开启了多个端口，并且多个端口同时提供 Web 服务，其中只有部分端口需要防护，那只需要接入需要防护的域名及端口即可。

注意：

WAF 在提供端口防护时，默认将请求的目标端口作为回源端口，例如请求 80 端口，则回源也是通过 80 端口进行回源；请求 443 端口，则默认通过 443 端口回源。

但当开启了强制 HTTPS 回源或强制 HTTP 回源时，WAF 会将所有请求强制转换为对应的请求进行回源，即强制 HTTP 回源，则会通过 80 端口进行回源；强制 HTTPS 回源，则会通过 443 端口回源。

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。

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.ctyun.cn，b.ctyun.cn 和 c.ctyun.cn 对应的服务器 IP 地址相同，可以直接添加泛域名*.ctyun.cn。

注意：

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、a.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。

如果同时存在单域名和泛域名，则单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。

Q：域名添加到 WAF 后，是否可以修改?

A：防护域名添加到 Web 应用防火墙后，用户可以针对所防护的域名配置对应的安全防护策略，同时当对应域名产生请求数据和安全防护数据时，Web 应用防火墙也会存储对应的日志数据，考虑用户所做的安全配置、对应的安全数据都与所防护的域名强相关，为了保证用户能够准确地对域名进行防护，故已经配置的域名不能修改。

如果需要增加新的防护域名但所购买的授权不足时：

您可以通过购买域名扩展包的方式增加防护域名的授权，一个域名扩展包包含 10 个域名，详情请参见升级扩容。

也可以删除原域名后再重新添加待防护的域名。

Q：WAF 对于用户添加的防护端口个数有限制吗？

WAF SaaS 版对端口个数有限制：

- 基础版仅支持标准 80、443 端口的防护。
- 标准版、企业版、旗舰版，支持标准的 80、8080、443、8443 端口，在一般情况下，该端口就能满足用户业务的需求。

当用户业务有其他情况，天翼云 WAF 根据用户订购的版本不同，为用户提供了不同的防护端口数，WAF SaaS 版端口防护限制数见下表：

服务版本	端口防护限制数
基础版	2 个
标准版	20 个
企业版	30 个
旗舰版	60 个

Q：Web 应用防火墙支持哪些非标准端口

A： WAF SaaS 模式基础版仅支持标准 80、443 端口的防护。

WAF SaaS 模式标准版、企业版、旗舰版支持标准的 80、8080、443、8443 端口，为了满足用户业务场景的需求，还支持配置非标准端口，具体支持的端口范围如下：

端口分类	HTTP 协议端口范围	HTTPS 协议端口范围
标准端口	80、8080	443、8443

端口分类	HTTP 协议端口范围	HTTPS 协议端口范围
非标准端口	1936, 1937, 1985, 2001, 3333, 3501, 3601, 4050, 5000, 5100, 5106, 5107, 5110, 5222, 5601, 5666, 5667, 5668, 5901, 6001, 6640, 6666, 6868, 7000, 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, 7744, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8012, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8095, 8096, 8097, 8098, 8099, 8106, 8181, 8334, 8336, 8443, 8686, 8765, 8780, 8800, 8880, 8888, 8889, 8980, 9000, 9001, 9002, 9003, 9011, 9021, 9023, 9027, 9037, 9040, 9080, 9081, 9082, 9100, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9999, 10000, 10001, 10040, 10080, 11033, 12601, 13201, 15080, 18080, 19090, 20080, 20202, 20203, 20204, 20205, 20443, 28080, 33702, 48800, 50751, 50761, 50776, 50780, 51654	4443, 5000, 5100, 5443, 5601, 5680, 6443, 6646, 6648, 6649, 6918, 7201, 7443, 7741, 7745, 7746, 7748, 7749, 7753, 7763, 7786, 8000, 8002, 8020, 8081, 8082, 8096, 8100, 8445, 8553, 8663, 8860, 8868, 8883, 8887, 8999, 9000, 9010, 9020, 9060, 9070, 9090, 9180, 9181, 9182, 9443, 9553, 9663, 10002, 10101, 10211, 10443, 10809, 12000, 12002, 12004, 12006, 13000, 13001, 13202, 13203, 18072, 18073, 18702, 18703, 18980, 30080, 30223, 30443, 33005

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.ctyun.cn，则泛域名证书必须为*.b.ctyun.cn，不能是*.ctyun.cn 或*.a.b.ctyun.cn。

Q：如何更新已绑定域名的证书?

1. 登录 Web 应用防火墙（原生版）管理控制台。
2. 在左侧导航栏选择“域名接入”，进入域名列表页。
3. 定位到需要更新证书的域名，单击操作列的“详情”，进入域名详情页。
4. 单击“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。

负载方式	原理说明	适用场景
轮询算法	按照顺序将请求依次分发到服务器列表中的各个服务器上。 当新的请求到来时，轮询算法会依次将请求分发给下一个服务器，直到所有服务器都接收到了相同数量的请求，然后再次从第一个服务器开始，保证每台服务器都能平均分担负载。	轮询算法简单公平，适用于大多数情况。
IP Hash	根据客户端的 IP 地址计算出一个哈希值，然后使用该哈希值来确定请求应该转发到服务器列表中的哪一台服务器上。 这样可以保证同一个客户端的请求始终被转发到同一台服务器上，从而实现会话保持。	IP 哈希算法适用于需要保持会话的场景。

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。

注意：

- 用户可以选择 HTTP 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。
- 也可以选择 HTTPS 回源，选择 HTTPS 回源默认回源端口是 443，开启 HTTPS 回源需要上传业务系统证书才能实现回源。

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?

域名接入

源站 IP 不可以填写云主机的内网 IP。

域名接入采用 CNAME 的方式将原本去向网站的请求转向的 WAF，从而实现对网站访问的安全防护，这些用户请求将在 WAF 进行安全检测和过滤后，发送回源站。当前 WAF 提供的 CNAME 为公网解析的 CNAME，只能解析到公网 IP 地址，无法解析到内网 IP，所以源站 IP 地址不能填写云主机的内网 IP。

注意：

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。

独享型接入

独享型实例与业务主机部署在同一 VPC，源站 IP 可以填写云主机的内网 IP。

Q：WAF 原生版是否支持配置多个源站 IP?

A：支持。回源地址支持 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设置的服务器地址。当前 1 个域名支持最多配置 40 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。每填写一个 IP 地址，按回车进行确认，支持自动识别 IPv4 和 IPv6 地址，多个地址之间按照选择的负载方式（轮询或 IP Hash）进行负载均衡。

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。

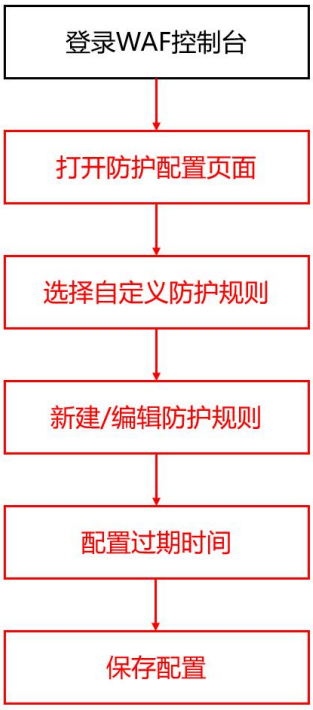
注意：

WAF 云 SaaS 模式的基础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 Web 应用防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防护配置 > 对象防护配置”。

3. 在“安全防护”页签定位到“精准访问控制”模块，选择自定义防护规则，单击“前去配置”。

4. 新建/编辑防护规则。

5. 设置过期时间。

6. 单击“保存”，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 Web 应用防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防护配置 > 对象防护配置”进入防护配置页面，在“安全防护”页签定位到“IP 黑白名单”模块，单击“前去配置”。

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 Web 应用防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防护配置 > 对象防护配置”进入防护配置页面，在“安全防护”页签定位到“防护白名单”模块，单击“前去配置”。

3. 新建白名单。

4. 进行白名单配置。

5. 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 2，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 1，如下图。

那此时系统会优先执行优先级为 2 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。

反之，如果将规则 2 的优先级设置为 2，即拦截所有 POST 请求。规则 1 的优先级设置为 1，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 Web 应用防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防护配置 > 对象防护配置”进入防护配置页面。
3. 在“安全防护”页签定位到需要设置优先级的模块，单击“前去配置”。

> 说明：
>
> CC 防护、BOT 防护、精准访问控制这三个防护模块支持设置规则优先级。

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?

可以防护。

- 域名接入：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。
- 独享型接入：WAF 的防护对象是域名或 IP 地址，如果多个域名使用了同一个源站对外提供服务，可以将多个域名都接入 WAF 实现所有域名的防护，或将网站 IP 接入 WAF 进行防护。

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：域名接入时，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。
- 对于客户端 IP，如果有白名单需要，建议您通过 WAF 白名单配置进行放行，不建议直接放行所有客户端 IP。

6.4.2. 如何删除 WAF 接入域名

域名还未完全接入 WAF

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。

域名已接入 WAF 进行防护

域名接入防护后，用户请求链路如下，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。