天翼云 •Web 应用防火墙（企业版）

用户使用指南

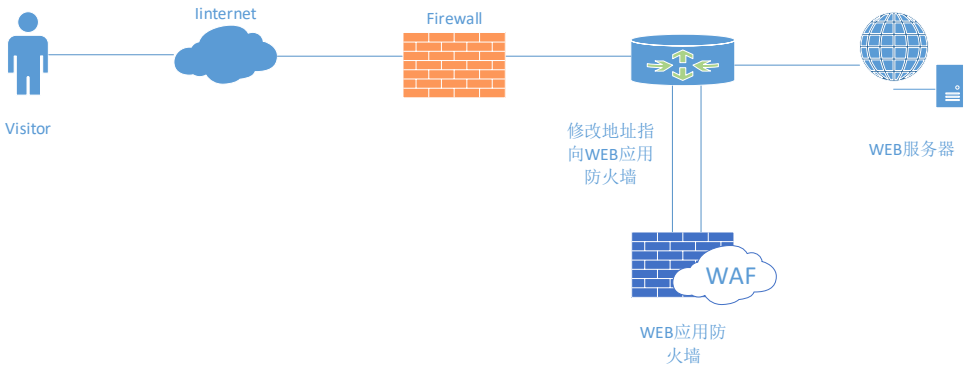
天翼云科技有限公司

目 录

1 产品概述

1.1 产品定义

Web 应用防火墙：Web Application Firewall，简称:WEB 应用防火墙。 Web 应用防火墙是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品，承担了抵御常见的 SQL 注入、XSS、远程命令执行、目录遍历等攻击的作用。



天翼云 Web 应用防火墙为用户自助配置 Web 防护的能力,通过 DNS 牵引的方式,将业务流量牵引至 WEB 应用防火墙清洗设备，再由 WEB 应用防火墙清洗设备回源至源站，同时配套提供一个高度管控、灵活使用的管理平台，达到配置简单、服务资源监控方便的目标。

1.2 产品功能

1、网络层防护

1）Http/HttpS Flood（CC 攻击）防护

2、 应用层防护和功能

1）黑白名单：

对指定访问源加白名单，对恶意访问来源进行封禁，支持 IP、URL、Useragent（用户代理）、Referer（Http 访问来源）。

2）HTTP 协议规范攻击防护：

包括特殊字符过滤、请求方式、内容传输方式，例如：multipart/form-data，text/xml，application/x-www-form-urlencoded。

3）注入攻击（form 和 URL 参数，post 和 get）防护

包括 SQL 注入防御、LDAP 注入防御、命令注入防护（OS 命令，webshell 等）、XPath 注入、Xml/Json 注入。

4）XSS 攻击访问

Form 和 URL 参数，post 和 get，包括三类攻击：存储式，反射式、基于 Dom 的 XSS。

5）目录遍历（Path Traversal）攻击防护。

6）认证管理和会话劫持攻击防护：

阻断认证管理、cookie 信息被盗用、会话劫持攻击。

7）内容过滤：

过滤 post form 和 get 参数。

8）Web 服务器漏洞探测攻击防护。

阻断 web 服务器漏洞探测。

9）爬虫防护：

限制阻断爬虫访问。

10）站点转换（URL rewrite）访问防护。

限制阻断访问站点转换访问。

11）网页检测到异常自动阻断源地址

12）认证管理和会话劫持

13）防护 CSRF

2 购买指南

2.1 价格

基础套餐包月（元/月）	域名扩展包（元/月）	带宽扩展包（元/月）
3488	540	900

备注：

1、基础套餐：版本默认包含一个域名包（支持 10 个子域名防护(限制仅支持 1 个一级域名)、200MB 带宽

2、域名扩展包：每增加 1 个域名包规格，支持 10 个子域名防护(限制仅支持 1 个一级域名)

3、带宽扩展包：每单位规格 50MB，逐级增加，最大支持 800MB

4、针对一次性包年付费服务，标准价格按照下述列表内容进行操作，且在订购时间期间不允许退订服务：

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%

2.2 订购

登录天翼云账号，在服务列表中找到安全组 Web 应用防火墙，点击“  ”进入订购页面，如下图。防护带宽默认显示 200M，域名包为 1 个，此为基础套餐包的量，用户可根据自己需要，增加防护带宽和域名包数量。并选择定能够时长。

2.3 续订

在产品实例列表点击【续订】跳转续订页面，页面显示当前服务规格和购买时长，选择续订时长，点击【立即购买】。

2.4 升级

在产品实例列表点击【升级】跳转升级页面，页面显示当前服务规格和升级后规格，用户可以选择升级后的防护带宽和域名包数量，勾选协议，点击【立即购买】。

2.5 退订

退订需要人工审核，点击【退订】，提交退订理由。等待人工审核，审核完成后停止业务并退款。

3 WEB 应用防火墙管理

3.1 WEB 应用防火墙实例管理

收到公测申请创建成功的通知后，重新登录天翼云控制中心下的 Web 应用防火墙，点击【WEB 应用防火墙实例列表】菜单，页面显示客户购买的 WEB 应用防火墙防护实例。购买后的实例可以续订及退订，但公测期内暂不支持续订及退订，待公测期结束后开放此功能。用户新增 WEB 应用防火墙防护时必须选择已经购买的实例 ID。

防护实例展示了实例 ID、防护域名包数量、防护带宽、购买时间、到期时间以及操作。

实例 ID：公测申请成功后系统自动分配实例 ID

防护域名包数量：每个防护域名包支持一个一级域名下包含二级域名在内 10 个防护配置；

防护带宽：防护的带宽；

购买时间：显示生成购买实例时间；

到期时间：显示实例到期时间；

操作：续订，点击续订转跳至续订页面，选择续订时间，生成订单续订成功后，到期时间延长。

退订，点击退订转跳至退订页面，点击确认退订，退订时请确认：务必将 DNS 指回服务器源站 IP，否则该域名的流量将无法正常转发。

公测阶段：续订、退订功能暂不开放。

3.2 域名备案

3.2.1 WEB 应用防火墙防护配置

防护配置管理为用户提供域名防护的配置操作功能：

1、 WEB 应用防火墙防护配置列表

显示如下，展示用户的防护配置清单列表，展示字段包括：

防护域名、CNAME、源站 IP、源端口、协议类型、状态、防护带宽、操作

防护域名：展示被防护的域名，例如；www.ctyun.com

CNAME：展示防护域名 CNAME（CNAME 规则：**源域名+.iname.damddos.com**）

源站 IP：用户配置的最终服务客户的主机 IP

源端口:源站 IP 的对外服务端口

状态：展示配置的防护状态，包括防护、未防护、启动防护中、防护配置失败；

防护带宽：用户购买实例的业务带宽大小；

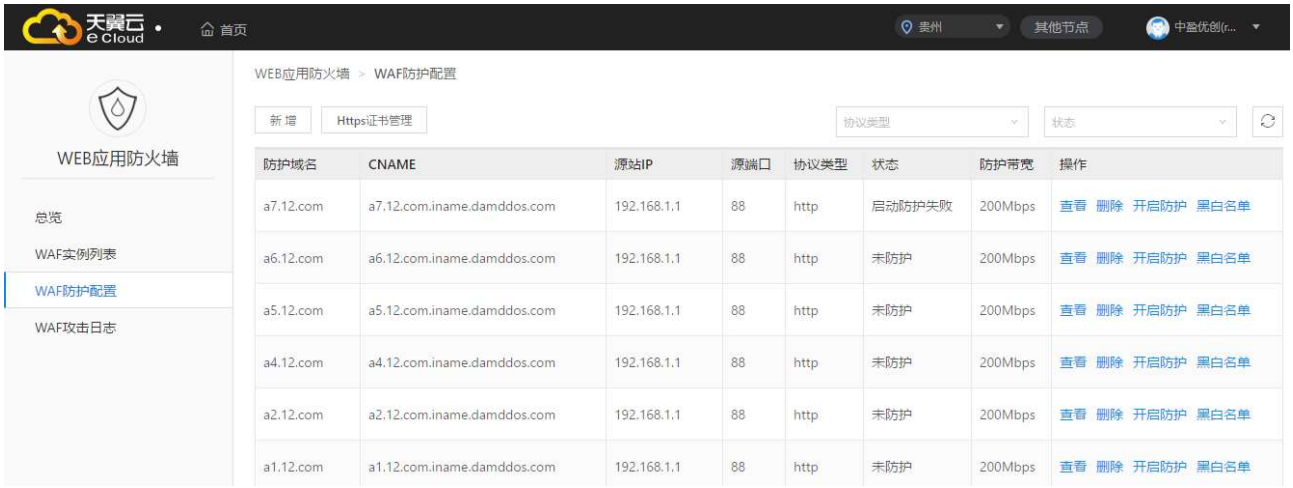
操作：查看，查看防护配置详情，不能进行修改；

删除，点击删除，将当前的防护配置清除，需要确保防护域名指回源站；

关闭防护，将正在防护中的任务关闭，需要确保防护域名指回源站；

开启防护，开启已新增（或者关闭过）的防护配置，开启成功后，您可以联系域名服务商将 DNS 域名指向防护 Cname 地址，届时防护配置正式生效。

黑白名单，配置黑白名单，详见黑白名单配置。



2、 新增：在 WEB 应用防火墙配置菜单下，点击新增，弹出 WEB 应用防火墙配置对话框：

1、 选择实例 ID；

2、 输入防护域名；

输入格式示例：

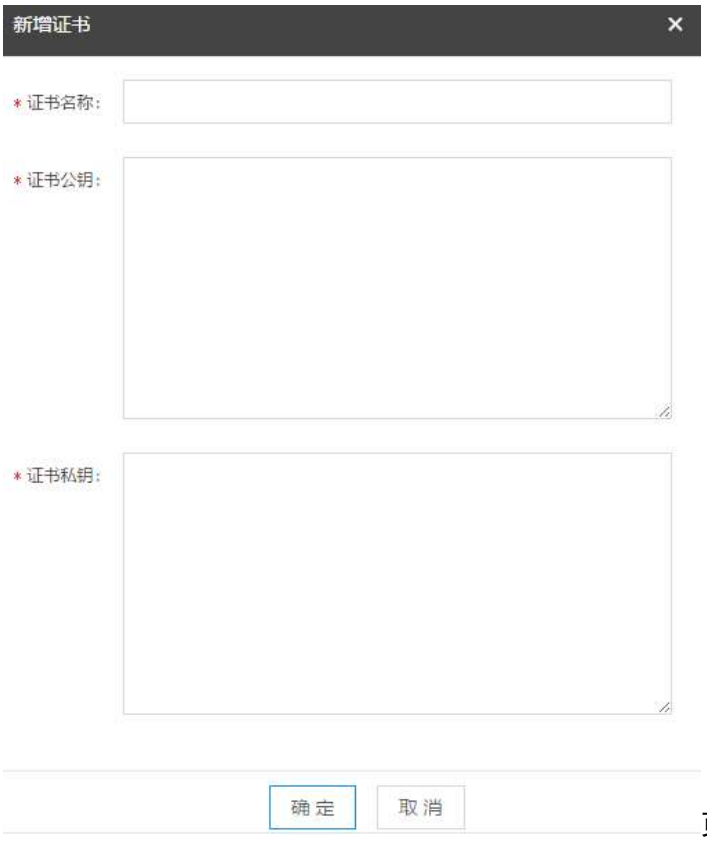
防护网站域名：如 www. ctyun. cn， 如果为二级域名：如 abc. ctyun. cn

3、 填入源站 IP；

4、 选择协议类型，填入源端口，http+https 最多合在一起最多填入 10 个端口，多个端口之间用英文逗号分隔；

5、 如果有 Https 情况下，需要选择 https 证书（https 证书可以通过新增 https 证书实现上传）

如果为初次填入 https 证书，可以点击“新增证书”



进入： 页面创建证书，证书创建成功后选择刚刚创建的证书。

6、 开启防护（默认勾选），如果未选中开启防护按钮，该配置不会生效，业务不会下发至 WEB 应用防火墙设备进行 WEB 应用防火墙防护。

7、 点击保存，确认后，正式下发防护配置。

3.2.2 Https 证书管理

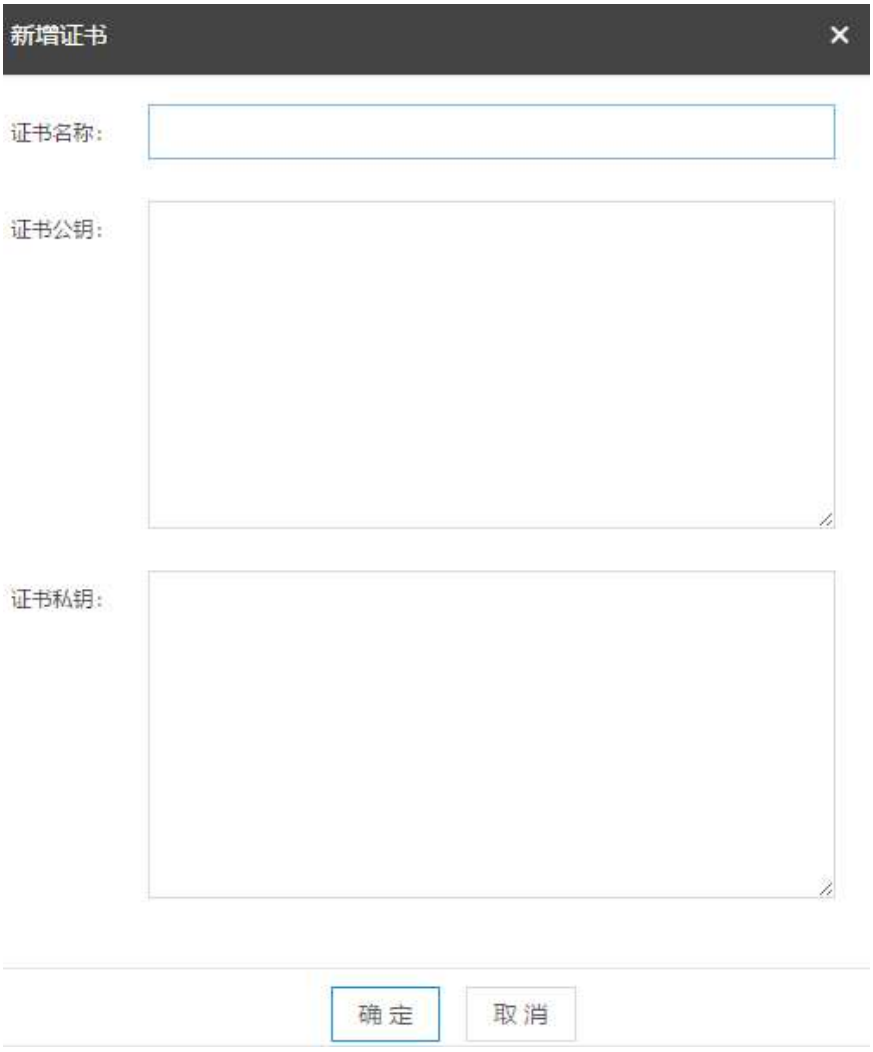
点击 https 证书管理 

，弹出 https 证书管理：

可以新增、删除证书。

Notice：删除证书需要确保证书未被使用或未被配置。

点击新增：



证书名称：输入证书名称，证书名称客户可以自行定义；

证书公钥：填入公钥字符串，如果用户公钥为文件格式，通过记事本打开公钥文件后，拷贝证书公钥字符串填入。

证书私钥：填入私钥字符串，如果用户私钥为文件格式，通过记事本打开私钥文件后，拷贝证书私钥字符串填入。

点击确认，保存公钥、私钥。

点击“删除证书”：删除证书时需要确认防护配置中（包括未启动的防护）未使用该证书，否则删除不成功。

3.2.3 域名解析

配置成功后，防护配置的状态变为：“防护中”；

之后客户可以进行域名解析：

如域名：www.ctyun.com

需要客户联系 DNS 服务商将域名解析指向 Cname：www.ctyun.com.iname.damddos.com

即：源域名+.iname.damddos.com

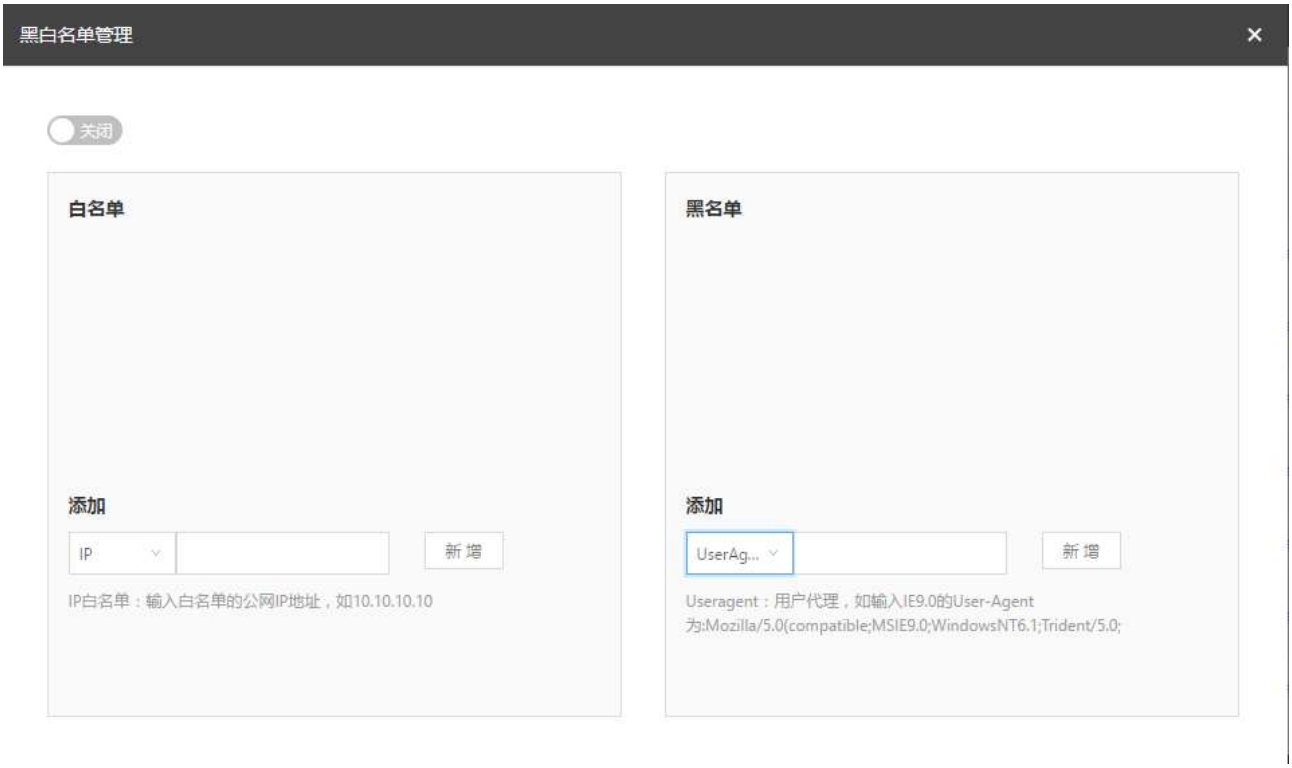
DNS 牵引指向 Cname 后，WEB 应用防火墙防护正式完成配置。

3.2.4 黑白名单管理

WEB 应用防火墙防护可以配置黑白名单，配置的参数包括：IP、URL、UserAgent、Referer

黑名单：配置了黑名单，所有访问来源全部屏蔽。

白名单：配置了白名单，所有访问来源全部放行。



IP 黑白名单：输入黑白名单的公网 IP 地址，如 10.10.10.10；

URL 黑白名单：输入黑白名单的 URL 地址，如 www.ctyun.cn；

Referer 黑白名单：指 HTTP 来源地址，比如如果点击一个网页的网址链接，那么浏览器会产生一个送到目标的 Web 服务器的 HTTP 请求，该请求中则会包含一个 Referer 字段（网页的地址），如网页 URL 为 http://www.ctyun.cn/product/cda，则输入 http://www.ctyun.cn/product/cda；

Useragent 黑白名单：Useragent 为用户代理，输入代理 Useragent 标识，如 IE9.0 的 Useragent 为:Mozilla/5.0(compatible;MSIE9.0;WindowsNT6.1;Trident/5.0;

当选择为关闭时，黑白名单配置不生效；

当选择为开启时，黑白名单配置生效

3.2.5 关闭防护

WEB 应用防火墙防护配置中：

点击关闭防护，关闭防护需要首先确保将 DNS 指回源站，否则该域名的流量将无法正常转发，请确定关闭该域名的防护功能。

3.3 攻击日志

攻击日志展示被防护域名的所有攻击事件。

点击菜单【攻击日志】，进入【攻击日志】页面；

攻击日志显示：

- 域名：告警域名
- 请求方法：http get/http post
- 访问 URL
- 告警级别
- 客户端 ip
- 地区
- 请求时间
- 处理方式

3.4 总览

1. 点击菜单【总览】，进入页面；
2. 展示监控网站详情：

包括监控的网站数（域名），当然攻击数，今日攻击数 102 个，以及攻击网站详单。

3. 展示攻击溯源：

- 攻击流量溯源图（BPS）

  显示的通过 Web 应用防火墙的每秒流量，包括总流量、CC 攻击流量、放行流量

- 攻击流量溯源图（TPS）

  显示通过 Web 应用防火墙的每秒访问数，包括总个数、CC 攻击个数。

- URL 访问分布统计

  展示 TOP4+other 访问分布饼状图

- 地区访问分布（地图）

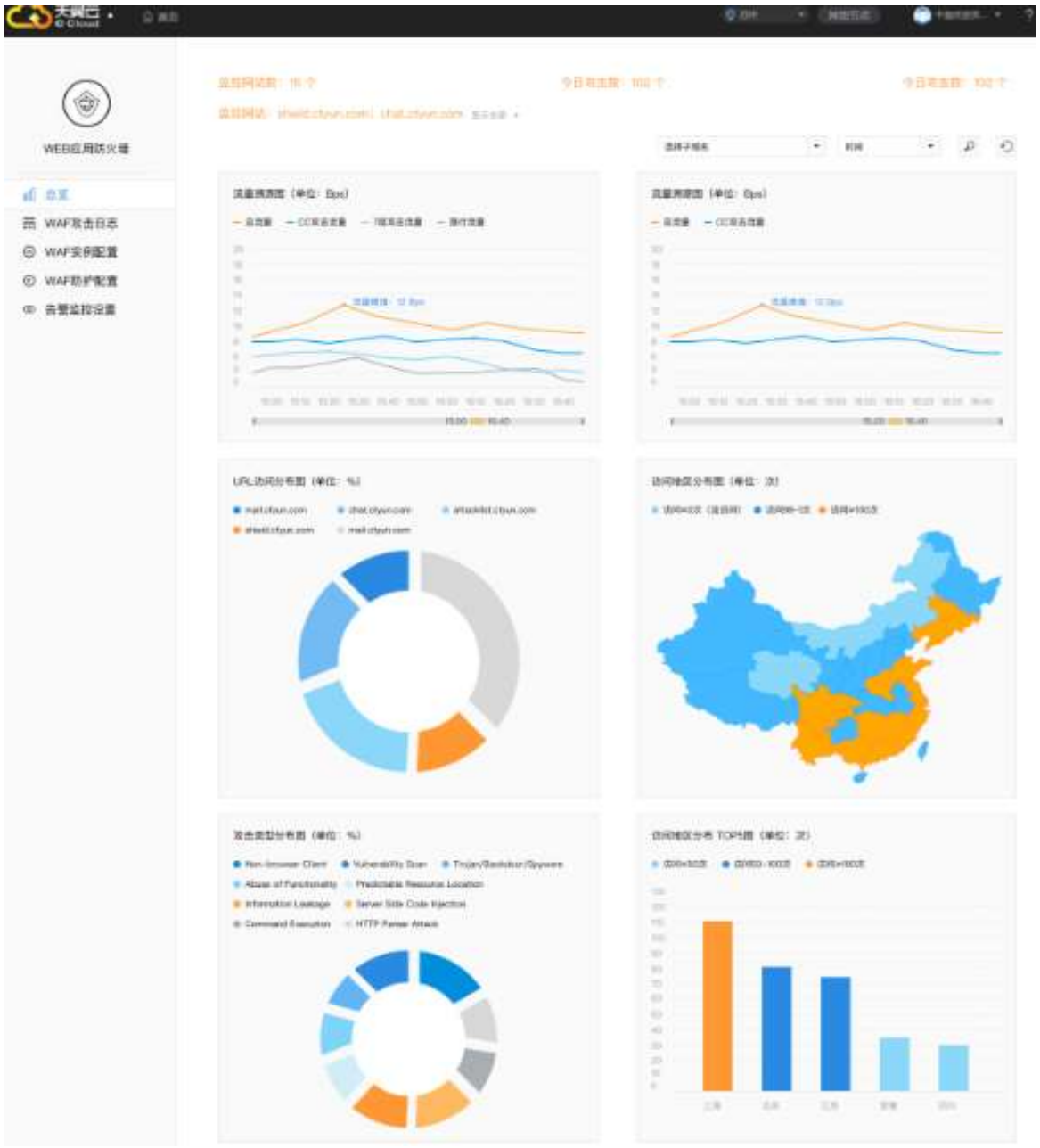
  展示按省份访问来源分布图

- 攻击类型分布

  展示 TOP4+other 攻击类型分布饼状图

- 地区访问分布 Top5

  展示 top5 攻击来源（省/市）柱状图


WEB应用防火墙
总览
WAF攻击日志
WAF实例配置
WAF防护配置
告警监控设置

4 常见问题

4.1 什么是 WEB 应用防火墙（WEB 应用防火墙）？

Web 应用防火墙：Web Application Firewall，简称:WEB 应用防火墙。 Web 应用防火墙是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品，承担了抵御常见的 SQL 注入、XSS、远程命令执行、目录遍历等攻击的作用，

4.2 天翼云 WEB 应用防火墙是付费产品吗？

天翼云 Web 应用防火墙作为天翼云安全业务的一个重要产品，作为付费的增值业务服务产品提供给天翼云客户，需要用户购买。

收费的标准详见天翼云 WEB 应用防火墙实例购买页面。

4.3 天翼云 WEB 应用防火墙流量牵引方式及步骤？

天翼云 Web 应用防火墙采用 DNS 牵引的方式，属于常引流。

在 WEB 应用防火墙自服务页面中防护配置生效后，需要客户联系 DNS 服务器商将网站域名解析指向 CNAME 地址，CNAME 规则为：防护域名+.iname.damddos.com，例如原域名 www.ctyun.cn，CNAME 为 www.ctyun.cn.iname.damddos.com）。

如果用户需要关闭实例、关闭防护，**首选需要确保已经联系 DNS 服务商将域名指向切换至源地址，**否则将影响客户的正常访问。

服务到期需要尽快续费，或者需要确保配置失效时将 DNS 指回源站。

4.4 天翼云 WEB 应用防火墙支持 HTTPS 协议吗？

支持。

天翼云 WEB 应用防火墙既支持 http，又支持 https，同时支持单个域名既有 https 又有 http。

每个二级域名支持 10 个 IP 端口。

4.5 一个域名包支持多少个二级域名？

一个域名包支持包含一个一级域名以及这个一级域名下二级域名总计十个域名的防护。如果超过 10 个，需要购买实例增加域名包数量以支持域名防护。

4.6 WEB 应用防火墙支持 IP 负载均衡吗？

不支持，天翼云 Web 应用防火墙只支持单个 IP 的访问，不支持 IP 负载均衡。

4.7 天翼云 WEB 应用防火墙需要关注的问题？

天翼云 WEB 应用防火墙防护需要注意确保 DNS 牵引的正确性。

天翼云 WEB 应用防火墙面向的客户为采用天翼云主机作为网站服务的客户，客户购买服务前提必须提供正确的网站域名。