文档中心

DDoS攻击防护 UDDoS

产品文档

目录

DDoS攻击防护 UDDoS

DDoS攻击防护 UDDoS

UDDoS（UCloud DDoS）DDoS攻击防护是为客户提供DDoS攻击防护产品。包括两种防护方式，一种是通过高防机房，另外一种是在IP带宽上直接抗DDoS攻击(清洗)。

	简介	优点	缺点
高防	为已备案的域名或源站IP（包括非UCloud的弹性外网IP）提供DDoS攻击防护。当用户的域名或源站IP（包括非UCloud的弹性外网IP）在遭受大流量的DDoS攻击时，可以通过高防IP代理源站IP面向用户，隐藏源站IP，将攻击流量引流到高防IP，确保源站的稳定正常运行。	能够抵抗更大的攻击，最大可支持1.2T的防护能力。并且可支持UCloud和非UCloud的源站IP。	需要更换新IP，操作较复杂，切换到高防上需要一定时间。
清洗	清洗是一款自研产品，为UCloud的弹性外网IP提供DDoS攻击防护，经过多年的攻防经验积累，采用多种防御策略，支持防御网络层攻击，比如TCP类报文攻击、SYN Flood攻击、ACK Flood攻击等	无需更换IP，受到攻击秒级切换，更低延迟响应。	无法抵抗更大的攻击，最大目前可支持10G防护。仅支持UCloud的弹性外网IP，不支持非UCloud的IP。

概览

- UCloud黑洞策略
- 封堵清洗告警回调说明
- 主机对外DDoS自查
- FAQ

UCloud黑洞策略

什么是黑洞?

黑洞是指当外网IP的入向流量速率超过其所在数据中心的限定阈值时,该IP会触发流量封堵机制,即对该IP的访问流量会被丢弃。

黑洞策略的必要性

为什么会有黑洞策略?为什么不能直接帮用户免费抗攻击?

1. 发生大流量攻击时,除了被攻击者,整个云网络都会受到影响,为了避免影响范围扩大,所以需要有黑洞策略。
2. DDoS防御需要两方面的成本:1)带宽成本,2)清洗成本。最大的成本就是带宽费用,而收取带宽费用的联通、电信、移动等运营商不会区分是正常流量还是攻击流量。UCloud会尽力为客户提供基础的攻击防御,但是当攻击超过限定的阈值就需要采取黑洞策略封堵IP。

黑洞时长多久?

对于被封堵的IP,一般会在24小时后进行解封。

注意:

针对最近一周内连续多次触发封堵机制的用户,UCloud保留延长封堵时间、限制购买外网IP及解绑并冻结外网IP等措施的权利。

被黑洞了怎么办?

如果不希望被黑洞,希望避免DDoS攻击影响业务应该怎么办?

如果是境内的机房:

受到攻击后,为了避免IP再被攻击而影响业务,建议更换源站IP并接入 高防 进行防护。

如果是境外的机房:

受到攻击后,无需更换源站IP,采用境外防护服务,保证业务的正常进行。

附:各数据中心的防护阈值

地域名称	防护阈值
华北一	3Gbps
华北二	3Gbps
上海	2Gbps
广州	2Gbps
香港	2Gbps,回内地方向1500Mbps
洛杉矶	2Gbps
华盛顿	2Gbps
法兰克福	2Gbps

曼谷	2Gbps，泰国国际线路1000Mbps
首尔	1Gbps
新加坡	2Gbps
东京	2Gbps
台北	2Gbps
迪拜	2Gbps
雅加达	1Gbps
孟买	2Gbps
圣保罗	2Gbps
伦敦	2Gbps
拉各斯	900Mbps
胡志明市	1Gbps
马尼拉	1Gbps

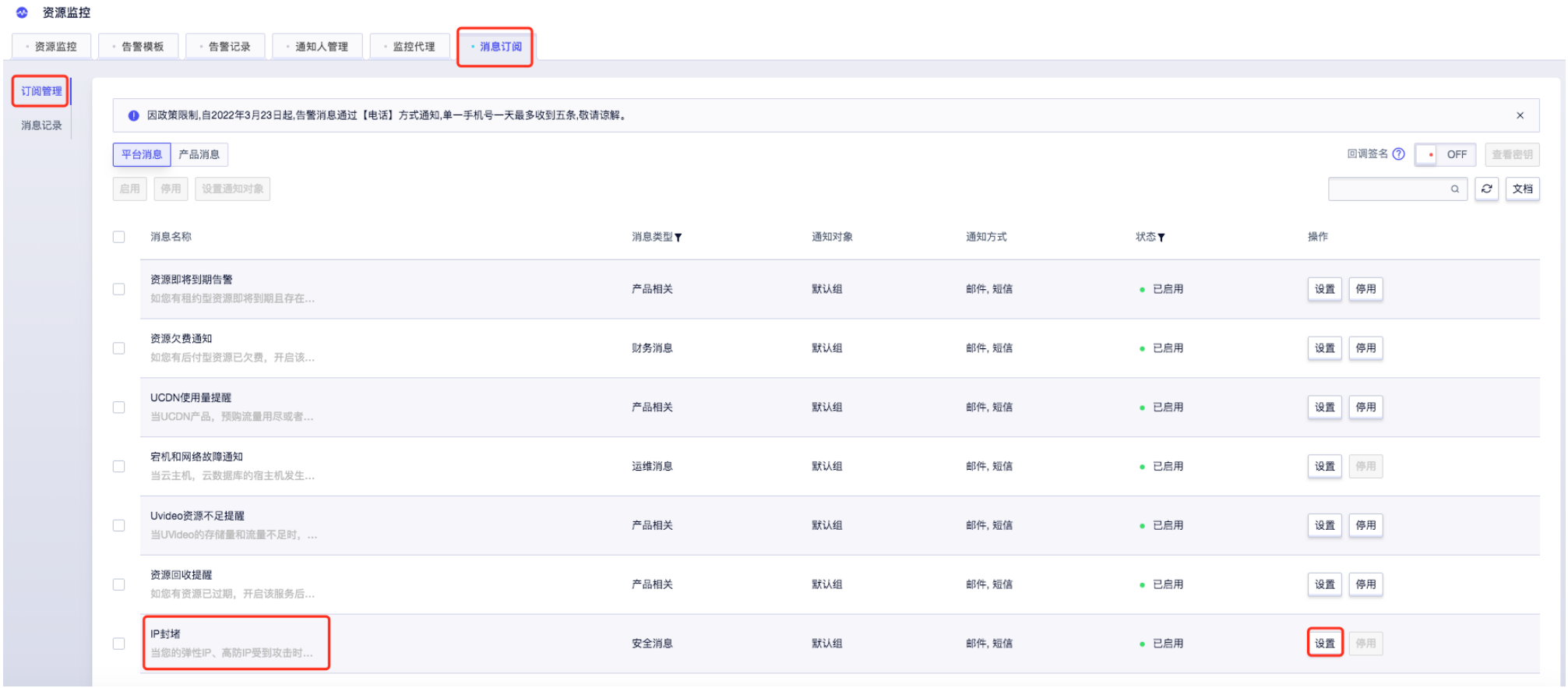
注：实际的防护阈值可能会根据您所购买的带宽及机房出口带宽有所调整。

封堵清洗告警回调说明

当外网IP被封堵或者清洗时都会产生相应的告警信息，您可通过配置回调来订阅这两类告警信息。

封堵告警回调配置

1. 在 资源监控UMon –> 消息订阅 –> 订阅管理 –> IP封堵，点击右边的设置按钮



2. 在弹出的订阅设置框中勾上回调按钮，填入对应的回调地址

3. **回调接口说明参考 https://docs.ucloud.cn/umon/guide/webhook 消息内容格式如下：**


```
{
"Title": "IP封堵告警",
"SessionId": "4356840c-661b-44e2-8449-e5674209069e",
"TopicName": "ip_blocking",
"TopicNameCn": "IP封堵",
"CustomInfo": "{\"EIPId\":\"eip-mcxxxx38\",\"Ip\":\"x.x.x.x\",\"PeakBps\":\"2032.00\",\"ProjectId\":\"org-4g5111\",\"Region\":10010,\"RegionZh\":\"迪拜
\",\"Time\":\"2023-08-08 17:15:40\",\"Type\":\"StartBlocking\"}",
"Content": "xxx(告警内容)",
"Signature": "xxx"
}
```


备注：

以上字段仅供参考，以实际告警为准。

其中PeakBps和PeakPps的单位分别为Mbps和Kpps。

清洗告警回调配置

1. 在 资源监控UMon -> 消息订阅 -> 订阅管理 -> IP流量清洗告警，点击右边的设置按钮

2. 在弹出的订阅设置框中勾上回调按钮，填入对应的回调地址

3. 回调接口说明参考 https://docs.ucloud.cn/umon/guide/webhook 消息内容格式如下:(主要关注CustomInfo字段,其他字段以实际告警为准,其中PeakBps和PeakPps的单位分别为Mbps和Kpps)


```
{
"Title": "IP清洗告警",
"SessionId": "6b54fb76-d304-4699-ac16-ae87a0b6a74b",
"TopicName": "ip_clean_alarm",
"TopicNameCn": "IP流量清洗告警",
"CustomInfo": "{\"CleanType\":\"UDP_FRAG|R_CLDAP_FLOOD\",\"EIPId\":\"eip-
mcxxxx38\",\"Ip\":\"x.x.x.x\",\"PeakBps\":\"2032.72\",\"PeakPps\":\"226.89\",\"ProjectId\":\"org-4g5111\",\"Region\":10010,\"RegionZh\":\"迪拜
\",\"Time\":\"2023-08-08 17:15:38\",\"Type\":\"StartClean\"}",
"Content": " xxx(告警内容)",
"Signature": ""
}
```


{
"Title": "IP撤出清洗告警",
"SessionId": "6b54fb76-d304-4699-ac16-ae87a0b6a74b",
"TopicName": "ip_clean_alarm",
"TopicNameCn": "IP流量清洗告警",
"CustomInfo": "{\"CleanType\":\"UDP_FRAG|R_CLDAP_FLOOD\",\"EIPId\":\"eip-mcxxxx38\",\"Ip\":\"x.x.x.x\",\"PeakBps\":\"2032.72\",\"PeakPps\":\"226.89\",\"ProjectId\":\"org-4g5111\",\"Region\":10010,\"RegionZh\":\"迪拜\",\"Time\":\"2023-08-08 17:15:38\",\"Type\":\"StopClean\"}",
"Content": " xxx(告警内容)",
"Signature": ""
}

备注：

以上字段仅供参考，以实际告警为准。

其中PeakBps和PeakPps的单位分别为Mbps和Kpps。

主机对外DDoS自查

云主机存在漏洞会被黑客攻击后会作为DDoS向外攻击的宿主机，此内容协助您对云主机进行安全自查，避免出现安全隐患。

PHPMyAdmin

检查

- 是否安装
- 有没有删除/install/目录
- 是否没密码

修复

- mysql增加强密码
- 限制phpmyadmin的访问

Tomcat

检查

- 是否存在管理页面/manager/
- 后台是否使用弱口令，常见弱口令admin/admin、tomcat/tomcat、manager/manager

修复

- 不需要使用tomcat管理页面的话就删掉，需要使用的话就增强密码，具体设置在 conftomact_user.xml里面增加密码强度

其它常见开源CMS

检查

- 是否使用常见开源cms，dede，其版本是否存在漏洞。
- 后台是否使用弱密码

修复

- 升级到最新版
- 增强密码

structs2

检查

- 是否使用structs2框架
- 查询该版本的structs2框架是否存在漏洞

修复

- 管理后台做访问控制

- 增强密码

编辑器

检查

- 检查是否安装fckeditor
- 是否允许任何人访问
- 是否存在如下页面 fckeditor/editor/filemanager/connectors/test.html fckeditor/editor/filemanager/*

修复

- 限制fckeditor的访问
- 删除测试test测试页面

常见页面

- ewebeditor是否安装，是否默认密码，admin，admin888
- ewebeditor本身问题众多，建议能不用就不用
- 修复：增加强密码，ewebeditor的数据库可以被下载，弱密码没用

ftp暴力破解

检查

- ftp是否弱密码，可查看/var/log/vsftpd.log是否有异常登录

修复

- 增强密码

ssh弱口令

检查

- last命令检查是否有异常登录
- 查看/var/log/secure，确认是否有暴力破解，暴力破解是否成功

修复

- 增强密码

ElasticSearch

检查

- ElasticSearch 1.2及以下版本默认开启动态脚本执行，导致被黑

修复

修改配置文件，添加"script.disable_dynamic: true"，来禁用动态脚本

- 关闭动态脚本执行
- 做访问控制

SQL Server

检查

- sqlserver是否允许外连,密码强度是否足够

修复

- 增强密码
- 做访问控制

Windows远程桌面

检查

- 是否有弱密码

修复

- 增强密码

mysql、nagios、zabbix、phpmyadmin、cacti、redis等开源软件

检查

- 如果有使用这些开源软件，检查版本
- 通过官方确认该版本是否存在漏洞
- 这些开源软件的系统账号是否有弱口令、空口令

修复

- 升级到最新版
- 做访问控制
- 增强口令
- 这些服务类账号如果不需要ssh登陆系统，设置登陆shell为/sbin/nologin

FAQ

1. 黑洞以后可以提前解封么?

可以申请提前解封,但是如果持续被攻击,或者被攻击多次,则可能将无法提前解封了。

2. 如果想提升主机的安全性怎么办?

推荐使用主机入侵检测产品,目前免费安装和使用。

3. EIP封堵后，如何看攻击情况?

在 云安全中心->安全事件->网络攻击 中可以看到。

4. 机房是否有免费清洗服务?

有,基础防护为免费服务,默认开通,机房免费清洗能力参考机房清洗能力。

5. EIP清洗触发条件是什么?

EIP的入向包量超过清洗阈值则会进行清洗,清洗后会对异常流量进行过滤,机房默认清洗阈值参考机房清洗能力。

6. EIP封堵触发条件是什么?

EIP的入向流量超过封堵阈值则会进行封堵,封堵后入向流量无法到达云主机,机房默认封堵阈值参考UCloud黑洞策略。

7. EIP封堵后，为何还有少数区域仍可ping通?

因为封堵是在运营商骨干网实施的,会存在封堵后城域网内的机器仍能ping通的情况。

8. EIP的封堵阈值是否可以调高?

可以根据购买带宽情况和机房带宽情况进行适当调高,具体请联系技术支持或者客户经理。

9. EIP的清洗阈值是否可以调高?

可以在控制台可自助调高,最高支持调至500kpps,如有更高的包量要求,请联系技术支持或者客户经理。

10. EIP封堵后有何对策?

如果是攻击，推荐购买高防进行防御。如果不是攻击，可申请解封并调高封堵阈值。

11. 被攻击后如何报案?

可向当地网监部门进行报案，并根据网监部门要求提供相关信息。然后网监部门判断是否符合立案标准，并进入网监处理流程。正式立案后，UCloud会配合网监部门接口人提供攻击取证(流量图、攻击事件、抓包信息等)。

12. 云主机被小流量攻击了，怎么不进行防护?

由于基础防护是公共的DDoS防护服务，不对小流量攻击（小于清洗阈值）进行防护。建议优化服务器性能、安装主机入侵检测产品来应对小流量攻击。

13. EIP封堵后，为什么云主机流量监控没看到大流量数据?

因为DDoS防护的流量监控系统是部署在机房网络边界(粒度为2秒)，位于云主机上层，所以一般情况下，DDoS防护的流量监控数据会大于在云主机上看到的流量数据。

14. 云主机还没开始使用，为什么会被DDoS攻击?

只要是业务连接外网通信，就有风险遭受DDOS攻击。

15. 云主机被攻击，对方攻击的是什么?

一般攻击针对的是IP或者是业务。

16. 为什么在云主机配置禁止udp流量后，仍会遭受到udp的攻击流量?

只要外网可以访问到IP，就可以发起DDoS攻击，而策略配置是在主机边界，并不能阻止攻击流量到达机房网络边界。

17. 没有受到攻击，为什么会触发清洗?

因为入流量超过清洗阈值时，就会触发流量清洗。如果不想被清洗，可以调高流量清洗阈值。

18. 正常下载业务，为什么会触发封堵?

因为下载时会存在流量的瞬时突发，而入流量超过封堵阈值时，就会触发封堵。如果不想被封堵，建议进行限速或者申请调高封堵阈值。

概览

产品概述

基本概念

内地高防为源站IP(包括非UCloud的弹性外网IP)提供DDoS攻击防护。

内地高防是通过高防IP来代理源站IP,并面向用户,既起到防护作用,又确保源站IP不直接暴露出去。

- **源站IP**: 源站服务器所使用的外网IP,也是被防护的IP地址
- **高防IP**: 与源站IP一一对应,用于代替源站IP来面向用户,使源站IP不直接暴露出去
- **回源IP**: 是高防数据中心代替用户去与源站服务器通信的若干个IP地址(高防数据中心会将用户的IP随机转换成某个回源IP,并由这个回源IP代替用户IP去与源站服务器通信)
- **高防线路**:

不同的线路代表机房所在的线路不同,攻击不管是电信的还是联通的或者教育网任何线路过来的都可以给引流到高防机房进行清洗。不同在于正常的访问如果是同线路则会更快,比如正常访问是电信线路的,经过电信高防,延迟会比经过联通高防更小。

使用场景

适用客户:所有需要网络安全防护的客户。(设备可以不在UCloud上面)

用户被黑客通过DDoS攻击以后,可以采用高防服务抗住攻击,过滤掉恶意的访问请求,让正常请求可以顺利访问网站或游戏。黑客发现攻不下的时候自然就会知难而退了。

名词解释

DDoS

分布式拒绝服务(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。

高防线路

指高防机房采用的IDC运营商，比如中国电信或者中国联通。购买高防产品后，用户的服务器采用的IDC运营商如果和高防线路一致，则网络访问的延时将比不一致的情况更小。

BGP机房

BGP机房将保证不同网络运营商（比如电信、联通或者移动）用户的高速访问。BGP的最主要功能在于控制路由的传播和选择最好的路由，使用BGP协议互联后，网络运营商的所有骨干路 由设备将会判断到IDC机房IP段的最佳路由，以保证不同网络运营商用户的高速访问。

产品优势

高防（UADS）是UCloud面向所有用户推出的抗DDoS攻击的增值付费产品，该产品能够为用户提供如下优质服务：

复杂穿墙攻击防护

在攻防中往往不仅仅是简单的攻击，通过机器可以直接过滤，为了保证防护效果，高防机房采用自有专用设备，支持防护各类ACK、SYN、连接耗尽、CC透过防火墙。此外通过以下三点达到防护复杂穿墙攻击的效果：

- 定制化专属策略
- 7X24专家支持
- 可选水印防护

超大流量防护

中国大陆（内地）最大可为单用户提供峰值1.2Tbps的DDoS攻击防护能力，港澳台区域支持高达400Gbps的防护能力，可轻松抵御大流量DDoS攻击。

隐藏用户服务资源

高防IP可对用户站点进行更换并隐藏。使用高防IP作为源站的前置，使攻击者无法找到用户的网络资源，增加源站安全性。

弹性防护

提供“保底防护+弹性防护”相结合的计费方式，为用户降低日常安全费用，需要时可在控制台自助按需调整弹性防护值，秒级生效，且无需新增任何设备。同时，业务上也无需进行任何调整，整个过程服务无中断。

当攻击流量超过保底防护值时，仍为用户继续防护，保障业务不中断，按当天实际攻击量收费。

主要功能

功能点	功能描述
基本防护	畸形数据包拦截 syn flood、ack flood、udp flood、icmp flood等防护 连接耗尽攻击、http get/post flood等防护 dns request/response flood等防护
DNS检防	根据DNS查询/应答报文的NAME、TYPE、CLASS特征进行检测防护
自动检防	根据算法进行基线学习、行为建模等自动检测与防护
深度防护	根据源/目的IP、协议、端口、包长、标记为、包内容等条件进行深度匹配防护
访问控制	根据源/目的IP、协议、端口配置三四层黑白名单、限速； 根据源/目的IP、协议、端口、域名、URL、User-Agent等条件配置七层黑白名单、限速
监控功能	流量监控、包量监控、事件监控等
高可用功能	主备部署、负载均衡等
攻击取证	根据源/目的IP、协议、端口等条件实时抓包取证
一键切换	一键关闭或开启防护

高防机房差异说明

IP配额

高防机房	免费IP配额	收费IP配额
扬州	2	0
枣庄	2	0
石家庄	2	0

UDP协议封堵

高防机房	电信	联通	移动
扬州	运营商封堵	运营商封堵	运营商封堵
枣庄	否	否	否
石家庄	机房封堵	机房封堵	机房封堵

说明:

运营商封堵表示流量在运营商骨干网中直接被丢弃。流量无法到达高防机房，机房检测系统统计不到流量。

机房封堵表示流量达到高防机房后由防护策略丢弃。流量会被机房的检测系统统计到。

转发模式

高防机房	IP转发	TCP端口转发
扬州	支持	支持
枣庄	支持	支持
石家庄	支持	不支持

回源模式

高防机房	IP回源	域名回源
扬州	支持	不支持
枣庄	支持	支持
石家庄	支持	不支持

网站业务访问模式

高防机房	IP访问	域名访问
扬州	不支持	支持
枣庄	支持	支持
石家庄	支持	支持

重要提示:扬州机房HTTPS业务访问要求

1.SNI携带要求

客户端访问扬州机房HTTPS网站业务时,必须携带SNI(Server Name Indication)扩展信息。若未提供SNI,请求将被判定为IP访问并触发拦截机制。

2.技术背景说明

SNI协议于2004年提出,通过TLS扩展实现多域名服务共享同一IP的能力。当前所有主流浏览器(Chrome/Firefox/Safari等)、Web服务器(Nginx/Apache等)及测试工具均已原生支持SNI规范

架构和原理简介

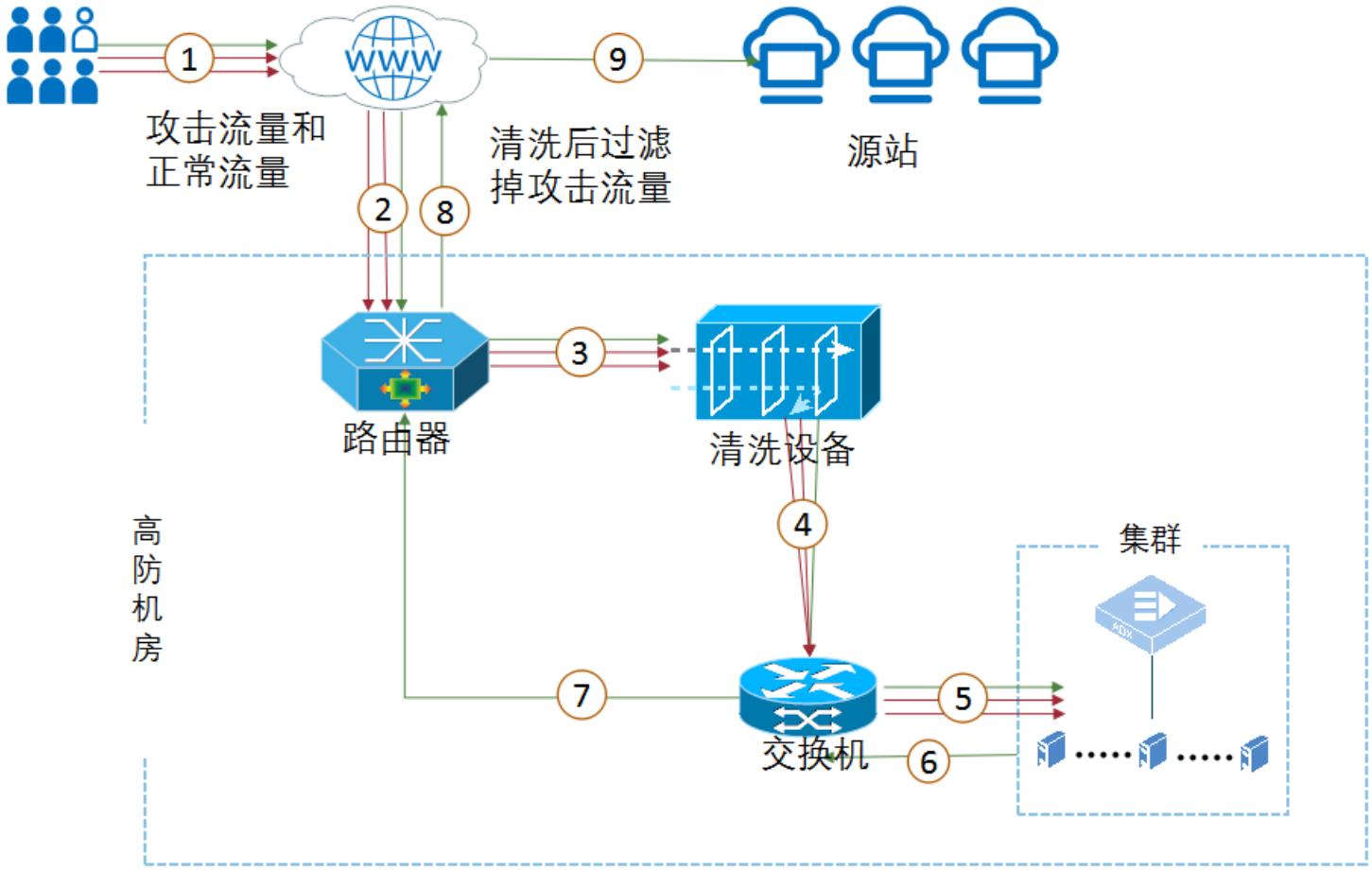
DDoS攻击简介

拒绝服务攻击（英语：Denial of Service Attack，缩写：DoS）亦称洪水攻击，是一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其对目标客户不可用。

分布式拒绝服务攻击（英语：Distributed Denial of Service attack，缩写：DDoS），是黑客使用网络上两个或以上被攻陷的电脑作为“僵尸”向特定的目标发动拒绝服务攻击。

高防原理简介

高防服务是针对互联网服务器（包括非UCloud云主机）在遭受大流量的DDoS攻击后导致服务不可用的情况，推出的一款增值防护服务。该服务可为客户提供DDoS、CC等攻击的防护能力，可防护SYN Flood、ACK Flood、UDP Flood、ICMP Flood、连接耗尽攻击、DNS Request/Response Flood、HTTP Get/Post Flood等3到7层的攻击。



正常的时候用户直接访问源站。

客户通过配置高防服务后，把业务切入到高防（有域名的业务，把域名解析到高防的IP或CNAME；无域名的业务，把业务IP换成高防IP），之后所有公网流量都会先到高防机房，高防机房会将攻击流量进行清洗过滤，并将正常流量转发给源站IP，从而确保源站提供稳定正常的服务。

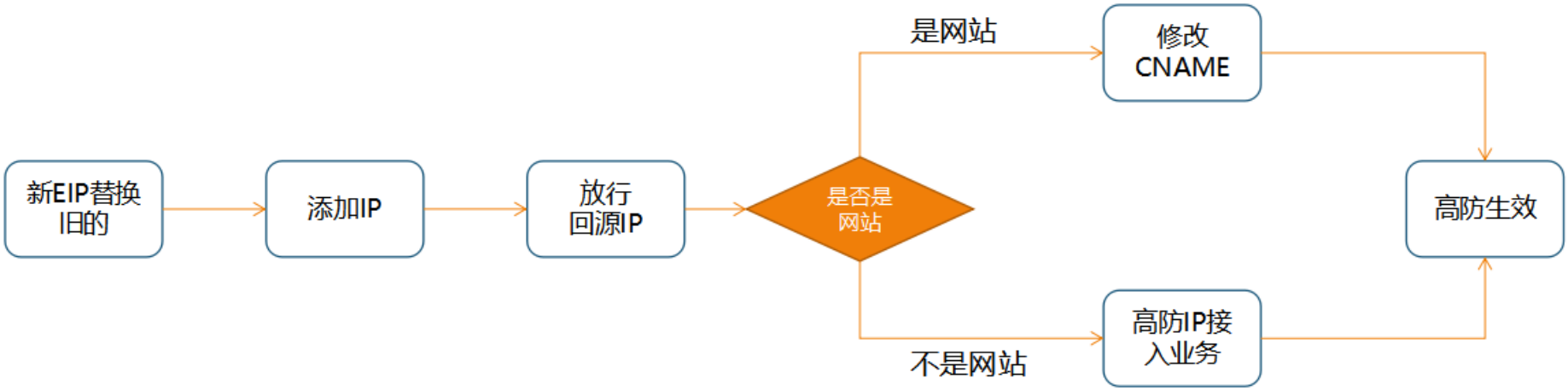
备注：

用户指访问客户业务的使用者。

客户指购买高防的使用者。

快速上手

内地高防



1. 使用新IP替换旧IP

如果IP已经被封，购买新的源站IP替换旧的源站IP。

如果IP没有被封，建议申请新的源站IP替换旧的源站IP，旧的源站IP可能因攻击而被封堵或已经暴露，存在被直接攻击的风险。

注意：

被封的IP一定要使用新的IP替换被封的IP后才能正常使用高防。

2. 添加IP，开通服务

在【安全防护】-【DDoS攻击防护 UDDoS】-【高防】页面，点击“详情”-“IP管理”-“添加IP”。注意 下图适用石家庄**BGP**。扬州**BGP**配置请见操作指南-添加转发规则。

高防线路： 指将采用哪种线路的高防机房，有以下两方面影响：(1) 相同线路的高防机房弹性收费的时候仅取IP攻击峰值最高的进行收费；(2) 假设高防机房采用的是电信线路，则回源时是同线路，延迟较小。如果源站是联通，则延迟比源站是电信的延迟要大一些。

源站IP： 填写需要防护的源站IP地址。

备注说明： 填写备注说明，可以为空。

3. 防火墙或相关安全防护软件上对所有回源IP放行

如果有安全软件或者硬件限制访问真实源站的来源IP，则需要将回源IP放行。

4.1 修改CNAME记录

如果是网站业务，并且具有域名，可以通过修改cname的方式进行高防防护。

首先获取高防的cname（添加源站IP后会在列表中给出），如下图所示：

到DNS服务商处删除A记录，添加CNAME记录。

说明：上一步添加IP后，每条记录会生成对应的CNAME值，需要去修改对应网站域名的DNS解析为CNAME解析方式。

4.2 使用高防IP接入业务

如果是非网站业务，或者不具有域名。一般需要修改客户端配置文件中对应的源站IP或者对应域名的解析IP。将原来解析到源站IP的地方填写为高防IP。

注意：

内地高防到期后，我们将为您保留配置一天，请及时重新购买并开启服务，或者确保不再使用高防IP接入相关业务，否则服务到期一天后配置将自动回收，会导致业务中断。

产品价格

计费方式

付费方式： 基础防护（预付费保底）+弹性按天后付费，如果弹性上限=保底，则无按天后付费

计费标准： 以需要防护的流量速率峰值、防护时长形成一个计费标准。

计费周期： 可按月、年计费。

基础防护（预付费保底）价格

基础防护保底值	BGP（元/月）
防护峰值30Gbps	15000
防护峰值40Gbps	18800
防护峰值50Gbps	22500
防护峰值60Gbps	26300
防护峰值70Gbps	30000
防护峰值80Gbps	33750

防护峰值100Gbps	47500
防护峰值200Gbps	60000
防护峰值300Gbps	72500
防护峰值400Gbps	97500
防护峰值500Gbps	122500
防护峰值600Gbps	147500
防护峰值700Gbps	172500
防护峰值800Gbps	197500

弹性（后付费按天）价格

1）以当天入向流量速率峰值为结算标准，按如下规则计费：

- 当天入向流量速率峰值小于等于保底值，不另外收费；
- 当天入向流量速率峰值大于保底值且小于等于用户选择的最大限额，根据“后付费价格表”按天收费；
- 当天入向流量速率峰值大于用户选择的最大限额，会收取最大限额的费用，并且进行封堵。

2）最大防护限额支持随时调整。

3）服务到期后自动关闭弹性计费模式。

后付费价格表：

弹性峰值（Gbps）	价格（元/天）

31~40	4880
41~50	6400
51~60	7800
61~70	9200
71~80	10600
81~100	11800
101~200	14600
201~300	28000
301~400	40000
401~500	50000
501~600	60000
601~700	70000
701~800	80000
801~900	90000
901~1000	100000

业务带宽价格

业务带宽以10Mbps为梯度进行增加，不支持降级。价格为：¥1000.00/10Mbps/月。

1.1.添加高防（初次购买）

注意：

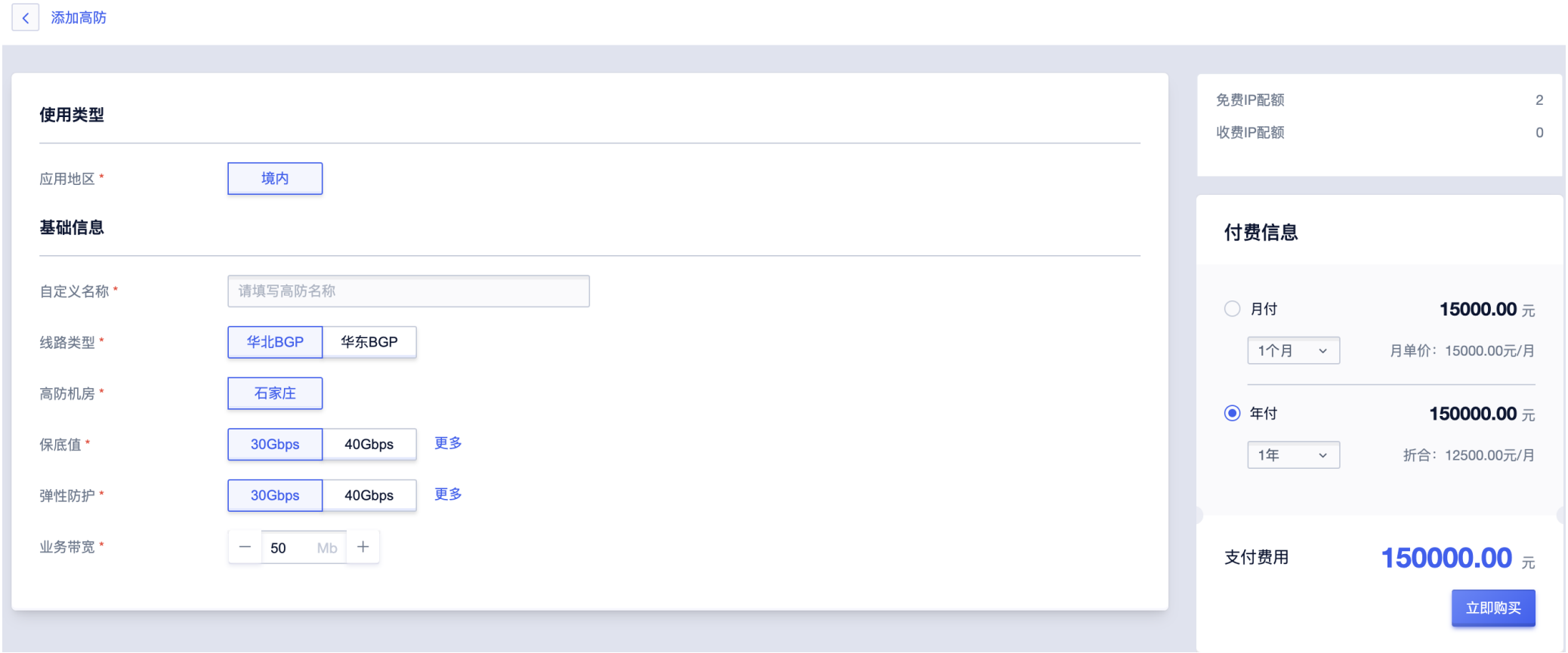
1. 源站的线路类型如果跟高防线路类型不一致可能会导致访问变慢的问题。

2. 成功购买高防以后不支持退费。产品有效期间，无法删除高防。需特别注意！

3. 高防不允许降级，因此如果选择的是30G的固定将无法在中途切到20G的弹性。

4. 自动续费是默认开启，如果不希望自动续费，请注意切换到关闭。

5. 如果需要防护的源站IP已经被封，请购买一个新的IP替换旧IP。



- **自定义名称:** 自定义内地高防的名称,可以是中英文、数字以及- _ .(最多32个字符)。
- **线路类型:** 高防机房的线路类型。「华北、华东」指高防机房所在区域,「BGP」指高防机房为三线BGP。
- **高防机房:**
  - **石家庄:** 不支持CC防护,每个套餐最多添加2个高防IP(2个免费,0个收费)。
  - **枣庄、扬州:** 支持CC防护,每个套餐最多添加2个高防IP(2个免费,0个收费)。

- **保底值:** 高防机房基础的防护峰值,攻击在保底值范围内的不再额外收费。
- **弹性防护:** 最大防护峰值,指超过保底值的攻击将按天收费,用户可以自己设定一个最大限额,当超过最大限额时将停止防护,封堵高防IP。
- **业务带宽:** 指从高防机房到源站服务器的带宽大小,50M以内不另外收费。

1.2.添加IP

机房类型	代理模式	特殊IP（可以屏蔽udp协议）	额外添加IP（非免费的高防IP）
石家庄BGP	支持	机房出口屏蔽UDP协议	不支持
扬州BGP	支持	运营商默认屏蔽UDP协议	不支持
枣庄BGP	支持	不支持	不支持

注意：

华东BGP高防默认屏蔽UDP协议，如果业务是采用UDP协议的，请使用枣庄机房。

添加IP

UCloud高防产品采用代理模式回源。代理模式指采用NAT代理转发的技术，由高防机房替代源站面向用户，用户访问网站先经过高防机房再由高防机房将访问发送至源站。

优势：允许添加非UCloud上的外网IP。

源站IP:填写需要防护的源站IP,如果源站IP已经暴露,建议更换一个新IP后再填写。

备注:自定义的说明文字。

1.3 添加转发规则

添加域名转发规则

购买高防->选择“华东BGP 扬州”线路高防->购买成功->详情->IP管理->管理。配置域名转发策略、CC防护规则.

添加IP或TCP转发规则

购买高防->选择对应线路高防->购买成功->详情->IP管理->添加IP->确定->高防IP添加成功。

点击规则管理----添加规则，可以配置高防IP的转发规则。

注意：

每个高防IP最多可配置50条转发规则，其中负载模式规则最多可配置10条

回源模式：

- IP地址：源站以IP形式。

- 域名：源站以域名形式，域名需能正常解析到IP地址。

  注意：只有枣庄BGP高防同时支持两种回源模式，其他高防只支持IP地址回源模式

负载模式：

- 不负载：高防IP+端口对应源站IP+端口进行转发。
  - IP地址回源：每条不负载转发规则最多可配置1个源站。
  - 域名回源：不支持配置不负载转发规则。
- 负载：将访问到高防IP+端口的流量在源站池中进行轮询负载。
  - IP地址回源：每条负载转发规则最多可配置31个源站。
  - 域名回源：每条负载转发规则最多可以配置8个源站域名。

源站IP端口： 真实业务服务器的IP和端口，支持非UCloud平台的主机。建议使用一个未曾使用过的源站IP接入高防，避免之前的源站IP暴露导致黑客绕过高防直接攻击源站。

高级设置： 如果不勾选只能配置高防IP和源站IP一对一的IP转发。勾选后可以配置高防IP和源站IP直接的TCP端口转发。

协议类型：

- IP：高防IP和源站IP进行一对一的IP转发。
- TCP：高防IP和源站IP进行TCP端口转发。

高防IP端口： 对外提供服务的高防IP和端口。

TOAID：源站TOA模块将根据此ID通过TCP option获取用户真实IP。UCloud提供的TOA模块默认值是200。

> TOA模块安装方式参考：https://docs.ucloud.cn/uantiddos/uads/faq/howtogetip

配置完后续的转发规则后。将业务切到高防IP或者将域名通过cname的方式解析的高防域名即可完成业务切换。

1.4 添加域名白名单

注意：

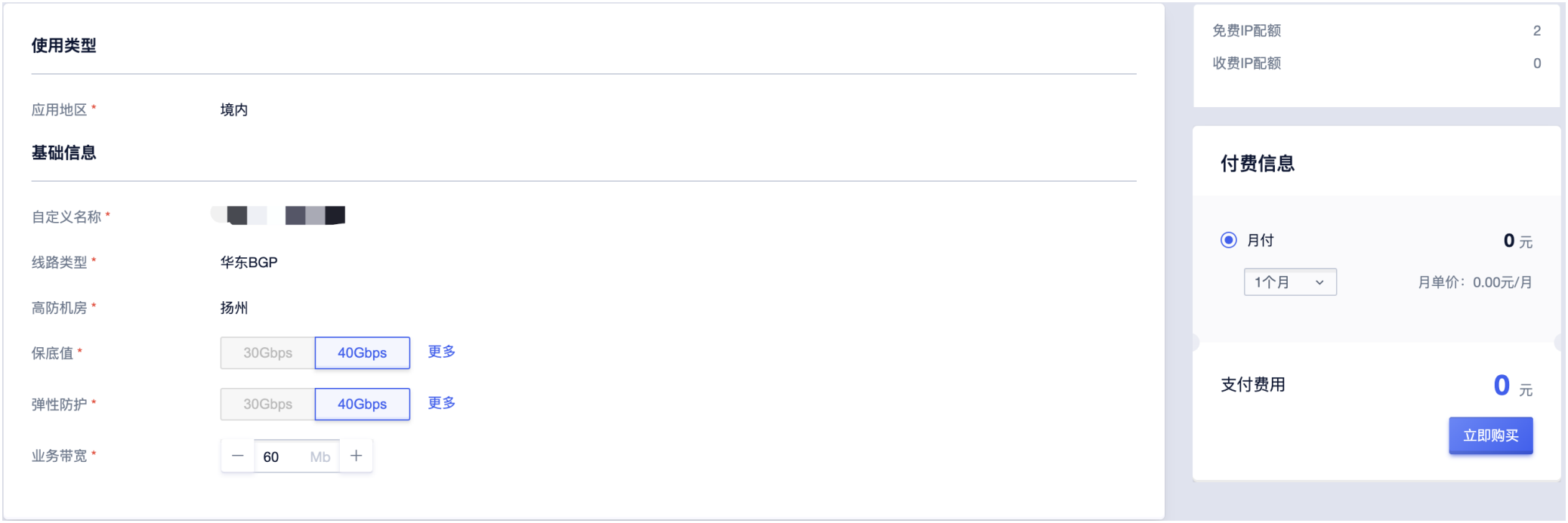
所有解析到高防IP上的主域名都需要添加。如将www.a.com和www.b.net解析到高防IP，需要添加a.com和b.net即可。

添加的域名必须为已经完成备案，否则将添加失败。

在初次完成购买高防后会提示将域名添加到白名单，后续需要增加新的域名：选择高防资源->详情->概览->域名白名单->添加：


基本信息
调整高防
名称
资源ID
usecure_ghp-jdmnvbqi3tc
高防路线
华东BGP
高防机房
扬州
业务带宽
60M
DDoS防护峰值
40-40Gbps 弹性
高防状态
开启
计费信息
续费
创建时间
2023-05-25 14:17:27
到期时间
2023-06-25 14:17:27
付费方式
19800/月 月付
免费IP配额
0/2
收费IP配额
0/0
自动续费
开启 关闭
监控信息
实时数据
历史数据
全部高防IP
您还未添加IP，未产生任何数据
域名白名单
新增
删除
域名
状态
创建时间
备注
操作
暂无数据

2.调整高防



注意：

1. 「保底值」仅允许升级，不允许降级。升级后需要补差价。
2. 「弹性防护」调整不收取额外的费用。
3. 「业务带宽」调整后需要补差价。
4. 「收费IP配额」调整后需要补差价。

3.监控视图


概览
IP管理
规则管理
基本信息
调整高防
名称
资源ID
usecure_ghp-jdmnvbqi3tc
高防路线
华东BGP
高防机房
扬州
业务带宽
60M
DDoS防护峰值
40-40Gbps 弹性
高防状态
开启
计费信息
续费
创建时间
2023-05-25 14:17:27
到期时间
2023-06-25 14:17:27
付费方式
19800/月 月付
免费IP配额
0/2
收费IP配额
0/0
自动续费
开启 关闭
监控信息
实时数据
历史数据
全部高防IP
您还未添加IP，未产生任何数据
域名白名单
新增
删除
域名
状态
创建时间
备注
操作
暂无数据

表1.基本信息

项目	描述
名称	添加高防的时候，自定义的名称
资源ID	高防的唯一标识，当出现问题，需要定位和排查的时候请提交资源ID
高防线路	购买时选择的高防机房
业务带宽	高防机房回源站的带宽大小
DDoS防护峰值	显示已购买的防护能力范围
高防状态	共有三种状态，「开启」、「过期」和「关闭」

表2.计费信息

项目	描述
创建时间	高防购买的时间
到期时间	高防到期的时间
付费方式	计费方式包括三种「按天」、「按月」和「按年」，其中「按天」需要跟客户经理单独申请开通
免费IP配额	套餐内可免费添加的高防IP数量
收费IP配额	套餐内可收费添加的高防IP数量
自动续费	显示自动续费的状态，包括「开启」和「关闭」，可以在高防状态是「开启」的时候任意开关

表3.监控信息

默认显示「全部高防IP」累计的数据，监控的指标包括：

- **入向流量：** 显示入向流量速率趋势图(单位: M/s)。入向指从「所有外网」到「高防机房」的流量。
- **实时数据：** 每30秒刷新一次，显示最近10分钟的数据
- **历史数据：** 按天，显示一整天的入向流量情况。最多支持显示30天的历史流量信息。按月，显示一整个月的历史流量信息。

表4.域名白名单

显示所有已经添加的域名白名单，处于白名单列表中的域名将不会被机房域名检测系统拦截：

- **成功：** 已成功添加到机房域名检测系统的域名。
- **失败：** 因域名未备案或者查询不到备案信息未添加到机房检测系统中的域名。

4. 到期说明

在服务到期前7天开始，我们将会通过短信、邮件的方式通知您服务即将到期，并提醒您续费。

内地高防到期后将为您保留高防IP 1天，如果1天后还没有续费，则将释放高防IP，不再提供高防服务。

5. 升降级高防服务

1. 升级

允许从低防护峰值套餐升级到高防护峰值套餐，比如从防护峰值20Gbps升级到30Gbps。

2. 降级

不允许 降级。也就是不允许从防护峰值30Gbps降为20Gbps。

3. 退费

购买成功后 **不允许** 退费。

4. 续费

资源过期后不支持续费，需要重新购买。

默认开启自动续费开关，允许手动配置关闭自动续费。

使用注意事项

1. 高防购买之后不退费
2. 域名必须是已经备案的。
3. 高防不允许降级，因此如果选择的是30G的保底将无法在中途切到20G。
4. 自动续费是默认开启的，如果不希望自动续费，请注意切换到关闭。
5. 如果需要防护的源站IP已经被封，请购买一个新的IP替换旧IP

常见问题

1. 高防服务是否可以试用，有什么规定或限制吗?

不支持试用。

2. 高防能抗多少层的攻击?

3-7层攻击。

3. 购买高防服务后，没有受到攻击收不收费?

如果您已经购买高防服务，无论您是否接入或受到攻击，我们将从购买时间开始计费。

4. 高防服务有好几个套餐，该如何选择?

高防服务的套餐是按DDoS防护峰值（Gbps）设定，建议选择防护峰值大于历史攻击流量峰值的套餐。

5. 如果遭遇的攻击流量峰值超过了已购买的高防服务防护峰值，该怎么办?

如果攻击流量峰值超过了购买的防护峰值，相应的高防IP也会触发自动封堵机制，一般会在封堵30分钟后自动解封。

为了不影响您的业务，您可以采用补差价升级防护套餐的方式来提高防护峰值、改善防护效果。升级生效后，如果被封堵的高防IP未自动解封，可向我们申请提前解封。

6. 没有备案的域名可以接入高防吗?

不行。高防服务会对接入的域名进行备案检查，如果域名未备案，会有被封堵高防IP的风险。

7. 使用高防服务会影响网站的备案吗?

不会。

8. 网站接入高防服务后，多长时间会生效?

网站接入高防服务的生效时间取决于DNS解析生效时间，在所有配置正确的情况下，一般10-60分钟生效。

9. 非80端口的网站是否可以接入高防服务?

可以。高防服务除了支持常用的80、443端口外，还支持一些自定义的端口，内地高防无需配置端口默认即可支持，如有问题可联系我们。

10. 非HTTP协议的服务是否可以接入高防服务?

内地高防不但支持HTTP/HTTPS的业务,还支持其他TCP/UDP等协议的业务。

11. 接入高防是否会和其他软防或硬防产生冲突?

接入高防后,需要在相应软防或硬防里将高防回源IP放行。(相应回源IP会在内地高防的界面上给出)

12. 使用高防服务后，为什么ping出来的IP不是源站IP?

开启高防服务后,ping网站域名显示的将是高防服务的IP,源站IP会被隐藏起来了,使攻击者无法直接攻击源站IP。(请注意源站IP不要泄露或直接对外提供服务)

13. 内地高防如何获取用户的真实IP地址?

内地高防获取真实IP地址需要通过toa模块实现,目前仅支持部分64位的linux系统,其他系统暂不支持。

64位的linux系统可运行"modprobe toa"尝试加载模块,成功后无需其他操作。

如提示未找到该模块,可按如下步骤进行手工编译与加载:

(1)下载对应版本的源码包,目前只有Centos 6.5和Centos 7的源码包供下载:

---

http://ddospcap.ufile.ucloud.cn/toa_centos6.5_v2.tar.gz

```
http://ddospcap.ufile.ucloud.cn/toa_centos7_v3.tar.gz
```

(2)编译与加载

```
yum install gcc

yum install kernel-headers

yum install kernel-devel

·#以上环境如已安装可忽略

tar -zxvf toa_centos6.5_v1.tar.gz 或 tar -zxvf toa_centos7_v3.tar.gz

cd toa

make

mv toa.ko /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko

insmod /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko
```

有问题请联系我们,如版本不符合,需升级内核再加载该模块;或者可直接使用UCloud 64位Centos 6.5/7系统的云主机,默认带有toa模块。

14. 使用高防服务后，如何使用FTP/SSH/3389远程桌面等服务?

可以直接使用源站IP来连接FTP、SSH及3389远程桌面。

15. 使用高防服务后，更换了源站IP需要在高防配置界面做更改吗?

更换源站IP时，需要在对应高防界面上同步变更配置。

16. 使用高防服务后，为什么建议更换一下源站IP?

因为在接入高防前，您的源站IP可能已经暴露，攻击者可以直接对该IP进行攻击，攻击流量将直接到达源站。

所以，在使用高防服务后，建议更换一下源站IP，使得新的源站IP被高防服务隐藏并防护着。

17. 可以临时关闭防护吗?

内地高防在页面上不支持关闭防护，可以自行将业务切出高防来关闭防护。

18. 如何切出高防服务?

不同业务切出方式不同，如站点业务可将域名解析会源站IP即可，其他业务只要保证不再使用高防IP接入业务即为切出高防。

如何获取用户的真实IP地址?

操作存在一定风险,建议备份环境,并在不影响业务的时候进行。

方式一:安装toa模块

内地高防获取真实IP地址, 可以在您的源站服务器上加载UCloud专有的内核模块,让应用直接获取到源IP,这时候,再去查看日志,就是访问者的真实IP了。

由于经过高防后,在日志中看到的访问者IP全部变为高防的回源IP。如果需要获取真实的客户端IP, 可以在您的源站服务器上加载UCloud专有的内核模块,让应用直接获取到源IP,这时候,再去查看日志,就是访问者的真实IP了。

Linux系统

64位的linux系统可运行"modprobe toa"尝试加载模块,成功后无需其他操作。

如提示未找到该模块,可按如下步骤进行手工编译与加载:

1. 查看当前内核版本号,确认依赖kernel-devel、kernel-headers是否安装以及版本号是否与内核一致(uname -r && rpm -qa |egrep 'kernel-devel|kernel-headers'):

- 若一致,跳过步骤2,进行toa模块的编译安装
- 若不一致,如下图:

```
[root@10-7-168-121 ~]# uname -r
3.10.0-693.11.6.el7.x86_64
[root@10-7-168-121 ~]# rpm -qa |egrep 'kernel-devel|kernel-headers'
kernel-devel-3.10.0-862.14.4.el7.x86_64
kernel-headers-3.10.0-862.14.4.el7.x86_64
```

需要卸载后进行步骤2操作(rpm -e --nodeps kernel-devel kernel-headers)

- 若未安装依赖,如下图:

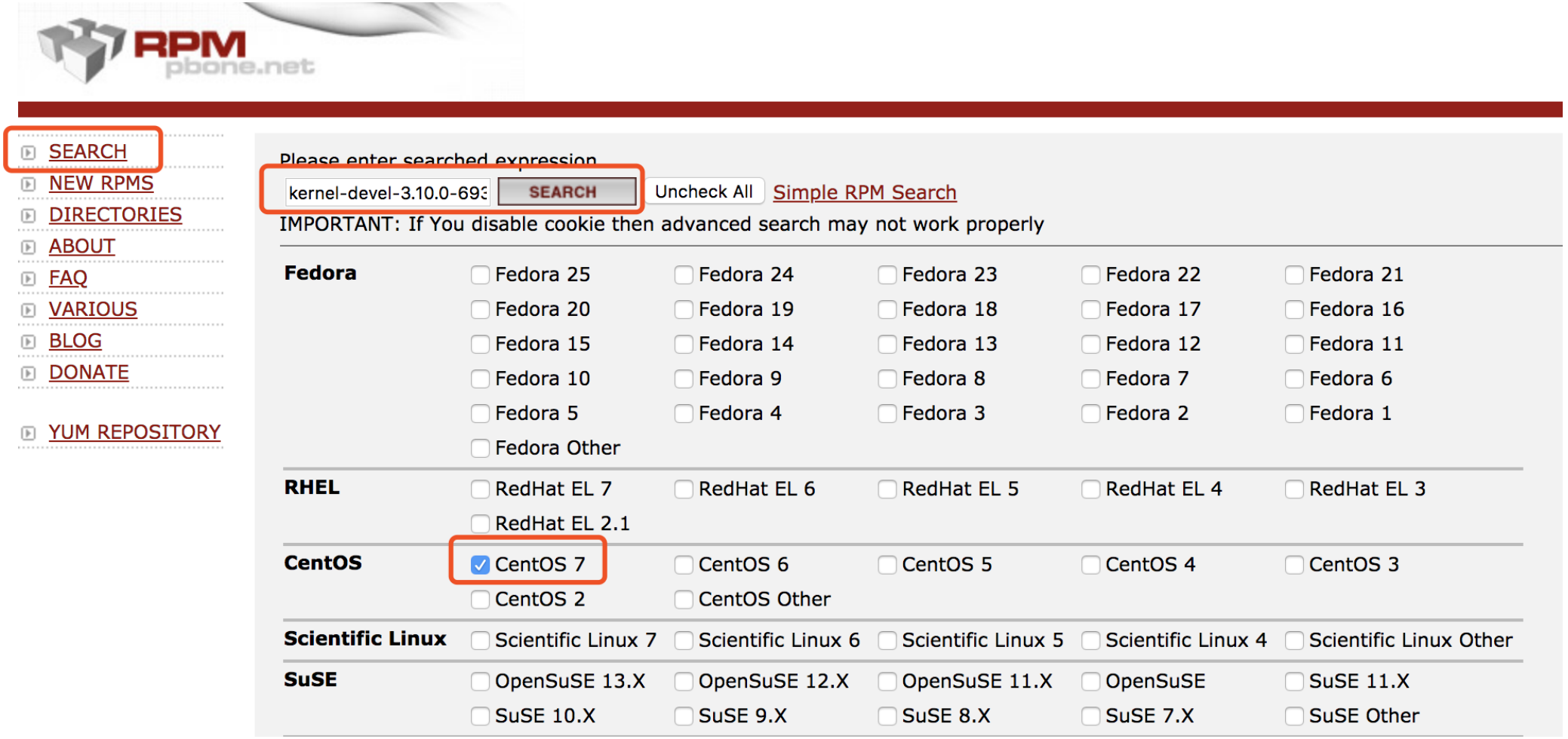
```
[root@10-7-168-121 ~]# uname -r
3.10.0-693.11.6.el7.x86_64
[root@10-7-168-121 ~]# rpm -qa |egrep 'kernel-devel|kernel-headers'
[root@10-7-168-121 ~]#
```

2. yum搜索是否有与当前内核版本对应的'kernel-devel、kernel-headers'包

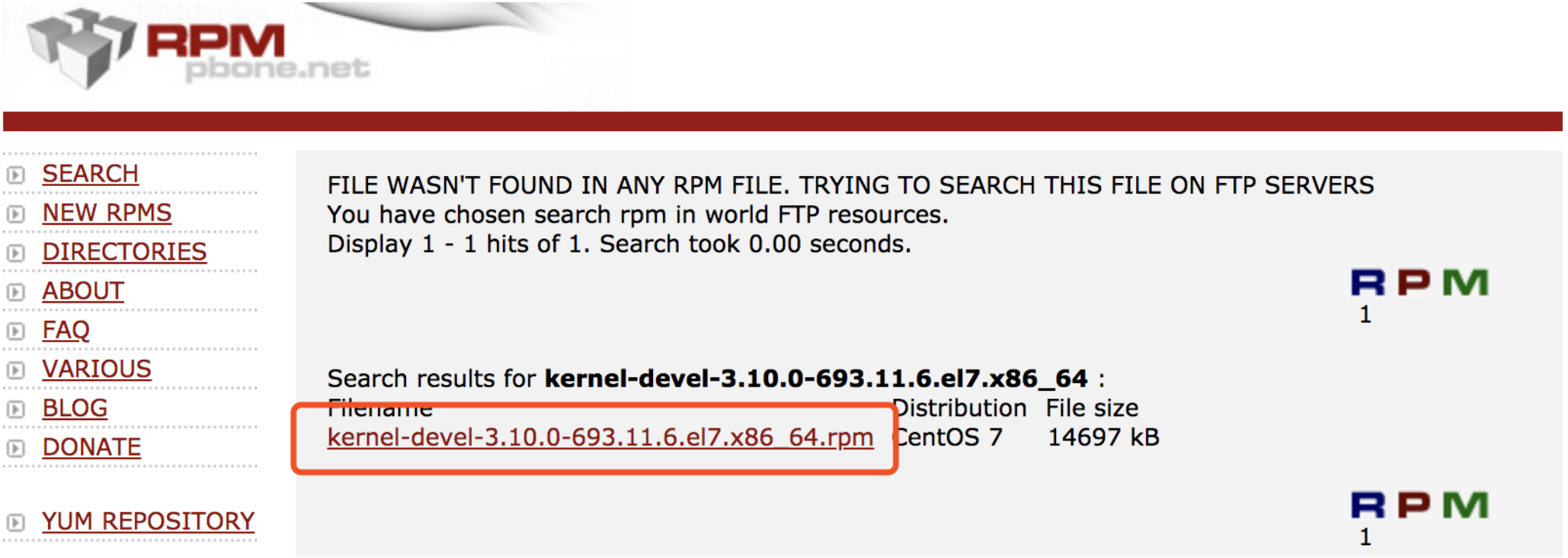
- 若有,则安装对用版本(yum install pkgname-version.x86_64)
- 若无,如下图

```
[root@10-7-168-121 ~]# yum list | egrep 'kernel-devel|kernel-headers'
kernel-devel.x86_64                     3.10.0-862.14.4.el7            updates
kernel-headers.x86_64                   3.10.0-862.14.4.el7            updates
```

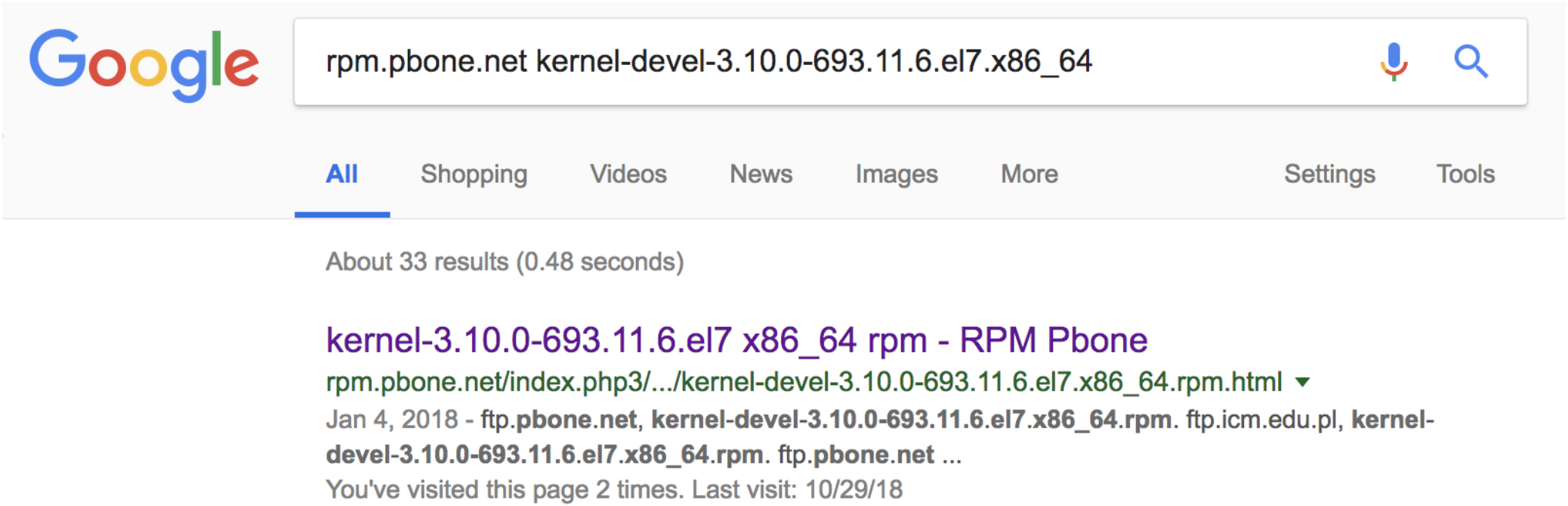
- 则打开网站 http://rpm.pbone.net ,点击左侧SEARCH标签,填入包名+版本号(如:kernel-devel-3.10.0-693.11.6.el7.x86_64),选择对应的系统发行版本(此处为CentOS7),点击搜索



搜索结果:



或使用谷歌用关键字rpm.pbone.net kernel-devel-3.10.0-693.11.6.el7.x86_64搜索



下载后rpm方式安装，kernel-headers的安装同理

```
[root@10-7-168-121 ~]# rpm -ivh kernel-devel-3.10.0-693.11.6.el7.x86_64.rpm
警告：kernel-devel-3.10.0-693.11.6.el7.x86_64.rpm: 头V4 DSA/SHA1 Signature, 密钥 ID 192a7d7d: NOKEY
准备中...                          ################################# [100%]
正在升级/安装...
   1:kernel-devel-3.10.0-693.11.6.el7 ################################# [100%]
[root@10-7-168-121 ~]# rpm -ivh kernel-headers-3.10.0-693.11.6.el7.x86_64.rpm
警告：kernel-headers-3.10.0-693.11.6.el7.x86_64.rpm: 头V4 DSA/SHA1 Signature, 密钥 ID 192a7d7d: NOKEY
准备中...                          ################################# [100%]
正在升级/安装...
   1:kernel-headers-3.10.0-693.11.6.el################################# [100%]
```

确认安装结果(uname -r && rpm -qa|egrep 'kernel-devel|kernel-headers')，如下图：

```
[root@10-7-168-121 ~]# uname -r && rpm -qa |egrep 'kernel-devel|kernel-headers'
3.10.0-693.11.6.el7.x86_64
kernel-devel-3.10.0-693.11.6.el7.x86_64
kernel-headers-3.10.0-693.11.6.el7.x86_64
```

3. 下载linux通用版的源码包，该版本支持Centos 6.9和Centos 7、ubuntu14.04等绝大多数的linux发行版，并已经适配了linux内核5.0：

- 国内：wget http://pathx.cn-bj.ufileos.com/linux_toa.tar.gz
- 海外：wget http://toa.hk.ufileos.com/linux_toa.tar.gz

4. 编译加载

```
yum install -y gcc
tar -zxvf linux_toa.tar.gz
```

```
cd linux_toa
make
mv toa.ko /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko
insmod /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko
```

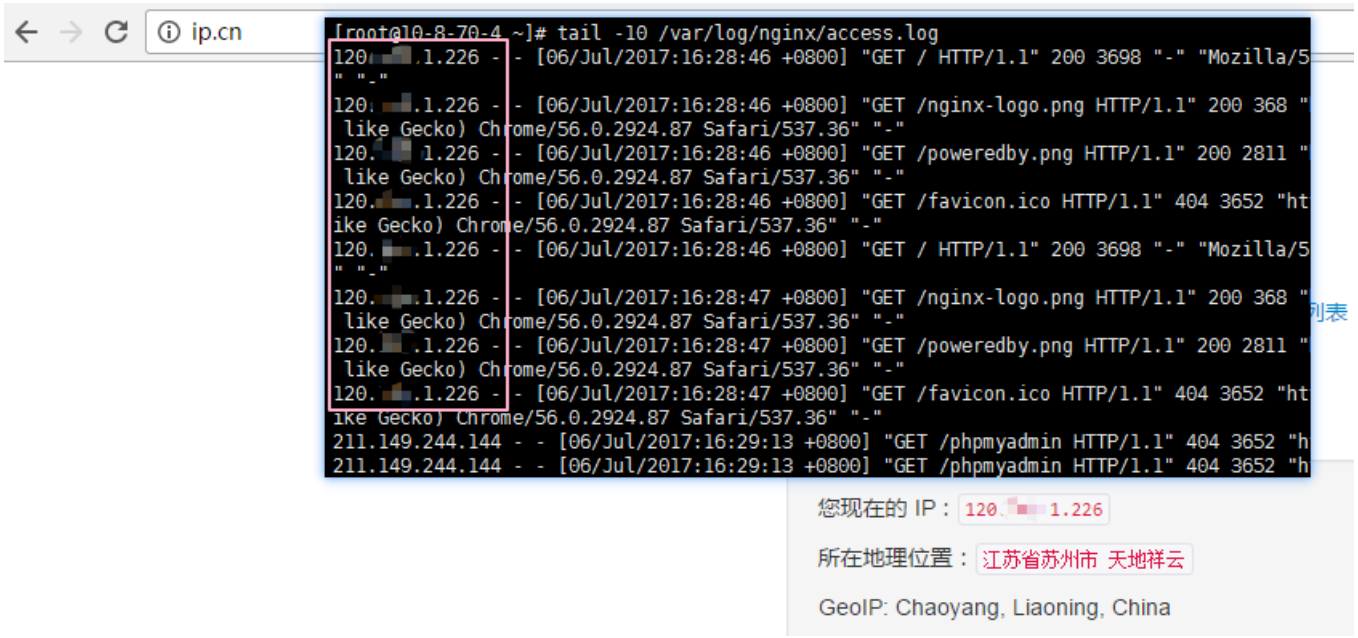
toa模块安装验证如下(lsmod |grep toa)：

```
[root@10-7-168-121 linux_toa]# lsmod |grep toa
toa                    12884  0
```

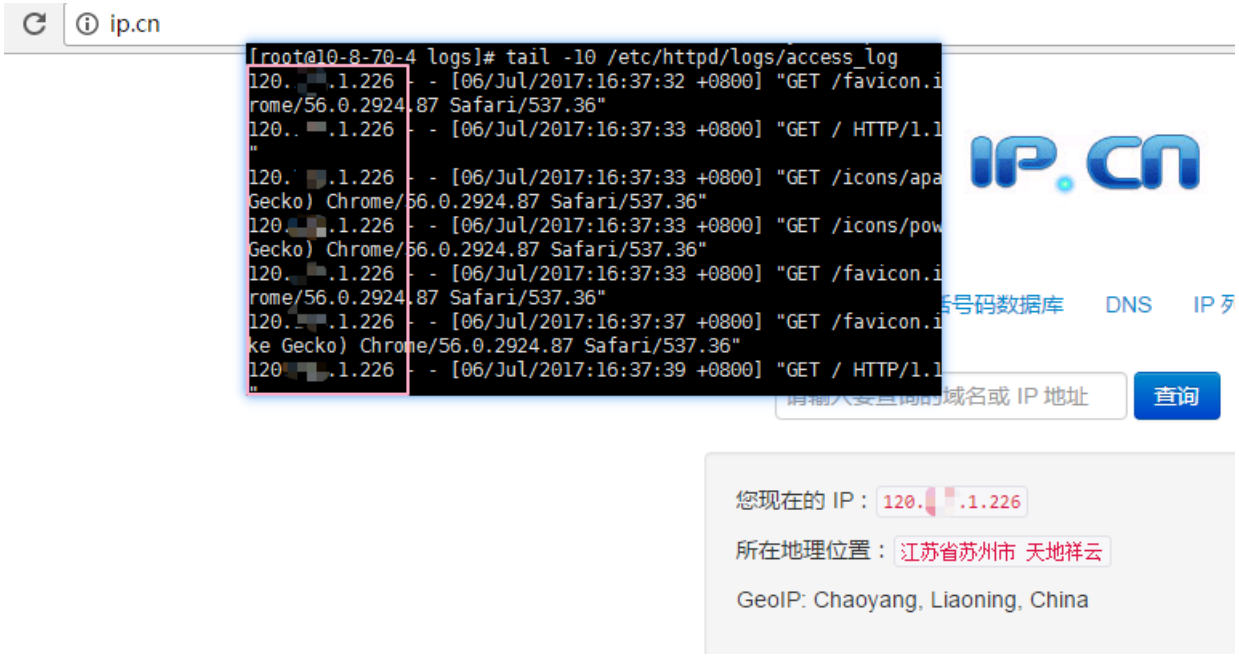
5. 添加开机模块自动加载

```
echo "insmod /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko">> /etc/rc.local
```

nginx环境下，直接在nginx 日志中查看真实访问者地址,日志路径：/var/log/nginx/access.log



apache环境下,直接在apache日志中查看真实访问者地址,日志路径:/etc/httpd/logs/access_log



- 其他web配置环境，采用同样方法在相关web 日志文件中检查即可

方式二：搭配UWAF一起使用

如果不满足方式一的要求，还可以购买UWAF搭配一起使用。将域名先解析到高防，源站指定为uwaf的IP。操作参见此处。

概览

- 产品简介
  - 产品概述
- 产品价格
- 操作指南
  - 1.创建高防
  - 2.调整高防
  - 3.监控视图
  - 4.到期说明
  - 5.升降级高防服务
- FAQ
  - 常见问题

产品概述

基本概念

海外高防是一款针对UCloud云内资源提供DDoS防御能力的增值安全产品，可以直接把防御能力加载到云产品上，部署简单，购买后只需将高防IP绑定到需要防护的云产品上即可生效，具有实时防御、低延时、高可靠、大防护的特点。

海外高防通过将高防IP在高防机房进行BGP宣告，将流量引流到高防机房通过基于 IP 画像、行为模式分析、AI 智能识别等防护算法，有效应对常见 DDoS 攻击行为。同时提供多样化、灵活的 DDoS 防护策略等对三层和四层流量型攻击进行防御，保障被防护用户在攻击持续状态下仍然可以对外提供服务。

产品功能

防护类型	描述
畸形报文攻击	支持TearDrop, IpLand, Smurf, Fraggle等攻击的清洗以及 IP/TCP/UDP畸形包过滤
泛洪攻击	针对 Udp Flood, SYN Flood, Icmp Flood, ACK Flood, FIN Flood, RST Flood等泛洪攻击进行防护
反射放大攻击	提供对Dns, Ntp, Ssdp, Memcached, Chargen, Cldap等反射攻击清洗

使用场景

海外高防适用于业务部署在UCloud云上的业务，能够满足大规模业务、对网络质量要求高的用户。

- 业务部署在UCloud 中国香港、中国台北、新加坡、东京、首尔、雅加达、曼谷、胡志明市、法兰克福、洛杉矶、华盛顿、伦敦机房
- 游戏、电商等容易受超大DDoS攻击防护场景
- 直播、视频等对网络访问质量要求较高的场景
- 新品发布、新游戏、促销等按需DDoS防护
- 公有基础DDoS防护无法满足，需更高防护能力的场景

IP配额

付费类型	免费配额	收费配额
年付	5	0
月付	5	0
周付	1	0

产品价格

计费方式

付费方式： 基础防护（预付费保底）+弹性按天后付费，如果弹性上限=保底，则无按天后付费

计费标准： 以需要防护的流量速率峰值、防护时长形成一个计费标准。

计费周期： 可按周、月、年计费。注意：按周计费，仅提供一个高防IP，且不支持调整！

海外高防基础防护（预付费保底）价格

基础防护保底值	保底价格（元/月）	保底价格（元/周）
防护峰值50Gbps	30000.00	10494.96
防护峰值100Gbps	58000.00	20294.40
防护峰值200Gbps	80000.00	27993.84

海外高防弹性（后付费按天）价格

1）以当天入向流量速率峰值为结算标准，按如下规则计费：

- 当天入向流量速率峰值小于等于保底值，不另外收费；
- 当天入向流量速率峰值大于保底值且小于等于用户选择的最大限额，根据“后付费价格表”按天收费；
- 当天入向流量速率峰值大于用户选择的最大限额，会收取最大限额的费用，并且进行封堵。

2）最大防护值支持随时升级，但不支持降级

后付费价格表：

弹性峰值（Gbps）	价格（元/天）
51~100	21800.00
101~150	28800.00
151~200	39800.00
201~300	43880.00
301~400	48800.00

1.海外高防

- **自定义名称:** 自定义海外高防的名称,可以是中英文、数字以及- _ .(最多32个字符)。
- **防护地域:** 指业务主机所在的机房。

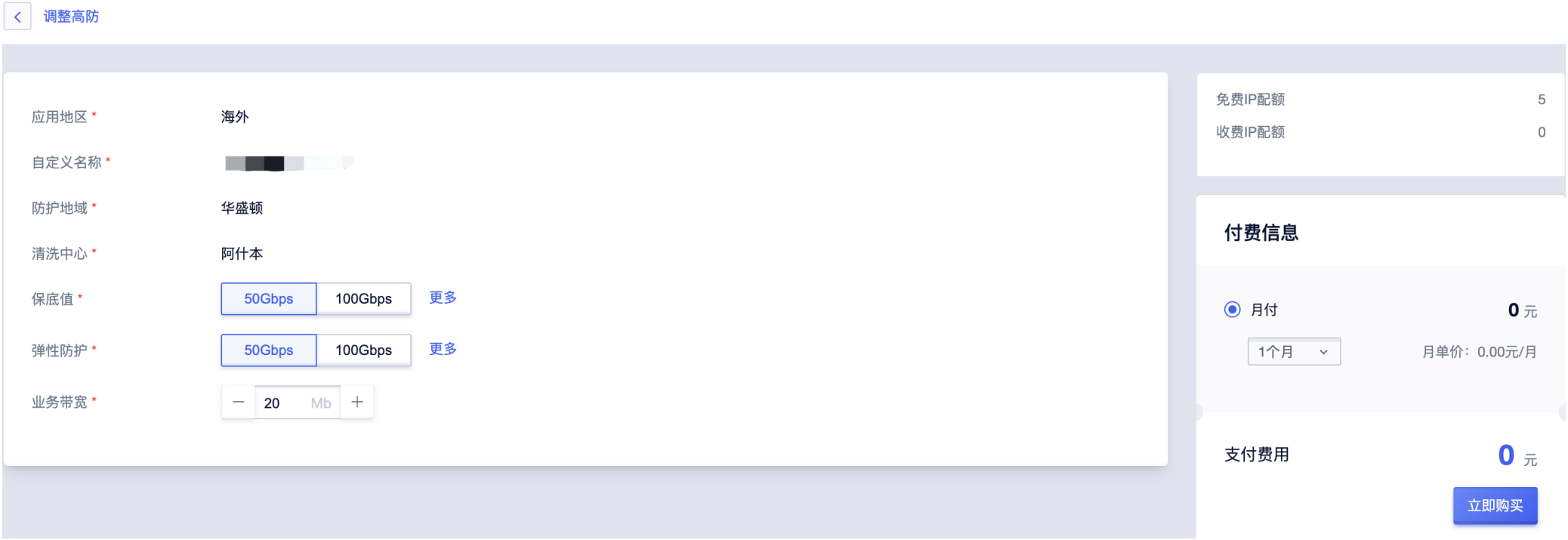
> 注意:
> 海外高防区分项目,创建时请确保在需要防护的业务主机项目下。海外高防仅支持对UCloud云内主机提供防护!

- **清洗中心:** 清洗中心所在位置。
- **保底值:** 高防机房基础的防护峰值，攻击在保底值范围内的不再额外收费。
- **弹性防护:** 弹性防护峰值，指超过保底值的攻击将按天收费，用户可以自己设定一个最大限额，当超过最大限额时将停止防护，封堵高防IP。
- **业务带宽:** 指通过高防IP发生的出入向带宽，20M以内不另外收费。

2.IP管理

- **添加IP:** 添加新的高防IP。
- **业务机房:** 创建高防时所选择的防护地域。
- **备注:** 添加IP的备注信息。
- **绑定|解绑操作:** 将高防IP从指定资源（Uhost|ULB等）绑定|解绑。具体操作步骤参见此处的绑定/解绑外网弹性IP。

2.调整高防



注意：

1. 「保底值」仅允许升级，不允许降级。升级后需要补差价。
2. 「业务带宽」只允许升级，不支持降级

3.监控视图

表1.基本信息

项目	描述
名称	添加高防的时候，自定义的名称
资源ID	高防的唯一标识，当出现问题，需要定位和排查的时候请提交资源ID
防护地域	针对此机房的业务进行防护
清洗中心	流量将被引流到清洗中心进行清洗
业务带宽	高防机房回源站的带宽大小
DDoS防护峰值	显示已购买的防护能力范围
高防状态	共有三种状态，「开启」、「过期」和「关闭」

表2.计费信息

项目	描述
创建时间	高防购买的时间
到期时间	高防到期的时间
付费方式	计费方式包括三种「按周」、「按月」和「按年」
免费IP配额	套餐内可免费添加的高防IP数量
收费IP配额	套餐内可收费添加的高防IP数量
自动续费	显示自动续费的状态，包括「开启」和「关闭」，可以在高防状态是「开启」的时候任意开关

表3.监控信息

默认显示「全部高防IP」累计的数据，监控的指标包括：

- **入向流量：** 显示入向流量速率趋势图（单位: Mbps）。入向指从「所有外网」到「高防机房」的流量。
- **实时数据：** 每30秒刷新一次，显示最近10分钟的数据
- **历史数据：** 按天，显示一整天的入向流量情况。最多支持显示30天的历史流量信息。按月，显示一整个月的历史流量信息。

4. 到期说明

在服务到期前7天开始，我们将会通过短信、邮件的方式通知您服务即将到期，并提醒您续费。

通用高防到期后将为您保留高防IP 1天，如果1天后还没有续费，则将释放高防IP，不再提供高防服务。

5. 升降级高防服务

1. 升级

允许从低防护峰值套餐升级到高防护峰值套餐，比如从防护峰值20Gbps升级到30Gbps。

2. 降级

不允许 降级。也就是不允许从防护峰值30Gbps降为20Gbps。

3. 退费

购买成功后 不允许 退费。

4. 续费

资源过期后不支持续费，需要重新购买。

默认开启自动续费开关，允许手动配置关闭自动续费。

常见问题

1. 海外高防服务是否可以试用，有什么规定或限制吗?

不支持试用，仅支持业务部署在UCloud 中国香港、中国台北、新加坡、东京、首尔、雅加达、曼谷、胡志明市、法兰克福、洛杉矶、华盛顿、伦敦机房。如果业务不在上述机房，需要搭建代理进行转发。

2. 海外高防能抗多少层的攻击?

可以有效防御3-4层攻击。具体支持类型如下:

防护类型	描述
畸形报文攻击	支持TearDrop, IpLand, Smurf, Fraggle等攻击的清洗以及 IP/TCP/UDP畸形包过滤
泛洪攻击	针对 Udp Flood, SYN Flood, Icmp Flood, ACK Flood, FIN Flood, RST Flood等泛洪攻击进行防护
反射放大攻击	提供对Dns, Ntp, Ssdp, Memcached, Chargen,Cldap等反射攻击清洗

3. 购买服务后，没有受到攻击收不收费?

如果您已经购买高防服务，无论您是否接入或受到攻击，我们将从购买时间开始计费。

4. 高防服务有好几个套餐，该如何选择?

高防服务的套餐是按DDoS防护峰值（Gbps）设定，建议选择防护峰值大于历史攻击流量峰值的套餐。

5. 如果遭遇的攻击流量峰值超过了已购买的高防服务防护峰值，该怎么办?

如果攻击流量峰值超过了购买的防护峰值，相应的高防IP也会触发自动封堵机制，一般会在封堵30分钟后自动解封。

为了不影响您的业务，您可以采用补差价升级防护套餐的方式来提高防护峰值、改善防护效果。升级生效后，如果被封堵的高防IP未自动解封，可向我们申请提前解封。

6. 没有备案的域名可以接入高防吗?

海外高防对接入域名没有限制。

7. 使用高防服务会影响网站的备案吗?

不会。

8. 网站接入高防服务后，多长时间会生效?

网站接入高防服务的生效时间取决于DNS解析生效时间，在所有配置正确的情况下，一般10-60分钟生效。

9. 非80端口的网站是否可以接入高防服务?

可以。高防服务除了支持常用的80、443端口外，还支持一些自定义的端口，通用高防无需配置端口默认即可支持，如有问题可联系我们。

10. 非HTTP协议的服务是否可以接入高防服务?

海外高防不但支持HTTP/HTTPS的业务，还支持其他TCP/UDP等协议的业务。

11. 接入海外高防是否会和其他软防或硬防产生冲突?

海外高防通过BGP路由宣告方式将流量牵引到高防机房进行清洗后通过专线将清洗后流量再路由到云机房，不影响服务器端部署的软防或则硬防。

12. 海外高防如何获取用户的真实IP地址?

海外高防是采用路由牵引方式进行防护，IP可以直接绑定到云主机使用。在云主机上看到的连接信息均为用户真实连接情况。

14. 使用高防服务后，如何使用FTP/SSH/3389远程桌面等服务?

可以直接使用高防IP来连接FTP、SSH及3389远程桌面。

15. 使用高防服务后，为什么建议更换一下源站IP?

因为在接入高防前，您的源站IP可能已经暴露，攻击者可以直接对该IP进行攻击，攻击流量将直接到达源站。

所以，在使用高防服务后，建议更换一下源站IP，使得新的源站IP被高防服务隐藏并防护着。

16. 可以临时关闭防护吗?

海外高防在页面上不支持关闭防护，可以自行将业务切出高防来关闭防护。

17. 如何切出高防服务?

不同业务切出方式不同，如站点业务可将域名解析回普通EIP即可，其他业务只要保证不再使用高防IP接入业务即为切出高防。

概览

产品概述

基本概念

清洗是一款自研产品，为UCloud的弹性外网IP提供DDoS攻击防护，经过多年的攻防经验积累，采用多种防御策略，支持防御网络层攻击，比如TCP类报文攻击、SYN Flood攻击、ACK Flood攻击等确保源站的正常访问。

清洗是为机房中所有的IP提供DDoS攻击防护，无需切换IP地址，每个机房的防护能力由机房上限带宽大小决定，最大可支持10G的防护。如果攻击超过10G，则建议使用高防。

使用场景

适用客户：购买了UCloud的外网弹性IP的客户。

采用清洗产品以后，能够对机房中所有的IP进行保护，当受到10G以下的DDoS攻击时，无需切换IP等待高防生效，直接抵御DDoS攻击，并且享受动态BGP带宽，延迟相比高防而言更低。

产品优势

秒级响应，防护无需等待

清洗产品使用时无需做任何操作，当有攻击发生的时候，秒级响应，实时防护。

丰富的安全防护策略

支持网络层攻击防护，各类常见攻击包括syn flood、ack flood、udp flood、icmp flood等。

超低延迟，告别卡顿

由于直接在IP上做抗DDoS攻击防护，不需要引流到高防机房，延迟是同类抗DDoS攻击产品中最低的。

自助调整防护阈值

根据自身业务特性，调整业务清洗阈值，防止误清洗。

机房清洗能力

地域	收费清洗上限
洛杉矶	10G
华盛顿	20G
法兰克福	20G
新加坡	10G
东京	15G
台北	20G
迪拜	5G
孟买	20G
圣保罗	10G
伦敦	10G
胡志明	15G
首尔	15G
曼谷	10G
雅加达	10G

机房免费清洗能力

地域名称	免费清洗上限
华北一	3Gbps
华北二	3Gbps
上海	2Gbps
广州	2Gbps
香港	2Gbps
洛杉矶	2Gbps
华盛顿	2Gbps
法兰克福	2Gbps
曼谷	2Gbps, 泰国国际线路1000Mbps
首尔	1Gbps
新加坡	2Gbps
东京	2Gbps
台北	2Gbps
迪拜	2Gbps

雅加达	1Gbps
孟买	2Gbps
圣保罗	2Gbps
伦敦	2Gbps
拉各斯	900Mbps
胡志明市	1Gbps
马尼拉	1Gbps

机房默认清洗阈值

地域名称	默认清洗阈值
华北一	syn:30wpps,ack:30wpps,icmp:2wpps,udp:30wpps dns:2wpps,ssdp:2wpps,ntp:2wpps,other:2wpps
华北二	syn:30wpps,ack:30wpps,icmp:2wpps,udp:30wpps dns:2wpps,ssdp:2wpps,ntp:2wpps,other:2wpps
上海	syn:20wpps,ack:20wpps,icmp:2wpps,udp:20wpps dns:2wpps,ssdp:2wpps,ntp:2wpps,other:2wpps
广州	syn:20wpps,ack:20wpps,icmp:2wpps,udp:20wpps dns:2wpps,ssdp:2wpps,ntp:2wpps,other:2wpps
香港	syn:20wpps,ack:20wpps,icmp:2wpps,udp:20wpps dns:2wpps,ssdp:2wpps,ntp:2wpps,other:2wpps
其他	syn:10wpps,ack:10wpps,icmp:2wpps,udp:10wpps dns:2wpps,ssdp:2wpps,ntp:2wpps,other:2wpps

架构和原理简介

清洗原理简介

清洗是针对UCloud服务器在遭受大流量的DDoS攻击后导致服务不可用的情况，推出的一款增值防护服务。

通过在本地机房安装清洗检测设备，配置防护策略提供抗DDoS攻击服务，可防护3到7层的攻击，包括SYN Flood攻击、SYN-ACK Flood 攻击、ACK Flood 攻击、FIN/RST Flood 攻击、DNS Request Flood 攻击等各类攻击。

快速上手

1. 进入清洗页面

选中 “全部产品”->"安全防护"->"DDoS攻击防护"

选择“清洗”

2. 添加清洗，开通服务

点击【清洗升级】按钮，在弹出框中选择需要防护IP所在的地域，确认付费后即可完成服务的开通。

注意：

1.同一个地域下的所有IP都在清洗的防护范围内，如果该地域新增加了IP，则将自动加入防护。

2.当某一IP的流量达到了上限清洗值，则将封堵IP。当所有IP同一时间受到的攻击流量达到机房防护上限的80%，将会依次封堵TOP1的IP。

3.当攻击大于上限清洗值，建议购买高防进行防护。

产品价格

境外

机房可以提供的清洗能力参见此处。

付费方式:预付费

上限清洗值	价格（元/月/地域）
5G	10000
10G	20000
15G	50000
20G	100000

升降级： 允许升级，不支持降级。可以预约到期后降级。

注意:

1、同一个地域下的所有IP都在清洗的防护范围内，如果该地域新增加了IP，则将延迟10分钟自动加入防护。

2、当某一IP的流量达到了上限清洗值，则将封堵IP。当所有IP同一时间受攻击流量达到机房总防护上限的80%，将会依次封堵流量TOP1的IP。

3、当攻击大于上限清洗值，建议购买高防进行防护。

4、由于攻击不可预测，建议长期使用，默认不支持删除。

5、台北支持20G以上清洗，但是需要更换IP，详细请咨询技术支持。

1. 添加清洗

进入“全部产品”->"DDoS攻击防护"->"清洗"

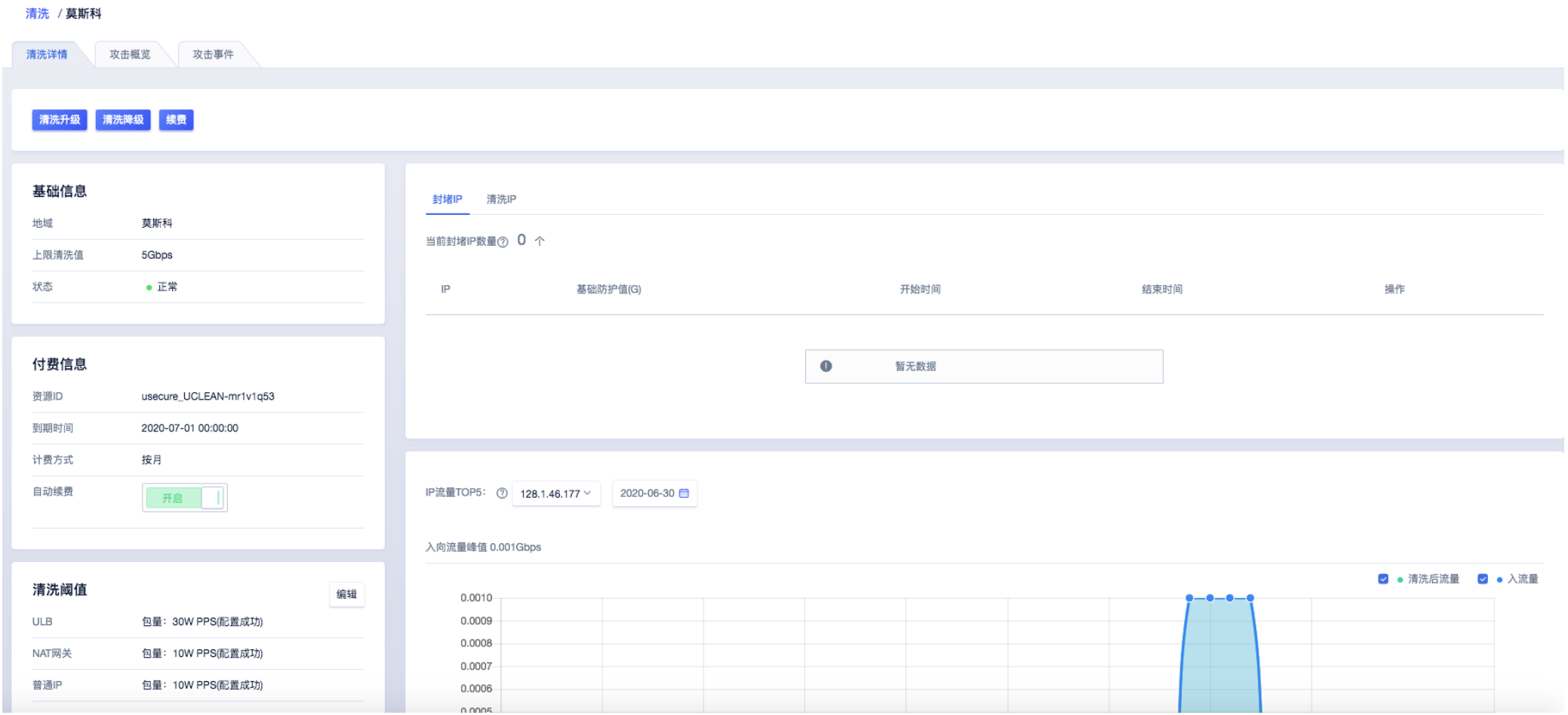
点击【清洗升级】按钮。

地域：弹性外网IP所在的地域，比如香港。

上限清洗值：允许地域范围内，所有IP，同一时间段（5分钟内）达到的最大流量值。

清洗范围：所选地域全部的UCloud外网IP,共享清洗值。

2. 查看清洗详情



清洗详情页中，支持查看清洗的基本信息、付费信息和攻击流量情况，支持调整清洗阈值，支持查看当前封堵IP和清洗IP的情况。

其中包含【清洗升级】、【清洗降级】和【自动续费开关】的操作。

3. 清洗升级

清洗升级操作是立即生效的。

升级需要补差价，付费后即升级成功！

4. 清洗降级

清洗在有效期内不允许降级，降级操作将于清洗到期后进行。

注意：

1. 清洗降级需要关闭自动续费，如果需要自动续费，可以在降级成功后再次开启。
2. 降级不是立即生效的，而是生成一个预约触发器，在到期前都可以随时取消降级预约。
3. 上限清洗值设置为1G，则代表将不再使用清洗服务。产品到期后不再收取任何费用。

5. 清洗阈值调整

当EIP的入向包速超过默认清洗阈值时，会被拉入清洗，清洗过程中如果对正常业务有影响，可根据自身业务带宽情况，自助调高清洗阈值。

操作步骤

1. 选择地域，点击详情按钮，进入详情页。

2. 在清洗阈值区域点击编辑按钮，进入设置页面，可根据EIP绑定的资源类型进行设置，目前有ULB/NAT网关/普通EIP三种类型。

3. 根据业务带宽情况，设置相应的清洗阈值档位，比如设置ULB的清洗阈值为500Kpps，那么当前账号下的所有外网ULB的清洗阈值为：

syn:500Kpps,ack:500Kpps,icmp:20Kpps,udp:500Kpps dns:20Kpps,ssdp:20Kpps,ntp:20Kpps,other:20Kpps

FAQ

1.清洗服务开通后，新增的EIP是否实时加入清洗服务?

不是,目前清洗服务是每隔10分钟刷新配置,如需立即生效,请联系技术支持或客户经理。

2.清洗服务是否可以试用?

不支持试用。

3.清洗服务能抵御多少层攻击?

主要防御4层攻击,7层攻击建议使用UWAF进行防御。

4.被攻击的流量超出购买的清洗服务上限清洗值后，怎么办?

可以升级清洗服务,如果攻击流量超过清洗服务的最大上限清洗值,建议使用高防抵御攻击。

5.清洗详情中是否为实时流量?

不是,流量会延后5分钟刷新到界面上。

6.开通清洗服务后，没有接入清洗是否可以看到流量?

可以,未接入清洗时控制台上看到的清洗前后流量值是一样的。

7.客户业务没有UDP流量，能否直接在清洗时丢弃UDP流量?

可以,请联系技术支持或客户经理。

8.开通清洗服务后是否会立即接入清洗?

不会,只有在超过清洗阈值的情况下才会接入清洗

9.如何判断是否接入清洗，接入清洗的条件是什么?

当流量超过清洗阈值时会接入清洗,同时会以短信和邮件的形式进行通知。

10.如何查看清洗效果?

可以在控制台上对比清洗前后的流量,以此来判断清洗的效果。

11.购买/升级清洗套餐进行清洗时是否能自动解封IP?

是,在新购/升级清洗套餐后3分钟内会自动解封账户内所有被封堵IP,无需人工干预。