百度智能云

# DDOS 文档

# 目录

# DDoS基础防护

## 产品简介

### 产品描述

产品介绍

百度智能云 DDoS 基础防护，是百度云免费为云上客户提供基础的DDoS防护能力，满足客户的日常安全运营需求，保证云资源正常可靠的运行。百度智能云客户可免费享受最高 5Gbps 的 DDoS 防护能力（香港地区基础防护为1Gbps），DDoS 基础防护默认开启，实时监控网络流量，发现攻击后立即清洗。如需百Gbps级别的 DDoS 防护能力，您可以购买流量突发服务包服务，无需更换IP。如需Tbps级别的DDoS防护阈值可购买DDoS高防服务，使用时需要将流量切换至高防IP。

### 核心概念

核心概念

**DDoS**

分布式拒绝服务DDoS（Distributed Denial of Service ）攻击是指借助于客户/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。

通常，攻击者使用一个偷窃账号将DDoS主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通讯，代理程序已经被安装在Internet上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

**CC (Challenge Collapsar)攻击**

HTTP Flood，是针对Web服务在 OSI 协议第七层协议发起的攻击，攻击者极力模仿正常用户的网页请求行为，发起方便、过滤困难，极其容易造成目标服务器资源耗尽无法提供服务。

**清洗**

当目标 IP 的公网网络流量超过设定的防护阈值时，百度智能云 DDoS 系统将自动对该 IP 的公网入向流量进行清洗。通过策略路由将流量从原始网络路径中重定向到 DDoS 清洗设备上，通过清洗设备对该 IP 的流量进行识别，丢弃攻击流量，将正常流量转发至目标 IP。

**封禁**

当目标 IP 受到的攻击流量超过云资源所在区域（机房）的封禁阈值时，百度智能云将屏蔽该 IP 的所有外网访问，保护云平台其他用户免受影响。

- **封禁阈值**
  - 中国大陆及新加坡区域用户遭受攻击且攻击流量峰值最高达到5G时，会触发封禁。
  - 中国香港区域用户遭受攻击流量峰值最高达到1G时，会触发封禁。
- **封禁时长** 封禁时长默认为2小时，实际封禁时长与当日被攻击持续时长和攻击峰值相关，最长可达24小时。封禁时长主要受以下因素影响：

  * 攻击是否持续；若攻击一直持续，封禁时间会延长，封禁时间从延长时刻开始重新计算。

  * 攻击是否频繁；被频繁攻击的用户被持续攻击的概率较大，封禁时间会自动延长。

  * 攻击流量大小；被超大型流量攻击的用户，封禁时间会自动延长。

注意：针对个别攻击较频繁，攻击流量较大的用户，百度智能云保留延长封禁时长和降低封禁阈值的权利，具体黑洞阈值和黑洞时长以控制台显示为准。

**为什么需要封禁策略？为什么百度智能云不能免费帮用户无限抵御DDoS攻击？**

百度智能云通过共享基础设施的方式降低云上用户用云成本，所有用户共用百度智能云的外网出口。当发生大流量 DDoS 攻击时，除了会影响被攻击对象，整个百度智能云的网络都可能会受到影响。为了避免因DDoS对其他未被攻击的用户造成影响，保障整个云平台网络的稳定，需要进行封堵。

DDoS 防御需要极高的成本，其中最大的成本就是带宽费用。带宽是百度智能云向电信、联通、移动等运营商购买，运营商计算带宽费用时不会把 DDoS 攻击流量清洗掉，而是直接收取百度智能云的总带宽费用。百度智能云DDoS基础防护在控制成本的情况下会尽量为云平台用户免费防御 DDoS 攻击，但是当攻击流量超出阈值时，百度智能云会屏蔽被攻击 IP 的流量，从而避免超额费用的产生。

如果您的 IP 遭受的攻击流量超出阈值触发封禁时，如需将DDoS防护阈值提升到百Gbps级别，可购买流量突发服务包服务，并无需更换IP。如需Tbps级的DDoS防护阈值可购买DDoS高防服务，绑定高防IP后请您工单反馈工作人员将受攻击的EIP解除封禁状态，此时业务可通过高防地址访问，EIP仍需要24小时解除黑洞状态。

**基础防护阈值太低不满足需求怎么办？**

购买流量突发服务包服务，获得百Gbps级别的防御能力，并无需更换IP。如需Tbps级的DDoS防护阈值可购买DDoS高防服务，使用时需要将流量切换至高防IP。

## 产品优势

**全方位多层防护**

弹性公网IP、云服务器、负载均衡等云资源全方位防护，实时监测网络流量，发现攻击立即清洗。有效解决SYN Flood/ACK Flood/ICMP Flood/UDP Flood等多种网络层 DDoS 攻击，以及 CC 攻击等应用层攻击。

**更快，更强，更高效**

总计T级的DDoS防护能力，BGP线路，速度更快，延迟更小，线路更稳定。

**更聪明，更智能**

特有 DDoS 智能分析系统，面对攻击能够快速反应。

**免费防护**

DDoS基础防护为云上客户提供最高5G免费防护能力。

**专业可信赖**

专业安全团队，多年百度实战经验，值得信赖。

## 产品特性

**基于网络传输的攻击防护**

有效抵御SYN flood，ACK flood，SYN-ACK flood，FIN/RST flood，UDP flood，ICMP flood等攻击。

**基于应用层的威胁防护**

有效抵御HTTP get /post flood，CC，HTTP slow header/post，TCP连接耗尽等攻击。

**探测包、畸形包过滤**

基于多种协议字段的畸形数据包过滤，以及各种协议探测型攻击。

**攻击趋势报表**

多种数据报表监测，从流量、数据报文等多个维度全面反应攻击详情。

## 应用场景

DDoS 基础防护能够为百度智能云上用户提供免费 DDoS 防护能力，满足日常安全运营需求，主要为遭受攻击概率不大，攻击流量不超过5Gbps的云上用户业务提供防护。

说明：如需获得更高的 DDoS 防护能力，可根据自身业务需求，选用流量突发服务包服务，快速应对攻击。

# 操作指南

## 简介

简介

**背景信息**

结合云服务器部署业务的实际需求，设置合理的流量清洗阈值，包括每秒请求流量和每秒报文数量，当系统检测到服务器入流量超过设定阈值后，会自动清洗异常攻击流量，保证用户的业务不受攻击影响。当系统检测到攻击行为时，会通过用户设定的通知方式邮件或短信及时通知到用户，用户可以登录控制台查看相应的攻击记录以及具体的流量统计信息，结合流量数据用户可以在业务层面采取再进一步的处理措施。

**应用场景**

用户可以根据业务需求，针对单个弹性公网IP 实例进行配置防护参数。系统结合用户购买的BCC实例带宽数据，提供推荐配置。

## 操作指南

1.进入百度智能云官网。

2.登录百度智能云平台：

- 若没有用户名，请先完成注册，操作请参考注册。
- 若有用户名，登录操作请参考登录。

3.登录成功后，选择“产品服务 > DDoS防护服务”，在左侧导航栏点击“弹性公网IP”，进入DDoS 防护服务列表页，查看当前 EIP 实例及绑定的云服务器 BCC实例，当前 DDoS 的防护状态，清洗启动阈值，最大防护能力等信息。参见下表：

| 参数列表 | 说明 |
| --- | --- |
| 弹性公网IP | DDoS防护中的EIP实例 |
| 绑定关系 | 每个弹性公网IP对应绑定的BCC/BLB |
| 状态 | EIP实例的当前状态，包括“黑洞”、“黑洞解禁时间”、“正在清洗”、“正常” |
| 清洗启动阈值 | 每秒请求流量、每秒报文数量、每秒HTTP请求 |
| 最大防护能力/防护阈值 | 黑洞触发阈值 |
| 操作 | 查看当前EIP实例的DDoS防护服务详情 |


设置DDoS基础防护参数

**应用场景**

用户能够防护SYN Flood，UDP Flood，ACK Flood，ICMP Flood，DNS Flood，CC攻击等4到7层DDoS的攻击。 详细设置方法如下：

**操作步骤**

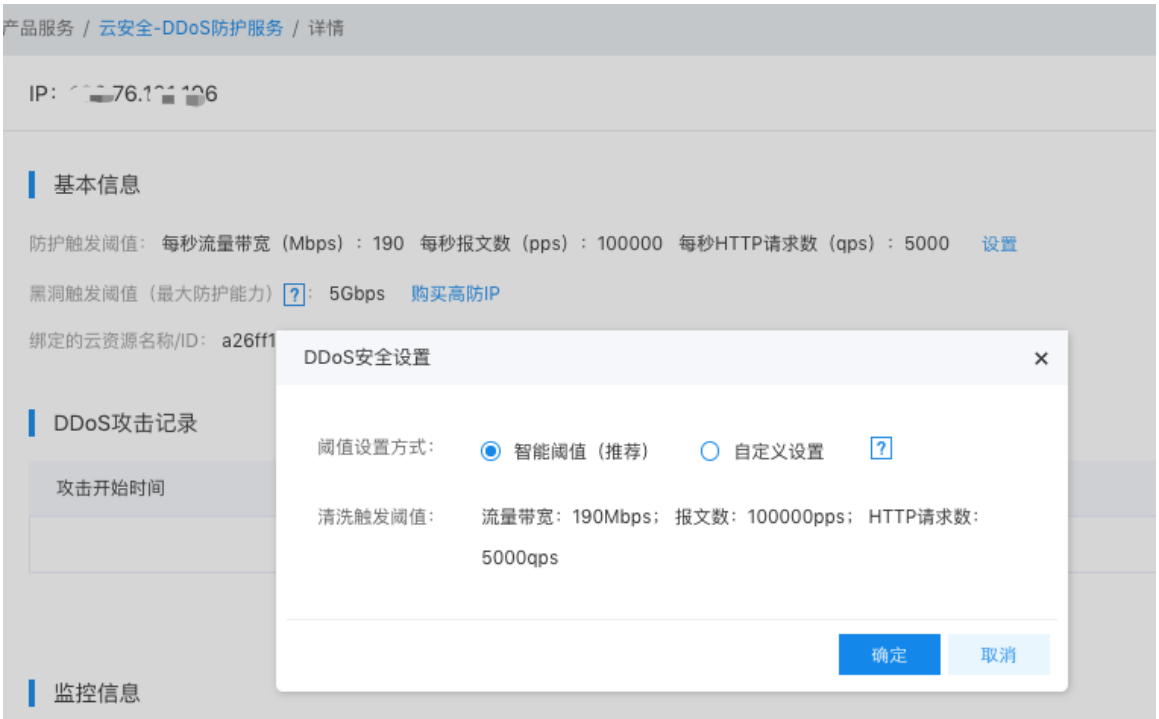
1.在左侧导航选择“DDoS防护服务->弹性公网IP”，进入“DDoS防护服务列表”页面。

2.选择需要防护参数的 EIP 实例，点击“查看详情”。


3.进入详情页，在基本信息中点击“设置”，对单个云服务器BCC或负载均衡BLB实例的清洗触发值进行设置。 开启清洗阈值，只要达到了阈值，就会触发防护。

系统结合用户购买的BCC实例带宽数据，提供推荐清洗阈值，详见如下：

- 智能阈值：会根据用户业务流量实际情况进行计算，不断调整修正DDoS清洗阈值。不用担心业务增长导致的误清洗。
- 自定义设置：用户自定义设置流量清洗阈值。当用户自定义设置阈值时，百度智能云将不再会根据用户业务增长情况进行阈值的自动调整。




4.点击“确定”，完成DDoS安全设置。

> **说明：**
>
> - 百度智能云DDoS基础防护支持 CC 防护，默认提供7层防护。
> - 如需百Gbps级别的DDoS防护阈值，请购买流量突发服务包服务，Tbps级的DDoS防护阈值请购买DDoS高防服务。

## 查看DDoS攻击记录

**应用场景**

用户能够查看单个BCC或BLB实例遭受的DDoS攻击记录。

**操作步骤**

1.在左侧导航选择“DDoS基础防护”，选择需要防护参数的 EIP 实例，点击“查看详情”。

2.查看“DDoS攻击记录”区域，可以查看攻击发生时间、状态、原因。


## 查看DDoS流量报表

**应用场景**

用户能够查看DDoS基础防护单个 BCC/BLB 实例的网络流量报表。

**操作步骤**

1.在左侧导航选择“DDoS防护服务”，选择需要防护参数的 EIP 实例，点击“查看详情”。

2.查看“监控信息”区域的趋势图，即可查看流量报表。

## 设置DDoS攻击通知方式

**应用场景**

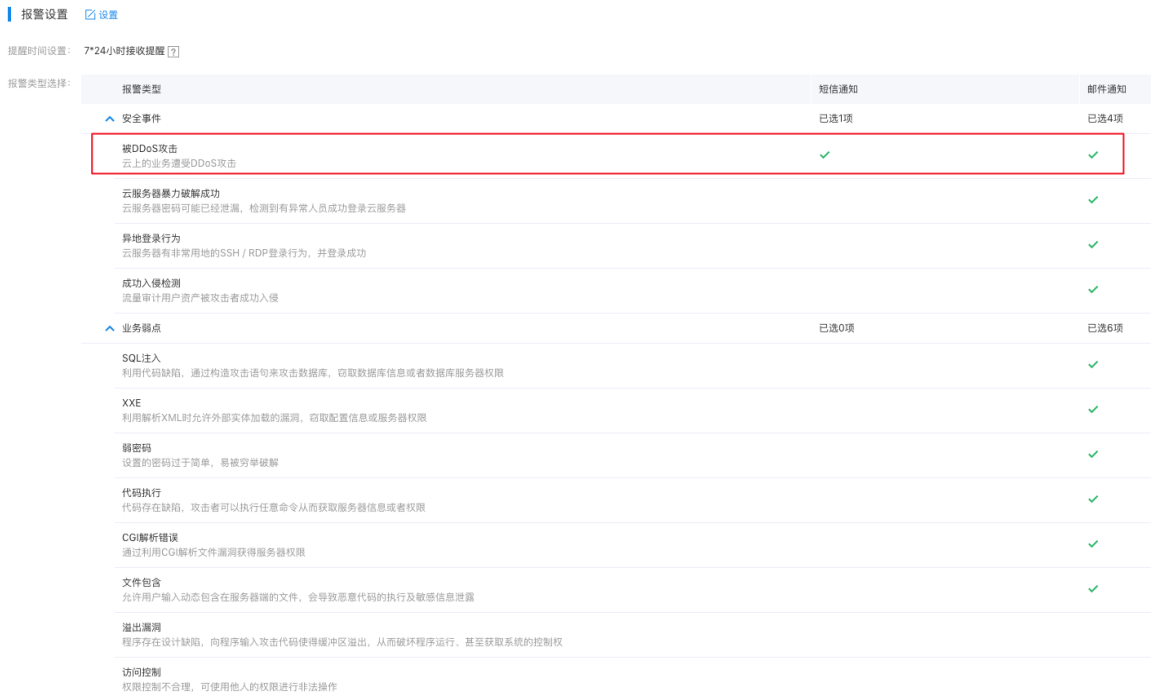
用户能够统一设定针对不同安全服务的报警方式和策略。

用户可以设置针对不同安全服务报警方式以及短信报警时间：邮件或者短信。

**操作步骤**

1.选择“产品服务>安全和管理>DDoS防护服务”，进入DDoS防护服务页面。

2.选择左侧导航的“报警设置”，进入“云安全-报警设置”界面。




3.根据实际情况，选择通知方式，短信或者邮件，并设置提醒时间。

4.点击“确定”，完成DDos的报警设置。

# DDoS高防防护

## 产品描述

### 产品介绍

DDoS 高防 是百度智能云针对游戏、互联网、金融及政企等行业遭受大流量 DDoS 攻击导致用户服务不可用的情况而推出的付费防护服务。

百度智能云 DDoS 高防 采用 BGP 线路，相较传统的静态IDC高防IP服务，百度智能云 BGP 高防 IP 天然具有灾备能力、线路更稳定、访问速度更快。

百度智能云 DDoS 高防 使用DNS解析的接入方式，支持 TCP，UDP，HTTP，HTTPS，WEBSOCKET和WEBSOCKETS等协议，覆盖游戏、互联网、金融及政务等各类业务。

### 产品优势

**实时监测秒级防御**

基于独有智能高敏数据包比例模型算法，最快100ms发现流量攻击，秒级执行防御。

**更快，更强，更高效**

总计T级的DDoS防护能力，BGP线路，速度更快，延迟更小，线路更稳定。

**更聪明，更智能**

特有智能分析系统，实时提取攻击特征，辅助全网IP威胁库、攻击IP进行恶意请求拦截，多维度精确缓解攻击。

**高效联动防御**

弹性公网IP等百度云资源或私有化本地部署防御系统，在检测到超量攻击后自动联动云防防御。

**专业可信赖**

专业安全团队，多年百度实战经验，值得信赖。

### 产品特性

**基于网络传输的攻击防护**

有效抵御SYN flood，ACK flood，SYN-ACK flood，FIN/RST flood，UDP flood，ICMP flood等攻击。

**基于应用层的威胁防护**

有效抵御HTTP get /post flood，CC，HTTP slow header/post，TCP连接耗尽等攻击。

**探测包、畸形包过滤**

基于多种协议字段的畸形数据包过滤，以及各种协议探测型攻击。

**攻击趋势报表**

多种数据报表监测，从流量、数据报文等多个维度全面反应攻击详情。

### 应用场景

**使用范围**

百度智能云 高防 服务，可以为百度智能云以及百度智能云之外的客户提供防护服务。

**使用场景**

百度智能云 高防 服务能够为游戏、互联网、金融和政府门户等客户提供大流量DDoS攻击防护。适配连续性要求高、实时性体验好的业务场景。

## 产品定价

### 计费概述

DDoS高防包括“保底防护套餐费用”和“弹性防护费用”，采用“预付费+后付费”混合计费模式。

#### 计费项

详细定价见：价格详情。

- 保底防护套餐费用：采用预付费、按月/年计费，购买时生成预付费订单。
  - 高防IP：包含实例内高防IP数（支持IPv4和IPv6）、保底防护峰值、端口数、防护域名数及业务带宽峰值。
  - 高防EIP：包含实例内高防EIP数、保底防护峰值。
- 弹性业务带宽费用：启用弹性业务带宽计费后，超出套餐保底业务带宽的费用，采用后付费、根据选择按日或月计费，次日或每月1日凌晨出账单。
- 弹性防护费用：超出套餐保底防护的费用，采用后付费、按日计费，次日凌晨出账单。

> **注意：**
>
> - 购买前需保证账户无欠款。

#### 计费公式

DDoS高防费用=保底防护套餐费用+弹性业务带宽费用+弹性防护费用

付费方式=预付费+后付费

**保底防护套餐费用**

用户可以根据业务需求自主选择保底防护套餐，不同套餐规格的价格也不相同。

> **注意：**
>
> - 如果实际业务需要超出实例的默认业务规格，您可以通过升级实例或在购买实例时对相应规格进行扩展。

**弹性业务带宽费用（按日/月后付费）**

启用弹性业务带宽后，最大业务带宽为已选保底防护套餐中业务带宽峰值的9倍，上限20Gbps。支持选择日第6峰值和月95峰值计费。

| 对比项 | 日第6峰值 | 月95峰值 |
| --- | --- | --- |
| 结算周期 | 按自然日结算 | 按自然月结算 |
| 计费带宽取值 | 合并自然日内同一实例内相同时间全部高防IP带宽，每5分钟计算一个入向或出向平均业务带宽，分别去除最大的5个，剩余最大值为**日第6峰值带宽**。 | 合并自然月内同一实例内相同时间全部高防IP带宽，每5分钟计算一个入向或出向平均业务带宽，分别去除最大的5%计费点，剩余最大值为**月95峰值带宽**。 |
| 产生费用条件 | 日第6峰值带宽大于实例保底业务带宽 | 月95峰值带宽大于实例保底业务带宽 |
| 计费公式 | 弹性业务带宽费用=（日第6峰值带宽(Mbps) - 实例保底业务带宽(Mbps)）* 日业务带宽单价（3.75元/日/Mbps） | 弹性业务带宽费用=（月95峰值带宽(Mbps) - 实例保底业务带宽(Mbps)）* 月业务带宽单价（75元/月/Mbps） * 实际使用天数占比 |
| 出账时间 | 次日，北京时间凌晨 | 下月1日，北京时间凌晨 |

> **注意：**
>
> - 日第6峰值：如使用不足一日，按一日计算。
> - 月95峰值：如使用不足一个自然月，按实际使用天数占比计算。实际使用天数占比=自然月实际使用天数/自然月总天数。
> - 实例下全部高防IP同时间合并，实际使用业务带宽持续超过保底业务带宽（未开启弹性）或弹性业务带宽（开启弹性）后，将被执行限流。
> - 暂不支持自助关闭弹性业务带宽，如需修改请通过对应的销售或工单系统联系我们。

**弹性防护费用（按日后付费）**

- 没有超过保底防护套餐时，不额外收费；超过保底防护套餐的弹性防护峰值，按照每Gbps：100元/日计费。
- 防护带宽为高防IP产生的最大攻击带宽峰值，计费上限为实例的弹性防护带宽值。如果保底防护带宽与弹性防护带宽相同，则不会产生弹性防护后付费用。
- 按日计费，不足1天按1天计费。
- 北京时间每日凌晨推送上一自然日弹性防护费用。
- 若实例包含多个高防IP，各个高防IP共享防护峰值。同一实例内多个高防IP同一计费周期(某日00:00:00-23:59:59)都遭受攻击，弹性计费按照各高防IP峰值叠加计算。例如：高防IP1和IP2，归属于同一个实例。IP1在10:00产生今日最大10Gbps防

护带宽，IP2在15点产生今日最大20Gbps防护带宽，叠加后的防护带宽计费值为30Gbps。

到期提醒和欠费处理

**到期提醒**

保底防护套餐到期前7天、3天和1天，系统会发送到期提醒。

**到期后处理**

到期后立即停止服务，系统会发送停服通知。数据为您保留7天，期间不收取费用，7天内未续费则释放，释放前1天和释放时系统都会发送释放通知。

**欠费处理**

如账号已欠费（包含使用其他云上产品导致的欠费），高防会停止弹性业务带宽和弹性防护能力，保底业务带宽和保底防护不受影响。

不支持退费

已购买的保底防护套餐实例不支持提前退费

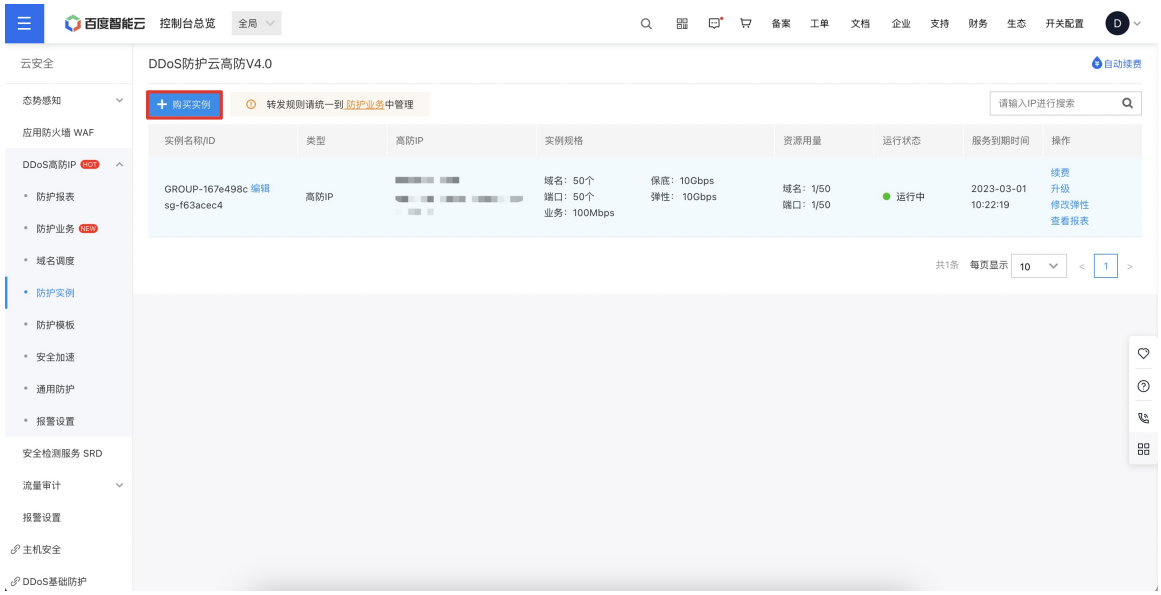
## 购买DDoS高防IP

**购买前提**

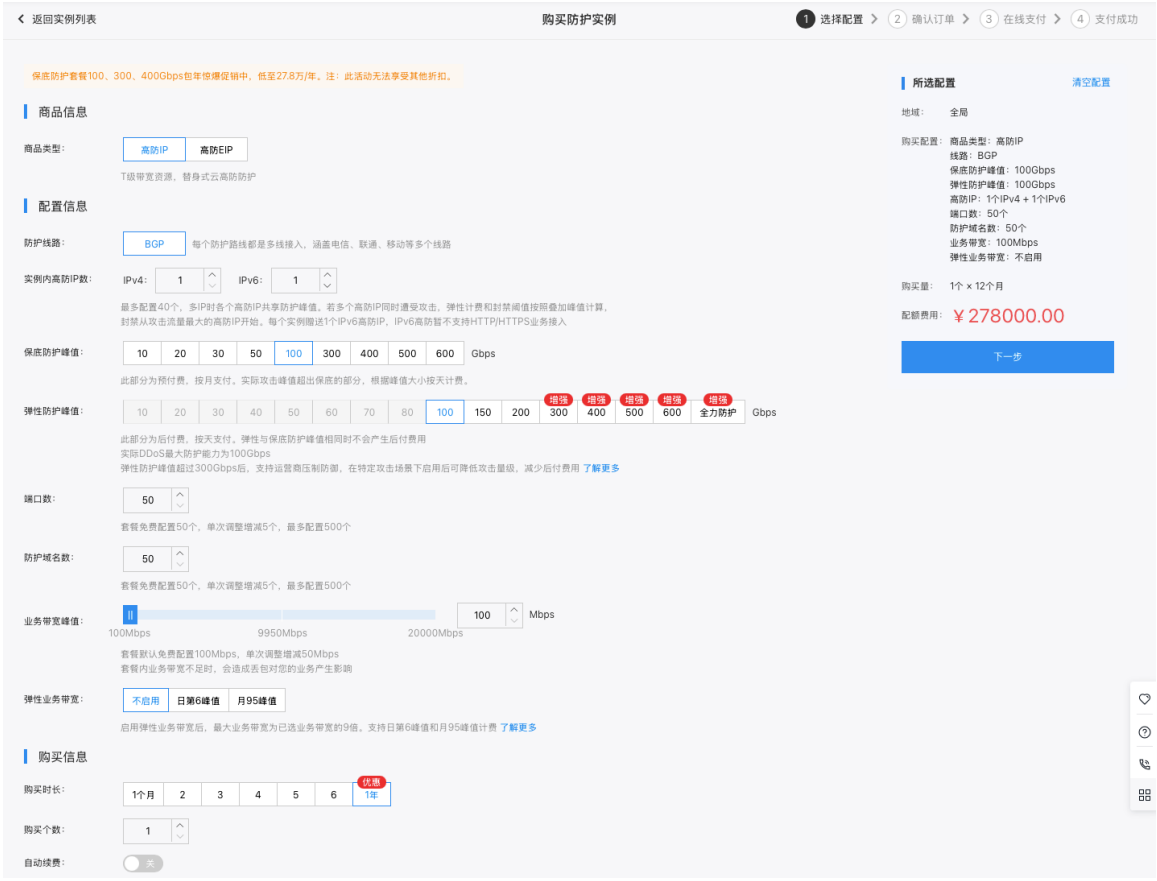
1. 进入百度智能云官网。
2. 登录百度智能云平台：
   - 若没有用户名，请先注册，并完成实名认证，操作请参考注册。
   - 若有用户名，登录操作请参考登录。

**操作步骤**

1. 登录成功后，选择“产品服务 > 安全 > DDoS防护服务”,进入产品页面。
2. 在页面左上角点击“购买实例”。




3. 根据实际业务需求，选择套餐规格,在配置区域选择实例内高防IP数、保底防护峰值、弹性防护峰值、端口数、防护域名数、业务带宽峰值、是否启用弹性业务带宽




- 实例内高防IP数：实例内高防IP数量，默认为2个最多配置20个（默认1个IPv4和1个IPv6，IPv6高防当前仅支持TCP和UDP业务接入防护）。多IP时各个高防IP共享防护峰值。若多个高防IP同时遭受攻击，弹性计费和封禁阈值按照叠加峰值计算，封禁从攻击流量最大的高防IP开始。
- 保底防护峰值：指高防IP实例的保底防护带宽。根据所选择的保底防护峰值规格及购买时长，生成预付费账单。建议参考历史攻击流量的平均值，选择的保底防护峰值略高于平均值，可以防御大部分攻击行为。
- 弹性防护峰值：指高防IP实例的最高弹性防护带宽。对于超出保底防护峰值的攻击进行弹性防护，并根据实际发生的超出保底防护峰值的攻击峰值生成后付费账单。建议参考历史最高攻击流量，选择的弹性防护峰值略高于历史最高攻击峰值，可以防御大流量攻击，避免超过防护峰值而引起的IP封禁。

> **注意：**
>
> - 若您不需要启用弹性防护能力，只需将弹性防护峰值与保底防护峰值设置一致即可，高防IP实例将不会产生后付费防护费用，且该实例的最高防护带宽为保底防护峰值。

- 端口数：指高防IP实例支持的转发端口数量，即配置TCP/UDP协议转发规则的最大数量。套餐免费配置50个，单次调整增减5个，最多配置500个。
- 防护域名数：指高防IP实例支持接入防护HTTP/HTTPS域名的数量。套餐免费配置50个，单次调整增减5个，最多配置500个。
- 业务带宽峰值：指非攻击状态下高防IP实例所支持正常业务的转发带宽。套餐默认免费配置100Mbps，单次调整增减50Mbps。套餐内业务带宽不足时，会造成限流丢包对您的业务产生影响。
- 弹性业务带宽：启用后支持日第6峰值和月95峰值计费，最大业务带宽峰值为已选业务带宽峰值的9倍，上限为20Gbps。

4. 购买时长：设置高防IP需要购买的时长，将根据 IP 数量、保底防护峰值、防护域名数、端口数、业务带宽以及购买时长计算需要预付的费用。默认1个月，购买1年8.3折(10个月)。
5. 购买个数：设置需要购买的高防IP实例数量。

6. 自动续费：用户可自行勾选。开启自动续费后，在百度智能云账号余额充足情况下，服务到期后将按月自动续费，保障安全防护不中断。

7. 点击“下一步”，确认订单后，完成支付即可

## 购买DDoS高防EIP

EIP联合高防为百度智能云客户提供高防EIP产品，该产品具备EIP在基础云产品上灵活使用特性，同时拥有更强大的高防防护能力。能够满足游戏、金融、政企等客户便捷使用需求。

高防EIP产品购买和开通需要分别在EIP和DDoS高防产品上进行：

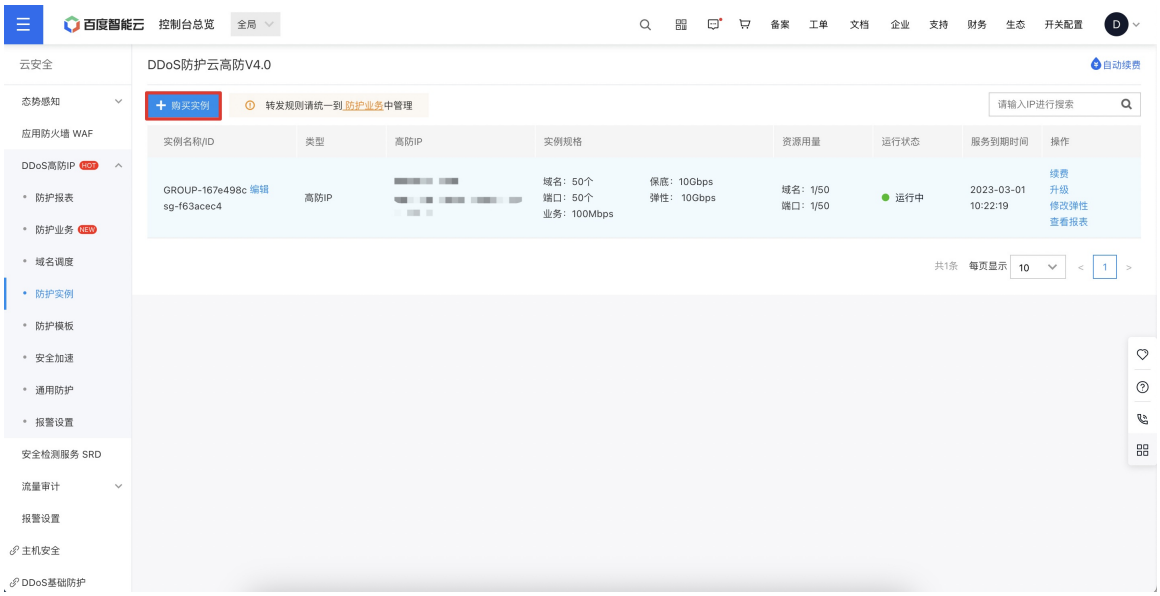
- EIP，负责正常业务带宽/流量的开通和使用，当前支持在北京、保定、武汉region使用，了解详情请访问EIP计费和开通；
- DDoS高防，负责业务被DDoS攻击时的防护，需要购买高防防护实例，下文详细介绍购买DDoS高防EIP实例过程。

**购买前提**

1. 进入百度智能云官网。
2. 登录百度智能云平台：
    - 若没有用户名，请先注册，并完成实名认证，操作请参考注册。
    - 若有用户名，登录操作请参考登录。

**操作步骤**

1. 登录成功后，选择“产品服务 > 安全 > DDoS防护服务”,进入产品页面。
2. 在页面左上角点击“购买实例”。

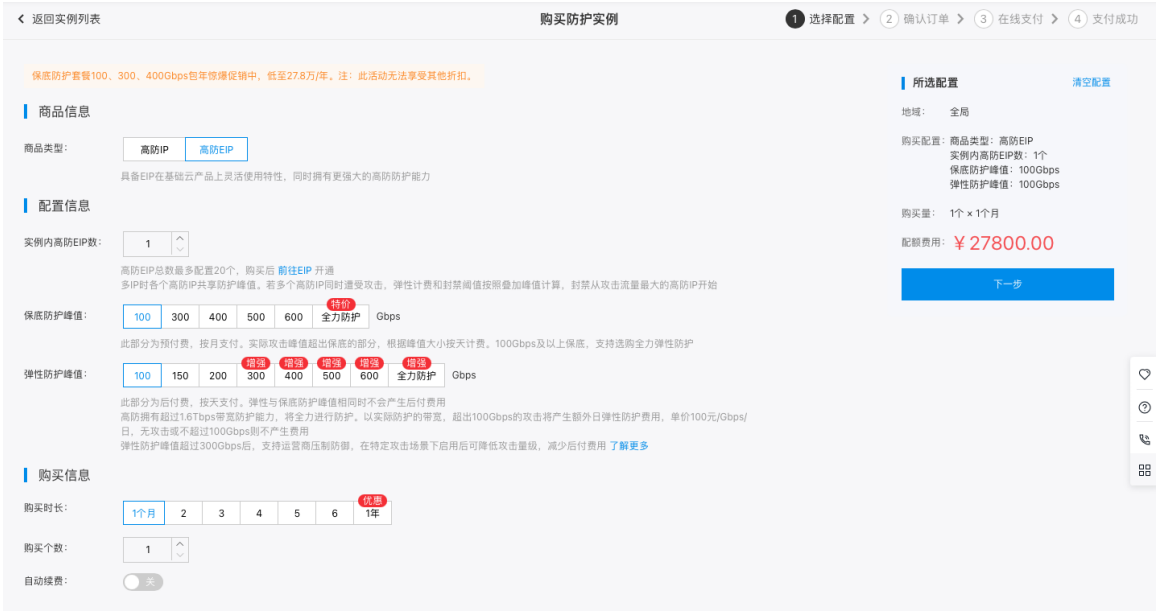



3. 选择 高防EIP 商品类型，根据实际业务需求，选择套餐规格，在配置区域选择实例内高防IP数、保底防护峰值、弹性防护峰值

    - 实例内高防IP数：实例内高防IP数量，默认为1个最多配置20个。多IP时各个高防IP共享防护峰值。若多个高防IP同时遭受攻击，弹性计费和封禁阈值按照叠加峰值计算，封禁从攻击流量最大的高防IP开始。
    - 保底防护峰值：指高防EIP实例的保底防护带宽。根据所选择的保底防护峰值规格及购买时长，生成预付费账单。建议参考历史攻击流量的平均值，选择的保底防护峰值略高于平均值，可以防御大部分攻击行为。
    - 弹性防护峰值：指高防EIP实例的最高弹性防护带宽。对于超出保底防护峰值的攻击进行弹性防护，并根据实际发生的超出保底防护峰值的攻击峰值生成后付费账单。建议参考历史最高攻击流量，选择的弹性防护峰值略高于历史最高

攻击峰值，可以防御大流量攻击，避免超过防护峰值而引起的IP封禁。

> **注意：**
>
> - 若您不需要启用弹性防护能力，只需将弹性防护峰值与保底防护峰值设置一致即可，高防实例将不会产生后付费防护费用，且该实例的最高防护带宽为保底防护峰值。




4. 购买时长：设置高防EIP需要购买的时长，将根据IP数量、保底防护峰值、购买时长计算需要预付的费用。默认1个月，购买1年8.3折(10个月)。
5. 购买个数：设置需要购买的高防EIP实例数量。
6. 自动续费：用户可自行勾选。开启自动续费后，在百度智能云账号余额充足情况下，服务到期后将按月自动续费，保障安全防护不中断。
7. 点击“下一步”，确认订单后，完成支付即可

## 续费高防实例

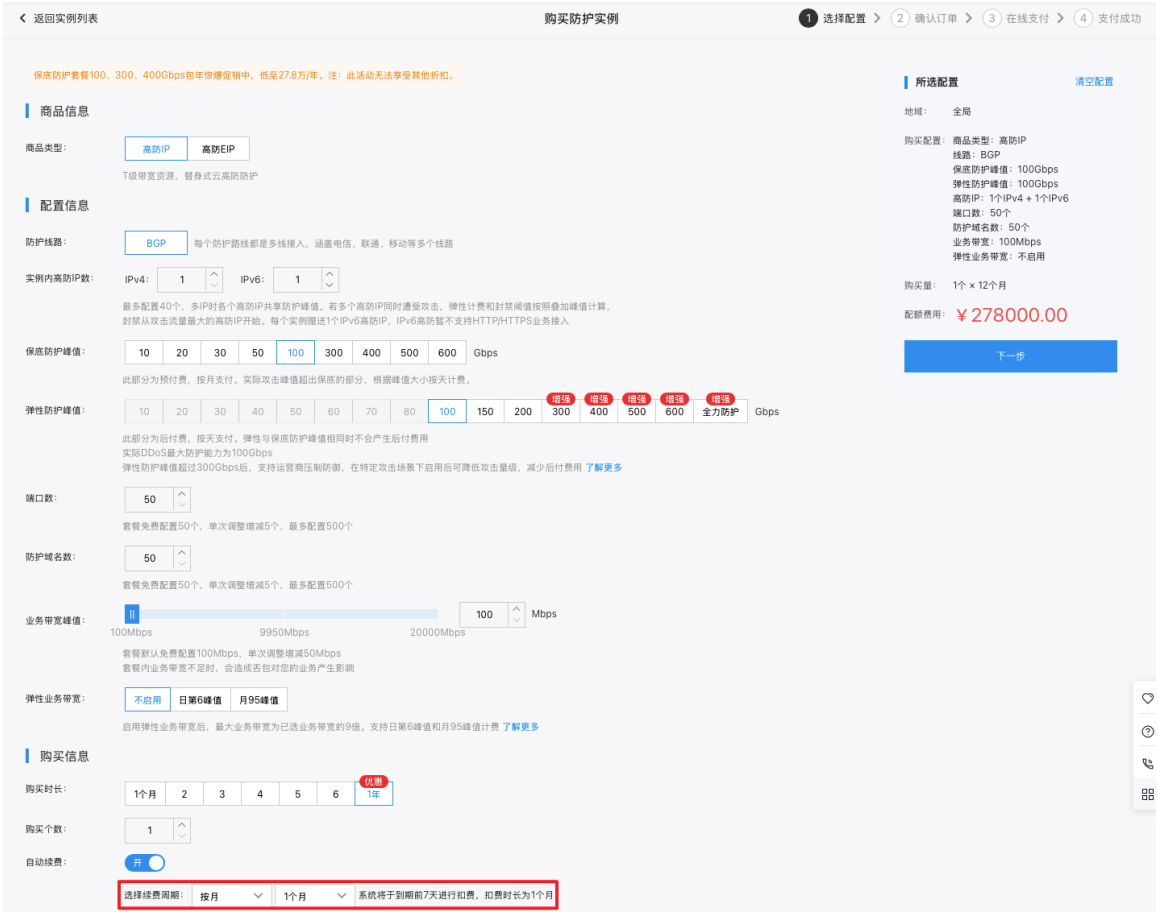
为了能享受持续的安全防护服务，您需要在高防 服务到期前为其手动续费，也可以开通到期自动续费。

高防 服务到期前7天、3天、1天，百度智能云会向您推送服务即将到期、请及时续费等相关信息，信息通过短信及邮件的方式通知到您。

**自动续费**

- 购买实例时开通自动续费

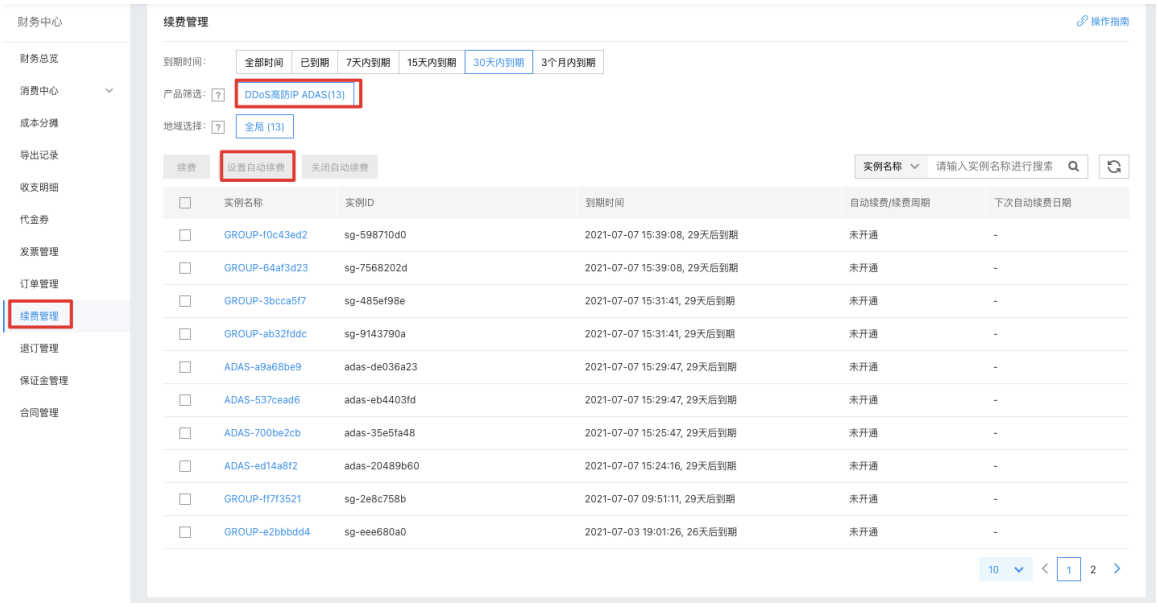
在购买高防实例时，若已同意并开通自动续费。在实例到期前7天，系统会向您发送提醒信息并自动生成续费订单，无需手动续费。




**注意：**

- 按月开通的高防 IP 实例，其自动续费周期默认是1个月，支持自定义调整续费周期。
- 按年开通的高防 IP 实例，其自动续费周期默认是1年，支持自定义调整续费周期。

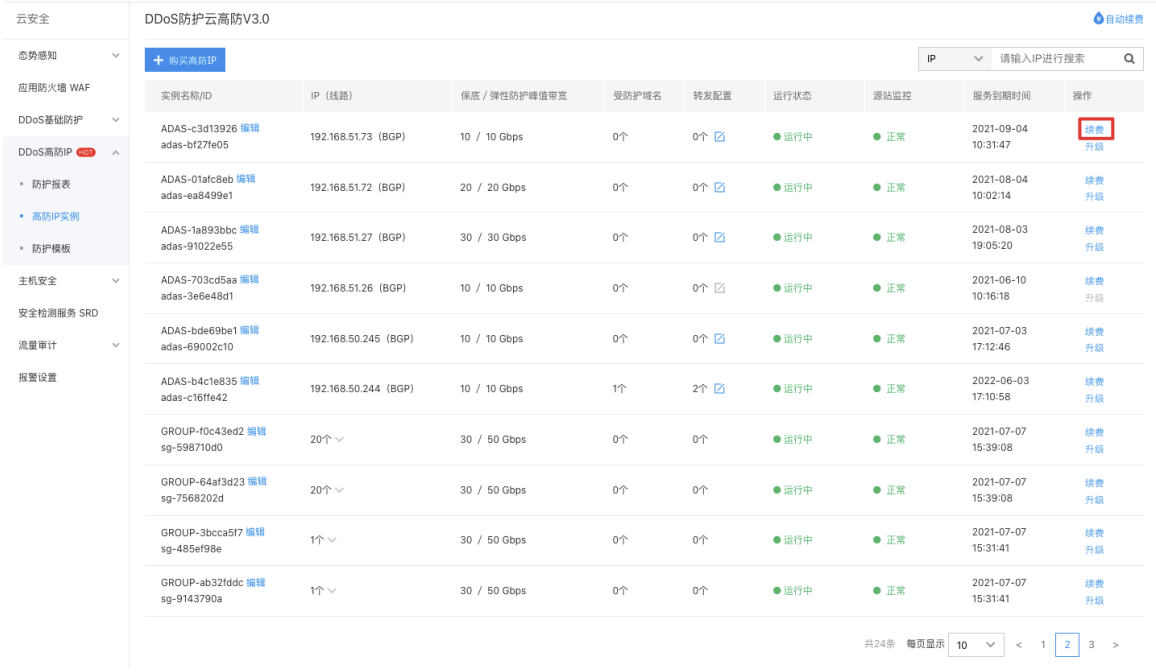
- 购买后开通自动续费 可以对未开通自动续费的实例设置自动续费功能。可以通过高防实例列表右上角自动续费或“财务 > 续费管理”开通自动续费功能。



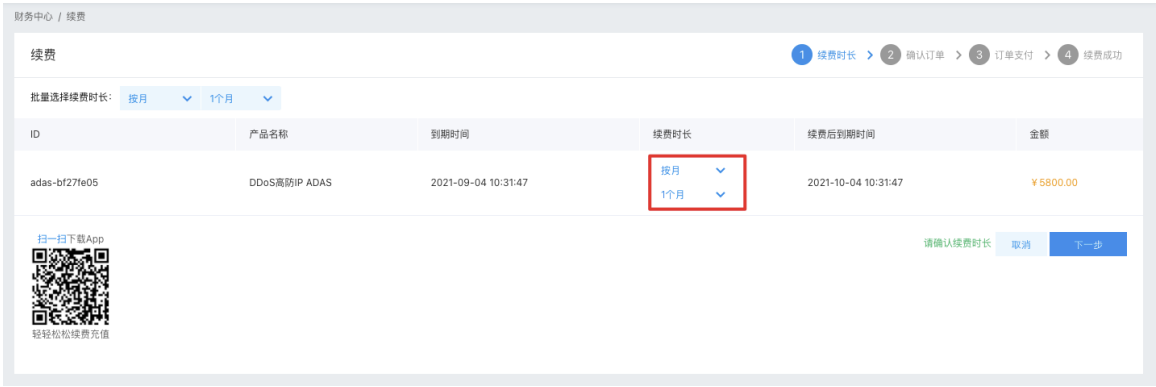

**控制台续费**

1.登录百度智能云 DDoS高防 控制台。

2.在高防 IP 实例列表页，选择需升级的 高防 实例，点击“续费”。




3.在**续费**界面，选择续费时长后，完成订单支付即可。




## 升级高防实例规格

您购买高防 实例后，如果所购买的实例规格（保底防护峰值、弹性防护峰值、实例内高防IP数、端口数、防护域名数或业务带宽峰值）已无法满足您实际业务的防护需要，您可以随时在百度智能云高防 实例控制台升级当前高防实例规格。

> **注意：**
>
> - 升级不支持降低已购买高防实例的规格（包括保底防护峰值、弹性防护峰值、实例内高防IP数、端口数、防护域名数和业务带宽峰值）；
> - 如有降低或增加弹性防护需求，可通过「防护实例」页面操作中的「修改弹性」完成，每个实例1天只能调整一次弹性防护配置。

升级高防 实例规格，需要加收额外的升级费用。支付完成后，高防IP实例规格升级即时生效。

**保底防护峰值**

调高保底防护峰值遵循不满1月按天补差价，满1月按照包月价格补差价，计费方式：升配费用 = 合同剩余时长 * 新旧配置差价

- 合同剩余时长 = 当月剩余天数/30（日历天数）+ 剩余整月数
- 新旧配置差价 = 升级后服务的包月价格 - 当前服务的包月价格

- 若调整的保底防护峰值等于或大于已设置的弹性防护峰值，则弹性防护不生效。
- 升配不影响资源到期时间。
- 升配可以使用代金券抵扣费用。

**弹性防护峰值**

- 升级弹性防护峰值不产生预付费用。

**实例内高防IP数、端口数与防护域名数**

- 实例内高防IP数： 新增高防IP按每个 800 元/月的价格与当前服务剩余时长计算差价。
- 端口数： 新增端口按每 5 个 250 元/月的价格与当前服务剩余时长计算差价。
- 防护域名数：新增防护域名按每 5 个域名 250元/月的价格与当前服务剩余时长计算差价。

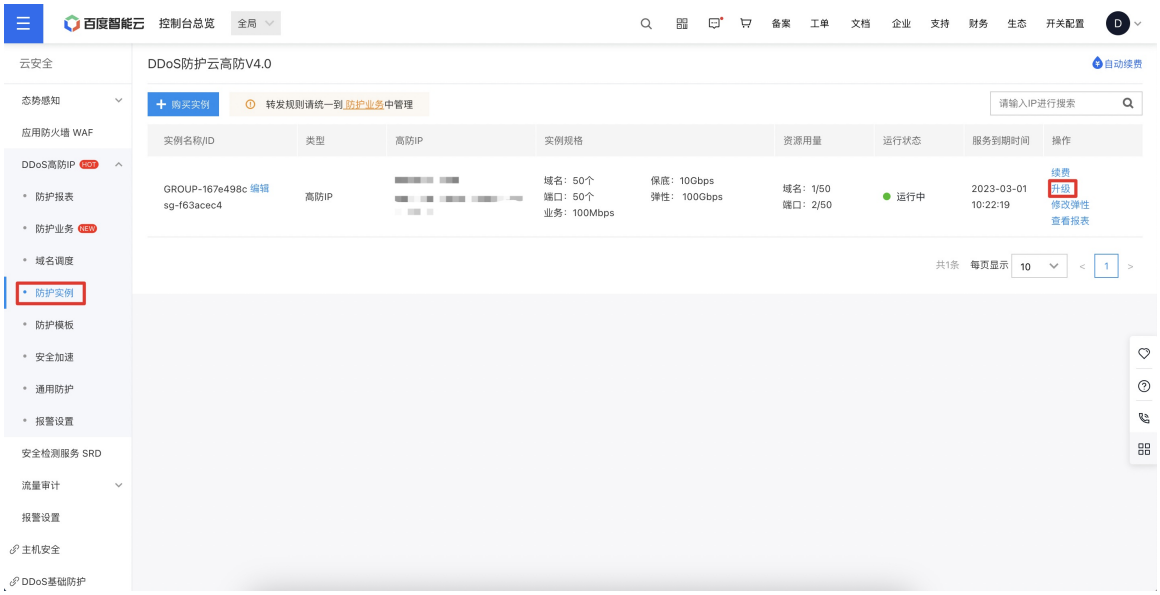
**业务带宽**

- 扩展业务带宽规格按 75元/月的单价（每增加 1 M）与当前服务剩余时长计算差价。

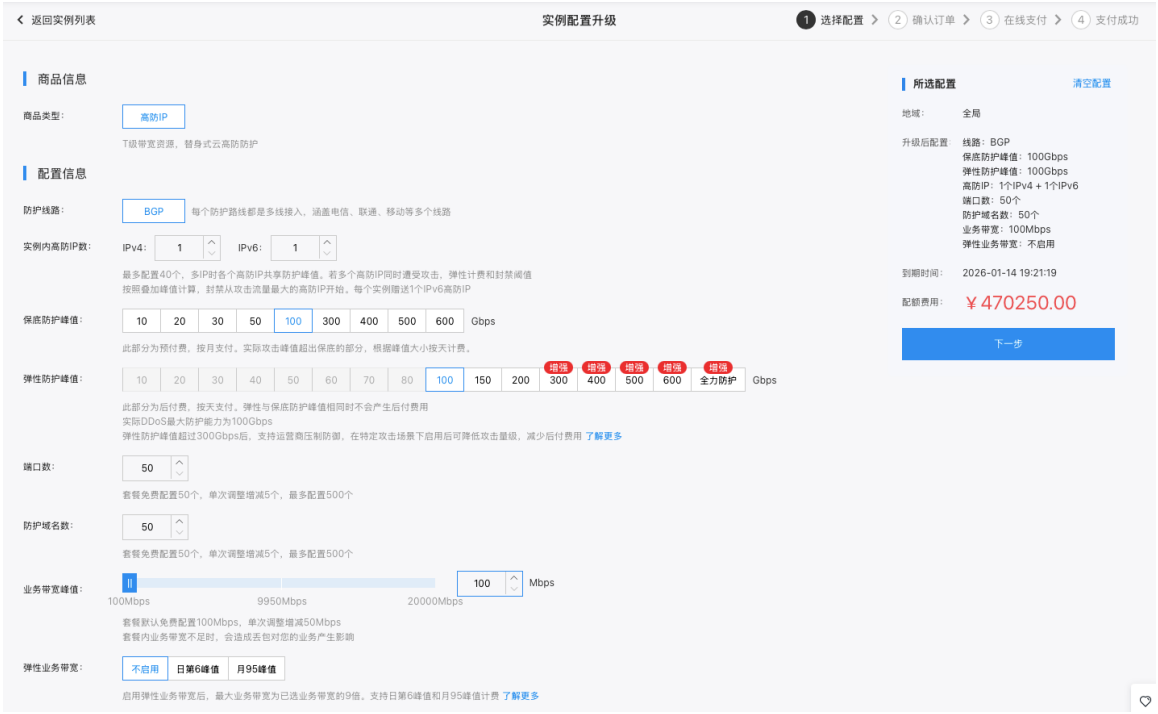
**操作步骤**

1.登录百度智能云 DDoS防护服务 控制台。

2.在 防护实例 列表页，选择需升级的实例，单击“升级”。




3.在**配置升级**界面，扩展保底防护峰值、弹性防护峰值、端口数、防护域名数及业务带宽。




# 操作指南

## 接入防护业务

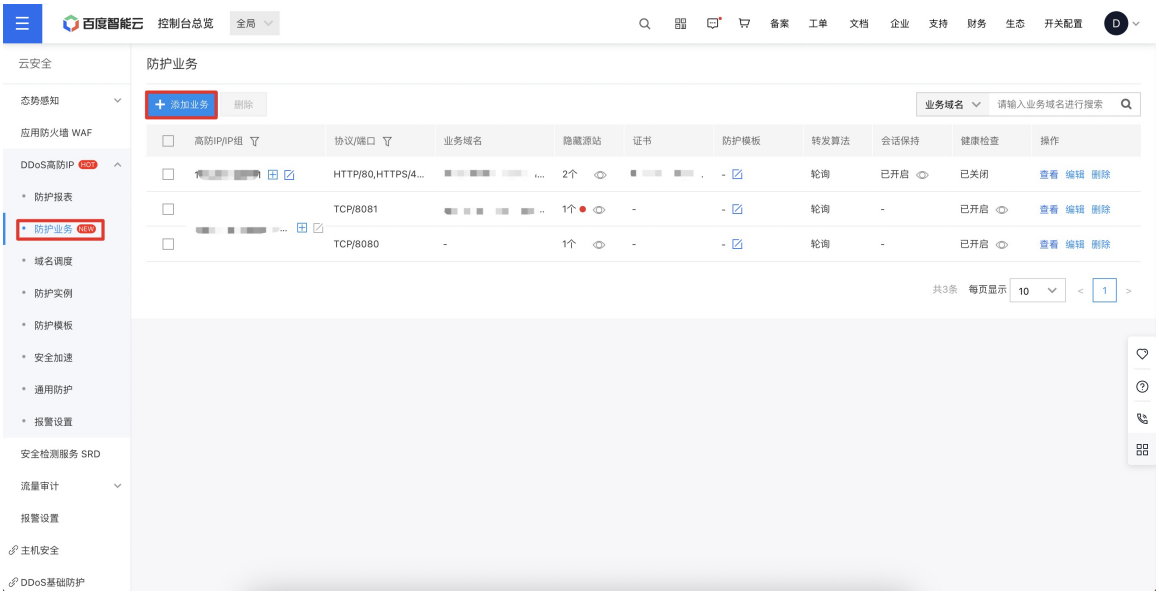
**操作步骤**

第一步：进入高防IP防护业务配置页面

1.在左侧导航选择“产品服务->安全->DDoS防护服务”，进入“DDoS防护”页面。

2.在“DDoS高防IP”左侧导航选择“防护业务”。

3.进入“防护业务”页面“添加业务”。添加后，可以在防护业务列表页快速切换防护模版。




第二步：添加防护业务

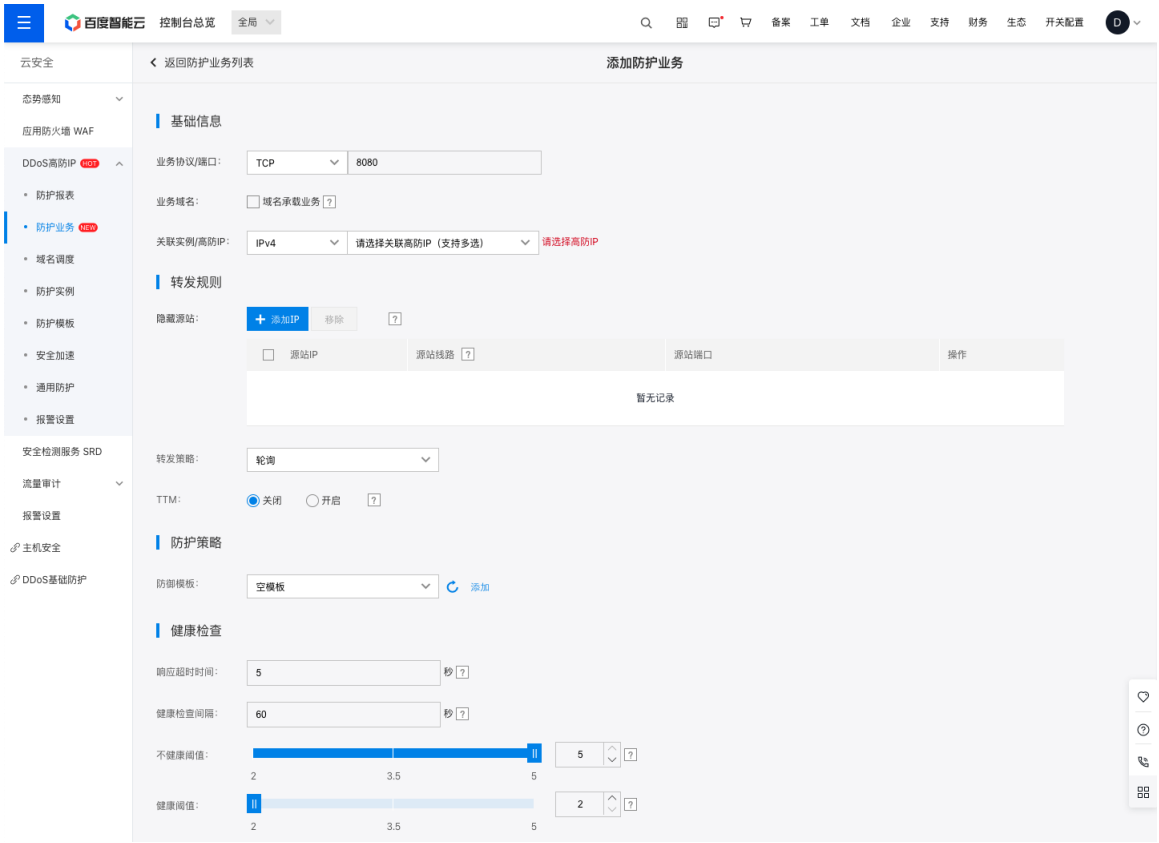
详细防护业务如下图所示：


下表是对防护业务架构图中出现的名词的解释：

| 名称 | 描述 |
| --- | --- |
| 业务协议/端口 | 指定高防中心监听的协议和端口（即用户最终想通过什么协议和端口来访问高防中心）。协议支持HTTP（WebSocket）、HTTPS（WebSockets）、TCP、UDP，端口输入范围为1～65535间的整数。 |
| 隐藏源站 | 即业务源站。高防中心转发请求至源站，支持IP或域名源站；<br>对IP源站，支持设置源站IP运营商线路。设置后回源转发集群将优先匹配相同线路的源站进行转发，提升网络性能；<br>域名源站，仅HTTP或HTTPS业务协议支持并只能配置1个；<br>**建议：为高防防护业务，配置隐藏源站。切入高防后，即使在公开源站被攻击导致黑洞时，依然可以正常服务并隐藏源站。** |
| 转发策略 | 轮询：将请求轮流发送给后端服务器；<br>最小连接数：优先将请求发给拥有最少连接数的后端服务器；<br>源IP：仅针对前端协议配置为TCP和UDP的情况，将请求的源IP进行hash运算后派发请求至某匹配的服务器，这可以保证同一个客户端IP的请求始终被派发至某特定的服务器。源IP算法为TCP和UDP监听器提供会话保持机制。 |

**1.新建TCP/UDP防护业务**

业务协议选择TCP或UDP并填写业务端口，然后填写回源IP和回源端口（源站提供服务的真实端口），选择转发策略。

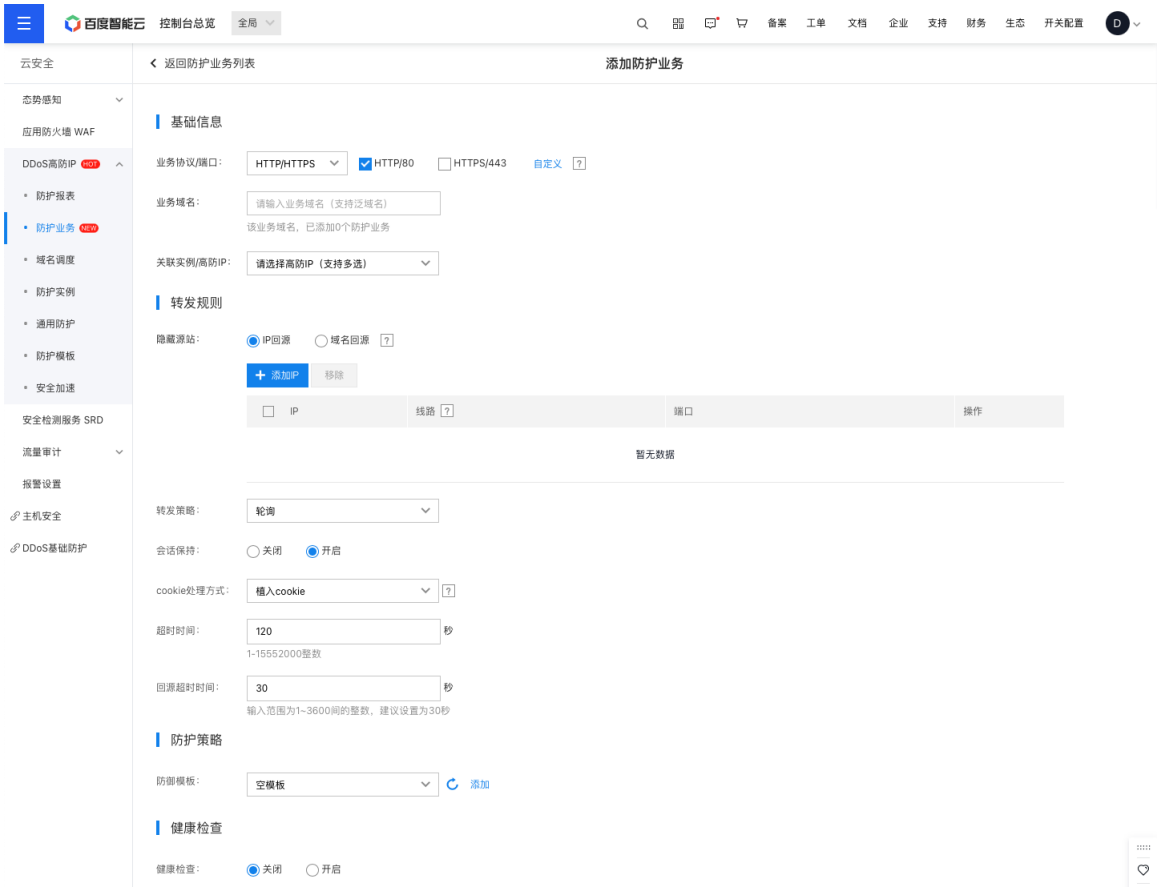


**注意：**

- TCP/UDP防护业务支持关联一个或多个高防IP防护实例下的单个或多个高防IP；
- TCP/UDP防护业务同一高防IP下，相同业务协议/端口仅能添加一次；如果已配置HTTP、HTTPS协议端口，对应端口的TCP协议不能添加。例如：高防IP：111.111.111.111下TCP/8080仅能添加一次；111.111.111.111下已添加HTTP/80网站防护业务，不能再添加TCP/80的端口防护业务；
- 高防中心会将数据转发至源站，TCP/UPD防护业务仅支持IP源站。IP源站最多配置50个，不能为私有、127.0.0.1等特殊IP地址；
- 关联实例选购IPv6高防IP后，支持选择IPv6高防IP，选择后支持配置IPv4或IPv6源站。IPv6高防暂不支持通过TTM获取用户IP；
- 转发策略包括轮询、最小连接数、源IP，以实现多源站的负载均衡。

### 2.新建HTTP/HTTPS防护业务

业务协议选择HTTP/HTTPS，端口选择HTTP/80、HTTP/443或自定义协议端口，然后填写回源IP和回源端口（源站提供服务的真实端口），最后选择转发策略。




**注意：**

- 选择为HTTPS时，相对于HTTP协议，会多出：
  HTTPS证书：用户可以选择已添加证书，也可以添加新的证书和申购SSL证书；
  HTTPS证书的TLS版本：设置证书TLS版本，支持1.0及以上、1.1及以上、1.2及以上和1.3，默认为1.0及以上；
  HTTPS回源协议：可设置HTTPS业务回源协议为HTTP，默认为HTTPS。
- 网站防护业务支持关联一个或多个高防IP防护实例下的单个或多个高防IP；
- 回源端口默认和业务端口保持一致，可自定义修改；

- 高防中心会将数据转发至源站，HTTPS/HTTPS防护业务支持IP源站或域名源站。IP源站最多配置50个，回源IP不能为私有、127.0.0.1等特殊IP地址；域名源站只能配置1个；
- IPv6高防暂不支持HTTP/HTTPS业务接入；
- 转发规则包括轮询、最小连接数，以实现多源站的负载均衡。

其他

配置健康检查屏蔽异常源站

查看流量报表

获取真实客户端IP

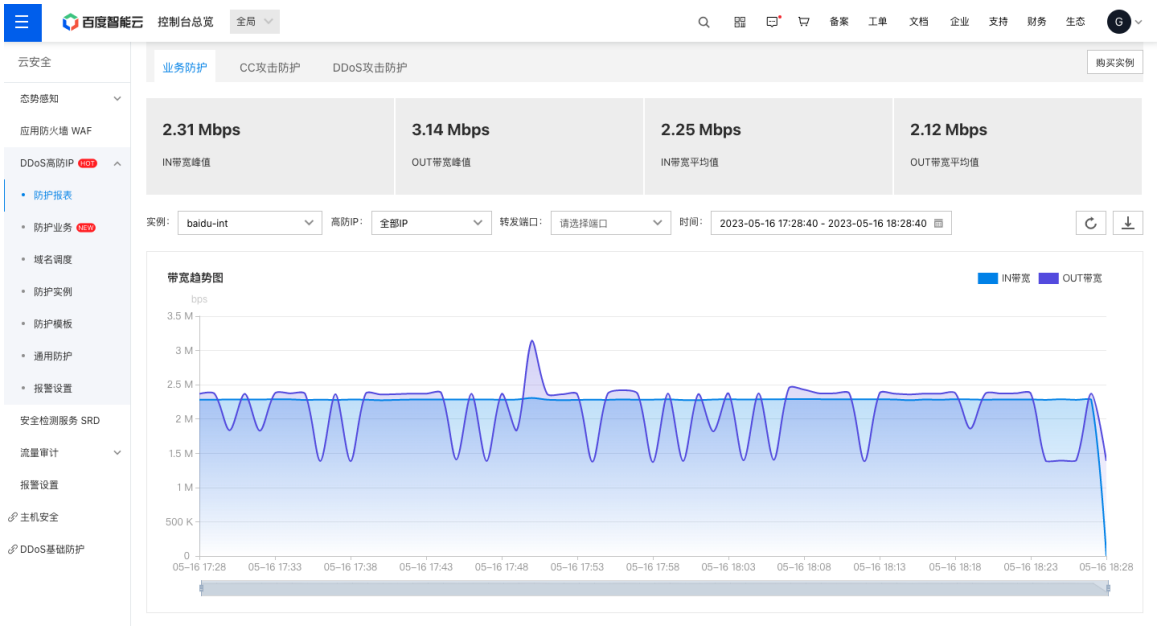
验证防护业务配置

自动或一键切入切出高防

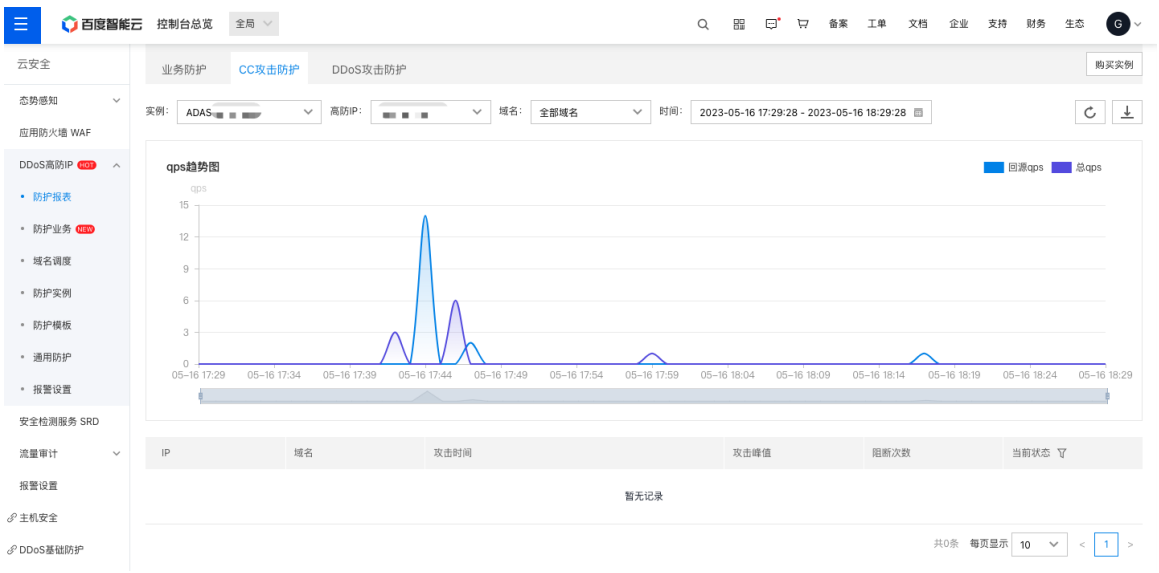
## 查看流量报表

百度智能云高防 IP 管理控制台的防护报表提供丰富的信息，可帮助用户快速了解当前业务或 DDoS 攻击情况。 当用户收到 DDoS 攻击提示或发现业务出现异常时，可通过防护报表快速了解当前攻击情况，包括被攻击域名、攻击持续时间、攻击流量大小、当前防护状态等。

**业务带宽报表** 查看某时刻的业务带宽情况，包括IN带宽峰值、OUT带宽峰值、IN带宽平均值、OUT带宽平均值




**CC攻击报表** 查看CC攻击情况，包括被攻击的高防IP、被攻击域名、攻击持续时间、攻击峰值、攻击类型及当前的防护状态。




**DDoS攻击报表** 查看DDoS攻击情况，包括被攻击的高防IP、攻击持续时间、攻击峰值、攻击类型及当前的防护状态。


# 最佳实践

## 获取真实客户端IP

1.网站接入（HTTP/HTTPS协议）

当接入高防防护服务后，网站服务器访问日志中的IP地址都将记录为高防防护的反向代理服务IP，无法取得客户端的真实IP地址。

为解决这个问题，我们在高防防护转发的HTTP头信息中增加了 X-Forwarded-For HEAD信息，记录的是请求过程中使用的代理IP列表，包括与我们代理直连的IP，WEB服务器日志或服务器程序就可以根据自己的方法来获取真实的客户端IP。

### 1.1.服务器日志类记录方法

- Nginx服务器

源站是Nginx搭建的服务器，配置文件中指定日志格式时使用$http_x_forwarded_for变量，相应的配置如下：

在nginx.conf中，配置log_format，定义访问日志记录的格式中用到$http_x_forwarded_for，示例如下：

```
 log_format   main  '$http_x_forwarded_for - $remote_user [$time_local] "$request" ''$status $body_bytes_sent "$http_referer" ''"$http_user_agent" ';
```

上述示例配置了main的日志模板，在日志记录指令中指定这个模板就可以输出。

- Apache服务器

源站是Apache服务器的，日志记录方案与nginx类似，配置指令不同，参考如下：

```
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
```

### 1.2.服务器程序类读取方法

防御过程中，我们透传客户端IP采用http的HEAD头，不同的服务器程序读取HEAD头的方式不一样，下面分别介绍常用程序的读取方法

- ASP程序

```
Request.ServerVariables("HTTP_X_FORWARDED_FOR")
```

- PHP

```
$_SERVER["HTTP_X_FORWARDED_FOR"]
```

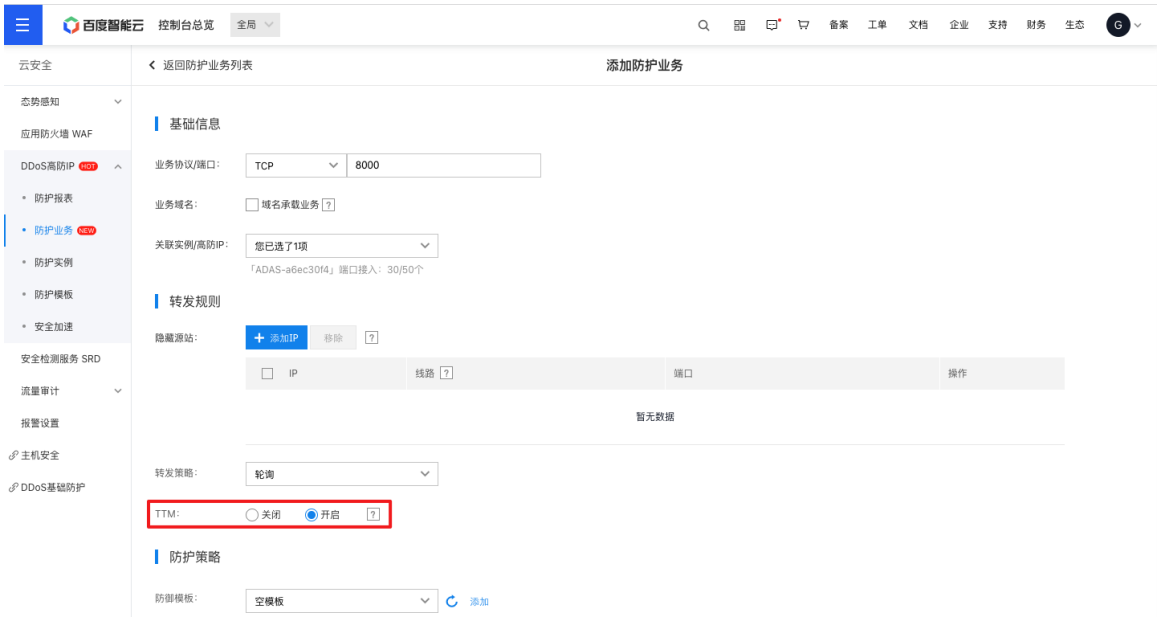
- JSP

```
request.getHeader("HTTP_X_FORWARDED_FOR")
```

## 2.端口接入（TCP协议）

对于TCP业务的源站需要加载TTM模块后才能获取到客户端真实源IP，您可以使用本文介绍的方法下载并安装TTM模块。

这种方式需要在防护业务中配置开启TTM功能（默认为开启）。配置路径：防护业务->编辑/添加 TCP协议防护业务。




### 2.1.TTM模块原理

客户端的数据包经过高防IP转发后，会将数据包的源地址和端口号，改成高防IP回源的地址和端口号。为了将客户端真实源IP和端口号发送给服务端，高防IP转发报文时会将客户端真实源IP和端口号添加到TCP报文的tcp option字段。源站加载TTM模块后，TTM模块通过hook Linux内核TCP协议栈的相关函数，从TCP报文的tcp option字段中解析出客户端真实源IP和端口号，详细描述如下：

1. Linux TCP协议栈在建连阶段收到客户端三次握手的ACK报文后，会调用tcp_v4_syn_recv_sock函数。TTM模块hook了tcp_v4_syn_recv_sock函数，hook后的tcp_v4_syn_recv_sock_ttm函数首先会调用原来的tcp_v4_syn_recv_sock函数，然后调用get_ttm_data_from_ack函数，从ACK报文的tcp option字段中，提取出客户端真实源IP和端口号，并存储在sock的

sk_user_data变量中，其中每条流对应一个sock。

2. 客户端应用程序在用户态调用getpeername或者accept接口时，最终都会调用到inet_getname函数，TTM模块hook了inet_getname函数，hook后的inet_getname_ttm函数首先会调用原有的inet_getname函数，然后判断sock中的sk_user_data变量是否为空，如果sk_user_data变量不为空则从该变量中提取出客户端真实源IP和端口号，替换原有inet_getname返回的高防IP回源地址和端口号，这样客户端应用程序调用getpeername或者accept接口获取到的就是客户端真实源IP和端口号。

### 2.2.TTM模块支持的操作系统

- Linux

> **注意**
>
> 1. 建议先在测试环境进行测试，待确认功能正常且运行稳定后再部署上线到正式环境。
> 2. TTM模块目前仅支持IPv4，且只支持64位操作系统。
> 3. 非TCP协议不支持获取客户端真实源IP和端口号。
> 4. 如果源站已经加载了类似的模块，hook了Linux协议栈的tcp_v4_syn_recv_sock和inet_getname函数，加载TTM模块后，会导致原有模块的功能不生效。
> 5. 七层业务（HTTP/HTTPS协议）可以在http header中直接通过X_forwarded_for字段来获取客户端真实源IP。

### 2.3.TTM模块安装步骤

1. 下载Linux对应版本的TTM模块，并进行加载

| 系统 | 版本号 | 下载地址 |
| --- | --- | --- |
| CentOS | 3.10.0-514.26.2.el7.x86_64 | https://sdk.bce.baidu.com/console-sdk/3.10.0-514.26.2.el7.zip |
| CentOS | 3.10.0-693.el7.x86_64 | https://sdk.bce.baidu.com/console-sdk/3.10.0-693.el7.zip |
| CentOS | 3.10.0-957.1.3.el7.x86_64 | https://sdk.bce.baidu.com/console-sdk/3.10.0-957.1.3.el7.zip |

```
 wget https://sdk.bce.baidu.com/console-sdk/3.10.xxx.zip
unzip 3.10.xxx.zip
cd 3.10.xxx
mv bce_ttm.ko /lib/modules/$(uname -r)/kernel/net/ipv4/
insmod /lib/modules/$(uname -r)/kernel/net/ipv4/bce_ttm.ko
```

> **注意：**
> 如果没有/lib/modules/$(uname -r)/kernel/net/ipv4/目录，也可以将bce_ttm.ko放在其它任意目录，以下操作步骤的路径也需要替换成bce_ttm.ko所在目录

2. 查看TTM模块加载情况

```
lsmod |grep bce_ttm
```

3. 如果需要机器重启后能自动加载TTM模块，可执行以下命令

```
echo 'insmod /lib/modules/$(uname -r)/kernel/net/ipv4/bce_ttm.ko' >> /etc/rc.local
```

4. 如果不再使用TTM模块，可以执行如下命令进行卸载

```
rmmod bce_ttm
```

**2.4.制作TTM模块**

如果TTM下载列表里没有对应Linux版本的TTM模块，也可以按照以下步骤手动制作TTM模块并进行加载。

1. 安装编译环境

```
yum -y install gcc kernel-headers kernel-devel
```

2. 下载bce_ttm模块源文件，并进行解压

```
wget -c "https://codeload.github.com/baidu/ttm/zip/master" -O bce_ttm.zip
unzip bce_ttm.zip
```

3. 编译TTM模块，编译后会在当前目录生成bce_ttm.ko文件

```
cd ttm-master/
make
```

4. 加载TTM模块，加载方法同TTM模块安装步骤

**2.5.特殊说明** 高防后端连接百度智能云BLB或者其他负载均衡器的情况，需要关闭BLB或者其他负载均衡设备的TOA模块（与高防的TTM冲突），同时要确保BLB或者其他负载均衡设备开启FULL NAT转发模式。

## 验证防护业务配置

在添加完防护业务，正式接入高防/分布防护前，建议在本地验证转发配置准确，避免非预期的接入。

详细验证方法如下：

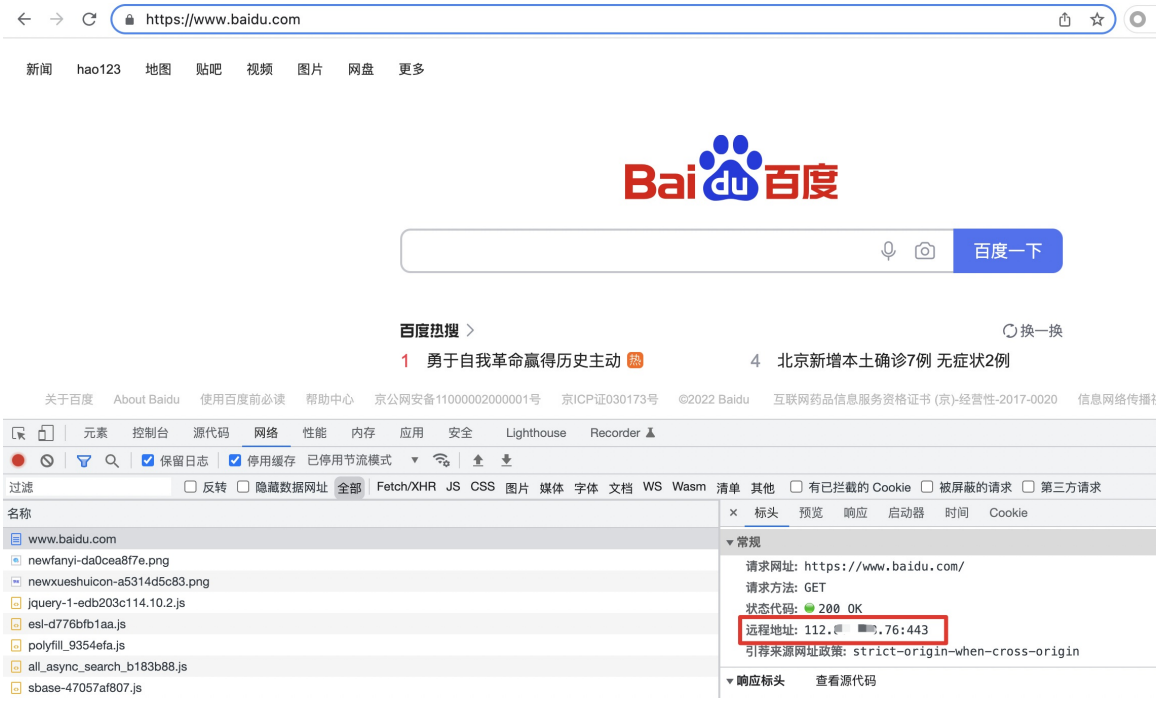
1.网站接入

**1.1.通过浏览器验证**

- 修改本地hosts文件，通常hosts文件路径：mac下/etc/hosts，windows下C:\windows\system32\drivers\etc\hosts
- 使用文本编辑器打开hosts文件，在最后一行添加：高防IP 防护网站域名，并保存文件。例如：112.xx.xx.76 www.baidu.com

```
127.0.0.1       localhost
255.255.255.255 broadcasthost
::1             localhost
112.[redacted].76 www.baidu.com
```

- 新打开一个浏览器（建议谷歌）访问测试域名。通过开发者工具，确认访问域名已绑定高防IP，并且测试页面内容符合预期。 ***如果依然是源站IP地址，请尝试刷新本地的DNS缓存（windows在命令提示符中运行ipconfig /flushdns命令，mac在终端中运行sudo dscacheutil -flushcache）***




> 注意：
>
> *HTTP和HTTPS网站需分别进行本地验证，全部符合预期方可正式接入。*

### 1.2.通过curl工具验证

- curl绑定高防IP，命令可参考（请将命令中的IP地址替换为实际的高防IP地址）：

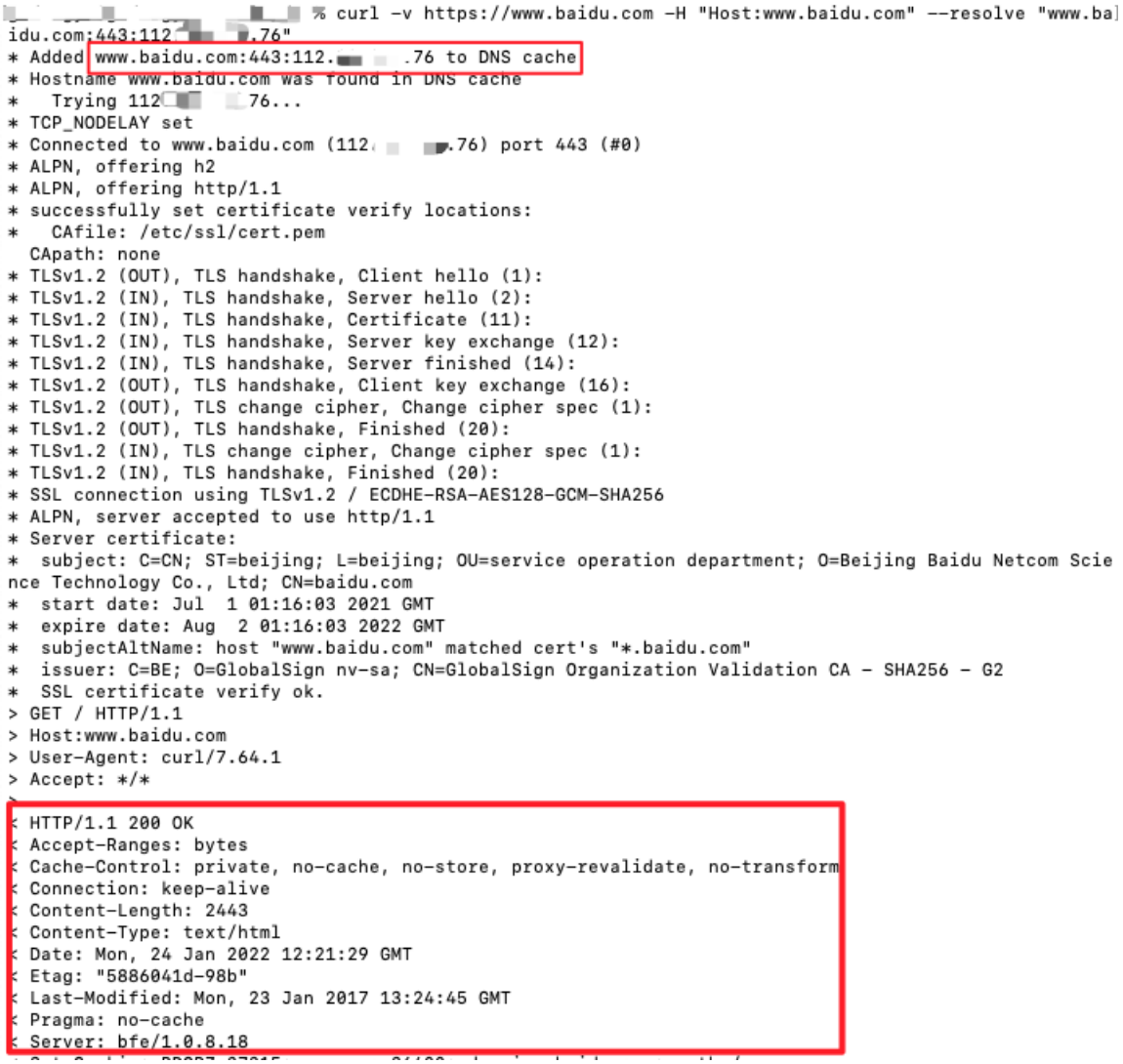
测试https：

```
curl -v https://www.baidu.com -H "Host:www.baidu.com" --resolve "www.baidu.com:443:112.xx.xx.76"
```

测试http：

```
curl -v http://www.baidu.com -H "Host:www.baidu.com" --resolve "www.baidu.com:80:112.xx.xx.76"
```

返回结果：



```
[redacted] % curl -v https://www.baidu.com -H "Host:www.baidu.com" --resolve "www.ba
idu.com:443:112.[redacted].76"
* Added www.baidu.com:443:112.[redacted].76 to DNS cache
* Hostname www.baidu.com was found in DNS cache
*   Trying 112.[redacted].76...
* TCP_NODELAY set
* Connected to www.baidu.com (112.[redacted].76) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/cert.pem
  CApath: none
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: C=CN; ST=beijing; L=beijing; OU=service operation department; O=Beijing Baidu Netcom Scie
nce Technology Co., Ltd; CN=baidu.com
*  start date: Jul  1 01:16:03 2021 GMT
*  expire date: Aug  2 01:16:03 2022 GMT
*  subjectAltName: host "www.baidu.com" matched cert's "*.baidu.com"
*  issuer: C=BE; O=GlobalSign nv-sa; CN=GlobalSign Organization Validation CA - SHA256 - G2
*  SSL certificate verify ok.
> GET / HTTP/1.1
> Host:www.baidu.com
> User-Agent: curl/7.64.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Accept-Ranges: bytes
< Cache-Control: private, no-cache, no-store, proxy-revalidate, no-transform
< Connection: keep-alive
< Content-Length: 2443
< Content-Type: text/html
< Date: Mon, 24 Jan 2022 12:21:29 GMT
< Etag: "5886041d-98b"
< Last-Modified: Mon, 23 Jan 2017 13:24:45 GMT
< Pragma: no-cache
< Server: bfe/1.0.8.18
```

- curl直接访问 ，命令可参考：

测试https：

```
curl -v https://www.baidu.com
```

测试http：

```
curl -v http://www.baidu.com
```

直接访问，返回结果：

```
[redacted] % curl -v https://www.baidu.com
*   Trying 112.[redacted].76...
* TCP_NODELAY set
* Connected to www.baidu.com (112.[redacted].76) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/cert.pem
  CApath: none
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: C=CN; ST=beijing; L=beijing; OU=service operation department; O=Beijing Baidu Netcom Sc:
nce Technology Co., Ltd; CN=baidu.com
*  start date: Jul  1 01:16:03 2021 GMT
*  expire date: Aug  2 01:16:03 2022 GMT
*  subjectAltName: host "www.baidu.com" matched cert's "*.baidu.com"
*  issuer: C=BE; O=GlobalSign nv-sa; CN=GlobalSign Organization Validation CA - SHA256 - G2
*  SSL certificate verify ok.
> GET / HTTP/1.1
> Host: www.baidu.com
> User-Agent: curl/7.64.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Accept-Ranges: bytes
< Cache-Control: private, no-cache, no-store, proxy-revalidate, no-transform
< Connection: keep-alive
< Content-Length: 2443
< Content-Type: text/html
< Date: Mon, 24 Jan 2022 12:19:19 GMT
< Etag: "5886041e-98b"
< Last-Modified: Mon, 23 Jan 2017 13:24:46 GMT
< Pragma: no-cache
< Server: bfe/1.0.8.18
```

- 确认直接访问和绑定高防IP访问返回内容一致。

> 注意：
>
> *HTTP和HTTPS网站需分别进行本地验证，全部符合预期方可正式接入。*

2.端口接入

**2.1.绑定域名解析为高防IP**

- 修改本地hosts文件，内容同1.1
- 在本地计算机终端中对防护的域名运行Ping命令。***预期解析到的IP地址是在hosts文件中绑定的高防IP地址。如果依然是源站地址，请尝试刷新本地的DNS缓存（windows在命令提示符中运行ipconfig /flushdns命令，mac在终端中运行sudo dscacheutil -flushcache）***
- 确认本地解析已经切换到高防IP以后，使用原来的域名进行测试，如果能正常访问则说明配置已经生效。

**2.2.直接访问高防IP**

- 使用高防IP访问服务，假设高防IP是112.xx.xx.76，高防防护端口为443。
- 通过telnet命令访问高防IP：112.xx.xx.76的443端口。***命令参考（请将命令中的IP地址替换为实际的高防IP地址）：***

```
telnet 112.xx.xx.76 443
```

```
[ [redacted] ~ % telnet 112 [redacted].76 443 ]
Trying 112 [redacted].76...
Connected to www.baidu.com.
Escape character is '^]'.
```

- telnet命令能连通则说明转发成功

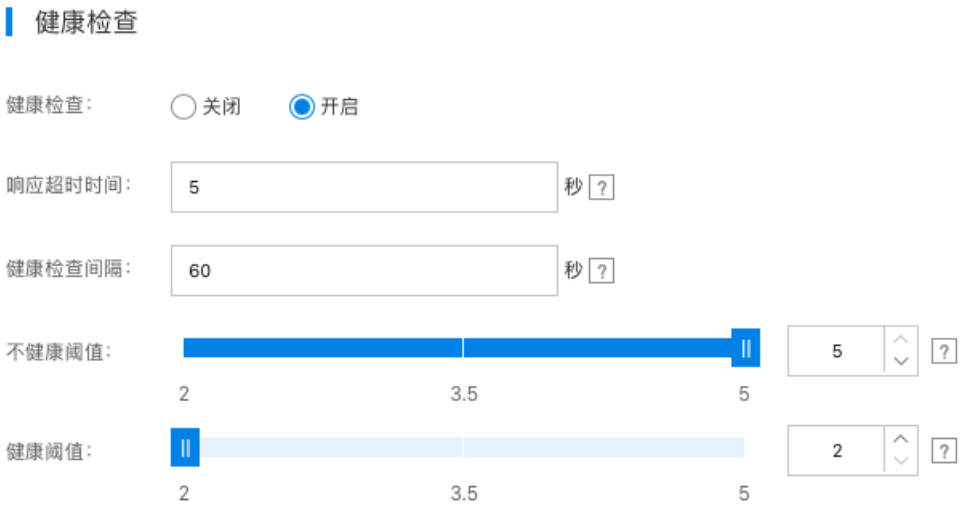
## 配置健康检查屏蔽异常源站

### 1.背景

DDoS高防防护通过反向代理的方式为客户提供高防防护服务，具备海量防御带宽的同时可以隐藏真实源站。用户的请求首先到达高防，由高防清洗掉攻击以及其他异常请求后将正常的用户请求转发到源站。在向源站转发时，支持配置源站健康检查策略，对健康检查判断为异常的源站不进行转发，以保障客户业务正常响应。

### 2.网站防护业务配置健康检查

配置路径：在“DDoS高防IP”左侧导航选择“防护业务”->编辑已添加的网站或添加新的网站




| 配置项 | 描述 |
| --- | --- |
| 健康检查 | 源站健康检查开关，网站防护业务默认为关闭 |
| 响应超时时间 | 超过设置时间源站未响应，该次检查判定为失败，支持1-60间整数，默认为5秒 |
| 检查检查间隔 | 源站健康检查的频率，支持20-120间整数，默认为60秒 |
| 不健康/健康阈值 | 连续超过这个阈值将被判定为异常或正常。判定为异常后将不在进行回源转发，直到恢复正常 |

### 3.端口防护业务配置健康检查

端口防护业务健康检查为强制开启，不能关闭。***为保障业务可正常提供服务，建议端口业务配置多个源站。***详细配置内容如下：

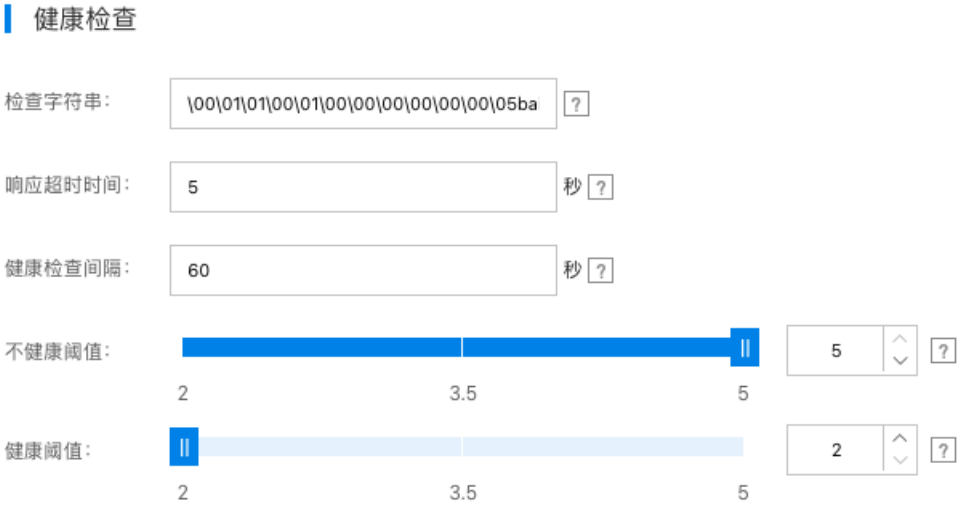
#### 3.1.TCP协议

配置路径：在“DDoS高防IP”左侧导航选择“防护业务”->编辑已添加的TCP协议端口业务或添加新的

配置项与网站相同，详细请查看网站健康检查配置项描述。

#### 3.2.UDP协议

配置路径：在“DDoS高防IP”左侧导航选择“防护业务”→编辑已添加的UDP协议端口业务或添加新的




| 配置项 | 描述 |
| --- | --- |
| 检查字符串 | 高防采用给源站发送带有用户指定字符串的UDP包实现健康检查，如果后端服务器运行正常，则能够接收高防的健康检查包并给予返回。高防服务接收到了后端服务器返回的UDP包，就认为其是健康的。<br>为了表达方便，检查字符串统一用16进制来表示，如果载荷里有ASCII字符，也可以用ASCII字符来替代相应内容。<br>默认值为baidu.com（00\01\01\00\01\00\00\00\00\00\00\05baidu\03com\00\00\01\00\01） |

其他配置项与网站相同，详细请查看网站健康检查配置项描述。

## 自动或一键切入切出高防

### 1.背景

DDoS高防支持CNAME记录、A记录和直连高防三种接入方式。CNAME和A记录接入，需要在域名服务商处将需要接入的业务域名解析指向分配的高防CNAME或高防IP完成，直连接入通常使用在端类业务上。切入切出高防、资源变更等场景，需要跨多个平台操作存在极大的不便利。特别在非常态接入高防的情况下，遭受DDoS攻击公开源站已经中断服务，手动（非百度云源站的情况下）操作切入高防，在防御的时效上无法有效保证。

### 2.域名调度功能

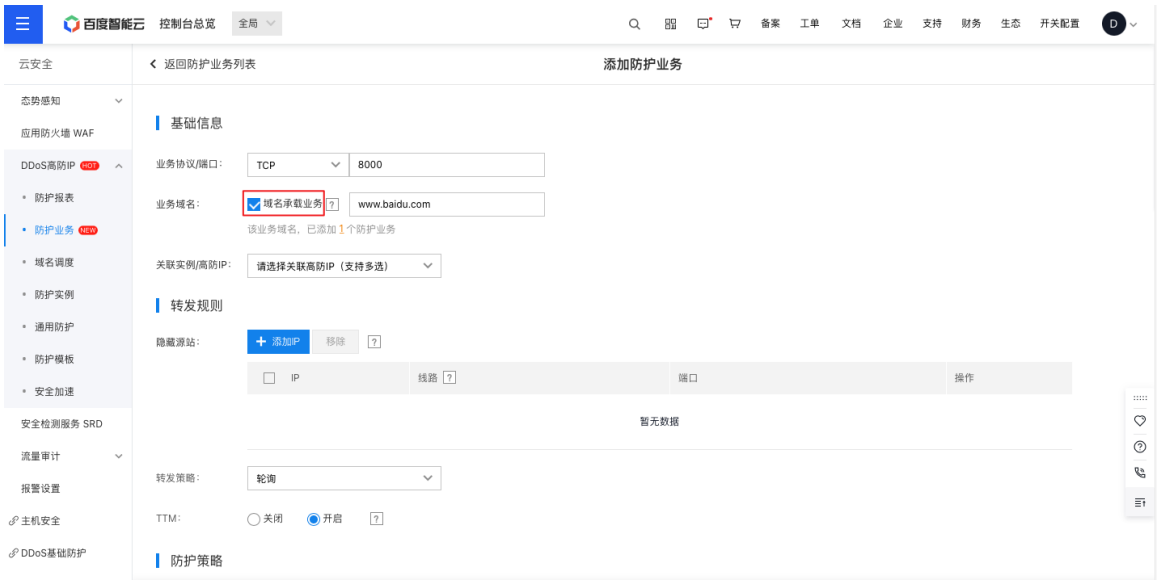
DDoS高防深度洞察用户使用场景，支持域名调度功能。实现常态访问公开源站提升覆盖性、减少业务带宽成本，在公开源站被攻击或故障时，能够自动或一键切入高防，增加使用的便捷性、提升切入时效。


适用场景

无攻击/故障时，DDoS高防做备用。被攻击或不可用时，一键/自动切入DDoS高防

### 3.创建可调度域名

除了HTTP/HTTPS协议外TCP或UDP协议，同样支持域名调度功能。需要在添加TCP或UDP协议防护业务时，勾选域名承载业务，并填写对应的业务域名。对有业务域名的防护业务，将自动完成调度域名的识别。

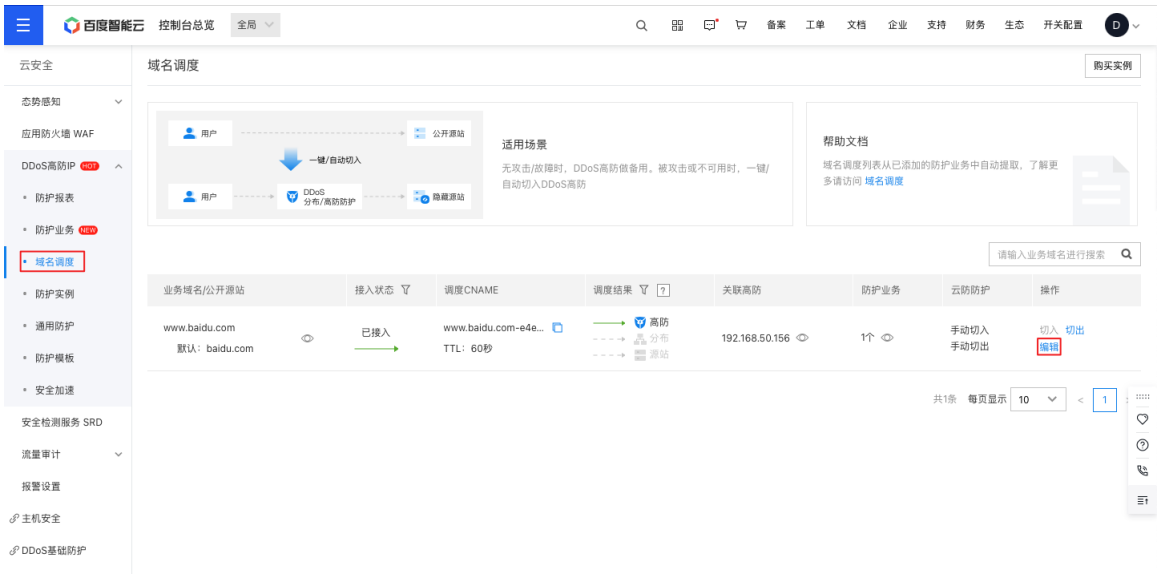


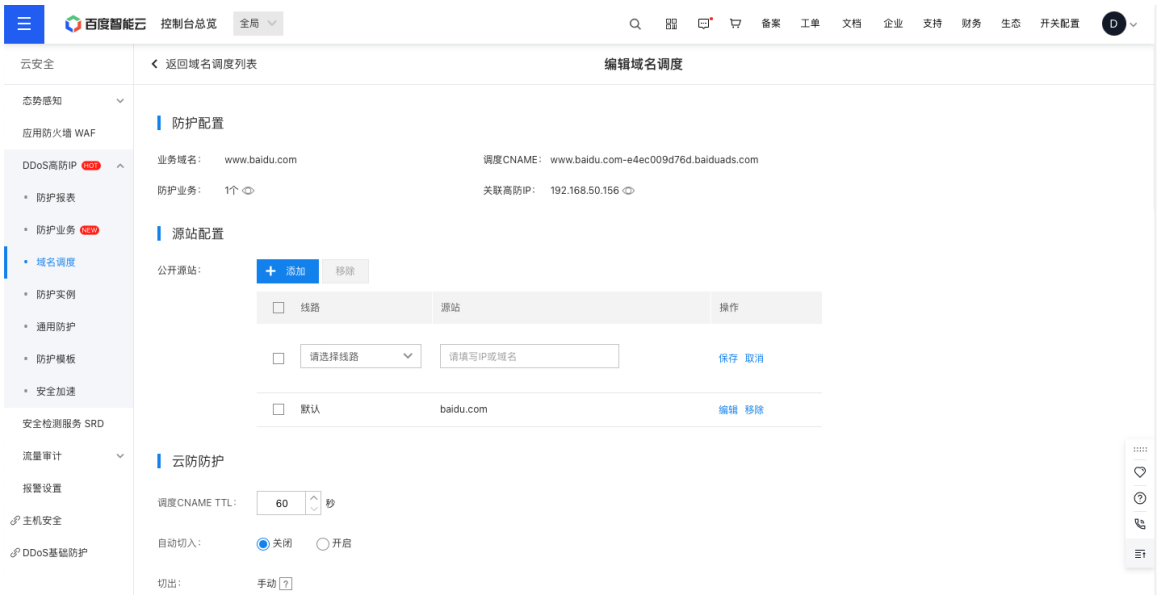

> **注意：**
>
> - 同一业务域名，将分配相同的高防CNAME，需关联相同的实例或高防IP；

### 4.确认和设置公开源站

完成有业务域名的防护业务添加后，将自动创建可调度的域名，并识别业务域名当前配置的公开源站。因可能存在分区解析而无法完整识别公开源站的情况，需要用户确认和设置业务域名对应的公开源站，以保证接入后可准确的实现一键切出。

设置路径：域名调度->点击对应业务域名操作中的编辑





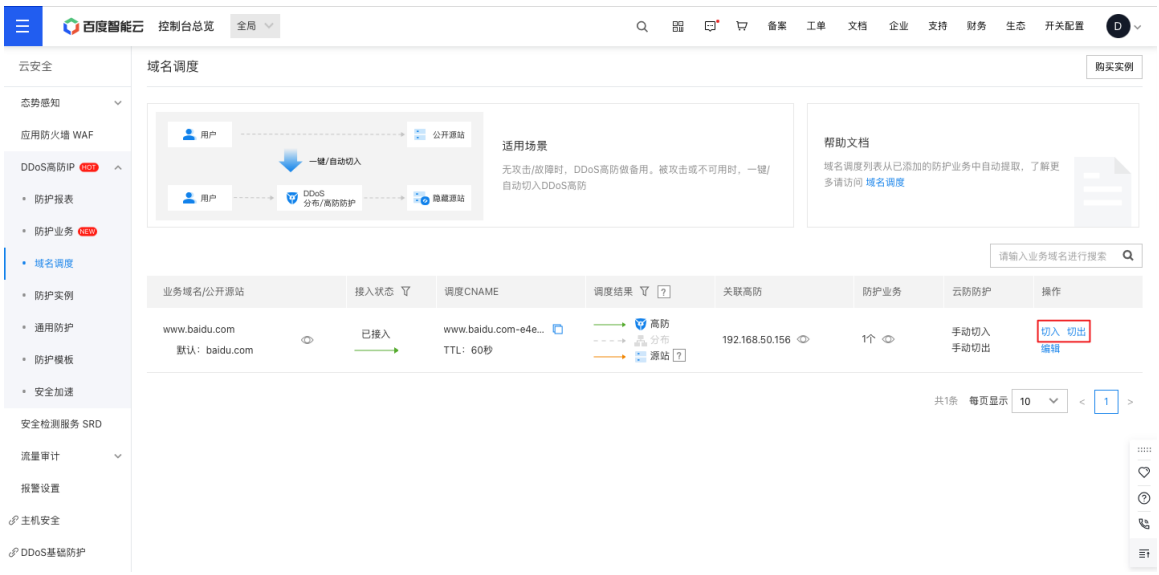

| 配置项 | 描述 |
| --- | --- |
| 线路 | 公开源站覆盖的运营商线路，支持电信、联通、移动、教育和默认 |
| 源站 | 支持IP和域名源站，同一线路仅可选择一种 |

> **注意：**
>
> - 公开源站必须设置默认线路，同一线路仅支持一个域名源站；
> - 操作切出到源站后，业务域名对应的高防CNAME将根据配置的公开源站，创建指向源站的解析记录。
> - **调度CNAME，高防实例默认指向高防IP，分布防护实例默认指向分布节点。在正式接入前，需确认默认指向是否满足需求，如果期望默认指向源站请先操作切出到源站并确认解析生效后，再完成接入。**

### 5.自助切入/切出

在完成接入后，可通过域名调度实现一键的切入和切出。

操作路径：域名调度->点击对应业务域名操作中的切入/切出。

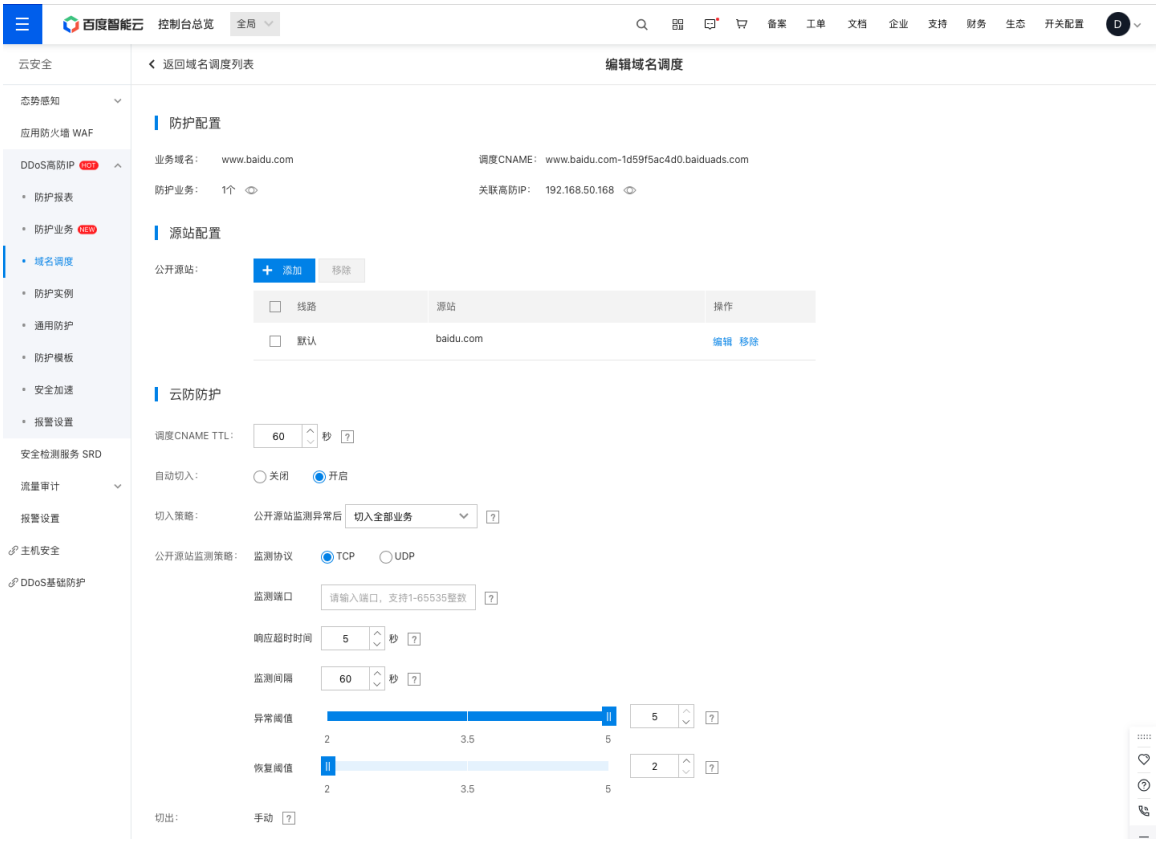


| 操作项 | 描述 |
| --- | --- |
| 切入 | 指从源站切入分布或高防节点，从分布节点切入高防节点，支持：<br>全部切入，将调度CNAME全部指向对应的节点；<br>部分切入-指定线路，匹配选择的线路，将调度CNAME分线路指向对应的节点；<br>部分切入-指定源站，根据公开源站配置的线路，将调度CNAME分线路指向对应的节点。 |
| 切出 | 指从高防或分布节点切出到源站，从高防节点切出到分布节点，支持：<br>全部切出，将调度CNAME全部指向对应的节点或公开源站；<br>部分切出：匹配选择的线路，将调度CNAME分线路指向对应的节点或公开源站。 |

> **注意：**
>
> - 有识别或配置过公开源站，才能操作切入、切出；
> - 仅分布防护实例支持分布节点，分布防护实例仅支持全部切入；

6.设置自动切入等策略

设置路径：域名调度->点击对应业务域名操作中的编辑



| 配置项 | 描述 |
| --- | --- |
| 调度CNAME TTL | 设置高防调度CNAME，在DNS服务上的缓存时间。支持60～300间的整数，建议设置为60秒。 |
| 切入策略 | 在监测公开源站不可用时，自动切入云高防策略，支持，<br>切入全部业务，将调度CNAME解析全部指向云高防；<br>仅切入不可用源站，仅将不可用公开IP/域名源站对应的线路指向修改到云高防。 |
| 公开源站监测策略 | 设置公开源站健康检查策略，在健康检查异常后根据切入策略配置，将调度CNAME解析修改到高防IP完成自动切入。包括：<br>监测协议和端口，用于对公开源站进行健康检查的协议+端口，高防基于配置进行持续探测。如果是HTTP或HTTPS网站，可对应设置TCP协议的80或433端口；<br>响应超时时间，支持1～60间的整数，建议设置为5秒，超过设置阈值未响应将被判定为一次健康检查异常；<br>监测间隔，健康检查的间隔时间，支持20～120间的整数，建议设置为60秒；<br>异常阈值，连续健康检查失败次数，超过这个阈值源站将被认定为故障，执行自动切入；<br>恢复阈值，连续健康检查成功次数，超过这个阈值源站将被认定为从故障中恢复。 |

> **注意：**
>
> - 因攻击发生的不确定性，切出需手动操作；

## 通过BLS获取高防七层日志

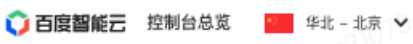
DDoS高防联合BLS为用户提供高防七层日志的存储和分析功能，要获取高防七层日志，需要以下三个步骤：

1.开通BLS服务；

2.创建BLS日志集；

3.通知高防客服进行配置。

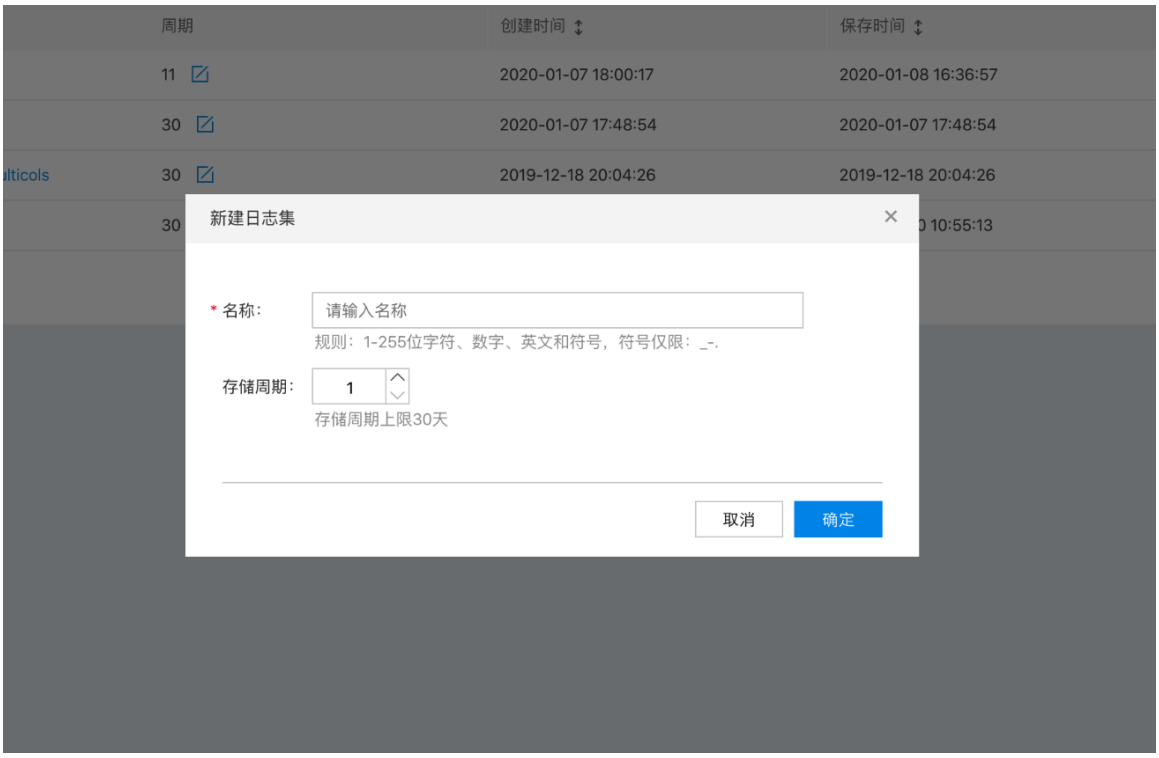
### 开通BLS服务

日志服务BLS是一站式实时日志分析服务，提供日志数据采集传输、检索分析、实时消费与转储等功能，帮助用户轻松应对运维管理、商业趋势洞察、安全监控审计等业务场景。 访问 https://cloud.baidu.com/product/bls.html 点击立即使用，选择区域***华北-北京***，完成开通。 


### 创建BLS日志集

开通完BLS服务后，需要创建一个名为 "adas-log"的日志集，进行高防七层日志的传输。

1. 登录百度智能云官网，点击右上角的“管理控制台”，进入控制台界面。
2. 选择“产品服务>日志服务BLS”，进入“日志集”页面。
3. 点击“新建日志集”，弹出新建日志集页面，填写配置信息 ，名称**必须**填写adas-log。存储周期根据需求自定义。




更多参考：https://cloud.baidu.com/doc/BLS/s/5k5ao6rxj

通知高防客服

通过创建工单的方式联系高防客服进行配置

> ***注意：***
>
> 默认开通全部高防IP，如您仅需获取指定高防IP的7层日志请在工单中说明

## EIP被攻击联动高防防护

1.背景

百度智能云EIP免费提供最大5Gbps的基础DDoS防护能力，当EIP被攻击超过基础防护阈值后，EIP将会被执行封禁，导致业务服务中断。

针对此场景EIP联合高防建设联动防护功能，在EIP被攻击执行封禁时自动切入高防防护，提升客户防御DDoS攻击能力，减少业务中断风险。

联动防护功能需要在「高防控制台-EIP联动防护」中进行配置，包括：

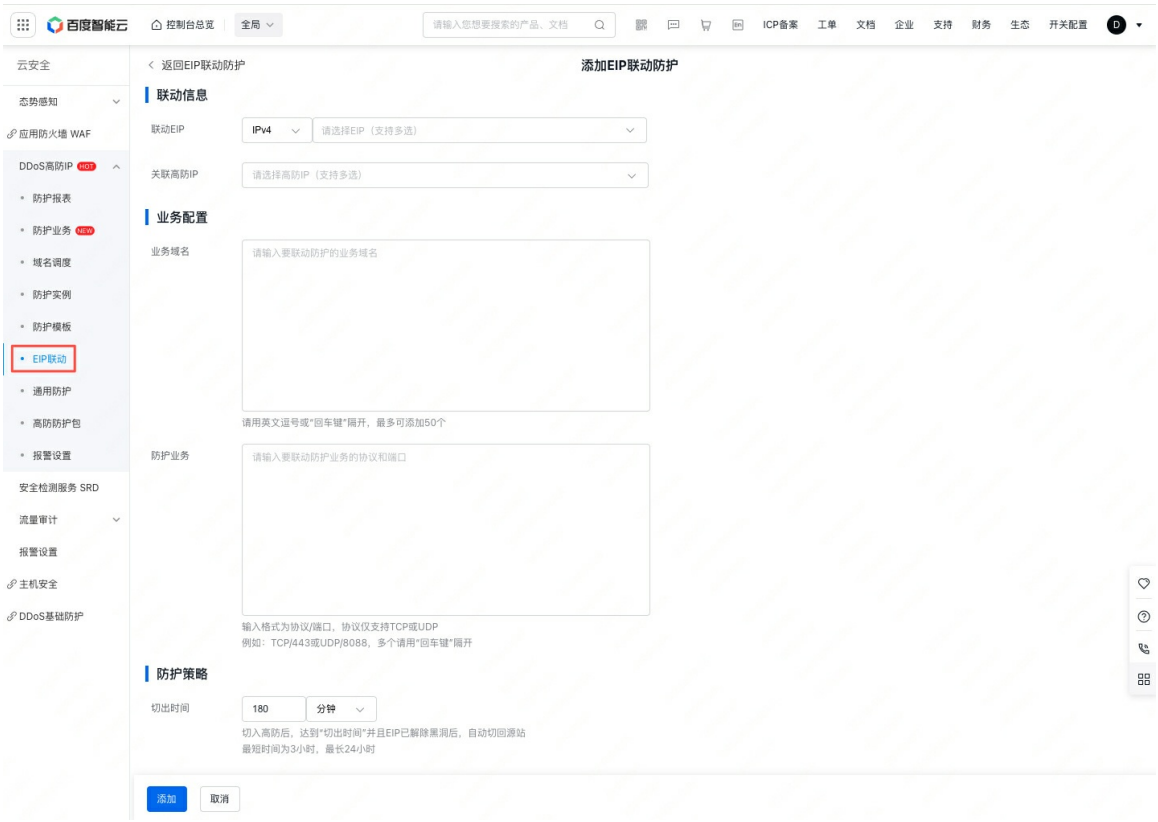
- 添加EIP联动
- 接入防护
- 切入/切出防护

2.添加EIP联动

**前提条件：已购买EIP和DDoS防护服务**

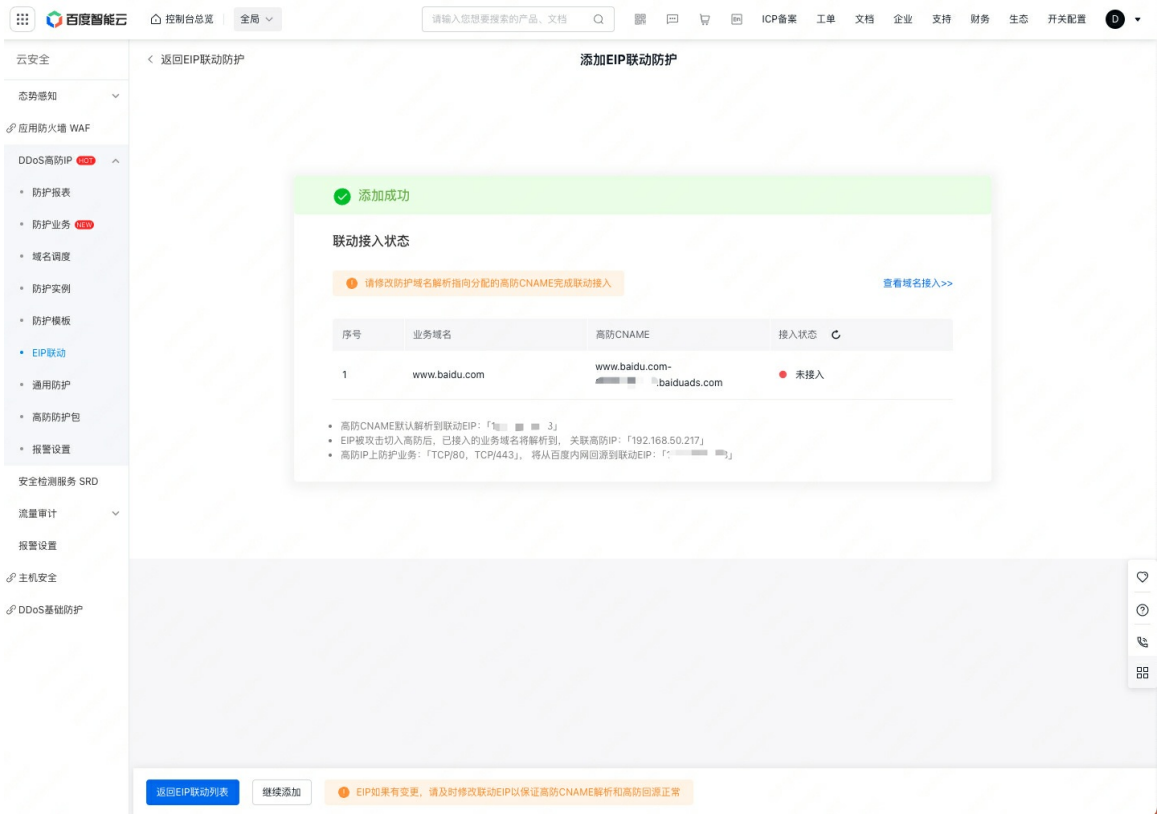
1. 登录百度智能云官网，点击右上角的“管理控制台”，进入控制台界面；
2. 选择“产品服务>DDoS防护服务”，进入“EIP联动”页面；
3. 点击“添加”联动防护，进入添加联动防护页面，完成配置。

| 配置项 | 描述 |
| --- | --- |
| 联动EIP | 账号下已购买的EIP，可以同时选择多个，IPv4和v6需要分别配置 |
| 关联高防IP | 联动防护需要关联的高防IP，可以同时关联多个。v4或v6的EIP仅能分别关联v4或v6的高防IP |
| 业务域名 | 选择EIP上业务对应的域名，最多可添加50个 |
| 防护业务 | 选择EIP上需要进行防护的业务，格式为协议/端口，协议仅支持TCP或UDP，例如：TCP/443或UDP/8088，多个请用“回车键”隔开 |
| 切出时间 | 切入高防后，达到“切出时间”并且EIP已解除封禁/黑洞后，自动切回源站。最短时间为3小时，最长24小时 |




### 3.接入防护

添加/编辑联动防护后，根据引导页面提示，前往域名服务商将业务域名解析修改为高防CNAME完成接入。

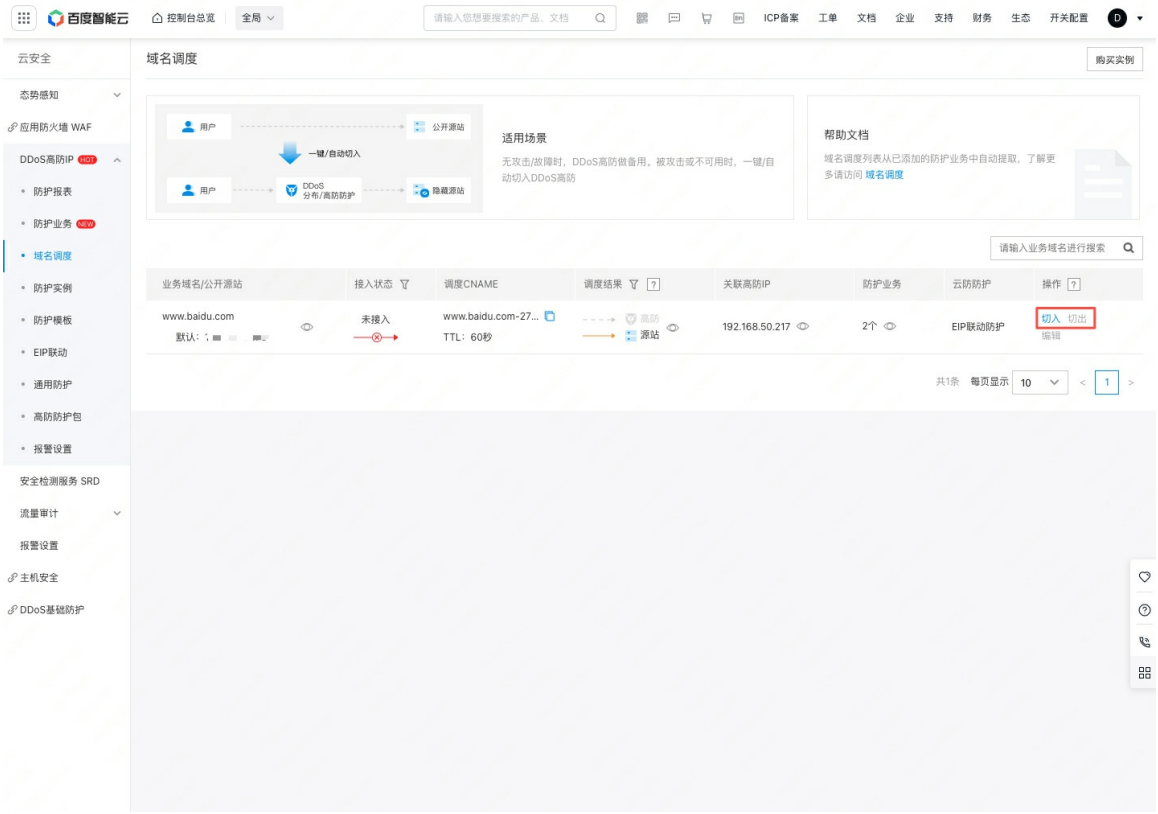



> **注意：**
>
> - 高防CNAME默认解析到联动EIP；EIP被攻击切入高防后，已接入的业务域名将解析到关联高防IP；高防IP上防护业务将从百度内网回源到联动的EIP。
> - ***EIP如果有变更，请及时修改联动EIP以保证高防CNAME解析和高防回源正常。***

4.切入/切出防护

完成联动防护配置并修改业务域名解析指向高防CNAME后，即具备了EIP被攻击导致封禁后自动切入/切出高防，以及手动切入/切出高防能力。

手动切入/切出防护操作路径：进入DDoS高防IP控制台-域名调度>点击对应业务域名操作中的切入或切出




> **注意：**
>
> - 手动切入高防防护的域名，不会进行自动切出，即只能手动操作切出防护。

# API参考

## 自有高防调度API参考

### 概述

#### 简介

自有高防调度，是指用自有高防实例为遭受攻击的IP进行DNS调度。首先，用户在百度智能云管理控制台购买高防实例，并配置好转发规则；在IP遭受攻击时，用户手动调用触发调度接口，将流量调度到高防机房，经高防机房清洗攻击流量后，根据已有高防实例配置好的转发规则，将正常流量回源到指定目标；攻击结束时，用户手动调用解除调度动作接口，流量正常到达IP。该场景配置时，需要指定调度IP、private区域、高防实例。

如果您是初次调用百度智能云产品的API，可以观看API入门视频指南，快速掌握调用API的能力。

#### 服务域名

产品是全局产品，服务域名为adas.baidubce.com。

#### 通用说明

API调用遵循HTTP协议，数据交换格式为JSON，所有request/response body内容均采用UTF-8编码。URL参数中所使用的IP均使用点分十进制表示。

#### API认证机制

所有API的安全认证一律采用Access Key与请求签名机制。 Access Key由Access Key ID和Secret Access Key组成，均为字符串。 对于每个HTTP请求，使用下面所描述的算法生成一个认证字符串。提交认证字符串放在Authorization头域里。服务端根据生成算法验证认证字符串的正确性。 认证字符串的格式为`bce-auth-v{version}/{accessKeyId}/{timestamp}/{expirationPeriodInSeconds}/{signedHeaders}/{signature}`。

- version是正整数。
- timestamp是生成签名时的UTC时间。
- expirationPeriodInSeconds表示签名有效期限。
- signedHeaders是签名算法中涉及到的头域列表。头域名之间用分号（;）分隔，如host;x-bce-date。列表按照字典序排列。（本API签名仅使用host和x-bce-date两个header）
- signature是256位签名的十六进制表示，由64个小写字母组成。

当百度智能云接收到用户的请求后，系统将使用相同的SK和同样的认证机制生成认证字符串，并与用户请求中包含的认证字符串进行比对。如果认证字符串相同，系统认为用户拥有指定的操作权限，并执行相关操作；如果认证字符串不同，系统将忽略该操作并返回错误码。

鉴权认证机制的详细内容请参见鉴权认证。

**幂等性**

当调用某些接口时如果遇到了请求超时或服务器内部错误，用户可能会尝试重发请求，这时用户通过clientToken参数避免创建出比预期要多的资源，即保证请求的幂等性。

幂等性基于clientToken，clientToken是一个长度不超过64位的ASCII字符串，通常放在query string里，如`http://bcc.bj.baidubce.com/v1/instance?clientToken=be31b98c-5e41-4838-9830-9be700de5a20`。

如果用户使用同一个clientToken值调用创建接口，则服务端会返回相同的请求结果。因此用户在遇到错误进行重试的时候，可以通过提供相同的clientToken值，来确保只创建一个资源；如果用户提供了一个已经使用过的clientToken，但其他请求参数（包括queryString和requestBody）不同甚至url Path不同，则会返回IdempotentParameterMismatch的错误代码。

clientToken的有效期为24小时，以服务端最后一次收到该clientToken为准。也就是说，如果客户端不断发送同一个clientToken，那么该clientToken将长期有效。

**日期与时间规范**

日期与时间的表示有多种方式。为统一起见，除非是约定俗成或者有相应规范的，凡需要日期时间表示的地方一律采用UTC时间，遵循ISO 8601，并做以下约束：

1. 表示日期一律采用YYYY-MM-DD方式，例如2014-06-01表示2014年6月1日
2. 表示时间一律采用hh:mm:ss方式，并在最后加一个大写字母Z表示UTC时间。例如23:00:10Z表示UTC时间23点0分10秒。
3. 凡涉及日期和时间合并表示时，在两者中间加大写字母T，例如2014-06-01T23:00:10Z表示UTC时间2014年6月1日23点0分10秒。

**请求参数**

请求参数包括如下4种：

| 参数类型 | 说明 |
| --- | --- |
| URI | 通常用于指明操作实体,如:PUT /v1/schedule/{scheduleId} |
| Query参数 | URL中携带的请求参数 |
| HEADER | 通过HTTP头域传入,如:x-bce-date |
| Requestbody | 通过JSON格式组织的请求数据体 |

**返回值说明**

返回值分为两种形式：

| 返回内容 | 说明 |
| --- | --- |
| HTTP STATUS CODE | 如200,400,403,404等 |
| ResponseBody | JSON格式组织的响应数据体 |

**公共请求头**

下表列出了所有AdasSchedule API所携带的公共头域。HTTP协议的标准头域不在此处列出

| 头域（HEADER） | 是否必须 | 说明 |
| --- | --- | --- |
| Authorization | 是 | 包含Access Key与请求签名 |
| Content-Type | 是 | application/json; charset=utf-8 |
| x-bce-date | 否 | 表示日期的字符串，符合BCE API规范 |

**公共响应头**

下表列出了所有AdasSchedule API的公共响应头域。HTTP协议的标准响应头域不在此处列出

| 头域（HEADER） | 说明 |
| --- | --- |
| Content-Type | 只支持JSON格式，application/json; charset=utf-8 |
| x-bce-request-id | AdasSchedule后端生成，并自动设置到响应头域中 |

**错误码**

请求发生错误时通过respone body返回详细错误信息，遵循如下格式：

| 参数名 | 类型 | 说明 |
| --- | --- | --- |
| code | String | 错误码 |
| message | String | 错误描述 |
| requestId | String | 本次请求的requestId |

示例：

```
 {
 "requestId" : "ae2225f7-1c2e-427a-a1ad-5413b762957d",
 "code" : "NoSuchKey",
 "message" : "The resource you requested does not exist"
}
```

**公共错误码**

| 错误码 | 消息 | HTTP状态码 | 语义 |
| --- | --- | --- | --- |
| AccessDenied | Access denied. | 403 Forbidden | 无权限访问对应的资源 |
| InappropriateJSON | The JSON you provided was well-formed and valid, but not appropriate for this operation. | 400 Bad Request | 请求中的JSON格式正确，但语义上不符合要求。如缺少某个必需项，或者值类型不匹配等。出于兼容性考虑，对于所有无法识别的项应直接忽略，不应该返回这个错误。 |
| InternalE | We encountered an internal error. Please try again. | 500Internal | 所有未定义的其他错误。在有明确对应的其他类型的错误时（包括通用的和服务自定义的）不应该使 |

| | | | |
|---|---|---|---|
| rror | | Server Error | 用。 |
| InvalidAccessKeyId | The Access Key ID you provided does not exist in our records. | 403 Forbidden | Access Key ID不存在 |
| InvalidHTTPAuthHeader | The HTTP authorization header is invalid. Consult the service documentation for details. | 400 Bad Request | Authorization头域格式错误 |
| InvalidHTTPRequest | There was an error in the body of your HTTP request. | 400 Bad Request | HTTP body格式错误。例如不符合指定的Encoding等 |
| InvalidURI | Could not parse the specified URI. | 400 Bad Request | URI形式不正确。例如一些服务定义的关键词不匹配等。对于ID不匹配等问题，应定义更加具体的错误码，例如NoSuchKey。 |
| MalformedJSON | The JSON you provided was not well-formed. | 400 Bad Request | JSON格式不合法 |
| InvalidVersion | The API version specified was invalid. | 404 Not Found | URI的版本号不合法 |
| OptInRequired | A subscription for the service is required. | 403 Forbidden | 没有开通对应的服务 |
| PreconditionFailed | The specified If-Match header doesn't match the ETag header. | 412 Precondition Failed | 详见ETag |
| RequestExpired | Request has expired. Timestamp date is XXX. | 400 Bad Request | 请求超时。XXX要改成x-bce-date的值。如果请求中只有Date，则需要将Date转换为datetime。 |
| IdempotentParameterMismatch | The request uses the same client token as a previous, but non-identical request. | 403 Forbidden | clientToken对应的API参数不一样。 |
| SignatureDoesNotMatch | The request signature we calculated does not match the signature you provided. Check your Secret Access Key and signing method. Consult the service documentation for details. | 400 Bad Request | Authorization头域中附带的签名和服务端验证不一致 |

**AdasSchedule业务错误码**

| 错误码 | 错误描述 | HTTP状态码 | 语义 |
| --- | --- | --- | --- |
| ScheduleInstanceNotFound | The specified schedule instance does not exist. | 404 | 调度实例不存在 |
| UnsupportedScheduleInstanceOperation | The status of specified schedule instance does not support this operation. | 400 | 指定的调度实例状态不支持此类型操作 |
| AdasInstanceIsInvalid | The specified adas instance is invalid. | 400 | 高防实例不合理 |
| ScheduleNatAlreadyExist | The specified schedule nat already exist. | 400 | 调度nat已经存在 |
| ScheduleNatNotFound | The specified schedule nat does not exist. | 404 | 调度nat不存在 |
| VpcInstanceNotFound | The specified vpc instance does not exist. | 404 | vpc实例不存在 |
| NatInstanceNotFound | The specified nat instance does not exist. | 404 | nat实例不存在 |

**名词解释**

下表列出了所有AdasSchedule API的涉及到的关键名词及解释。

| 名词 | 解释 |
| --- | --- |
| 调度实例IP | 需要配置调度服务的IP，为用户自有IP |
| 高防实例IP | 用户预先配置的高防实例IP |
| 高防回源IP | 调度发生后，高防回源到用户后端服务器的流量的源IP |
| 高防调度域名 | 正常情况下，解析到调度实例IP；调度发生后，解析到高防实例IP |

调度实例相关接口

**创建调度实例**

- 描述

创建一个调度实例，用于绑定调度的IP。

需要开启两个白名单：AdasAutoSchedule（高防自动化调度）和 RouteOpenSourceAddress（自定义路由白名单）。

创建调度实例需要实名认证，若未通过实名认证可以前往百度开放云官网控制台中的安全认证下的实名认证中进行认证。

- 请求语法

  POST /v{version}/schedule?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| scheduleId | String | 创建的调度实例id |

**请求示例**

```
 POST /v1/schedule?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
    "scheduleId":"sche-12345678"
}
```

**配置调度实例**

- 描述

只有在调度实例正常状态下，才能进行配置，即调度实例的status必须是normal。

需要指定scheduleIp，region，adasId。其中，region如果为private，表示scheduleIp只能手动调度，否则，表示scheduleIp既可以手动调度，又可以使用该region触发自动化调度；adasId必须为用户可使用的高防短ID。

- 请求结构

  PUT /v{version}/schedule/private/{scheduleId}?action={action}&clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

  { "scheduleIp": "182.61.1.1", "region": "private", "adasId": "adas-5e501b83", }

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| scheduleId | String | 是 | Query参数 | 调度实例ID |
| action | String | 是 | Query参数 | 对实例执行的动作，本接口中该参数取值update |
| clientToken | String | 是 | Query参数 | 幂等性Token |
| scheduleIp | String | 是 | RequestBody参数 | 配置调度实例IP：用户自己的IP |
| region | String | 是 | RequestBody参数 | 调度区域 |
| adasId | String | 是 | RequestBody参数 | 用户自有的高防实例ID |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

无特殊返回参数

**请求示例**

```
 PUT /v1/schedule/private/sche-1234abcd?action=update&clientToken=be31b98c-5e41-4838-9830-9be700de5a20
HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "scheduleIp": "182.61.1.1",
    "region": "private",
    "adasId": "adas-5e501b83",
}
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
```

**查询调度实例列表**

- 描述

可以指定scheduleIp，region，status，查询指定条件的调度实例的列表。

region必须为private。

根据status字段，可以查询处于不同调度状态下的调度实例。

- 请求语法

  GET /v{version}/schedule?scheduleIp={scheduleIp}®ion={region}&clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| scheduleIp | String | 否 | Query参数 | 要查询的调度实例IP，点分十进制 |
| region | String | 是 | Query参数 | 查询的区域 |
| status | String | 否 | Query参数 | 要查询的调度实例状态 |
| marker | String | 否 | Query参数 | 批量获取列表的查询的起始位置，是一个由系统生成的字符串 |
| maxKeys | int | 否 | Query参数 | 每页包含的最大数量，最大数量通常不超过1000。缺省值为1000 |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应返回状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| scheduleList | list<ScheduleInstanceModel> | 调度实例列表 |
| marker | String | 标记查询的起始位置，若结果列表为空，此项不存在 |
| isTruncated | boolean | true表示后面还有数据，false表示已经是最后一页 |
| nextMarker | String | 获取下一页所需要传递的marker值。当isTruncated为false时，该域不出现 |
| maxKeys | int | 每页包含的最大数量 |

**请求示例**

```
 GET /v1/schedule?region=bj&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
 "nextMarker": "sche-62a7vb3m",
 "marker": "sche-1234abcd",
 "maxKeys": 1000,
 "isTruncated": true,
 "scheduleList": [
  {
   'scheduleId': 'sche-1234abcd',
   'scheduleIp': '1.2.3.4',
   'region': 'private',
   'scheduleBandwidthInGbps': 5,
   'cname': '1234abcd.baiduads.com',
   'status': "normal",
   'rsIp': '180.76.1.1',
      'healthCheckPort': 80,
      'adasBgpIp': '180.76.198.100',
      'adasId': 'adas-0343ebb9',
      'updateTime': "2018-04-23 14:14:16",
      'scheduleStartTime': "2018-04-23 14:14:16",
  },
  ...
 ]
}
```

**查询调度实例详情**

- 描述

指定调度实例ID, 查询调度实例详情。

- 请求语法

  GET /v{version}/schedule/{scheduleId}?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

**请求头域**

除公共头域外，无其他特殊头域

**请求参数**

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| scheduleId | String | 是 | Query参数 | 调度实例ID |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| schedule | ScheduleInstanceModel | 调度实例信息 |

**请求示例**

```
 GET /v1/schedule/{sche-1234abcd}?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
 "schedule": {
  'scheduleId': 'sche-1234abcd',
  'scheduleIp': '1.2.3.4',
  'region': 'private',
  'scheduleBandwidthInGbps': "5",
  'cname': '1234abcd.baiduads.com',
  'status': "normal",
  'healthCheckPort': "",
  'adasBgpIp': '180.76.198.100',
  'adasId': 'adas-0343ebb9',
  'updateTime': "2018-04-23 14:14:16",
  'scheduleStartTime': "2018-04-23 14:14:16",
 }
}
```

**删除调度实例**

- 描述

删除调度实例。

- 请求语法

  DELETE /v{version}/schedule/{scheduleId}?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| scheduleId | String | 是 | Query参数 | 调度实例ID |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

无特殊返回参数

**请求示例**

```
 DELETE /v1/schedule/sche-1234abcd?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
```

**触发、解除调度动作**

- 描述

发生攻击时，触发调度，将流量切换到高防实例IP。

攻击结束时，解除调度，将流量切换到调度实例IP。

- 请求语法

PUT /v{version}/schedule/public/action?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

{ "scheduleList": { "sche-1111aaaa": { "message": "ATTACK_STARTED", }, "sche-2222bbbb": { "message": "ATTACK_STOPPED", }, ... } }

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| scheduleId | String | 是 | Query参数 | 调度实例ID |
| clientToken | String | 是 | Query参数 | 幂等性Token |
| scheduleList | list<ScheduleActionModel> | 是 | RequestBody参数 | 调度实例执行的动作列表 |

- 响应返回状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

无特殊返回参数

**请求示例**

```
 PUT /v{version}/schedule/public/action?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "scheduleList": {
      "sche-1111aaaa": {
       "message": "ATTACK_STARTED",
      },
      "sche-2222bbbb": {
       "message": "ATTACK_STOPPED",
      },
        ...
    }
}
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
```

查询高防相关接口

**查询高防回源IP网段**

- 描述

查询高防回源IP网段。

如果后端服务机器开启了防火墙，请配置高防回源IP网段允许通过，防止回源流量被阻断。

- 请求语法

  GET /v{version}/adasBackendIp?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| adasBackendIp | Array | 高防回源IP网段列表 |

**请求示例**

```
 GET /v1/adasBackendIp?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
 "adasBackendIp": [
  "119.188.178.0/23",
    "150.138.240.0/20"
   ]
}
```

附录1

**Model对象定义**

**ScheduleInstanceModel**

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| scheduleId | String | 调度实例ID |
| scheduleIp | String | 调度实例IP |
| region | region | 调度实例IP所属区域 |
| scheduleBandwidthInGbps | String | 触发攻击开始调度的带宽 |
| cname | String | 高防域名 |
| status | scheduleInstanceStatus | 调度实例的状态 |
| healthCheckPort | String | 健康检查端口 |
| adasIp | String | 高防实例IP |
| adasId | String | 高防实例ID |
| updateTime | String | 调度实例最新一次更新记录时间，配置状态更新或调度状态更新都会更新该时间 |
| scheduleStartTime | String | 调度开始时间 |

**ScheduleActionModel**

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| scheduleId | String | 调度实例ID |
| message | actionMessage | 自有高防调度动作消息 |

**区域编码定义**

**region**

| 区域 | 描述 |
| --- | --- |
| private | 用户自有IP |
| bj | 公有云-北京 |
| gz | 公有云-广州 |
| su | 公有云-苏州 |
| hk02 | 公有云-香港二区 |
| hkg | 公有云-香港三区 |
| fsh | 公有云-上海 |

**状态编码定义**

**scheduleInstanceStatus**

| 状态 | 描述 |
| --- | --- |
| normal | 正常 |
| startScheduling | 触发调度中 |
| scheduled | 已调度 |
| stopScheduling | 解除调度中 |

**调度动作消息定义**

**actionMessage**

| 状态 | 描述 |
| --- | --- |
| ATTACK_STARTED | 攻击开始 |
| ATTACK_STOPPED | 攻击结束 |

## 高防自动化调度API参考

### 概述

**简介**

BGP高防自动化调度，是指为遭受攻击的EIP创建临时高防实例并进行DNS调度。在EIP遭受攻击时，通过DNS调度的方式将流量自动调度到高防机房，经高防机房清洗攻击流量后，将正常流量回源到调度EIP，最终到达EIP绑定的BCC/BLB；攻击结束时，自动结束DNS调度，流量正常到达EIP。该场景配置时，需要指定调度EIP、公有云区域、健康检查端口。

如果您是初次调用百度智能云产品的API，可以观看API入门视频指南，快速掌握调用API的能力。

**服务域名**

产品是全局产品，服务域名为adas.baidubce.com。

**通用说明**

API调用遵循HTTP协议，数据交换格式为JSON，所有request/response body内容均采用UTF-8编码。URL参数中所使用的IP均使用点分十进制表示。

**API认证机制**

所有API的安全认证一律采用Access Key与请求签名机制。 Access Key由Access Key ID和Secret Access Key组成，均为字符串。 对于每个HTTP请求，使用下面所描述的算法生成一个认证字符串。提交认证字符串放在Authorization头域里。服务端根据生成算法验证认证字符串的正确性。 认证字符串的格式为`bce-auth-v{version}/{accessKeyId}/{timestamp}/{expirationPeriodInSeconds}/{signedHeaders}/{signature}`。

- version是正整数。
- timestamp是生成签名时的UTC时间。
- expirationPeriodInSeconds表示签名有效期限。
- signedHeaders是签名算法中涉及到的头域列表。头域名之间用分号（;）分隔，如host;x-bce-date。列表按照字典序排列。（本API签名仅使用host和x-bce-date两个header）
- signature是256位签名的十六进制表示，由64个小写字母组成。

当百度智能云接收到用户的请求后，系统将使用相同的SK和同样的认证机制生成认证字符串，并与用户请求中包含的认证字符串进行比对。如果认证字符串相同，系统认为用户拥有指定的操作权限，并执行相关操作；如果认证字符串不同，系统将忽略该操作并返回错误码。

鉴权认证机制的详细内容请参见鉴权认证。

**幂等性**

当调用某些接口时如果遇到了请求超时或服务器内部错误，用户可能会尝试重发请求，这时用户通过clientToken参数避免创建出比预期要多的资源，即保证请求的幂等性。

幂等性基于clientToken，clientToken是一个长度不超过64位的ASCII字符串，通常放在query string里，如`http://bcc.bj.baidubce.com/v1/instance?clientToken=be31b98c-5e41-4838-9830-9be700de5a20`。

如果用户使用同一个clientToken值调用创建接口，则服务端会返回相同的请求结果。因此用户在遇到错误进行重试的时候，可

以通过提供相同的clientToken值，来确保只创建一个资源；如果用户提供了一个已经使用过的clientToken，但其他请求参数（包括queryString和requestBody）不同甚至url Path不同，则会返回IdempotentParameterMismatch的错误代码。

clientToken的有效期为24小时，以服务端最后一次收到该clientToken为准。也就是说，如果客户端不断发送同一个clientToken，那么该clientToken将长期有效。

**日期与时间规范**

日期与时间的表示有多种方式。为统一起见，除非是约定俗成或者有相应规范的，凡需要日期时间表示的地方一律采用UTC时间，遵循ISO 8601，并做以下约束：

1. 表示日期一律采用YYYY-MM-DD方式，例如2014-06-01表示2014年6月1日
2. 表示时间一律采用hh:mm:ss方式，并在最后加一个大写字母Z表示UTC时间。例如23:00:10Z表示UTC时间23点0分10秒。
3. 凡涉及日期和时间合并表示时，在两者中间加大写字母T，例如2014-06-01T23:00:10Z表示UTC时间2014年6月1日23点0分10秒。

**请求参数**

请求参数包括如下4种：

| 参数类型 | 说明 |
| --- | --- |
| URI | 通常用于指明操作实体,如:PUT /v1/schedule/{scheduleId} |
| Query参数 | URL中携带的请求参数 |
| HEADER | 通过HTTP头域传入,如:x-bce-date |
| Requestbody | 通过JSON格式组织的请求数据体 |

**返回值说明**

返回值分为两种形式：

| 返回内容 | 说明 |
| --- | --- |
| HTTP STATUS CODE | 如200,400,403,404等 |
| ResponseBody | JSON格式组织的响应数据体 |

**公共请求头**

下表列出了所有AdasSchedule API所携带的公共头域。HTTP协议的标准头域不在此处列出

| 头域（HEADER） | 是否必须 | 说明 |
| --- | --- | --- |
| Authorization | 是 | 包含Access Key与请求签名 |
| Content-Type | 是 | application/json; charset=utf-8 |
| x-bce-date | 否 | 表示日期的字符串，符合BCE API规范 |

**公共响应头**

下表列出了所有AdasSchedule API的公共响应头域。HTTP协议的标准响应头域不在此处列出

| 头域（HEADER） | 说明 |
| --- | --- |
| Content-Type | 只支持JSON格式，application/json; charset=utf-8 |
| x-bce-request-id | AdasSchedule后端生成，并自动设置到响应头域中 |

**错误码**

请求发生错误时通过respone body返回详细错误信息，遵循如下格式：

| 参数名 | 类型 | 说明 |
| --- | --- | --- |
| code | String | 错误码 |
| message | String | 错误描述 |
| requestId | String | 本次请求的requestId |

示例：

```
 {
 "requestId" : "ae2225f7-1c2e-427a-a1ad-5413b762957d",
 "code" : "NoSuchKey",
 "message" : "The resource you requested does not exist"
}
```

**公共错误码**

| 错误码 | 消息 | HTTP状态码 | 语义 |
| --- | --- | --- | --- |
| AccessDenied | Access denied. | 403 Forbidden | 无权限访问对应的资源 |
| InappropriateJSON | The JSON you provided was well-formed and valid, but not appropriate for this operation. | 400 Bad Request | 请求中的JSON格式正确，但语义上不符合要求。如缺少某个必需项，或者值类型不匹配等。出于兼容性考虑，对于所有无法识别的项应直接忽略，不应该返回这个错误。 |
| InternalError | We encountered an internal error. Please try again. | 500Internal Server Error | 所有未定义的其他错误。在有明确对应的其他类型的错误时（包括通用的和服务自定义的）不应该使用。 |
| InvalidAccessKeyId | The Access Key ID you provided does not exist in our records. | 403 Forbidden | Access Key ID不存在 |
| InvalidHTTPAuthHeader | The HTTP authorization header is invalid. Consult the service documentation for details. | 400 Bad Request | Authorization头域格式错误 |
| InvalidHTTPRequest | There was an error in the body of your HTTP request. | 400 Bad Request | HTTP body格式错误。例如不符合指定的Encoding等 |
| InvalidURI | Could not parse the specified URI. | 400 Bad Request | URI形式不正确。例如一些服务定义的关键词不匹配等。对于ID不匹配等问题，应定义更加具体的错误码，例如NoSuchKey。 |
| MalformedJSON | The JSON you provided was not well-formed. | 400 Bad Request | JSON格式不合法 |

| | | | |
|---|---|---|---|
| InvalidVersion | The API version specified was invalid. | 404 Not Found | URI的版本号不合法 |
| OptInRequired | A subscription for the service is required. | 403 Forbidden | 没有开通对应的服务 |
| PreconditionFailed | The specified If-Match header doesn't match the ETag header. | 412 Precondition Failed | 详见ETag |
| RequestExpired | Request has expired. Timestamp date is XXX. | 400 Bad Request | 请求超时。XXX要改成x-bce-date的值。如果请求中只有Date，则需要将Date转换为datetime。 |
| IdempotentParameterMismatch | The request uses the same client token as a previous, but non-identical request. | 403 Forbidden | clientToken对应的API参数不一样。 |
| SignatureDoesNotMatch | The request signature we calculated does not match the signature you provided. Check your Secret Access Key and signing method. Consult the service documentation for details. | 400 Bad Request | Authorization头域中附带的签名和服务端验证不一致 |

**AdasSchedule业务错误码**

| 错误码 | 错误描述 | HTTP状态码 | 语义 |
|---|---|---|---|
| ScheduleInstanceNotFound | The specified schedule instance does not exist. | 404 | 调度实例不存在 |
| UnsupportedScheduleInstanceOperation | The status of specified schedule instance does not support this operation. | 400 | 指定的调度实例状态不支持此类型操作 |
| AdasInstanceIsInvalid | The specified adas instance is invalid. | 400 | 高防实例不合理 |
| ScheduleNatAlreadyExist | The specified schedule nat already exist. | 400 | 调度nat已经存在 |
| ScheduleNatNotFound | The specified schedule nat does not exist. | 404 | 调度nat不存在 |
| VpcInstanceNotFound | The specified vpc instance does not exist. | 404 | vpc实例不存在 |
| NatInstanceNotFound | The specified nat instance does not exist. | 404 | nat实例不存在 |

**名词解释**

下表列出了所有AdasSchedule API的涉及到的关键名词及解释。

| 名词 | 解释 |
|---|---|
| 调度实例IP | 需要配置调度服务的IP，为用户EIP |
| 高防实例IP | 调度发生后，创建的高防实例对应的IP |
| 高防回源IP | 调度发生后，高防回源到用户后端服务器的流量的源IP |
| 高防调度域名 | 正常情况下，解析到调度实例IP；调度发生后，解析到高防实例IP |

调度实例相关接口

**创建调度实例**

- 描述

创建一个调度实例，用于绑定调度的IP。

需要开启两个白名单：AdasAutoSchedule（高防自动化调度）和 RouteOpenSourceAddress（自定义路由白名单）。

创建调度实例需要实名认证，若未通过实名认证可以前往百度开放云官网控制台中的安全认证下的实名认证中进行认证。

- 请求语法

  POST /v{version}/schedule?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| scheduleId | String | 创建的调度实例id |

**请求示例**

```
 POST /v1/schedule?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
    "scheduleId":"sche-12345678"
}
```

**配置调度实例**

- 描述

只有在调度实例正常状态下，才能进行配置，即调度实例的status必须是normal。

需要指定scheduleIp，region, healthCheckPort, 其中，region只能为公有云的区域，healthCheckPort为后端机器开放的TCP端口。

- 请求语法

PUT /v{version}/schedule/{scheduleId}?action={action}&clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com
Authorization: authorization string

{ "scheduleIp": "182.61.1.1", "region": "bj", "healthCheckPort": 80,
}

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| scheduleId | String | 是 | Query参数 | 调度实例ID |
| action | String | 是 | Query参数 | 对实例执行的动作，本接口中该参数取值update |
| clientToken | String | 是 | Query参数 | 幂等性Token |
| scheduleIp | String | 是 | RequestBody参数 | 配置调度实例IP：eip |
| region | String | 是 | RequestBody参数 | 调度实例IP所属的区域 |
| healthCheckPort | String | 是 | RequestBody参数 | 用于健康检查的后端的端口。 |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

无特殊返回参数

**请求示例**

```
 PUT /v1/schedule/sche-1234abcd?action=update&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "scheduleIp": "182.61.1.1",
    "region": "bj",
    "healthCheckPort": 80,
}
```

**响应示例**

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
```

**查询调度实例列表**

- 描述

可以指定scheduleIp，region，status，查询指定条件的调度实例的列表。

根据region字段，可以查询指定区域的调度实例。region为bj，gz，su，hk02，hkg，fsh可查询指定区域的BGP高防自动化调度实例列表。

根据status字段，可以查询处于不同调度状态下的调度实例。

- 请求结构

GET /v{version}/schedule?scheduleIp={scheduleIp}®ion={region}&clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
|---|---|---|---|---|
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| scheduleIp | String | 否 | Query参数 | 要查询的调度实例IP，点分十进制 |
| region | String | 否 | Query参数 | 要查询的调度实例所属区域 |
| status | String | 否 | Query参数 | 要查询的调度实例状态 |
| marker | String | 否 | Query参数 | 批量获取列表的查询的起始位置，是一个由系统生成的字符串 |
| maxKeys | int | 否 | Query参数 | 每页包含的最大数量，最大数量通常不超过1000。缺省值为1000 |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

| 参数名称 | 类型 | 描述 |
|---|---|---|
| scheduleList | list<ScheduleInstanceModel> | 调度实例列表 |
| marker | String | 标记查询的起始位置，若结果列表为空，此项不存在 |
| isTruncated | boolean | true表示后面还有数据，false表示已经是最后一页 |
| nextMarker | String | 获取下一页所需要传递的marker值。当isTruncated为false时，该域不出现 |
| maxKeys | int | 每页包含的最大数量 |

**请求示例**

```
 GET /v1/schedule?region=bj&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
 "nextMarker": "sche-62a7vb3m",
 "marker": "sche-1234abcd",
 "maxKeys": 1000,
 "isTruncated": true,
 "scheduleList": [
  {
   'scheduleId': 'sche-1234abcd',
   'scheduleIp': '180.76.1.1',
   'region': 'bj',
   'scheduleBandwidthInGbps': 5,
   'cname': '1234abcd.baiduads.com',
   'status': "normal",
   'rsIp': '180.76.1.1',
      'healthCheckPort': 80,
      'adasBgpIp': '180.76.198.100',
      'adasId': 'adas-0343ebb9',
      'updateTime': "2018-04-23 14:14:16",
   'scheduleStartTime': "2018-04-23 14:14:16",
  },
  ...
 ]
}
```

**查询调度实例详情**

- 描述

指定调度实例ID, 查询调度实例详情。

- 请求语法

  GET /v{version}/schedule/{scheduleId}?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| scheduleId | String | 是 | Query参数 | 调度实例ID |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| schedule | ScheduleInstanceModel | 调度实例信息 |

**请求示例**

```
 GET /v1/schedule/{sche-1234abcd}?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
 "schedule": {
  'scheduleId': 'sche-1234abcd',
  'scheduleIp': '180.76.1.1',
  'region': 'bj',
  'scheduleBandwidthInGbps': "5",
  'cname': '1234abcd.baiduads.com',
  'status': "normal",
  'healthCheckPort': "80",
  'adasBgpIp': '180.76.198.100',
  'adasId': 'adas-0343ebb9',
  'updateTime': "2018-04-23 14:14:16",
  'scheduleStartTime': "2018-04-23 14:14:16",
 }
}
```

**删除调度实例**

- 描述

删除调度实例。

- 请求语法

DELETE /v{version}/schedule/{scheduleId}?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| scheduleId | String | 是 | Query参数 | 调度实例ID |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

无特殊返回参数

**请求示例**

```
DELETE /v1/schedule/sche-1234abcd?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
```

NAT配置相关接口

如果用户EIP绑定的是BCC且有主动访问外网的需求。用户可以为EIP绑定的虚机所在的VPC配置NAT实例，在触发攻击调度后，保持主动访问外网的能力。

**查询NAT配置列表**

- 描述

查询NAT配置列表。

可指定vpcId, region进行查询。

- 请求语法

GET /v{version}/scheduleNat?vpcId={vpcId}&region={region}&clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| vpcId | String | 否 | Query参数 | 要查询的vpcId |
| region | String | 否 | Query参数 | 要查询的vpc区域, 只能为公有云区域 |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| natList | list | 调度实例列表 |

**请求示例**

```
 GET /v1/scheduleNat?region=bj&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
 "natList": [
  {
      'natId': 'nat-bu2hiyq4270h',
      'vpcId': 'vpc-0h82pc5dvmzc',
      'region': 'bj',
  },
  ...
 ]
}
```

**添加调度NAT**

- 描述

添加NAT配置。

需要开启自定义路由白名单：RouteOpenSourceAddress。

在指定region里，需满足：natId对应的NAT实例必须属于vpcId对应的VPC，且一个VPC只能配置一个调度NAT实例。

- 请求语法

  POST /v{version}/scheduleNat?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

  { 'natId': 'nat-bu2hiyq4270h', 'vpcId': 'vpc-0h82pc5dvmzc', 'region': 'bj', }

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| clientToken | String | 是 | Query参数 | 幂等性Token |
| natId | String | 是 | RequestBody参数 | 要添加的natId |
| vpcId | string | 是 | RequestBody参数 | natId对应的vpcId |
| region | String | 是 | RequestBody参数 | vpc所属的区域，必须为公有云区域 |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

无特殊返回参数

**请求示例**

```
 POST /v1/scheduleNat?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
 'natId': 'nat-bu2hiyq4270h',
 'vpcId': 'vpc-0h82pc5dvmzc',
 'region': 'bj',
}
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
```

**删除调度NAT配置**

- 描述

删除NAT配置。

- 请求语法

DELETE /v{version}/scheduleNat/{region}/{natId}?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com
Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| region | String | 是 | Query参数 | nat所属的区域，必须为公有云区域，不能为private |
| natId | String | 是 | Query参数 | 要删除的natId |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

无特殊返回参数

**请求示例**

```
DELETE /v1/scheduleNat/bj/nat-bu2hiyq4270h?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
```

查询高防相关接口

**查询高防回源IP网段**

- 描述

查询高防回源IP网段。

如果后端服务机器开启了防火墙，请配置高防回源IP网段允许通过，防止回源流量被阻断。

- 请求语法

  GET /v{version}/adasBackendIp?clientToken={clientToken} HTTP/1.1 Host: adas.baidubce.com Authorization: authorization string

- 请求头域

除公共头域外，无其他特殊头域

- 请求参数

| 参数名称 | 类型 | 是否必需 | 参数位置 | 描述 |
| --- | --- | --- | --- | --- |
| version | String | 是 | URL参数 | API版本号，当前取值1 |
| clientToken | String | 是 | Query参数 | 幂等性Token |

- 响应状态码

成功返回200，失败返回见错误码

- 响应头域

除公共头域外，无其他特殊头域

- 响应参数

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| adasBackendIp | Array | 高防回源IP网段列表 |

**请求示例**

```
 GET /v1/adasBackendIp?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST adas.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

**响应示例**

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
 "adasBackendIp": [
  "119.188.178.0/23",
    "150.138.240.0/20"
   ]
}
```

附录1

**Model对象定义**

**ScheduleInstanceModel**

| 参数名称 | 类型 | 描述 |
| --- | --- | --- |
| scheduleId | String | 调度实例ID |
| scheduleIp | String | 调度实例IP |
| region | region | 调度实例IP所属区域 |
| scheduleBandwidthInGbps | String | 触发攻击开始调度的带宽 |
| cname | String | 高防域名 |
| status | scheduleInstanceStatus | 调度实例的状态 |
| healthCheckPort | String | 健康检查端口 |
| adasIp | String | 高防实例IP |
| adasId | String | 高防实例ID |
| updateTime | String | 调度实例最新一次更新记录时间，配置状态更新或调度状态更新都会更新该时间 |
| scheduleStartTime | String | 调度开始时间 |

**区域编码定义**

**region**

| 区域 | 描述 |
| --- | --- |
| bj | 公有云-北京 |
| gz | 公有云-广州 |
| su | 公有云-苏州 |
| hk02 | 公有云-香港二区 |
| hkg | 公有云-香港三区 |
| fsh | 公有云-上海 |

**状态编码定义**

**scheduleInstanceStatus**

| 状态 | 描述 |
| --- | --- |
| normal | 正常 |
| startScheduling | 触发调度中 |
| scheduled | 已调度 |
| stopScheduling | 解除调度中 |

# 功能发布记录

本文介绍DDoS高防的新功能发布记录

# 2025年

| 发布日期 | 功能概要 | 相关文档 |
| --- | --- | --- |
| 2025-6-26 | HTTPS证书的TLS支持设置成1.3版本，向源站返回的头中增加JA3和JA4头 | 接入防护业务 |
| 2025-3-05 | 业务带宽支持日第6峰值和月95峰值计费 | 弹性业务带宽计费 |

# 2024年

| 发布日期 | 功能概要 | 相关文档 |
| --- | --- | --- |
| 2024-11-07 | 上线高防EIP产品，支持北京、保定、武汉region使用 | 购买DDoS高防EIP |
| 2024-07-01 | 上线EIP被攻击联动高防防护功能 | EIP被攻击联动高防防护 |
| 2024-05-01 | 新上线华东高防节点，面向邀请客户开放使用。最大防御量级达到3.1Tbps | 如有需求，可前往工单系统申请 |
| 2024-03-04 | 支持电话和机器人告警。最大防御量级达到1.6Tbps | 详细前往控制台-报警设置中查看和配置 |

2023年

| 发布日期 | 功能概要 | 相关文档 |
| --- | --- | --- |
| 2023-08-16 | 支持弹性防护包，用于抵扣弹性防护费用 | 计费概述-弹性防护 |
| 2023-08-03 | DDoS高防联合BLS为用户提供高防七层日志的存储和分析功能 | 通过BLS获取高防七层日志 |
| 2023-07-27 | 上线“守护者”计划，为正在遭受DDoS攻击或勒索的企业客户提供24小时免费高防防护服务 | DDoS应急防护 |
| 2023-06-29 | 报表支持最长6个自然月历史数据 | 查看流量报表 |
| 2023-06-12 | HTTPS业务支持限制低版本TLS | 接入防护业务 |
| 2023-02-14 | 支持IPv6接入高防和攻击防御 | 购买DDoS高防IP |

2022年

| 发布日期 | 功能概要 | 相关文档 |
| --- | --- | --- |
| 2022-09-19 | 上线自助解除封禁功能，并支持每日自助调整一次弹性防护峰值 | 高防限流封禁策略 |
| 2022-06-17 | 上线域名调度：在公开源站故障后自动切入高防 | 自动或一键切入切出高防 |
| 2022-05-22 | 支持全力防护，最大防御量级达到1.4Tbps | 购买DDoS高防IP |
| 2022-02-22 | 上线分布防护产品 | - |

# 常见问题

## 常见问题总览

使用类问题

- 怎样启动DDOS防护服务？

- 高防IP回源地址支持IPv6吗？
- 使用高防IP后如何获得用户真实访问IP？
- 域名没有备案，可以使用百度智能云 DDoS 高防 IP 服务吗？
- 域名已在其它服务商处备案，使用百度智能云 DDoS 高防 IP 有什么限制？
- 防护类型有哪些呢？
- DDoS高防有没有抓包？
- DDoS高防支持多少条转发配置？
- DDoS高防与DDoS基础防护的区别？
- CC防护支持多少域名、支持哪些端口？
- 购买DDoS高防服务后还需要注意哪些？

计费类问题

- DDoS收费吗？

## 使用类问题

怎样启动DDOS防护服务？

DDoS防护服务，分为基础防护和高级防护。

- DDoS 基础防护，每个对外网提供服务的EIP都会默认启动DDoS防护服务，根据所在区域的不同最大能够提供5Gbps的防护能力，当攻击流量超过用户设置的清洗触发值时，将自动启动清洗设备进行流量清洗。
- DDoS 高防防护服务，也称为DDoS 高防 IP ，通过付费获得5Gbps以上的防护能力，在付费购买后需要在控制台进行相关配置才能使用。

高防IP回源地址支持IPv6吗？

支持。需要防护实例选购IPv6高防IP，在tcp/udp防护业务关联IPv6高防IP后,可配置IPv6源站。

使用高防IP后如何获得用户真实访问IP？

- 七层业务（HTTP/HTTPS协议）可以在http header中直接通过X_forward_for字段来获取客户端真实源IP；
- 四层业务如果后端服务器是百度云BCC，无需进行额外的配置，服务器获取到的就是客户端真实源IP，如果后端服务器不是百度云BCC，可以通过在服务器加载TTM模块来获取客户端真实源IP，详见非百度云主机获取客户端真实源IP；

域名没有备案，可以使用百度智能云 DDoS 高防 IP 服务吗？

百度智能云受监管要求，DDoS 高防 IP 服务不支持为未备案域名提供防护服务。

域名已在其它服务商处备案，使用百度智能云 DDoS 高防 IP 有什么限制？

- 若您的源站不在百度智能云，则没有其它限制
- 若您的源站在百度智能云，则需要将域名的备案信息在百度智能云做新增接入

> **注意：**
>
> - 新增接入的效果是增加一个新服务商，如果您在接入备案时填写的信息与原有备案信息一致，则对原有服务商处的备案数据不会产生影响。接入完成后，您可以同时使用原有服务商和百度智能云的服务器。

### 防护类型有哪些呢？

防护下列网络层攻击：

- SYN flood攻击；
- ACK flood攻击；
- FIN/RST flood攻击；
- UDP flood攻击；
- ICMP flood；
- TCP连接耗尽攻击等；

应用层攻击：

- 有效抵御HTTP get/post flood攻击；
- CC 攻击；
- HTTP slow header/post攻击等。

### DDoS高防有没有抓包？

DDoS高防服务暂时不支持抓包功能。

### DDoS高防支持多少条转发配置？

- DDoS高防是业务代理模式，每个高防 IP 支持最多配置200个端口和200个域名的转发规则。
- 每个高防套餐可免费配置50个端口和50个域名的转发规则。
- 支持TCP/UDP／HTTP／HTTPS/WS/WSS协议。

### DDoS高防与DDoS基础防护的区别？

| **服务** | **DDoS 高防服务** | **DDoS 基础防护服务** |
| --- | --- | --- |
| 防护能力 | 总计提供最大1Tbps防护能力 | 华北-北京区域提供最高5Gbps防护能力<br>华南-广州区域最高提供5Gbps防护能力 |
| 资源 | 支持外网资源 | 仅支持百度智能云EIP资源 |
| 防护策略 | 防护策略丰富，专业的 CC 防护能力，用户可以自助配置策略 | 防护策略固定，基础的 CC 防护能力，采用全局通用策略 |
| 重大活动保障 | 专家服务（大客户专享） | 无 |
| 详细报表 | 提供详细报表 | 提供概述报表 |
| 网络调优 | 暂不支持 | 暂不支持 |
| 故障排查速度 | 工单响应 | 工单响应 |
| 技术支持 | 7x24小时 | 7x8小时 |
| 通知方式 | 电话或短信 | 短信 |

### CC防护支持多少域名、支持哪些端口？

基础防护服务的 CC 防护采用流量重组的方式进行防护，对域名和端口没有限制。

### 购买DDoS高防服务后还需要注意哪些？

购买DDoS高防服务后请关注下列事项:

1. 由于DDoS高防是转发架构，真实用户的源IP经过高防中心时会转换成高防中心的IP地址，回源IP为固定IP段，所以需要将服务器的安全防护软件进行卸载或者关闭对回源IP段的限制，防止误杀；
2. 对于源服务器在百度开放云内的用户需要将控制台中的DDoS防护服务的清洗阈值提高，建议设置为最高清洗阈值；
3. 尽量将所有业务都走高防中心，不要暴露到外网；防止攻击者绕过高防中心，直接攻击源站。

## 计费类问题

### DDoS收费吗？

百度智能云为EIP免费提供最大5Gbps的基础防护能力，如需更大的DDoS防护能力，请购买DDoS高防IP。

## 高防限流封禁策略

### 1.背景

DDoS高防根据您购买的实例规格分配资源，规格越高分配资源越多。超量使用会影响预分配资源的稳定性，存在此风险时将会触发保障系统执行管控。

管控方式包括：限流和封禁。

本文介绍DDoS高防的限流和封禁策略、以及如何解除限流/封禁和降低被限流/封禁风险。

### 2.限流策略

DDoS高防根据您购买实例的业务带宽和弹性防护带宽默认进行限流：

当高防IP的带宽用量***持续超过实例的业务带宽或者弹性防护带宽后***，会触发限流策略，对超过的流量进行丢弃。丢弃时不区分攻击和业务流量，因此限流时可能造成部分正常用户无法访问。

### 3.封禁策略

在高防IP遭受DDoS攻击，入向带宽持续20秒超过***浮动防护峰值***后，执行封禁。

浮动防护峰值匹配高防IP对应实例的弹性防护峰值，实例的弹性防护峰值越大可浮动的量级越大。

特别：

- 弹性防护峰值超过300Gbps的高防IP，在触发封禁时将优先执行运营商海外访问封禁，启用后可降低攻击量级，减少弹性防护后付费用；
- 对购买全力防护的高防IP，封禁仅在攻击可能造成高防节点运营商线路出口有拥堵风险时执行。并通过更换高防IP等方式，在封禁时能够自动切换保证业务可用。

> **注意：**
>
> - 被封禁的高防IP上的业务将无法提供服务即无法访问，通过升级或修改更大的弹性防护峰值将减少被封禁风险。

### 4.解除限流/封禁

### 4.1.解除限流

DDoS高防在高防IP带宽用量低于实例业务带宽和弹性防护带宽后自动解除限流。

### 4.2.解封封禁

- 自动解封

高防IP根据用户购买的防御资源情况，执行不同的自动解封策略，默认封禁1小时后自动解封。 对购买保底防护超过100Gbps或弹性浮动（弹性防护峰值-保底防护峰值）≥ 200Gbps的实例，30分钟自动解封。

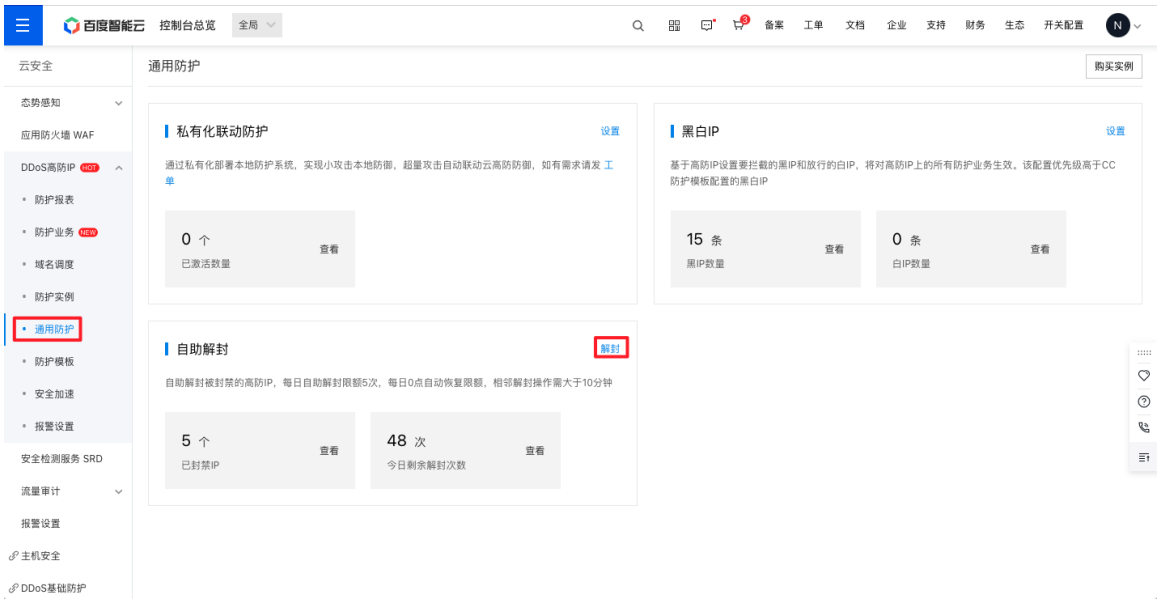
- 自助解封

如在封禁期间急需恢复业务，可以自助解除封禁，每日每个账号限额5次。 自助解封时，被解封的高防IP必须无攻击流量或攻击流量小于对应实例的弹性防护峰值，否则将解封失败。同一账号相邻自助解封操作需大于10分钟，解封失败不会占用每日解封限额，每日0点自动恢复限额次数。

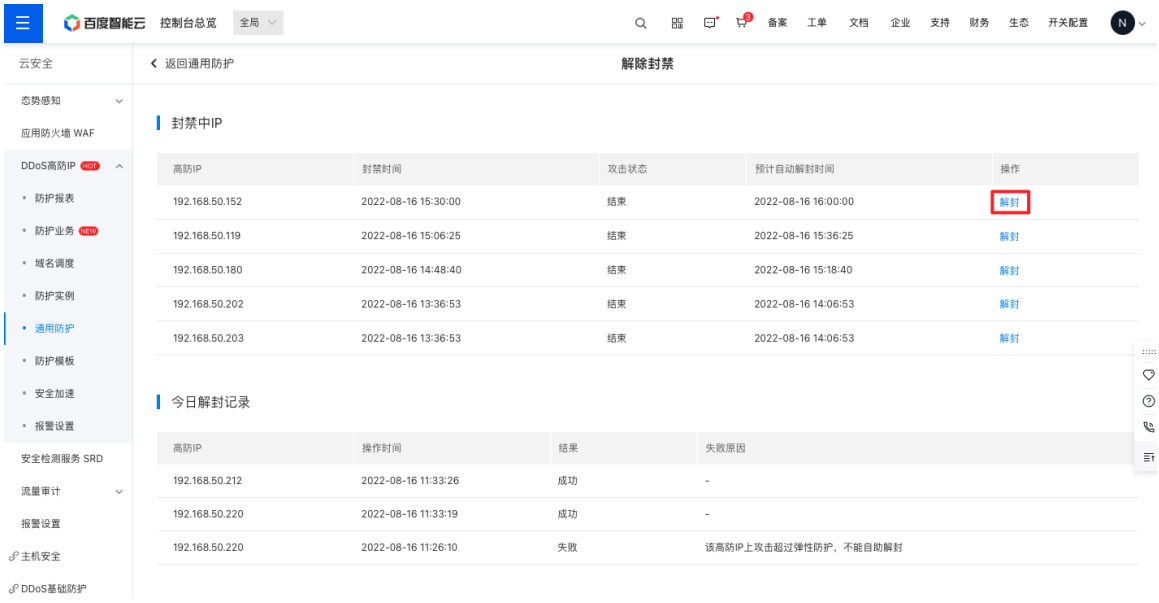
> **注意：**
>
> - 自动或自助解封后，如果DDoS攻击没有结束，扔可能再次被封禁。

您可以通过如下方式进行自助解封：

1.进入DDoS高防IP控制台，点击左侧导航“通用防护”进入通用防护页面；




2.在通用防护页面，点击“自助解封”模块的“解封”进入解除封禁页面，选择封禁中的高防IP解除封禁。

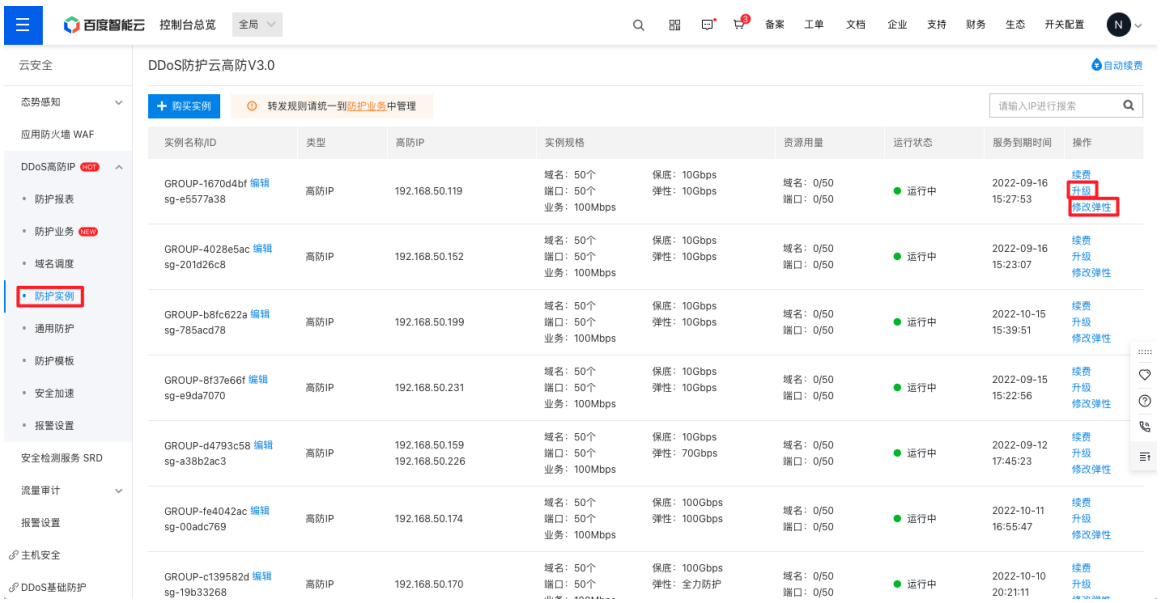


5.降低被限流/封禁风险

只有当带宽用量或DDoS攻击的峰值带宽持续超过高防IP的业务带宽和弹性防护带宽时，才会导致高防IP被限流/封禁。高防IP的实例规格越大，则其被限流/封禁的可能就越低。因此提升高防IP的业务带宽和弹性防护峰值，可以降低被限流/封禁风险。

您可以通过如下方式提升高防IP的实例规格：

1. 升级高防IP对应实例的业务带宽或保底防护带宽 进入DDoS高防IP控制台，点击左侧导航“防护实例”进入防护实例页面，点击要升级实例操作中的“升级”，进入“实例配置升级”升级业务带宽或保底/弹性防护峰值。
2. 修改高防IP对应实例弹性防护峰值 进入DDoS高防IP控制台，点击左侧导航“防护实例”进入防护实例页面，点击要修改实例操作中的“修改弹性”，进入“修改弹性防护峰值”升级弹性防护峰值。




> **注意：**
>
> - 同一实例弹性防护每日仅能修改一次，下限为保底防护带宽，修改后即时生效；
> - 修改弹性防护峰值前产生的后付费弹性防护带宽按照原配置计费，修改后产生的后付费弹性防护带宽，将按照新配置计费。单价为100元/Gbps/天；
> - 弹性防护与保底防护峰值相同时不会产生后付费用。

# 服务等级协议SLA

## DDoS服务等级协议（SLA）

**协议生效时间：2019 年 01 月 15 日**

百度智能云DDoS防护服务高防IP等级协议（简称“SLA”） 规定了百度智能云向客户（简称“您”）提供的DDoS高防IP（简称“高防IP”）的服务可用性等级指标及赔偿方案。特别提示您，本服务等级协议仅限于您未使用任何非百度智能云提供的清洗服务或设备的前提下适用，如您在使用DDoS高防IP服务的同时使用了第三方提供的任何清洗服务或设备，则本服务等级协议将不适用。

1. 指标定义

**服务周期**：一个服务周期为一个自然月。
**服务周期总分钟数**：服务周期内的总天数 * 24（小时） * 60（分钟）计算。
**高防IP不可用**：当某一分钟内，客户所有试图与指定的高防IP建立转发的连续尝试均失败，则视为该分钟内该监听的服务不可用。接入DDoS高防IP之后整个业务系统将会由一系列请求转发系统构成，高防IP的服务不可用仅限于自身服务不可用性，不对

针对整条链路的可用性适用（如客户的源站带宽跑满、客户源站的机房故障等）。

**服务不可用分钟数**：服务周期内DDoS高防IP不可用的分钟数之和。

## 2. 服务可用性

### 2.1 服务可用性计算公式

$$服务可用性=\left(\frac{服务周期总分钟数-服务不可用分钟数}{服务周期总分钟数}\right)\times 100\%$$

### 2.2 服务可用性承诺

百度智能云防护服务承诺DDoS高防IP服务可用性不低于99.9%。如未达到该承诺的，您可以根据本服务等级协议第3条约定获得相应赔偿。

## 3. 赔偿方案

### 3.1 赔偿标准

根据客户某一百度智能云账号下DDoS高防IP服务可用性比例，按照下表中的标准计算赔偿金额，赔偿方式仅限于用于购买DDoS高防服务的代金券，赔偿总额不超过该月DDoS高防服务基础包月费用的50%。

| 服务可用性 | 赔偿代金券金额 |
| --- | --- |
| 低于99.9%但等于或高于99% | 月度服务费用的10% |
| 低于99%但等于或高于95% | 月度服务费用的20% |
| 低于95% | 月度服务费用的50% |

但因下述原因导致的服务不可用时长，不进行赔付：

(1) 由于网络运营商严重故障导致的服务不可用；

(2) 由于您不付费或是欠款导致的服务不可用；

(3) 超过您购买的DDoS高防IP服务规格的流量攻击导致IP被黑洞引起的服务不可用；

(4) 由于您未按规定或者违法使用百度智能云产品引发的服务不可用；

(5) 由于DDoS高防IP业务后端的各类源站的问题（如源站带宽跑满，源站IP暴露，源站机房故障、源站链路网络抖动等）引起的服务不可用；

(6) 由于您或您的最终用户对百度智能云提供的服务造成安全威胁或存在欺诈或者违法行为而导致的服务不可用；

(7) 由于您或者任何第三方（不受百度智能云直接控制）设备、软件或技术引起的服务不可用；

(8) 由于您未按照百度智能云规定配置使用产品引起的服务不可用；

(9) 由于您违反任何百度智能云产品条款引起的服务不可用；

(10) 由于网络、硬件或服务的维护、升级导致的服务不可用（百度会在计划发生中断维护与升级的前3天通过邮件、短信以及官网通知中心的形式，告知您）；

(11) 由于不可抗力或紧急事件等引起的服务不可用。

(12) 其他非百度智能云原因所造成的不可用。

### 3.2 赔偿申请时限

赔偿申请必须限于在百度智能云DDoS高防IP服务没有达到服务可用性承诺比例的相关月份结束后两个月内提出。超出申请时限的赔偿申请将不被受理。百度智能云收到您的赔偿申请且在您资料提交齐全的情况下启动赔偿申请审核，审核期间可能会与您核实相关情况，并根据核实的结果对您提出的赔偿申请依据本等级服务协议及相关协议作出处理。

## 4. 其他

(1) 在法律法规允许的范围内，百度智能云负责对本协议进行解释说明。

(2) 本协议一经公布立即生效，百度智能云有权对本SLA条款作出修改。如本SLA条款有任何修改，百度智能云将以网站公示或发送邮件的方式通知您。如您不同意百度智能云对SLA所做的修改，您有权停止使用DDoS服务，如您继续使用DDoS服务，则视为您接受修改后的SLA。

(3) 本协议项下百度智能云对于用户所有的通知均可通过网页公告、站内信、电子邮件、手机短信或其他形式等方式进行；该等通知于发送之日视为已送达收件人。因用户未及时获知百度智能云的服务变更或终止条款遭受损失的，百度智能云不承担任何责任。
(4) 本协议的订立、执行和解释及争议的解决均应适用中国法律并受中国法院管辖。如双方就本协议内容或其执行发生任何争议，双方应尽量友好协商解决；协商不成时，任何一方均可向北京市海淀区人民法院提起诉讼。
(5) 本协议构成双方对本协议之约定事项及其他有关事宜的完整协议，除本协议规定的之外，未赋予本协议各方其他权利。
(6) 如本协议中的任何协议无论因何种原因完全或部分无效或不具有执行力，本协议的其余协议仍应有效并且有约束力。
(7) 关于用户约束条款，详见百度智能云用户服务协议中的"用户的权利与义务"相关条款内容。
(8) 关于服务商免责条款，详见百度智能云用户服务协议中的"免责声明"相关条款内容。

# 守护者计划

## DDoS应急防护

### 应用场景

DDoS高防“守护者计划”，为正在遭受DDoS攻击或勒索的企业客户提供24小时免费高防防护服务。

### 申请条件

感谢您对我们的关注！在申请使用高防应急防护服务之前，请先了解以下申请条件：

- 企业客户并完成实名认证；
- 正常业务 QPS （每秒查询数）不超过1万次；
- 每个申请账号和企业每年最多可以申请一次一天应急防护服务；
- DDoS攻击峰值需小于100Gbps。

如您符合以上条件，请提交申请，我们将尽快为您审核并提供服务。如有任何疑问，请随时联系我们的客户支持团队！

### 申请入口

点击前往工单系统

### 申请资料

在工单中需提供以下信息：

- 企业名称：*请填写完整的企业名称*
- 申请人及职务：*请填写申请人姓名及职位*
- 手机号：*请填写手机号码*
- DDoS攻击量级：*请填写攻击的量级例如：50Gbps或10万QPS*
- DDoS攻击勒索证据：*请提供被勒索的截图（如有）*
- 业务类型：*请填写客户端类业务（如游戏等）、网站类业务（包括API）或其他*
- 业务协议：*请填写TCP/UDP/HTTP/HTTS*
- 业务最大QPS：*非攻击状态下业务的最大QPS*

### 购买1日免费防护

对符合申请条件的，将发放可购买1天100Gbps防护实例的代金券。在您收到发送代金卷通知后，请及时登录DDoS高防-购买防护实例，开通一天应急版本（购买时长配置为1天）。

### 接入防护

完成购买后，请参照接入防护业务，完成接入并开始防御。

### 长期防护

DDoS高防“守护者计划”24小时免费应急防护服务，仅帮助您暂时防御DDoS攻击。如需长期使用DDoS高防防护，请及时续费实例。