DDoS 高防 IP

DDoS 高防IP（境外企业版）

产品文档

腾讯云

文档目录

设置安全事件通知

查看操作日志

DDoS 高防IP（境外企业版）
产品简介
产品概述

最近更新时间：2021-11-29 11:17:27

简介

DDoS 高防 IP（境外企业版）是针对业务部署在腾讯云内的用户提升 DDoS 境外防护能力的付费产品。

- DDoS 高防 IP（境外企业版）提供全球各地10个腾讯云入口，分担各单个入口带宽压力，并提供全力防护服务。最大限度保证各地节点访问的畅通。
- Anycast 实现近源清洗、近源回注，提供全球 T 级防护能力。通过各清洗节点之后的正常业务流量将会近源回注到服务器，保证业务流量的畅通与低延迟。DDoS 高防 IP（境外企业版）直接对腾讯云上 IP 生效。

产品功能

多类型防护

防护分类	描述
畸形报文过滤	过滤 frag flood，smurf，stream flood，land flood 攻击，过滤 IP 畸形包、TCP 畸形包、UDP 畸形包。
网络层 DDoS 攻击防护	过滤 UDP Flood、SYN Flood、TCP Flood、ICMP Flood、ACK Flood、FIN Flood、RST Flood、DNS/NTP/SSDP 等反射攻击、空连接。
应用层 DDoS 攻击防护	过滤 CC 攻击和 HTTP 慢速攻击，支持 HTTP 自定义特征过滤，如 host 过滤、user-agent 过滤、referer 过滤。

防护对象可切换

DDoS 高防 IP（境外企业版）支持防护对象 IP 切换，满足腾讯云非中国大陆区资源公网 IP 需要防护的需求，支持切换的对象包括 CVM、CLB。

> 说明：
> 当前支持：莫斯科、硅谷、法兰克福、首尔、中国香港、东京、新加坡、曼谷、孟买。

安全防护策略

DDoS 高防 IP（境外企业版）默认提供基础安全策略，策略基于 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，您可根据特殊业务特点灵活设置，应对不断变化的攻击手法。

封堵自助解除

当攻击流量突发或 DDoS 高防 IP（境外企业版）防护带宽较小，造成接入高防的业务 IP 被封堵时，您可通过控制台进行自助解除。

防护统计报表

DDoS 高防 IP（境外企业版）提供多维度流量报表及攻击防护详细信息，帮助您及时、准确了解境外 Anycast DDoS 高防 IP 的防护效果。

> 说明：
> 当前只支持 DDoS 攻击防护报表展示，CC 攻击防护报表和业务报表暂未支持，后续开放。

产品优势

最近更新时间：2022-12-21 16:10:29

DDoS 高防 IP（境外企业版）是一键为腾讯云内 CVM、CLB 提升 DDoS 防护能力的付费安全服务，具有如下优势：

贴合云原生的防护架构，一键接入

产品方案更贴合云原生的防护架构，接入配置便捷。购买 DDoS 高防 IP（境外企业版）后，只需要将高防实例关联到所需的防护对象，实现一键式接入，快速部署。

超大防护资源

DDoS 高防 IP（境外企业版）整合腾讯云中国大陆以外的高防清洗中心能力，覆盖境外10个清洗节点，提供全球 T 级防护能力，满足活动大促、活动上线等重要业务的安全稳定性保障需求。

领先的清洗能力

依托腾讯自研防护集群，采用 IP 画像、行为分析、Cookie 挑战等多维算法，并通过 AI 智能引擎持续更新防护算法，精准快速检测业务流量，灵活应对各类攻击行为。

稳定访问体验

腾讯云 BGP 链路对接多家运营商，覆盖面广，能有效解决访问时延问题保证网络质量。智能选择路由并自动完成网络调度，保障各类用户群的访问稳定性，带来稳定与流畅的访问体验。

丰富的防护报表

DDoS 高防 IP（境外企业版）提供多维度统计报表，展示清晰、准确的攻击防护流量，以及攻击详情信息，让用户及时了解攻击实况。

优化安全成本

1. 简化计费方式，您可以根据业务规模及防护需要，灵活选择 “防护 IP 数+无限次全力防护”，当遭受大流量攻击时：

- 利用全球多个节点防护能力，来同时分担和抵御 DDoS 攻击流量实现全力防护。
- 采用调度&封堵结合的方式，为客户最大化提供的业务可用性，增加被攻击时的可用性。

2. 业务带宽按需后付费，季度售卖的灵活计费模式，为您降低日常安全支出。

应用场景

最近更新时间：2021-07-14 20:01:24

游戏

游戏境外业务是 DDoS 攻击的重灾区，DDoS 高防 IP（境外企业版）能有效保障游戏的可用性和持续性，保障游戏在全球的玩家流畅体验，同时为活动、新游戏发布或节假日游戏收入旺季时段保驾护航，确保游戏业务正常。

电商

电商境外业务遍布世界各地，伴随着不同地区的节日与各种促销，访问与订单不断上升。DDoS 高防 IP（境外企业版）能有效保障全球的业务正常不中断，对电商大促等重大活动时段，提供安全护航。

互联网

保障境外业务网页的流畅访问，全球的业务正常不中断，对特殊节日、特殊事件突发的大量访问与日常正常访问提供稳定安全的服务。

相关概念

最近更新时间：2021-07-14 20:01:45

DDoS 攻击

分布式拒绝服务攻击（Distributed Denial of Service，DDoS）是指攻击者通过网络远程控制大量僵尸主机向一个或多个目标发送大量攻击请求，堵塞目标服务器的网络带宽或耗尽目标服务器的系统资源，导致其无法响应正常的服务请求。

网络层 DDoS 攻击

网络层 DDoS 攻击主要是指攻击者利用大流量攻击拥塞目标服务器的网络带宽，消耗服务器系统层资源，导致目标服务器无法正常响应客户访问的攻击方式。

常见攻击类型包括 SYN Flood、ACK Flood、UDP Flood、ICMP Flood 以及 DNS/NTP/SSDP/memcached 反射型攻击。

CC 攻击

CC 攻击主要指通过恶意占用目标服务器应用层资源，消耗处理性能，导致其无法正常提供服务的攻击方式。常见的攻击类型包括基于 HTTP 或 HTTPS 的 GET/POST Flood、四层 CC 以及 Connection Flood 等攻击方式。

防护能力

防护能力指抵御 DDoS 攻击的能力。 DDoS 高防 IP（境外企业版）智能调度全球不同节点资源进行全力防护。

Anycast

防护地址 Anycast EIP 通过 BGP Anycast 方式广播到各区域运营商，在将此 IP 地址与后端资源进行绑定后，接入区域内的用户流量将引导流量（包括业务流量和攻击流量）就近调度到腾讯云节点（anycast 接入点）完成近源清洗。智能选择路由与自动完成网络调度将用户的网络访问请求稳定送达至腾讯云内实例。

清洗

当目标 IP 的公网网络流量超过设定的防护阈值时，腾讯云 DDoS 防护系统将自动对该 IP 的公网入向流量进行清洗。通过 BGP 路由协议将流量从原始网络路径中重定向到腾讯云 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。

通常情况下，清洗不会影响正常访问，仅在特殊场景或清洗策略配置有误时，可能会对正常访问造成影响。当流量持续一定时间（根据攻击情况动态判断）没有异常时，清洗系统会判定攻击结束，停止清洗。

封堵

当目标 IP 受到的攻击流量超过其封堵阈值时，腾讯云将通过运营商的服务屏蔽该 IP 的所有外网访问，保护云平台其他用户免受影响。简而言之，当您的某个 IP 受到的攻击流量超过当前地域腾讯云最大防护能力时，腾讯云将屏蔽该 IP 的所有外网访问。当您的防护 IP 被封堵时，您可以登录管理控制台进行自助解封。

封堵时长

封堵时长默认为2小时，实际封堵时长与当日封堵触发次数和攻击峰值相关，最长可达24小时。
封堵时长主要受以下因素影响：
• 攻击是否持续：若攻击一直持续，封堵时间会延长，封堵时间从延长时刻开始重新计算。
• 攻击是否频繁：被频繁攻击的用户遭遇持续攻击的概率较大，封堵时间会自动延长。
• 攻击流量大小：被超大型流量攻击的用户，封堵时间会自动延长。

封堵级别

- 单运营商：单个运营商进行封堵，通过此运营商一个或多个区域的业务无法访问。
- 单区域节点：单区域的节点进行封堵，该区域的业务无法访问。
- 全区域：腾讯云直接对访问业务的进行封堵，全局业务无法访问。

> 说明：
>
> - 根据攻击的影响面的程度，将触发不同的级别的封堵。
> - 例如：某客户在遭受 DDoS 攻击后，当攻击流量达到该运营商的封堵阈值时，将进行单运营商封堵。若该区域攻击流量达到该区域节点封堵阈值时，将进行该区域节点封堵，该区域的业务将无法访问。若该客户的各个节点的攻击总量达到全区域封堵阈值，则进行该客户的业务全区封堵，将导致全区域的业务无法访问。

调度

当流量达到当下运营商的阈值时，会进行运营商间的调度以保证业务可用性。

> 说明：
> 为了保证业务的可用性，可能会出现多次调度的情况。

购买指南
计费概述

最近更新时间：2022-09-30 10:52:20

背景信息

DDoS 高防 IP (境外企业版)为您部署在中国大陆以外的业务提供针对 DDoS 攻击的不限次数的全力防护服务，致力于帮助客户防护每一次 DDoS 攻击。

一般来说，恶意攻击者发起攻击的目的是为了对目标业务造成损失。由于发起攻击本身也存在成本，如果攻击始终无法达到目的，攻击便会停止。因此，DDoS 高防 IP (境外企业版)提供不限次数的防护服务，调用腾讯云中国大陆以外的高防清洗中心能力，全力保障您的业务。

注意：

- 如果您的业务遭受的攻击，影响到腾讯云中国大陆以外高防清洗中心的基础设施，则腾讯云保留控制流量的权利。DDoS 高防 IP (境外企业版)实例受到流量压制时，可能对您的业务造成一定影响，如：业务访问流量可能会被限速，可能被黑洞。
- 该产品为月度后付费模式，该规格最少购买时长为12个月，期间不支持实例销毁。超过该期限后，将自动续约。若想暂停服务，销毁资源请 联系我们。
- 开通该产品需要冻结3个月授信额度，请保证您有足够的授信额度。
- 本产品不支持退款。

DDoS 高防 IP (境外企业版)的具体计费模式如下：

IP 数(个)	服务费用（美元/月）	付费模式
1	7500	预付费
5	33000	预付费
30	180000	预付费
100	600000	预付费

业务带宽的计费模式如下：

业务带宽计费模式为后付费，将用户账户下所使用带宽的总曲线进行95消峰后，选择出带宽和入带宽中较高的方向收费，单价为18.86美元/ Mbps /月。

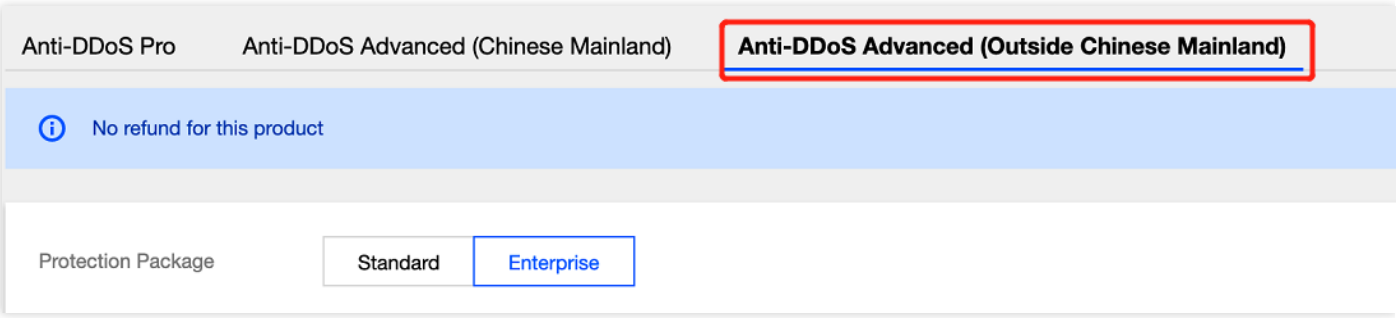
购买指引

最近更新时间：2022-09-30 10:52:21

注意：

- 该产品为月度后付费模式，该规格最少购买时长为12个月，期间不支持实例销毁。超过该期限后，将自动续约。若想暂停服务，销毁资源请 联系我们。
- 开通该产品需要冻结3个月授信额度，请保证您有足够的授信额度。
- 本产品不支持退款。

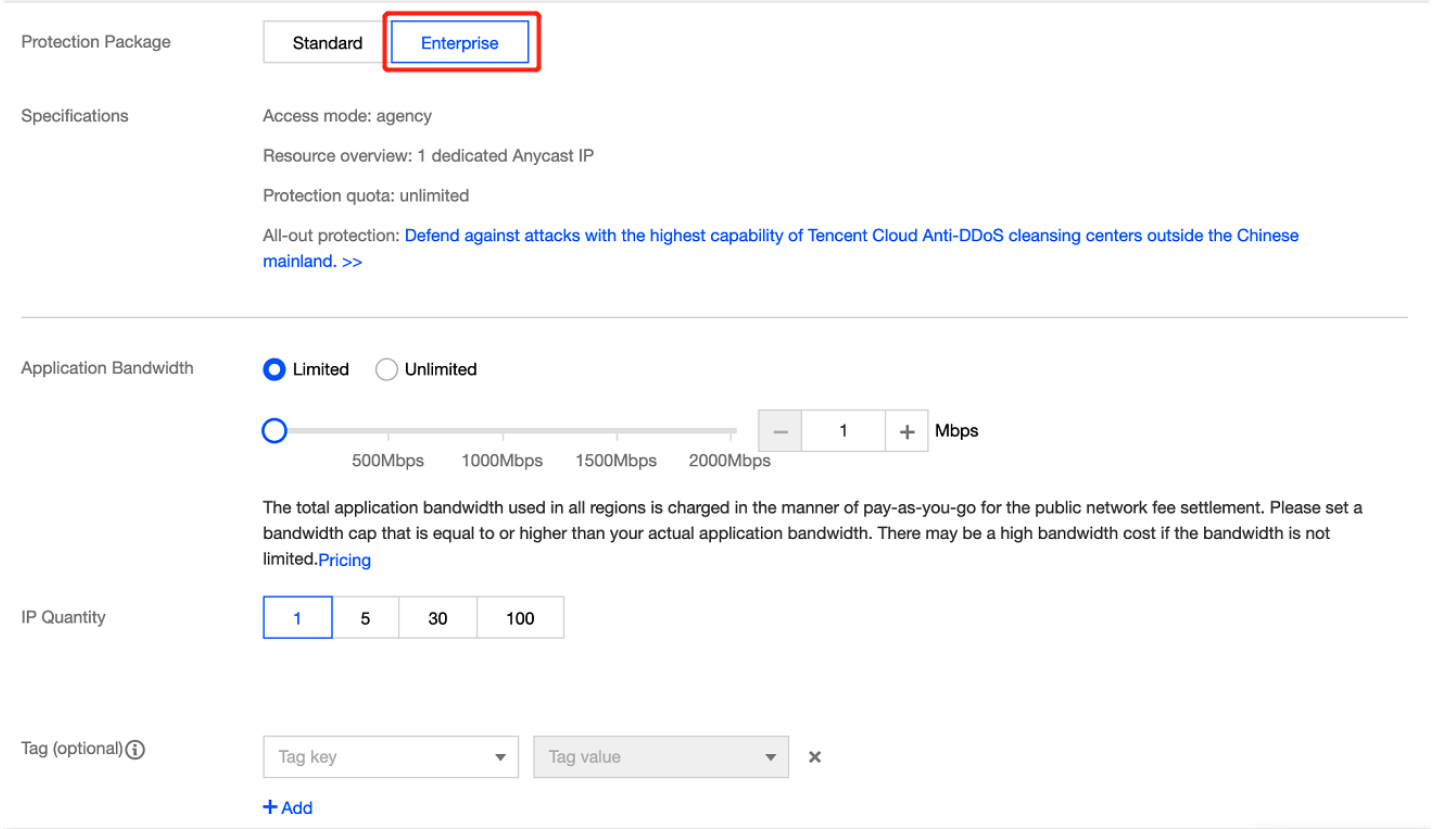
1. 登录 DDoS 高防 IP (境外企业版) 购买页面。
2. 单击“DDoS高防IP(境外)”，进入 DDoS 高防 IP(境外)页面。



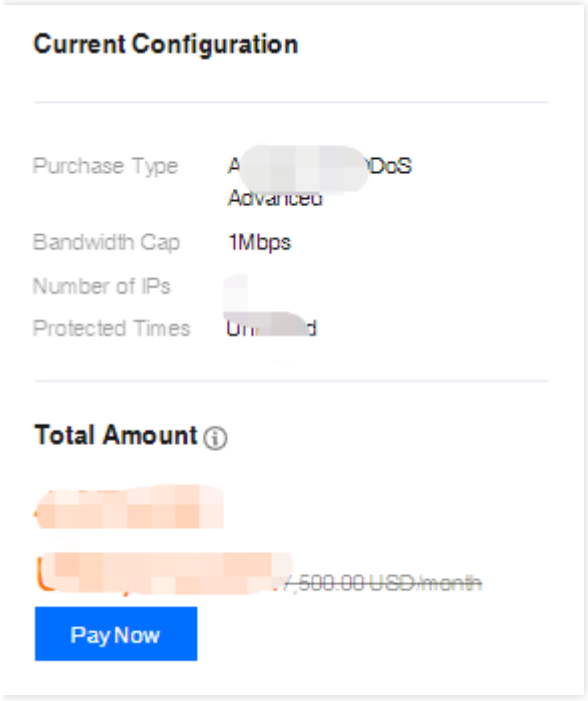
3. 在 DDoS 高防 IP(境外)页面，防护套餐处单击**企业版**，设置“业务带宽”、“IP 数量”、“购买时长”、“自动续费”等相关参数，并选择相对应的业务带宽的类型或上限带宽。

说明：

- 其中自动续费周期为1个月。
- 业务带宽为后付费，在购买页**总计费用**中展示的价格不包含需后付费的业务带宽费用。

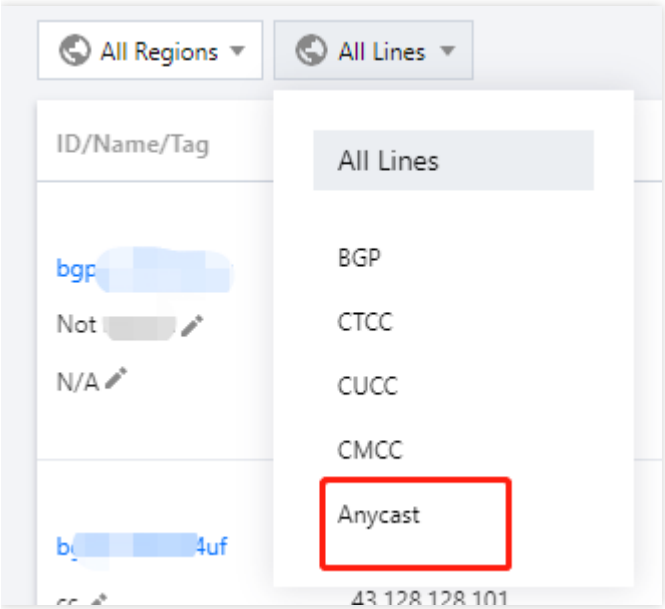


4. 单击**立即支付**,支付费用后即完成服务购买。



5. 登录 DDoS 高防 IP（境外企业版） 控制台，单击 **DDoS 高防 IP** > **实例列表**，进入实例列表页面。

6. 在实例列表页面中，单击选择**全部线路** > **Anycast**可以看到购买的 DDoS 高防 IP (境外企业版)实例信息。



快速入门

最近更新时间：2022-06-10 14:12:06

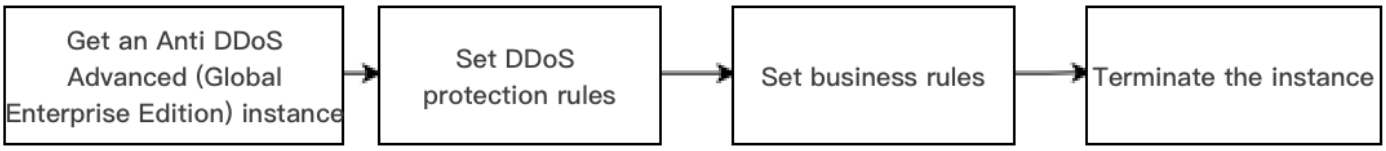
DDoS 高防 IP（境外企业版）是针对业务部署在腾讯云内境外地区的用户，以提升 DDoS 境外防护能力的付费产品。

- DDoS 高防 IP（境外企业版）可以独立购买和持有的公网 IP 地址资源。
- DDoS 高防 IP（境外企业版）绑定云资源后，云资源可以通过 DDoS 高防 IP（境外企业版）与公网通信。

本文以 DDoS 高防 IP（境外企业版）关联云资源为例介绍 DDoS 高防 IP（境外企业版）的使用生命周期。

背景信息

DDoS 高防 IP（境外企业版）的使用生命周期包括购买 DDoS 高防 IP（境外企业版）、DDoS 高防 IP（境外企业版）实例配置防护规则、DDoS 高防 IP（境外企业版）配置业务规则，DDoS 高防 IP（境外企业版）销毁。



1. 购买 DDoS 高防 IP（境外企业版）：根据实际使用需求，购买 DDoS 高防 IP（境外企业版）资源。
2. DDoS 高防 IP（境外企业版）实例 配置防护规则：配置贴合业务的防护策略。
3. DDoS 高防 IP（境外企业版）配置业务规则：将 DDoS 高防 IP（境外企业版） 的实例关联到需防护的云上资源。
4. DDoS 高防 IP（境外企业版）销毁：将 DDoS 高防 IP（境外企业版）与云资源取消关联后，您可以将该 DDoS 高防 IP（境外企业版）与其他云资源关联。取消关联操作可能会导致对应云资源的网络不通，且未绑定云资源的 DDoS 高防 IP（境外企业版）会产生 IP 资源费。

操作步骤

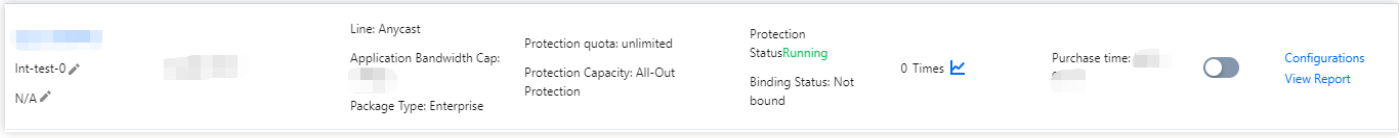
购买 DDoS高防IP（境外企业版）

1. 登录 DDoS 高防 IP（境外企业版） 控制台。

2. 参考上文 购买指引 进行套餐购买。

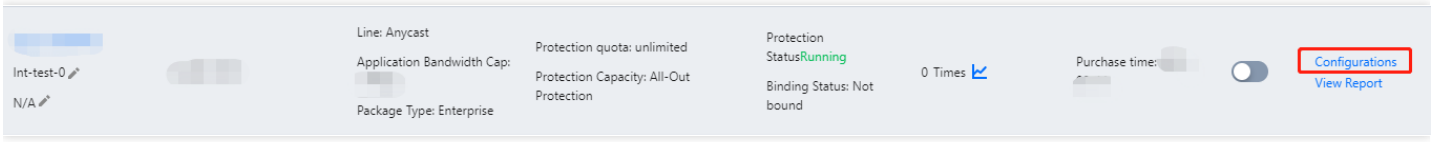
3. 单击控制台 **DDoS 高防 IP** > **实例列表**，即可查看已购买的 DDoS 高防 IP（境外企业版），此时处于未绑定状态。

> 说明：
> 建议您及时为处于未绑定状态的 DDoS 高防 IP（境外企业版）绑定云资源，节省 IP 资源费。IP 资源费按小时计费，精确到秒级，不足一小时，按闲置时间占比收取费用，因此请及时绑定云资源。详细标准可参考 计费概述。



配置防护规则

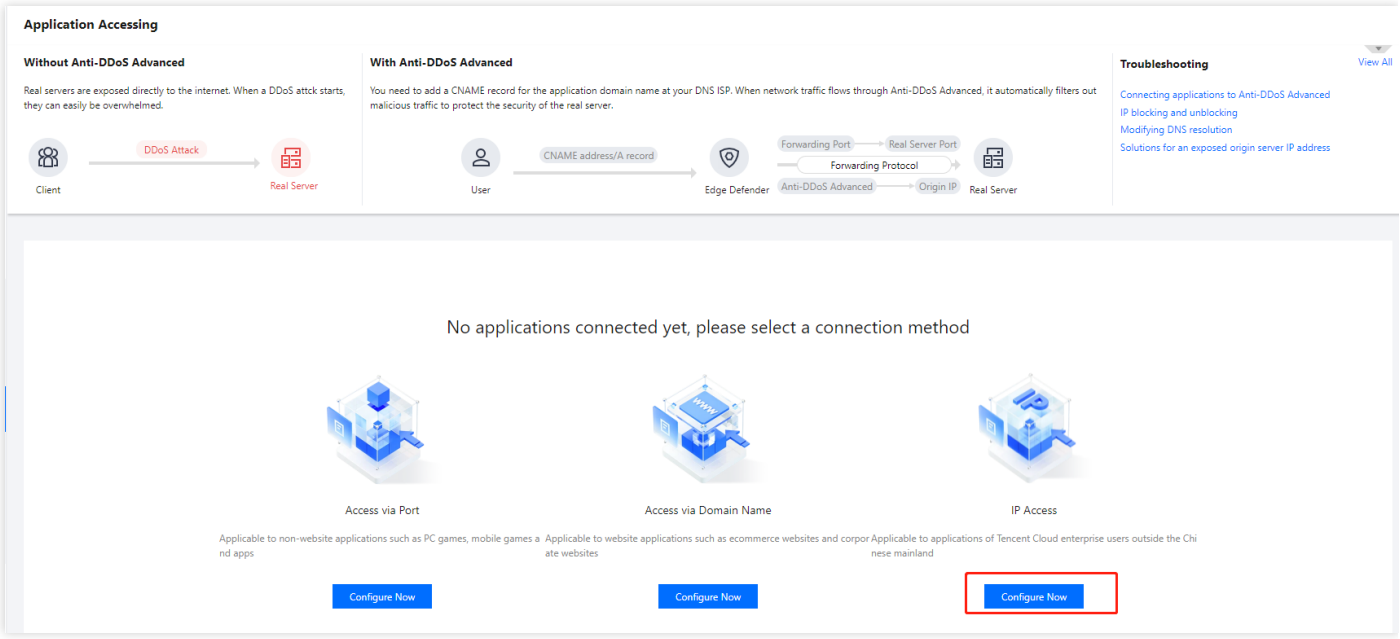
登录 DDoS 高防 IP（境外企业版）控制台，单击 **DDoS 高防 IP** > **实例列表**中，选择对应 DDoS 高防 IP（境外企业版）实例，单击**防护配置**，配置方式可参考 配置防护规则。



关联云资源

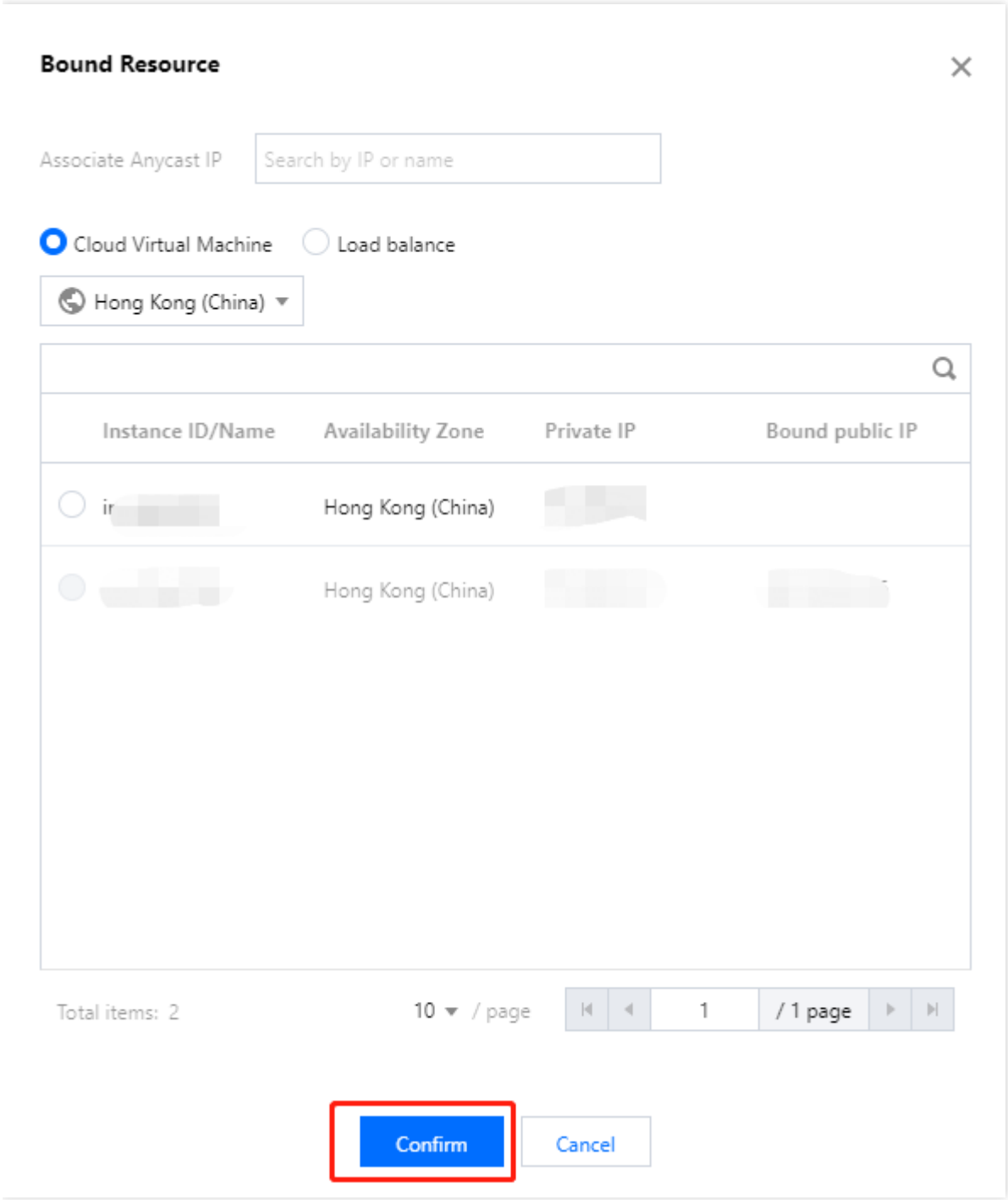
1. 登录 DDoS 高防 IP（境外企业版） 控制台，单击 **DDoS 高防 IP** > **业务接入** > **IP 接入**。

2. 在 IP 接入页面，单击**开始接入**，弹出绑定资源页面。



3. 在 IP 接入页面，“关联 Anycast 高防 IP”处选择 DDoS 高防 IP（境外企业版）实例，单击**确定**，即可完成与云资源的绑定。

> 说明：
> 已绑定公网 IP 或 Anycast IP 的资源不能重复绑定。



解除云资源绑定

1. 在 IP接入页面，选择所需实例，单击操作列的**删除**。
2. 在解除绑定弹窗中，单击**确定**，即可取消关联。

> 注意：
> 解除绑定可能导致您的云资源网络不通，请谨慎操作。解绑后，您可以将该资源绑定其他云资源。

操作指南
操作概览

最近更新时间：2022-05-18 14:14:54

您在使用 DDoS 高防 IP（境外企业版）时，可能碰到如配置 DDoS 高防 IP（境外企业版） 实例、查看安全防护概览、查看操作日志以及设置安全事件通知等问题。本文将介绍使用 DDoS 高防 IP（境外企业版） 的常用操作，供您参考。

防护概览

防护概览

防护配置

DDoS 防护等级
协议封禁
特征过滤
AI 防护
连接类攻击防护
IP 黑白名单
IP 端口限速
区域封禁
端口过滤
水印防护

业务接入

业务接入

实例管理

查看实例信息
设置实例别名与标签

安全事件通知

设置安全事件通知

操作日志

查看操作日志

防护概览

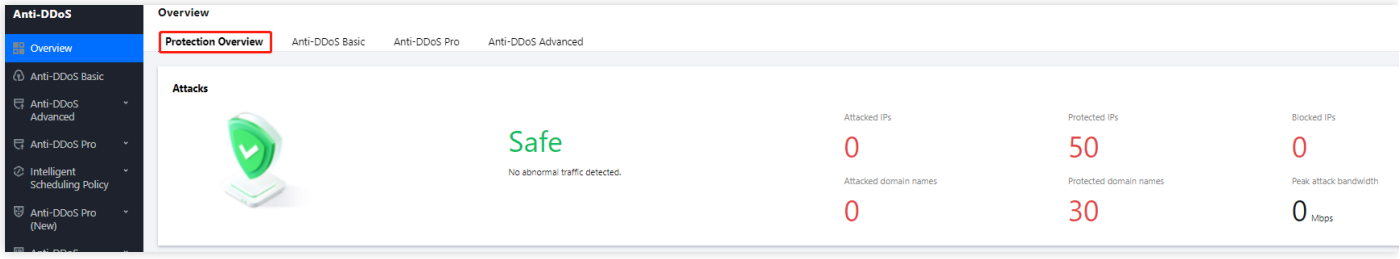
最近更新时间：2023-06-09 09:48:52

防护概览（总览）

用户将业务接入 DDoS 高防 IP（境外企业版） 服务，且将业务流量切换至 DDoS 高防 IP（境外企业版） 后，可在控制台查看业务流量情况和 DDoS 攻击防护情况。支持抓包下载攻击数据，便于用户分析与溯源。

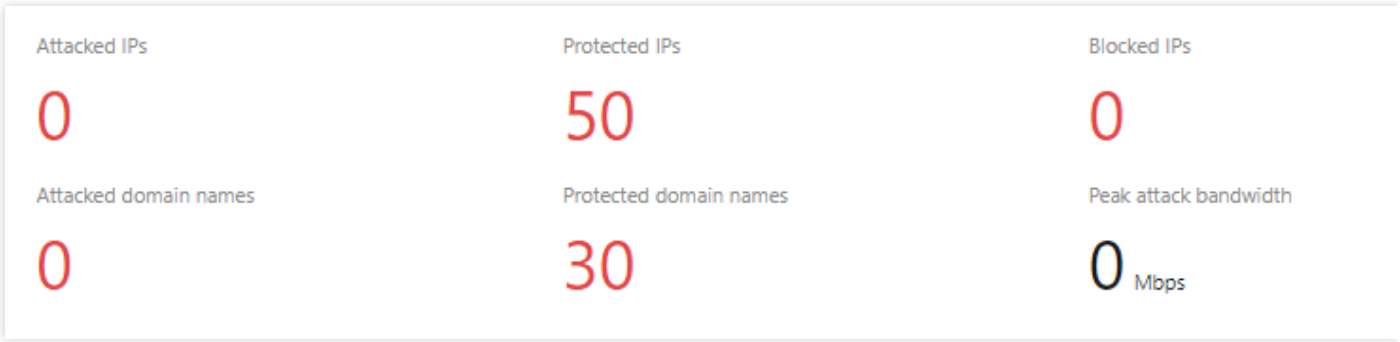
查看攻击态势

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航栏中，单击**防护概览 > 防护总览**。



2. 在攻击态势模块中，可查看当前业务是否存在风险，和最近一次攻击的时间的攻击类型。当有攻击存在时，单击**升级防护**可进入购买页。

3. 在攻击态势模块中，还可以直观查看各项数据情况。



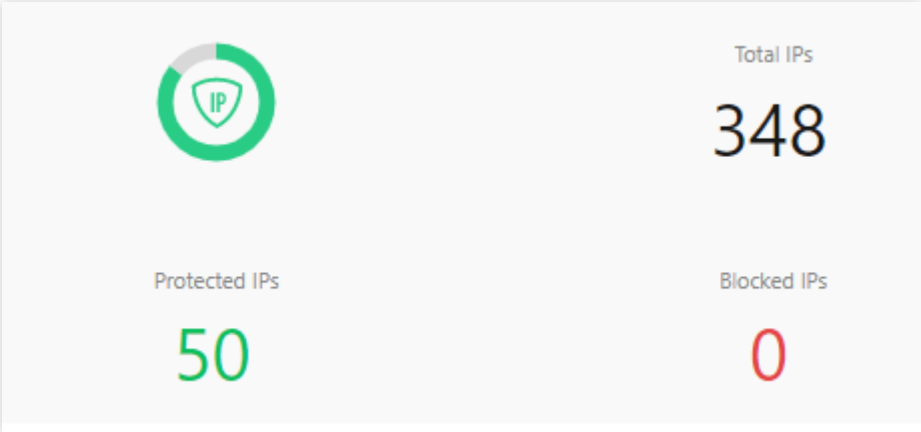
字段说明：

- 被攻击 IP 数：受到攻击的业务 IP 总数。包括基础防护被攻击 IP 数、接入高防包后被攻击的业务 IP 数、高防 IP 实例被攻击数。
- 已防护 IP 数：接入高防包的业务 IP 和高防 IP 实例。

- 被封堵 IP 数：被屏蔽所有外网访问的业务 IP 数。包括基础防护的业务 IP、接入高防包的业务 IP 和高防 IP 实例。
- 被攻击域名数：高防 IP 被攻击的域名数、被攻击的端口所影响的域名数。
- 已防护域名数：高防 IP 实例的域名接入数量。
- 攻击峰值：当前攻击事件中的最高攻击带宽。

查看防御态势

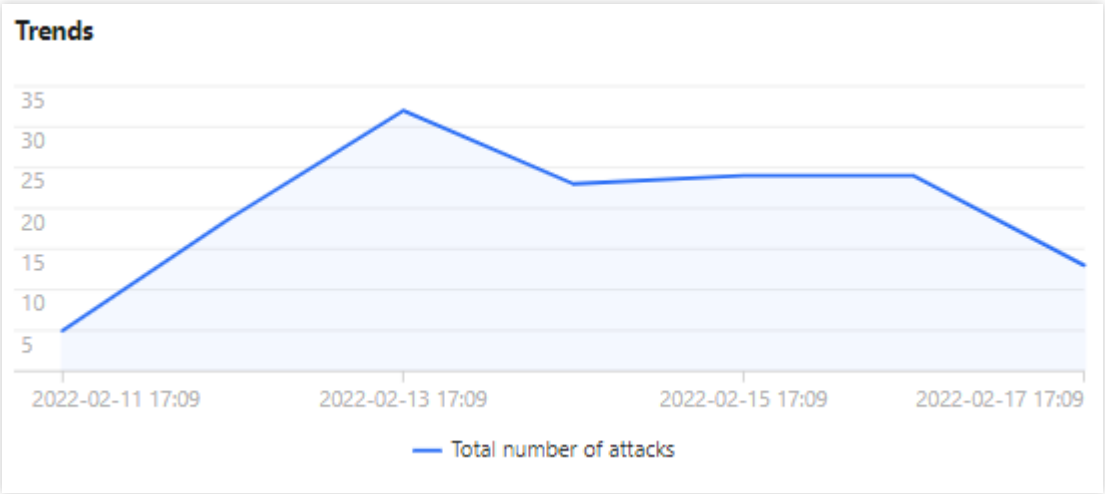
1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航栏中，单击**防护概览 > 防护总览**。
2. 在防御态势模块的统计图中，展示业务 IP 状态数据，可以快速了解业务 IP 健康状态。



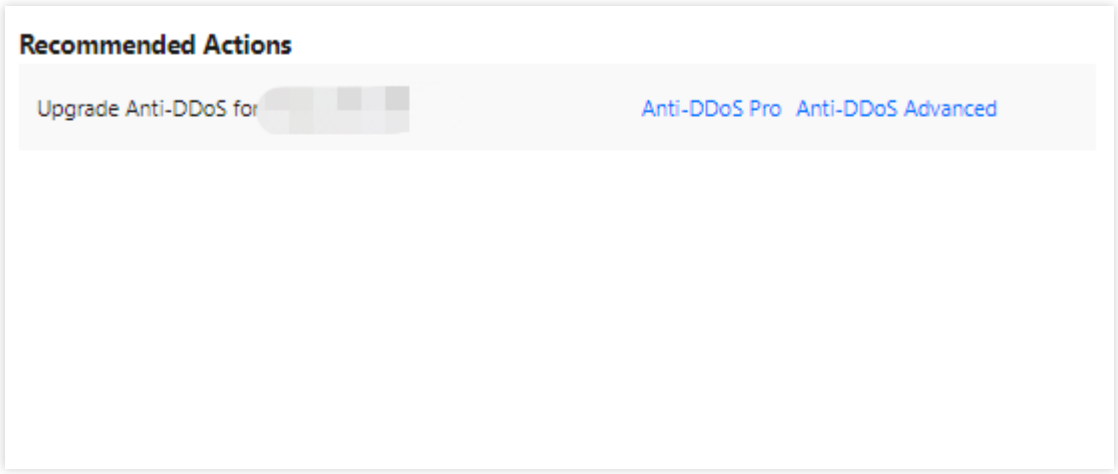
字段说明：

- IP 总数：当前全部业务 IP 总数，包括基础防护的业务 IP、接入高防包的业务 IP 和高防 IP 实例。
- 已防护 IP 数：接入高防包的业务 IP 和高防 IP 实例。
- 封堵 IP 数：被屏蔽所有外网访问的业务 IP 数。包括基础防护的业务 IP、接入高防包的业务 IP 和高防 IP 实例。

3. 在防御态势模块的防护趋势中，展示一周内全量业务受攻击总次数，可以快速了解近期攻击状态分布情况。

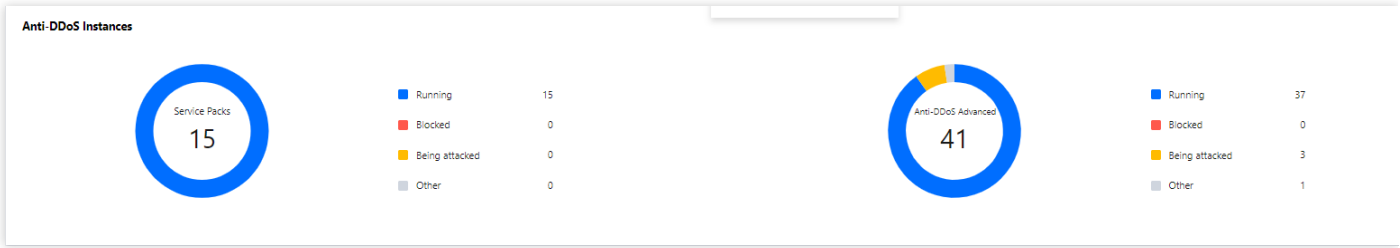


4. 在防御态势模块的防护建议中，展示基础防护状态下受到攻击的业务 IP，提示接入高级防护。方便用户快速为被攻击 IP 接入高级防护，保证业务安全。



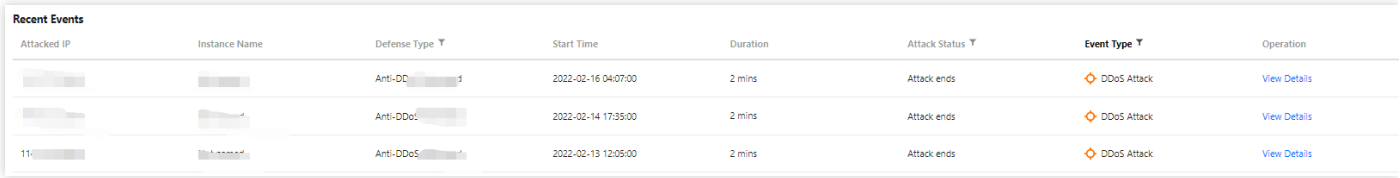
查看高防 IP 实例统计

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航栏中，单击**防护概览 > 防护总览**。
2. 在高防实例统计模块中，展示高防 IP 资源的安全状态，可以快速全面了解风险业务分部。

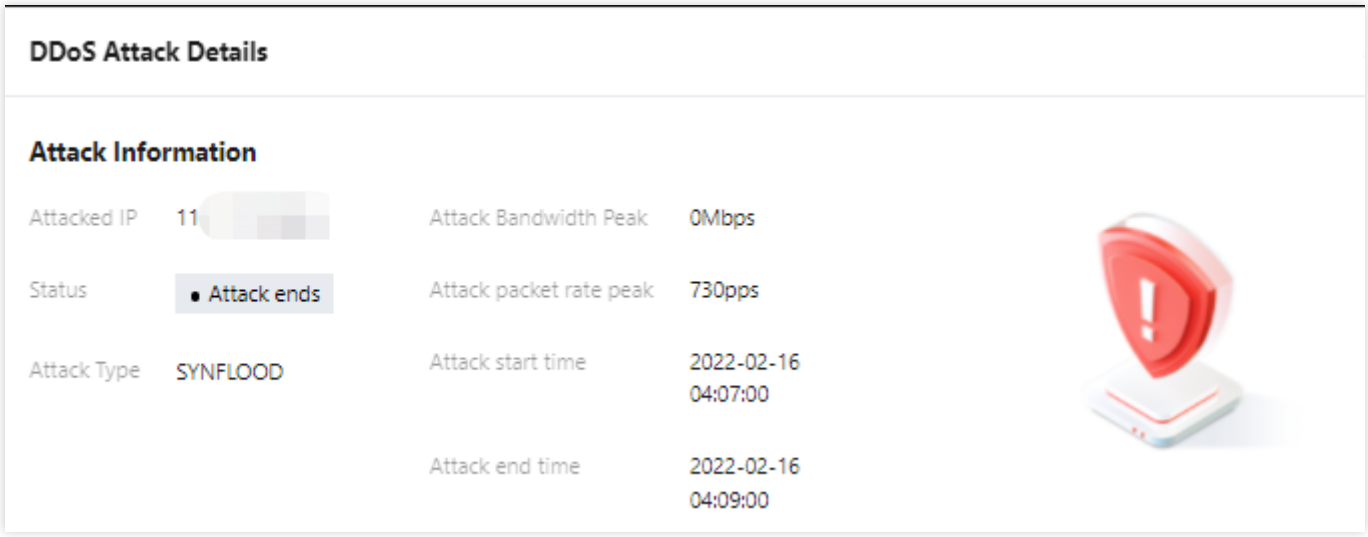


查看近期安全事件

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航栏中，单击**防护概览 > 防护总览**。
2. 在近期安全事件模块中，展示最近全量的攻击事件。单击**查看详情**，进入事件详情页面，供用户进行 DDoS 攻击分析及溯源支撑。

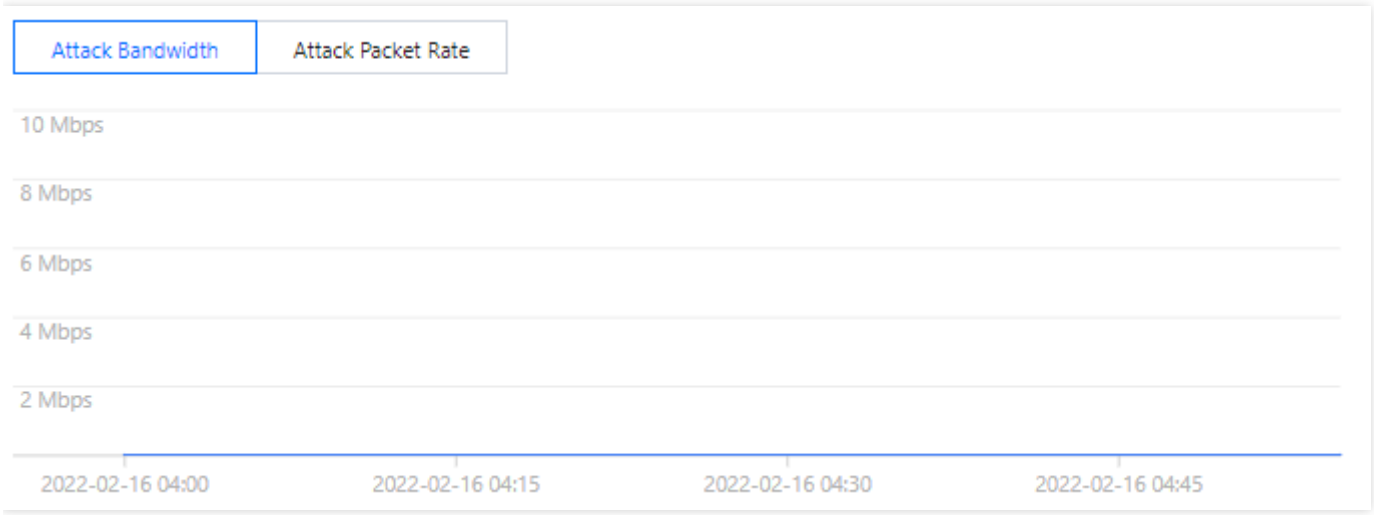


3. 在事件详情页面的攻击信息模块，查看该时间范围内的 IP 遭受的攻击情况，包括被攻击 IP、状态、攻击类型（采样数据）、攻击带宽峰值和攻击包速率峰值、开始时间结束时间基础信息。



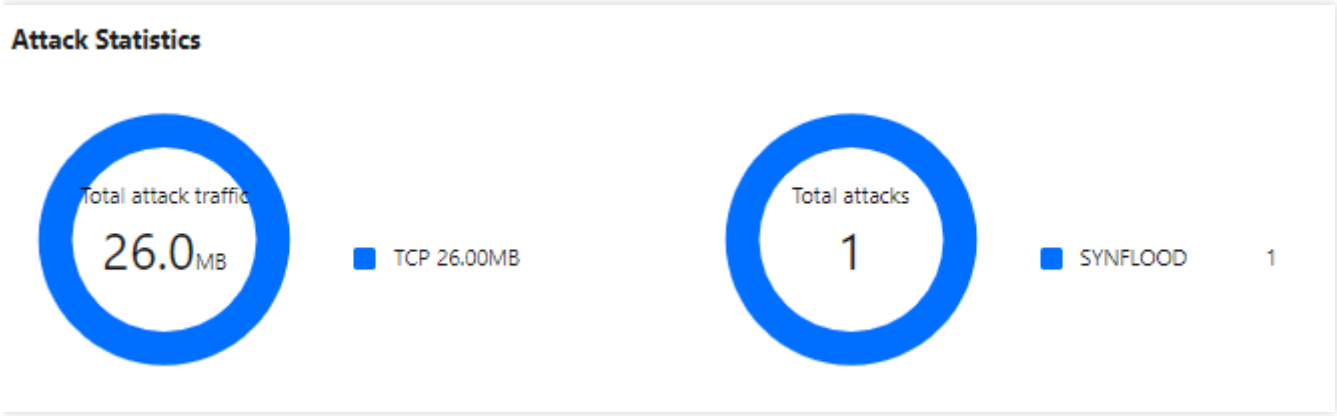
4. 在事件详情页面的攻击趋势模块，可查看网络攻击流量带宽或攻击包速率趋势。当遭受攻击时，在流量趋势图中可以明显看出攻击流量的峰值。

> 说明：
> 此处数据为该攻击时间段全量实时数据。



5. 在事件详情页面的攻击统计模块，可通过攻击流量协议分布、攻击类型分布，查看这两个数据维度下的攻击分布情况。

> 说明：
> 此处数据为该攻击时间段内攻击采样数据，非全量数据。

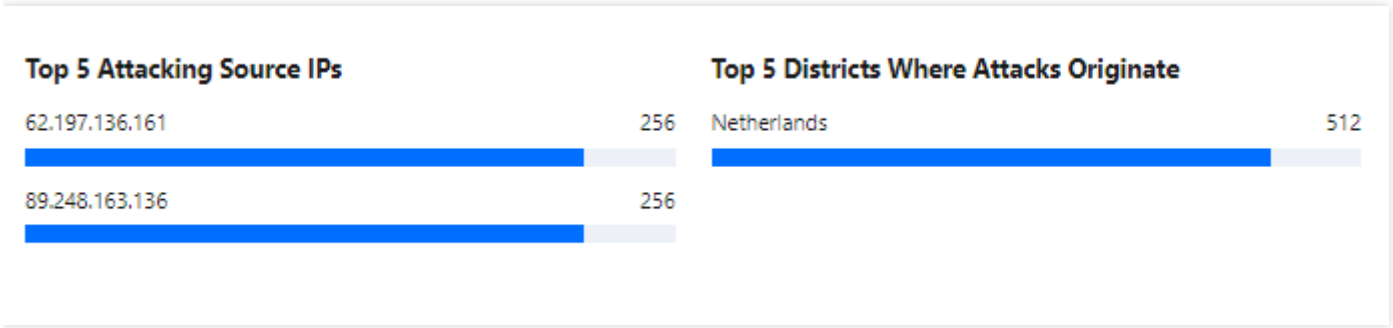


字段说明：

- 攻击流量协议分布：查看该时间范围内，所选择的高防 IP 实例遭受攻击事件中各协议总攻击流量的占比情况。
- 攻击类型分布：查看该时间范围内，所选择的高防 IP 实例遭受的各攻击类型总次数占比情况。

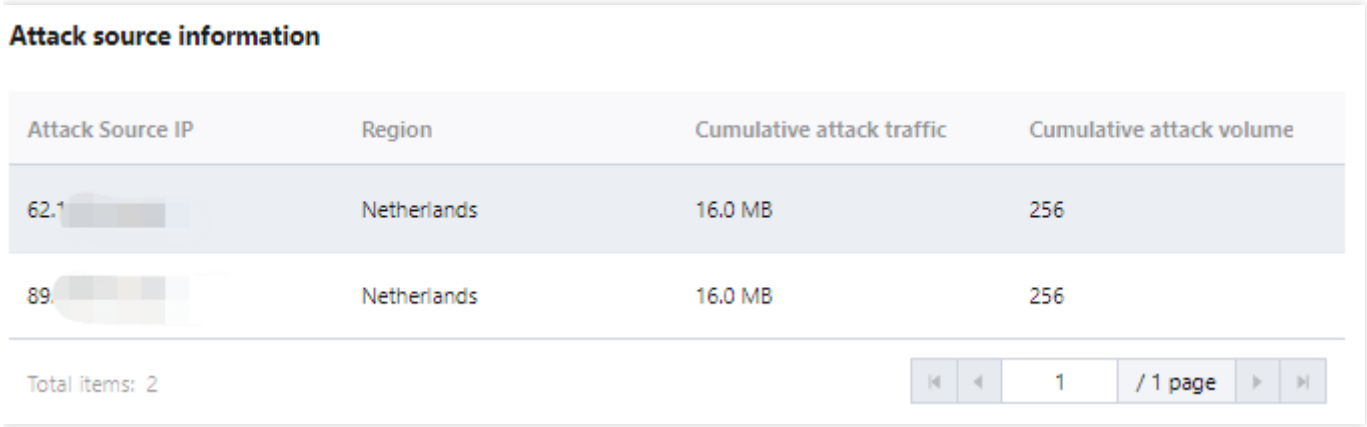
6. 在事件详情页面 “TOP5 展示”模块，可查看攻击源 IP TOP5 和攻击源地区TOP5，准确把握攻击源的详细情况便于精准防护策略的制定。

> 说明：
> 此处数据为该攻击时间段内攻击采样数据，非全量数据。



7. 在事件详情页面的攻击源信息模块，可查看该攻击时间段内攻击详情的随机采样数据，尽可能详细的展示出此次攻击的细节，主要包括攻击源 IP、地域、累计攻击流量、累计攻击包量。

> 说明：
> 此处数据为该攻击时间段内攻击采样数据，非全量数据。

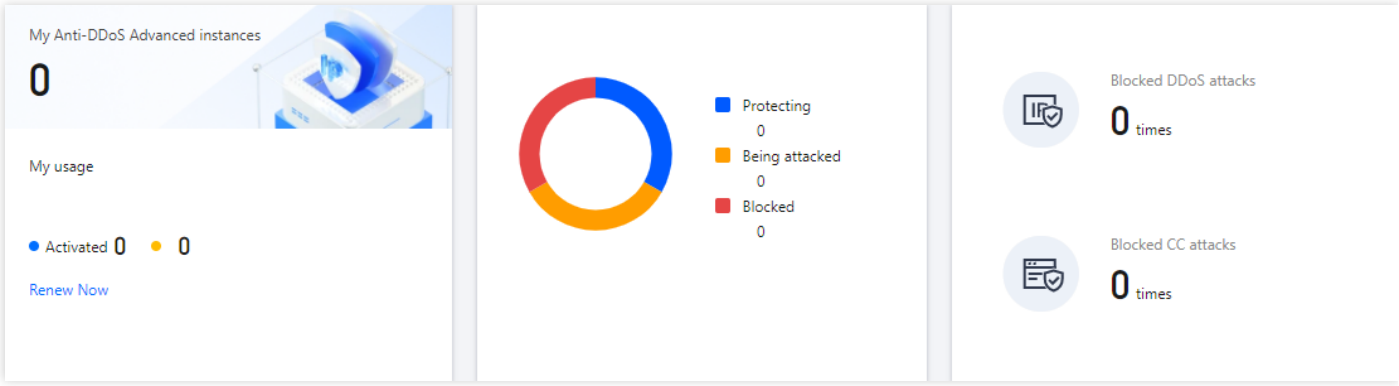


DDoS 高防 IP 概览

将防护 IP 接入到 DDoS 高防 IP 服务后，当用户收到 DDoS 攻击提醒信息或发现业务出现异常时，需要快速了解攻击情况，包括攻击流量大小、防护效果等，可在控制台进行查看。在掌握足够信息后，才可以采取更有效的处理方式，第一时间保障业务正常。

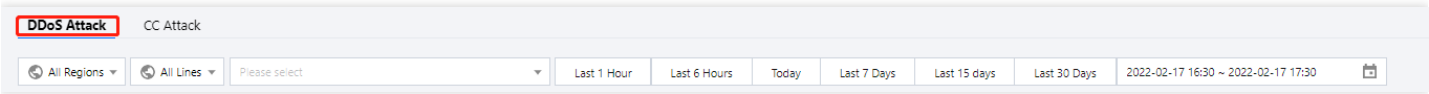
查看 DDoS 攻击防护情况

1. 登录 DDoS 高防 IP（境外企业版） 控制台。在左侧导航栏中，单击**防护概览** > **DDoS 高防 IP**。

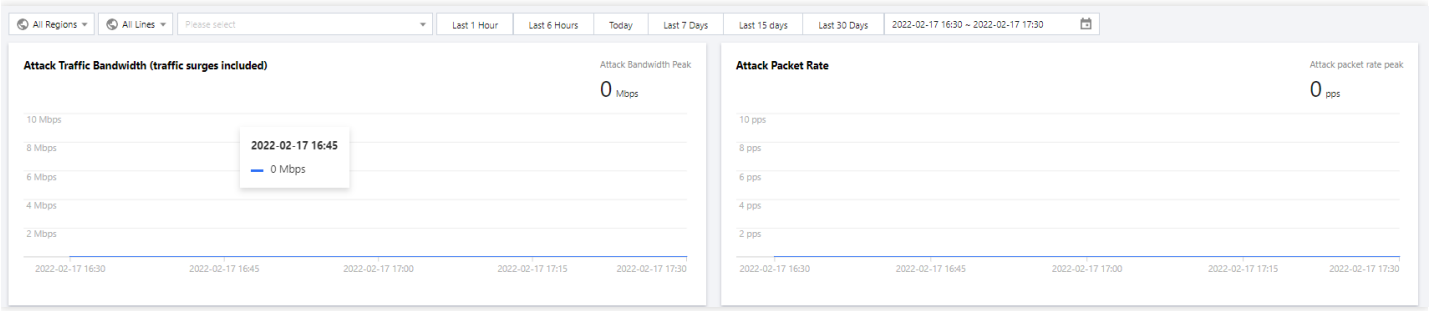


2. 在 DDoS 攻击页签，设置查询时间范围，单击选择**全部线路** > **Anycast**，查看是否存在攻击。默认展示全量资产的DDoS攻击数据。

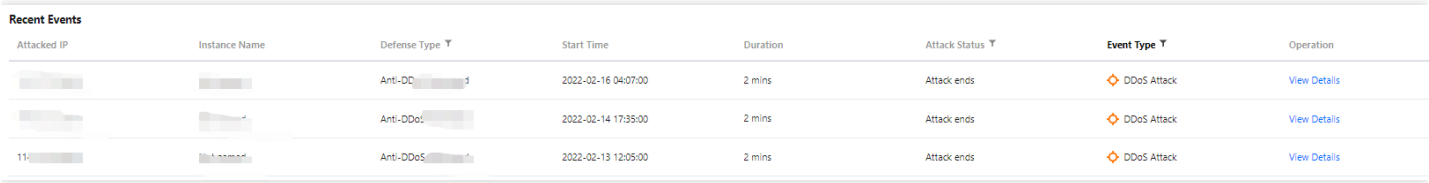
> 说明：
> 支持查询最多180天以内的攻击流量信息及 DDoS 攻击事件。



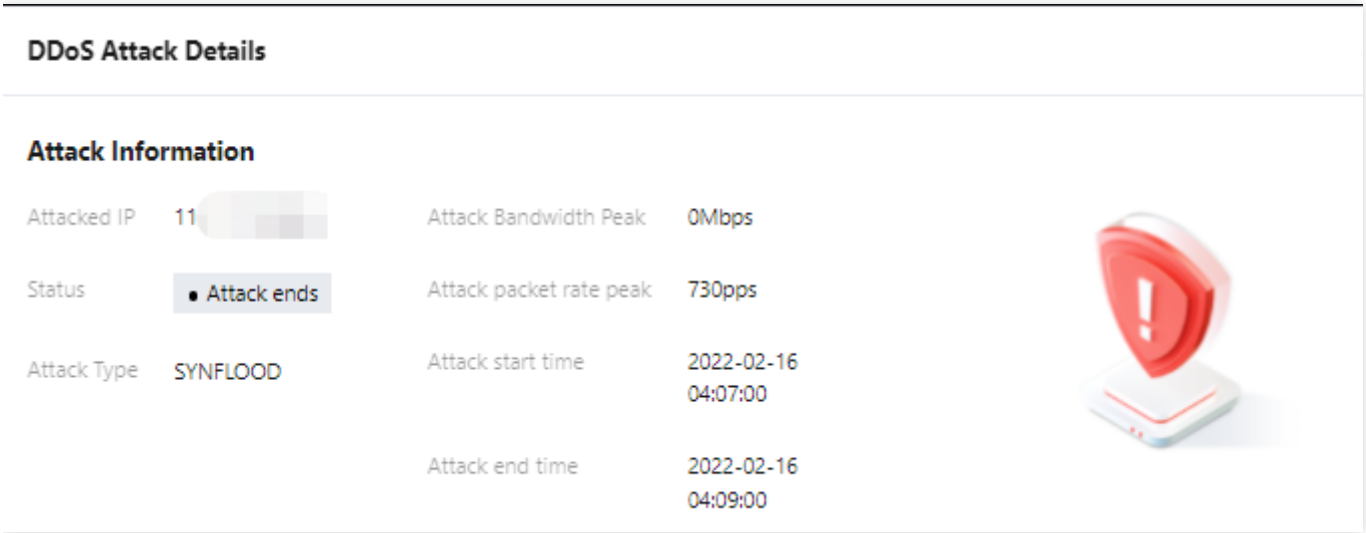
2. 查看该时间范围内所选择的高防 IP 防护遭受的攻击情况，包括网络攻击流量带宽 / 攻击包速率趋势。



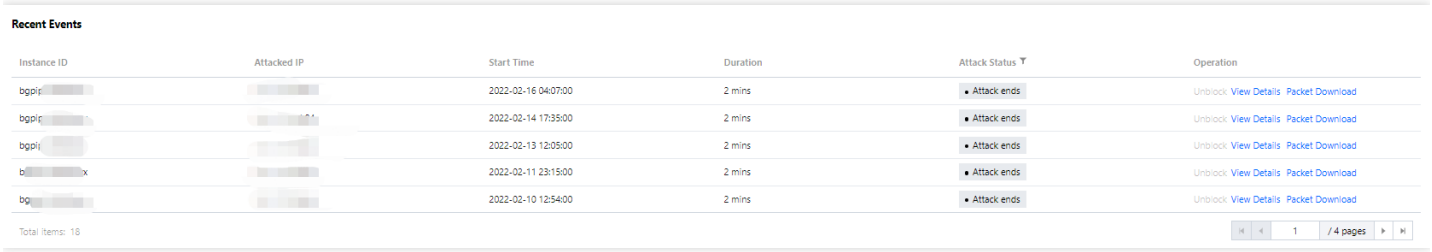
3. 在近期安全事件模块中，可展示所遭受的 DDoS 攻击事件。单击**查看详情**，可查看该事件的具体详情。



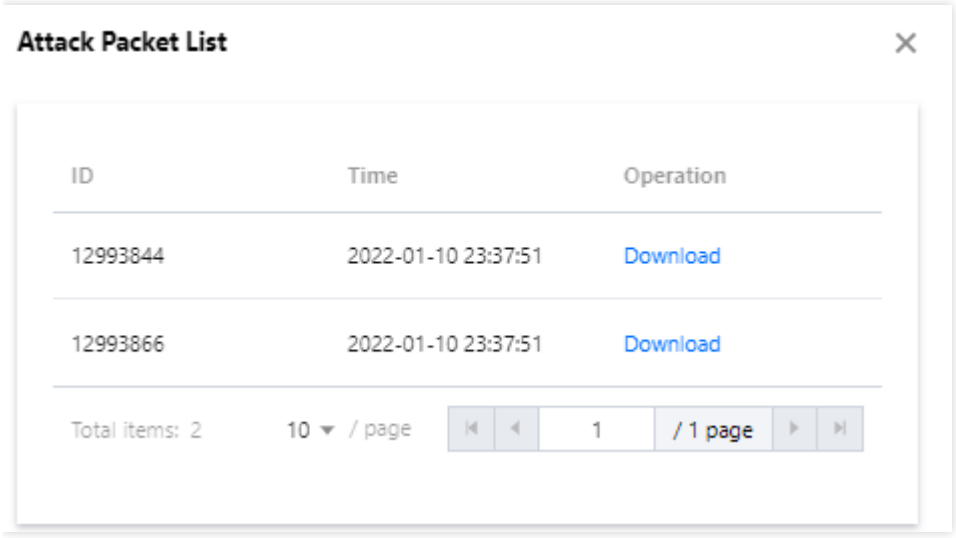
- 支持查看攻击源信息、攻击源地区、产生的攻击流量及攻击包量大小等。供用户进行 DDoS 攻击分析及溯源支撑。



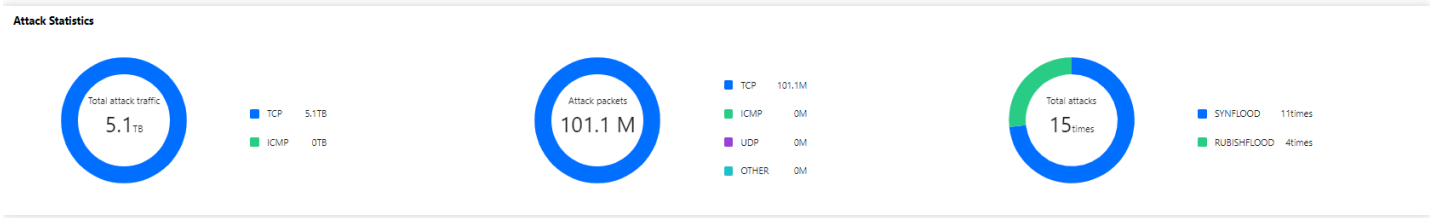
- 单击**攻击包下载**，可看到该攻击时间段的攻击采样数据列表。



- 下载本次攻击计时间段的攻击包采样数据，了解攻击详情，为制定针对性的防护方案提供数据支撑。



4. 在攻击统计模块中，可通过攻击流量协议分布、攻击包协议分布和攻击类型分布，查看这三个数据维度下的攻击分布情况。

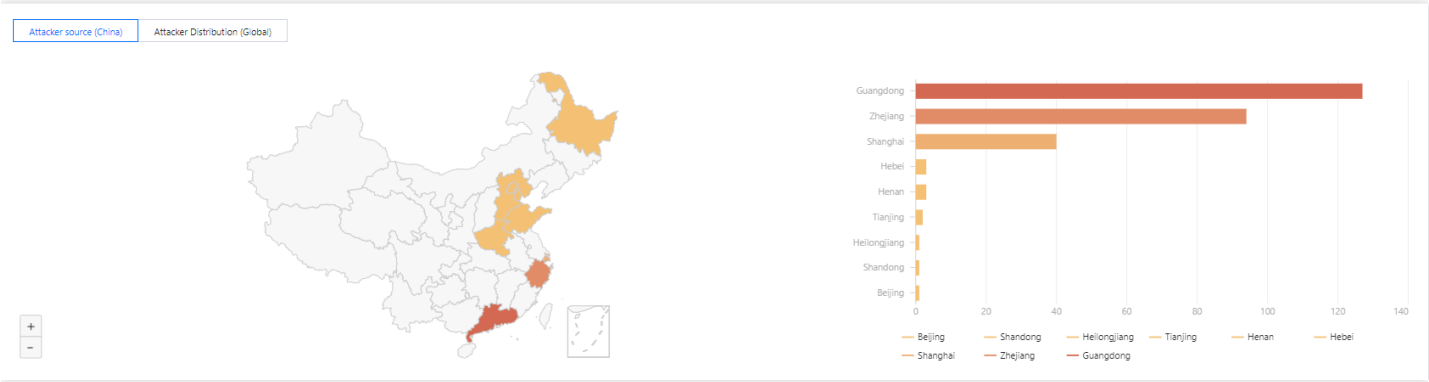


字段说明：

- 攻击流量协议分布：查看该时间范围内，所选择的高防 IP 实例遭受攻击事件中各协议总攻击流量的占比情况。
- 攻击包协议分布：查看该时间范围内，所选择的高防 IP 实例遭受攻击事件中各协议攻击包总数的占比情况。
- 攻击类型分布：查看该时间范围内，所选择的高防 IP 实例遭受的各攻击类型总次数占比情况。

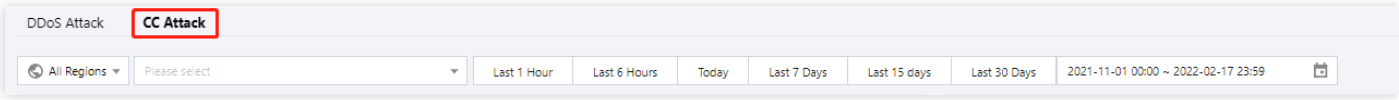
5. 在攻击来源模块中，可查看该时间范围内，所遭受 DDoS 攻击事件的攻击源在国内、全球的分布情况，便于用户

清晰了解攻击来源情况，为进一步防护措施提供基础依据。

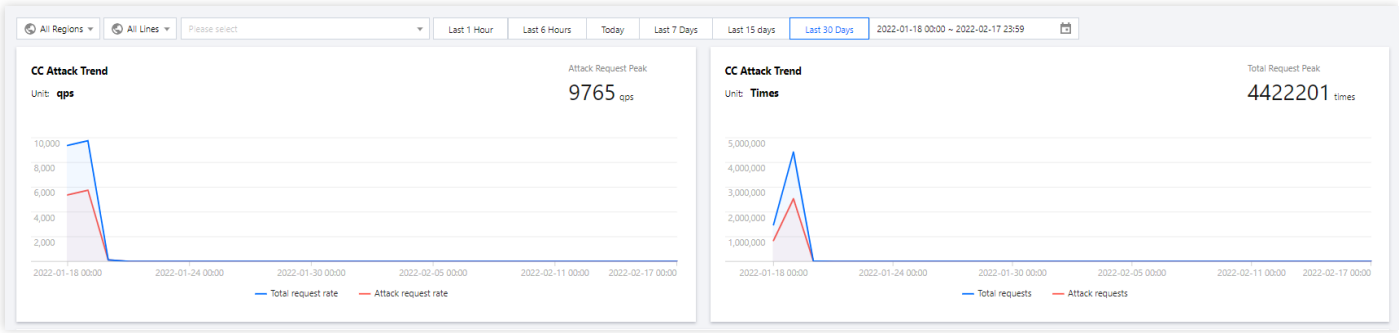


查看 CC 攻击防护情况

1. 单击 **CC 攻击**防护页签，设置查询时间范围，单击选择**全部线路** > **Anycast**，查看是否存在 CC 攻击。



2. 用户可以选择**今天**，查看所选择的高防包的请求数趋势和请求速率的相关数据。通过观察总请求速率、攻击请求速率、总请求数量、攻击请求次数相关数据判定业务受影响程度。

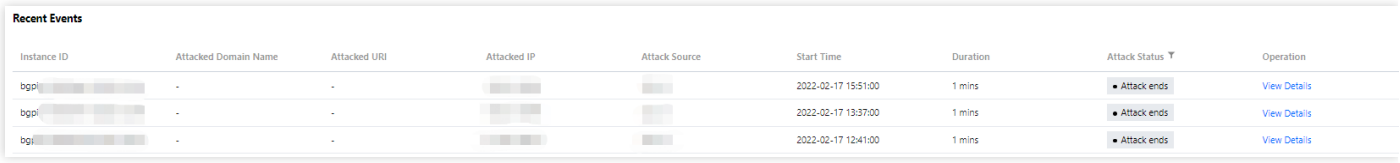


字段说明：

- 总请求速率：统计当前，高防 IP 接收到的总请求流量的速率（QPS）。
- 攻击请求速率：统计当前，攻击请求流量的速率（QPS）。
- 总请求数量：统计当前，高防 IP 接收到的总请求数量。
- 攻击请求次数：统计当前，高防 IP 接收到的攻击请求的次数。

3. 在近期安全事件模块中，如果存在 CC 攻击，系统会记录下攻击的开始时间、结束时间、被攻击域名、被攻击 URI 、总请求峰值、攻击请求峰值和攻击源等信息。单击**查看详情**，展示该事件的具体详情。支持查看攻击信

息、攻击趋势、CC 详细记录。



防护配置
DDoS 防护
DDoS 防护等级

最近更新时间：2022-04-28 10:09:41

本文档将为您介绍针对 DDoS 攻击，DDoS 高防 IP（境外企业版） 提供的不同防护等级的相关操作及应用场景，并为您介绍如何在控制台中设置 DDoS 防护等级。

应用场景

DDoS 高防 IP 服务提供防护策略调整功能，针对 DDoS 攻击提供三种防护等级供您选择，各个防护等级的具体防护操作如下：

- 宽松防护
- 适中防护
- 严格防护

防护等级	防护操作	描述
宽松	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 过滤具有明确攻击特征的 UDP 数据包。	• 清洗策略相对宽松，仅对具有明确攻击特征的攻击包进行防护。 • 建议在怀疑有误拦截时启用，遇到复杂攻击时可能会有攻击透传。

说明：

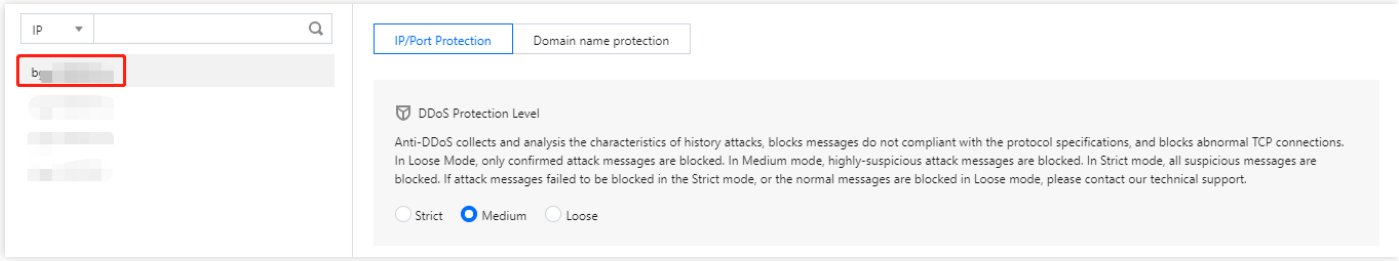
- 如果您的业务需要使用 UDP，建议您联系 腾讯云技术支持 进行策略定制，以免严格模式影响业务流程。
- 默认情况下，您所购买的 DDoS 高防 IP（境外企业版） 实例采用适中防护等级,您可以根据实际业务情况自由调整 DDoS 防护等级。同时，您还可以自定义设置清洗阈值，当攻击流量超过设置的阈值时，将启动清洗。

前提条件

您需要成功 购买 DDoS 高防 IP （境外企业版） ，并设置防护对象。

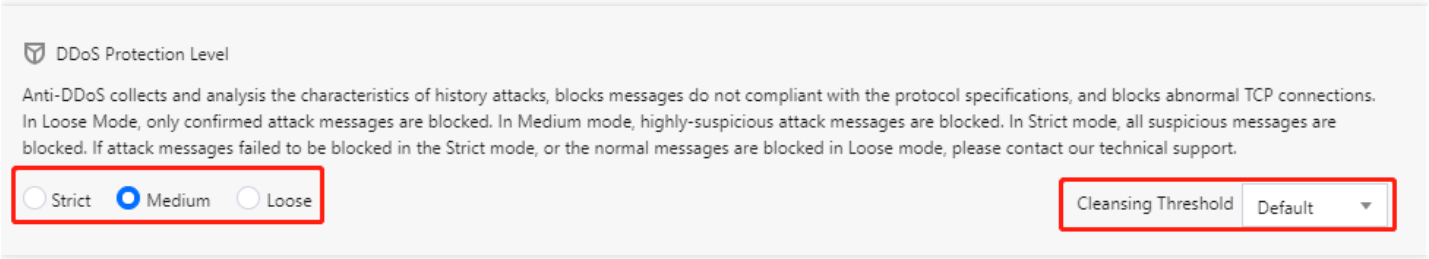
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台 ，在左侧导航中，单击 **DDOS 高防 IP** > **防护配置** > **DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。



3. 在右侧“DDoS 防护等级”卡片中，设置“防护等级”与“清洗阈值”。

> 说明：
> 若明确该清洗阈值，可进行自定义设置。若无法明确该清洗阈值，DDoS 防护系统将根据 AI 算法自动学习并生成一套专属的默认阈值。



配置参数说明：

- **防护等级**
  默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防 IP 实例采用适中防护等级，您可以根据实际业务防护需求自由调整 DDoS 防护等级。
- **清洗阈值**
  - 清洗阈值是高防产品启动清洗动作的阈值，当流量小于阈值时，即使检测到攻击也不会进行清洗操作。
  - 默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防 IP 实例的清洗阈值采用默认值，并随着接入业务流量的变化规律，系统自动学习形成一个基线值。您可以根据实际业务情况自由设置清洗阈值。

协议封禁

最近更新时间：2022-04-28 10:55:43

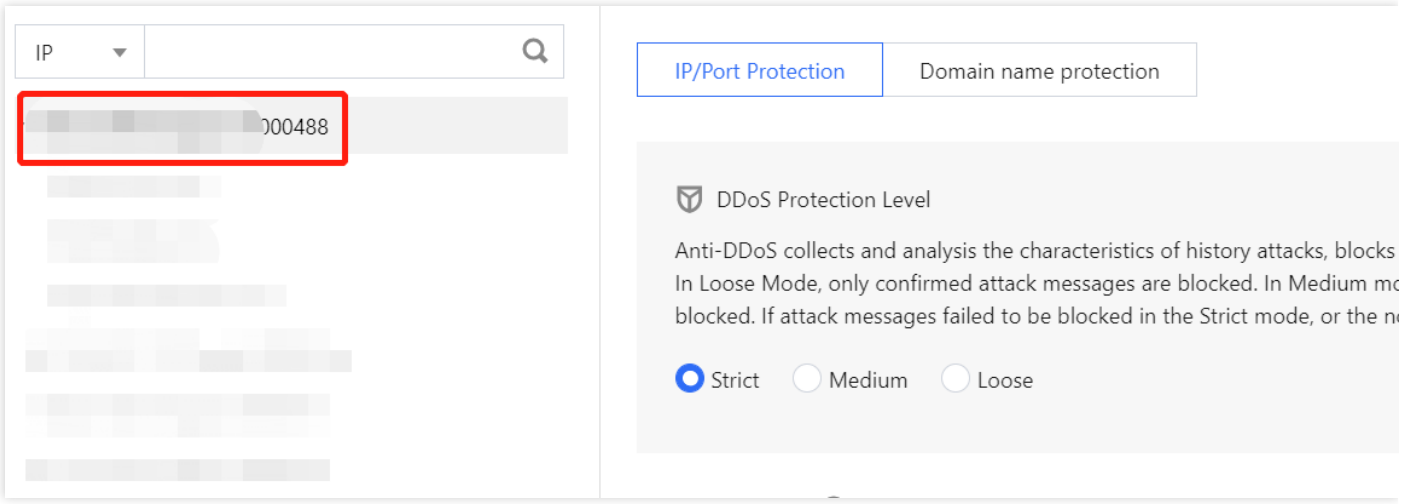
DDoS 高防 IP （境外企业版）支持对访问 DDoS 高防 IP 的源流量按照协议类型一键封禁。您可配置 ICMP 协议封禁、TCP 协议封禁、UDP 协议封禁和其他协议封禁，配置后相关访问请求会被直接截断。由于 UDP 协议的无连接性（不像 TCP 具有三次握手过程）具有天然的不安全性缺陷，若您没有 UDP 业务，建议封禁 UDP 协议。

前提条件

您需要成功 购买 DDoS 高防 IP （境外企业版），并设置防护对象。

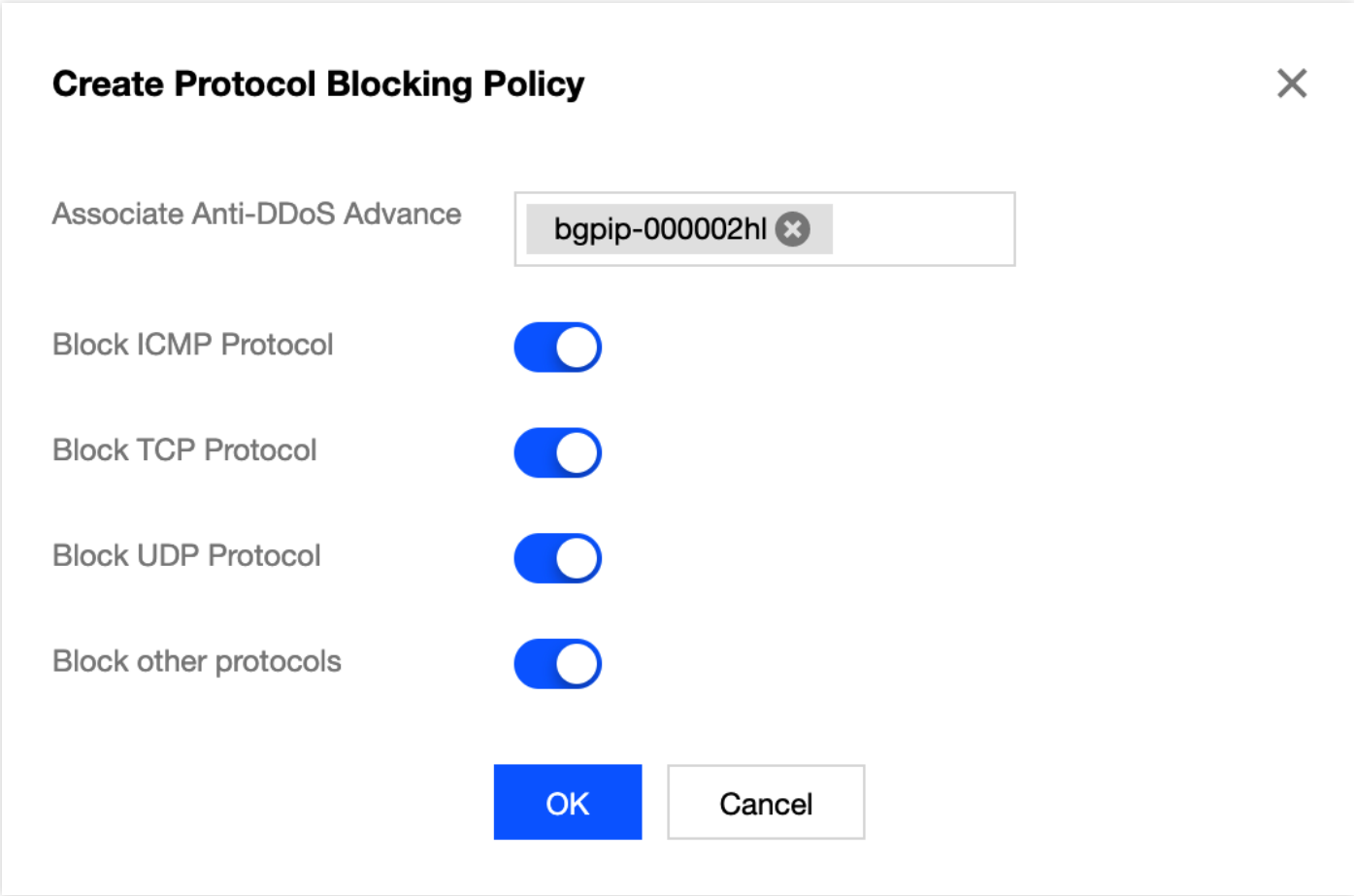
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDOS 高防 IP>防护配置 > DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。

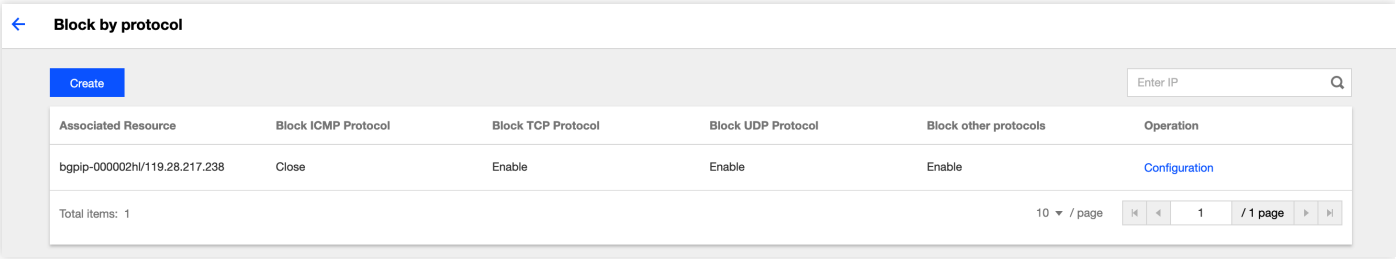


3. 在协议封禁卡片中，单击**设置**。

4. 在协议封禁页面，单击**新建**，设置相关条件，单击**确定**，创建协议封禁规则。



5. 新建完成后，协议封禁列表将新增一条协议封禁规则，单击“开关”，可修改协议封禁规则。



特征过滤

最近更新时间：2022-04-28 10:55:43

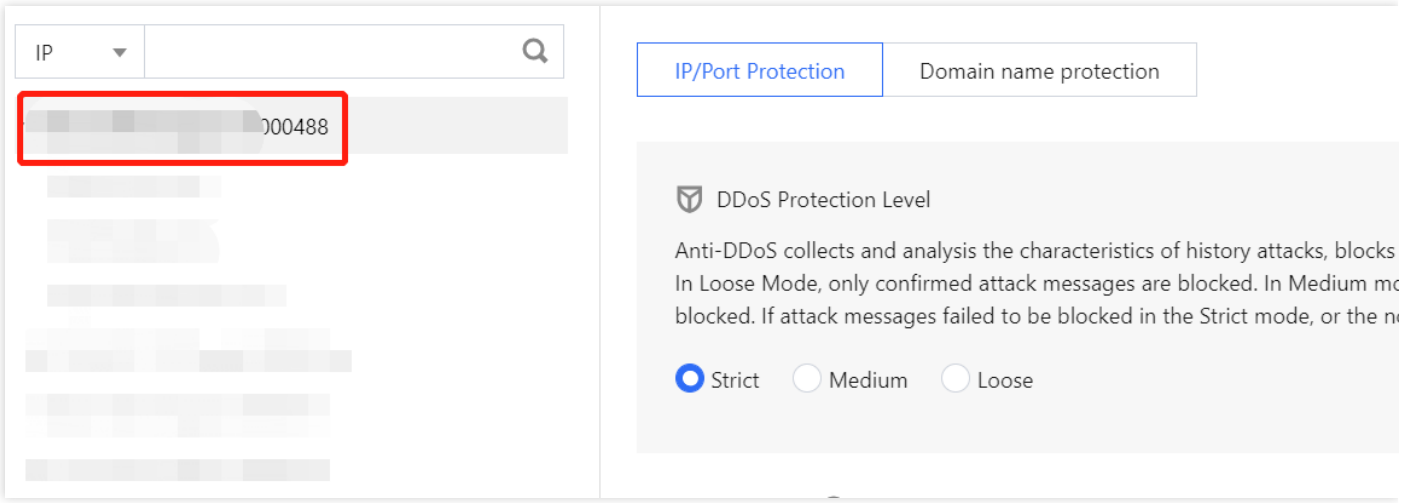
DDoS 高防 IP （境外企业版）支持针对 IP、TCP 及 UDP 报文头或载荷中的特征自定义拦截策略。开启特征过滤后，您可以将源端口、目的端口、报文长度、IP 报文头或荷载的匹配条件进行组合，并对命中条件的请求设置放行、拦截、丢弃、拦截并拉黑15分钟、丢弃并拉黑15分钟、继续防护等策略动作，特征过滤可以精准制定针对业务报文特征或攻击报文特征的防护策略。

前提条件

您需要成功 购买 DDoS 高防 IP （境外企业版），并设置防护对象。

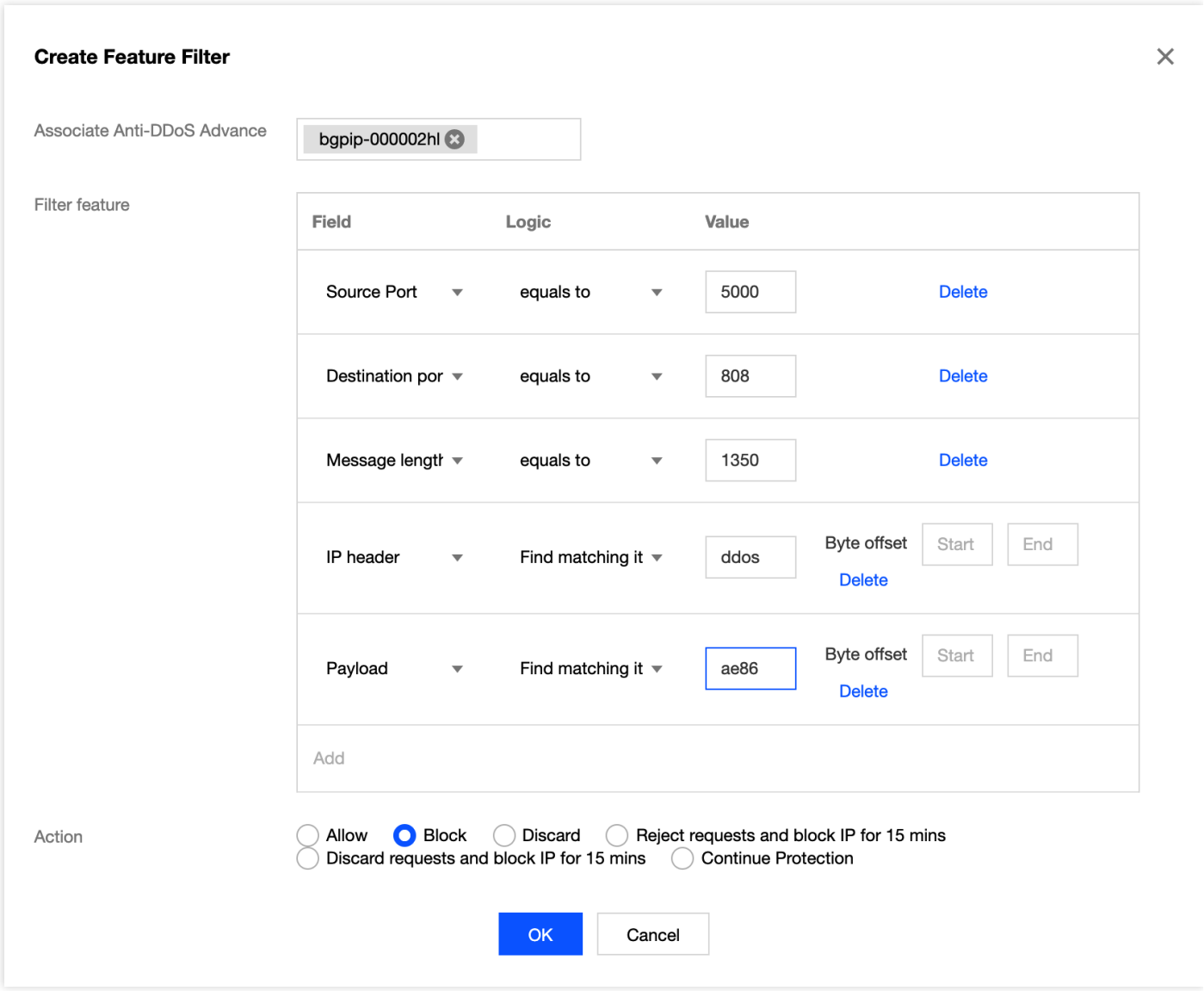
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDOS 高防 IP>防护配置 > DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。

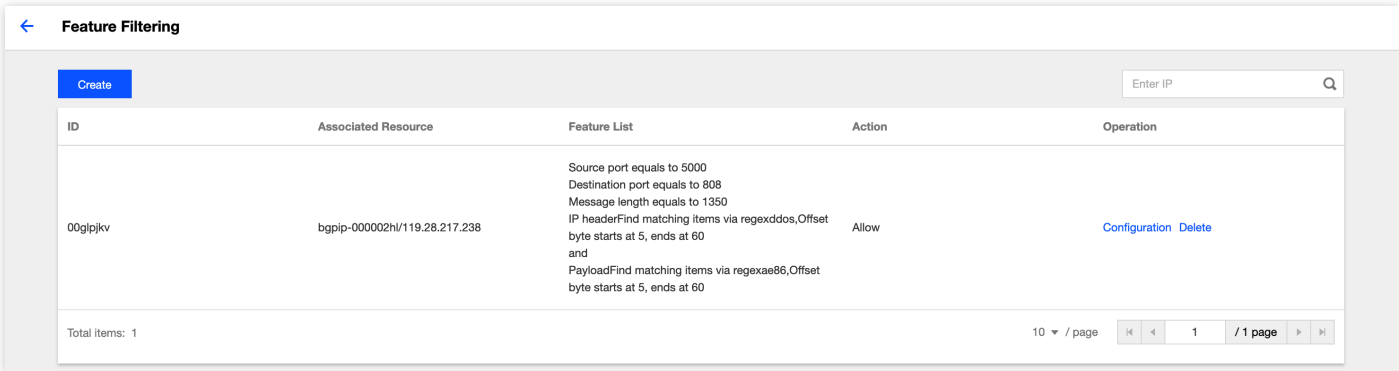


3. 在特征过滤卡片中，单击**设置**。

4. 在特征过滤页面中，单击**新建**，创建特征过滤规则，根据需求，选择不同防护动作并填写相关字段，单击**确定**。



5. 新建完成后，特征过滤列表将新增一条特征过滤规则，可以在右侧操作列，单击**配置**，可以修改特征过滤规则。



AI 防护

最近更新时间：2022-04-28 11:14:17

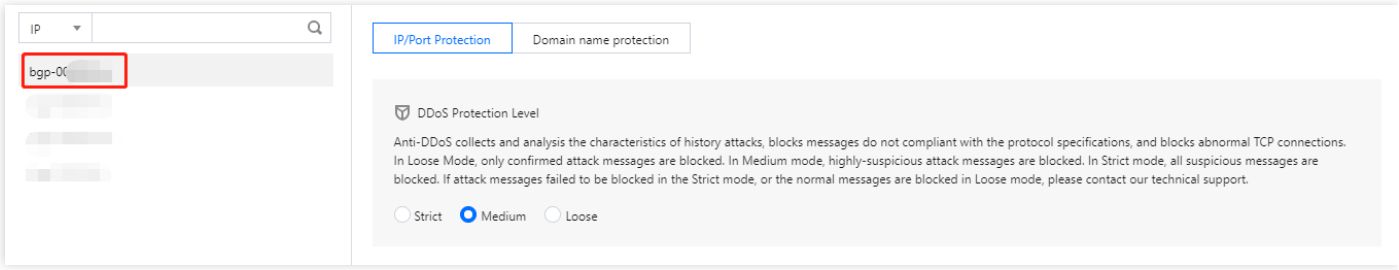
DDoS 高防 IP （境外企业版）支持智能 AI 防护功能，开启 AI 防护后，DDoS 高防将通过算法自主学习连接数基线与流量特征，自适应调整清洗策略，发现并阻断四层连接型 CC 攻击，提供最佳防御效果。

前提条件

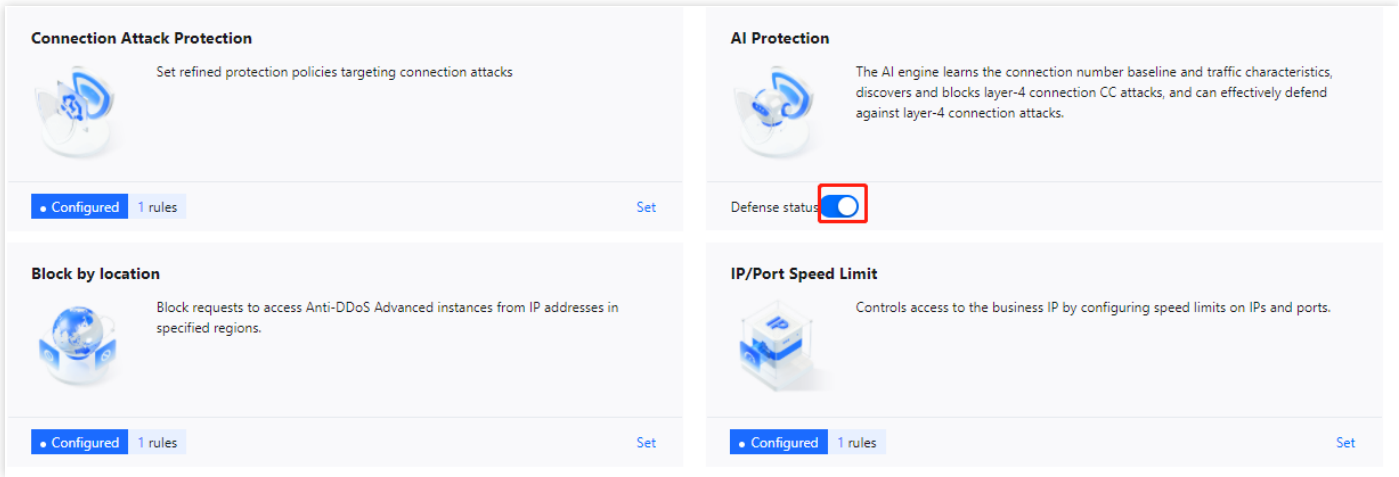
您需要成功 购买 DDoS 高防 IP （境外企业版），并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDOS 高防 IP>防护配置 > DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。



3. 在 AI 防护卡片中，单击  ，打开 AI 防护开关。



连接类攻击防护

最近更新时间：2022-04-28 11:17:18

当连接类发起异常，DDoS 高防 IP （境外企业版）支持自动发起禁封惩罚策略。在源IP最大异常连接数开启防护后，当 DDoS 高防 IP （境外企业版）检测到同一个源 IP 短时间内频繁发起大量异常连接状态的报文时，会将该源 IP 纳入黑名单中进行封禁惩罚，封禁时间为15分钟，等封禁解除后可恢复访问。支持以下字段：

说明：

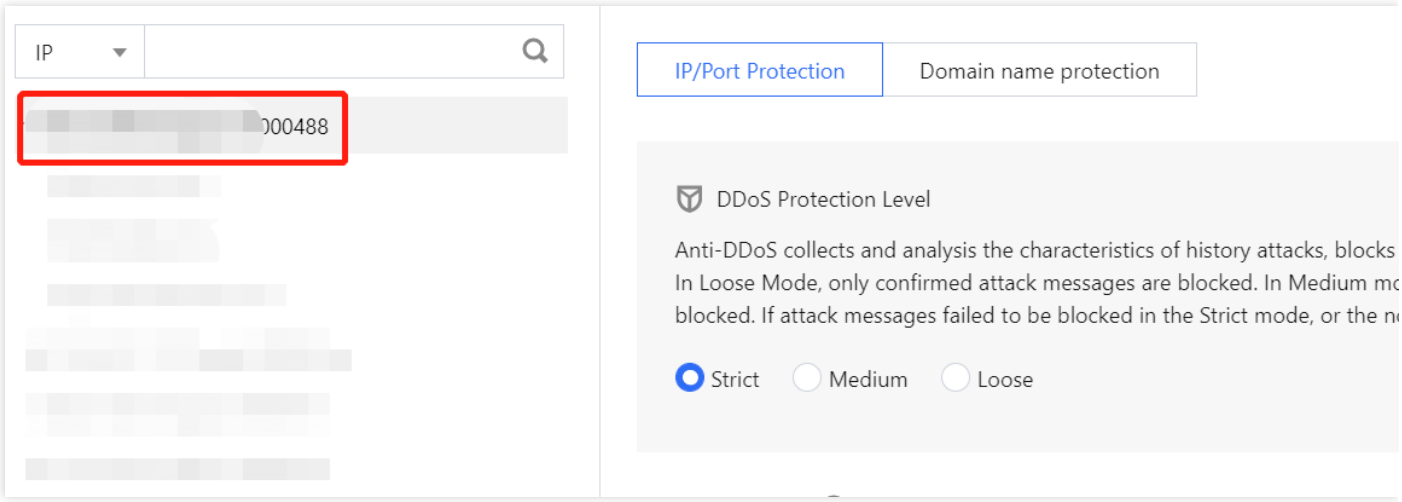
- 源新建连接限速：基于源地址端口新建连接频率限制。
- 源并发连接限制：访问源某一刻 TCP 的活跃连接数达到限制。
- 目的新建连接限速：目的 IP 地址端口新建连接频率限制。
- 目的并发连接限制：目的 IP 地址某一刻 TCP 的活跃连接数达到限制。
- 源 IP 最大异常连接数：访问源 IP 支持最大的异常连接数。

前提条件

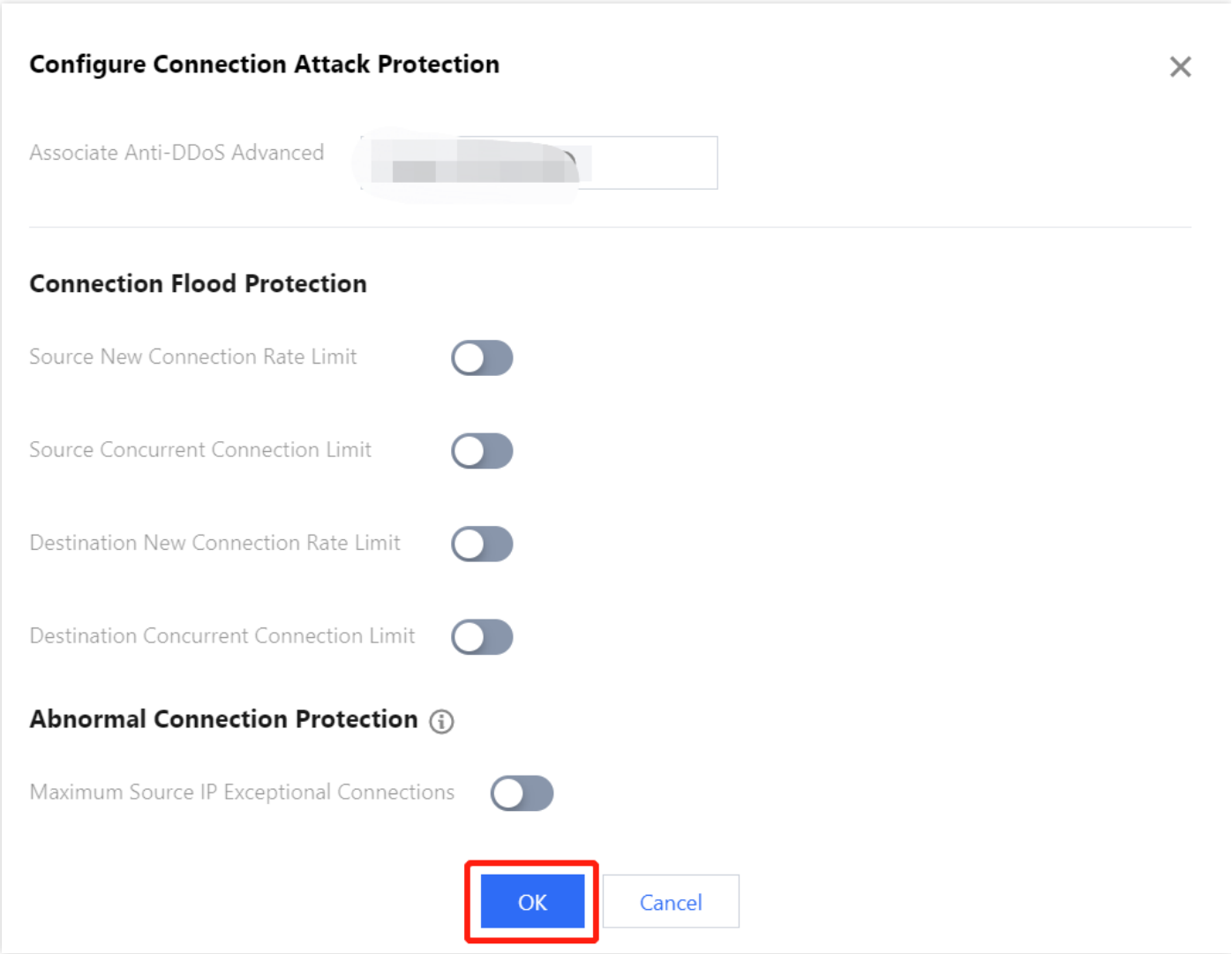
您需要成功 购买 DDoS 高防 IP （境外企业版） ，并设置防护对象。

操作步骤

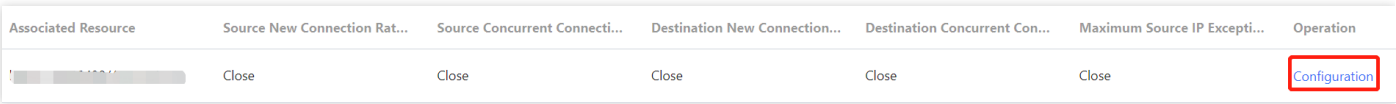
1. 登录 DDoS 高防 IP（境外企业版） 控制台 ，在左侧导航中，单击 **DDOS 高防 IP>防护配置 > DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。



3. 在连接类攻击防护卡片中，单击**设置**。
4. 在连接类攻击防护页面中，单击**新建**，配置连接类攻击防护，开启异常连接防护，单击**确定**。



5. 新建完成后，连接类攻击防护列表将增加一条连接类攻击防护规则，可以在右侧操作列，单击**配置**，修改异常连接规则。



IP 黑白名单

最近更新时间：2022-04-28 11:20:20

DDoS 高防 IP （境外企业版）支持通过配置 IP 黑名单和白名单实现对访问 DDoS 高防 IP （境外企业版）的源 IP 封禁或者放行，从而限制访问您业务资源的用户。配置 IP 黑白名单后，当流量超过清洗阈值时，若白名单中的 IP 进行访问，将被直接放行，不经过任何防护策略过滤。若黑名单中的 IP 进行访问，将会被直接阻断。

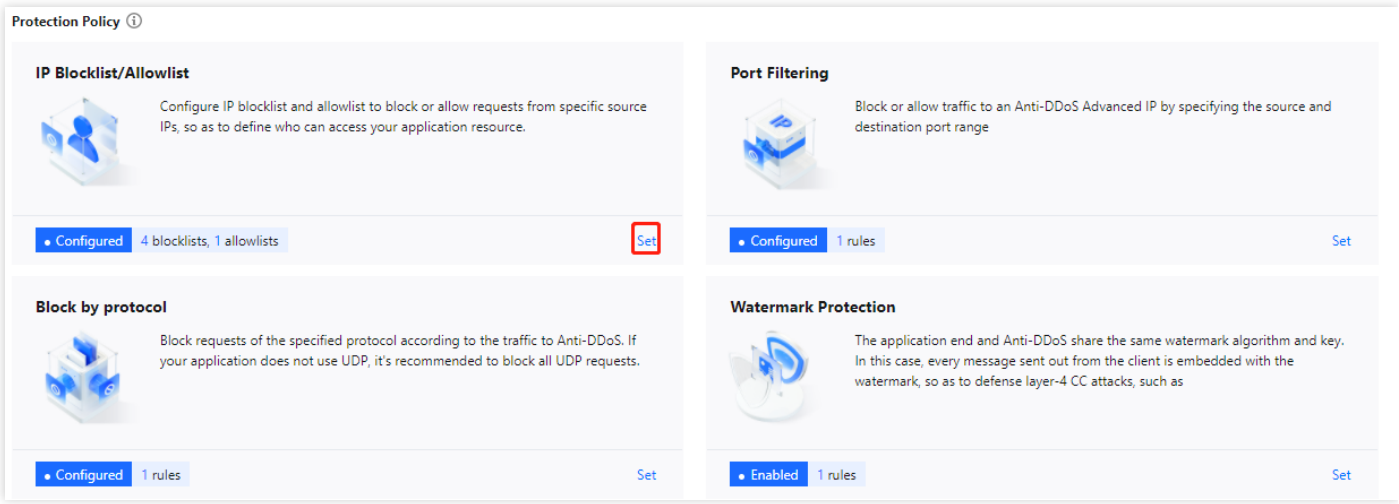
前提条件

- 您需要成功 购买 DDoS 高防 IP （境外企业版），并设置防护对象。

> 说明：
> 当发生 DDoS 攻击时，IP 黑白名单的过滤才会生效。
> - 白名单中的 IP，访问时将被直接放行，不经过任何防护策略过滤。
> - 黑名单中的 IP，访问时将会被直接阻断。

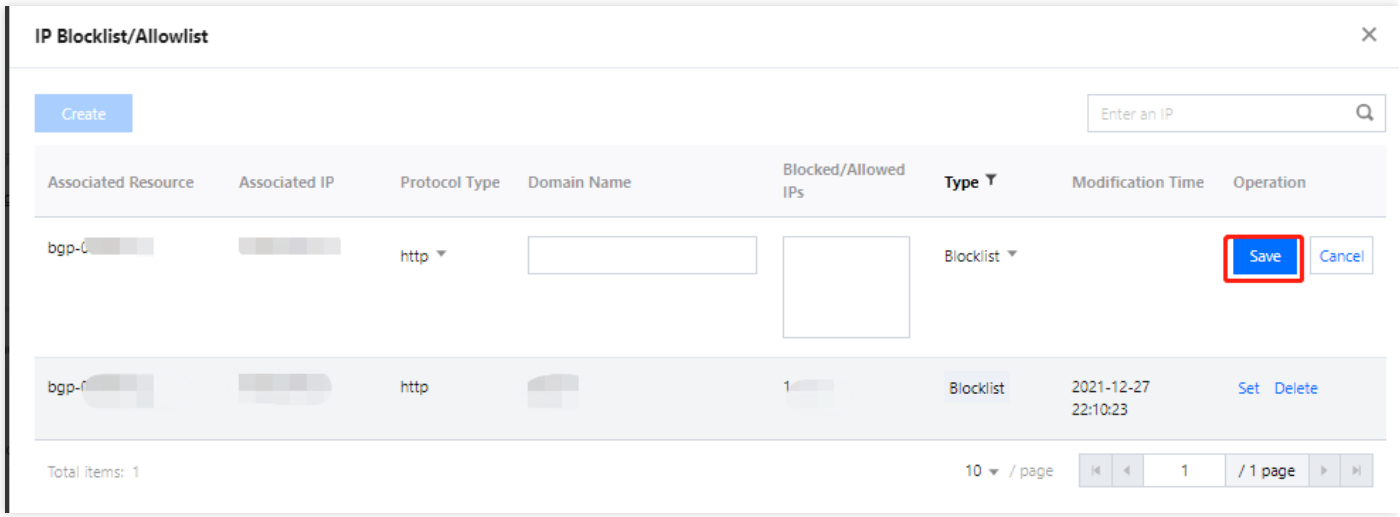
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDOS 高防 IP>防护配置 > DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。

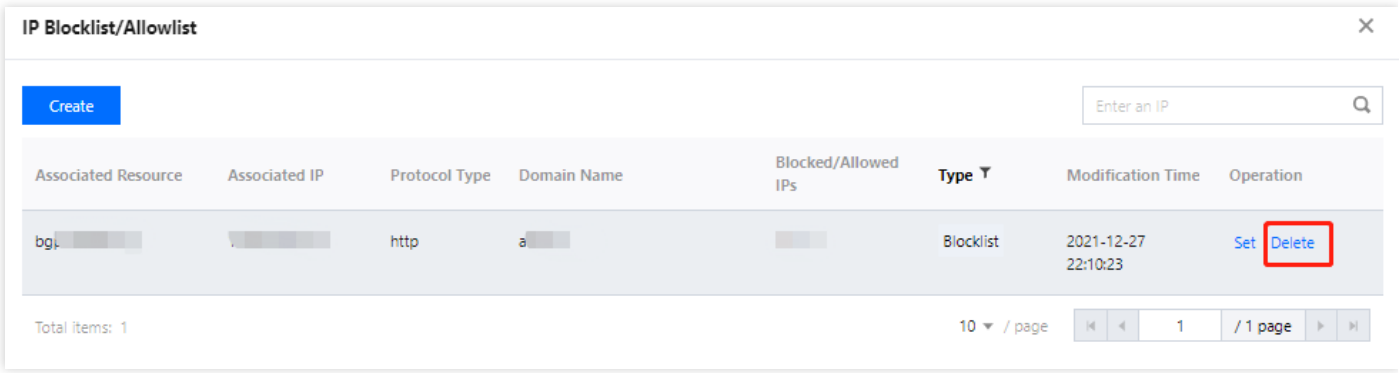


3. 在 IP 黑白名单卡片中，单击**设置**。

4. 在 IP 黑白名单列表中，单击**新建**，选择类型并输入 IP，单击**保存**。



5. 新建完成后，IP 黑白名单列表将新增一条 IP 黑白名单规则，可以在右侧操作列，单击**删除**，删除 IP 黑白名单规则。



IP 端口限速

最近更新时间：2022-04-28 11:20:00

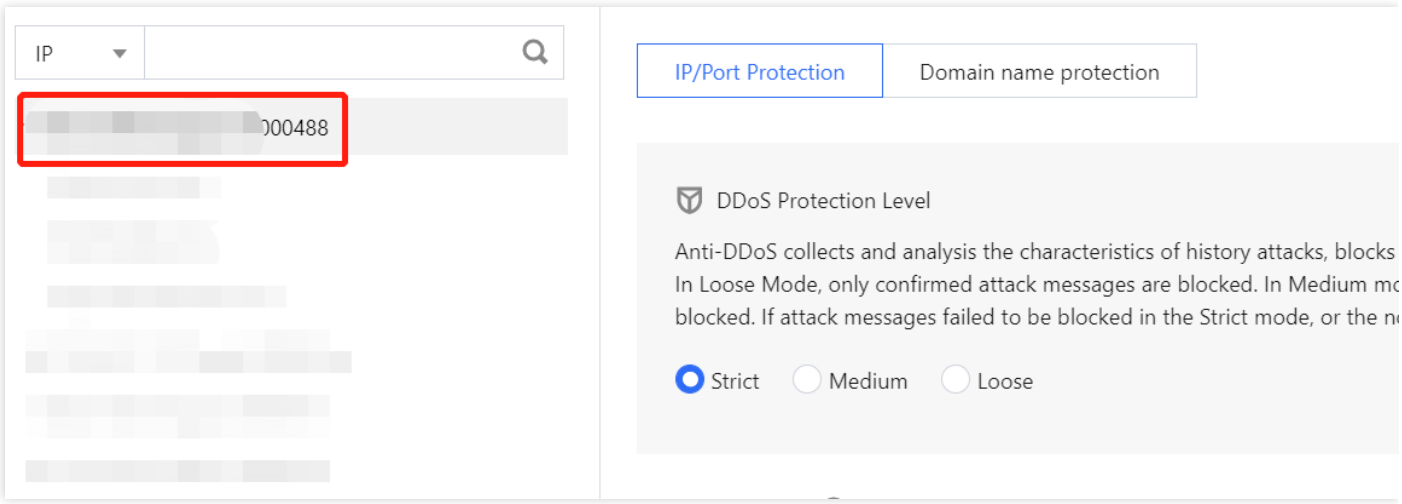
DDoS 高防 IP （境外企业版）支持对于业务 IP，基于 IP+端口的维度进行流量访问限速。

前提条件

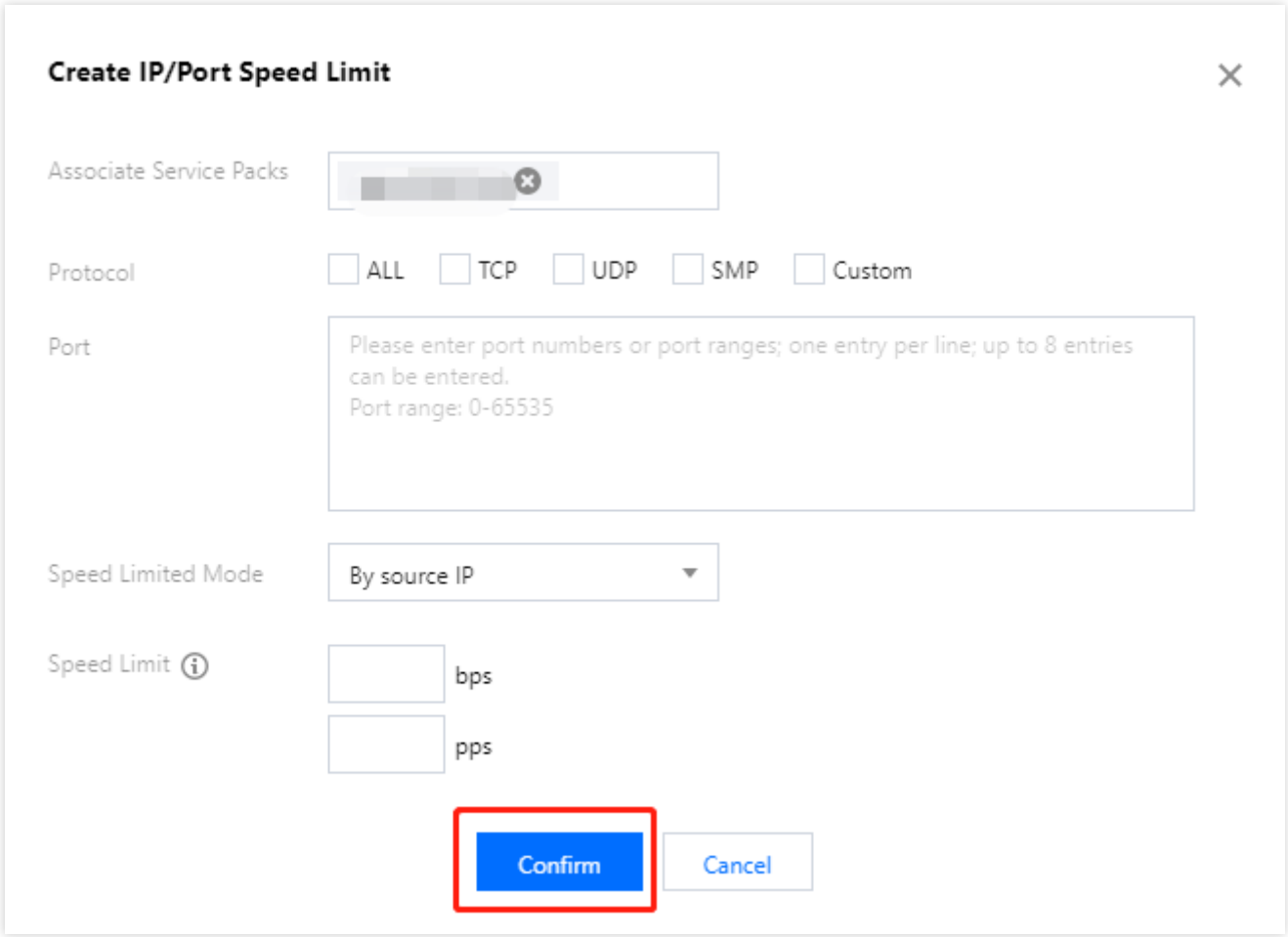
您需要成功 购买 DDoS 高防 IP （境外企业版） ，并设置防护对象。

操作步骤

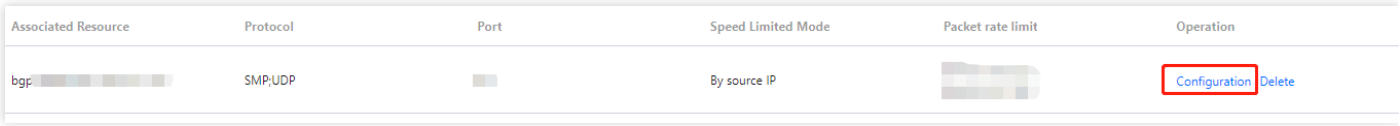
1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDOS 高防 IP>防护配置 > DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。



3. 在 IP 端口限速卡片中，单击**设置**。
4. 在 IP 端口限速列表中，单击**新建**，选择相关协议、具体的端口及限速模式，并输入限速阈值。单击**确定**，创建 IP 端口限速规则。



5. 新建完成后，IP 端口限速列表将新增一条 IP 端口限速规则，可以在右侧操作列，单击**配置**，修改 IP 端口限速规则。



区域封禁

最近更新时间：2022-04-28 11:22:22

DDoS 高防 IP（境外企业版）支持对访问 DDoS 高防 IP（境外企业版）的源流量，按照源IP地理区域在清洗节点进行一键封禁。支持多地区、国家进行流量封禁。

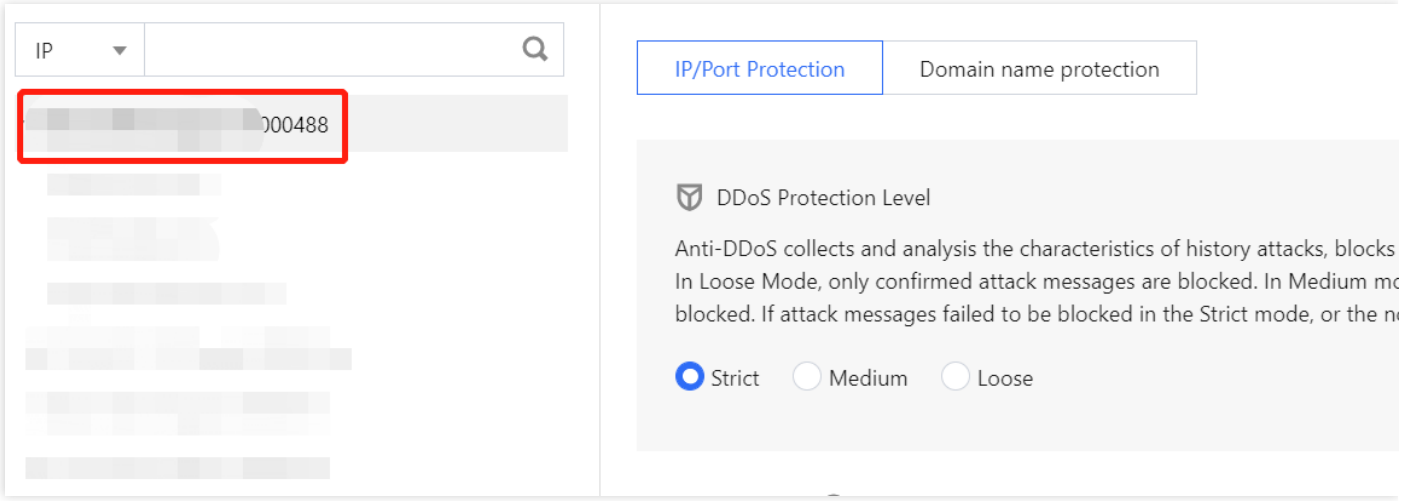
> 说明：
> 在配置了区域封禁后，该区域的攻击流量依然会被平台统计和记录，但不会流入业务源站。

前提条件

您需要成功 购买 DDoS 高防 IP （境外企业版） ，并设置防护对象。

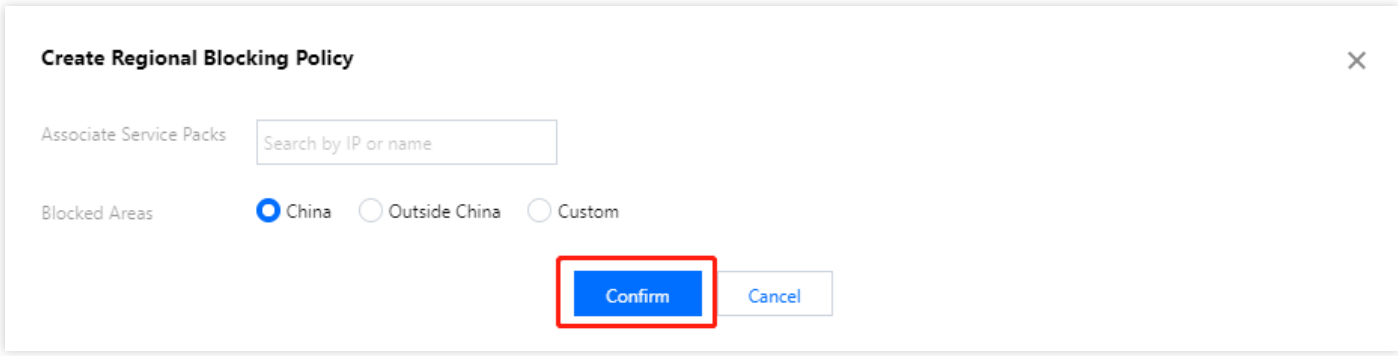
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台 ，在左侧导航中，单击 **DDOS 高防 IP>防护配置 > DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。

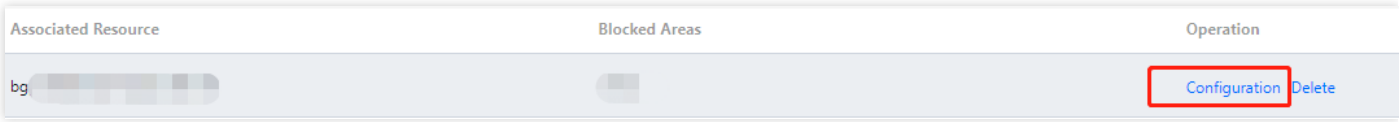


3. 在区域封禁卡片中，单击**设置**。

4. 在区域封禁列表中，单击**新建**，选择封禁区域，单击**确定**，创建区域封禁规则。



5. 新建完成后，区域封禁列表将新增一条区域封禁规则，可以在右侧操作列，单击**配置**，修改区域封禁规则。



端口过滤

最近更新时间：2022-12-02 11:05:26

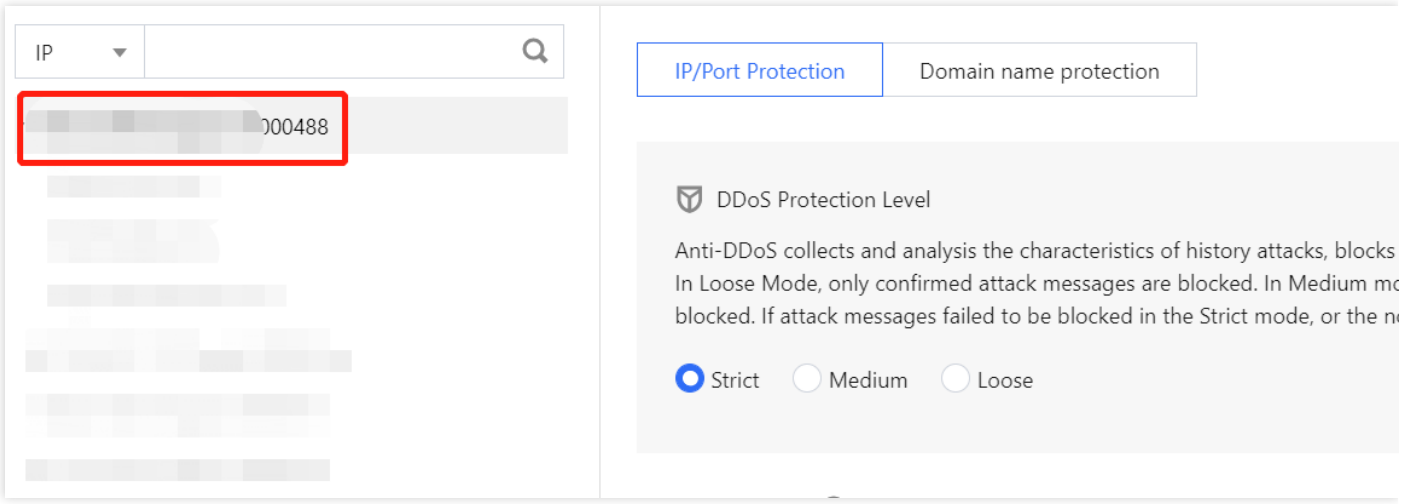
DDoS 高防 IP（境外企业版）支持针对访问 DDoS 高防 IP（境外企业版）的源流量，基于端口进行一键封禁或者放行。开启端口过滤后，可以根据需求自定义协议类型、源端口范围、目的端口范围的组合，并对匹配中的规则进行设置丢弃、放行、继续的防护策略动作。端口过滤可以精准制定针对访问的源流量，进行端口设置的防护策略。

前提条件

您需要成功 购买 DDoS 高防 IP（境外企业版），并设置防护对象。

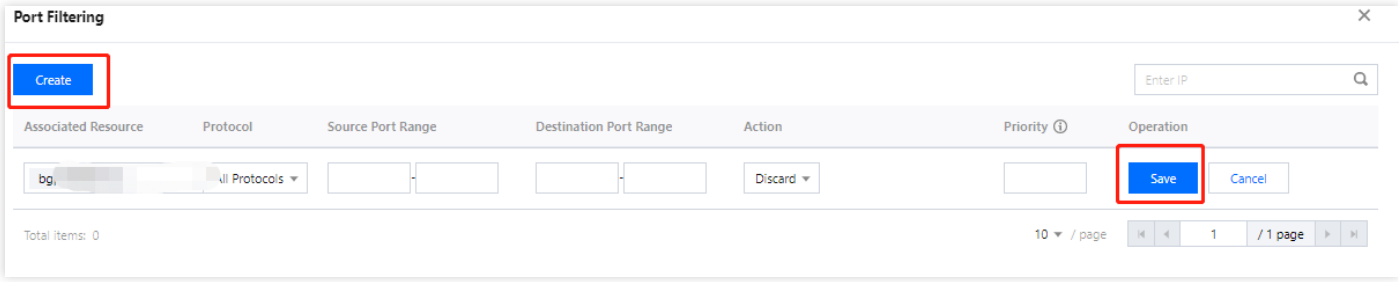
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDOS 高防 IP** > **防护配置** > **DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。

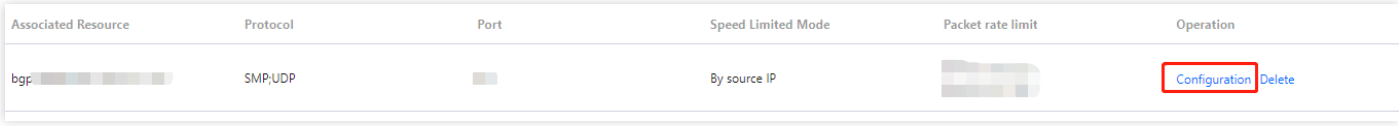


3. 在端口过滤卡片中，单击**设置**。

4. 在端口过滤列表中，单击**新建**，根据需求，选择不同防护动作并填写相关字段。



5. 单击**保存**，创建端口过滤规则。
6. 新建完成后，端口过滤列表将新增一条端口过滤规则，可以在右侧操作列，单击**配置**，可以修改端口过滤规则。



水印防护

最近更新时间：2022-04-28 10:55:43

DDoS 高防 IP（境外企业版）支持对业务端发出的报文增加水印防护，在您配置的 UDP 和 TCP 报文端口范围内，业务端和 DDoS 防护端共享水印算法和密钥，配置完成后，客户端每个发出的报文都嵌入水印特征，而攻击报文无水印特征，借此甄别出攻击报文并将其丢弃。通过接入水印防护能高效全面防护4层 CC 攻击，如模拟业务报文攻击和重放攻击等。

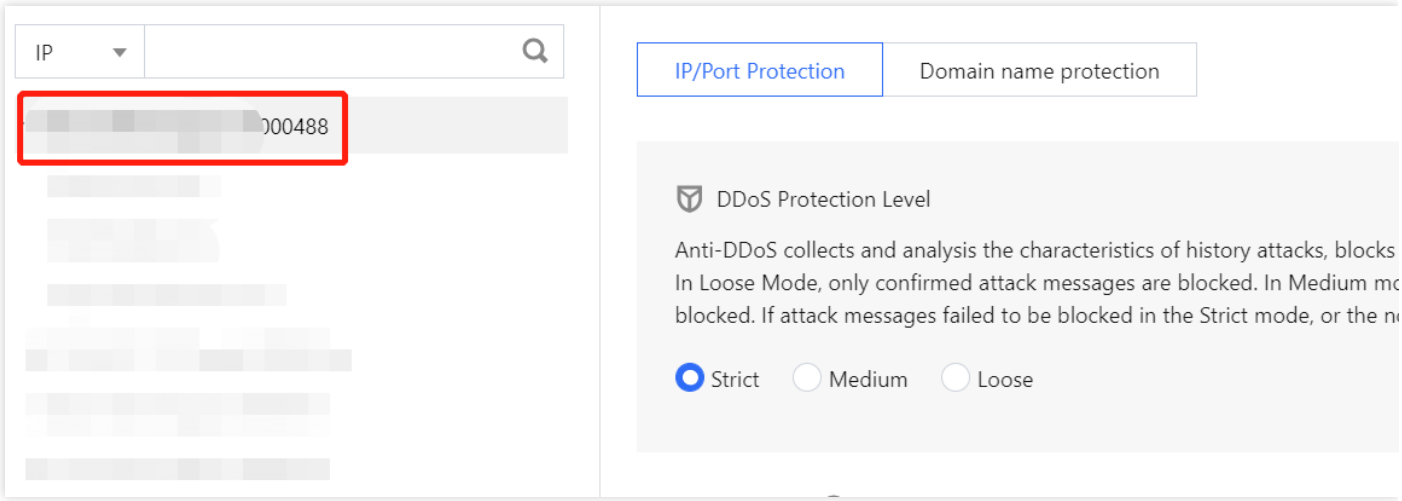
前提条件

您需要成功 购买 DDoS 高防 IP（境外企业版），并设置防护对象。

> 说明：
> 此功能为额外付费功能，请 联系我们 进行开通。

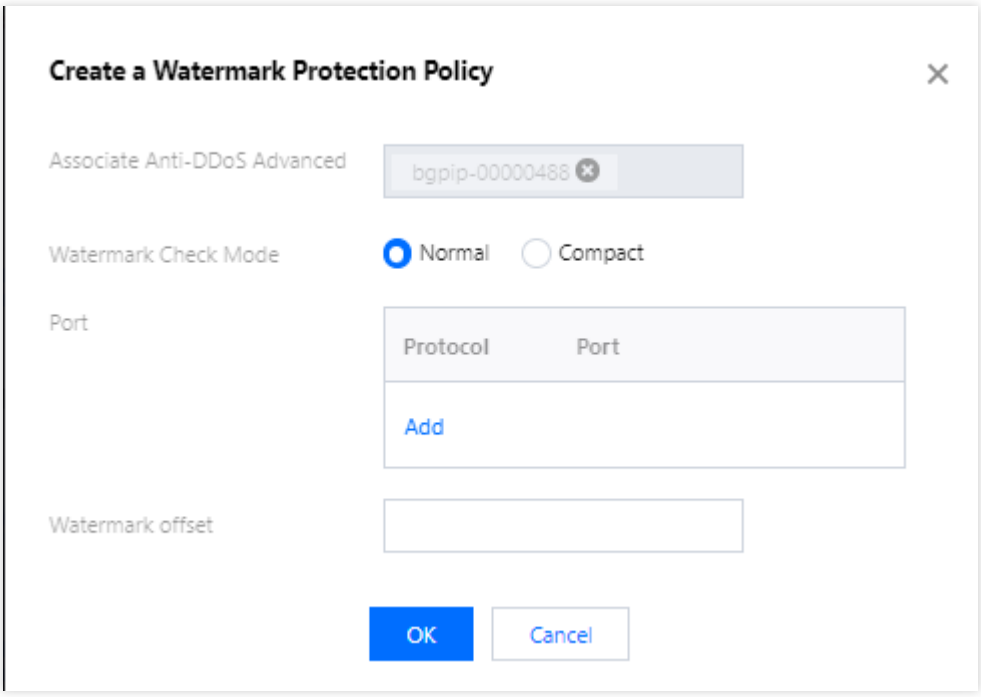
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDOS 高防 IP** > **防护配置** > **DDoS 防护**。
2. 在左边的列表选中高防 IP 的 ID，如“xxx.xx.xx.xx bgpip-000003n2”。

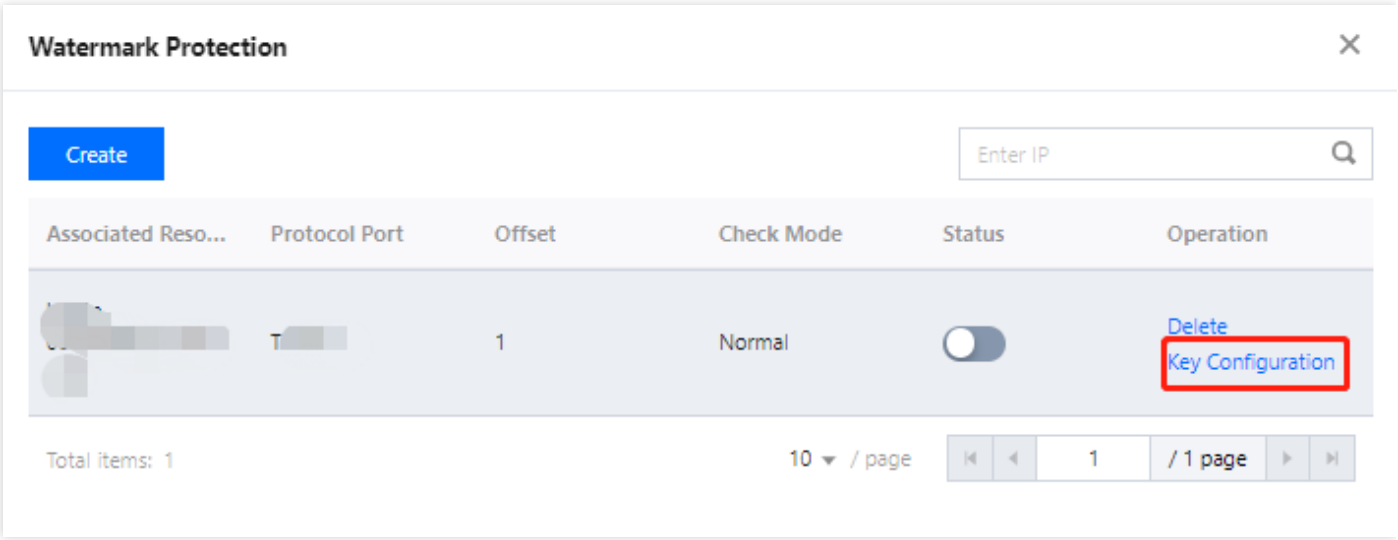


3. 在水印防护卡片中，单击**设置**。

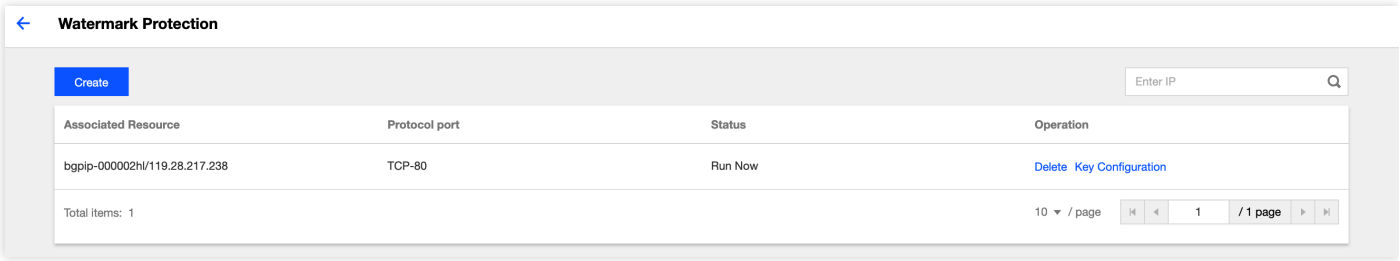
4. 在水印防护列表中，单击**新建**，填写相关字段，单击**确定**，创建水印防护规则。



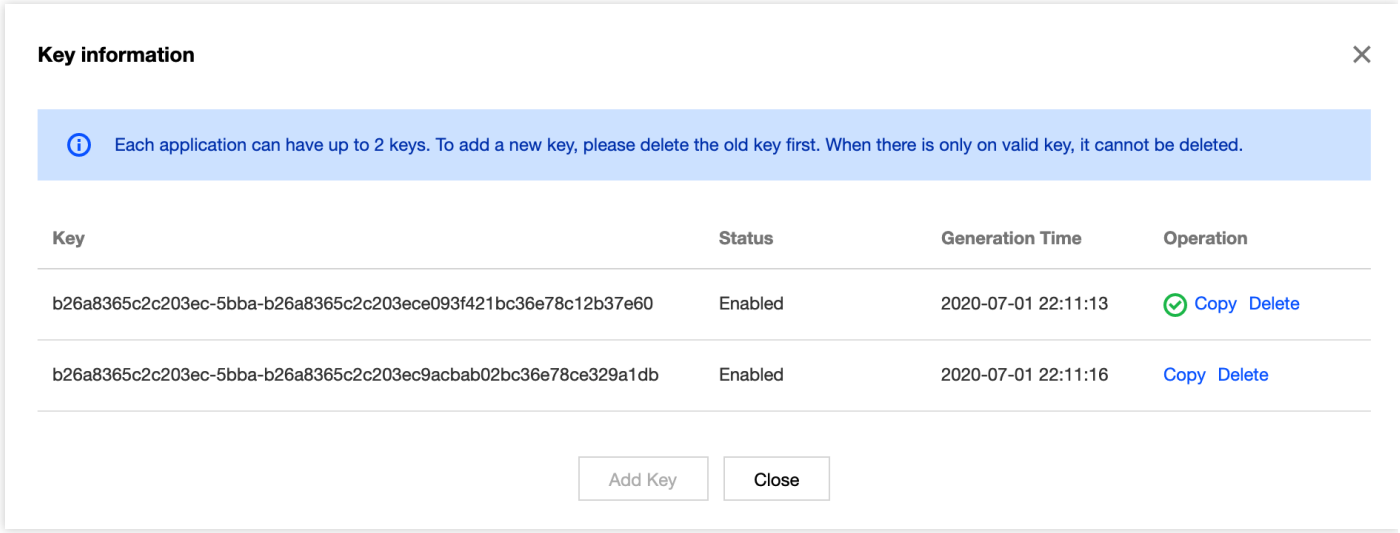
5. 新建完成后，水印防护列表将新增了一条水印防护规则，可以在右侧操作列，单击**密钥配置**，可以查看和配置密钥。



6. 在密钥信息窗口中，用户可以查看或复制密钥。



7. 在密钥信息窗口中，可以添加或删除密钥，只有在两个密钥时可以删除一个密钥，最多只能有两个水印密钥。



CC 防护
CC 防护开关及清洗阈值

最近更新时间：2022-04-28 10:55:43

防护说明

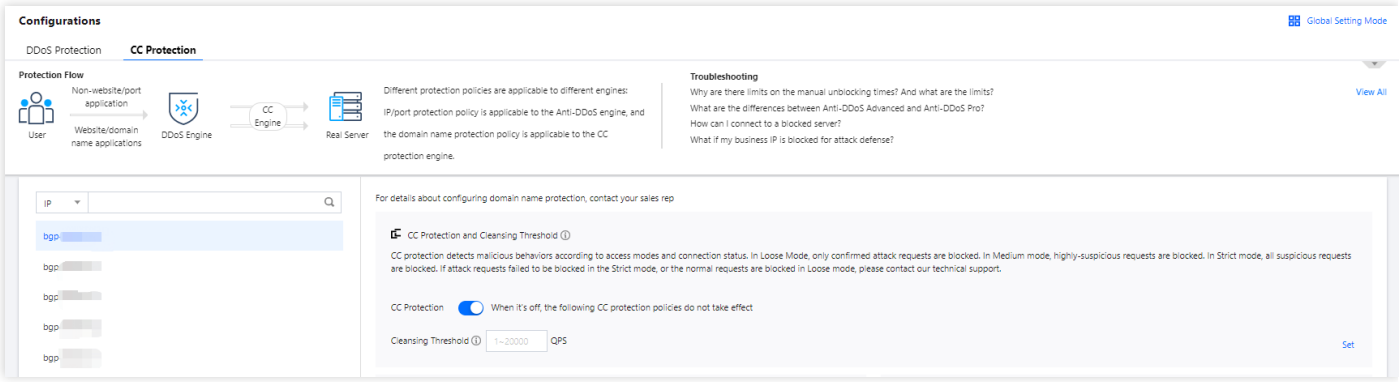
CC 防护根据访问特征和连接状态判定恶意行为， 阻断黑客的攻击。可根据不同的攻击场景配置相应的防护策略，保证业务稳定。清洗阈值是高防产品启动清洗动作的阈值。

前提条件

您需要成功 购买 DDoS 高防 IP（境外企业版） ，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台 ，在左侧导航中，单击 **DDoS 高防 IP** > **防护配置** > **CC 防护**。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID，如“bgp-00xxxxxx”。



3. 在 CC 防护开关和清洗阈值卡片中，单击**设置**。
4. 在 CC 防护开关及清洗阈值列表，单击**新建**，输入所需参数和清洗阈值。
5. 单击**保存**，添加规则。

> 注意：
> 精细化的规则优先级高于高防 IP 实例全局维度下的规则。

6. 新建完成后，在 CC 防护开关及清洗阈值列表中，将新增一条 CC 防护域名规则。在自定义模式下，单击 和  ，支持修改 CC 防护域名开关和清洗阈值。

区域封禁

最近更新时间：2022-04-28 10:55:43

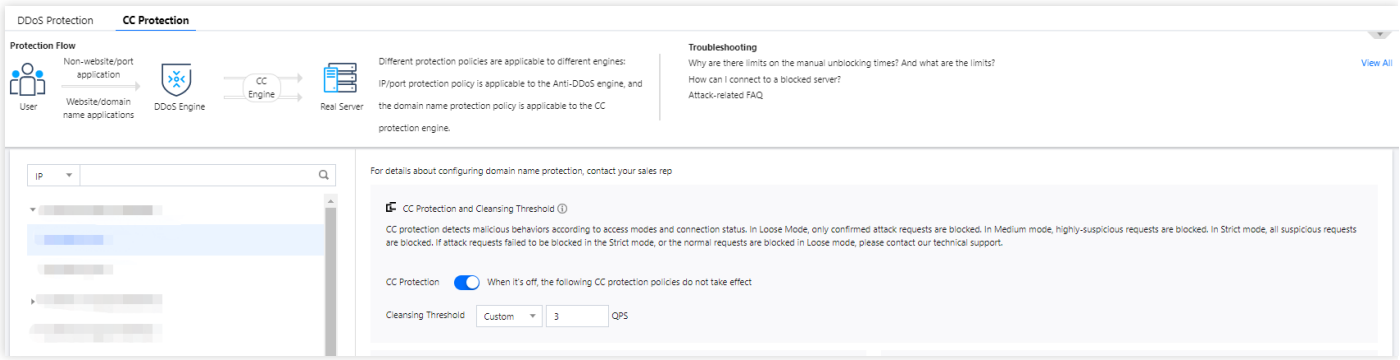
DDoS 高防 IP（境外企业版）支持对已接入防护的网站业务，设置基于地理区域的访问请求封禁策略。开启针对域名的区域封禁功能后，您可以一键阻断指定地区来源 IP 对网站业务的所有访问请求。支持多地区、国家进行流量封禁。

前提条件

您需要成功 购买 DDoS 高防 IP（境外企业版） ，并设置防护对象。

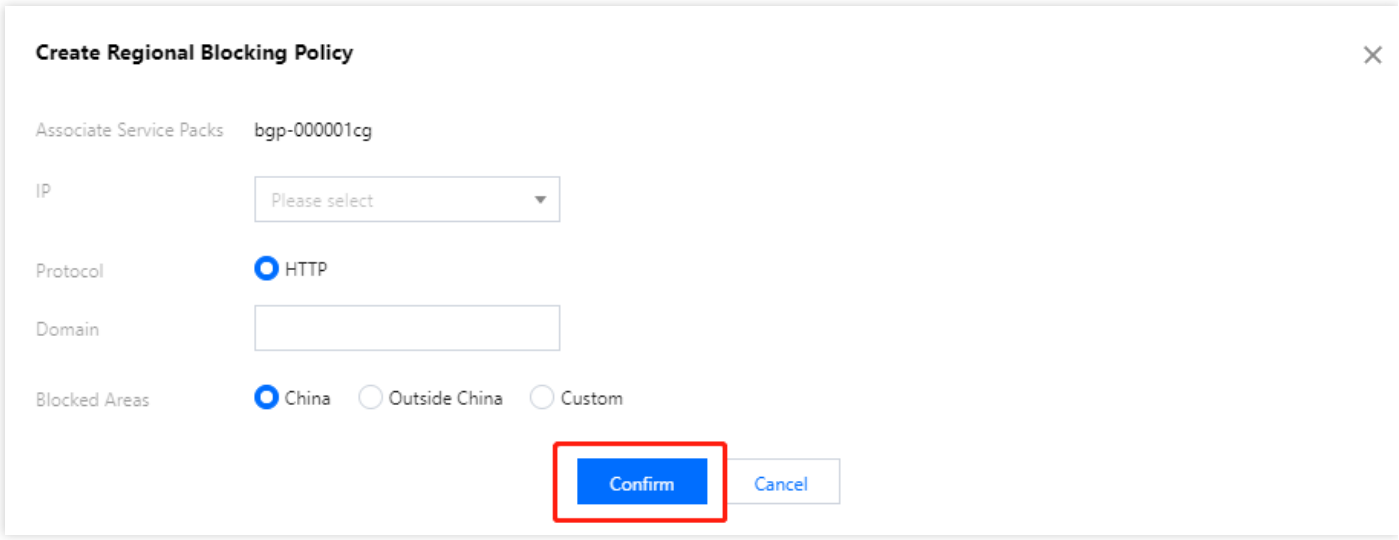
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台 ，在左侧导航中，单击 **DDoS 高防 IP** > **防护配置** > **CC 防护**。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID，如“bgp-00xxxxxx”。



3. 在区域封禁卡片中，单击**设置**。

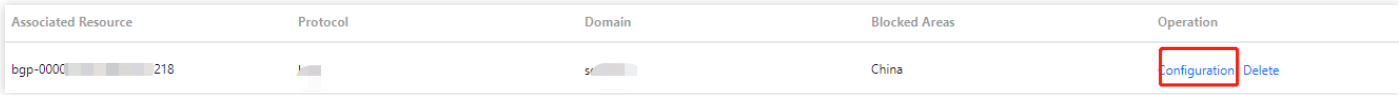
4. 在区域封禁列表，单击**新建**，选择 IP、域名、所封禁的区域，单击**确定**，创建区域封禁规则。



5. 单击**保存**，添加规则。

> 注意：
> 精细化的规则优先级高于高防 IP 实例全局维度下的规则。

6. 新建完成后，在区域封禁列表将新增一条区域封禁规则，可以在右侧操作列，单击**配置**，修改区域封禁规则。



IP 黑白名单

最近更新时间：2022-04-28 10:55:44

DDoS 高防 IP（境外企业版）支持通过配置 IP 黑名单和白名单，实现对访问 DDoS 高防已接入防护的网站业务封禁或者放行，从而限制访问您业务资源的用户。配置 IP 黑白名单后，当白名单中的 IP 访问时，将被直接放行，不经过任何防护策略过滤。当黑名单中的 IP 访问时，将会被直接阻断。

说明：
当发生 CC 攻击时，IP 黑白名单的过滤才会生效。

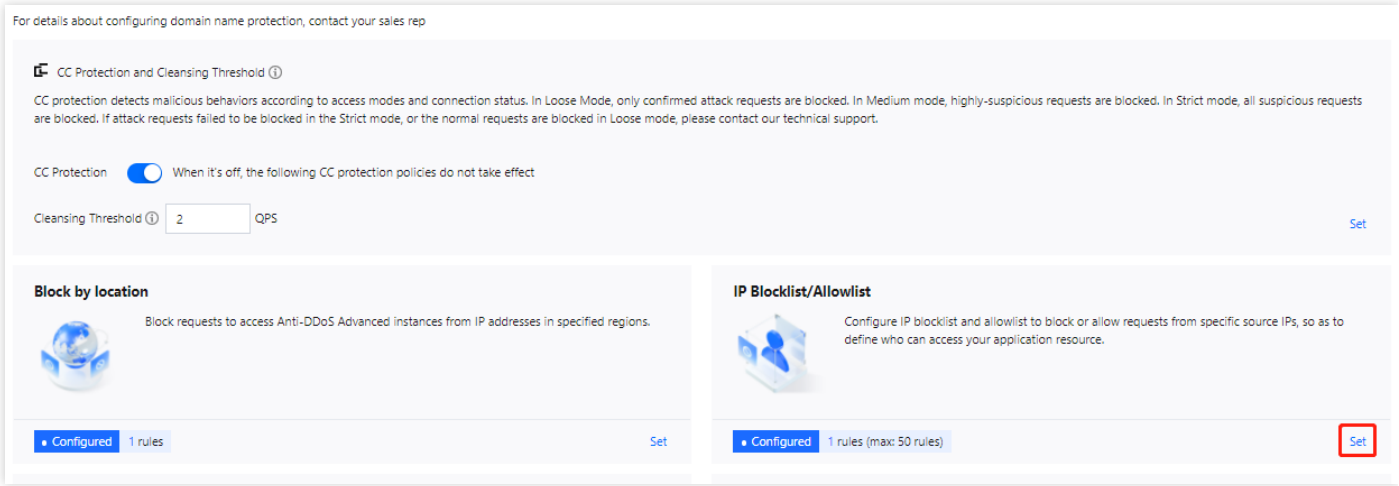
- 白名单中的 IP，访问时将被直接放行，不经过任何防护策略过滤。
- 黑名单中的 IP，访问时将会被直接阻断。

前提条件

您需要成功 购买 DDoS 高防 IP（境外企业版），并设置防护对象。

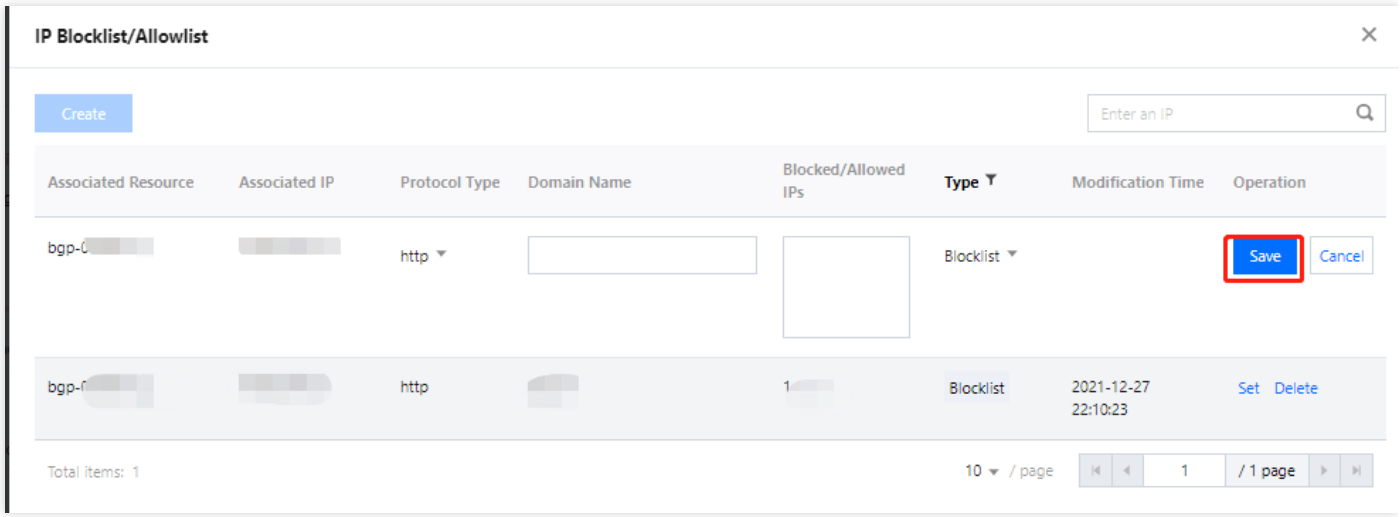
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDoS 高防 IP** > **防护配置** > **CC 防护**。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID，如“bgp-00xxxxxx”。



3. 在 IP 黑白名单卡片中，单击**设置**。

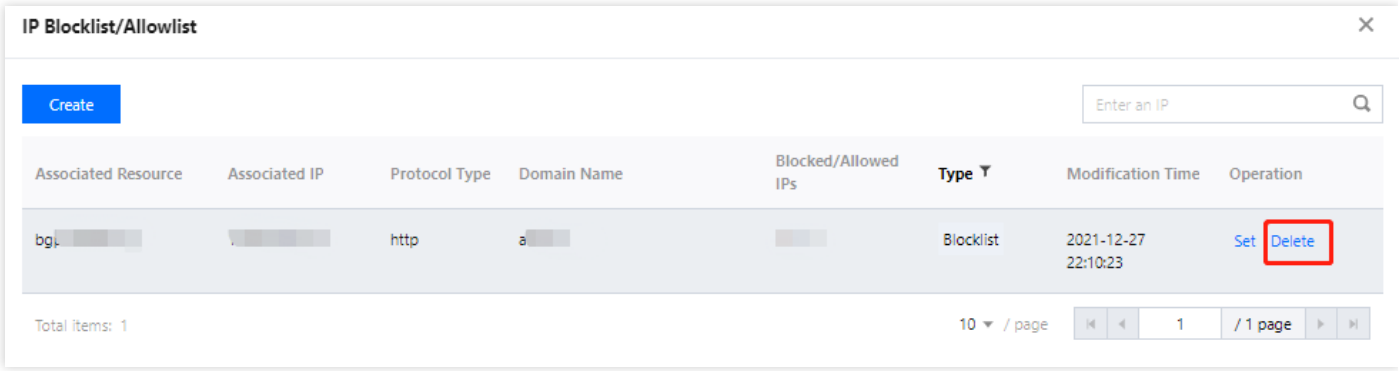
4. 在 IP 黑白名单列表，单击**新建**，填写相关字段。



参数说明：

- 协议类型：根据实际需求选择 http 或 https。
- 域名：该资源 IP 下的业务域名。
- IP 名单：支持IP 或 IP 段，以 IP 或 IP/掩码的格式填写。
- 类型：根据实际需求选择黑名单或白名单。

5. 单击**保存**，添加规则。
6. （可选）新建完成后，IP 黑白名单列表将新增一条 IP 黑白名单规则，可以在右侧操作栏中，单击**删除**，删除 IP 黑白名单规则。



精准防护

最近更新时间：2022-04-28 10:55:44

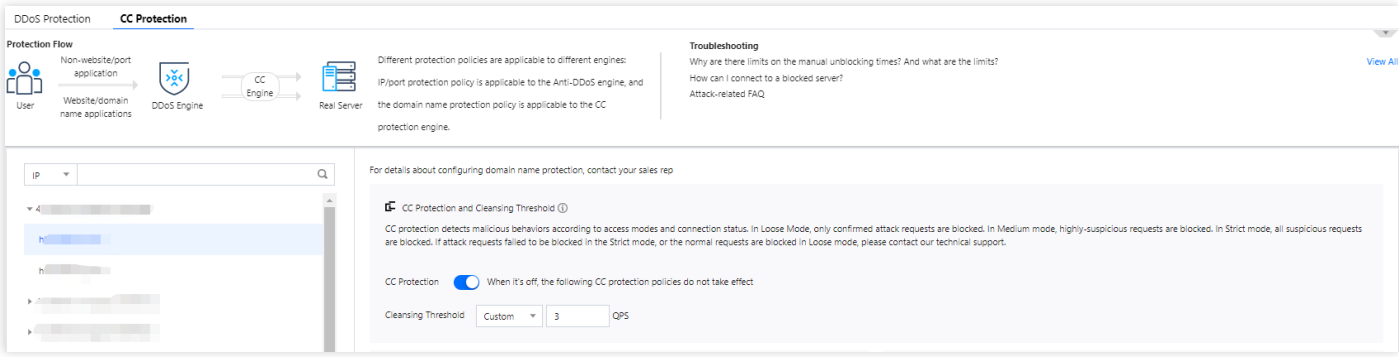
DDoS 高防 IP（境外企业版）支持对已接入防护的网站业务配置精准防护策略。开启精确访问控制后，您可以对常见的 HTTP 字段（例如 URI、UA、Cookie、Referer 及 Accept 等）做条件组合防护策略，筛选访问请求，并对命中条件的请求设置人机校验、丢弃或放行的策略动作。精准防护支持业务场景定制化的防护策略，可用于精准定制针对性的 CC 防御。

前提条件

您需要成功 购买 DDoS 高防 IP（境外企业版），并设置防护对象。

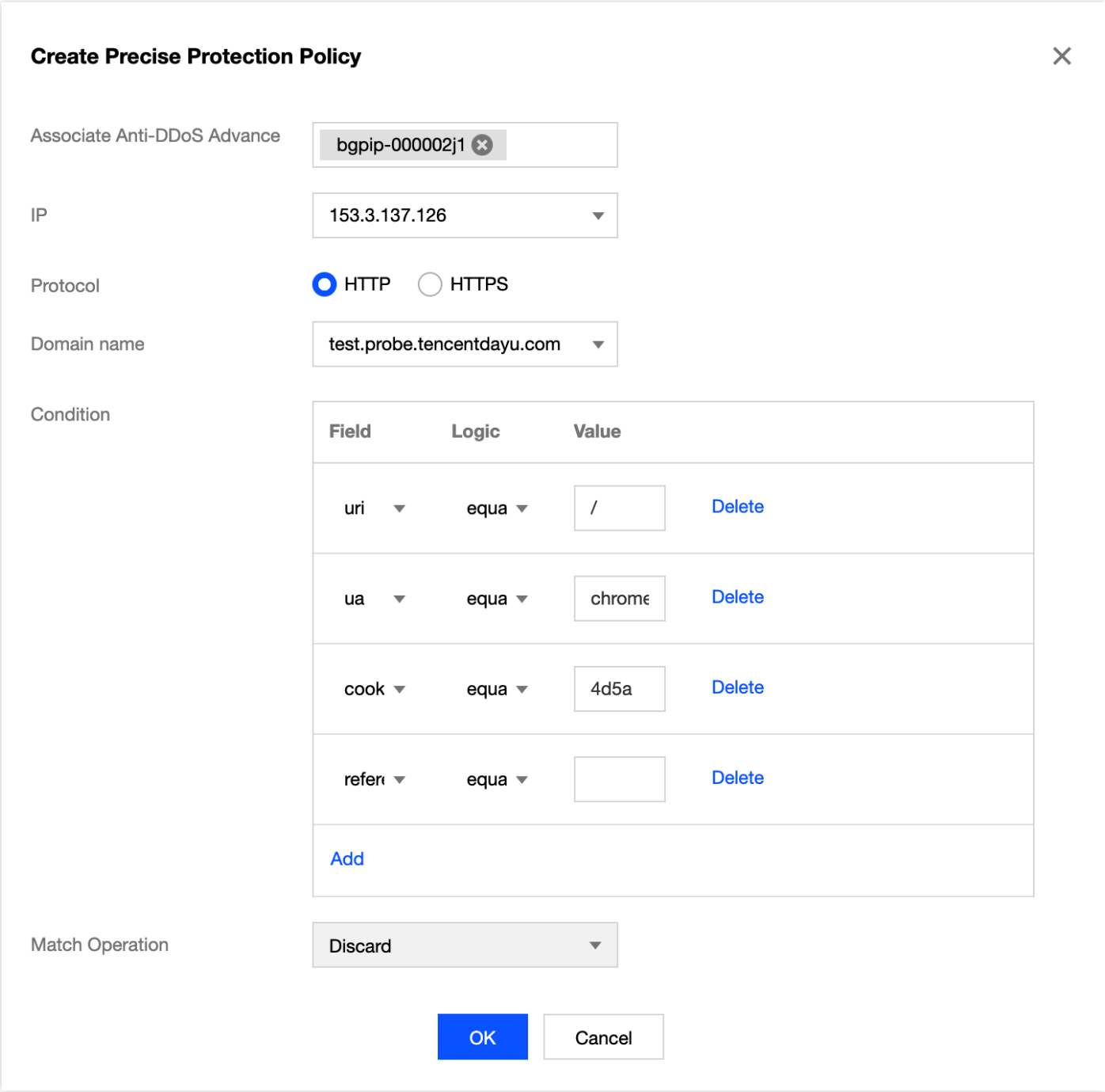
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDoS 高防 IP** > **防护配置** > **CC 防护**。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID，如“bgp-00xxxxxx”。



3. 在精准防护卡片中，单击**设置**。

4. 在精准防护列表，单击**新建**，创建精准防护规则，填写相关字段，填写完成后，单击**确定**。



参数说明：

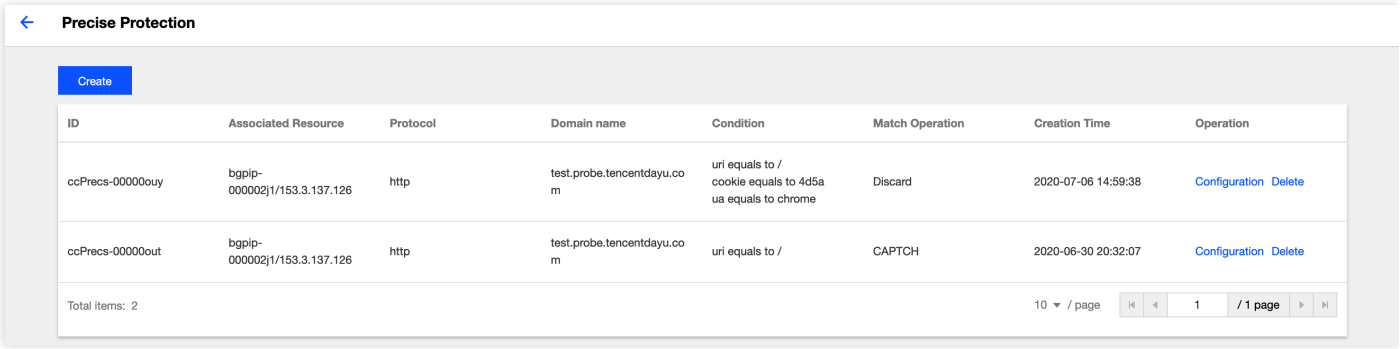
- 域名：该资源 IP 下的业务域名。
- 匹配条件：定义了要识别的请求特征，具体指访问请求中 HTTP 字段的属性特征，精确防护规则支持匹配的 HTTP 字段如下表所示。

匹配字段	字段描述	适用逻辑

匹配字段	字段描述	适用逻辑
URI	访问请求的 URI 地址	等于、包含、不包含
UA	发起访问请求的客户端浏览器标识等相关信息	等于、包含、不包含
Cookie	访问请求中的携带的 Cookie 信息	等于、包含、不包含
Referer	访问请求的来源网址，即该访问请求是从哪个页面跳转产生的	等于、包含、不包含
Accept	发起访问请求的客户端希望接受的数据类型	等于、包含、不包含

- 匹配动作
  - 人机校验：对命中匹配条件的请求发起人机识别校验。
  - 封禁：阻断命中匹配条件的访问请求。
  - 放行：放行命中匹配条件的访问请求。

5. 新建完成后，精准防护列表将会新增一条精准防护规则，可以在右侧操作栏单击**配置**，修改精准防护规则。



CC 频率限制

最近更新时间：2022-04-28 10:57:16

DDoS 高防 IP（境外企业版）为已接入防护的网站业务提供 CC 频率限制防护策略，支持限制源 IP 的访问频率。频率控制防护开启后自动生效，默认使用超级宽松防护模式，频率控制防护提供多种防护模式，供您在不同场景下调整使用。您也可以自定义频率限制规则，检测到单一源 IP 在短期内异常频繁地访问某个页面时，将设置人机校验或丢弃策略。

频率控制防护提供不同的防护模式，允许您根据网站的实时流量异常调整频率控制策略，具体包括如下模式：

- 宽松等级
- 适中等级
- 严格等级
- 攻击紧急
- 自定义

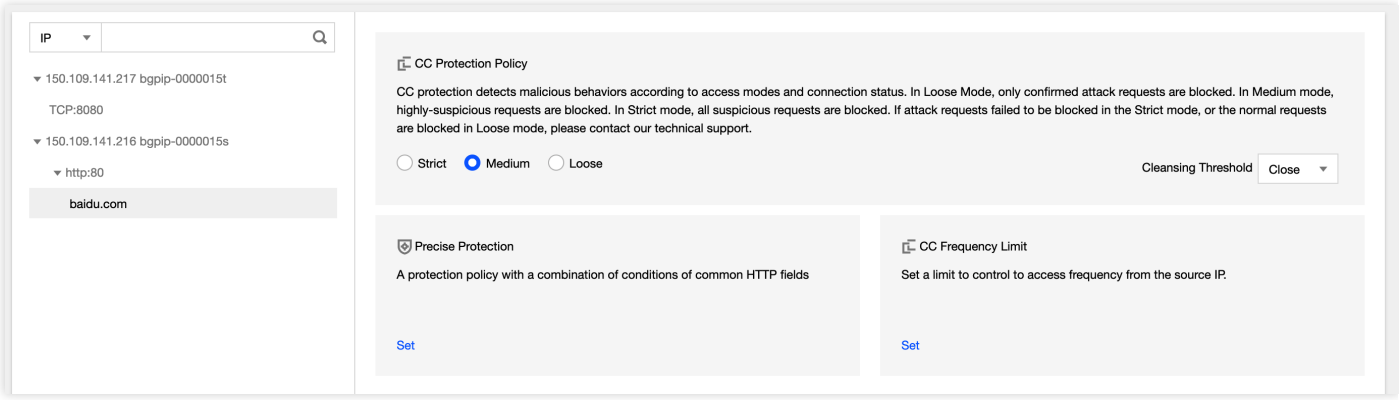
此等级下的 CC 防护策略较为宽松，可能会存在少部分异常请求透传的风险。注意：当发生攻击时，可切换防护等级进行防护。也可以配置自定义 CC 频率限制策略进行防护。

前提条件

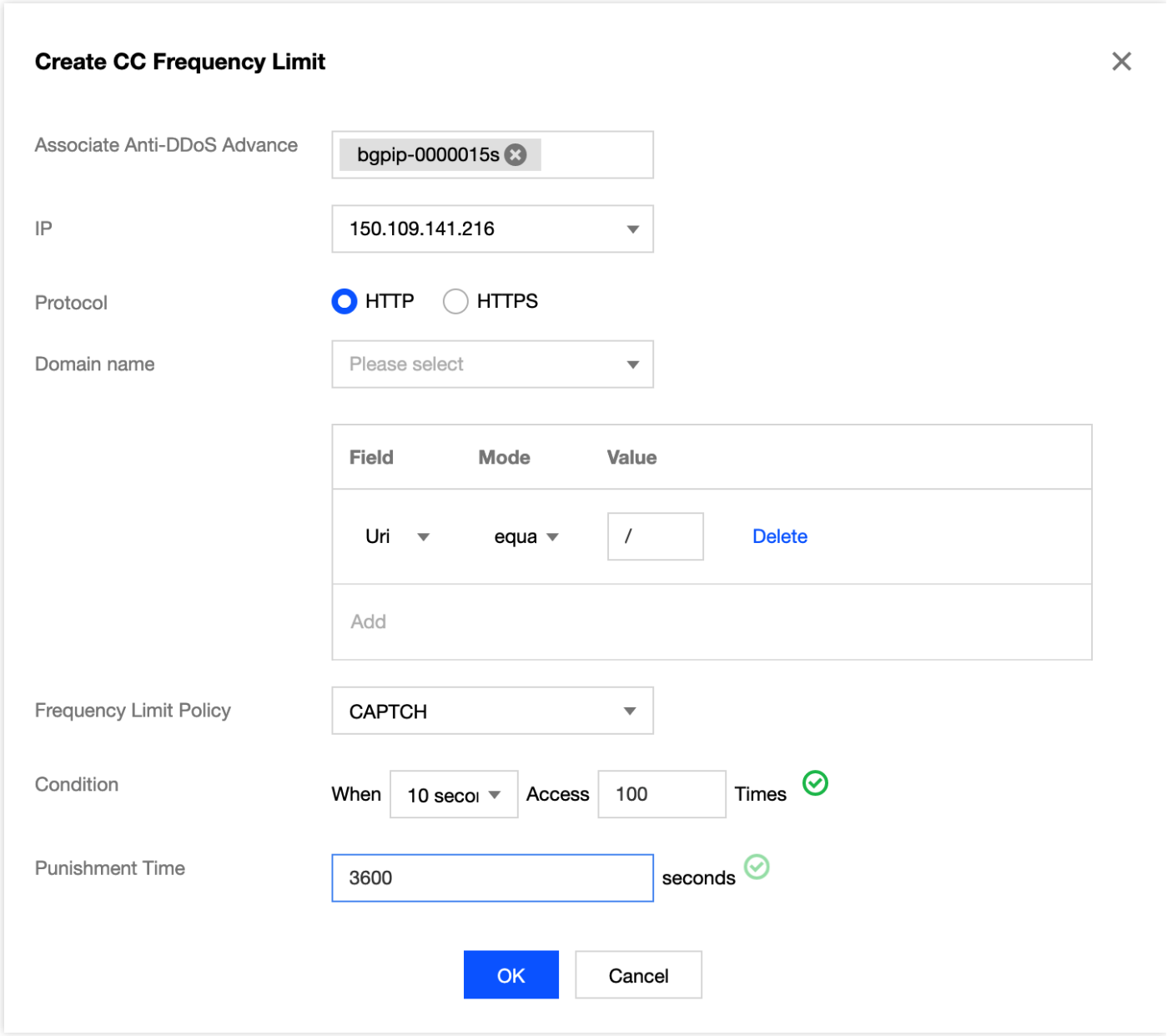
您需要成功 购买 DDoS 高防 IP（境外企业版），并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDoS 高防 IP** > **防护配置** > **CC 防护**。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID，如“bgp-00xxxxxx”。



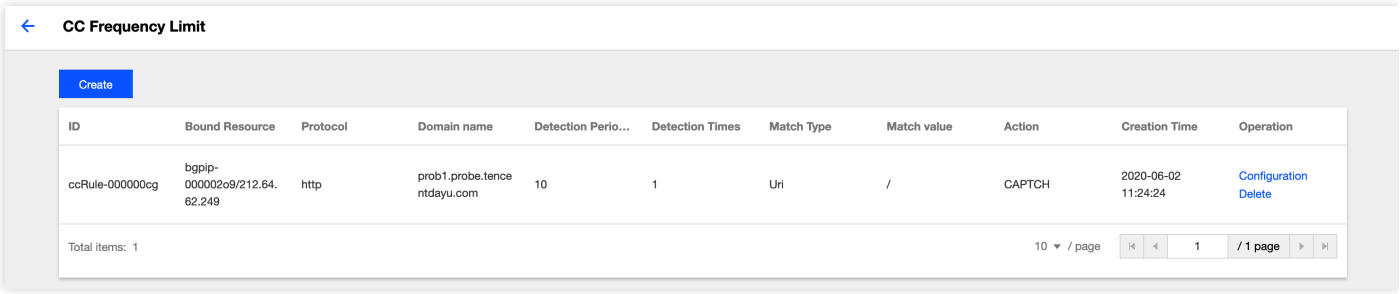
3. 在 CC 频率限制卡片中，单击**设置**。
4. 在 CC 频率限制列表，单击**新建**，选择或新增该 IP 下的域名，打开防护状态，选择相应的防护等级。
5. 如需设置自定义规则，单击**新增规则**，创建频率限制规则，填写相关字段，单击**确定**。



参数说明：

- 域名：该资源 IP 下的业务域名。
- 频率限制策略
  - 丢弃：触发条件后，直接断开连接。
  - 人机校验：对命中匹配条件的请求发起人机识别校验。
- 检测条件：指定在检测时长内，允许源 IP 访问被防护地址的次数。
- 惩罚时间：根据实际需求填写。

6. 新建完成后，在 CC 频率限制列表将新增一条 CC 频率限制规则，可以在右侧操作列单击**配置**，修改 CC 频率限制规则。

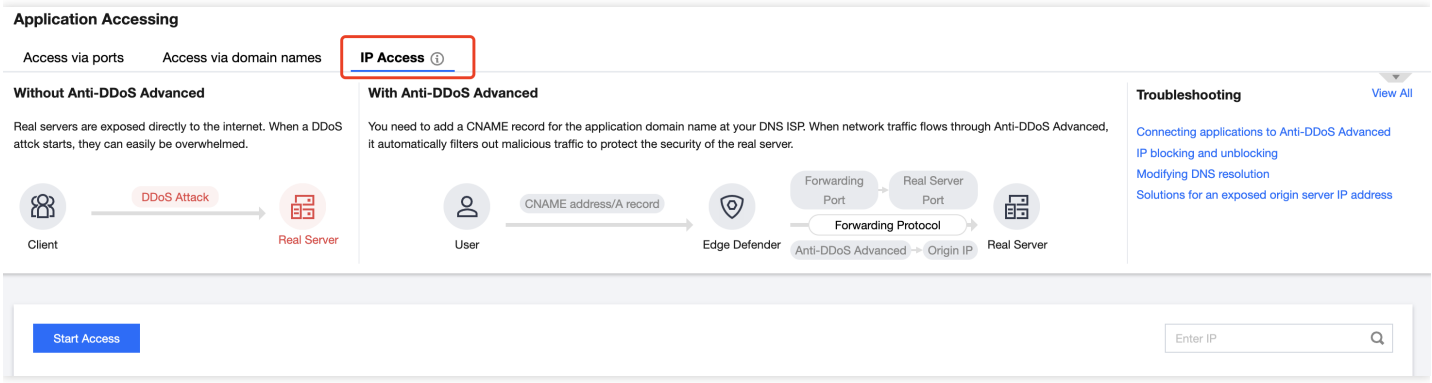


业务接入

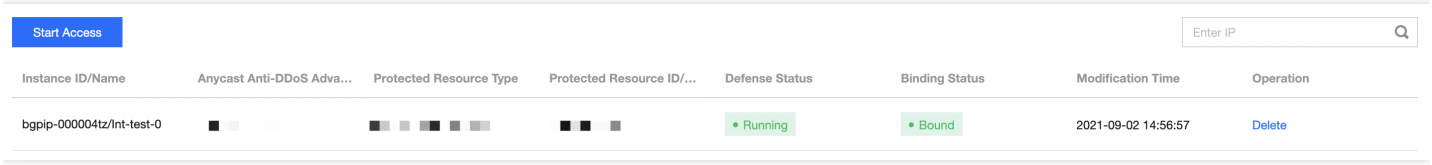
最近更新时间：2022-05-09 10:14:41

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDoS 高防 IP > 业务接入 > IP 接入**。

> 说明：
> DDoS 高防 IP（境外企业版）仅支持 IP 接入。

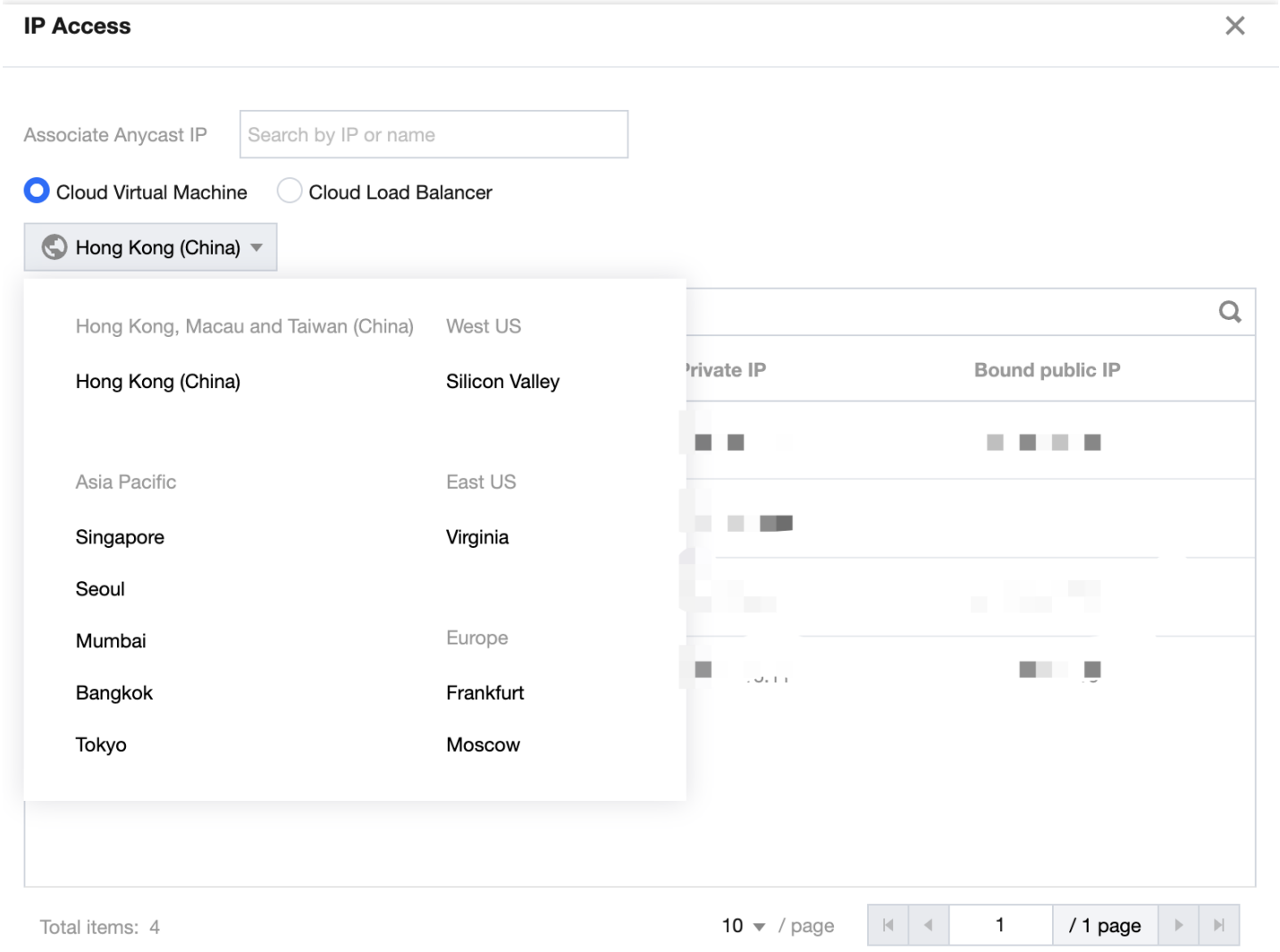


2. 在 IP 接入页面，单击**开始接入**，进入“绑定资源”弹窗。



3. 在“绑定资源”弹窗中，选择关联 Anycast 高防 IP、地区和可用实例后，单击**确定**，即可完成绑定资源。

> 说明：
> - 可用实例支持中国香港、新加坡、首尔、孟买、曼谷、东京、硅谷、弗吉尼亚、法兰克福、莫斯科地区筛选。
> - 当前支持绑定实例类型：云主机（CVM）和负载均衡（CLB）。


IP Access
Associate Anycast IP
Search by IP or name
Cloud Virtual Machine
Cloud Load Balancer
Hong Kong (China)
Hong Kong, Macau and Taiwan (China)
Hong Kong (China)
Asia Pacific
Singapore
Seoul
Mumbai
Bangkok
Tokyo
West US
Silicon Valley
East US
Virginia
Europe
Frankfurt
Moscow
rivate IP
Bound public IP
Total items: 4
10 / page
1
/ 1 page

实例管理
查看实例信息

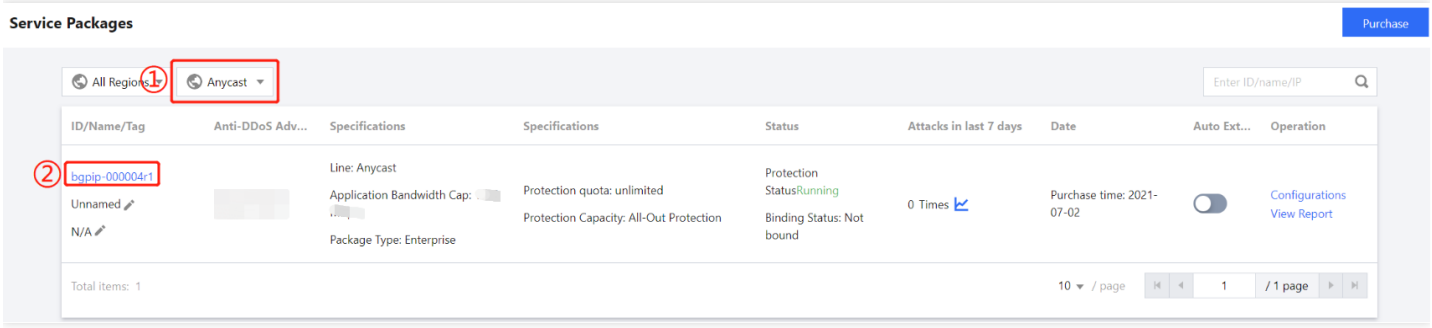
最近更新时间：2022-04-28 10:55:44

您可以通过 DDoS 防护管理控制台，查看所购买的 DDoS 高防 IP（境外企业版） 的基础信息（如实到期时间及运行状态）及实例的防护配置。

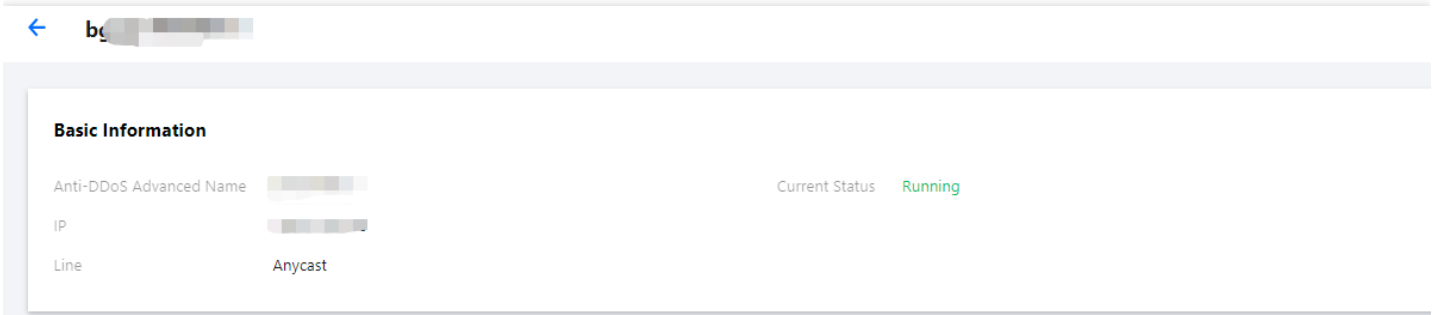
操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击 **DDoS 高防 IP** > **实例列表**。
2. 单击**全部线路**筛选为“Anycast”，选择所需实例 ID，单击“实例 ID ”查看实例详细信息。

> 说明：
> 如果实例数量较多可以使用右上角的搜索框过滤。



3. 在弹出的页面中查看如下信息：



参数说明：

- **高防 IP 名称**
  该 DDoS 高防 IP 实例的名称，用于辨识与管理 DDoS 高防 IP 实例。长度为1 - 20个字符，不限制字符类型。资源名称由用户根据实际业务需求自定义设置。
- **IP**
  该 DDoS 高防 IP（境外企业版） 实例所提供的 Anycast 高防 IP 的 IP 地址。
- **当前状态**
  DDoS 高防 IP 实例当前的使用状态。状态包括运行中，清洗中以及封堵中等。
- **到期时间**
  根据 购买 时选择的【购买时长】以及支付购买订单的具体时间计算所得，精确到秒级。腾讯云会在此时间前的前7天内，通过站内信、短信及邮件的方式向腾讯云账号的创建者以及所有协作者推送服务即将到期并提醒及时续费的信息。
- **标签**
  表示该 DDoS 高防 IP（境外企业版） 实例所属的标签名称，可以编辑、删除。

设置实例别名与标签

最近更新时间：2022-03-18 10:15:43

当使用多个 DDoS 高防 IP 实例时，可通过设置资源名称快速辨识与管理实例。

前提条件

您需要成功 购买 DDoS 高防 IP （境外企业版），并设置防护对象。

操作步骤

方式一

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击【DDoS 高防 IP】>【实例列表】。
2. 在实例列表中，找到需要编辑名称的实例，单击目标实例的“ID/名称/标签”列的第二行  图标，输入名称即可。

> 说明：
> 名称长度为1 - 20个字符，不限制字符类型。

方式二

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击【DDoS 高防 IP】>【实例列表】。
2. 在实例列表中，找到需要编辑名称的实例，单击目标实例的“ID/名称/标签”列的实例 ID，进入实例的基础信息页面。
3. 在实例的基础信息页面中，单击高防 IP 名称右侧  图标，输入名称即可。

设置安全事件通知

最近更新时间：2021-08-26 12:15:14

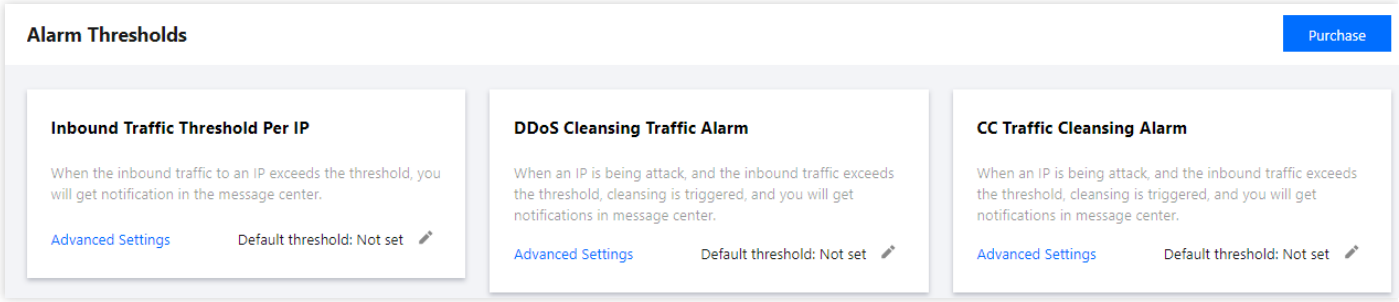
当您所使用的高防 IP 受到攻击、受攻击结束、IP 被封堵以及解除封堵时，系统将以站内信、短信、邮件等方式（实际接收方式以您在 消息中心订阅 配置为准），向您推送告警消息：

- 攻击开始时，您将会收到攻击开始提示。
- 攻击结束后15分钟，您将收到攻击结束提示。
- IP 被封堵时，您将收到封堵提示。
- IP 解除封堵时，您将收到解除封堵提示。

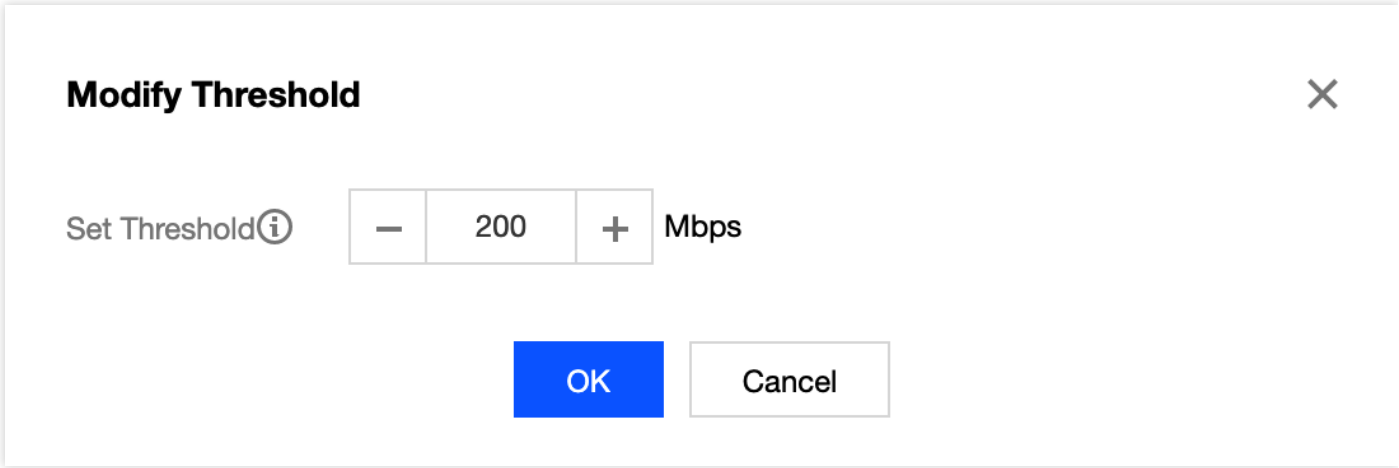
您可以根据实际情况修改告警信息的接收人和接收方式。

设置告警阈值

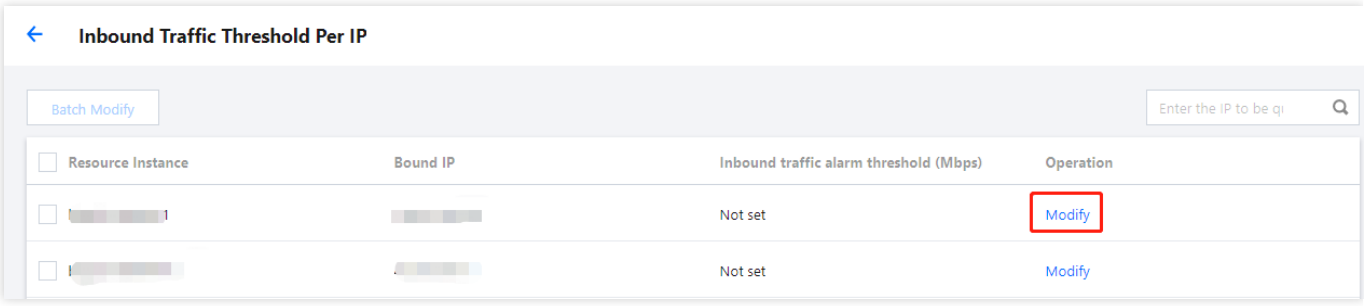
1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击【DDoS 高防 IP】>【告警通知】。
2. 在右侧的功能卡片中可以分别设置“单 IP 入流量告警阈值”、“DDoS 清洗阈值”和“CC 清洗流量告警”。



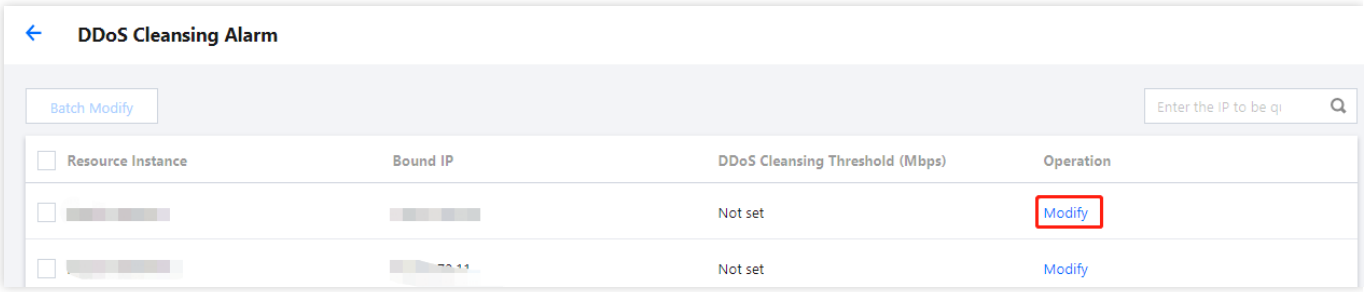
3. 单击单 IP 默认阈值右边的铅笔可以修改默认阈值，修改完成后，单击【确定】即可。



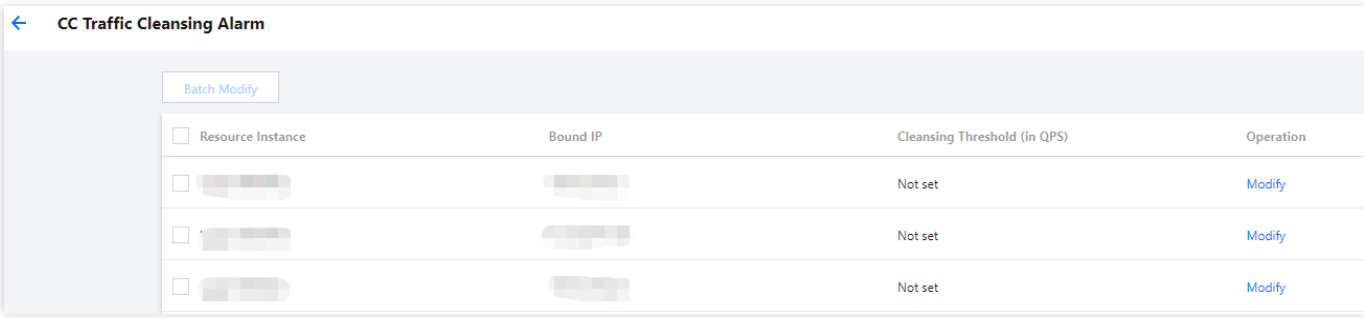
4. 单击卡片的【高级设置】，可以进入告警设置列表，单击【修改】为每个资源实例设置不同的告警阈值。
   - 单 IP 入流量告警



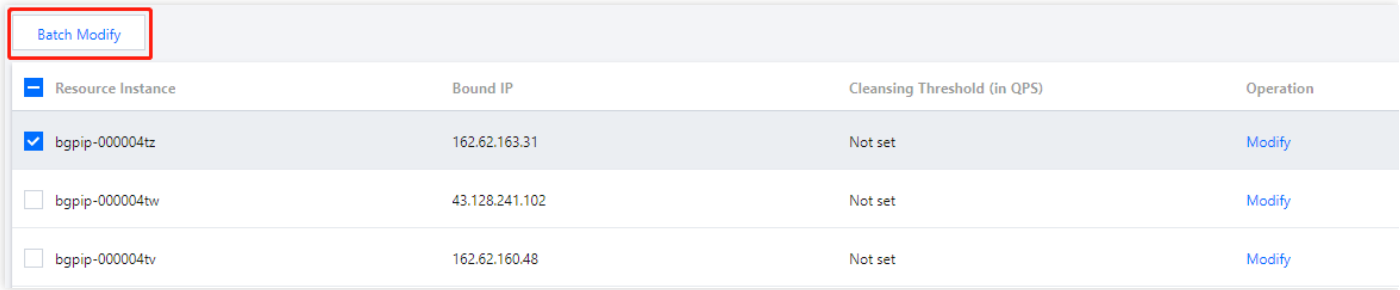
   - DDoS 清洗阈值



   - 设置 CC 清洗流量告警



5. 支持多个实例进行批量修改。选取多个实例后，单击【批量修改】，对选中多个实例进行批量修改。

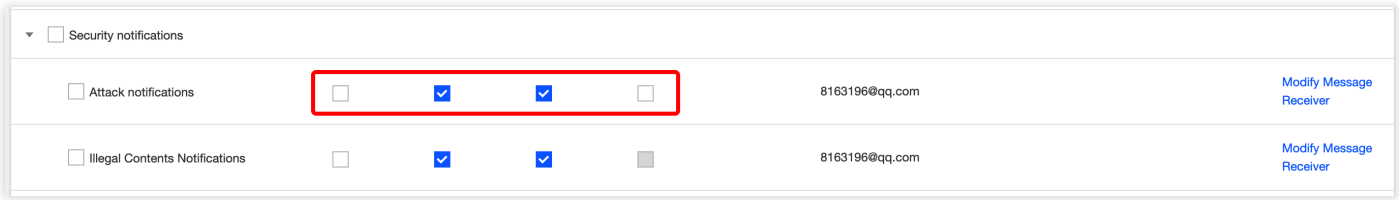


设置通知方式

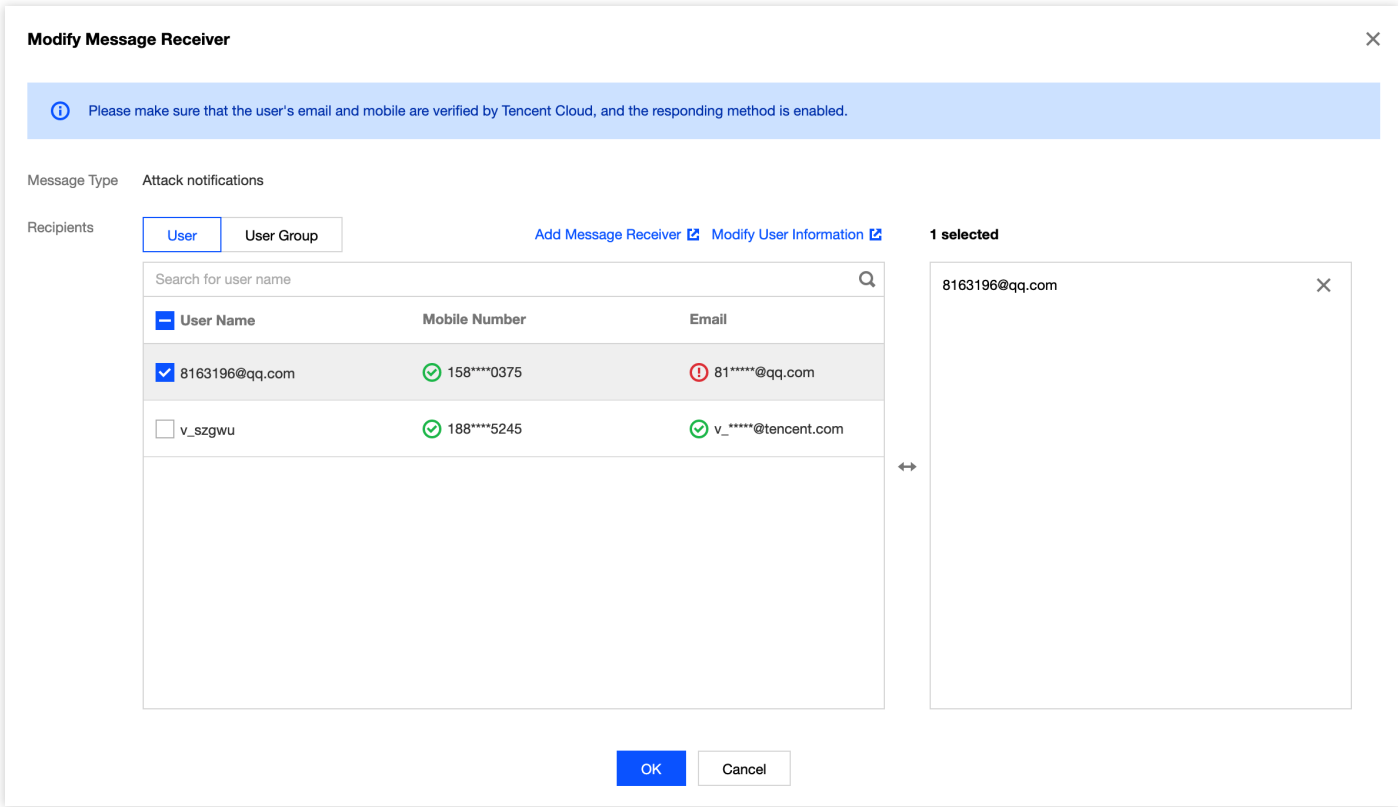
1. 登录您的腾讯云账号，进入 消息中心 。

> 说明：
>
> 您也可以登录 控制台 ，单击右上角的 ，在弹出页面，单击【查看更多】，进入消息中心。

2. 在左侧目录中，单击【消息订阅】，进入消息列表。
3. 在消息列表中，在安全事件通知所在列，选择接收方式，单击【修改消息接收人】，进入修改消息接收人页面。



4. 在修改消息接收人页面，进行消息接收人的设置，设置完成后，单击【确定】即可。



查看操作日志

最近更新时间：2021-07-14 20:08:40

应用场景

DDoS 高防IP（境外企业版）支持查看近180天内重要操作的日志，如有需要，您可以登录 DDoS 高防IP操作日志界面查看。可查看的日志包含以下类别：

- 防护对象 IP 更换日志
- DDoS 防护策略变更操作日志
- 清洗阈值调整日志
- 防护等级变更日志
- 资源名称的修改日志

操作步骤

1. 登录 DDoS 高防 IP（境外企业版） 控制台，在左侧导航中，单击【DDoS高防IP】>【操作日志】。
2. 在操作日志页面，可根据时间范围查询对应的操作记录，在右侧操作栏，单击【展开】，可查看日志详情。