

# DDoS 防护

## 操作指南

### 产品文档



Tencent Cloud

## 【版权声明】

©2013–2025 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

## 【商标声明】



及其他腾讯云服务相关的商标均为腾讯集团下的相关公司主体所有。另外，本文档涉及的第三方主体的商标，依法由权利人所有。

## 【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

# 文档目录

## 操作指南

操作概览

防护概览（总览）

使用限制

资产中心

云资产列表

云上防护实例

查看实例信息

管理防护对象

设置实例别名与标签

弹性修改防护宽带

解封防护 IP

业务接入

IP 透明接入

域名接入

IP 接入

端口接入

配置会话保持

配置健康检查

智能调度

防护配置

DDoS 防护

DDoS 防护等级

IP 黑白名单

端口过滤

协议封禁

水印防护

连续类攻击防护

AI 防护

区域封禁

IP 端口限速

特征过滤

CC 防护

CC 防护开关及清洗阈值

智能 CC 防护

精准防护

CC 频率限制

区域封禁

IP 黑白名单

安全运营

攻击分析

业务分析

操作日志

服务管理

解封中心

查看封堵时间

解除封堵

连接已被封堵的服务器

告警中心

设置安全事件通知

设置通知方式

# 操作指南

## 操作概览

最近更新时间：2024-07-01 11:33:59

您在使用 DDoS 基础防护、DDoS 高防包、DDoS 高防 IP 时，可能碰到诸如配置实例、查看统计报表、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 防护的常用操作，供您参考。

### 概览与限制

[防护概览（总览）](#)

[使用限制](#)

### 资产中心

[云资产列表](#)

[查看实例信息](#)

[管理防护对象](#)

[设置实例别名与标签](#)

[修改弹性防护宽带](#)

[解封防护 IP](#)

### 业务接入

[IP 透明接入](#)

[端口接入](#)

[域名接入](#)

[IP 接入](#)

### 调度与解封

[智能调度](#)

### 防护配置

#### DDoS 防护

[DDoS 防护等级](#)

[IP 黑白名单](#)

[端口过滤](#)

[协议封禁](#)

[水印防护](#)

[连接类攻击防护](#)

[AI 防护](#)[区域封禁](#)[IP 端口限速](#)[特征过滤](#)

## CC 防护

[CC 防护开关及清洗阈值](#)[智能 CC 防护](#)[精准防护](#)[CC 频率限制](#)[区域封禁](#)[IP 黑白名单](#)

## 安全运营

[攻击分析](#)[业务分析](#)[操作日志](#)

## 服务管理

[查看封堵时间](#)[解除封堵](#)[连接已被封堵的服务器](#)[设置安全事件通知](#)[设置通知方式](#)

# 防护概览（总览）

最近更新时间：2024-07-01 11:33:59

## 查看攻击态势

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击防护概览 > 防护总览，进入防护总览页面。
2. 在实时防御态势模块中，展示业务 IP 状态数据，可以快速了解业务 IP 健康状态。

安全态势 i



**安全**

资产健康，暂未发现异常流量恶意攻击

最近一次攻击： - 攻击类型： 暂无攻击

3. 在攻击态势模块中，还可以直观查看各项数据情况。



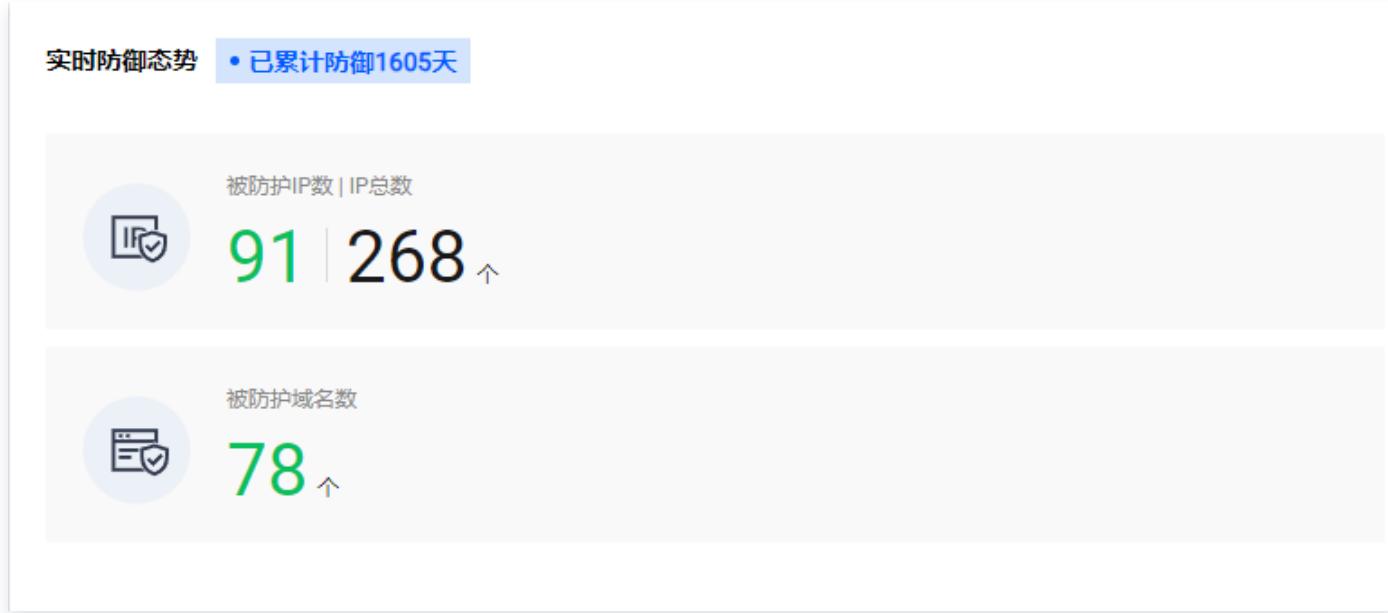
### 字段说明：

- 总攻击次数：受到攻击的总数，包括基础防护的业务、接入高防实例。
- 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。
- 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。

- 攻击峰值：当前攻击事件中的最高攻击带宽。
- 攻击包速率：当前攻击事件中的最高攻击包速率。
- 攻击请求峰值：当前攻击事件中最高攻击请求。

## 查看防御态势

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击防护概览 > 防护总览，进入防护总览页面。
2. 在实时防御态势模块中，展示业务 IP 状态数据，可以快速了解业务 IP 健康状态。

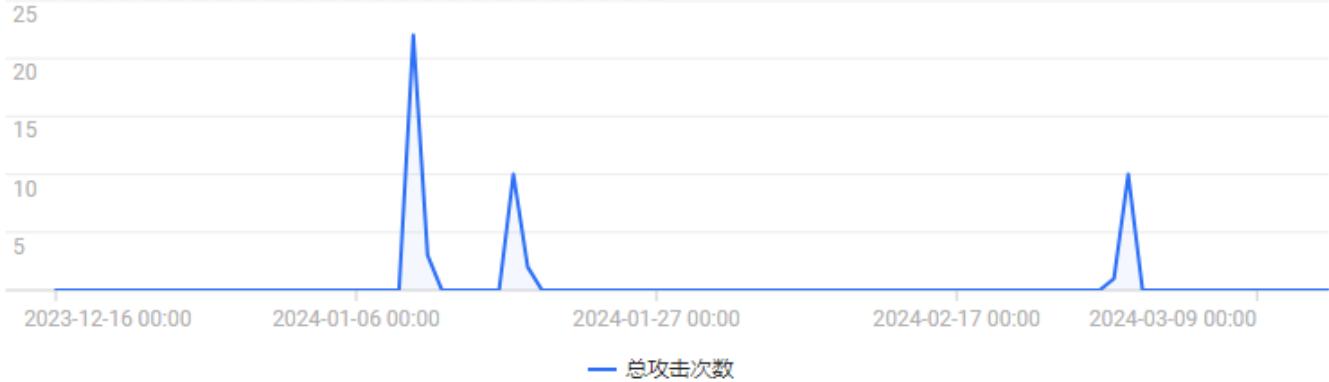


### 字段说明：

- 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的，可以快速了解近期攻击状态分布情况。

## 防护趋势



- 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。

## 查看防护实例详情

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击防护概览 > 防护总览，进入防护总览页面。
- 在防护实例详情模块中，展示高防资源的安全状态，可以快速全面了解风险业务分布。右侧展示防护配额状态，可以快速了解高防包、高防 IP 已用防护配额。



## 查看近期安全事件

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击防护概览 > 防护总览，进入防护总览页面。
- 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。

A table titled '近期安全事件' (Recent Security Events) listing two recent DDoS attacks. Each row includes details such as the attack name, target, start and end times, duration, status, event type, and actions taken.

攻击名称	高防资源	资产名称	防护类型	攻击时间	攻击时长	攻击状态	事件类型	操作
1	高防IP	未命名	高防IP	开始: 2024-02-29 17:07:00 结束: 2024-02-29 17:12:00	5分钟	结束	DDoS 攻击	<a href="#">查看详情</a> <a href="#">升级防护</a> <a href="#">攻击也下载</a>
2	高防IP	未命名	高防IP	开始: 2024-02-29 16:44:00 结束: 2024-02-29 16:49:00	5分钟	结束	DDoS 攻击	<a href="#">查看详情</a> <a href="#">接入防护</a> <a href="#">攻击也下载</a>

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。

### DDoS 攻击事件详情

**攻击信息**

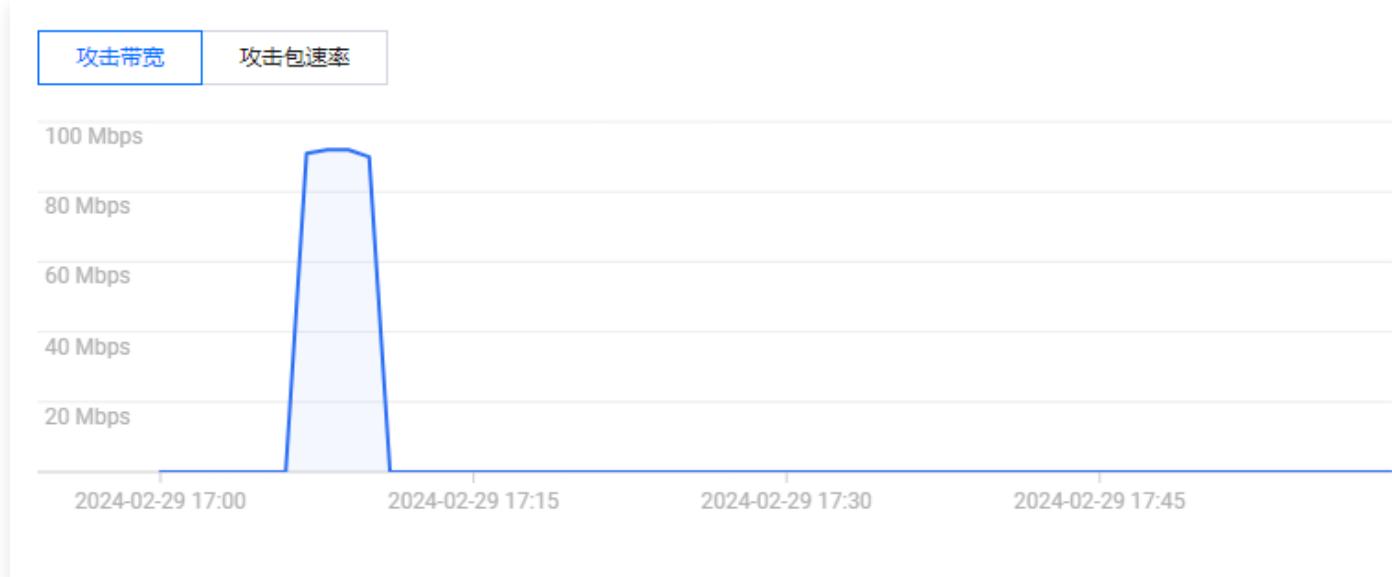
高防资源		攻击带宽峰值	92Mbps
状态	• 攻击结束	攻击包速率峰值	11073pps
攻击类型	SYNFLOOD	攻击开始时间	2024-02-29 17:07:00
		攻击结束时间	2024-02-29 17:12:00



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。

### 攻击相关统计



TCP 2.10GB



SYNFLOOD 1

#### 字段说明:

- 攻击流量协议分布：查看该时间范围内，所选择的 DDoS 防护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 DDoS 防护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。

#### TOP5 攻击源IP ①



#### TOP5 攻击源地区 ①



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。

### 攻击源信息 ①

攻击源IP	地区	累计攻击流量	累计攻击包量
██████████	美国	26.4 MB	24894
██████████	德国	26.6 MB	25106

共 2 条 / 1 页

8. 在近期安全事件模块中，可展示所遭受的 DDoS 攻击事件。

- 选择所需事件，单击查看详情，右侧将展示该事件的具体详情。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。

Recent Events								
Attack name	Anti-DDoS Resources	Instance Name	Defense Type	Attack time	Attack duration	Attack status	Event type	Operation
SYNFLOOD attacks	██████████	██████████	Anti-DDoS Basic	Started at: ██████████ Ended at: ██████████	7 mins	Attack ended	DDoS Attack	<a href="#">View details</a> <a href="#">Access</a> <a href="#">Packet Download</a>
SYNFLOOD attacks	██████████	██████████	Anti-DDoS Basic	Started at: ██████████ Ended at: ██████████	5 mins	Attack ended	DDoS Attack	<a href="#">View details</a> <a href="#">Access</a> <a href="#">Packet Download</a>

- 选择所需事件，单击攻击包下载，在攻击包列表中，选择所需 id，可下载本次攻击计时间段的攻击包采样数据，详细了解攻击数据和类型，用户制定针对性的防护方案提供数据支撑。

攻击包列表		
id	时间	操作
[REDACTED]	2024-02-29 17:07:31	<a href="#">下载</a>
[REDACTED]	2024-02-29 17:07:31	<a href="#">下载</a>
共 2 条	10 ▾ 条 / 页	<a href="#">1</a> / 1 页 <a href="#">▶</a> <a href="#">◀</a> <a href="#">◀◀</a> <a href="#">▶▶</a>

## 查看 DDoS 攻击防护情况

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击防护概览 > 攻击态势。
- 在 DDoS 攻击页签，设置查询时间范围，选择目的地域、线路和高防包实例，查看是否存在攻击。默认展示全量资产的 DDoS 攻击数据。

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



- 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。



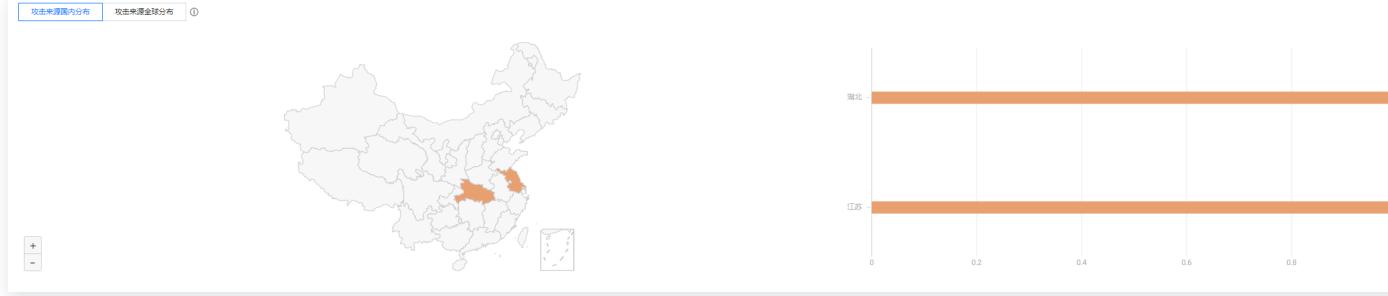
字段说明：

- 攻击流量协议分布：查看该时间范围内，所选择的DDoS 防护 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DDoS 防护 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DDoS 防护 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 攻击页签，设置查询时间范围，选择目的地域和高防包实例，查看是否存在 CC 攻击。



2. 用户可以选择所需时间，查看所选择的高防实例请求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，高防实例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，高防实例接收到的总请求数量。
- 攻击请求次数：统计当前，高防实例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、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。

# 使用限制

最近更新时间：2024-07-01 11:33:59

## DDoS 基础防护

### 防护对象限制

为腾讯云内 CVM、CLB 及 NAT 网关等云产品，提供免费的基础 DDoS 防护。

## DDoS 高防包

### 防护对象限制

DDoS 高防包仅适用于腾讯云产品，包含 CVM、CLB、WAF、NAT 网关、VPN 网关、轻量应用服务器等。

### 接入限制

DDoS 高防包仅支持绑定同一地域内的腾讯云公网 IP。

#### 黑白名单配置限制

- DDoS 黑白 IP 名单之和最多支持添加100条记录（IP 地址 + IP 段）。
- CC URL 白名单暂不支持配置。

### 地域限制

DDoS 高防包只能绑定同一地域内的腾讯云设备，目前开放购买的地域包括：北京、上海、广州、中国香港、新加坡、首尔、东京、曼谷、法兰克福。

#### 说明：

当前 DDoS 高防包境外区域通过开白名单的形式进行售卖，如需购买境外区域的 DDoS 高防包，可以直接[联系我们](#)开白名单。

## DDoS 高防 IP

### 防护对象建议

建议使用 DDoS 高防 IP 为腾讯云内外的业务 IP 或域名提供防护，支持对网站（七层）业务和非网站（四层）业务进行防护。

### 转发能力限制

1个 DDoS 高防 IP 实例默认支持60个转发规则（四层接入加七层接入共60个），最高支持500个转发规则，非网站（四层）协议下每条规则支持20个源站 IP/域名，网站（七层）协议下则支持16个源站 IP/域名。

**!** 说明:

转发规则数为 TCP/UDP 协议 + HTTP/HTTPS 协议转发规格条目总数，最高可升级至 500条。对于 TCP、UDP 协议，若使用相同的转发端口值，则需要配置两条。

## 黑白名单配置限制

- DDoS 黑白 IP 名单之和最多支持添加100个 IP 地址。
- URL 不支持白名单配置。

## 地域限制

目前已开放 DDoS 高防 IP 的地域覆盖中国大陆区域和非中国大陆区域，非中国大陆区域包括中国香港、中国台湾、新加坡、首尔、东京、弗吉尼亚、硅谷、法兰克福。

# 资产中心

## 云资产列表

最近更新时间：2024-11-01 16:10:14

### 查看资产安全状态

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击云资产列表页面。
- 在资产安全状态模块中，展示业务 IP 安全状态数据，可以快速了解业务 IP 安全状态。



- 在资产防护状态模块中，展示业务 IP 防护状态数据，可以快速了解业务 IP 安全状态，可直接接入防护。



### 查看资产实例详情

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击云资产列表页面。
- 以云主机为例。在详情页面可以查看该资产的详细信息，包括资产实例名称、IP 地址、防护类型、防护实例ID、防护能力、攻击状态等信息。

云主机	负载均衡	Web应用防火墙	NAT网关	VPN网关	弹性网卡	GAAP	互联网通道	云原生API网关	API网关	黑石物理机	黑石负载均衡	黑石弹性IP	轻量应用服务器
资产ID/名称	资产IP	防护类型	防护实例ID	最大防护能力	攻击状态	操作	广州	请输入IP或名称 (支持模糊搜索,暂不支持精确搜索)					

使用 DDoS 高防可为如下产品提升 DDoS 防护能力：

- 云服务器**：是腾讯云提供的可扩展的计算服务。使用云服务器 CVM 避免了使用传统服务器时需要预估资源用量及前期投入的问题，帮助您在短时间内快速启动任意数量的云服务器并即时部署应用程序。
- 负载均衡**：提供安全快捷的流量分发服务，访问流量经由 CLB 可以自动分配到云中的多台云服务器上，扩展系统的服务能力并消除单点故障。
- Web 应用防火墙**：是一款基于 AI 的一站式 Web 业务运营风险防护方案。
- NAT 网关**：是一种支持 IP 地址转换服务，提供 SNAT 和 DNAT 能力，可为私有网络（VPC）内的资源提供安全、高性能的 Internet 访问服务。

- **VPN 连接**：是一种基于网络隧道技术，实现本地数据中心与腾讯云上资源连通的传输服务，它能帮您在 Internet 上快速构建一条安全、可靠的加密通道。
- **裸金属云服务器**：是一种可按需购买、按量付费的物理服务器租赁服务，提供给您云端专用的高性能、安全隔离的物理服务器集群。
- **黑石负载均衡**：通过虚拟服务地址（VIP），将位于同一可用区的多台物理服务器资源虚拟成一个高性能、高可用的应用服务池。
- **黑石弹性公网 IP**：黑石弹性公网 IP（Elastic IP, EIP）地址是专用于动态云计算的 IP 地址，是可以独立申请的公网 IP 地址。
- **全球应用加速**：是一款实现业务全球最佳访问延迟的 PAAS 类产品，依赖全球节点之间的高速通道、转发集群及智能路由技术，实现各地用户的就近接入，并将流量转发至源站，帮助业务解决全球用户访问卡顿或者延迟过高的问题。
- **弹性网卡**：是绑定私有网络（VirtualPrivate Cloud, VPC）内云服务器的一种弹性网络接口，可在多个云服务器间自由迁移。弹性网卡对配置管理网络与搭建高可靠网络方案有较大帮助。
- **轻量应用服务器**：是新一代开箱即用、面向轻量应用场景的云服务器产品，助力中小企业和开发者便捷高效的在云端构建网站、Web 应用、小程序/小游戏、App、电商应用、云盘/图床和各类开发测试环境，相比普通云服务器更加简单易用且更贴近应用，以套餐形式整体售卖基础云资源并提供高带宽流量包，将热门开源软件融合打包实现一键构建应用，提供极简上云体验。

## 管理云资产

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击云资产列表。
2. 在云资产列表页面，可单击上方的产品，找到该产品的资产。如果实例数量较多可以使用右上角的搜索框过滤。



3. 选中所需资产后，可以对该资产进行如下操作：

- 单击设置告警阈值，可以根据需求自定义告警策略，单击确定。



- 升级防护，当业务增长需要同一个高防包防护多个业务 IP 时，可以升级防护为覆盖所有业务 IP 的防护。
- 单击攻击分析，页面跳转至防护概览（总览）页面，查看攻击态势。
- 单击防护配置，页面跳转至 DDoS 防护页面，查看 DDoS 防护配置。

# 云上防护实例

## 查看实例信息

最近更新时间：2024-07-01 11:33:59

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击云上防护实例，进入云上防护实例页面。
2. 在云上防护实例页面，支持查看所购买的 DDoS 高防包的基础信息（如实例保底防护峰值、运行状态）；所购买的 DDoS 高防 IP 的基础信息（如实例保底防护峰值及运行状态）及实例的弹性防护配置。

## 操作步骤

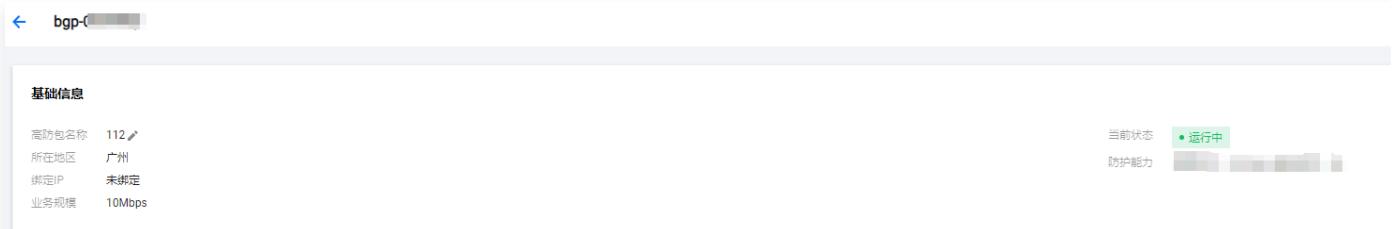
### 示例：查看 DDoS 高防包“bgp-00000jt3”的实例信息

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击云上防护实例，进入云上防护实例页面。
2. 在云上防护实例页面，可单击上方的全部地域选择地域或选择防护套餐类型，找到实例 ID 为“bgp-00000jt3”的高防包，单击 ID“bgp-00000jt3”查看实例详细信息。如果实例数量较多可以使用右上角的搜索框过滤。



The screenshot shows the 'Cloud Protection Instances' section of the DDoS Protection (New Version) control panel. It lists instances based on filters:地域 (Region) is set to 全部地域 (All Regions), 套餐类型 (Plan Type) is set to DDoS高防包 (DDoS High Defense Package), and the search term is 'bgp-00000jt3'. The table columns include 实例ID/名称/标签 (Instance ID/Name/Label), 实例类型 (Instance Type), IP协议 (IP Protocol), 接入资源 (Access Resource), 业务规格 (Business Specification), 防护规格 (Protection Specification), 防护状态 (Protection Status), 实例状态 (Instance Status), 最近7天攻击 (Recent 7 Days Attacks), 日期 (Date), and 操作 (Operations). One instance row is expanded to show detailed information.

3. 在弹出的页面中查看如下信息：



The screenshot shows the detailed view for the DDoS instance 'bgp-00000jt3'. The 'Basic Information' section displays the following details:

- 高防包名称 (Instance Name): bgp-00000jt3
- 所在地区 (Region): 广州 (Guangzhou)
- 绑定IP (Bound IP): 未绑定 (Not Bound)
- 业务规格 (Business Specification): 10Mbps
- 当前状态 (Current Status): 运行中 (Running) - indicated by a green dot
- 防护能力 (Protection Capacity): 显示了三个灰色进度条，分别代表不同的防护能力指标。

参数名称	说明
高防名称	该 DDoS 高防包实例的名称，用于辨识与管理 DDoS 高防实例。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。
所在地区	为购买 DDoS 高防时选择的地域。
当前状态	DDoS 高防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。 <ul style="list-style-type: none"><li>● 创建中：正在创建高防实例。</li><li>● 运行中：实例防护进行中。</li><li>● 受攻击：遭受攻击。</li><li>● 封堵中：正在对实例进行封堵。</li></ul>

	<ul style="list-style-type: none"> <li>解封中：实例正在解封中。</li> <li>回收中：实例已到期，正在进行回收。</li> </ul>
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。DDoS 高防资源到期前7天内，系统会向您推送资源即将到期提醒，消息通过站内信、短信、邮件、微信等方式（实际接收方式以您在消息中心订阅配置为准）通知到腾讯云账号创建者以及所有协作者。

## 示例：查看高防 IP 的实例信息

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击云上防护实例，进入云上防护实例页面。
- 在云上防护实例页面，选择所需实例，单击“ID”查看实例详细信息。如果实例数量较多可以使用右上角的搜索框过滤。

The screenshot shows the 'Cloud Protection Instances' section of the DDoS Protection console. It lists several instances, each with a unique ID, name, type (e.g., 'DDoS High-Defense IP'), protocol (e.g., 'IPv4'), and various configuration details like 'CNAME' and 'Line'. A search bar at the top right is highlighted with a red box. The interface includes filters for 'Region' (set to 'All Regions'), 'DDoS High-Defense IP', 'Protection Status' (set to 'Running'), and a date range.

- 在弹出的页面中查看如下信息：

The screenshot shows the detailed view of a specific DDoS High-Defense IP instance. It includes sections for 'Basic Information' and 'Advanced Configuration'. In the 'Basic Information' section, key details are listed: 'High-Defense IP Name' (未命名), 'Location' (中国香港), 'CNAME' (bgpip-...), 'Peak Protection Bandwidth' (1 Gbps), 'CC Protection Bandwidth' (1 QPS), 'Line' (BGP), and 'Discovery Rule Status' (Normal). The 'Advanced Configuration' section shows 'Resolution Target IP' (\*\*\*\*\*), 'Current Status' (Running), and 'Return IP Segment' (bgpip-...).

参数名称	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。
解析目标 IP	该 DDoS 高防 IP 实例具有高防属性的 IP。此 IP 地址将不定期更换。 注意：建议将您的 DNS 解析地址修改至 CNAME，避免 DNS 解析失败。
所在地区	购买 DDoS 高防 IP 时选择的地域。
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。
CNAME	该 DDoS 高防 IP 实例的 CNAME。由该 CNAME 解析至拥有高防属性的 IP

上，通过清洗中心后并转发回源站，实现防护。

**注意：建议将您的 DNS 解析地址修改至 CNAME，避免 DNS 解析失败。**

保底防护峰值	该 DDoS 高防 IP 实例的保底防护带宽能力，即购买时选择的保底防护峰值。若未开启弹性防护，则保底防护峰值为高防服务实例的最高防护峰值。
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 实例所属的标签名称，可以编辑、删除。
回源 IP 段	清洗集群转发至源站所用 IP。

# 管理防护对象

最近更新时间：2024-07-01 11:33:59

DDoS 高防包为腾讯云公网 IP 提供更高的 DDoS 防护能力，可支持防护 CVM、CLB、NAT、WAF 等产品和服务。用户根据实际业务需求，可以增加或删除 DDoS 高防包实例的防护对象 IP。

## 前提条件

设置防护对象 IP，您需要成功 [购买 DDoS 高防包](#)。

### 说明：

DDoS 高防包（企业版）仅针对腾讯云弹性公网 IP 下的高防 EIP 生效，使用企业版高防包需要将云上普通 IP 更换为高防 EIP，购买企业版高防包需与最终绑定云资源的地域相同，并绑定高防 EIP 后才实际生效。高防 EIP 操作详情请参见 [高防 EIP 创建使用指引](#)。

## 操作步骤

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航中，单击云上防护实例。
- 在云上防护实例页面，单击目标 DDoS 高防包实例所在行的管理防护对象。

The screenshot shows the 'Manage Protection Objects' page for a DDoS High Defense instance. The instance details are as follows:

实例ID/名称/标签	实例类型	IP协议	接入类型	业务规格	防护规则	防护状态	实例状态	最近7天攻击	日期	操作
未命名 ✓ 无 ✕	DDoS高防IP	IPv4	CNAME: 解析目标IP: [REDACTED]	线路: BGP(中国香港) 业务带宽: 50Mbps 弹性业务带宽: ① [Switched On] <input checked="" type="checkbox"/> 套餐信息: 标准套餐	保底峰值: 20Gbps 弹性峰值: 未开启 ✓ CC峰值: 40000QPS	端口防护: 0 域名防护: 2	运行中	0 次	购买时间: 2024-01-09	<a href="#">防护策略</a>

- 在管理防护对象页面，根据实际防护需求选择关联设备类型与资源实例。

- 关联设备类型：支持云主机，负载均衡，Web 应用防火墙等公有云具有公网 IP 的资源。

### 说明：

高防包企业版仅支持高防 EIP。

- 选择资源实例：单击资源 ID 前面的选项复选框，将资源添加到高防包的防护对象，允许多选，选择资源实例数量不得超过可绑定 IP 数。
- 已选择：单击资源后面的删除，将资源从高防包的防护对象中删除。

**防护配置**

**DDoS防护逻辑**

策略对所有经过带宽的流量进行生效，命中规则执行防护动作。

不同策略类型的生效优先级为：

IP黑白名单、端口封禁、协议封禁、连接类攻击防护、水印防护、特征过滤、区域封禁、黑洞限速

**防护配置说明**

各类型的防护应用在对应的引擎上，IP黑白防护策略仅应用在DDoS引擎上，域名防护策略仅应用在CC防护引擎上。

**常见问题**

为什么我的防护台有欠款待付？有哪些限制？  
如何查看已经封禁的服务器？  
攻击级别设置

**DDoS防护等级**

CNAME

防护实例: bgoip-  
防护业务:

防护策略  严格  中等  宽松  清洗阈值

**防护子策略**

<b>IP黑白名单</b> 通过配置IP黑名单和白名单来实现对访问DDoS高防的源IP封禁或者放行，从而限制访问业务选择的用户。  已设置 0 个黑名单 <input type="button"/> 已设置 0 个白名单 <input type="button"/>	<b>端口过滤</b> 针对访问DDoS高防的源流量，基于端口进行一键封禁放行。  已设置 0 个过滤规则 <input type="button"/>
<b>协议封禁</b> 针对访问DDoS高防的源流量，按照协议类型一键封禁，如果没有VIP业务，建议封禁UDP协议。  已设置 0 个协议封禁 <input type="button"/>	<b>水印防护</b> 通过对业务和DDoS高防共享水印算法和密钥，客户跨每个发出的报文都嵌入水印特征，能有效识别4层CC攻击报文次数和重放攻击。  已启用 0 个防护规则 <input type="button"/>
<b>连接类攻击防护</b> 针对连接类攻击设置精细化防护策略。  已设置 0 个防护策略 <input type="button"/>	<b>AI防护</b> 智能AI引擎学习业务数据轨迹与流量特征，发现并阻断四类典型CC攻击，可有效防护僵尸网络攻击。  当前防护状态: <input checked="" type="checkbox"/> <input type="button"/>
<b>区域封禁</b> 针对访问DDoS高防的源IP，按地理区域在清洗节点进行封禁。  已设置 0 个区域封禁 <input type="button"/>	<b>IP端口限速</b> 对于业务IP，基于IP+端口的维度进行流量访问限速。  已设置 0 个限速规则 <input type="button"/>

### 说明：

- DDoS 高防包如果有 IP 处于封堵状态下，则不允许用户解绑该 IP。
- 当关联云资产时，支持批量搜索和选择。
- 当前支持检测 CLB、CVM 产品的销毁状态，并进行解绑。

4. 单击确定即可。

# 设置实例别名与标签

最近更新时间：2024-07-01 11:33:59

使用多个 DDoS 高防包实例或 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 高防包 或 DDoS 高防 IP。

## 操作步骤

### 方式一

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击云上防护实例。

2. 在云上防护实例页面，单击目标实例的“ID/名称”列的第二行 ，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。



The screenshot shows a table of cloud protection instances. One row is selected, showing the following details:

实例ID/名称/标签	实例类型	IP协议	接入类型	业务规格	防护规格	防护状态	实例状态	最近7天攻击	日期	操作
DDoS高防包	DDoS高防包	IPv4 IPv6	未绑定	所属地域：广州 套餐类型：企业版 业务规模：10Mbps 已使用 / 防护带宽：0/1 弹性业务带宽：○	保底速率：30000bps 弹性速率：未开启 ✓	接口防护：适中 ✕	运行中	未绑定IP	购买时间：2024-01-19	<a href="#">管理防护对象</a> <a href="#">购买配置</a>

### 方式二

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击云上防护实例。

2. 在云上防护实例页面，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。



The screenshot shows a table of cloud protection instances. One row is selected, showing the following details:

实例ID/名称/标签	实例类型	IP协议	接入类型	业务规格	防护规格	防护状态	实例状态	最近7天攻击	日期	操作
bgp-...	DDoS高防包	IPv4 IPv6	未绑定	所属地域：广州 套餐类型：企业版 业务规模：10Mbps 已使用 / 防护带宽：0/1 弹性业务带宽：○	保底速率：30000bps 弹性速率：未开启 ✓	接口防护：适中 ✕	运行中	未绑定IP	购买时间：2024-01-19	<a href="#">管理防护对象</a> <a href="#">购买配置</a>

3. 在实例的基础信息页面中，单击高防包名称或高防 IP 名称右侧的 ，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。

[←](#) bgp-[REDACTED]

**基础信息**

高防包名称	
所在地区	广州
绑定IP	未绑定
业务规模	10Mbps

# 弹性修改防护宽带

最近更新时间：2024-07-01 11:33:59

弹性防护峰值指 DDoS 高防服务可提供抵御攻击流量的能力范围。若攻击流量超过最高防护峰值，则被攻击 IP 将触发封堵。

## 前提条件

您需要成功 购买 DDoS 高防 IP 。

## 操作步骤

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击云上防护实例。
- 在目标 DDoS 高防 IP 实例所在行的防护规格中，单击弹性峰值后 。

实例ID/名称/标签	实例类型	IP协议	接入资源 	业务规格	防护规格	实例状态 	最近7天攻击	日期	操作
未命名  	DDoS高防IP	IPv4	CNAME: 	解析目标IP: 	线路: BGP(中国香港) 业务带宽: 50Mbps 弹性带宽: ①   套餐信息: 标准套餐	保底峰值: 20Gbps 弹性峰值: 未开启  CC峰值: 40000QPS	端口防护: 0 域名防护: 2	 运行中 0 次	购买时间: 2024-01-09 
未命名  	DDoS高防IP	IPv4	解析目标IP: 	线路: BGP(广州) 业务带宽: 100Mbps 弹性带宽: ①   套餐信息: 标准套餐	保底峰值: 30Gbps 弹性峰值: 未开启  CC峰值: 40000QPS	端口防护: 2 域名防护: 7	 运行中 0 次	购买时间: 2024-01-04 	

- 在设置弹性防护弹框中，根据实际防护需求选择弹性防护峰值。

设置弹性防护

ID/服务包名 bgpip-0000057s / 未命名

保底防护 20Gbps

弹性防护峰值  30Gbps  40Gbps  50Gbps  60Gbps  70Gbps  80Gbps  90Gbps  100Gbps  150Gbps  200Gbps

费用说明 未触发弹性防护，不另收费用。  
如果攻击发生当日流量带宽峰值超出20Gbps，会按照当日流量带宽峰值落入的计费区间进行计算，产生后付账账单。

计费区间如下:

弹性防护峰值(Gbps)	20~30	30~40	40~50	50~60	60~70	70~80	80~90	90~100	100~120	120~150	150~200	200~250	250~300	300~400
弹性防护费用(美元/天)	400	700	800	1200	1800	2200	2500	2700	2900	3200	4000	4800	5600	6600

### 说明:

由于弹性防护峰值和费用受到不同地区以及不同版本的影响，实际弹性防护峰值和费用以控制台显示为准。

- 选择完成后，单击确定即可。

# 解封防护 IP

最近更新时间：2024-07-01 11:33:59

DDoS 防护对进入封堵状态的防护 IP 提供解封的功能，您可以登录 [DDoS 防护（新版）控制台](#) 进行自助解封操作。

## 自助解封次数

使用 DDoS 高防包或 DDoS 高防 IP 用户每天将拥有三次自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

### 说明：

- 在执行解封操作前，建议您先查看预计解封时间，预计解封时间受到部分因素影响，可能会推后。如果您可以接受预计时间，则无需手动操作。
- 当天自助解封配额为0时，建议增加防护 IP 数量和防护次数，以便足够防御大流量攻击，避免被持续封堵。

## 自助解封操作

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航中，单击解封中心。
- 在解封操作页面，找到状态为“自动解封中”的防护 IP，单击解封。

## 解封操作记录

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航中，选择解封中心 > 解封记录。
- 在解封记录页面，根据时间范围筛选，可查看所有解封操作记录，包括自动解封、自助解封等操作记录。

总封堵次数	当前封堵 IP 数	自助解封已配额	当日剩余配额	自助解封次数	自动解封次数
144 次	0 次	3 次	3 次	16 次	83 次

封堵列表

筛选记录

近24小时 | 近7天 | 近30天 | **近90天** | 2023-12-16 00:00 ~ 2024-03-15 23:59

IP	防护类型	封堵时间	实际解封时间	解封操作类型
██████████	DDoS高防IP	2024-01-31 16:50:47	2024-01-31 17:05:48	自助解封
██████████	DDoS高防IP	2024-01-31 13:49:10	2024-01-31 14:04:12	自助解封

# 业务接入

## IP 透明接入

最近更新时间：2024-07-01 11:33:59

### ⚠ 注意：

IP 透明接入为 DDoS 高防包直接绑定云上资产的接入方式，一键接入，配置便捷；如您购买的实例为 DDoS 高防包（企业版），则需要前往 CVM 控制台解绑原公网 IP 并重新绑定 EIP，如您需要对外隐藏源站 IP，请根据业务需要通过高防 IP 的形式选择端口业务或域名业务接入。

## 前提条件

设置防护对象 IP，您需要成功 [购买 DDoS 高防包](#)。

## 操作步骤

1. 登录 [DDoS防护（新版）控制台](#)，在左侧导航中，单击业务接入 > IP 透明接入。
2. 在 IP 透明接入页面，单击开始接入。
3. 在 IP 透明接入页面，选择防护实例。

IP透明接入 X

**注意:** 已配置的防护策略仅对当前绑定的IP生效, 如存在防护策略不适用于当前IP, 请前往修改。

选择防护实例 可搜索IP或名称

选择资源实例 ①

请输入IP或名称 (支持精确搜索, 暂不支持模糊搜索)			Q
<input type="checkbox"/> 资源ID/实例名	IP地址	资源类型	
暂无数据			

共 0 条    10 条 / 页    1 / 1 页

已选择 (0)

资源ID/实例名	IP地址	资源类型
暂无数据		

支持按住 shift 键进行多选

**① 说明:**

- DDoS 高防包如果有 IP 处于封堵状态下, 则不允许用户解绑该 IP。
- 当关联云资产时, 支持批量搜索和选择。
- 当前支持检测 CLB、CVM 产品的销毁状态, 并进行解绑。

4. 单击确定即可。

# 域名接入

最近更新时间：2024-07-01 11:33:59

## ⚠ 注意：

高防资源将提供 CNAME，请将 DNS 解析地址修改为该 CNAME 高防资源。CNAME 解析目的高防 IP 将不定期更换。（不涉及三网资源）

## 接入规则

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击业务接入 > 域名接入。
2. 在域名接入页面，单击开始接入。



业务接入

IP透明接入 端口接入 域名接入 ① IP接入

域名业务接入

如果您的业务为网站类业务，可以通过高防IP 域名业务接入的方式添加转发规则，有效为网站业务抵御DDoS及CC攻击。根据您配置的规则，业务流量会先经过DDoS高防进行清洗，再回源到目标源站服务器，可针对已有规则进行删除或编辑等操作。[查看详情](#)

**开始接入** **批量导入** **批量导出** **批量删除**

3. 在域名业务接入页面，选择关联实例 ID，单击下一步：协议端口。

## ⓘ 说明：

支持多选，多实例同时接入。

## 域名业务接入

X



\* 关联实例ID

可搜索IP、名称或高防资源

4. 选择转发协议，填写业务域名，单击下一步：回源方式。

## 域名业务接入

X



\* 转发协议

 http https

\* 业务域名

域名长度不超过67

推荐开启防护配置  CC防护 + 智能CC防护 ⓘ

5. 选择回源方式，填写源站IP+端口或源站域名。如有备用源站可选中备用源站，添加备用源站及权重，单击下一步：修改 DNS 解析。

**说明：**

备用源站：当源站转发异常会自动切换转发至备用源站。

**域名业务接入**

选择实例 > 协议端口 > 3 回源方式 > 4 修改DNS解析

**回源方式**

**IP回源** (selected) | **域名回源**

回源方式：清洗后的干净业务流量可通过IP、域名两种方式访问源站服务器

**\* 源站IP+端口**

源站IP	源站端口
示例：1.1.1.1, 请根据实际源站填写	示例：80
<b>删除</b>	
<b>+ 添加</b>	

注意：请输入源站IP+端口，最多支持16个

6. 单击完成，接入的规则会出现在域名接入列表中，在接入状态查看是否接入成功。

#### 说明：

- 当因证书问题配置失败时，接入状态右侧会冒泡提醒“因所选证书获取失败，请到 [SSL证书管理](#) 查看详情”。
- 当已经接入成功的域名更新证书时，会产生秒级闪断，如需更新证书，建议低高峰期更新。

## 配置规则

1. 在 [域名接入页面](#)，选择所需规则，单击操作列的配置。

操作	批量导入	批量导出	批量删除	CNAME	通知人
<input type="checkbox"/>	业务域名	转发协议	转发端口	源站IP/站点	关联防护资源 健康检查 会话保持 接入状态 CC防护状态 修改时间 操作
<input type="checkbox"/>	test0229.tencentddos.com	http	80	106.55.58.59.80.175.178.241.90.80	px52oj40.dayugzlb.com 关闭 配置 暂不支持 成功 关闭 配置 2024-02-29 17:00:29 <b>配置 配置</b>
<input type="checkbox"/>	test0229.tencentddos.com	https	443	106.55.58.59.443.175.178.241.90.443	px52oj40.dayugzlb.com 关闭 配置 暂不支持 成功 关闭 配置 2024-02-29 17:05:33 <b>配置 配置</b>

2. 在配置七层转发规则页面，可修改相关参数，单击确定保存。

### 配置七层转发规则

关联高防资源 b [ ] ⓘ 最多可添加 60 条规则，已添加 18 条

域名: [ ] 请输入域名，长度不超过67

协议: http [ ] https [ ] 端口: 80

回源方式: IP回源 [ ] 域名回源 [ ]

源站IP	源站IP	源站端口	
[ ]	[ ]	80	<a href="#">删除</a>
[ ]	[ ]	80	<a href="#">删除</a>
<a href="#">+ 添加</a>			

注意: 请输入源站IP+端口，最多支持16个

## 删除规则

1. 在 [域名接入页面](#)，支持删除单个或批量删除规则。

- 单个: 选择所需规则，单击操作列的删除，弹出删除规则弹窗。

开始输入	批量导入	批量导出	批量删除	CNAME	请输入要查询的
<input type="checkbox"/>	业务域名	转发协议	转发端口	源站IP/站点	关联高防资源 健康检查 会话保持 接入状态 CC防护状态 修改时间 操作
<input type="checkbox"/>	[ ]	http	80	[ ]	关闭 配置 暂不支持 成功 关闭 配置 2024-02-29 17:00:39 <a href="#">删除</a>

- 批量: 选择一个或多个规则，单击批量删除，弹出删除规则弹窗。

开始输入	批量导入	批量导出	批量删除	CNAME	请输入要查询的
<input checked="" type="checkbox"/>	业务域名	转发协议	转发端口	源站IP/站点	关联高防资源 健康检查 会话保持 接入状态 CC防护状态 修改时间 操作
<input checked="" type="checkbox"/>	[ ]	http	80	[ ]	关闭 配置 暂不支持 成功 关闭 配置 2024-02-29 17:00:39 <a href="#">配置</a> <a href="#">删除</a>
<input checked="" type="checkbox"/>	[ ]	https	443	[ ]	关闭 配置 暂不支持 成功 关闭 配置 2024-02-29 17:05:33 <a href="#">配置</a> <a href="#">删除</a>

2. 在删除规则弹窗，单击删除，即可删除所选规则。

# IP 接入

最近更新时间：2024-07-01 11:33:59

## 接入规则

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击业务接入 > IP 接入。
2. 在 IP 接入页面，单击开始接入。



3. 在 IP 接入页面，选择关联 Anycast 高防 IP。

### IP接入

关联Anycast高防IP 可搜索IP或名称 ▾

绑定实例类型  云主机  负载均衡

中国香港 ▾

请输入实例ID或IP信息			
实例ID/名称	可用区	内网IP	已绑定普通公网IP
[REDACTED]	中国香港	[REDACTED]	[REDACTED]
[REDACTED]	中国香港	[REDACTED]	[REDACTED]
[REDACTED]	中国香港	[REDACTED]	[REDACTED]

共 3 条 10 条 / 页 1 / 1 页

## 删除规则

1. 在 IP 接入页面，选择所需规则，单击操作列的删除，弹出删除规则弹窗。

开始接入	Anycast高防IP	防护资源类型	防护资源ID/名称	防护状态	绑定状态	修改时间	操作
bgrp-[REDACTED]	[REDACTED]	云主机	[REDACTED]	运行中	已绑定	2022-12-15 20:22:44	<input type="button" value="删除"/>
bgrp-[REDACTED]	[REDACTED]	云主机	[REDACTED]	运行中	已绑定	2021-11-24 20:58:53	<input type="button" value="删除"/>

2. 在删除规则弹窗，单击删除，即可删除所选规则。

# 端口接入

最近更新时间：2024-07-01 11:33:59

## ⚠ 注意：

高防资源将提供 CNAME，请将 DNS 解析地址修改为该 CNAME 高防资源。CNAME 解析目的高防 IP 将不定期更换。（不涉及三网资源）

## 接入规则

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击业务接入 > 端口接入。
2. 在端口接入页面，单击开始接入。

### 业务接入

IP透明接入    端口接入    域名接入    IP接入  ⓘ

#### 端口业务接入



如果您的业务是非网站业务，如端游、手游、App等客户端应用程序，可通过高防IP端口业务接入的方式添加转发规则，根据您配置的规则，业务流量会先经过DDoS高防进行清洗，再回源到目标源站服务器，可针对已有规则进行删除或编辑等操作，[查看详情](#)

[开始接入](#)

[批量导入](#)

[批量导出](#)

[批量删除](#)

3. 在端口业务接入页，选择关联实例 ID，单击下一步：协议端口。

## ⓘ 说明：

支持多选，多实例同时接入。



4. 选择转发协议，填写转发端口和源站端口，单击下一步：回源方式。

端口业务接入

1 选择实例 > 2 协议端口 > 3 回源方式 > 4 修改DNS解析

This screenshot shows the second step of the port business connection wizard, 'Protocol Port'. The 'Forwarding Protocol' dropdown is highlighted in blue, indicating it is the current configuration point. Below it, there are fields for 'Forwarding Port' (set to '示例：如 80') and 'Source Port' (set to '示例：如 80').

\* 转发协议  TCP  UDP  
\* 转发端口 示例：如 80  
\* 源站端口 示例：如 80

5. 选择回源方式，填写源站IP+端口或源站域名。如有备用源站可选中备用源站，添加备用源站及权重，单击下一步：修改 DNS 解析。

### 端口业务接入

3 回源方式 > 4 修改DNS解析

通过Cname地址  
或通过A记录

用户 安全实例 源站IP 源站服务器

转发端口 转发协议

\* 回源方式

IP回源 域名回源

回源方式：清洗后的干净业务流量可通过IP、域名两种方式访问源站服务器

\* 源站IP+权重

源站IP	权重 ⓘ
示例: 1.1.1.1, 请根据实际源站填写	0~100
删除	
+ 添加	

注意：请输入源站IP+权重，最多支持20个

#### 说明：

- 备用源站：当源站转发异常会自动切换转发至备用源站。
- 在端口业务接入的第二步协议端口。输入转发端口后，会判定此高防IP资源下此端口是否已被占用。若是被占用，无法进入下一步。

6. 单击完成，即可完成接入规则。

## 配置规则

1. 在 端口接入页面，选择所需规则，单击操作列的配置。

开始接入	批量导入	批量导出	批量删除	多个关键字用竖线“ ”分隔					操作
<input type="checkbox"/>	转发协议	转发端口	源站端口	源站	关联高防资源	负载均衡方式	健康检查	会话保持	修改时间
<input type="checkbox"/>	UDP	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	加权轮询	暂不支持	暂不支持	2024-02-29 16:54:14
<input type="checkbox"/>	TCP	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	加权轮询	暂不支持	暂不支持	2024-02-29 16:53:20

2. 在配置四层转发规则页面，可修改相关参数，单击确定保存。

### 配置四层转发规则

**重要提示**  
端口接入方式不支持域名业务CC攻击防护，如果您的业务是网站业务类型请到【域名接入】进行业务接入配置

关联高防资源 bgpip-[REDACTED] / [\(i\)](#)  
最多可添加 60 条规则，已添加 18 条

转发协议 UDP

转发端口 [REDACTED]

源站端口 [REDACTED]

回源方式 IP回源 [\(i\)](#) 域名回源

负载均衡方式 加权轮询

源站IP+权重

源站IP	权重 <a href="#">(i)</a>	操作
[REDACTED]	100	<a href="#">删除</a>
<a href="#">+ 添加</a>		

注意：请输入源站IP+权重，最多支持20个

## 查询规则

在端口接入页面，单击搜索框通过源站 IP/域名、源站端口、关联高防 IP、转发协议、转发端口和关联高防资源 (CNAME) 关键字对规则进行查询。

The screenshot shows the 'Port Access' interface. At the top, there are four buttons: 'Start Access' (blue), 'Batch import', 'Batch export', and 'Batch delete'. Below is a table with columns: 'Forwarding protocol', 'Forwarding port', 'Origin port', 'Origin', 'Associate high defense re...', 'Load balancing mode', and 'Health check'. A red box highlights the search bar 'Real Server IP/Domain Name' and the filter options 'Origin port', 'Anti-DDoS Advanced IP', 'Forwarding protocol', and 'Forwarding port'. To the right, a modal window titled 'Associate multiple keywords with ' shows a list of items: 'Real Server IP/Domain Name', 'Origin port', 'Anti-DDoS Advanced IP', 'Forwarding protocol', 'Forwarding port', and 'Associating Anti-DDoS Pro resources (CNAME)'. The main table lists several rules, each with 'Edit' and 'Delete' links.

## 删除规则

1. 在 [端口接入页面](#)，支持删除单个或批量删除规则。

- 单个：选择所需规则，单击操作列的删除，弹出删除规则弹窗。

The screenshot shows the 'Port Access' interface with a single rule selected for deletion. The 'Batch Delete' button is highlighted with a red box. The rule details are shown in the table: 'Forwarding protocol' (UDP), 'Forwarding port' (80), 'Origin port' (80), 'Origin' (www.example.com), 'Associate high defense resource' (1.1.1.1), 'Load balancing mode' (Weighted round robin), 'Health check' (Disable), 'Session persistence' (暂不支持), and 'Modification time' (2024-02-29 16:54:14). The 'Delete' link in the 'Operation' column is also highlighted with a red box.

- 批量：选择一个或多个规则，单击批量删除，弹出删除规则弹窗。

The screenshot shows the 'Port Access' interface with multiple rules selected for bulk deletion. The 'Batch Delete' button is highlighted with a red box. The selected rules are: 'Forwarding protocol' (UDP), 'Forwarding port' (80), 'Origin port' (80), 'Origin' (www.example.com), 'Associate high defense resource' (1.1.1.1), 'Load balancing mode' (Weighted round robin), 'Health check' (Disable), 'Session persistence' (暂不支持), and 'Modification time' (2024-02-29 16:54:14). The 'Delete' link in the 'Operation' column is highlighted with a red box. Another rule is selected: 'Forwarding protocol' (TCP), 'Forwarding port' (80), 'Origin port' (80), 'Origin' (www.example.com), 'Associate high defense resource' (1.1.1.1), 'Load balancing mode' (Weighted round robin), 'Health check' (Disable), 'Session persistence' (暂不支持), and 'Modification time' (2024-02-29 16:53:20).

2. 在删除规则弹窗，单击删除，即可删除所选规则。

# 配置会话保持

最近更新时间：2024-07-01 11:33:59

DDoS 高防 IP 非网站业务防护提供基于 IP 地址的会话保持，支持将来自同一 IP 地址的请求转发到同一台后端服务器进行处理。

四层转发场景支持简单会话保持能力，会话保持时间可设为30秒 – 3600秒中的任意整数值，若超过该时间阈值，且会话中无新的请求，则自动断开连接。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧目录中，单击业务接入 > 端口接入。
2. 在端口接入页签，选择目的 DDoS 高防 IP 实例和相应规则，单击其会话保持列下的编辑。

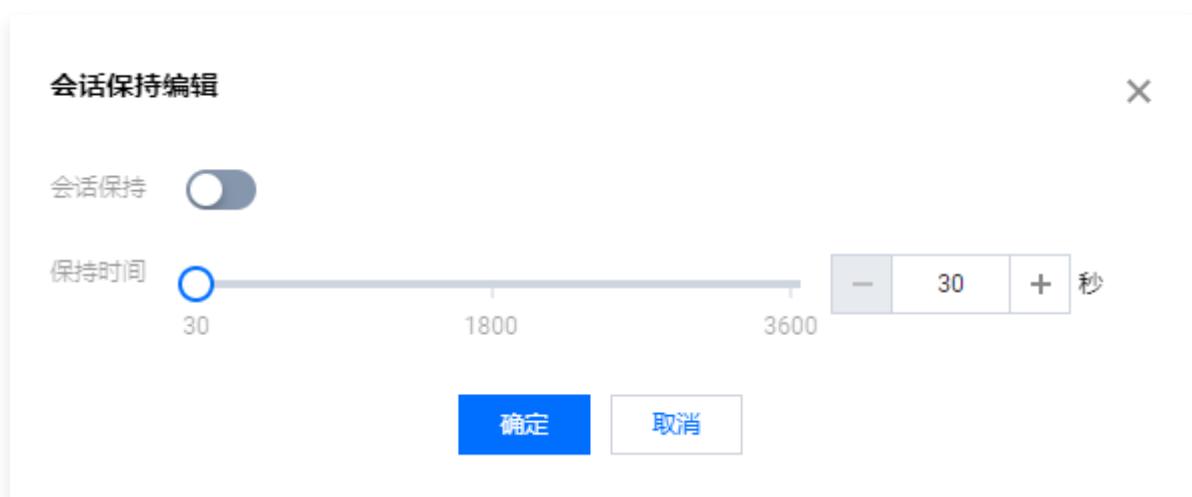
The screenshot shows a table with columns for protocol (转发协议), port (转发端口), source port (源站端口), destination (源站), associated high-defense resources (关联高防资源), load balancing method (负载均衡方式), health check (健康检查), session persistence (会话保持), and last modified time (修改时间). Two rows are visible: one for UDP and one for TCP. The session persistence column for UDP shows '关闭' (disabled) with a red box around it, while for TCP it shows '关闭 (编辑)' with a red box around the edit link.

转发协议	转发端口	源站端口	源站	关联高防资源	负载均衡方式	健康检查	会话保持	修改时间
UDP	1	1	1	1	加权轮询	关闭 (编辑)	关闭 (编辑)	2024-01-04 15:48:09
TCP	1	1	1	1	加权轮询	关闭 (编辑)	关闭 (编辑)	2024-01-04 15:48:13

3. 在会话保持编辑页面，设置保持时间，单击确定即可。

### 说明：

默认关闭会话保持，在设置保持时间时，建议使用默认值。



# 配置健康检查

最近更新时间：2024-07-01 11:33:59

## 应用场景

DDoS 高防 IP 通过健康检查帮助用户自动识别后端服务器的运行状况，自动隔离异常的服务器，以此降低了后端服务器异常对整体业务可用性的影响。

### 四层业务健康检查

DDoS 高防 IP 四层业务防护的健康检查机制，由高防集群节点向配置中指定的服务器端口发起访问请求，如果端口访问正常则视为后端服务器运行正常，否则视为后端服务器运行异常。

在 TCP 协议下，探测端口能否连接。在 UDP 协议下，使用 ping 进行可达性检查。

### 七层业务健康检查

DDoS 高防 IP 七层业务防护的健康检查机制，由高防转发集群向后端服务器发送 HTTP 请求的方式来检查后端服务，高防系统根据 HTTP 返回状态码来判断服务是否正常。

用户可以自定义设置响应代码所代表的状态。假定在某场景下，HTTP 返回值为 http\_1xx、http\_2xx、http\_3xx、http\_4xx 和 http\_5xx，用户可以根据业务需要勾选 http\_1xx 及 http\_2xx 为服务正常状态，则返回 http\_3xx 至 http\_5xx 的值则代表异常状态。

#### ⚠ 注意：

配置转发规则时，如果单条规则中仅配置1个源站 IP，健康检查功能将不开启，该功能适合多源站 IP 的情况下开启。

## 操作步骤

### 四层业务健康检查配置

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击业务接入 > 端口接入。
- 在端口接入页签，选择目的 DDoS 高防 IP 实例和相应规则，单击其健康检查列下的编辑。

开始接入	批量导入	批量导出	批量删除	多个关键字用竖线 “ ” 分隔					Q
转发协议	转发端口	源站端口	源站	关联高防资源	负载均衡方式	健康检查	会话保持	修改时间	操作
<input type="checkbox"/>	TCP	██████	██████	██████	加权轮询	关闭 <a href="#">编辑</a>	开启 <a href="#">编辑</a>	2024-01-12 16:24:07	<a href="#">配置</a> <a href="#">删除</a>
<input type="checkbox"/>	UDP	██████	██████	██████	加权轮询	关闭 <a href="#">编辑</a>	关闭 <a href="#">编辑</a>	2024-01-10 21:25:11	<a href="#">配置</a> <a href="#">删除</a>

- 在健康检查编辑页面，单击显示高级选项，设置配置项后，单击确定即可。

**说明:**

- 默认开启健康检查。在配置健康检查时，建议使用默认值。
- 在 TCP 协议下，探测端口能否连接。在 UDP 协议下，使用 ping 进行可达性检查。

**健康检查编辑** i

健康检查



隐藏高级选项

检查方式

 被动检查

检测间隔



30

150

300



60



秒

不健康阈值



3

5

20



5



次

不健康屏蔽时间



360

600

1800



600



秒

确定

取消

**七层业务健康检查配置**

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击业务接入 > 域名接入。
- 在域名接入页签，选择目的 DDoS 高防 IP 实例和相应规则，单击其健康检查列下的配置。

开始接入	批量导入	批量导出	批量删除	CNAME	请输入要查询的内容
<input type="checkbox"/> 业务域名	转发协议	转发端口	源站IP/站点	关联高防资源	健康检查 <span style="color: #0070C0;">关闭 配置</span>
<input type="checkbox"/> http	http	80	源站IP/站点	关闭 <span style="color: #0070C0;">配置</span>	暂不支持 成功 关闭 配置 2024-02-29 17:00:39 配置 删除
<input type="checkbox"/> https	https	443	源站IP/站点	关闭 <span style="color: #0070C0;">配置</span>	暂不支持 成功 关闭 配置 2024-02-29 17:05:33 配置 删除

- 在健康检查编辑页面，单击显示高级选项，设置配置项后，单击确定即可。

**说明:**

默认关闭健康检查。

健康检查编辑 

健康检查

隐藏高级选项 

检查方式

 被动检查

检测间隔

30

150

300



60



秒

不健康阈值

3

5

20



5



次

不健康屏蔽时间

360

600

1800



600



秒

确定

取消

## 配置项说明

## 四层健康检查

配置项	说明
响应超时	每次健康检查响应的最大超时时间。如果后端服务器在指定的时间内没有正确响应，则判定为健康检查失败。
检测间隔	进行健康检查的时间间隔。
不健康阈值	在健康检查状态为成功时，连续 n 次（n 为填写的数值）收到健康检查失败状态，则识别为不健康，控制台显示异常。
健康阈值	在健康检查状态为失败时，连续 n 次（n 为填写的数值）收到健康检查成功状态，则识别为健康，控制台无显示。

## 七层健康检查

配置项	说明
检测间隔	进行健康检查的时间间隔，默认为15秒。

不健康阈值	在健康检查状态为成功时，连续 n 次（n 为填写的数值）收到健康检查失败状态，则识别为不健康，控制台显示异常。
健康阈值	在健康检查状态为失败时，连续 n 次（n 为填写的数值）收到健康检查成功状态，则识别为健康，控制台无显示。
HTTP 请求方式和检查路径 URL	<p>默认使用 HEAD 方法，服务器仅返回响应消息报文头。使用 GET 方法，服务器返回完整的响应消息。对应后端服务器需要支持 HEAD 和 GET。</p> <ul style="list-style-type: none"><li>如果用来进行健康检查的页面并不是应用服务器的缺省首页，用户需要指定具体的检查路径。</li><li>如果对 HTTP HEAD 请求限定了 host 字段的参数，用户需要指定检查路径，即用于健康检查页面文件的 URI。</li></ul>
HTTP 状态码检测	判断健康检查是否正常的 HTTP 状态码。默认情况或不做任何选择时，该值为 http_1xx、http_2xx、http_3xx 和 http_4xx，如果 HTTP 返回状态码非默认状态值，则识别为不健康，支持修改。

# 智能调度

最近更新时间：2024-07-01 11:33:59

## 应用场景

一般每个账号下可能拥有多个高防实例，且每个高防实例至少拥有一条高防线路，因此每个账号下可能会存在多条高防线路。当将业务添加至高防实例进行防护后，表示您已经为该业务配置一条高防线路作为防护线路。若您的业务配置存在多条高防线路作为防护线路，您需要考虑该业务流量的最佳调度方式，即如何将业务流量调度到最优的高防线路进行防护，保证业务访问速度和高可用性。

目前 DDoS 防护服务提供优先级方式的 CNAME 智能调度功能，您可以根据实际需要，勾选高防实例并设置高防线路的优先级。

### 说明：

- 支持设置解析的高防实例有 DDoS 高防包、DDoS 高防 IP，其中 DDoS 高防 IP 包括 BGP 高防 IP、电信高防 IP、联通高防 IP 和移动高防 IP。
- 如果只有一条高防线路时不需要智能调度。

## 优先级调度方式

指针对所有的 DNS 请求均以优先级最高的高防线路进行响应，即所有访问流量被调度至当前优先级最高的高防线路。您可以编辑高防线路的优先级，默认优先级为100，优先级的值越小，则表示该高防线路优先级越高。具体调度规则如下：

- 如果业务配置的高防实例包含多条不同高防线路，且优先级相同时，则按照 DNS 请求的运营商来源进行响应。当其中某条高防线路遭遇封堵后，将按 BGP > 电信 > 联通 > 移动 > 境外（包括中国香港、中国台湾）的线路顺序进行调度。
- 如果同一优先级的高防线路均遭遇封堵后，访问流量将自动调度到当前可用的优先级次高的高防线路。

### 注意：

若当前无次高优先级的高防线路可用，则无法进行自动调度，业务访问将会中断。

- 如果业务配置的高防实例，包含多条相同高防线路，且优先级相同时，则按负载均衡方式进行调度，将访问流量平均分发至这些相同运营商的高防线路上进行处理。

## 示例

假设您拥有高防实例：BGP 高防 IP 1.1.1.1 和 1.1.1.2、电信高防 IP 2.2.2.2、联通高防 IP 3.3.3.3，其中 1.1.1.1、2.2.2.2 和 3.3.3.3 的优先级都为1，1.1.1.2 的优先级为2。正常情况下，所有流量被调度至当前优先级为1的一组高防线路进行分发处理，因此来自联通的流量调度到3.3.3.3进行处理，来自电信的流量调度到 2.2.2.2 进行处理，来自其他运营商的流量调度到1.1.1.1进行处理。当1.1.1.1进入封堵时，该 IP 下的访问流量将自动调度到2.2.2.2进行处理，当

1.1.1.1和3.3.3.3都被封堵时，则原本调度至1.1.1.1和3.3.3.3的访问流量，都将分发至2.2.2.2进行处理，当该组高防线路全部进入封堵时，流量将被调度至1.1.1.2进行处理。

## 前提条件

- 在开启智能调度前，请将需要防护的业务接入高防实例进行防护。

### 说明:

- 若您需要将防护的云上产品 IP 添加至已购买的高防包实例，请参见 DDoS 高防包 [快速入门](#)。
- 若您需要将四层或七层业务添加至已购买的 DDoS 高防 IP 实例，请参见 DDoS 高防 IP [端口接入](#) 或 [域名接入](#)。

- 在修改 DNS 解析前，您需要成功购买域名解析产品，例如腾讯云的 DNS 解析 DNSPod。

## 设置路线优先级

请参考以下步骤，按照设想的调度方案为您的高防实例设置优先级：

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击智能调度。
- 在智能调度页面，单击新建调度，系统自动生成一个 CNAME 记录。

名称	CNAME	解析状态	关联防护实例	调度模式	最后修改时间	操作
未命名	██████████	• 正在运行	1个关联资源 ①	定向	2024-04-22 14:51:11	<a href="#">编辑</a> <a href="#">删除</a>
未命名	██████████	• 正在运行	2个关联资源 ①	优先级	2023-10-09 19:02:23	<a href="#">编辑</a> <a href="#">删除</a>

- 在新建智能调度页面，TTL 值默认60秒，取值范围为1（秒） – 3600（秒），调度模式默认优先级。回切时间为，当多个资源发生联动时，触发回切流程的等待时间。考虑封堵解除等待时间以及避免频繁触发联动切换，最短时间为10分钟。默认推荐设置为60分钟。

X

## 新建智能调度

名称 未命名 CNAME TTL值 60 秒 模式   优先级模式  定向模式回切时间  60 联动资源  [添加高防资源IP](#) [添加非高防资源IP](#)

## IPv4

高防资源	IP协议	优先级	线路	地区	运行状态	域名解析	操作
暂无数据							

## IPv6

高防资源	IP协议	优先级	线路	地区	运行状态	域名解析	操作
暂无数据							

 确定 取消

4. 在新建智能调度页面，分为优先级模式和定向模式，不同模式操作如下所示：

4.1 优先级模式：以优先级的方式设置（通过数值的方式），提供资源之间的调度。

4.1.1 单击[添加高防资源 IP](#)，勾选需要设置智能调度的高防实例及 IP，单击确定。

## 添加高防实例

选择实例类型 高防包

选择资源实例

已选择 (0)

请输入实例ID/资源IP		
实例ID/实例名	绑定资源	实例类型
<input type="checkbox"/> [REDACTED]	[REDACTED]	高防包
<input type="checkbox"/> [REDACTED]	[REDACTED]	高防包
<input type="checkbox"/> [REDACTED]	[REDACTED]	高防包
<input type="checkbox"/> [REDACTED]	[REDACTED]	高防包
<input type="checkbox"/> [REDACTED]	[REDACTED]	高防包

实例ID/实例名	绑定资源	实例类型

支持按住 shift 键进行多选

确定

取消

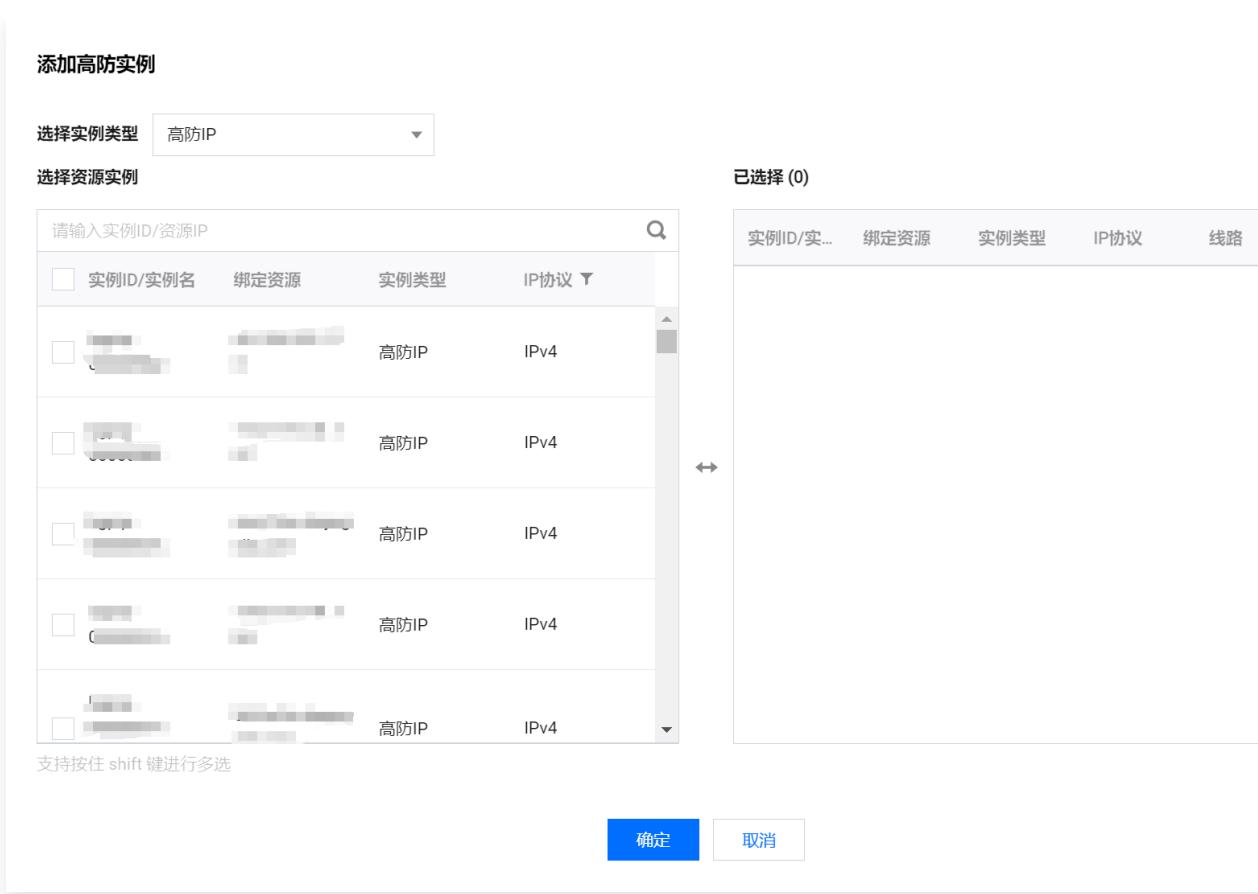
4.1.2 选择高防 IP 实例后，实例的高防线路默认开启域名解析，再为其设置优先级。

IPv4

高防资源	IP协议	优先级	线路	地区	运行状态	域名解析	
[REDACTED]	IPv4	100 	境外	中国香港	运行中 		

4.2 定向模式：通过定向模式，指定资源间的调度关系。

4.2.1 单击添加高防资源 IP，勾选需要设置智能调度的高防实例及 IP，并选择需要的线路，单击确定。



4.2.2 在新建智能调度页面，看到选择调度的资源，单击配置联动资源。

IPv4				
高防资源	线路类型	运行状态	联动资源数	操作
高防IP	默认	运行中	0	<a href="#">配置联动资源</a> <a href="#">解除绑定</a>
高防IP	默认	运行中	0	<a href="#">配置联动资源</a> <a href="#">解除绑定</a>

4.2.3 在联动资源管理页，单击添加资源，输入联动 IP，并选择自相应线路，单击确认，即可配置指定资源间的调度关系。

## 联动资源管理

高防资源信息

线路

默认

联动资源 (i)

+添加资源

资源记录

线路选择

### 示例

例如，您想要将业务流量先调度到 BGP 高防线路，当 BGP 高防线路被攻击遭到封堵后，将流量自动调度到电信高防线路。如果电信高防线路也被封堵，则将流量调度到联通高防线路。当 BGP 高防线路的封堵解除后，流量将自动恢复调度至 BGP 高防线路。

优先级设置方式：您可以将防护业务的高防实例中属于 BGP 高防线路的优先级设置成1、电信高防线路的优先级设置成2、联通高防 IP 线路的优先级不变，即可满足上述调度方案。

高防资源	IP协议	优先级	线路	地区	运行状态	域名解析	操作
...	IPv4	100	BGP	广州	运行中		解除绑定
...	IPv4	100	境外	中国香港	运行中		解除绑定

如果您暂时不希望联通高防 IP 线路加入流量调度机制，单击 关闭域名解析即可，后面再根据需要重新开启域名解析并设置优先级。若想从当前调度机制中剔除该线路，可直接找到该线路对应实例所在行，单击解除绑定即可。

### 修改 DNS 解析

使用 CNAME 智能调度前，建议您将业务域名 DNS 的 CNAME 记录，修改为 DDoS 防护智能调度系统自动生成的 CNAME，使所有用户访问业务网站的流量都牵引至高防系统。

# 防护配置

## DDoS 防护

### DDoS 防护等级

最近更新时间：2024-07-01 11:33:59

## 应用场景

DDoS 防护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：

防护等级	防护操作	描述
宽松	<ul style="list-style-type: none"><li>过滤明确攻击特征的 SYN、ACK 数据包。</li><li>过滤不符合协议规范的 TCP、UDP、ICMP 数据包。</li><li>过滤具有明确攻击特征的 UDP 数据包。</li></ul>	<ul style="list-style-type: none"><li>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。</li><li>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。</li></ul>
适中	<ul style="list-style-type: none"><li>过滤明确攻击特征的 SYN、ACK 数据包。</li><li>过滤不符合协议规范的 TCP、UDP、ICMP 数据包。</li><li>过滤具有明确攻击特征的 UDP 数据包。</li><li>过滤常见基于 UDP 的攻击数据包。</li><li>对部分访问源 IP 进行主动验证。</li></ul>	<ul style="list-style-type: none"><li>清洗策略适配绝大多数业务，可有效防护常见攻击。</li><li>默认为适中模式。</li></ul>
严格	<ul style="list-style-type: none"><li>过滤明确攻击特征的 SYN、ACK 数据包。</li><li>过滤不符合协议规范的 TCP、UDP、ICMP 数据包。</li><li>严格检查过滤具有明确攻击特征的 UDP 数据包和基于 UDP 的攻击数据包。</li><li>对部分访问源 IP 进行主动验证。</li><li>过滤 ICMP 攻击包。</li></ul>	清洗策略相对严格，建议在正常模式出现攻击透传时使用。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 DDoS 防护。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防 IP 的 ID，如"bgp-00xxxxxx"。



3. 在 DDoS 防护等级卡片中，设置防护等级即可。

# IP 黑白名单

最近更新时间：2024-07-01 11:33:59

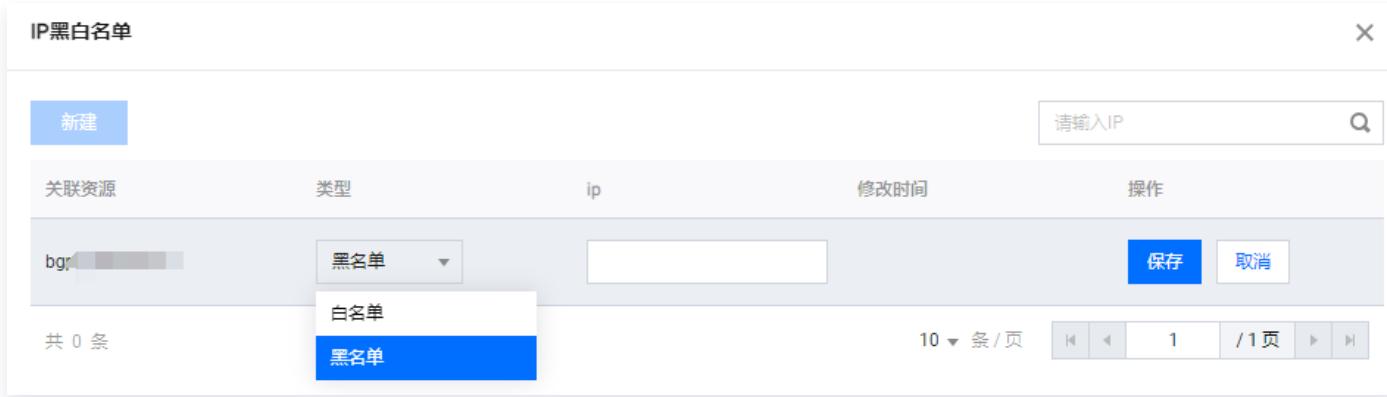
DDoS 高防支持通过配置 IP 黑名单和白名单实现对访问 DDoS 高防的源 IP 封禁或者放行，从而限制访问您业务资源的用户。配置 IP 黑白名单后，当白名单中的 IP 访问时，将被直接放行，不经过任何防护策略过滤。当黑名单中的 IP 访问时，将会被直接阻断。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 DDoS 防护。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"。



3. 在 IP 黑白名单卡片中，单击设置，进入 IP 黑白名单页面。
4. IP 黑白名单页面，单击新建，选择黑白名单类型，填写相关字段，单击保存。



关联资源	类型	ip	修改时间	操作
bgp-00xxxxxx	黑名单			<button>保存</button> <button>取消</button>

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，可以在右侧操作栏中，单击删除，删除 IP 黑白名单规则。

IP黑白名单					X
新建	请输入IP			X	
关联资源	类型	ip	修改时间	操作	
	白名单		2024-03-18 15:34:37	设置	删除
共 1 条		10 ▾ 条 / 页	  1  / 1 页 		

# 端口过滤

最近更新时间：2024-07-01 11:33:59

DDoS 高防支持针对访问 DDoS 高防的源流量，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。端口过滤可以针对访问的源流量精准制定端口设置的防护策略。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 DDoS 防护。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"。



3. 在端口过滤卡片中，单击设置，进入端口过滤页面。
4. 在端口过滤页面，单击新建，创建端口过滤规则，根据需求，选择不同防护动作并填写相关字段，单击保存。

### 说明：

支持选择多个实例资源批量创建，未绑定防护资源的实例，不允许创建规则。



5. 新建完成后，在端口过滤列表，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。

端口过滤						×
新建					请输入IP	🔍
关联资源	协议	源端口范围	目的端口范围	动作	优先级 ①	操作
██████████	所有协议	44-66	77-99	丢弃	10	<span style="border: 2px solid red; padding: 0 2px;">配置</span> <span style="border: 1px solid red; padding: 0 2px;">删除</span>
共 1 条						10 ▾ 条 / 页 <span style="border: 1px solid #ccc; padding: 0 2px;">1</span> / 1 页 <span style="border: 1px solid #ccc; padding: 0 2px;">1</span> <span style="border: 1px solid #ccc; padding: 0 2px;">2</span> <span style="border: 1px solid #ccc; padding: 0 2px;">3</span> <span style="border: 1px solid #ccc; padding: 0 2px;">4</span> <span style="border: 1px solid #ccc; padding: 0 2px;">5</span> <span style="border: 1px solid #ccc; padding: 0 2px;">6</span> <span style="border: 1px solid #ccc; padding: 0 2px;">7</span> <span style="border: 1px solid #ccc; padding: 0 2px;">8</span> <span style="border: 1px solid #ccc; padding: 0 2px;">9</span> <span style="border: 1px solid #ccc; padding: 0 2px;">10</span>

# 协议封禁

最近更新时间：2024-07-01 11:33:59

DDoS 高防支持对访问 DDoS 高防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，配置完成后，当检测到攻击流量有相关访问请求会被直接截断。

由于 UDP 协议的无连接性（如 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。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 DDoS 防护。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防 IP 的 ID，如"bgp-00xxxxxx"。



3. 在协议封禁卡片中，单击设置，进入协议封禁页面。
4. 在协议封禁页面，单击 ，修改协议封禁规则开关。



关联资源	ICMP协议封禁	TCP协议封禁	UDP协议封禁	其它协议封禁
bgp-00xxxxxx				

共 1 条

10 条 / 页

1 / 1 页

# 水印防护

最近更新时间：2024-07-01 11:33:59

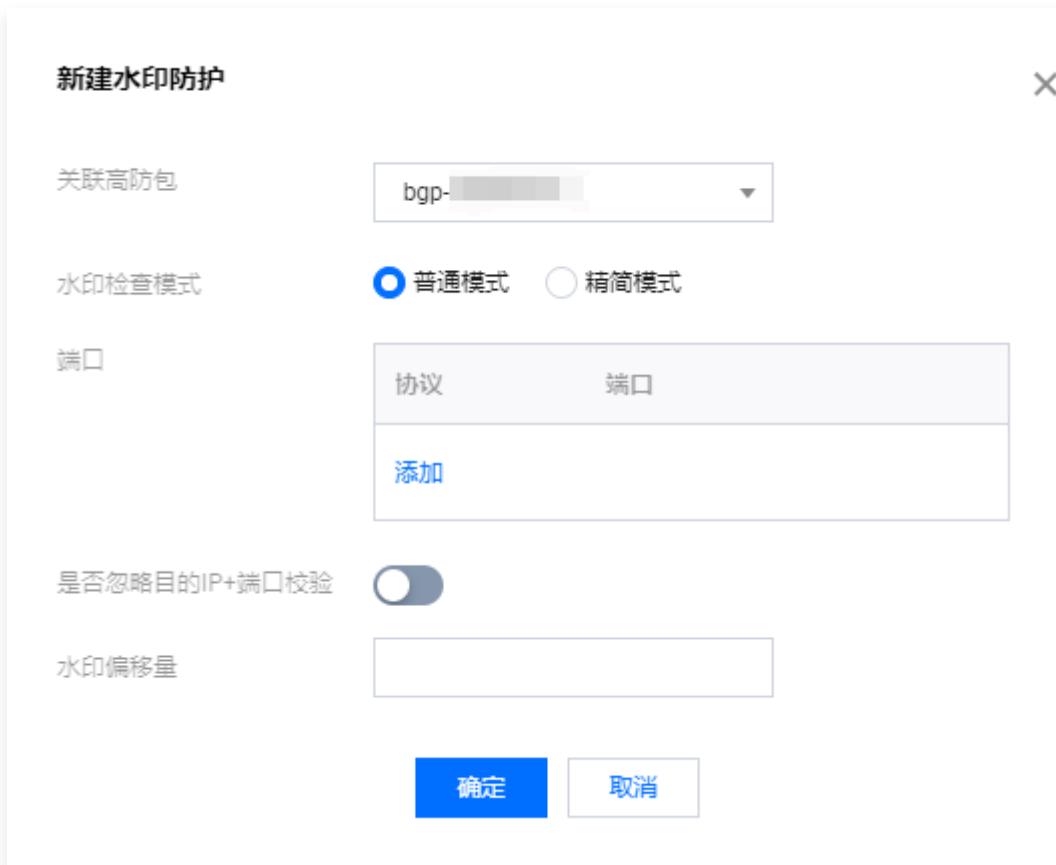
DDoS 高防支持对业务端发出的报文增加水印防护，在您配置的 UDP 和 TCP 报文端口范围内，业务端和 DDoS 防护端共享水印算法和密钥，配置完成后，客户端每个发出的报文都嵌入水印特征，而攻击报文无水印特征，借此甄别出攻击报文并将其丢弃。通过接入水印防护能高效全面防护四层 CC 攻击，如模拟业务报文攻击和重放攻击等。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 DDoS 防护。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"。



3. 在水印防护卡片中，单击设置，进入水印防护页面。
4. 在水印防护页面，单击新建，并填写相关字段，单击确定，创建水印防护规则。



新建水印防护

关联高防包  
bgp-00xxxxxx

水印检查模式  
 普通模式  精简模式

端口

协议	端口
添加	

是否忽略目的IP+端口校验

水印偏移量

**确定** **取消**

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，单击配置密钥，可以查看和配置密钥。

水印防护

新建  ×

关联资源	协议端口	是否忽略目的IP+端口校验	偏移量	检查模式	状态	操作
[REDACTED]	[REDACTED]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	普通模式 <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">删除</a> <a href="#">密钥配置</a>

共 1 条 10 ▾ 条 / 页 1 / 1 页



6. 在配置密钥的界面，用户可以查看或复制密钥，并支持添加或删除密钥，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。

密钥信息 ×

每个业务最多可以使用2个密钥，如果您需要添加新密钥，请先删除旧密钥；当仅有一个生效密钥时，不可删除。

密钥	状态	生成时间	操作
[REDACTED]	已开启	2022-05-12 15:00:00	<a href="#">复制</a> <a href="#">删除</a>

[添加密钥](#) [关闭](#)



# 连续类攻击防护

最近更新时间：2024-07-01 11:33:59

当连接类发起异常，DDoS 高防支持自动发起封禁惩罚策略。在源 IP 最大异常连接数开启防护后，如果 DDoS 高防检测到同一个源 IP，在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。其中封禁时间为15分钟，等封禁时间过后可恢复访问。

## 说明：

- 轻量应用服务器（Lighthouse）定制版不支持 DDoS 防护的自定义防护配置。
- 链接类攻击防护支持以下字段：
  - 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。

## 操作步骤

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 DDoS 防护。
- 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"



- 在连接类攻击防护卡片中，单击设置，进入连接类攻击防护页面。
- 在连接类攻击防护页面，单击新建，并开启连接耗尽防护和异常连接防护，单击确定。

### 配置连接类攻击防护

关联高防IP: bgp

#### 连接耗尽防护

源新建连接限速:

源并发连接限制:

目的新建连接限速:

目的并发连接限制:

#### 异常连接防护 (i)

源IP最大异常连接数:

**确定** **取消**

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。

### 连接类攻击防护

新建

关联资源	源新建连接限速	源并发连接限制	目的新建连接限速	目的并发连接限制	源IP最大异常连接数	操作
bgp	关闭	关闭	关闭	关闭	关闭	<b>配置</b>

共 1 条 10 条 / 页 1 / 1 页

# AI 防护

最近更新时间：2024-07-01 11:33:59

DDoS 高防支持智能 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。

## 说明：

DDoS 高防包（轻量版）不支持 DDoS 防护、CC 防护的自定义防护配置。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 DDoS 防护。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"



3. 在 AI 防护卡片中，单击 ，打开 AI 防护开关。



# 区域封禁

最近更新时间：2024-07-01 11:33:59

DDoS 高防支持对访问 DDoS 高防的源流量，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。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 DDoS 防护。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防 IP 的 ID，如"bgp-00xxxxxx"



3. 区域封禁卡片中，单击设置，进入区域封禁页面。
4. 在区域封禁页面中，单击新建，并选择封禁区域，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。



# IP 端口限速

最近更新时间：2024-07-01 11:33:59

DDoS 高防支持对于业务 IP，基于 IP+端口的维度进行流量访问限速。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 DDoS 防护。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防 IP 的 ID，如"bgp-00xxxxxx"



3. 在 IP 端口限速卡片中，单击设置，进入 IP 端口限速页面。
4. 在 IP 端口限速页面中，单击新建，弹出新建 IP 端口限速弹窗。



关联资源	协议	端口	限速模式	限速速率	操作
...	...	...	单个源IP限速	包速率:3pps 带宽:4bps	配置 删除

5. 在新建 IP 端口限速弹窗中，选择所需协议、端口和限速模式，并输入限速阈值后，单击确定，创建 IP 端口限速规则。

### 新建IP端口限速

关联高防IP: bgpi [▼]

协议:  ALL  TCP  UDP  SMP  自定义

端口: 请填写端口号或端口范围, 以换行符分隔, 最多填写8个  
端口范围格式: 0-65535

限速模式: 单个源IP限速 [▼]

限速阈值 (i):  bps  
 pps

**确定** **取消**

6. 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。

### IP端口限速

**新建**  **Q**

关联资源	协议	端口	限速模式	限速速率	操作
bgpip-0000051h/43.152.80.115	ALL	435	单个源IP限速	包速率:3pps 带宽:4bps	<b>配置</b> <b>删除</b>

# 特征过滤

最近更新时间：2024-07-01 11:33:59

DDoS 高防支持针对 IP, TCP, 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。

## 操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 DDoS 防护。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如“bgp-00xxxxxx”



3. 在特征过滤卡片中，单击设置，进入特征过滤页面。
4. 在特征过滤页面，单击新建，弹出新建特征过滤弹窗。



5. 在新建特征过滤弹窗中，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。

新建特征过滤

关联高防IP: bgf [下拉菜单]

过滤特征:

字段	逻辑	值
添加		

防护动作:

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 (i)

**确定** **取消**

6. 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。

特征过滤

**新建**

ID	关联资源	特征列表	动作	修改时间	操作
[Redacted]	[Redacted]	源端口等于98 目的端口等于8 报文长度等于256	丢弃并拉黑15分钟	2022-06-30 21:39:18	<b>配置</b> <b>删除</b>

# CC 防护

## CC 防护开关及清洗阈值

最近更新时间：2024-07-01 11:33:59

### 防护说明

CC 防护根据访问特征和连接状态判定恶意行为来阻断黑客的攻击。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

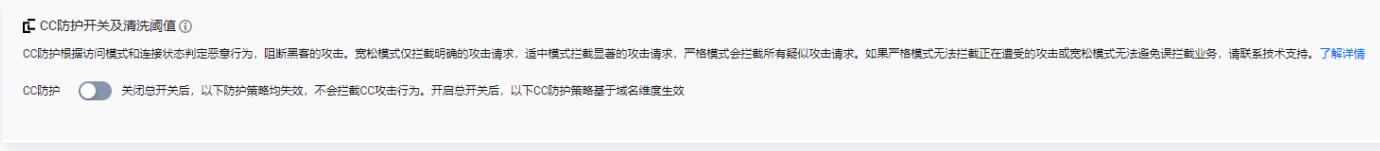
- 您需要已成功购买 DDoS 高防 IP，并设置防护对象。
- CC 防护当前仅支持域名接入的规则生效。

### 操作步骤

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 CC 防护。
- 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



- 在右侧 CC 防护开关及清洗阈值卡片中，单击 开启CC 防护，当防护开启后必须进行清洗阈值设置否则无法开 CC 防护。



#### 说明：

CC 防护开关是控制是否启用 CC 防护的总开关，开启后下方的防护策略才能生效。

- 清洗阈值是高防产品启动清洗动作的阈值，当接入的域名收到的 HTTP 请求超过清洗阈值时，触发 CC 防护。当 CC 防护开启后，业务实例的清洗阈值采用默认值（推荐），并随着接入业务流量的变化规律，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。同时，您也可以根据实际业务情况自定义清洗阈值。

#### 说明：

- 自定义具体的阈值可以设置为正常业务峰值的1.5倍。
- 自定义阈值越小，检测要求越严格。
- 当清洗阈值低于默认值时，可能存在误杀。当清洗阈值高于默认值时，可能存在透传。推荐开启默认清洗阈值。

# 智能 CC 防护

最近更新时间：2024-07-01 11:33:59

开启智能防护后，AI 智能防护基于腾讯云的大数据能力，能够自学习网站业务流量基线，结合算法分析攻击异常，并自动下发精确的防护规则，动态调整业务防护模型，帮助您及时发现并阻断恶意攻击。

## 操作步骤

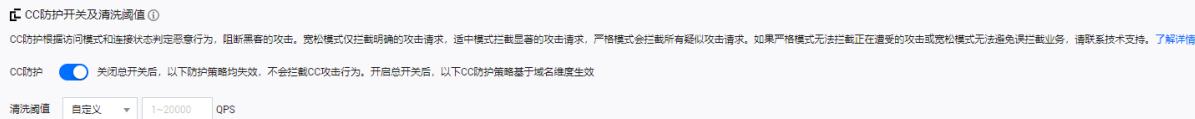
1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 CC 防护。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



3. 在 CC 防护开关及清洗阈值卡片中，单击 开启 CC 防护开关，当防护开启后必须设置清洗阈值，否则无法使用智能 CC 防护。

### 说明：

- 清洗阈值是高防产品启动清洗动作的阈值，当指定域名收到的 HTTP 请求超过阈值时，将触发 CC 防护。
- 当高防包的 IP 为“Web 应用防火墙”的 IP 时，需要先到 [Web 应用防火墙控制台](#) 为此 IP 开启 CC 防护，详情请参见 [CC 防护规则设置](#)。



4. 在智能 CC 防护卡片中，单击 开启智能防护。



5. 单击查看，可查看智能生成的防护规则。若需要调整，请单击右侧查看编辑智能防护规则。

**⚠ 注意：**

- 开启智能 CC 防护后，基于每次攻击，智能防护自动生成防护规则。
- 防护模式：智能防护下发的规则存在单次有效期，单次攻击结束后，防护规则自动失效并清除。
- 观察模式：仅生成规则展示，不生效。

**智能防护**

X

以下智能防护规则基于单次攻击自动生成与生效。智能防护下发的规则存在单次有效期，单次攻击结束后，防护规则自动失效并清除。根据防护需求，可删除以下防护规则。（如有正常业务客户端被拦截，可将之加入 IP 白名单）

防护开关  防护状态 防护模式 ▾

防护模式 观察模式

共 0 条 规则 请输入IP 🔍

域名	匹配条件	处置方式 ▾	生效时间	失效时间	操作
 暂无数据					

共 0 条 10 ▾ 条 / 页 ◀ ◀ 1 / 1 页 ▶ ▶

6. 智能防护规则基于单次攻击自动生成与生效。智能防护下发的规则存在单次有效期，单次攻击结束后，防护规则自动失效并清除。根据防护需求，可单击删除，删除对应防护规则。

# 精准防护

最近更新时间：2024-07-01 11:33:59

## 应用场景

DDoS 高防 IP 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、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。

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
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
Srcip	访问请求的来源网址	等于、不等于

## 操作步骤

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 CC 防护。
- 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



- 在精准防护卡片中，单击设置，进入精准防护页面。
- 在精准防护页面，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。

## 新建精准防护

X

关联高防IP

bgp



域名

请选择



匹配条件

字段

逻辑

值

添加

匹配动作

人机校验

确定

取消

5. 新建完成后，在精准防护列表将新增一条精准防护规则，可以在右侧操作列，单击配置，修改精准防护规则。

## 精准防护

X

新建

ID	关联资源	域名	匹配条件	匹配动作	创建时间	修改时间	操作
			uri 包含 12345	人机校验	2023-08-21 20:15:59	2023-08-21 20:15:59	<span>配置</span> <span>删除</span>

共 1 条

10 条 / 页

◀ ◀ 1 / 1 页 ▶ ▶

# CC 频率限制

最近更新时间：2024-07-01 11:33:59

DDoS 高防 IP 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，具体包括以下模式。

等级分类	说明
宽松等级	<p>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。</p>
适中等级	<p>将启动人机校验算法，访问者通过算法验证后才允许访问源站。 注意：此防护等级只适用于 Web 网站业务，不适用于 API/APP 类业务。如果为 API/APP 类业务，请配置自定义 CC 频率限制策略进行防护。 攻击紧急：当发现源站访问量突然增加，导致源站服务器负载过高或者响应异常时，可选择此等级进行防护。</p>
严格等级	<p>针对全网每一个访问者都会进行人机识别验证，同时验证算法升级，认证过程更加严格，可能会存在一定误判。 注意：此防护等级只适用于 Web 网站业务，不适用于 API/APP 类业务。如果为 API/APP 类业务，请配置自定义 CC 频率限制策略进行防护。</p>
攻击紧急	<p>当发现源站访问量突然增加，导致源站服务器负载过高或者响应异常时，可选择此等级进行防护。</p>
自定义	<p>基于设置的自定义频控规则进行防护，针对特征符合频控规则设置条件的流量进行访问频率限制。</p>

## 操作步骤

- 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 CC 防护。
- 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



- 在 CC 频率限制卡片中，单击 开启 CC 频率限制功能，选择符合业务需求的防护等级，单击设置进入 CC

频率限制列表。



4. 在 CC 频率限制规则列表中，默认展示该域名下全部规则。单击新增规则，创建频率限制规则，填写相关字段。

**⚠ 注意：**

- 当没有创建规则时，自定义等级不允许开启。
- 经过优化后，无需添加首条默认规则；并且支持配置子域名频控限速。

### 自定义规则设置

关联高防IP bgp [i]

域名  [i]

字段	模式	值
添加		

频率限制策略  [i]

检测条件 每  秒 访问  次 [i]

惩罚时间  秒

确定 取消

5. 新建完成后，在 CC 频率限制列表中，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。

规则ID	域名	检测时间(秒)	检测次数	匹配类型	匹配值	执行动作	惩罚时间(秒)	创建时间	修改时间	操作
[REDACTED]	[REDACTED]	60	10	Uri	/	人机校验	120	2022-04-22 17:32:49	2022-04-22 17:32:54	<span style="border: 1px solid red; border-radius: 5px; padding: 2px 5px;">配置</span> <span style="border: 1px solid red; border-radius: 5px; padding: 2px 5px;">删除</span>

# 区域封禁

最近更新时间：2024-07-01 11:33:59

DDoS 高防 IP 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。

## 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。

## 操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 CC 防护。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



3. 在区域封禁卡片中，单击设置，进入区域封禁页面。
4. 在区域封禁页面，单击新建，选择 IP、协议、域名和所封禁的区域，单击确定，创建区域封禁规则。



5. 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。

## 区域封禁

X

新建

关联资源	域名	封禁区域	修改时间	操作
[REDACTED]	[REDACTED]	中国地区	2024-03-18 15:57:55	<a href="#">配置</a> <a href="#">删除</a>

# IP 黑白名单

最近更新时间：2024-07-01 11:33:59

DDoS 高防 IP 支持通过配置 IP 黑名单和白名单，实现对访问 DDoS 高防 IP 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：

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，访问时将被直接阻断。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击 CC 防护。

2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



3. 在 IP 黑白名单卡片中，单击设置，进入 IP 黑白名单页面。

4. 在 IP 黑白名单页面，单击新建，填写相关字段，填写完成后，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，可以在右侧操作栏中，单击删除，删除 IP 黑白名单规则。

IP黑白名单						X
新建		请输入搜索的IP				×
关联资源	域名	IP名单	类型 T	修改时间	操作	
[REDACTED]	[REDACTED]	[REDACTED]	黑名单	2024-03-18 16:01:09	<a href="#">设置</a> <a href="#">删除</a>	
共 1 条						10 ▾ 条 / 页 <a href="#">1</a> <a href="#">/ 1 页</a>

# 安全运营 攻击分析

最近更新时间：2024-07-01 11:33:59

## 查看攻击概况统计

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击攻击分析。
- 在攻击概况统计模块中，可查看当前业务被攻击总次数、总封堵次数、正在攻击中、正在封堵中、攻击带宽峰值、攻击请求峰值。右侧可以查看7天/30天的攻击趋势。



## 查看近期安全事件

- 在事件详情页面，可通过资产ID/IP地址，尽可能详细的展示出此次攻击的细节，主要包括攻击源名称、被攻击资产、IP地址、攻击时间、攻击时长、攻击峰值、防护实例ID、防护类型、攻击状态。

DDoS高防IP	近24小时	近7天	近30天	近90天	2023-12-19 00:00 ~ 2024-03-18 23:59	筛选	请输入资产ID/IP地址	操作	
攻击名称	被攻击资产	IP地址	攻击类型	攻击时间	攻击时长	攻击峰值	防护实例ID	防护类型	
SYNFLOOD恶意攻击	[REDACTED]	[REDACTED]	DDoS攻击	开始: 2024-02-29 17:07:00 结束: 2024-02-29 17:12:00	5分钟	攻击带宽峰值: 92Mbps 攻击包速率峰值: 11073pps	bpo[REDACTED]	DDoS高防IP	已攻击结束 查看详情 攻击包下载
SYNFLOOD恶意攻击	[REDACTED]	[REDACTED]	DDoS攻击	开始: 2024-02-29 16:43:00 结束: 2024-02-29 16:49:00	6分钟	攻击带宽峰值: 94Mbps 攻击包速率峰值: 10946pps	bpo[REDACTED]	DDoS高防IP	已攻击结束 查看详情 攻击包下载

- 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。

### SYNFLOOD恶意攻击

#### 攻击信息

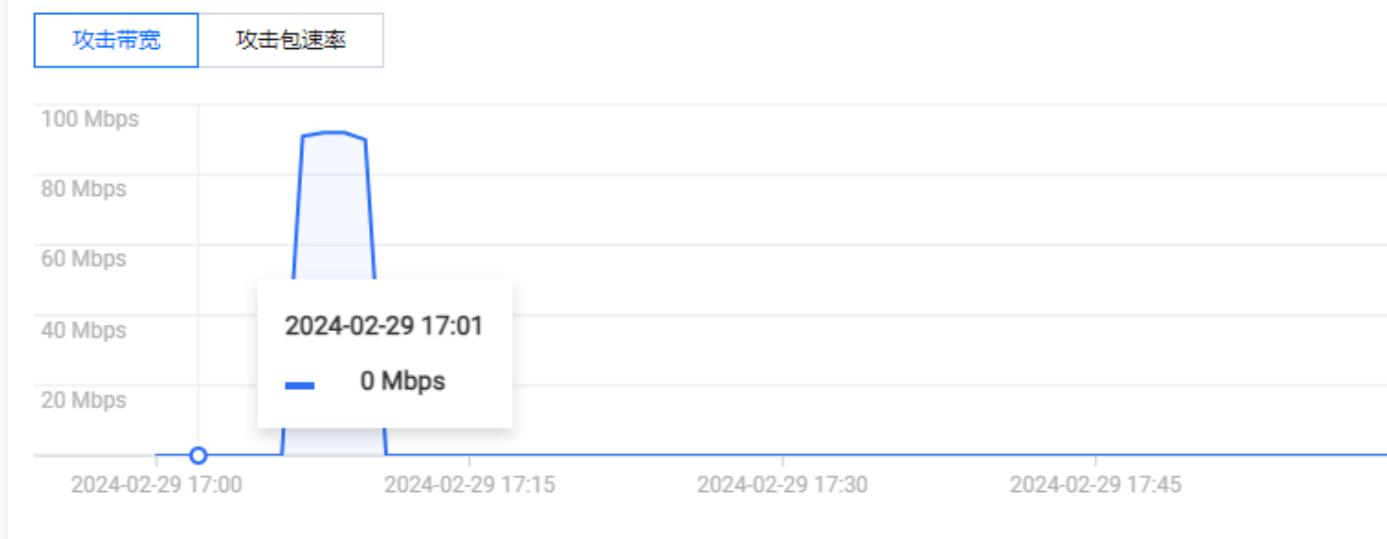
高防资源	[REDACTED]	攻击带宽峰值	92Mbps
状态	• 攻击结束	攻击包速率峰值	11073pps
攻击类型	SYNFLOOD	攻击开始时间	2024-02-29 17:07:00
		攻击结束时间	2024-02-29 17:12:00

- 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。

① 说明：

此处数据为该攻击时间段全量实时数据。



4. 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。

① 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，所选择的高防包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，所选择的高防包实例遭受的各攻击类型总次数占比情况。

5. 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。

**① 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。

**TOP5 攻击源IP ①**

43.157.49.250

170.106.101.94

25106

24894

**TOP5 攻击源地区 ①**

德国

美国

25106

24894

6. 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。

**① 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。

**攻击源信息 ①**

攻击源IP	地区	累计攻击流量	累计攻击包量
[REDACTED]	美国	26.4 MB	24894
[REDACTED]	德国	26.6 MB	25106

# 业务分析

最近更新时间：2024-07-01 11:33:59

DDoS 防护支持查看近90天内的日志业务保护天数、已接入业务数、受攻击业务数，如有需要可通过实例 ID 搜索。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击业务分析。
2. 在业务分析页面，单击立即处理。



3. 在防护待办页面，支持进行如下操作：

- 单击去解封，跳转至解封中心。

防护待办 聚焦DDoS攻击及资产防护核心待办项，助力解决云上恶意流量攻击问题

资源IP/名称	防护实例ID	状态	防护类型	防护状态	操作
1158天 或	gt	封堵中	高防IP	• 防护中	去解封 升级防护

- 单击升级防护，进入升级页面，根据实际防护需求选择“IP 数量”与“防护次数”。

升级 ×

i 高防IP产品在2022年3月24日进行调整。不支持升级至50Gbps规格。点击[查看详情](#)

ID/服务包名: bg [REDACTED]

过期时间: 20 [REDACTED]

保底防护带宽: 20 30 50 60 100 300

业务带宽: - 100 + Mbps

转发规则数: 60 70 80 90 100 150 200 250 300 350

400 450 500

总计费用: [REDACTED] 元

确定 取消

# 操作日志

最近更新时间：2024-07-01 11:33:59

DDoS 防护（新版）控制台支持查看近90天内重要操作的日志，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 防护（新版）控制台](#)，在左侧导航栏中，单击操作日志。
2. 在操作日志页面，支持设置时间范围，查询相关操作记录。

操作时间	RequestID	产品类型	操作内容	操作结果	操作账号	操作
2024-03-06 15:19:10	██████████	DDoS防护	██████████	成功	██████████	<a href="#">展开</a>
2024-03-06 15:18:54	██████████	-	██████████	成功	██████████	<a href="#">展开</a>

# 服务管理

## 解封中心

### 查看封堵时间

最近更新时间：2024-07-01 11:33:59

#### 查看未解封 IP 时间

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击解封中心。
- 在解封中心页面的解封列表页签，选择所需 IP 的所在行，可在“封堵时间”处，查看该 IP 的封堵时间。

总封堵次数	当前封堵IP数	自助解封总配额	当日剩余配额	自助解封次数	自动解封次数
734 次	1 次	3 次	3 次	40 次	195 次

封堵列表		解封记录			
IP	防护类型	防护状态	封堵时间	预计解封时间	状态
[IP]	DDoS基础防护	无	2023-06-08 16:06:00	2023-06-09 17:40:00	自动解封中

- 在解封列表页签，选择所需 IP 的所在行，可在“预计解封时间”处，查看该 IP 的预计解封时间。

总封堵次数	当前封堵IP数	自助解封总配额	当日剩余配额	自助解封次数	自动解封次数
734 次	1 次	3 次	3 次	40 次	195 次

封堵列表		解封记录			
IP	防护类型	防护状态	封堵时间	预计解封时间	状态
[IP]	DDoS基础防护	无	2023-06-08 16:06:00	2023-06-09 17:40:00	自动解封中

#### 查看已解封 IP 时间

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击解封中心 > 解封记录。
- 在解封记录页签，选择所需 IP 的所在行，可在“封堵时间”处，查看该 IP 的封堵时间。

封堵列表		解封记录			
近24小时	近7天	近30天	近90天	2023-12-16 00:00 ~ 2024-03-15 23:59	筛选
IP	防护类型	封堵时间	预计解封时间	实际解封时间	解封操作类型
[IP]	DDoS基础防护	2024-01-31 16:50:47	2024-01-31 17:05:48	2024-01-31 17:05:48	自助解封
[IP]	DDoS基础防护	2024-01-31 13:49:10	2024-01-31 14:04:12	2024-01-31 14:04:12	自助解封

- 在解封操作记录页面，选择所需 IP 的所在行，可在“预计解封时间”处，查看该 IP 的实际解封时间。

时段列表	操作记录			
近24小时				
近7天				
近30天				
近90天	2023-12-16 00:00 ~ 2024-03-15 23:59			
IP	防护类型	时间范围	实际防护时间	操作类型
██████████	DDoS高危IP	2024-01-31 16:50:47	2024-01-31 17:05:48	自助解封
██████████	DDoS高危IP	2024-01-31 13:49:10	2024-01-31 14:04:12	自助解封

# 解除封堵

最近更新时间：2024-07-01 11:33:59

## 自动解封

无需手动操作，等待到达预计解封时间，即可自动解封。可按照以下操作查看预计解封时间：

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击解封中心。
- 在解封中心页面的解封列表页签，选择所需 IP 的所在行，可在“封堵时间”处，查看该 IP 的封堵时间。

## 自助解封次数

使用 DDoS 高防的用户每天将拥有三次自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时，重置自助解封次数，当天未使用的解封次数不会累计到次日。

### 说明：

- 由于解封涉及腾讯云 DDoS 防护后台系统的风控管理策略，解封可能失败（解封失败不会扣减您的剩余解封次数），请您耐心等待一段时间后再次尝试。
- 在执行解封操作前，建议您先查看预计解封时间，预计解封时间受到部分因素影响，可能会推后。如果您可以接受预计时间，则无需手动操作。
- 当天自助解封配额为0时，建议提升保底防护能力或弹性防护能力，以便足够防御大流量攻击，避免被持续封堵。

## 自助解封

- 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击解封中心。
- 在解封中心页面的解封列表页签，找到状态为“自动解封中”的防护 IP，在右侧操作栏中，单击解封。

总封堵次数	当前封堵IP数	自助解封总配额	当日剩余配额	自助解封次数	自动解封次数
734 次	1 次	3 次	3 次	40 次	195 次

封堵列表		解封记录			
IP	防护类型	防护状态	封堵时间	预计解封时间	状态
[Redacted]	DDoS基础防护	无	2023-06-08 16:06:00	2023-06-09 17:40:00	自动解封中

- 在“解除封堵”对话框中，单击确定，您会收到解封成功提示信息，则表示封堵状态已成功解除，您可以刷新页面确认该防护 IP 是否已恢复运行中状态。

## 解封操作记录

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击解封中心 > 解封记录。
2. 在解封记录页签，根据时间范围筛选，可查看所有解封操作记录，包括自动解封、自助解封等操作记录。

封堵列表	解封记录		
<div style="display: flex; justify-content: space-between;"><span>近24小时</span><span>近7天</span><span>近30天</span><span>近90天</span></div> <div style="display: flex; justify-content: space-between; font-size: small;">2023-12-16 00:00 ~ 2024-03-15 23:59</div>			
IP	防护类型	封堵时间	实际解封时间
192.168.1.1	DDoS高防IP	2024-01-31 16:50:47	2024-01-31 17:05:48
192.168.1.2	DDoS高防IP	2024-01-31 13:49:10	2024-01-31 14:04:12

# 连接已被封堵的服务器

最近更新时间：2024-07-01 11:33:59

本文档为您介绍如何连接已被封堵的服务器。

## 操作步骤

1. 登录 [云服务器控制台](#)，在左侧导航中，单击实例，进入实例页面。
2. 在实例页面，单击左上角的区域下拉框，切换地域。
3. 在实例页面，单击搜索框，通过“实例名、实例 ID、实例状态”等关键字，查找对应的封堵服务器。
4. 在被封堵服务器所在行，单击登录，弹出登录 Linux 实例弹窗。
5. 在登录 Linux 实例弹窗，选择使用 VNC 登录单击立即登录，即可通过浏览器 VNC 方式连接。

# 告警中心

## 设置安全事件通知

最近更新时间：2024-07-01 11:33:59

当您所接入高防包的防护 IP 受到攻击、受攻击结束、IP 被封堵以及解除封堵时，将以站内信、短信、邮件、微信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。

## 操作步骤

1. 登录 [DDoS 防护（新版）控制台](#)，在左侧导航栏中，单击告警通知。
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 清洗阈值”。



3. 单击功能卡片的高级设置，进入告警配置列表为每个高防包资源设置不同的告警阈值。

○ 单 IP 入流量告警

This screenshot shows the 'Single IP Inbound Traffic Alert' configuration page. It lists several resource instances, each with a checkbox, a 'Bind IP' field, and an 'Inbound Traffic Alert Threshold (Mbps)' field set to 2. There is a 'Modify' button next to each row. A search bar at the top right allows filtering by IP.

○ DDoS 清洗阈值

This screenshot shows the 'DDoS Cleaning Alert' configuration page. It lists three resource instances, each with a checkbox, a 'Bind IP' field, and a 'DDoS Cleaning Threshold (Mbps)' field set to 4 or 2. There is a 'Modify' button next to each row. A search bar at the top right allows filtering by IP.

○ CC清洗流量告警

The screenshot shows a list of CC cleaning alerts. There are two entries:

资源实例	指定IP	CC清洗阈值(cps)	操作
bgp-1	192.168.1.1	2	修改
bgp-2	192.168.1.2	2	修改

A search bar at the top right is set to 'IP'.

# 设置通知方式

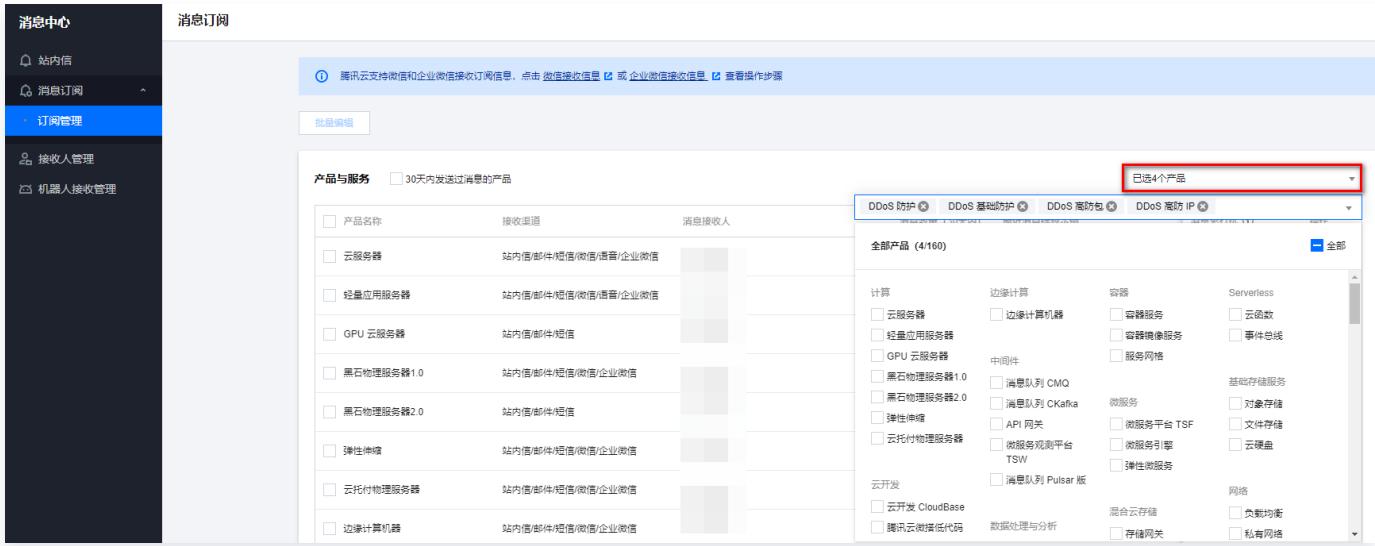
最近更新时间：2024-05-06 16:02:36

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 > 订阅管理，并选择需要接收消息的产品。



3. 在消息订阅页面，选择接收方式，单击编辑。



4. 在订阅编辑弹窗中，进行消息接收人的设置，设置完成后单击确定即可。

## 订阅编辑

① 邮箱、手机、微信未验证的用户将无法接收邮件、短信、语音、微信消息，验证通过并开启对应接收方式后即可接收  
非企业微信子用户无法接收企业微信消息，企业微信子用户且在腾讯云助手应用的成员可见范围内方可接收企业微信消息。

产品名称 DDoS 高防 IP

接收模式  免打扰

开启后，该产品的短信、语音、微信消息将无法接收，站内信、邮件、企业微信消息正常接收（勾选该类消息通道），  
免打扰模式下，无法编辑消息接收人及消息通道

接收渠道  站内信  邮件  短信  微信  语音  企业微信

消息接收人

用户组 IM 应用 机器人

新增消息接收人 [修改接收人联系方式](#)

搜索用户名	用户名称	用户类型	手机号码	邮箱	微信
	<input checked="" type="checkbox"/> 用户名称				
	<input checked="" type="checkbox"/> 主账号	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> 已验证

已选择(1)

接收人名称	接收人类型	操作
	主账号	<a href="#">X</a>

定制化配置产品子消息 点击进入[高级编辑模式](#)

[确定](#) [取消](#)