

DDoS 高防 IP 操作指南

产品文档





【版权声明】

©2013-2024 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】



及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。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

使用限制

防护配置

DDoS 防护

DDoS 防护等级

协议封禁

水印防护

特征过滤

AI 防护

IP 黑白名单

端口过滤

区域封禁

IP 端口限速

连接类攻击防护

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

业务接入

端口接入

域名接入

配置会话保持

实例管理

查看实例信息

设置实例别名与标签

配置智能调度

设置安全事件通知

查看操作日志

封堵相关操作

连接已被封堵的服务器



解除封堵



操作指南 操作概览

最近更新时间:2022-07-06 17:07:39

您在使用 DDoS 高防 IP 时,可能碰到如配置 DDoS 高防 IP 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 的常用操作,供您参考。

概览与限制

- 防护概览
- 使用限制

防护配置

DDoS 防护

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

CC 防护

- CC 防护开关及清洗阈值
- 精准防护
- CC 频率限制
- 区域封禁
- IP 黑白名单



业务接入

- 端口接入
- 域名接入
- 配置会话保持
- 配置健康检查

实例管理

- 查看实例信息
- 设置实例别名与标签
- 修改弹性防护带宽

调度与解封

配置智能调度

操作日志

查看操作日志

封堵相关操作

解除封堵



防护概览

最近更新时间:2022-06-10 14:09:01

防护概览(总览)

全部业务安全状态展示,您可以在 DDoS 防护控制台的防护概览页查看全量实时、业务指标和 DDoS 攻击事件的防护情况,包括基础防护业务、DDoS 高防包防护业务、DDoS 高防 IP 防护业务,便于您分析与溯源。

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。

Anti-DDoS	Overview						
🔝 Overview	Protection Overview	Anti-DDoS Basic	Anti-DDoS Pro	Anti-DDoS Advanced			
Anti-DDoS Basic	Attacks						
Anti-DDoS → Advanced					Attacked IPs	Protected IPs	Blocked IPs
다 Anti-DDoS Pro *				Safe	0	50	0
 Intelligent * Scheduling Policy 				No abnormal traffic detected.	Attacked domain names	Protected domain names	Peak attack bandwidth
Anti-DDoS Pro * (New)					0	30	0_{Mbps}

- 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。

Attacked IPs	Protected IPs	Blocked IPs
0	50	0
Attacked domain names	Protected domain names	Peak attack bandwidth
0	30	O Mbps

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 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。

Recommended Actions								
Upgrade Anti-DDoS for	Anti-DDoS Pro Anti-DDoS Advanced							

查看高防 IP 实例统计

- 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布。

Anti-DDoS Instances					
Service Packs 15	Running Biocked Being stacked Other	15 0 0	Anti-DDus Advanced 41	Running Biocked Being attacked Other	37 0 3 1

查看近期安全事件

- 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。

Recent Events							
Attacked IP	Instance Name	Defense Type 🔻	Start Time	Duration	Attack Status 🔻	Event Type T	Operation
	in the second seco	Anti-DD 1	2022-02-16 04:07:00	2 mins	Attack ends	DDoS Attack	View Details
		Anti-DDo	2022-02-14 17:35:00	2 mins	Attack ends	DDoS Attack	View Details
11.	in the second	Anti-DDo5	2022-02-13 12:05:00	2 mins	Attack ends	DDoS Attack	View Details

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 Atta	ck Details			
Attack Info	ormation			
Attacked IP	11	Attack Bandwidth Peak	0Mbps	
Status	Attack ends	Attack packet rate peak	730pps	
Attack Type	SYNFLOOD	Attack start time	2022-02-16 04:07:00	
		Attack end time	2022-02-16 04:09:00	

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。	

Attack Bandwidth	Attack Packet Rate
10 Mbps	
8 Mbps	
6 Mbps	
4 Mbps	
2 Mbps	
2022-02-16 04:00	2022-02-16 04:

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。

Top 5 Attacking Source IPs		Top 5 Districts Where Attacks Originate	
62.197.136.161	256	Netherlands	512
89.248.163.136	256		

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。



Attack source information			
Attack Source IP	Region	Cumulative attack traffic	Cumulative attack volume
62.1	Netherlands	16.0 MB	256
89.	Netherlands	16.0 MB	256
Total items: 2			1 / 1 page 🕨 🕅

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 防护(新版)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,选择目的地域、线路和高防 IP 实例,查看是否存在攻击。默认展示全量资产的DDoS攻击数据。





DDoS Attack	CC Attack										
S All Regions 🔻	S All Lines 🔻	Please select	Ŧ	Last 1 Hour	Last 6 Hours	Today	Last 7 Days	Last 15 days	Last 30 Days	2022-02-17 16:30 ~ 2022-02-17 17:30	ii i

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和攻击包速率趋势。

S All Regions * S All Lines * Please select	tt	Today Last 7 Days	Last 15 days Last 30 Days 2022-02-17 16:30 ~ 2022-02-17 17:30	
Attack Traffic Bandwidth (traffic surges in	cluded)	Attack Bandwidth Peak	Attack Packet Rate	Attack packet rate peak
10 Mbps 8 Mbps	2022-02-17 16:45		10 pps 8 pps	
6 Mbps 4 Mbps	— 0 Mbps		6 pps 4 pps	
2 Mbps			2 pps	
2022-02-17 16:30 2022-02-1	7 16/45 2022-02-17 17:00 2022-02-17 17:15	2022-02-17 17:30	2022-02-17 1630 2022-02-17 1645 2022-02-17 17:00 2022-02-17 17:15	2022-02-17 17:30

3. 在近期安全事件模块中,可展示所遭受的 DDoS 攻击事件。可单击**查看详情**,可查看该事件的具体详情;可单击 **攻击包下载**,可看到该攻击时间段的攻击采样数据列表。

- 查看详情: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。

DDoS Atta	ck Details			
Attack Info	ormation			
Attacked IP	11	Attack Bandwidth Peak	OMbps	
Status	Attack ends	Attack packet rate peak	730pps	
Attack Type	SYNFLOOD	Attack start time	2022-02-16 04:07:00	
		Attack end time	2022-02-16 04:09:00	

- 攻击包下载: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。



tack Packet List		>
ID	Time	Operation
12993844	2022-01-10 23:37:51	Download
12993866	2022-01-10 23:37:51	Download
Total items: 2	10 🔻 / page 🛛 🖌 🚽	1 / 1 page 🕨 🕨

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,选择目的地域和高防包实例,查看是否存在 CC 攻击。

DDoS Attack	CC Attack									
🔇 All Regions 🔻	Please select	Ŧ	Last 1 Hour	Last 6 Hours	Today	Last 7 Days	Last 15 days	Last 30 Days	2021-11-01 00:00 ~ 2022-02-17 23:59	ii i

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。

CC Attack Trend Unit gps	Attack Request Peak 9765 gps	CC Attack Trend Unit: Times	Total Request Peak 4422201 times
10,000		5,000,000 4,000,000 3,000,000	
4000 2,000 2022-01-16 00:00 2022-01-24 00:00 2022-01-30 00:00 2022-02-05 00:00 2022	-02-11 00:00 2022-02-17 00:00	2,000,000 1,000,000 2022,01.18 00:00 2022,01.24 00:00 2022,01.30 00 2022,01.30 00 2020,000 2020,000 2020,000 2020,000 2020,000 2020,000 2020,000 2020	

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。

Recent Events								
Instance ID	Attacked Domain Name	Attacked URI	Attacked IP	Attack Source	Start Time	Duration	Attack Status T	Operation
bgpi					2022+02+17 15:51:00	1 mins	Attack ends	View Details
bgpl					2022-02-17 13:37:00	1 mins	Attack ends	View Details
bgi				100 C	2022-02-17 12:41:00	1 mins	Attack ends	View Details

查看业务流量情况

- 1. 登录 DDoS 防护(新版)控制台,在左侧导航栏中,单击DDoS 高防 IP > 业务流量。
- 2. 在业务流量页面,设置查询时间范围,选择目的地域、线路和高防 IP 实例,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天以内的业务流量信息及 DDoS 攻击事件。

Last 1 Hour	Last 6 Hours	Today	Last 7 Days	Last 15 days	Last 30 Days	2022-04-28	8 13:15 ~ 2022-04-28 14:15	; 🗖	Φ
S All Regions	All Lines 🔻	Please se	elect			• (i)			
							_	_	
								0	

3. 在业务流量页面,可查看该时间范围内所选择的高防 IP 下域名业务流量情况,入/出业务流量带宽趋势、入/出业务包速率的趋势及活跃连接数和新建连接数的趋势。同时,还可以查看该时间范围内的业务带宽峰值、业务连接数峰值和业务请求峰值。

- 活跃连接数:当前时间所有 established 状态的 TCP 连接数。
- 新建连接数:客户端每秒内新增的与高防 IP 建立通信的 TCP 连接数。



使用限制

最近更新时间:2023-05-09 16:59:58

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。



防护配置 DDoS 防护 DDoS 防护等级

最近更新时间:2022-04-01 09:42:11

本文档将为您介绍针对 DDoS 攻击, DDoS 高防 IP 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:

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。
适中	 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。 过滤常见基于 UDP 的攻击数据包。 对部分访问源 IP 进行主动验证。 	 清洗策略适配绝大多数业务,可有效防护常见攻击。 默认为适中模式。
严格	 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。 过滤常见基于 UDP 的攻击数据包。 	清洗策略相对严格,建议在正常模式出现攻击透传 时使用。



- 对部分访问源 IP 进行主动验证。
- 过滤 ICMP 攻击包。
- 过滤常见的 UDP 攻击数据包。
- UDP 数据包严格检查。

说明:

- 如果您的业务需要使用 UDP, 建议您 联系销售 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,并设置防护对象。

操作步骤

- 1. 登录 DDoS 高防 IP(新版)管理控制台,在左侧导航中,单击【防护配置】。
- 2. 在左边的列表选中高防 IP 的 ID 或端口, 如"212.64.xx.xx bgpip-000002jt"或 "119.28.xx.xx bgpip-000002ju"> "tcp:8000"。
- 3. 在右侧"DDoS 防护等级"卡片中,设置"防护等级"与"清洗阈值"。

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。

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。





协议封禁

最近更新时间:2023-04-28 16:48:50

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

您需要已成功购买 DDoS 高防 IP,并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台,在左侧导航中,单击防护配置 > DDoS 防护。

2. 在 DDoS 防护页面的左侧,选中高防 IP 的 ID,如"bgpip-xxxxx"。

DDoS Protection Lev Anti-DDoS collects and a In Loose Mode, only cont blocked. If attack message	Domain name protection
Strict Medium	vel analysis the characteristics of history attacks, blocks firmed attack messages are blocked. In Medium mo ges failed to be blocked in the Strict mode, or the no Loose



3. 在协议封禁卡片中,单击**设置**,进入协议封禁页面。

IP Biocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.	Port Filtering Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Configured 4 blocklists, 1 allowlists Set	Configured 1 rules Set
Block by protocol Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.	Watermark Protection The application end and Anti-DDoS share the same watermark algorithm and key. In this case, every message sent out from the client is embedded with the watermark, so as to defense layer-4 CC attacks, such as
Configured 1 rules Set	• Enabled 1 rules Set

4. 在协议封禁页面,单击**新建**。





5. 在新建协议封禁弹窗中,单击开启所需协议后,单击确定,创建协议封禁规则。





6. 新建完成后,协议封禁列表将新增一条协议封禁规则,单击,修改

,修改协议封禁规则开关。

← Block by protocol					
Create					Enter IP Q
Associated Resource	Block ICMP Protocol	Block TCP Protocol	Block UDP Protocol	Block other protocols	Operation
bgpip-000002hl/119.28.217.238	Close	Enable	Enable	Enable	Configuration
Total items: 1				10 💌 / page	H A 1 /1 page H



水印防护

最近更新时间:2022-04-28 11:29:57

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

您需要已成功购买 DDoS 高防 IP,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 控制台,在左侧导航中,单击防护配置 > DDoS 防护。
- 2. 在 DDoS 防护页面的左侧,选中高防IP的 ID,如"bgpip-xxxxx"。

IP 💌	Q	IP/Port Protection	Domain name protection	
000488				
		DDoS Protection Anti-DDoS collects an In Loose Mode, only of blocked. If attack mes Strict Mediu	Level d analysis the characteristics of h confirmed attack messages are bl sages failed to be blocked in the um Loose	iistory attacks, blocks ocked. In Medium mc Strict mode, or the ni



3. 在水印防护卡片中,单击**设置**,进入水印防护页面。

IP Blocklist/Allowlist	Port Filtering
Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.	Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Configured 4 blocklists, 1 allowlists Set	Configured 1 rules Set
Block by protocol	Watermark Protection
Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.	The application end and Anti-DDoS share the same watermark algorithm and key. In this case, every message sent out from the client is embedded with the watermark, so as to defense layer-4 CC attacks, such as
Configured 1 rules Set	Enabled 1 rules Set

- 4. 在水印防护页面,单击新建。
- 5. 在新建水印防护弹窗中,填写相关字段,单击确定,创建水印防护规则。

Associate Anti-DDoS Advanced	bgpip-00000488 😵	
Watermark Check Mode	O Normal O Compact	
Port	Protocol Port	
	Add	
Watermark offset		

6. 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。



Watermark Protect	tion				×
Create				Enter IP	Q
Associated Reso	Protocol Port	Offset	Check Mode	Status	Operation
	Т	1	Normal		Delete Key Configuration
Total items: 1			10 💌 / page	.⊲	/ 1 page 🕨 🕨

7. 在配置密钥的界面,用户可以查看或复制密钥。

÷	Watermark Protection					
	Create				Enter IP	Q
	Associated Resource	Protocol port	Status	Operation		
	bgpip-000002hl/119.28.217.238	TCP-80	Run Now	Delete Key Con	figuration	
	Total items: 1			10 🔻 / page	Image Image	н

8. 在配置密钥界面,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。

y information				
Each application can have up to 2 keys. To add	a new key, please delete th	e old key first. When th	ere is only on valid key, it cann	ot be deleted.
ley		Status	Generation Time	Operation
26a8365c2c203ec-5bba-b26a8365c2c203ece093f42	1bc36e78c12b37e60	Enabled	2020-07-01 22:11:13	O Copy Delete
26a8365c2c203ec-5bba-b26a8365c2c203ec9acbab0	12bc36e78ce329a1db	Enabled	2020-07-01 22:11:16	Copy Delete
	Add Key	Close		
	Add Rey	01036		



特征过滤

最近更新时间:2022-03-11 12:28:20

DDoS 高防支持针对 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,并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台,在左侧导航中,单击防护配置 > DDoS 防护。

2. 在 DDoS 防护页面的左侧,选中高防 IP 的 ID,如"bgpip-xxxxx"。

IP 💌	Q	IP/Port Protection	Domain name protection	
000488				
		DDoS Protection Anti-DDoS collects an In Loose Mode, only o blocked. If attack mes Strict Mediu	Level d analysis the characteristics of his onfirmed attack messages are blo sages failed to be blocked in the S um Loose	story attacks, blocks ocked. In Medium mc Strict mode, or the n



3. 在特征过滤卡片中,单击**设置**,进入特征过滤页面。

Block by location Block requests to access Anti-DDoS Advanced Instances from IP addresses in specified regions.	IP/Port Speed Limit Controls access to the business IP by configuring speed limits on IPs and ports.
Configured 1 rules	et Configured 1 rules Set
Feature Filtering Configure custom blocking policy against specific IP, TCP, UDP message header or payload.	
Configured 2 rules	et

- 4. 在特征过滤页面中,单击**新建**。
- 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。

ssociate Anti-DDoS Advance	bgpip-000002hl 🙁			
ilter feature	Field	Logic	Value	
	Source Port	equals to 🔹	5000	Delete
	Destination por 🔻	equals to 🔹	808	Delete
	Message lengtł 🔻	equals to	1350	Delete
	IP header 🔹	Find matching it 💌	ddos Byte offset Delete	Start End
	Payload 👻	Find matching it 💌	ae86 Byte offset Delete	Start End
	Add			
ction	Allow OBlock	Discard Reject	requests and block IP for 15 Continue Protection	mins



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。

÷	Feature Filtering				
	Create				Enter IP Q
	ID	Associated Resource	Feature List	Action	Operation
	00gipjkv	bgpip-000002hl/119.28.217.238	Source port equals to 5000 Destination port equals to 808 Message length equals to 1350 IP headerFind matching items via regexddos,Offset byte starts at 5, ends at 60 and PayloadFind matching items via regexae86,Offset byte starts at 5, ends at 60	Allow	Configuration Delete
	Total items: 1				10 ▼ / page 🛛 🖂 1 /1 page 🕨 🕅



AI防护

最近更新时间:2022-03-11 12:28:20

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。

前提条件

您需要成功购买 DDoS 高防 IP,并设置防护对象。

操作步骤

- 1. 登录 DDoS 高防 IP 控制台,在左侧导航中,单击防护配置 > DDoS 防护。
- 2. 在 DDoS 防护页面的左侧,选中高防 IP 的 ID,如"bgpip-xxxxx"。





3. 在 AI 防护卡片中, 单击 , 打开 AI 防护开关。





IP 黑白名单

最近更新时间:2023-04-28 16:48:50

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,并设置防护对象。

说明:

创建 IP 黑白名单后常态化生效。

- 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 控制台,在左侧导航中,单击防护配置 > DDoS 防护。

2. 在 DDoS 防护页面的左侧,选中高防 IP 的 ID,如"bgpip-xxxxx"。

IP • 000488	Q	IP/Port Protection	Domain name protection	
		DDoS Protection Anti-DDoS collects an In Loose Mode, only blocked. If attack mer	Level nd analysis the characteristics of his confirmed attack messages are bloc ssages failed to be blocked in the S ium OLoose	tory attacks, blocks cked. In Medium mc trict mode, or the n



3. 在 IP 黑白名单卡片中,单击设置,进入 IP 黑白名单页面。

otection Policy 🛈	
IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.	Port Filtering Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Configured 4 blocklists, 1 allowlists	Configured 1 rules Set
Block by protocol	Watermark Protection
Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.	The application end and Anti-DDoS share the same watermark algorithm and key. In this case, every message sent out from the client is embedded with the watermark, so as to defense layer-4 CC attacks, such as
Configured 1 rules Set	• Enabled 1 rules Se

4. 在 IP 黑白名单页面中, 单击新建, 创建 IP 黑白名单规则, 选择黑白名单类型, 单击保存。

Create IP blacklist/whitelis	st	×
Associate Anti-DDoS Advance	bgpip-000002hl 😢	
Туре	O Blacklist O Whitelist	
IP	1.1.1.1 2.2.2.2	⊘
	OK Cancel	

5. (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,可以在右侧操作列,单击**删除**,删除 IP 黑 白名单规则。



Associated Resource	Source New Connection Rat	Source Concurrent Connecti	Destination New Connection	Destination Concurrent Con	Maximum Source IP Excepti	Operation
1	Close	Close	Close	Close	Close	Configuration



端口过滤

最近更新时间:2022-03-11 12:28:20

DDoS 高防 IP 支持针对访问 DDoS 高防 IP 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,并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台,在左侧导航中,单击防护配置 > DDoS 防护。

2. 在 DDoS 防护页面的左侧,选中高防 IP 的 ID,如"bgpip-xxxxx"。

IP • Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium mo blocked. If attack messages failed to be blocked in the Strict mode, or the n Strict Medium Loose



3. 在端口过滤卡片中,单击**设置**,进入端口过滤页面。

Protection Policy (j)	
IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.	Port Filtering Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Configured 4 blocklists, 1 allowlists Set	Configured 1 rules Set
Block by protocol	Watermark Protection
Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.	The application end and Anti-DDoS share the same watermark algorithm and key. In this case, every message sent out from the client is embedded with the watermark, so as to defense layer-4 CC attacks, such as
Configured 1 rules Set	• Enabled 1 rules Set

4. 在端口过滤页面中,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。
- 优先级:请填写一个介于1-1000的数字,数字越小优先级越高,该条规则排列位置越靠前,默认优先级为10。

Port Filtering							×
Create						Enter IP	Q
Associated Resource	Protocol	Source Port Range	Destination Port Range	Action	Priority (j	Operation	
bg,	Il Protocols 💌			Discard 💌		Save	Cancel
Total items: 0					10 🔻 / page	4	1 /1 page ▶ ▶

6. 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**,可以修改特征端口规则。

Associated Resource	Protocol	Port	Speed Limited Mode	Packet rate limit	Operation
bgp	SMP;UDP	-	By source IP		Configuration Delete



区域封禁

最近更新时间:2022-03-11 12:28:20

区域封禁支持对访问 DDoS 高防 IP 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,并设置防护对象。

操作步骤

- 1. 登录 DDoS 高防 IP 控制台,在左侧导航中,单击防护配置 > DDoS 防护。
- 2. 在 DDoS 防护页面的左侧,选中高防 IP 的 ID,如"bgpip-xxxxx"。

IP • 000488	Q	IP/Port Protection Domain name protection
		 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium me blocked. If attack messages failed to be blocked in the Strict mode, or the n Strict Medium Loose


3. 在区域封禁卡片中,单击**设置**,进入区域封禁页面。

Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.	IP/Port Speed Limit Controls access to the business IP by configuring speed limits on IPs and ports.
Configured 1 rules Set	Configured 1 rules Set
Feature Filtering Configure custom blocking policy against specific IP, TCP, UDP message header or payload.	
Configured 2 rules Set	

- 4. 在区域封禁页面,单击**新建**。
- 5. 在"新建区域封禁"弹窗中,选择封禁区域,单击确定,创建区域封禁规则。

Create Regional Bloc	ing Policy	×
Associate Service Packs	Search by IP or name	
Blocked Areas	O China Outside China Custom	
	Confirm Cancel	

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。

Associated Resource	Blocked Areas	Operation
bg	= [Configuration Delete



IP 端口限速

最近更新时间:2022-03-11 12:28:20

DDoS 高防 IP 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,并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台,在左侧导航中,单击防护配置 > DDoS 防护。

2. 在 DDoS 防护页面的左侧,选中高防 IP 的 ID,如"bgpip-xxxxx"。

IP • 200488	Q	IP/Port Protection Domain name protection
		 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium me blocked. If attack messages failed to be blocked in the Strict mode, or the n Strict Medium Loose



3. 在 IP 端口限速卡片中, 单击设置, 进入 IP 端口限速页面。

block by loc	ation		IP/Port Speed	Limit
P	Block requests to access Anti-DDoS Advanced instances from IP addresses specified regions.	in	A A	Controls access to the business IP by configuring speed limits on IPs and po
Configured	1 rules	Set	Configured	1 rules
Feature Filte	ring			
	Configure custom blocking policy against specific IP, TCP, UDP message he payload.	ader or		

- 4. 在"IP 端口限速"页面中, 单击新建。
- 5. 在新建 IP 端口限速弹窗中,选择相关协议与具体的端口,并输入限速阈值。单击确定,创建 IP 端口限速规则。

Create IP/Port Speed	d Limit	×
Associate Service Packs	8	
Protocol	ALL TCP UDP SMP Custom	
Port	Please enter port numbers or port ranges; one entry per line; up to 8 entries can be entered. Port range: 0-65535	
Speed Limited Mode	By source IP 💌	
Speed Limit 🚯	bps pps	
	Confirm	

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。



Associated Resource	Protocol	Port	Speed Limited Mode	Packet rate limit	Operation
bgp	SMP;UDP	-	By source IP		Configuration Delete



连接类攻击防护

最近更新时间:2022-06-10 14:12:06

当连接类发起异常, DDoS 高防 IP 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 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,并设置防护对象。

操作步骤

- 1. 登录 DDoS 高防 IP 控制台,在左侧导航中,单击防护配置 > DDoS 防护。
- 2. 在 DDoS 防护页面的左侧,选中高防 IP 的 ID,如"bgpip-xxxxx"。

IP • 000488	Q	IP/Port Protection	Domain name protection	
		DDoS Protection Lev Anti-DDoS collects and a In Loose Mode, only cont blocked. If attack messag Strict Medium	vel analysis the characteristics of h ifirmed attack messages are bl ges failed to be blocked in the Loose	istory attacks, blocks ocked. In Medium mo Strict mode, or the no



3. 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。

Protection Policy (j)	
IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource. Set	Al Protection The Al engine learns the connection number baseline and traffic characteristics, discovers and blocks layer-4 connection CC attacks, and can effectively defend against layer-4 connection attacks. Set
Connection Attack Protection Set refined protection policies targeting connection attacks	IP/Port Speed Limit Controls access to the business IP by configuring speed limits on IPs and ports. Set

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。



5. 在配置连接类攻击防护弹窗中,开启异常连接防护,单击确定。

Configure Connection Attack Protection	×
Associate Anti-DDoS Advanced	
Connection Flood Protection	
Source New Connection Rate Limit	
Source Concurrent Connection Limit	
Destination New Connection Rate Limit	
Destination Concurrent Connection Limit	
Abnormal Connection Protection 🛞	
Maximum Source IP Exceptional Connections	
OK Cancel	

6. 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。

Associated Resource	Source New Connection Rat	Source Concurrent Connecti	Destination New Connection	Destination Concurrent Con	Maximum Source IP Excepti	Operation
1	Close	Close	Close	Close	Close	Configuration



CC 防护 CC 防护开关及清洗阈值

最近更新时间:2022-03-02 13:25:43

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。

操作步骤

- 1. 登录 DDoS 高防 IP (新版)管理控制台,在左侧导航中,单击防护配置 > CC 防护。
- 2. 在 CC 防护页面的左侧列表中,选中高防 IP 的 ID 下面的域名。

Configurations		Global Setting Mode
DDoS Protection CC Protection Protection Flow Non-vebrile/port User Webrite/domain Networke/domain DDoS Engine CC Engine Real Server Real Server	Troubleshooting Different protection policies are applicable to different engines: Why are three limits on the manual unblocking time? And what are the limits? IP/poot protection policy is applicable to the Anti-DODS engine, and the domain name protection policy is applicable to the CC What are the differences between Anti-DODS Advanced and Anti-DODS Pro? How can I connect to a blocked server? protection engine. What if my business IP is blocked for attack deferse?	View Al
IP Y Q	For details about configuring domain name protection, contact your sales rep	
bgp	CC Protection and Cleansing Threshold () CC protection detects multicus behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all su are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, please contact our technical support.	ispicious requests
bge bge	CC Protection When it's off, the following CC protection policies do not take effect Cleansing Threshold () 1-20000 QPS	Set



3. 在右侧 CC 防护开关及清洗阈值卡片中,单击 法开启 CC 防护。

3. 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



Configurations	🔀 Global Setting Mode
DDoS Protection CC Protection Protection Flow User Non-web/let/goot Web/tet/somain User Veb/tet/somain Temme applications DoS Engine CC Engine Real Service Real Service	Trokkehooting Trokkehooting Ufferent protection policies are applicable to different engines Why are there limits on the manual unblocking times? And what are the limits? IPport protection policy is applicable to the Anti-DDOS engine, and Why are there limits on the manual unblocking times? And what are the limits? the domain name protection policy is applicable to the CC What if my busines? IP is blocked for attack defense?
IP V Q bap bap bap bap	For details about configuring domain name protection, contact your sales rep C protection and Ceansing Trreshold ① C protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests arest are blocked. In Strict

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。当指定域名收到的 HTTP 请求超过阈值时, 触发 CC 防护。
- 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。
- 若明确该清洗阈值,可进行自定义设置(现已支持清洗阈值自定义)。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。



智能 CC 防护

最近更新时间:2023-04-28 16:48:50

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。

前提条件

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

操作步骤

- 1. 登录 DDoS 高防 IP(新版)管理控制台,在左侧导航中,单击防护配置 > CC 防护。
- 2. 在 CC 防护页面的左侧列表中,选中高防 IP 的 ID 下面的域名。

IP v Q	For details about configuring domain name protection, contact your sales rep	^	Ī
bg 📕 🖥 o	CC Protection and Cleansing Threshold 🛈		
pðt	CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly- suspicious requests are blocked. In Strict mode, all suspicious requests are blocked if attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, please contact our technical support.		
pðt 📰	CC Protection OD When it's off, the following CC protection policies do not take effect		
bgp-		Set	



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。



C Protection and Cleansing Threshold (i)	bb/-
suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked. Loose mode, please contact our technical support.	d in
CC Protection When it's off, the following CC protection policies do not take effect	
Cleansing Threshold () 1~20000 QPS	Set
A. 在智能 CC 防护卡片中, 单击 开启智能防护。	
E CC Protection and Cleansing Threshold 🕄	
CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, high suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked Loose mode, please contact our technical support.	ly- in
CC Protection (When it's off, the following CC protection policies do not take effect	
Cleansing Threshold () 1~20000 QPS	Set
CC AI Protection	
After enabling CC AI protection, based on Tencent Cloud's big data capabilities, CC AI protection can self-learn website business traffic baselines, analyze attack anomalies in combination with algorithms, automatically issue accurate protection rules, and dynamically adjust business protection models to help you discover and prevent timely Block mali attacks.	cious Set

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。

CC AI Protection

🕥 腾讯云

The following CC AI protection is protection have a single validity protection rules can be deleted	rules are automatically generated period. After a single attack end based on protection requirement Q policy	d and take effect based on a single attack ds, the protection rules are automatically in hts. effective time	. The rules issued by intenvalidated and cleared. T	elligent The followin
The following CC AI protection is protection have a single validity protection rules can be deleted	rules are automatically generated period. After a single attack end based on protection requiremen	d and take effect based on a single attack ds, the protection rules are automatically ir nts.	. The rules issued by intenvalidated and cleared. T	elligent The followir
The following CC AI protection protection have a single validity protection rules can be deleted	rules are automatically generated period. After a single attack end based on protection requiremen	d and take effect based on a single attack ds, the protection rules are automatically ir nts.	. The rules issued by intenvalidated and cleared. T	elligent Fhe followii
CC AI Protection Enable				×
]失效并清除。根据防护需	需求,可单击 删除 ,删除对	付应防护规则。		
a能防护规则基于单次攻a	击自动生成与生效。智能陷	坊护下发的规则存在单次有效期,	单次攻击结束后,	防护规则
er a single attack ends, the protection rule es.	stection automatically generates protection es are automatically invalidated and cleare	n rules based on each attack. The rules issued by intellig	jent protection have a single val	idity period. otection View
EI GO AI FIOLEGLIUITIS EHADIEU. GO AI FIU	staation automatically generates protection	rules based on each attack. The rules issued by intellig	cont protoction have a single vali	idity pariod



精准防护

最近更新时间:2022-12-21 17:50:00

应用场景

DDoS 高防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

前提条件

您需要成功购买 DDoS 高防 IP,并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP (新版)管理控制台,在左侧导航中,单击防护配置 > CC 防护。



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

DDoS Protection CC Protection			
Protection Flow User Vacuum explication User Vebste/domain Doub Engine Cc Engine Cc Engine	Real Serv	Troubleshooting Different protection policies are applicable to different engines: Why are three limits on the manual unblocking times? And what are the limits? IP/port protection policy is applicable to the Anti-DDoS engine, and er the domain name protection policy is applicable to the CC How can I connect to a blocked serve? protection engine. Attack-related FAQ. Attack-related FAQ.	View All
P ▼ ▼4 h →	Q	For details about configuring domain name protection, contact your sales rep C details about configuring domain name protection, contact your sales rep C protection and Cleansing Threshold ① C protection detects millious behaviors accress modes and connection status in Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked. In Strict mode, al	

3. 在精准防护卡片中,单击**设置**,进入精准防护规则列表。

Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.	IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.
Configured 1 rules Set	Configured 5 rules (max: 50 rules) Set
Precise Protection A protection policy with a combination of conditions of common HTTP fields	CC Frequency Limit Set a limit to control to access frequency from the source IP.
Configured 1 rules Set	Defense Status 🚺 Defense Level 🕦 Urgent 💌 Set



4. 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。

Create Precise Protection	Policy	×
Associate Anti-DDoS Advance	bgpip-000002j1 😢	
IP	153.3.137.126	
Protocol		
Domain name	test.probe.tencentdayu.com	
Condition	Field Logic Value	
	uri 💌 equa 💌 / Delete	
	ua ▼ equa ▼ chrom∈ Delete	
	cook ▼ equa ▼ 4d5a Delete	
	refer v equa v Delete	
	Add	
Match Operation	Discard	
	OK Cancel	



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。

÷	Precise Protection							
	Create							
	ID	Associated Resource	Protocol	Domain name	Condition	Match Operation	Creation Time	Operation
	ccPrecs-00000ouy	bgpip- 000002j1/153.3.137.126	http	test.probe.tencentdayu.co m	uri equals to / cookie equals to 4d5a ua equals to chrome	Discard	2020-07-06 14:59:38	Configuration Delete
	ccPrecs-00000out	bgpip- 000002j1/153.3.137.126	http	test.probe.tencentdayu.co m	uri equals to /	САРТСН	2020-06-30 20:32:07	Configuration Delete
	Total items: 2						10 🔻 / page 🛛 🖌 🔌	1 /1 page 🕨 🕅



CC 频率限制

最近更新时间:2020-07-07 17:19:14

前提条件

您需要成功购买 DDoS 高防 IP,并设置防护对象。

操作步骤

- 1. 登录 DDoS 高防 IP(新版)管理控制台,在左侧导航中,选择【防护配置】。
- 2. 在左边的列表选中高防 IP 的 ID 下面的域名,如"212.64.xx.xx bgpip-000002je" > "http:80" > "www.xxx.com"。

IP Q * 150.109.141.217 bgpip-0000015t TCP:8080 * 150.109.141.216 bgpip-0000015s * http:80 baldu.com baldu.com	CC Protection Policy CC protection detects malicious behaviors according to access modes and connection highly-suspicious requests are blocked. In Strict mode, all suspicious requests are bloc are blocked in Loose mode, please contact our technical support. Strict O Medium C Loose	n status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, ked. If attack requests failed to be blocked in the Strict mode, or the normal requests Cleansing Threshold Close T
	Precise Protection A protection policy with a combination of conditions of common HTTP fields Set	CC Frequency Limit Set a limit to control to access frequency from the source IP. Set

3. 右侧卡片中单击"CC 频率限制"卡片中的【设置】,进入频率限制规则列表。

CC Fre	equency L	.imit									
Create	Э										
ID		Bound Resource	Protocol	Domain name	Detection Perio	Detection Times	Match Type	Match value	Action	Creation Time	Operation
						No data yet					
Total iter	ms: 0								10 💌 / page		/1 page 🕨 🕨



4. 单击【新建】, 创建频率限制规则, 填写相关字段, 填写完成后, 单击【确定】。

Create CC Frequency Limi	t	>
Associate Anti-DDoS Advance	bgpip-0000015s 🙁	
IP	150.109.141.216	
Protocol		
Domain name	Please select	
	Field Mode Value	
	Uri 💌 equa 💌 / Delete	
	Add	
Frequency Limit Policy	CAPTCH -	
Condition	When 10 secol - Access 100 Times	
Punishment Time	3600 seconds 🥯	
	OK Cancel	

5. 新建完成后,频率限制列表将增加一条频率限制规则,可以在右侧操作列,单击【配置】,修改频率限制规则。

CC Frequency Limit												
Create												
ID	Bound Resource	Protocol	Domain name	Detection Perio	Detection Times	Match Type	Match value	Action	Creation Time	Operation		
ccRule-000000cg	bgpip- 00000209/212.64. 62.249	http	prob1.probe.tence ntdayu.com	10	1	Uri	/	CAPTCH	2020-06-02 11:24:24	Configuration Delete		
Total items: 1								10 🔻 / page		/1 page ► ►		



区域封禁

最近更新时间:2022-03-11 12:28:21

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。

前提条件

您需要成功 购买 DDoS 高防 IP,并设置防护对象并接入了域名业务的防护。

操作步骤

- 1. 登录 DDoS 高防 IP (新版)管理控制台,在左侧导航中,单击防护配置 > CC 防护。
- 2. 在 CC 防护页面的左侧列表中,选中高防 IP 的 ID 下面的域名。

DDoS Protection CC Protection	
Protection Flow Protection Flow application User User Website/domain name application DD5 Engine CC Engine Ref	Different protection policy is applicable to different engines: Introduction policy is applicable to different engines: Introduction policy is applicable to the Anti-DDS engine, and biocet to a blocked server? Why are there limits on the manual unblocking times? And what are the limits? When the limits? Whe
↓ Q	For details about configuring domain name protection, contact your sales rep C C protection and Cleansing Threshold ① C protection and Cleansing Threshold ① C protection details malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are biocked. In Medium mode, highly-suspicious requests are biocked. In Strict mode, all suspicious requests are biocked. In Strict mode, all suspicious requests are biocked. In Strict mode, all suspicious requests are biocked. In Medium mode, highly-suspicious requests are biocked. In Strict mode, all suspicious requests are biocked. In Strict mode, all suspicious requests are biocked. In Medium mode, highly-suspicious requests are biocked. In Strict mode, all suspicious r



3. 在区域封禁卡片中,单击**设置**,进入区域封禁页面。

Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.	IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.
Configured 1 rules Set	Configured 5 rules (max: 50 rules) Set
Precise Protection A protection policy with a combination of conditions of common HTTP fields	CC Frequency Limit Set a limit to control to access frequency from the source IP.
Configured 1 rules Set	Defense Status 🚺 Defense Level 🛈 Urgent 💌 Set

4. 在区域封禁页面,单击**新建**。

Create			Enter IP	Q
Associated Resource	Blocked Areas	Operation		
	No data yet			

5. 在新建区域封禁弹窗中,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。

Create Regional Blo	cking Policy		×
Associate Service Packs	bgp-000001cg		
IP	Please select	•	
Protocol	О НТТР		
Domain			
Blocked Areas	O China Outside China	Custom	
		Confirm	

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。

Associated Resource	Protocol	Domain	Blocked Areas	Operation
bgp-0000 218		sr	China	Configuration Delete



IP 黑白名单

最近更新时间:2022-03-02 13:25:43

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:

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,并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP(新版)管理控制台,在左侧导航中,单击防护配置 > CC 防护。

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

DDoS Protection CC Protection Protection Flow User User Vesote/domain DDoS figure Cc Engine Real	Different protection policies are applicable to different engines: Troubleshooting Why are three limits on the manual unblocking times? And what are the limits? View IP/port protection policy is applicable to the Anti-DDOS engine, and whete the domain name protection policy is applicable to the CC protection policy. How can I connect to a blocked server? Attack-related FAQ
	For details about configuring domain name protection, contact your sales rep C C Protection and Cleansing Threshold C protection and Cleansing Threshold C protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests are blocked in Loose mode, please contact our technical support. CC Protection C Protection C When it's off, the following CC protection policies do not take effect. Cleansing Threshold Custom a gas



3. 在右侧 IP 黑白名单卡片中,单击设置,进入 IP 黑白名单列表。

For details about configuring domain name protection, contact your sales rep	
CC Protection and Cleansing Threshold ① CC protection detects malicious behaviors according to access modes and connection status. In Loose Mode, only confirmed a are blocked. If attack requests failed to be blocked in the Strict mode, or the normal requests are blocked in Loose mode, pleater blocked.	ttack requests are blocked. In Medium mode, highly-suspicious requests are blocked. In Strict mode, all suspicious requests se contact our technical support.
CC Protection When it's off, the following CC protection policies do not take effect Cleansing Threshold () 2 QPS	Set
Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.	IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.
Configured 1 rules Set	Configured 1 rules (max: 50 rules) Set

4. 单击**新建**,填写相关字段,填写完成后,单击**保存**。

IP Blocklist/Allowlist								×
Create							Enter an IP	Q
Associated Resource	Associated IP	Protocol Type	Domain Name	B	Blocked/Allowed	Туре Т	Modification Time	Operation
bgp-ú		http 🔻				Blocklist 🔻		Save Cancel
bgp-f		http		1		Blocklist	2021-12-27 22:10:23	Set Delete
Total items: 1						10 💌 / page		/1 page 🕨 🕨

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 Blocklist/Allowlist								×
Create						Enter an IP		Q
Associated Resource	Associated IP	Protocol Type	Domain Name	Blocked/Allowed IPs	Туре Т	Modification Time	Operation	
bg,		http	a		Blocklist	2021-12-27 22:10:23	Set Delete	
Total items: 1					10 🔻 / page		/1 page >	×



业务接入 端口接入

最近更新时间:2023-04-28 16:48:50

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 高防 IP (新版)管理控制台,在左侧目录中,单击业务接入 > 端口接入。

2. 在端口接入页面,单击**开始接入**。

ess via por	ts An	cess via domain na	ames						
Add rule	Enter	· IP	Q						
Forwa	Forwa	Origin Server P	Origin	Associated Protectin	Load Balancing Mode	Health check	Session Persistence	Modification Time	Operation
TCP	41900	80	150.158.199.231	212.64.62.249	Weighted polling	Close Edit	Close Edit	2020-07-02 11:22:35	Configuration Delete
TCP	234	234	119.29.205.248	150.109.130.57	Weighted polling	Not supported	Not supported	2020-06-30 19:27:00	Configuration Delete
TCP	8080	80	134.175.195.228 1.1.1.2	150.109.132.100	Weighted polling	Not supported	Not supported	2020-06-29 16:32:02	Configuration Delete
TCP	80	80	106.52.156.188	117.184.254.214	Weighted polling	Close Edit	Close Edit	2020-06-28 14:45:59	Configuration Delete
TCP	41900	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit	Close Edit	2020-06-28 10:45:20	Configuration Delete
TCP	41800	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit	Close Edit	2020-06-28 10:45:17	Configuration Delete
TCP	41700	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit	Close Edit	2020-06-28 10:45:14	Configuration Delete
TCP	41600	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit	Close Edit	2020-06-28 10:45:10	Configuration Delete
TCP	31500	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit	Close Edit	2020-06-28 10:45:07	Configuration Delete
TCP	31400	80	49.232.127.41	188.131.208.243	Weighted polling	Close Edit	Close Edit	2020-06-28 10:45:03	Configuration Delete
Total items	159							10 v / page 🖂 🖣 1	/ 16 pages 🕨 🕨

3. 在端口业务接入页面,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。

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。

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。
- 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。

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、转发协议和转发端口关键字对规则进行查询。

ieparate multiple keywords with " "											
Select a filter Origin IP/Domain Name	Real Server Port	Origin	Associated Protectin	Load Balancing Mode	Health Check	Session Persistence	Modification Time	Operation			
Real Server Port	1	1 9	42	Weighted	Disable Edit 🛈	Disable Edit	2021-11-25 21:08:09	Configuration Delete			
Associated Protecting IP Forwarding Protocol	(III.)	1 59	56.131	Weighted Round Robin	Disable Edit	Disable Edit	2021-11-24 20:34:56	Configuration Delete			
Forwarding Port		٤ 53	42. 31	Weighted Round Robin	Disable Edit 🛈	Disable Edit	2021-11-24 18:00:03	Configuration Delete			

配置规则

在端口接入页面,选择所需规则,单击操作列的配置。
 在配置四层转发规则页面,可修改相关参数,单击确定保存。

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。
- 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。

2. 在删除规则弹窗,单击删除,即可删除所选规则。

导入规则

在端口接入页面,单击**批量导入**。
 在批量导入四层转发规则弹窗,填写所需规则,单击确定。

导出规则

- 1. 在端口接入页面,单击导出规则。
- 2. 在批量导出四层转发规则弹窗,选择所需规则,单击复制。



域名接入

最近更新时间:2023-04-28 16:48:51

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 高防 IP (新版) 管理控制台,在左侧目录中,单击业务接入 > 域名接入。

2. 在域名接入页面,单击**开始接入**。

IP ACCess ()		
With Anti-DDoS Advanced	Troubleshooting View	
You need to add a CNAME record for the application domain name at your DNS ISP. When network traffic flows through Anti-DDoS Advanced, it automatically filters out malicious traffic to protect the security of the real server.	Connecting applications to Anti-DDoS Advanced IP blocking and unblocking	
CNAME address/A record O Forwarding Port Port	Modifying DNS resolution Solutions for an exposed origin server IP address	
User Edge Defender Anti-DDoS Advanced -> Origin IP Real Server		
bort Batch Delete	Enter a domain name or an as Q	
**	With Anti-DDoS Advanced You need to add a CNAME record for the application domain name at your DNS ISP. When network traffic flows through Anti-DDoS Advanced, it automatically filters out malicious traffic to protect the security of the real server. Image: CNAME address/A record Image: CNAME address/A record Image: User Image: CNAME address/A record Image: Edge Defender Forwarding Image: Port Image: Port Image: Port Im	

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。





Access via Domain N	ame					×
1 Select Instance 4 Modify DNS Res	> 2 Protocol Po	ort > (3 Set Forward	ding Method	>	
Q	CNAME address/A record	0	Forwarding Port	Real Server Port Protocol		
User		Edge Defender	Anti-DDoS Advanced	 Origin IP 	Real Server	
* Associated Instance	Search by IP or name					

3. 选择转发协议,填写业务域名,单击**下一步:回源方式**。

Access via Domain Name	×
 Select Instance > 2 Protocol Port > 3 Set Forwarding Method > Modify DNS Resolution 	
CNAME address/A record User CNAME address/A record CNAME address/A record User CNAME address/A record Edge Defender CNAME address/A record CNAME address/A	
* Forwarding Protocol http	
* Application domain name	

4. 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

🔗 腾讯云

步:修改 DNS 解析。

Access via Domain Na	ame	
Select Instance Modify DNS Res	> Protocol Port > 3 Set Forwarding Method > colution	
O User	CNAME address/A record CNAME address/A record Edge Defender Anti-DDoS Anti-DDoS Advanced IP CNAME address/A record Advanced Adv	
 Set Forwarding Method 	• Forwarding via IP • Forwarding via domain name Clean traffic can be forwarded back to the real server by the IP or domain name	
Real Server IP & Port	Origin IP Real Server Port	
	Enter the real server (eg: 1.1.1.1) Eg: 80 Delete	
	+ Add	

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。

5. 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, 建议低峰期更新。



Start Access Ba	Enter a domain r	ame or an as	Q							
Application dom	Forwarding Prot	Forwarding Port	Real Server IP/Site	Associated Prote	Health Check	Access Status	CC Protection Stat	Modification Time	Operation	
			-		Disable Configuration (Success	Disable 🚺 🚯	2022-04-25 19:04:02	Configuration Delete	
					Disable Configuration	Success	Disable Configuration	2022-04-25 19:04:09	Configuration Delete	

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。

Start Access Batch Import Batch Export Batch Delete									Enter a domain name or an as		
Application dom	Forwarding Prot	Forwarding Port	Real Server IP/Site	Associated Prote	Health Check	Access Status	CC Protection Stat	Modification Time	Operation		
					Disable Configuration	Success	Disable 🚺 🚯	2022-04-25 19:04:02	Configuration Delete		
m	-				Disable Configuration (i)	Success	Disable Configuration	2022-04-25 19:04:09	Configuration Delete		
		•			Disable Configuration	Success	Disable 🚺	2022-04-25 18:59:54	Configuration Delete		



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。

Configure Layer-7 Forv	varding Rule	×
Associated Protecting IP	Up to 60 rules can be added, 6 added now	
Domain Name	Please enter a domain name containing up to 67 characters.	
Protocol	http O https	
	Forward via HTTP for HTTPS requests	
Certificate Source	Tencent Cloud Hosting Certificate(🖸) SSL Certificate Management 🧔	
Certificate	· · · ·	
Set Forwarding Method	Forwarding via IP Forwarding via domain name	
Real Server Domain Name	Real Server Domain Name Real Server Port	
	Delete	
	+ Add	
	Please enter the real server domain name (CNAME) or the combination of real server domain name (CNAME) and port. It supports up to 16 entries.	

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。

Start Access Bat	ch Import Bato	h Export Batch	n Delete					Enter a domain	name or an as C
Application dom	Forwarding Prot	Forwarding Port	Real Server IP/Site	Associated Prote	Health Check	Access Status	CC Protection Stat	Modification Time	Operation
m	-				Disable Configuration	Success	Disable 🚺 🤖	2022-04-25 19:04:02	Configuration Delete
m		•			Disable Configuration	Success	Disable Configuration	2022-04-25 19:04:09	Configuration Delete

•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。

Start Access Batch Import	Batch Export Batc	h Delete					Enter a domain r	name or an as	Q
Application dom Forwarding Pr	ot Forwarding Port	Real Server IP/Site	Associated Prote	Health Check	Access Status	CC Protection Stat	Modification Time	Operation	
🕶 m 🖦	1.00			Disable Configuration	Success	Disable 🚺 🚯	2022-04-25 19:04:02	Configuration Delete	
•				Disable Configuration	Success	Disable Configuration	2022-04-25 19:04:09	Configuration Delete	

2. 在删除规则弹窗,单击**删除**,即可删除所选规则。

导入规则

1. 在域名接入页面,单击**批量导入**。



2. 在批量导入七层转发规则弹窗,填写所需规则,单击确定。



导出规则

1. 在域名接入页面,单击**导出规则**。



2. 在批量导入七层转发规则弹窗,选择所需规则,单击复制。

Search by IP or name		



配置会话保持

最近更新时间:2022-04-28 14:48:17

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 高防 IP (新版) 管理控制台,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】。

pplication Acc	cessing								Purc
Access via port	s Ac	cess via domain na	imes						
Add rule	Enter	IP	Q						
Forwa	Forwa	Origin Server P	Origin	Associated Protectin	Load Balancing Mode	Health check	Session Persistence	Modification Time	Operation
TCP	41900	80	150.158.199.231	212.64.62.249	Weighted polling	Close Edit	Close Edit	2020-07-02 11:22:35	Configuration Delete
TCP	234	234	119.29.205.248	150.109.130.57	Weighted polling	Not supported	Not supported	2020-06-30 19:27:00	Configuration Delete

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。







实例管理 查看实例信息

最近更新时间:2022-08-16 15:28:12

您可以通过 DDoS 防护管理控制台,查看所购买的 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:查看高防 IP 实例"bgpip-000002jf"的实例信息。

1. 登录 DDoS 高防 IP(新版)管理控制台,在左侧导航栏中,单击**实例列表**,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。

Instance List									Purchase	
S All Regions V	S All Lines 🔻							Enter ID	/name/IP (Q
ID/Name/Tag	IP Protocol	Anti-DDoS Advanced	Specifications	Specifications	Status T	Attacks in last 7 days	Date		Operation	
Not named p^* None p^*	IPv4	-	Line: CMCC(Shanghai) Application Bandwidth: 100Mbps Elastic Application Bandwidth:	Base bandwidth peak: 60Gbps Elastic Protection: not enabled P CC Protec	Protection Status Protected ports: 0 Protected domains: 0	0 times 🗠	Purchase time 04-15	ə: 2022-	Configurations View Report	
			Line: CLICC(Naniino)							

2. 在弹出的页面中查看如下信息:

←	bgpip-000002tb			
	Basic Information			
	Anti-DDoS Advanced Name	Unnamed 🎤	Current Status	Running
	Location	Hong Kong, China	Expiry Time	2020-08-06
	IP	119.28.217.248		
	Base Protection Bandwidth	50Gbps	Forwarding IP Range	119.28.191.0/24 119.28.44.0/24
	CC Protection Peak	150000QPS		119.28.85.0/24
	Line	BGP		119.28.3.0/24 119.28.187.0/24
	Max forwarding rules	60		119.28.186.0/24 119.28.193.0/24 119.28.193.0/24
				119.20.217.0/24


- 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。
- 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。
- 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 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。



设置实例别名与标签

最近更新时间:2020-07-07 17:19:16

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。

操作步骤

方式一

1. 登录 DDoS 高防 IP(新版)管理控制台,在左侧导航栏中,单击【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, 输入名称即可。

名称长度为1-20个字符,不限制字符类型。

ID/Name/Tag	Anti-DDoS Adv	Specifications
bgpip-000002tb Unnamed 🖍 N/A 🖍	119.28.217.248	Line: BGP(Hong Kong, China) Application Bandwidth: 100Mbps Package type: Standard pack

方式二

- 1. 登录 DDoS 高防 IP(新版)管理控制台,在左侧导航栏中,单击【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 名称右侧的修改铅笔按钮,输入名称。



名称长度为1-20个字符,不限制字符类型。

Basic Information								
Anti-DDoS Advanced Name	Unnamed 🎤							
Location	Hong Kong, China							
IP	119.28.217.248							
Base Protection Bandwidth	50Gbps							
CC Protection Peak	150000QPS							
Line	BGP							
Max forwarding rules	60							



配置智能调度

最近更新时间:2022-08-04 11:19:08

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(大禹)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。

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,将按照 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、2.2.2.2和3.3.3.3的优先级都为1,1.1.12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。

设置线路优先级

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:

1. 登录 DDoS 高防 IP(新版)管理控制台,在左侧导航栏,单击【智能调度】,进入列表页面,单击【新建调 度】,系统自动生成一个 CNAME 记录。

nart Scheduling							
New Scheduling Policy]				CNAME -	Please enter the co	Q
CNAME	Parsing Status	Associated IP	Scheduling Mode	Last Modified Time	Oper	ation	
j6z1mo4q.dayugslb.com	Not running	Add Anti-DDoS instance	Priority	2020-07-01 09:52:31	Configuration Delete		
v3drws2b.dayugslb.com	Not running	Add Anti-DDoS instance	Priority	2020-07-01 09:52:29	Conf	guration Delete	



2. 找到该 CNAME 记录所在行,单击【添加高防实例】,进入智能调度编辑页面。

Sma	Smart Scheduling								
	New Scheduling Policy					CNAME Please enter the co	Q		
	CNAME	Parsing Status	Associated IP	Scheduling Mode	Last Modified Time	Operation			
	j6z1mo4q.dayugslb.com	Not running	Add Anti-DDoS instance	Priority	2020-07-01 09:52:31	Configuration Delete			
	v3drws2b.dayugslb.com	Not running	Add Anti-DDoS instance	Priority	2020-07-01 09:52:29	Configuration Delete			
	qo0in9hm.dayugslb.com	Running	2 associated IPs (j)	Priority	2020-06-30 21:21:51	Configuration Delete			

3. 在智能调度编辑页面中, TTL 值默认60秒, 取值范围为1-3600(秒), 调度方式为默认优先级。





4. 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】。

elect resource type	Anti-DDoS Advance	•					
elect resource	Service Packs				Selected (0)		
	Anti-DDoS Advance		Q		Resource ID/Na	IP Address	Resource Type
Resource ID/Na	me IP Address	Res	ource Type				
bgpip-000002td	188.131.208.27	Ant	-DDoS Advance				
bgpip-000002tb	119.28.217.248	Ant	-DDoS Advance				
bgpip-000002ta	117.184.254.232	Ant	-DDoS Advance	+			
bgpip-000002t9	153.3.137.208	Ant	-DDoS Advance				
bgpip-000002t8	183.131.196.215	Ant	-DDoS Advance				
bgpip-000002rr	119.28.217.239	Ant	-DDoS Advance				

5. 选择高防实例后,实例的高防线路默认开启域名解析,再为其设置优先级。

CNAME	j6z1mo4q.dayugslb.	.com					
TTL Value	60 seconds 🧪						
Vlode	O Priority						
Associated IP	Add Anti-DDoS IP Ad	dd non-Anti-DDos	S IP				
	IP	Priority	Line	Region	Status	Domain Name	Operation
	119.28.217.248 (bgpip-000002tb)	100 🗨	Outside Mainland China	Hong Kong, China	Running		Unbind



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。

IP	Priority	Line	Region	Status	Domain Name	Operation
183.131.196.215 (bgpip-000002t8)	100 🗨	СТСС	Hangzhou	Running		Unbind
153.3.137.208 (bgpip-000002t9)	100 🗨	CUCC	Nanjing	Running		Unbind
2402:4e00:1400:e 57b:0:8f9c:903:5e 6e (bgp-000000cm)	100 🎤	BGP	Shanghai	Running		Unbind

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(大禹)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。



设置安全事件通知

最近更新时间:2020-07-07 17:19:18

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(新版)管理控制台,在左侧导航中,选择【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"和"DDoS 清洗阈值"。

Inbound Traffic Thresho	ld Per IP	DDoS Cleansing Traffic Alarm When an IP is being attack, and the inbound traffic exceeds the threshold cleansing is triggered, and you will get notifications in message center.		
When the inbound traffic to an notification in the message ce	n IP exceeds the threshold, you will get onter.			
Advanced Settings	Default threshold: 200 Mbps	Advanced Settings	Default threshold: 200 Mbps 🧪	



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。

Modify Thresho	d	×
Set Threshold	- 200 + Mbps	
	OK Cancel	

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

÷	Inbound Traffic Threshold Per IP					
	Batch Modify				Enter the IP to be q	Q
	Resource Instance	Bound IP	Inbound traffic alarm threshold (Mbps)	Operation		
	bgpip-000002td	188.131.208.27	200	Modify		
	bgpip-000002tb	119.28.217.248	200	Modify		

• DDoS 清洗阈值

÷	DDoS Cleansing Alarm					
	Batch Modify				Enter the IP to be q	Q
	Resource Instance	Bound IP	DDoS Cleansing Threshold (Mbps)	Operation		
	bgpip-000002td	188.131.208.27	200	Modify		
	bgpip-000002tb	119.28.217.248	200	Modify		

设置通知方式

1. 登录您的腾讯云账号, 进入 消息中心。

	Σ		
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。

Security notifications						
Attack notifications		~	<		8163196@qq.com	Modify Message Receiver
Illegal Contents Notifications		~			8163196@qq.com	Modify Message Receiver

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。

age Receiver				
make sure that the user's email and mo	bile are verified by Tencent Cloud, a	Ind the responding method is enabled.		
Attack notifications				
User Group	Add Messa	1 selected		
Search for user name		Q	8163196@qq.com	×
User Name	Mobile Number	Email		
✓ 8163196@qq.com	✓ 158****0375	() 81****@qq.com		
v_szgwu	✓ 188****5245	✓ v_*****@tencent.com		
			\leftrightarrow	
		OK Cancel		
	nge Receiver make sure that the user's email and mo Attack notifications User User Group Search for user name ■ User Name V_8163196@qq.com ↓ v_szgwu	nge Receiver make sure that the user's email and mobile are verified by Tencent Cloud, a Attack notifications User User Group Add Messa Search for user name User Name Mobile Number Search for user name User Name Mobile Number v_szgwu () 158****0375 () v_szgwu () 188****5245	nge Receiver make sure that the user's email and mobile are verified by Tencent Cloud, and the responding method is enabled. Attack notifications User User Group Add Message Receiver Mobile Number Email Search for user name User Name Mobile Number Email Search for user name Nobile Number Email Numer Search for user name Search for user name Numer Search for user name Numer	rage Receiver make sure that the user's email and mobile are verified by Tencent Cloud, and the responding method is enabled. Attack notifications User User Group Add Message Receiver [2] Modily User Information [2] 1 selected Search for user name Q 1 selected 8163196@qq.com User Name Mobile Number Email 8163196@qq.com User Sagewu 1 158****0375 0 81*****@qq.com **



查看操作日志

最近更新时间:2020-07-07 17:19:18

操作场景

DDoS 高防 IP 支持查看近90天内重要操作的日志,如有需要,您可以登录控制台查看。可查看的日志包含以下类别:

- 转发规则变更操作日志
- 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
- 实例名称的修改日志

操作步骤

- 1. 登录 DDoS 高防 IP(新版)管理控制台,在左侧导航栏中,单击【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。

Today Yesterday	Last 7 days Last 30 days	2020-06-06 00:00 ~ 2020-07-06	23:59			
Operation Time	Object ID	Product Type	Action	Result	Operator Account	Operation
2020-07-03 17:07:34	2687	Anti-DDoS Advance	Add layer-7 forwarding rule	Success	100001500880	Unfold
2020-07-03 17:07:07	2687	Anti-DDoS Advance	Delete layer-7 forwarding rule	Success	100001500880	Unfold
2020-07-03 17:06:30	2970	Anti-DDoS Advance	Delete layer-7 forwarding rule	Success	100001500880	Unfold



封堵相关操作 连接已被封堵的服务器

最近更新时间:2023-04-28 16:51:55

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。



解除封堵

最近更新时间:2022-12-21 16:13:27

解封操作

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:

- 1. 登录 DDoS 防护管理控制台,在左侧导航中,单击自助解封 > 解封操作,进入解封操作页面。
- 2. 在解封操作页面,选择所需 IP 的所在行,可在"预计解封时间"处,查看该 IP 的预计解封时间。

自助解封次数

使用 DDoS 高防 IP 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大禹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

1. 登录 DDoS 防护管理控制台,在左侧导航中,选择自助解封 > 解封操作,进入解封操作页面。



2. 在解封操作页面,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。

Anti-DDoS	Unblocking Operation					
Overview Anti-DDoS Basic Anti-DDoS Advanced	Total Guotas 3		Currently used		Not currently used	
다 Anti-DDoS Pro 🗸	IP	Defense Status	Blocking time	Estimated unblocking time	Status	Operation
Intelligent Scheduling Policy		Anti-DDoS	2022-11-15 17:00:00	2022-11-16 16:55:00	Automatically unblocking	Unblock
Anti-DDoS Pro						
Anti-DDoS Advanced (New)						
🖾 Edge Defender 🛛 👻						
Manual Onblocking						
Unblocking Operation						
Unblocking Log						

3. 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

登录 DDoS 防护管理控制台,在左侧导航中,选择自助解封 > 解封操作记录,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。

Unblocking Log						
2022-08-15 17:14:11 ~ 2022-11-15 17:14:11						
IP	Blocking time	Actual unblocking time	Unblocking operation type			
	2022-11-15 17:00:00	2022-11-15 17:01:00	Automatically unblock			
	2022-10-28 15:35:00	2022-10-28 16:48:58	Self-service unblocking			
	2022-10-28 15:30:00	2022-10-28 16:39:29	Self-service unblocking			
	2022-10-27 15:30:00	2022-10-28 16:16:58	Automatically unblock			
	2022-10-13 14:25:00	2022-10-13 14:28:00	Automatically unblock			
	2022-10-13 14:15:00	2022-10-13 14:18:00	Automatically unblock			
	2022-10-13 10:58:00	2022-10-13 11:00:00	Automatically unblock			
	2022-10-13 10:50:00	2022-10-13 10:52:00	Automatically unblock			