

DDoS 高防包

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 操作总览 防护概览 使用限制 实例管理 查看实例信息 管理防护对象 设置实例别名与标签 业务接入 IP 透明接入 域名接入 IP 接入 端口接入 防护配置 AI 防护 端口过滤 DDoS 防护等级 IP 黑白名单 IP 端口限速 协议封禁 特征过滤 连接类攻击防护 区域封禁 查看操作日志 封堵相关操作 设置安全事件通知 连接已被封堵的服务器 解除封堵



操作指南 操作总览

最近更新时间:2023-04-20 16:44:05

您在使用 DDoS 高防包时,可能碰到诸如配置 DDoS 高防包实例、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 高防包的常用操作,供您参考。

实例管理

- 查看实例信息
- 管理防护对象
- 设置实例别名与标签
- 解封防护 IP

防护配置

IP和端口防护

- 防护等级与清洗阈值
- 协议封禁
- 特征过滤
- AI 防护
- IP黑白名单
- IP 端口限速
- 连接类攻击防护
- 区域封禁

统计报表

- 防护概览
- 查看操作日志

封堵相关操作



- 设置安全事件通知
- 连接已被封堵的服务器
- 解除封堵



防护概览

最近更新时间:2022-05-09 17:05:45

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							
E Overview	Protection Overview	Anti-DDoS Basic	Anti-DDoS Pro	Anti-DDoS Advanced				
 Anti-DDoS Basic □ Anti-DDoS → Advanced 	Attacks				Attacked IPs	Protecte	d IPs	Blocked IPs
Anti-DDoS Pro Anti-DDoS Pro Scheduling Policy				Safe No abnormal traffic detected.	O Attacked domain name	50 es Protecte	d domain names	O Peak attack bandwidth
Anti-DDoS Pro * (New)					0	30		O Mops

- 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和攻击类型。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。

	Total IPs 348
Protected IPs 50	Blocked IPs

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。





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 Pacies 15	Running Blocked Being attacked Other	15 0 0	Anti-DOUS Advanced 41	Running Blocked Being attacked Other	37 0 3

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 🔻	Operation
	in the second	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	ODoS Attack	View Details
11-	the American and	Anti-DDo5	2022-02-13 12:05:00	2 mins	Attack ends	ODoS 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 Attack Details						
Attack Info	rmation					
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	可该攻击时间段全量实时数据。		

Attack Bandwidth	Attack Packet Rate		
Mbps			
Vlbps			
Mbps			
4 Mbps			
2 Mbps			
2022 02 16 04:00	2022 02 16 04	15 2022 02 16 0420	2022 02 16 0445

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。
- 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。

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 高防包概览

将防护 IP 接入到 DDoS 高防包服务后,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 高防包。

My Anti-DDoS Advanced instances	\frown	Protecting	38	E	Blocked DDoS attacks 109 times
My usage		Being attacked	2		
		Blocked	0		Blocked CC attacks
• Activated 40 • 1				EØ	519 times
Renew Now					

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。

说明	:
支持3	查询最多180天以内的攻击流量信息及 DDoS 攻击事件。

DDOS Attack	CC Attack										
🔇 All Regions 👻	🔇 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	Ċ.

2. 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 / 攻击包速率趋势。

DD-C Amarka



S All Regions • S All Lines • Please select	▼ 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	
Attack Traffic Bandwidth (traffic surges incl	uded)	Attack Bandwidth Peak	Attack Packet Rate	Attack packet rate peak O pps
10 Mbps			10 pps	
8 Mbps	2022-02-17 16:45		8 pps	
6 Mbps	- 0 Mbps		6 pps	
4 Mbps			4 pps	
2 Mbps			2 pps	
2022-02-17 16:30 2022-02-17	1645 2022-02-17 17:00 2022-02-17 17:15	2022-02-17 17:30	2022-02-17 16:30 2022-02-17 16:45 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。
- 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					
Instance ID	Attacked IP	Start Time	Duration	Attack Status 🔻	Operation
bgpir		2022-02-16 04:07:00	2 mins	Attack ends	Unblock View Details Packet Download
bgpir		2022-02-14 17:35:00	2 mins	Attack ends	Unblock View Details Packet Download
bgpli		2022-02-13 12:05:00	2 mins	Attack ends	Unblock View Details Packet Download
b x	Concerning States	2022-02-11 23:15:00	2 mins	Attack ends	Unblock View Details Packet Download
bg		2022-02-10 12:54:00	2 mins	Attack ends	Unblock View Details Packet Download
Total items: 18					

• 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。

Att	ack 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。
- 攻击包协议分布: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,所选择的高防包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中国内地(大陆)、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									
S 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	Ċ

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。



🖏 All Regions 👻 🔇	All Lines V Please select	v Last 1 Hour	Last 6 Hours	Today	Last 7 Days	Last 15 days	Last 30 Day	s 2022-01-18 00:00 ·	2022-02-17 23:59	Ħ			
CC Attack Trend Unit: qps			Atta	ck Request Per 765 gps	ak	CC Attack Tre Unit: Times	nd					Total Reque	st Peak 201 times
10,000 8,000 6,000 4,000 2,000						5,000,000 4,000,000 3,000,000 2,000,000 1,000,000							
2022-01-18 00:00	2022-01-24 00:00 2022-01-30 00:00 — Total request rate —	2022-02-05 00:00 - Attack request rate	2022-02-11 00:0	0 2022-02	-17 00:00	2022-01-18 (00:00	2022-01-24 00:00	2022-01-30 00:0 — Total requests	00 <u> </u>	2022-02-05 00:00 tck requests	2022-02-11 00:00	2022-02-17 00:

字段说明:

- 总请求速率:统计当前,高防包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,高防包接收到的总请求数量。
- 攻击请求次数:统计当前, 高防包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。

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
bgpi					2022-02-17 13:37:00	1 mins	Attack ends	View Details
bgi			10000	(100 C)	2022-02-17 12:41:00	1 mins	Attack ends	View Details



使用限制

最近更新时间:2020-07-07 16:04:04

防护对象限制

DDoS 高防包仅适用于腾讯云产品,包含云服务器、负载均衡、NAT 网关等。

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个 IP 地址。
- CC 黑白 IP 名单、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。



实例管理 查看实例信息

最近更新时间:2022-04-22 11:29:31

您可以通过 DDoS 防护管理控制台查看所购买的 DDoS 高防包的基础信息(如实例保底防护峰值、运行状态)及实例的弹性防护配置。

操作步骤

示例:查看广州地区独享包实例"bgp-0000008o"的实例信息。

1. 登录 DDoS 高防包(新版)管理控制台,在左侧导航栏中,单击【高防包】,找到实例 ID 为"bgp-00000080"的 高防包,单击 ID"bgp-00000080"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
🔇 All Regions 🔻						Nam	e v Please	enter the co Q
ID/Name	Protected IP	Specifications	Status T	Defense Status	Attacks in last 7 days	Date		Operation
bgp-000001da waf ℯ* None ℯ*	Not bound	Region: Guangzhou Package type: Standard Package (BGP) IPs allowed: 100 application bandwidth: 1000Mbps	Status: • Running Remaining protection times: Unlimited Protected IPs: 0	IP/Port Protection: Loose Configuration Domain Name Protection: Disable Configuration	0 times 🗠	Purchase tin	ne: 2022-04-06	Protected Resource Configurations View Report
bgp-000001d8 Not named p* None p*	ot bound	Region: Guangzhou Package type: Standard Package (BGP) IPs allowed: 10 application bandwidth: 100Mbps	Status: • Running Remaining protection times: Unlimited Protected IPs: 0	IP/Port Protection: Medium Configuration Domain Name Protection: Disable Configuration	0 times 🗠	Purchase tin	ne: 2022-03-24	Protected Resource Configurations View Report

2. 在弹出的页面中查看如下信息:

bgp-000000co				
Basic Information				
Anti-DDoS Pro instance name	test 🖋	Current Status	Running	
Location	Beijing	Expiry Time	2020-07-26	
Bound IP	49.232.199.28, 49.232.127.41, 49.233.50.203			
Base Protection Bandwidth	30 Gbps			

参数说明:

• 高防包名称

该 DDoS 高防包实例的名称,用于辨识与管理 DDoS 高防包实例。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

购买 DDoS 高防包 时选择的【地域】。

• 绑定 IP

该 DDoS 高防包实例所防护业务的实际 IP。

• 保底防护峰值

该 DDoS 高防包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 高防包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。

标签

表示该 DDoS 高防包实例所属的标签名称,可以编辑、删除。



管理防护对象

最近更新时间:2023-06-25 14:42:30

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

- 1. 登录 DDoS 高防包(新版)管理控制台,在左侧导航中,单击云上防护实例。
- 2. 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。

Purchase instance							S All regions 🔻	All instances	Name Please e	nter the conten 🛛 🔍
Instance ID/Nam	Instance type	IP Protocol	Access Resources (j)	Specifications	Specifications	Defense Status (j)	Instance T	Attacks in	Date	Operation
	Anti-DDoS Pro	IPv4		Region: Package type: application bandwidth:	Protection Ability: Full protection	Port protection: Medium 🎤	Ø Running	0 times	Purchase time: 2023-06-08	Protected Resource Configurations

- 3. 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按钮,将资源从高防包的防护对象中删除。

Protected Resource	
Note: Configured protection policy only works to the currently bound IP. If the current curr	ne protection policy is not applicable to the current IP, please change it.
IP/Resource name Region Plan information Enterprise Edition High Defense Package Max bound IP	
Device type	Selected (1)
Please enter IP (exact search is supported, fuzzy search is not supported; Q	Resource ID/Name IP address Resource type
Resource ID/Name IP address Resource type No data yet	
	\leftrightarrow
Total items: 0 10 🗸 / page 📕 4 1 / 1 page 🕨 🕨	
You can make multiple selection by holding down the Shift key OK	Cancel

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:2020-07-07 16:04:05

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

前提条件

设置防护对象 IP, 您需要成功 购买 DDoS 高防包。

操作步骤

方式一

1. 登录 DDoS 高防包(新版)管理控制台,在左侧导航中,选择【高防包】。

2. 单击目标实例的"ID/名称"列的第二行编辑按钮, 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	Protected IP	Specifications
bgp-00000cn test	1.1.1.240	Region: Guangzhou Package type: Standard pack IPs allowed: 5

方式二

- 1. 登录 DDoS 高防包(新版)管理控制台,在左侧导航中,单击【高防包】。
- 2. 在下方实例列表中,单击目标实例的"ID/名称"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,单击高防包名称右侧的编辑铅笔按钮,输入名称。

Basic Information	
Anti-DDoS Pro instance name	test 🧨
Location	Guangzhou
Bound IP	1.1.1.240
Base Protection Bandwidth	30 Gbps

名称长度为1-20个字符,不限制字符类型。



业务接入 IP 透明接入

最近更新时间:2024-01-24 15:12:09

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。



() 注意: 已配置的	财护策略仅对当前绑	定的IP生效,如存在防护领	策略不适用于	当前IP,请前往修改。	
选择防护实例		•			
地域					
套餐信息 标准	售餐(BGP)				
防护IP规格数 剩余市	可防护 8 个/共 10 个				
业务规模					
防护资产类型 云	主机	~			
选择资源实例 ()				已选择 (2)	
请输入IP或名称(支持			Q	资源ID/实例名	
资源ID/实例名	IP地址	资源类型			
		云主机	^		
		云主机			
		- 210		\leftrightarrow	
		云主机		\leftrightarrow	
		云主机 云主机		↔	
		云主机 云主机 云主机		↔	

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:2024-01-24 15:13:57

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	IP接入()
	域名业务报 如果您的业绩 业务抵御DD 到目标源站朋	₹入 各为网站类业务,同 0S及CC攻击,根 股务器,可针对已有	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 居您配置的规则,业务流量会先经过DDoS高防进行清洗,再回源 与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	
1 选择实例	> 2 协议端口 > 3 回源方式 > 4 修改DNS解析
	通过Cname地址 转发端□ 源站端□ 用户 安全实例 转发协议 源站服务器 或通过A记录 高防IP 源站IP
★ 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	
✓ 选择实例	> 2 协议端口 > 3 回源方式 > 4 修改DNS解析
	通过Cname地址 转发端口 源站端口 用户 安全实例 转发协议 源站服务器 或通过A记录 高防IP 源站IP
★ 转发协议	 ✓ http 80 ✓ https 443 仅支持标准协议端口(http:80、https:443),如需添加除80、443以外的非标准端口,请通过工单联系客服进行制
	https使用http协议回源
★ 选择证书	清选择
证书来源	腾讯云托普证书SSL证书管理 ☑ ♀ (证书作用:保证用户机密信息安全,防止用户信息、财务信息等重要数据被窃取或篡改)
★ 业务域名	域名长度不超过67
推荐开启防护曹	記置 ✓ 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。



─ 选择买例	>	💛 协议端口 🛛 👌	3 0	源方式 > (4)修改DNS解析
	用户 —	通过Cname地址 或通过A记录	→ 安全实例	转发端口 转发协议 高防IP ◀	→ 源站端口 源站服务 ····• 源站IP
* 回源方式		原 🗌 域名回源			
	回源方式	: 清洗后的干净业务流量可通	过IP、或名两种	方式访问源站服务器	
★ 源站IP+端口	回源方式 源站IP	: 清洗后的干净业务流量可通	辺IP、或名两种 源站端口	方式访问源站服务器	
★ 源站IP+端口	回源方式 源站IP 示例	: 清洗后的干净业务流量可通 : 1.1.1.1, 请根据实际源站填	辺IP、 域名两种 源站端口 写 示例:	 方式访问源站服务器 80 删除 	

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,建议低峰期更新。

开始接入 批	圭 导入 批量导出	批量删除						请输入业务均	战名/高防IP
业务域名	转发协议	转发端口	源站IP/站点	关联高防IP	健康检查	接入状态	CC防护状态	修改时间	操作
	http	80			关闭 配置 ① 因所说	<mark>配置失败</mark> 选证书获取失败,请到 <mark>SSL证</mark>	严格配置	2022-04-18 17:17:39	配置 删除
	https	443			关闭配置 ①	配置失败()	关闭 配置	2022-04-14 20:24:27	配置 删除
- 2010	https	443	1.1		关闭 配置 🚯	成功	关闭 配置	2022-04-14 19:31:08	配置 删除
27	http	880	10.00		关闭 配置 ①	成功	关闭 🔵 🛈	2022-04-14 19:28:58	配置 删除



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。

开始接入	批量导入	、批畫	重导出	批量删除					CNAME	Ŧ	请输入要查询的内容
业务域名	转发协议	转发端口	源站IP/	关联高防资源		健康检查	会话保持	接入状态	CC防护社	态	修改时间
					mc	关闭 配置 🚯	关闭 编辑	☞ 成功	宽松 配置	ł	
					γm	关闭 配置 🛈	关闭 编辑	☞ 成功	宽松 配置	ł	

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	by 3 () 最多可添加 200 条规则,已添加 39 条
域名	ti an 请输入域名,长度不超过67
协议	http Ohttps 443
	✓ https使用http协议回源
证书来源	腾讯云托管证书SSL证书管理 🗹 🗘
证书	请选择 ▼
回源方式	IP回源 域名回源
源站IP	源站IP 源站端口
	删除
	+添加
	注意:请输入源站IP+端口,最多支持16个
	备用源站

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。



开始接入	批量导入	批量	导出	批量删除					CNAME	Ŧ	请输入要查询的内容	Q
业务域名	转发协议	转发端口	源站IP/	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
					σm	关闭 配置 ()	关闭 编辑	☞ 成功	宽松 配	置		配置 删除
)m	关闭 配置	关闭 编辑	☞ 咸功	宽松 配	置		配置 删除

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。

开始接入	批量导)	批畫	重导出	批量删除				CNAME -	请输入要查询的内容		Q,
- 业务域名	转发协议	转发端口	源站IP/	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	
				om	开启 配置 ①	关闭 编辑	☞ 成功	宽松 配置	2 2 1	配置 删除	
				om	关闭 配置 ①	关闭 编辑	☞ 成功	宽松 配置		配置 删除	
e e				mc	关闭 配置 ③	关闭 编辑	☞ 成功	宽松 配置	2 2 1	配置 删除	

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:2024-01-24 15:15:12

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**。

业务接入					⊙ 显示接入诊
IP透明接入	端口接入	域名接入	IP接入 (i)		
开始接入					请输入IP
71341507					

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	DP或名称	Ŧ		
绑定实例类型 🛛 🔵 云主机	◯ 负载均衡			
⑤ 中国香港 ▼				
请输入实例ID或IP信息				Q,
实例ID/名称	可用区	内网IP	已绑定普通公网IP	
	中国香港			•
	中国香港			
共 28 条		10 * 条	/页 🛛 🚽 1 /3页 🕨	M

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						連邦	俞入IP
实例ID/名称	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
b t		负载均衡		 运行中 	● 绑定中	2023-(删除
	2	云主机	ins-oo5a6jg1	• 运行中	• 已绑定	2023-0	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:2024-01-24 15:24:29

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	ŧ入	
	如果您的业务	8是非网站业务,如 #发切则 相据您题	U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 BB665切则
	的方式添加# 源站服务器,	可针对已有规则进	12頁的规则,並旁流重去无经过DD0S局的进行清洗,再回源到目标 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。



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	
	用户	通过Cname地址 或通过A记录	•••••	转发端[安全实例 高防IP	转发	→ 源站端口 か议 → 源站服务 → 源站IP	
★ 关联实例ID	b <u>ç</u>			,			

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						
🗸 选择实	列 >	2 协议端口	>	③ 回源方式	>	4 修改DNS解析
	用户	通过Cname地址 或通过A记录		转发端口 安全实例 高防IP	转发	····· · 源站端口 协议 ······ · 源站服务器 ····································
* 转发协议		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	
🗸 选择实例	> 🗸 协议端口 > 3 回源方式 > 4 修改DNS解析
	通过Cname地址 转发端口 源站端口 用户 安全实例 转发协议 源站服务器 或通过A记录 高防IP ************************************
* 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 ① 示例: 1.1.1, 请根据实际源站填写 0~100
	+ 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 批量导出 批量删除						多个关键字用竖线 17 分隔			
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	554	554	106.55.58.59	lbj98qig.dayugslb.co m	加权轮询	关闭 編攝 🛈	关闭 编辑	2023-06-26 19:09:04	
TCP	1888	80	106.55.58.59	lbj98qig.dayugslb.co	加权轮询	关闭 編輯 🛈	关闭 编辑	2023-06-26	

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	וַאָּן
	Ā
· 主义证() 端口接/	↑ 、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	J (j)
ł	最多可添加 200 条规则,已添加 39 条
转发协议	UDP v
转发端口	
源站端口	
回源方式	IP回源 域名回源
负载均衡方式	加权轮询
源站IP+权重	源站IP 权重 ①
	100 删除
	+添加
ž	主意: 请输入源站IP+权重, 最多支持20个
[备用源站



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。

开始接入	批量导)	、 批量导出	批量删除		多个关键字用竖线" "分隔				
							选择资源属性进行过滤		
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	源站IP/域名	收时间	搷
				0			源站端口	2	
UDP					加权轮询	关闭编辑 (1)	关联高防IP	(Ē
							转发协议	25	
TCP					加权轮询	关闭编辑 (1)	转发端口	0	A
							关联高防资源(CNAME)	0	
UDP					加权轮询	关闭编辑 🛈	关闭 编辑 1	8	Ē

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。

开始接入	批量导)	入 批量导出	批量删除			多个关键字用竖线	ŧ " " 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	
UDP					加权轮询	关闭 编辑 🛈	关闭 编辑		配置删除	
TCP)	加权轮询	关闭 编辑 🛈	关闭 编辑	2	配置 删除	

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。

开始接入	批量导入批量导行	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
JDP	-		þ	加权轮询	关闭编辑 ()	关闭 编辑	21 11	配置 删除
🔽 ТСР	1		0	加权轮询	关闭 編攝 🛈	关闭 编辑	21 1!	配置删除
UDP	£			加权轮询	关闭 編輯 🛈	关闭 编辑	2(1{	配置 删除



2. 在删除规则弹窗,单击删除,即可删除所选规则。



防护配置 AI 防护

最近更新时间:2022-04-28 16:03:14

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 高防包,并设置防护对象。

操作步骤

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

2. 在 DDoS 防护页面的左侧列表中,选中高防包 ID,如"bgp-00xxxxx"。

IP v Q	IP/Port Protection Domain name protection
	DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support. Strict OMedium Coose







端口过滤

最近更新时间:2022-07-06 14:43:41

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。

前提条件

您需要成功 购买 DDoS 高防包,并设置防护对象。

操作步骤

- 1. 登录 DDoS 高防包控制台,在左侧导航中,单击防护配置 > DDoS 防护。
- 2. 在 DDoS 防护页面的左侧列表中,选中高防包 ID,如"bgp-00xxxxx"。

IP v Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support. Strict O Medium Loose

3. 在端口过滤卡片中,单击设置,进入端口过滤页面。

Configurations	: E Single Setting Mod
DDoS Protection CC Protection Protection Flow Non-website/port application Different protection policies are applicable to different engine User Website/domain mane applications DoS Engine Feal Server Different protection policy is applicable to the Anti-DDoS engine	s: Why are there limits on the manual unblocking times? And what are the limits? View A e, and How can Longer to a blocket server? What if my business IP is blocked for attack defense?
Protection Policy (1) 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
Set	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。

Create Port Filtering Policy		>
Associate Anti-DDoS Advanced	bg	
Protocol	All Protocols 💌	
Source Port Range	Starting Source - Ending Source	
Destination Port Range	Starting Destin - Ending Destina	
Action	Discard 💌	
	Confirm Cancel	

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。

Create					Enter IP	Q,
Associated Resource	Protocol	Source Port Range	Destination Port Range	Action	Operation	
bgpip	тср			Discard	Configuration Delete	



DDoS 防护等级

最近更新时间:2022-07-06 14:29:20

本文档将为您介绍针对 DDoS 攻击, DDoS 高防包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 高防包服务提供防护策略调整功能,针对 DDoS 攻击提供三种防护等级供您选择,各个防护等级的具体防护操作如下:

- 宽松防护
- 适中防护
- 严格防护

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

说明:

- 如果您的业务需要使用 UDP, 建议您联系 腾讯云技术支持 进行策略定制, 以免严格模式影响业务流程。
- 默认情况下,您所购买的 DDoS 高防包实例采用"适中"防护等级。
- 在以下情况可能发生短暂的秒级攻击透传到源站:切换防护等级或遭攻击时接入高防包。

前提条件

您需要成功 购买 DDoS 高防包,并设置防护对象。

操作步骤



- 1. 登录 DDoS 高防包控制台,在左侧导航中,单击防护配置 > DDoS 防护。
- 2. 在 DDoS 防护页面的左侧列表中,选中高防包 ID,如"bgp-00xxxxx"。

IP ¥ Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support. Strict O Medium Loose

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:2022-04-28 16:00:52

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。

前提条件

您需要成功 购买 DDoS 高防包,并设置防护对象。

说明:

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

操作步骤

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

2. 在 DDoS 防护页面的左侧列表中,选中高防包 ID,如"bgp-00xxxxx"。

IP v Q	IP/Port Protection Domain name protection
	DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support. Strict O Medium C Loose



3. 在 IP 黑白名单卡片中,单击设置,进入 IP 黑白名单页面。

Configurations	:Ξ Single Setting Mo
DDoS Protection CC Protection Protection Flow Different protection policies are applicable to different en application User Non-website/domain name application Doos Engine User Vebsite/domain name application Doos Engine	Troubleshooting gines: Wity are there limits on the manual unblocking times? And what are the limits? View ngine, and What are the differences between Anti-DDoS Advanced and Anti-DDoS Pro? How can I connect to a blocked server? What if my business IP is blocked for attack defense? What if my business IP is blocked for attack defense?
Protection Policy ① 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
Set	Set

4. 在 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。

Create IP blacklist/whitelist	
Associate Service Packs	bgp-00000co 😢
Туре	O Blacklist O Whitelist
IP	Please enter IP addresses, separated with carriage returns
	OK Cancel

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 Black/White List				
	Create				Enter IP Q
	Associated Resource	Туре	ip	Operation	
	bgp-000000co/49.232.127.41,49.232.199.28,49.233.50.203	Blacklist	1.1.1.6	Delete	
	Total items: 1			10 🔻 / page	I I /1 page ► ►



IP 端口限速

最近更新时间:2022-04-28 15:59:50

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。

前提条件

您需要成功 购买 DDoS 高防包,并设置防护对象。

操作步骤

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

2. 在 DDoS 防护页面的左侧列表中,选中高防包 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。



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。

Create IP/Port Speed	Limit	×
	*	
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 Cancel	

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



协议封禁

最近更新时间:2023-06-08 16:57:00

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。

前提条件

您需要成功 购买 DDoS 高防包,并设置防护对象。

操作步骤

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

2. 在 DDoS 防护页面的左侧列表中,选中高防包 ID,如"bgp-00xxxxx"。

IP v Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support. Strict O Medium C Loose

3. 在协议封禁卡片中,单击**设置**,进入协议封禁页面。

Protection Policy ①	
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
Set	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
Set	① This is a value-added feature. Please contact your after-sales rep if necessary.



4. 在协议封禁页面,单击新建,弹出新建协议封禁弹窗。

Create		
Associated Resource	Block ICMP Protocol	Block TCP Protocol

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。

Create Protocol Blocking Policy				
Associate Service Packs	Search by IP or name			
Block ICMP Protocol				
Block TCP Protocol				
Block UDP Protocol				
Block other protocols				
	Confirm			



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

,修改协议封禁规则开关。

Associated Resource	Block ICMP Protocol	Block TCP Protocol	Block UDP Protocol	Block other protocols	Operation
bg,	Disable	Disable	Disable	Disable	Configuration



特征过滤

最近更新时间:2022-04-28 15:58:55

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。

前提条件

您需要成功 购买 DDoS 高防包,并设置防护对象。

操作步骤

- 1. 登录 DDoS 高防包控制台,在左侧导航中,单击防护配置 > DDoS 防护。
- 2. 在 DDoS 防护页面的左侧列表中,选中高防包 ID,如"bgp-00xxxxx"。

lb 🔺 Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support. Strict OMedium Coose

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.
Set	Set
Feature Filtering Configure custom blocking policy against specific IP, TCP, UDP message header or payload. Set	

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, 单击保存。

sociate Service Packs	Search by IP or name			
tar fastura				
terreature	Field	Logic	Value	
	Add			
ction	Allow OBlock	Discard Reject rec	quests and block IP for 15 mins	
	O Discard requests and b	olock IP for 15 mins	Continue Protection	

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。

ID	Associated Resource	Feature List	Action	Operation
oc		Source port equals to 100 Destination port equals to 13 Message length equals to 198	Continue Protection	Configuration Delete



连接类攻击防护

最近更新时间:2022-02-22 16:40:04

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: 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。

前提条件

您需要成功购买 DDoS 高防包,并设置防护对象。

操作步骤

- 1. 登录 DDoS 高防包控制台,在左侧导航中,单击防护配置 > DDoS 防护。
- 2. 在 DDoS 防护页面的左侧列表中,选中高防包 ID,如"bgp-00xxxxx"。

IP × Q	IP/Port Protection Domain name protection
	 DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support. Strict O Medium Loose



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。

igurations	🗮 Single Setting M
SP Protection CC Protection tion Flow Non-website/port applicable Website/domain name applications Different protection policy is applicable to the Anti-DDoS engine,	Troubleshooting Why are there limits on the manual unblocking times? And what are the limits? View and What are the differences between Anti-DDoS Advanced and Anti-DDoS Pro? How can I connect to a blocked serve? What if my business IP is blocked for attack defense?
Perform Policy ① Perform Policy ① 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
Set	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
Set	() This is a value-added feature. Please contact your after-sales rep if necessary.
Connection Attack Protection Set refined protection policies targeting connection attacks	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.

4. 在连接类攻击防护页面中,单击新建,弹出配置连接类攻击防护弹窗。



5. 在配置连接类攻击防护弹窗中,开启连接耗尽防护和异常连接防护后,单击确定。

Configure Connection Attack Protection	×
Associate Service Packs	
Connection Flood Protection	
Source New Connection Rate Limit	
Source Concurrent Connection Limit	
Destination New Connection Rate Limit	
Destination Concurrent Connection Limit	
Abnormal Connection Protection (i)	
Maximum Source IP Exceptional Connections	
Confirm 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
	Disable	Disable	Disable	Disable	Disable	Configuration



区域封禁

最近更新时间:2022-02-22 16:40:04

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。

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 高防包,并设置防护对象。

操作步骤

- 1. 登录 DDoS 高防包控制台,在左侧导航中,单击防护配置 > DDoS 防护。
- 2. 在 DDoS 防护页面的左侧列表中,选中高防包 ID,如"bgp-00xxxxx"。

DDoS Protection CC Protection		
Protection Flow application User User Website/domain name applications DDoS Engine CC Engine Real Serv	Troubleshooting Different protection policies are applicable to different engines: Why are there limits on the manual unblocking times? And what are the limits? IP/port protection policy is applicable to the Arti-DDDS engine, and the domain name protection policy is applicable to the CC How can i connect to a blocked server? Attack-related FAQ Attack-related FAQ protection engine.	View A
P ▼ Q	For details about configuring domain name protection, contact your sales rep C C Protection and Ceansing Threshold () CC protection detects mail/outs behaviors according to access modes and connection status. In Lose 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. If attack requests all ele blocked in the Strict mode, all suspicious requests are blocked. If attack requests all ele blocked in Strict mode, all suspicious requests are blocked. If attack requests all ele blocked in Strict mode, all suspicious requests are blocked. If attack requests all ele blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked. If attack requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked. If attack requests are blocked in Strict mode, all suspicious requests are blocked in Strict mode, all suspicious requests a	



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. 在区域封禁页面中,单击新建,弹出新建区域封禁弹窗。
- 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	king Policy			×
Associate Service Packs	Search by IP or name			
Blocked Areas	O China Outside China	Custom		
		Confirm	Cancel	

6. 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。





查看操作日志

最近更新时间:2023-04-20 16:37:23

应用场景

DDoS 高防包支持查看近90天内重要操作的日志,如有需要,您可以登录 DDoS 高防包操作日志界面查看。可查看的日志包含以下类别:

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

操作步骤

- 1. 打开 DDoS 高防包(新版) 操作日志 界面。
- 2. 设置时间范围,查询相关操作记录。

ration Logs						Pu
Today Yesterday	Last 7 days Last 30 da	ays 2020-07-06 00:00 ~ 2020-0	7-06 23:59			
Operation Time	Object ID	Product Type	Action	Result	Operator Account	Operation
2020-07-06 16:15:53	455	Service Packs	CreateInstanceName	Success	100001500880	Unfold
Total items: 1					10 🔻 / page	 ✓ 1 /1 page ▶ ▶





封堵相关操作 设置安全事件通知

最近更新时间:2022-05-09 17:02:32

应用场景

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 高防包(新版)控制台,在左侧导航中,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 清洗流量告警"。



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。



• 设置单 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		
	bgp-000000co	49.232.199.28;49.233.50.203;49.232.127.41	101	Modify		
	bgp-000000cn	1.1.1.240	101	Modify		
	bgp-000000cm	2402:4e00:1400:e57b:0:8f9c:903:5e6e;118.89.113.189	200	Modify		
	Total items: 3			10 ▼ / page 🛛 🛤 🔌	1 / 1 page >	н

• 设置 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	
	bgp-000000co	49.232.199.28;49.233.50.203;49.232.127.41	Not set	Modify	
	bgp-000000cn	1.1.1.240	Not set	Modify	
	bgp-000000cm	2402:4e00:1400:e57b:0:8f9c:903:5e6e;118.89.113.189	Not set	Modify	
	Total items: 3			10 v / page H K 1 /1 page > >	M

• 设置 CC 清洗流量告警

← CC Traffic Cle	eansing Alarm			
	Batch Modify			Enter the IP to be qi Q
	Resource Instance	Bound IP	Cleansing Threshold (in QPS)	Operation
	bgp-000001bt	162.62.190.169	20	Modify
	bgp-000001bs	119.91.77.141	20	Modify
	bgp-0000016m	119.91.82.253	Not set	Modify
	bgp-000000ij	111.230.63.220	1	Modify
	Total items: 4			10 ▼ / page H 4 1 /1 page H H

设置通知方式

1. 登录您的腾讯云账号, 进入 消息中心。

说明:



		1			
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。

i Please	e make sure that the user's email and r	nobile are verified by Tencent Cloud, a	Ind the responding method is enabled.		
ssage Type sipients	Attack notifications User User Group	Add Messa	ge Receiver 🔽 Modify User Information 🗹	1 selected	
	Search for user name	Matthe Manufact	Q	8163196@qq.com	>
	 User Name 8163196@qq.com 	Mobile Number	email 81*****@qq.com		
	v_szgwu	⊘ 188****5245	⊘ v_*****@tencent.com		
				↔	



连接已被封堵的服务器

最近更新时间:2021-08-26 11:51:18

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 17:19:44

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

无需等待时间,可提前解除封堵。具体操作如下:

说明:

- DDoS 高防用户:每天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。
- 攻击如果持续进行未停止,则无法进行解封,需等待攻击结束自助解封或自动解封。
- 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。
- 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。