

Anti-DDoS 流量清洗

常见问题

文档版本 06
发布日期 2021-10-09



版权所有 © 华为技术有限公司 2021。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 产品咨询类	1
1.1 什么是 Anti-DDoS 流量清洗?	1
1.2 什么是 SYN Flood 攻击和 ACK Flood 攻击?	1
1.3 什么是 CC 攻击?	1
1.4 什么是慢速连接攻击?	2
1.5 什么是 UDP 攻击和 TCP 攻击?	2
1.6 如何理解“百万级的 IP 黑名单库”?	2
1.7 Anti-DDoS 的触发条件是什么?	2
1.8 Anti-DDoS 流量清洗进行防御时对正常业务有影响吗?	2
1.9 Anti-DDoS 清洗机制是怎样的?	2
1.10 Anti-DDoS 流量清洗服务有何使用限制?	3
1.11 Anti-DDoS 流量清洗免费提供多大的防护能力?	3
1.12 Anti-DDoS 流量清洗可以提供哪些数据?	3
1.13 Anti-DDoS 流量清洗服务支持哪些地区的防护?	3
1.14 华为云为用户免费提供的最大防护能力是多少?	3
1.15 哪些业务可以使用 Anti-DDoS 流量清洗服务?	3
1.16 Anti-DDoS 是否支持跨云使用?	3
1.17 如何判断是否有攻击发生?	4
2 基本功能类	5
2.1 什么是区域和可用区?	5
2.2 调整 Anti-DDoS 防护策略中, HTTP 请求速率指什么?	6
2.3 当遭受超过 500Mbps 的攻击时如何处理?	6
2.4 Anti-DDoS 流量清洗服务能帮助缓解哪些类型的攻击?	6
2.5 当业务经常被 DDoS 攻击时如何处理?	7
2.6 ELB 防护和 ECS 防护有什么区别?	7
2.7 为什么同一个公网 IP 地址的清洗次数和攻击次数不一致?	7
2.8 Anti-DDoS 攻击防护是不是默认开启的?	7
2.9 Anti-DDoS 防护是一个区域, 还是用户的单个 IP?	7
2.10 用户注销帐号是否需要清理 Anti-DDoS 流量清洗服务的资源?	7
2.11 如何查看 Anti-DDoS 流量清洗次数?	8
2.12 如何查看 Anti-DDoS 防护统计信息?	8
2.13 Anti-DDoS 如何查看公网 IP 监控详情?	8
2.14 如何查看 Anti-DDoS 拦截报告?	8

2.15 是否能彻底关闭流量清洗功能?	8
2.16 如何判断入网流量是否经过了 Anti-DDoS 流量清洗服务?	8
3 阈值及黑洞类.....	10
3.1 Anti-DDoS 流量清洗阈值指什么?	10
3.2 华为云黑洞策略是怎么样的?	10
3.3 Anti-DDoS 流量清洗阈值如何设置?	10
3.4 如何调整封堵阈值?	11
3.5 IP 被黑洞封堵, 怎么办?	11
4 告警通知类.....	13
4.1 攻击事件能否及时通知?	13
4.2 用户收到告警通知, 是否正常?	13
4.3 如何取消 Anti-DDoS 告警通知?	13
A 修订记录.....	16

1 产品咨询类

1.1 什么是 Anti-DDoS 流量清洗？

Anti-DDoS流量清洗服务（以下简称Anti-DDoS）为公网IP提供四到七层的DDoS攻击防护和攻击实时告警通知。同时，Anti-DDoS可以提升用户带宽利用率，确保用户业务稳定运行。

Anti-DDoS通过对互联网访问公网IP的业务流量进行实时监控，及时发现异常DDoS攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。同时，Anti-DDoS为用户生成监控报表，清晰展示网络流量的安全状况。

1.2 什么是 SYN Flood 攻击和 ACK Flood 攻击？

SYN Flood攻击是一种典型的DoS（Denial of Service）攻击，是一种利用TCP协议缺陷，发送大量伪造的TCP连接请求，从而使被攻击方资源耗尽（CPU满负荷或内存不足）的攻击方式。该攻击将使服务器TCP连接资源耗尽，停止响应正常的TCP连接请求。

ACK Flood攻击原理与SYN Flood攻击原理类似。

ACK Flood攻击是指攻击者通过使用TCP ACK数据包使服务器过载。像其他DDoS攻击一样，ACK Flood攻击的目的是通过使用垃圾数据来减慢攻击目标的速度或使其崩溃，从而导致拒绝向其他用户提供服务。目标服务器被迫处理接收到的每个ACK数据包，消耗太多计算能力，以至于无法为合法用户提供服务。

1.3 什么是 CC 攻击？

CC攻击是攻击者借助代理服务器生成指向受害主机的合法请求，实现DDoS和伪装攻击。攻击者通过控制某些主机不停地发送大量数据包给对方服务器，造成服务器资源耗尽，直至宕机崩溃。例如，当一个网页访问的人数特别多的时候，用户打开网页就慢了，CC攻击模拟多个用户（多少线程就是多少用户）不停地访问需要大量数据操作（需要占用大量的CPU资源）的页面，造成服务器资源的浪费，CPU的使用率长时间处于100%，将一直在处理连接直至网络拥塞，导致正常的访问被中止。

Anti-DDoS通过设置“CC防护”控制HTTP请求速率。

1.4 什么是慢速连接攻击？

慢速连接攻击是CC攻击的变种，该攻击的基本原理说明如下：

对任何一个允许HTTP访问的服务器，攻击者先在客户端上向该服务器建立一个content-length比较大的连接，然后通过该连接以非常低的速度（例如，1秒~10秒发一个字节）向服务器发包，并维持该连接不断开。如果攻击者在客户端上不断建立这样的连接，服务器上可用的连接将慢慢被占满，从而导致服务器拒绝用户正常的访问申请。

1.5 什么是 UDP 攻击和 TCP 攻击？

UDP攻击和TCP攻击是攻击者利用UDP和TCP协议的交互过程特点，通过僵尸网络，向服务器发送大量各种类型的TCP连接报文或UDP异常报文，造成服务器的网络带宽资源被耗尽，从而导致服务器处理能力降低、运行异常。

1.6 如何理解“百万级的 IP 黑名单库”？

百万级的IP黑名单库是指Anti-DDoS基于多年积累的DDoS防护经验，搜集的恶意IP数量已达到百万级别。当用户的业务受到这些恶意IP攻击时，Anti-DDoS可以快速响应，及时为用户提供DDoS攻击防护服务。

1.7 Anti-DDoS 的触发条件是什么？

Anti-DDoS检测到IP的入流量超过“防护设置”页面配置的“流量清洗阈值”时，触发流量清洗。

- 当实际业务流量触发该阈值时，Anti-DDoS仅拦截攻击流量。
- 当实际业务流量未触发该阈值时，无论是否为攻击流量，都不会进行拦截。

您可以根据实际情况调整Anti-DDoS流量清洗阈值，具体操作请参考[配置Anti-DDoS防护策略](#)。

1.8 Anti-DDoS 流量清洗进行防御时对正常业务有影响吗？

Anti-DDoS流量清洗不影响正常流量。

1.9 Anti-DDoS 清洗机制是怎样的？

Anti-DDoS检测到IP的入流量超过“防护设置”页面配置的“流量清洗阈值”时，触发流量清洗。

您可以[查看拦截报告](#)，查看所有公网IP的防护统计信息，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10排名和共拦截攻击次数。

1.10 Anti-DDoS 流量清洗服务有何使用限制？

提供最高500Mbps的DDoS攻击防护。

系统会对超过黑洞阈值的受攻击公网IP进行黑洞处理，正常访问流量会丢弃；对于可能会遭受超过500Mbps流量攻击的应用，建议您购买华为云DDoS高防服务，提升防护能力。

1.11 Anti-DDoS 流量清洗免费提供多大的防护能力？

Anti-DDoS免费提供最大500Mbps的防护能力（视华为云可用带宽情况）。对于可能会遭受超过500Mbps流量攻击的应用，建议您购买华为云DDoS高防服务，提升防护能力。

1.12 Anti-DDoS 流量清洗可以提供哪些数据？

- 您可以[查看Anti-DDoS监控报表](#)，查看单个公网IP的监控详情，包括当前防护状态、当前防护配置参数、24小时的流量情况、24小时的异常事件等。
- 您可以[查看Anti-DDoS拦截报告](#)，查看所有公网IP的防护统计信息，包括清洗次数、清洗流量，以及弹性云服务器、弹性负载均衡或裸金属服务器被攻击次数Top10排名和共拦截攻击次数。
- 您可以为Anti-DDoS[开启告警通知](#)，当公网IP遭受攻击时，您可以及时收到通知。否则，无论攻击流量多大，您都只能登录管理控制台自行查看，无法收到报警信息。

1.13 Anti-DDoS 流量清洗服务支持哪些地区的防护？

Anti-DDoS流量清洗服务目前仅支持对部署在华为云的业务提供防护，对于部署在非华为云的业务，无法提供防护。

华为云支持如下地区：中国-香港、亚太-曼谷、亚太-新加坡、非洲-约翰内斯堡、拉美-墨西哥城一、拉美-圣保罗一、拉美-圣地亚哥。

1.14 华为云为用户免费提供的最大防护能力是多少？

华为云为用户免费提供的最大防护能力为500Mbps。

1.15 哪些业务可以使用 Anti-DDoS 流量清洗服务？

Anti-DDoS流量清洗服务对用户购买的公网IP提供流量清洗功能。

1.16 Anti-DDoS 是否支持跨云使用？

Anti-DDoS流量清洗服务目前仅支持对部署在华为云的业务提供防护，对于部署在非华为云的业务，无法提供防护。

1.17 如何判断是否有攻击发生？

- 您可以登录华为云控制台[查看Anti-DDoS监控报表](#)，查看单个公网IP的监控详情，包括当前防护状态、当前防护配置参数、24小时的流量情况、24小时的异常事件等。
- 您可以登录华为云控制台[查看Anti-DDoS拦截报告](#)，查看所有公网IP的防护统计信息，包括清洗次数、清洗流量，以及弹性云服务器、弹性负载均衡或裸金属服务器被攻击次数Top10排名和共拦截攻击次数。

2 基本功能类

2.1 什么是区域和可用区？

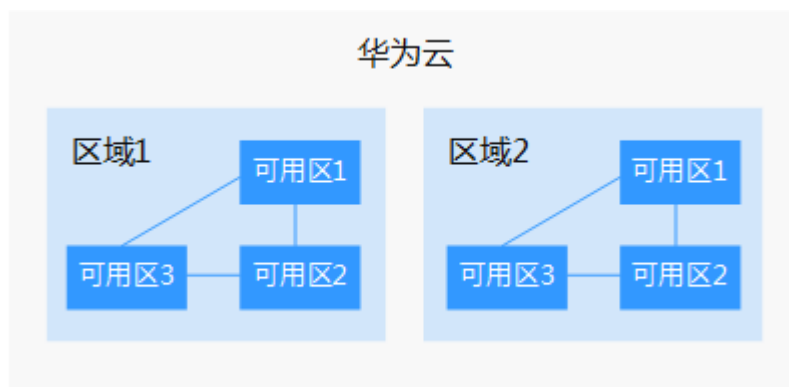
什么是区域、可用区？

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图2-1阐明了区域和可用区之间的关系。

图 2-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域？

选择区域时，您需要考虑以下几个因素：

- 地理位置

一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。不过，在基础设施、BGP网络品质、资源的操作与配置等方面，中国大陆各个区域间区别不大，如果您或者您的目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题。

- 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
- 在非洲地区有业务的用户，可以选择“南非-约翰内斯堡”区域。
- 在欧洲地区有业务的用户，可以选择“欧洲-巴黎”区域。

- 资源的价格

不同区域的资源价格可能有差异，请参见[华为云服务价格详情](#)。

如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参见[地区和终端节点](#)。

2.2 调整 Anti-DDoS 防护策略中，HTTP 请求速率指什么？

HTTP请求速率指您所部署的业务平均每秒能处理的HTTP请求个数，是按照总请求数计算的。如果Anti-DDoS检测到的总请求数超过您所设置的HTTP请求速率，就会自动开启流量清洗。

2.3 当遭受超过 500Mbps 的攻击时如何处理？

Anti-DDoS免费提供最大500Mbps的防护能力（视华为云可用带宽情况）。系统会对超过500Mbps的受攻击公网IP进行黑洞处理，正常访问流量会丢弃，建议用户购买华为DDoS高防，提升防护能力。

2.4 Anti-DDoS 流量清洗服务能帮助缓解哪些类型的攻击？

Anti-DDoS流量清洗服务可以帮助用户缓解以下攻击：

- Web服务器类攻击

SYN Flood攻击、HTTP Flood攻击、CC（Challenge Collapsar）攻击、慢速连接类攻击等。

- 游戏类攻击
UDP (User Datagram Protocol) Flood攻击、SYN Flood、TCP (Transmission Control Protocol) 类攻击、分片攻击等。
- HTTPS服务器的攻击
SSL DoS/DDoS类攻击等。
- DNS服务器的各类攻击
DNS (Domain Name Server) 协议栈漏洞攻击、DNS反射攻击、DNS Flood攻击、DNS CacheMiss攻击等。

2.5 当业务经常被 DDoS 攻击时如何处理？

当业务经常被DDoS攻击时，容易导致公网IP被拉黑，影响业务连续性，建议购买DDoS高防服务提升防御能力。

2.6 ELB 防护和 ECS 防护有什么区别？

EIP可绑定到弹性负载均衡（ELB）或弹性云服务器（ECS）上。对于Anti-DDoS流量清洗服务来说，只针对EIP进行DDoS攻击防护，ELB防护和ECS防护两者没有区别。

2.7 为什么同一个公网 IP 地址的清洗次数和攻击次数不一致？

当Anti-DDoS检测到公网IP地址被攻击时会触发一次清洗，该清洗将持续一段时间，且只清洗攻击流量，不会影响用户业务。如果在该清洗的持续时间内，同一个公网IP地址再次被攻击，该攻击将被Anti-DDoS一并清洗。因此，该公网IP地址的攻击次数增加了，但清洗次数并没有增加，用户查看到的清洗次数和攻击次数也就不一致。

2.8 Anti-DDoS 攻击防护是不是默认开启的？

是的。AntiDDoS攻击防护默认开启，使用的是默认防护策略，如果需要修改设置，请参考[配置Anti-DDoS防护策略](#)。

📖 说明

Anti-DDoS防护一旦开启，则不能关闭。

2.9 Anti-DDoS 防护是一个区域，还是用户的单个 IP？

单个IP。

2.10 用户注销帐号是否需要清理 Anti-DDoS 流量清洗服务的资源？

Anti-DDoS服务是免费服务。

- 没有资源或资源名称的概念。
- 本服务默认开通，使用时不需要购买资源，注销帐号时不需要清理资源。
- 本服务在购买公网IP时自动开启防护，不产生任何费用，用户可放心使用。

2.11 如何查看 Anti-DDoS 流量清洗次数？

您可以[查看拦截报告](#)，查看所有公网IP的防护统计信息，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10排名和共拦截攻击次数。

2.12 如何查看 Anti-DDoS 防护统计信息？

请参考[查看拦截报告](#)，查看所有公网IP的防护统计信息，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10排名和共拦截攻击次数。

2.13 Anti-DDoS 如何查看公网 IP 监控详情？

请参考[查看监控报表](#)，查看单个公网IP的监控详情，包括当前防护状态、当前防护配置参数、24小时的流量情况、24小时的异常事件等。

2.14 如何查看 Anti-DDoS 拦截报告？

请参考[查看拦截报告](#)，查看所有公网IP的防护统计信息，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10排名和共拦截攻击次数。

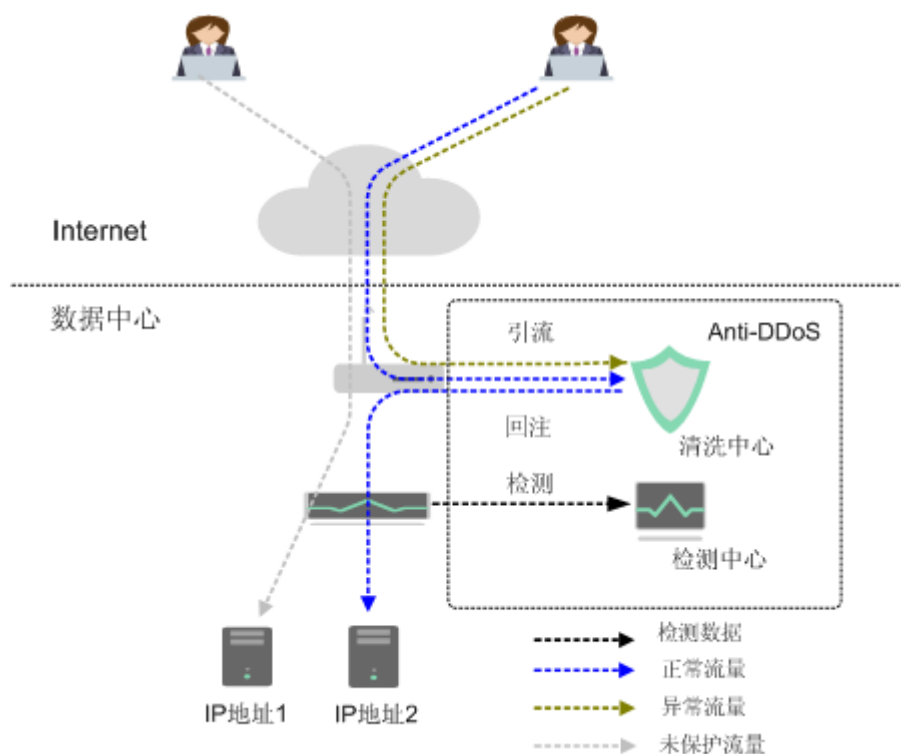
2.15 是否能彻底关闭流量清洗功能？

不能。

2.16 如何判断入网流量是否经过了 Anti-DDoS 流量清洗服务？

Anti-DDoS仅对华为云内的EIP提供DDoS攻击防护。Anti-DDoS设备部署在机房出口处，如[图2-2](#)所示。

图 2-2 网络拓扑架构图



若入网流量来自外网，则会经过Anti-DDoS流量清洗服务；若入网流量来自内网，则不会经过Anti-DDoS流量清洗服务。

- 若您从外网访问EIP，入网流量会先经过公网路由。您可以在EIP所在的虚拟机上查看一下访问的路由，若有经过公网路由，则经过了Anti-DDoS流量清洗服务。若经过了Anti-DDoS流量清洗服务，当EIP受到DDoS攻击时，会有以下信息：
 - Anti-DDoS流量清洗服务控制台会有流量清洗记录。
 - 您会收到告警提醒消息（短信或Email）。
- 若您从内网访问EIP，入网流量不会经过公网路由，不经过公网路由，则不经过Anti-DDoS流量清洗服务。

例如：您在华为云两个不同的region分别申请了一个EIP，那么两个EIP之间相互访问，则不经过Anti-DDoS流量清洗服务。

3 阈值及黑洞类

3.1 Anti-DDoS 流量清洗阈值指什么？

流量清洗阈值是触发DDoS防御动作生效的阈值，触发防御后，攻击流量将被拦截，业务流量会被正常放行。

Anti-DDoS流量清洗默认的清洗阈值为“120Mbps”，您可以根据实际业务带宽情况调整Anti-DDoS流量清洗阈值，具体操作请参考[配置Anti-DDoS防护策略](#)。

3.2 华为云黑洞策略是怎么样的？

什么是黑洞？

黑洞是指服务器（云主机）流量超过Anti-DDoS免费防护的黑洞阈值时，华为云Anti-DDoS系统屏蔽服务器（云主机）的外网访问。

华为云Anti-DDoS为什么要黑洞？

DDoS攻击不仅对用户自己的业务有影响，也会对华为云造成一定程度的影响。而且DDoS防御需要成本，其中最大的成本就是带宽费用。

带宽是华为云向各运营商购买所得，运营商计算带宽费用时不会把DDoS攻击流量清洗掉，而是直接收取华为云的带宽费用。

所以当流量超出Anti-DDoS免费防护的黑洞阈值时，华为云会屏蔽被攻击IP的流量。

黑洞规则是怎样的？

超过Anti-DDoS免费防护的黑洞阈值时，则触发黑洞。

Anti-DDoS流量清洗黑洞解封时间默认为24小时。若解封之后，系统监控到流量仍然超过免费防护的黑洞阈值，则再次触发黑洞。

3.3 Anti-DDoS 流量清洗阈值如何设置？

当您购买公网IP后，Anti-DDoS流量清洗服务自动开启防护，默认清洗阈值为“120Mbps”。

您可以根据实际业务带宽情况调整Anti-DDoS流量清洗阈值，具体操作请参考[配置Anti-DDoS防护策略](#)：

- 各攻击类型的清洗阈值会基于您的设置及业务流量自动生成，您无需关注。
- 当实际业务流量触发流量清洗阈值时，Anti-DDoS会自动清洗掉各类攻击流量，而不是直接阻断业务。

3.4 如何调整封堵阈值？

华为云为用户免费提供最高500Mbps的DDoS攻击防护（视华为云可用带宽情况），当攻击超过限定的阈值时，华为云会采取黑洞策略封堵IP，对于可能会遭受超过500Mbps流量攻击的应用，建议您购买华为云DDoS高防服务，提升防护能力。

3.5 IP 被黑洞封堵，怎么办？

原因分析

华为云为用户免费提供最高500Mbps的DDoS攻击防护（视华为云可用带宽情况），当攻击超过限定的阈值时，为了保障华为云网络的整体可用性，华为云采用黑洞策略封堵IP，对遭受大流量攻击的云主机在一定时间内限制外网通信。

处理方法

您可以通过以下两种方式，解除被黑洞封堵的IP：

- Anti-DDoS解封机制是当云主机进入黑洞24小时后，黑洞会自动解封。
若系统监控到攻击流量没有停止，依然超过限定的阈值时，IP会再次被黑洞封堵。
- DDoS高防解封机制是黑洞解封时间默认为30分钟，具体时长与当日黑洞触发次数和攻击峰值相关，最长可达24小时。如需提前解封，需要用户升级DDoS高防服务并联系华为技术人员。

Anti-DDoS流量清洗为用户提供基本防御，DDoS高防为付费增值服务，提供专家贴身保障，详细信息如[表3-1](#)所示。

表 3-1 Anti-DDoS 流量清洗和 DDoS 高防的区别

服务	Anti-DDoS流量清洗	DDoS高防
收费	免费	付费增值服务
防护能力	最高提供500Mbps防护能力	最高提供1Tbps防护能力
防护对象	仅华为云内资源	支持华为云、其他云及云下资源
防护策略	<ul style="list-style-type: none">• 防护策略固定• 基础CC防护能力• 全局通用策略	<ul style="list-style-type: none">• 防护策略丰富• 专业CC防护能力• 定制化策略

服务	Anti-DDoS流量清洗	DDoS高防
重大活动保障	无	专家服务（大客户专享）
详细报表	提供概述报表	提供详细报表
技术支持	7X24在线客服	7X24专家服务

4 告警通知类

4.1 攻击事件能否及时通知？

可以。

在Anti-DDoS流量清洗服务界面，选择“告警通知设置”页签，开启告警通知后，在受到DDoS攻击时用户会收到告警信息（通知方式由用户自行设置）。详情请参考[开启告警通知](#)。

4.2 用户收到告警通知，是否正常？

为Anti-DDoS流量清洗服务开启告警通知后，当公网IP受到DDoS攻击时用户会收到提醒消息（通知方式由用户设置，短信、Email等），属正常现象。

您可以登录管理控制台[查看弹性公网IP](#)的防护状态。

4.3 如何取消 Anti-DDoS 告警通知？

Anti-DDoS流量清洗的“告警通知”是通过“消息通知服务”发送告警通知。

当消息订阅者不需要接收“消息通知服务”推送的告警通知时，您可以取消/修改设置的Anti-DDoS流量清洗告警通知。

取消告警通知

若您不需要接收Anti-DDoS流量清洗的告警通知，可以在Anti-DDoS流量清洗的“告警通知”页签下，关闭告警通知。关闭告警通知后，您将无法收到告警信息。

步骤1 登录管理控制台。


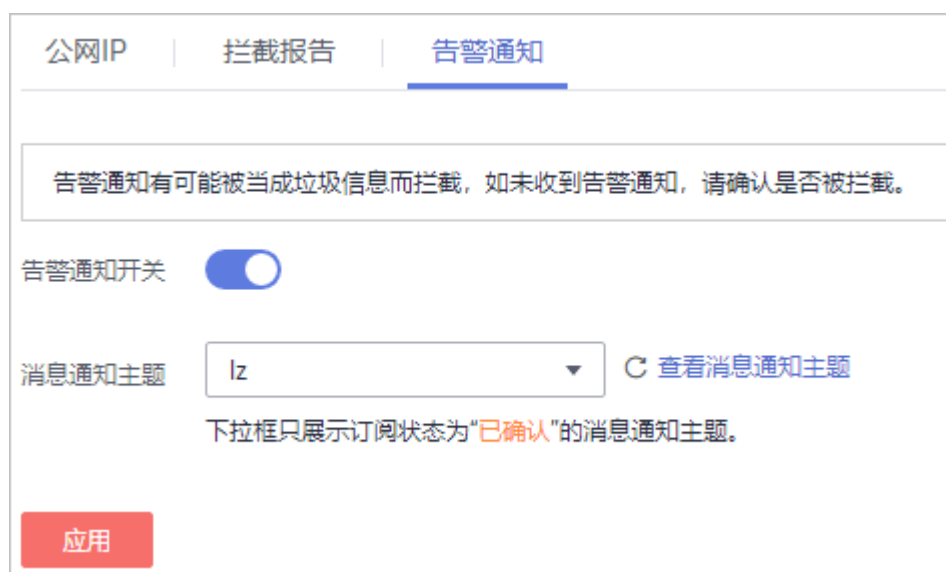
步骤2 单击页面左上方的，选择“安全与合规 > Anti-DDoS流量清洗”，进入Anti-DDoS服务管理界面。

图 4-1 Anti-DDoS 流量清洗



步骤3 选择“告警通知”页签，单击 ，关闭告警通知，如图4-2所示。

图 4-2 设置告警通知



----结束

删除订阅

如果接收告警通知的订阅终端（手机号或邮箱）变更，需要删除订阅。以“离职”为例，需要删除告警通知接收人。

例如：需要删除Anti-DDoS告警通知的消息主题名称是“antiddos-warning”，消息订阅终端是“test@example.com”。

前提条件

拥有SMN administrator权限。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择区域后，单击 ，选择“应用服务 > 消息通知服务”。

步骤3 单击“订阅”，进入订阅页面，搜索待删除订阅终端（手机号或者邮箱），如图4-3所示。

图 4-3 搜索符合条件的订阅终端



步骤4 请根据“订阅终端”和“主题名称”，确认该订阅终端接收的是Anti-DDoS流量清洗服务的告警通知。

步骤5 单击“删除”，删除订阅。

说明

删除订阅后，消息订阅者将无法接收Anti-DDoS推送的消息，请谨慎操作。

----结束

后续操作

重新添加消息订阅

如果删除离职人员的消息订阅后，需要重新为接替人员添加消息订阅，详细信息请参见[添加订阅](#)和[请求订阅](#)。

A 修订记录

发布日期	修改说明
2021-10-09	第六次正式发布。 删除“如何临时关闭Anti-DDoS防护?”。
2021-08-06	第五次正式发布。 修改管理控制台入口描述。
2020-05-27	第四次正式发布。 新增 如何取消Anti-DDoS告警通知?
2020-04-08	第三次正式发布。 新增如下常见问题： <ul style="list-style-type: none">● 华为云黑洞策略是怎么样的?● 如何取消Anti-DDoS告警通知?
2018-05-28	第二次正式发布。 新增以下常见问题： 如何临时关闭Anti-DDoS防护?
2017-12-31	第一次正式发布。