DDoS 防护 AAD

常见问题

文档版本 05

发布日期 2024-10-10

华为技术有限公司

商标声明


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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 公共问题

1.1 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1-1阐明了区域和可用区之间的关系。

图 1-1 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。
  - 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“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”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，请参阅**地区和终端节点**。

1.2 华为云黑洞策略是怎么样的?

当服务器（云主机）的流量超出基础防御阈值时，华为云将屏蔽该服务器（云主机）的外网访问，避免对华为云其他用户造成影响，保障华为云网络整体的可用性和稳定性。

什么是黑洞?

黑洞是指服务器（云主机）流量超出基础防御阈值时，华为云将屏蔽服务器（云主机）的外网访问。

为什么需要黑洞策略?

DDoS攻击不仅影响受害者，也会对华为云高防机房造成严重影响。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。华为云DDoS原生基础防护（Anti-DDoS流量清洗）服务为用户提供免费的DDoS攻击防御能力，但是当攻击流量超出Anti-DDoS流量清洗阈值时，华为云会采取黑洞策略封堵IP。

如何解除黑洞

当服务器（云主机）进入黑洞后，您可以参考**表1-1**进行处理。

表 1-1 解除黑洞方式

DDoS防护版本	解封策略	解除方法
DDoS原生基础防护（Anti-DDoS流量清洗） **说明** DDoS原生基础防护无需购买，默认开启。	• 当云主机进入黑洞24小时后，黑洞会自动解封。 • 如果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。	等待自动解封。
DDoS原生高级防护	黑洞解封时间默认为24小时。	等待自动解封。
DDoS高防	联系华为云技术支持提前解封。 建议提升弹性带宽规格避免再次封堵。	可以通过升级规格提升弹性防护带宽上限以提前解封黑洞。

1.3 DDoS 防护与 Anti-DDoS 流量清洗、DDoS 原生高级防护和 DDoS 高防是什么关系?

针对DDoS攻击，华为云提供多种安全防护方案，您可以根据您的实际业务选择合适的防护方案。华为云DDoS防护服务（Anti-DDoS Service，简称AAD）提供了DDoS原生基础防护（Anti-DDoS流量清洗）、DDoS原生高级防护和DDoS高防三个子服务。

其中，Anti-DDoS流量清洗为免费服务，DDoS原生高级防护和DDoS高防为收费服务。

三个子服务的应用场景和DDoS攻击防御能力说明如**表1-2**所示。

表 1-2 DDoS 防护方案说明

子服务	简介	应用场景	DDoS攻击防御能力
DDoS原生基础防护（Anti-DDoS流量清洗）	通过对互联网访问公网IP的业务流量进行实时监测，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。	使用华为云即可使用Anti-DDoS流量清洗服务，可以满足华为云内弹性公网IP（IPv4和IPv6）较低安全防护需求。	为普通用户免费提供500Mbps的DDoS攻击防护。
DDoS原生高级防护	为提升华为云ECS、ELB、WAF、EIP等云服务的DDoS防御能力，华为云推出DDoS原生高级防护。 DDoS原生高级防护对华为云上的IP生效，无需更换IP地址，通过简单的配置，提供的安全能力就可以直接加载到云服务上，提升云服务的安全防护能力。	DDoS原生高级防护适用于部署在华为云服务上，且华为云服务有公网IP资源的业务，能够满足业务规模大、对网络质量要求高的用户。 DDoS原生高级防护适用于具有以下特征的业务： ● 偶尔遭受DDoS攻击 **说明** 如果您需要Tbps级别的云原生防护能力，建议您选择：DDoS原生高级防护-全力防高级版。 ● 业务部署在华为云服务上，且云服务能提供公网IP资源 **须知** DDoS原生防护-全力防高级版的EIP必须为全力防护专属资源池中的EIP。 ● 业务带宽或QPS较大 例如，在线视频、直播等对业务带宽要求比较高的领域。 ● IPv6类型业务防护需求 ● 华为云上公网IP资源较多业务中大量端口、域名、IP需要DDoS攻击防护	● DDoS原生防护-全力防基础版 共享全力防护，防护能力不低于20G。 ● DDoS原生防护-全力防高级版 共享全力防护，防护能力最高可达1T。 除了支付防护费用，同时需要支付专属资源EIP和业务带宽费用。

子服务	简介	应用场景	DDoS攻击防御能力
DDoS高防	DDoS高防通过高防IP代理源站IP对外提供服务，将所有的公网流量都引流至高防IP，进而隐藏源站，避免源站（用户业务）遭受大流量DDoS攻击。	支持华为云、非华为云及IDC的互联网主机。 DDoS高防服务适用于如下场景： 业务频繁遭受DDoS攻击，需要持续性的防护，保障业务的连续性。 **须知** • DDoS高防不支持接入未经ICP备案的域名。如果您需要使用DDoS高防防护网站业务，请确认网站域名已经完成ICP备案。 • 中国内地用户访问内地以外地区的网络访问质量无法保证。	15T以上DDoS高防总体防御能力，单IP最高1T防御能力，抵御各类网络层、应用层的DDoS攻击。 • 15T是指DDoS高防机房的整体防御能力 • 1T是指单个高防IP的最大防护能力
DDoS高防国际版	业务服务器部署在中国内地以外地域，且业务主要用户来自中国内地以外地域，您需要购买DDoS高防国际版。	中国内地用户访问内地以外地区的网络访问质量无法保证。 购买DDoS高防国际版前，建议您考虑使用以下方案：中国内地以外地域的服务器选择使用DDoS高防国际版，并且不对中国内地用户提供业务访问。	5T以上DDoS高防总体防御能力，支持AnyCast无限次防护能力。

1.4 Anti-DDoS 流量清洗与 DDoS 高防有什么区别?

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，详细区别说明如**表1-3**所示。

表 1-3 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	• 防护策略固定 • 全局通用策略	• 防护策略丰富 • 基础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

1.5 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。

1.6 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。

1.7 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。

1.8 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。

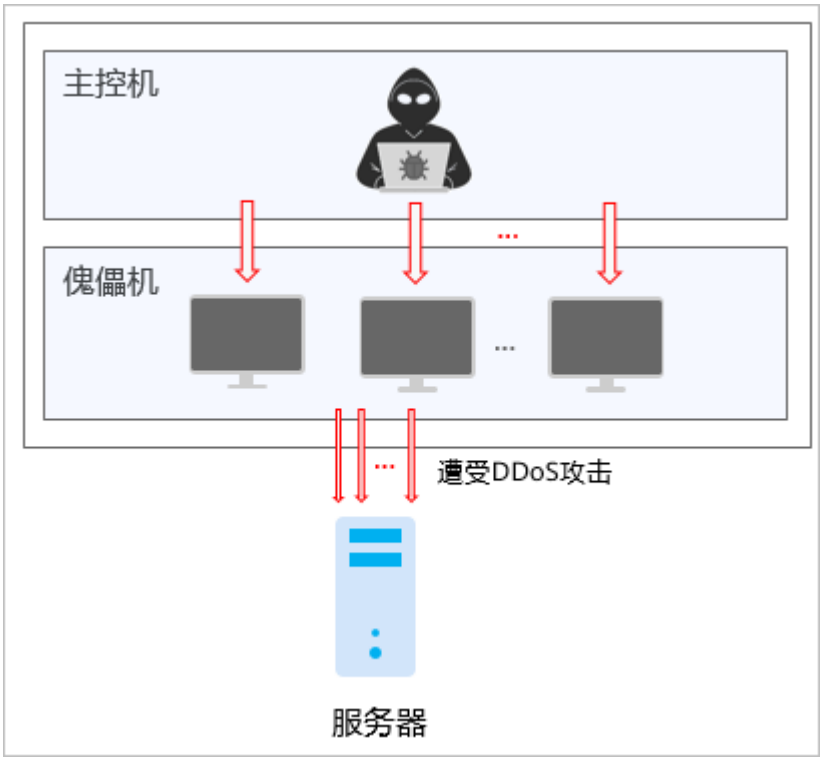
1.9 DDoS 攻击与 CC 攻击有什么区别?

CC（Challenge Collapsar）攻击是DDoS（Distributed Denial of Service）攻击的一种类型，详细说明如下：

DDoS 攻击

DDoS攻击是一种基于DoS特殊形式的拒绝服务攻击，是一种分布的、协同的大规模攻击方式，处于不同位置的多个攻击者同时向一个或多个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。攻击者进行一次DDoS攻击，需要经过了解攻击目标、攻占傀儡机、实际攻击三个主要步骤，如图1-2所示。

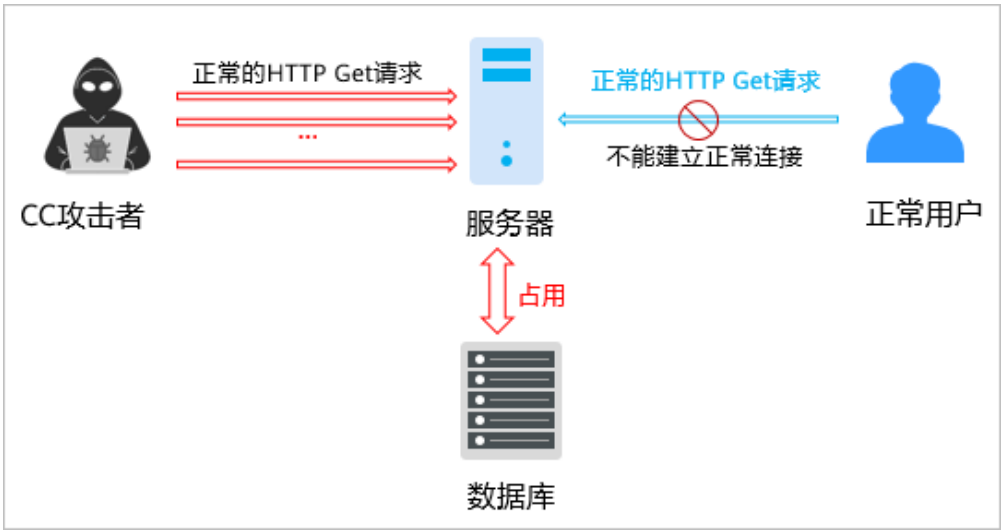
图 1-2 DDoS 攻击流程



CC 攻击

CC攻击是攻击者使用代理服务器向受害服务器发送大量貌似合法的请求，攻击者控制某些主机不停地发大量协议正常的数据包给对方服务器造成服务器资源耗尽，一直到宕机崩溃，如图1-3所示。

图 1-3 CC 攻击示意图



1.10 华为云为用户免费提供的最大防护能力是多少?

华为云为用户的每个EIP免费提供的最大防护能力为500Mbps。

1.11 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。

如何解除黑洞

当服务器（云主机）进入黑洞后，您可以参考如表1-4所示方式进行处理。

表 1-4 解除黑洞方式

DDoS防护版本	解封策略	解除方法
DDoS原生基础防护（Anti-DDoS流量清洗） **说明** DDoS原生基础防护无需购买，默认开启。	• 当云主机进入黑洞24小时后，黑洞会自动解封。 • 如果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。	• 等待自动解封。
DDoS原生高级防护	黑洞解封时间默认为24小时。	等待自动解封。

DDoS防护版本	解封策略	解除方法
DDoS高防	建议提升弹性带宽规格避免再次封堵。	可以通过升级规格提升弹性防护带宽上限以提前解封黑洞。

1.12 DDoS 防护支持透明接入模式吗?

DDoS原生基础防护（Anti-DDoS流量清洗）和DDoS原生高级防护支持透明接入模式，即Anti-DDoS流量清洗和DDoS原生高级防护无需修改域名解析、设置源站保护，可以直接对华为云上的公网IP资源进行DDoS攻击防护。

DDoS高防为代理模式，需要通过域名接入。接入DDoS高防后，DDoS高防将恶意攻击流量引流到高防IP清洗，确保重要业务不被攻击中断。

1.13 DDoS 防护支持 SDK 接入吗?

目前仅DDoS原生基础防护（Anti-DDoS流量清洗）支持SDK方式接入。

1.14 如何迁移企业项目下的实例资源?

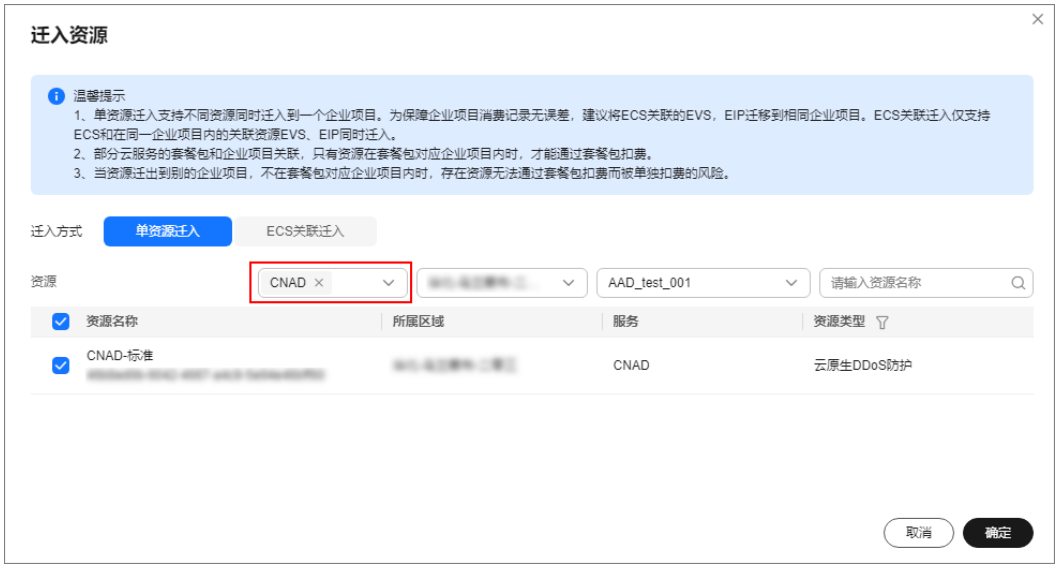
如果您需要迁移企业项目中的原生高级防护或高防实例资源，请参考**为企业项目迁入资源**进行操作。

- 迁移DDoS原生高级防护资源：“资源”选择“CNAD”。
- 迁移DDoS高防资源：“资源”选择“AAD”。

说明

已接入域名的高防实例无法迁移，请解绑域名后再进行迁移。

图 1-4 迁入资源



2 DDoS 原生基础防护常见问题

2.1 产品咨询类

2.1.1 Anti-DDoS 流量清洗的触发条件是什么?

Anti-DDoS流量检测主要包含以下检测项，不同流量清洗阈值档位对应的检测项阈值不一样。

当检测到流量超过流量阈值档位下某个检测项的阈值时，Anti-DDoS将触发流量清洗。

- TCP异常防御
- SYN Flood
- ACK Flood
- TCP分片攻击
- FIN\RST Flood
- UDP Flood
- 指纹防御
- UDP分片攻击防御
- UDP异常报文
- ICMP
- Other Flood
- DNS Query Flood
- DNS Reply Flood

2.1.2 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。

如担心产生误杀，可以通过将“流量清洗阈值”设置为高于业务带宽的值。

2.1.3 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。

2.1.4 Anti-DDoS 流量清洗免费提供多大的防护能力?

Anti-DDoS可防护包括CC、SYN flood、UDP flood等所有DDoS攻击方式，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。

2.1.5 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。

2.1.6 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。

2.1.7 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。

2.1.8 Anti-DDoS 是否支持跨云或跨账号使用?

Anti-DDoS流量清洗服务不支持跨账号使用。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。

2.1.9 如何判断是否有攻击发生?

当您需要查询公网IP是否被攻击时，您可以通过以下方法进行判断。

- 如果您需要查询24小时内的攻击流量信息和异常事件，请参考**方法一：查看监控报表**。
- 如果您需要查询一个月内被攻击的公网IP信息，请参考**方法二：查看拦截报告**。

方法一：查看监控报表

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

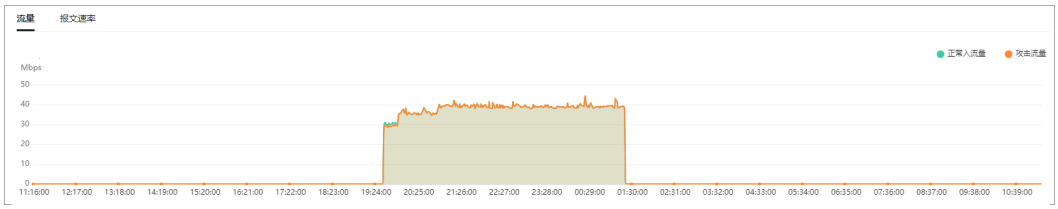
步骤3 选择“公网IP”页签，在待查看监控报表的公网IP地址所在行，单击“查看监控报表”。

图 2-1 查看监控报表

步骤4 查看是否存在攻击流量和异常事件。

- 查看“流量”页签对应时间段是否存在攻击流量，存在攻击流量表明该公网IP被攻击。
- 查看底部事件列表是否存在异常事件，对应时间段存在异常事件表明该公网IP被攻击。

图 2-2 监控报表



----结束

方法二：查看拦截报告

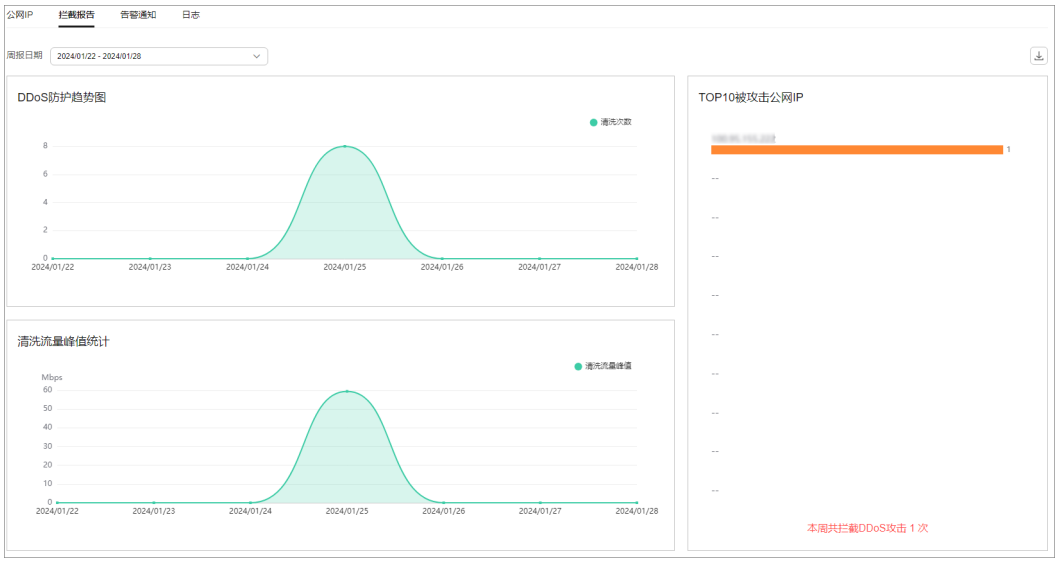
步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 单击“拦截报告”页签，选择需要查看的时间段，查看“TOP10被攻击公网IP”中是否存在查询的公网IP。

如果该时间段中“TOP10被攻击公网IP”中存在查询的公网IP，表明该公网IP被攻击。

图 2-3 拦截报告



----结束

2.2 基本功能类

2.2.1 当遭受超过 500Mbps 的攻击时如何处理?

有关Anti-DDoS流量清洗、DDoS原生高级防护和DDoS高防的详细介绍，请参见**什么是DDoS防护?** 。

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。

2.2.2 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。

2.2.3 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。

2.2.4 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。

2.2.5 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。

2.2.6 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。

2.2.7 Anti-DDoS 防护是一个区域，还是用户的单个 IP?

Anti-DDoS防护的是用户的单个IP。

2.2.8 用户注销账号是否需要清理 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，注销账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。

2.2.9 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。

2.2.10 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。

2.2.11 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。

2.2.12 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。

2.2.13 是否能彻底关闭流量清洗功能?

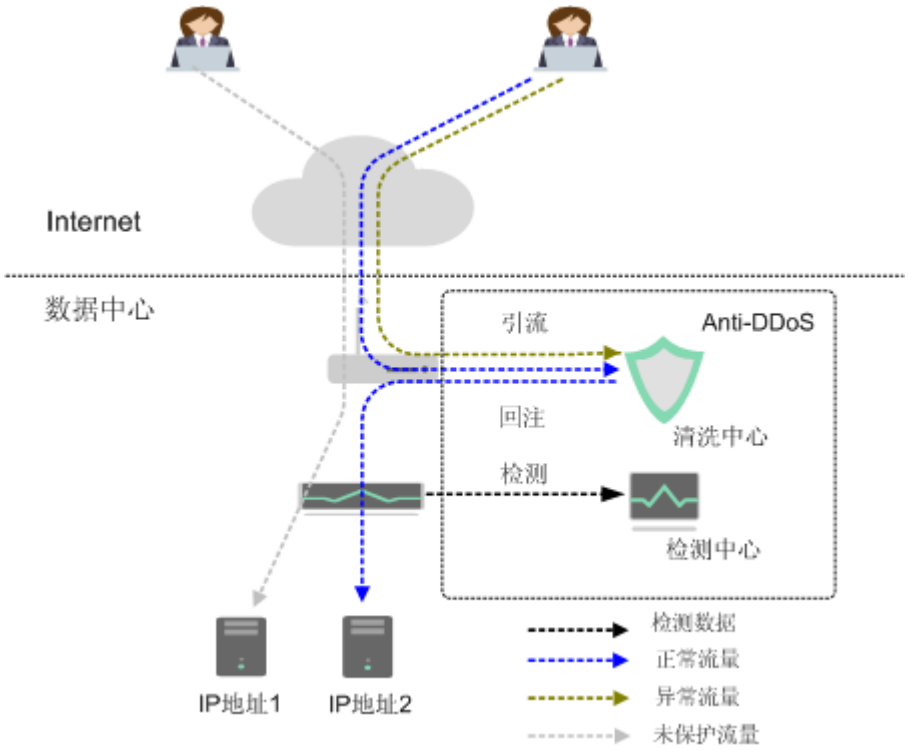
不能。

为保护华为云平台的安全，所有进入华为云的流量必须开启防护策略。

2.2.14 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2-4**所示。

图 2-4 网络拓扑架构图



如果入网流量来自公网，则会经过Anti-DDoS流量清洗服务；如果入网流量来自华为云内部，则不会经过Anti-DDoS流量清洗服务。

- 如果您从公网访问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访问的路由，如果有经过公网路由，则经过了Anti-DDoS流量清洗服务。

  如果经过了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）。
- 如果您从华为云内部访问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。

2.3 阈值及黑洞类

2.3.1 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**。

2.3.2 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。

2.3.3 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。

2.4 告警通知类

2.4.1 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攻击时用户会收到报警信息（短信或Email）。详情请参考**开启告警通知**。

2.4.2 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，例如短信或Email），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。如果不想被清洗，可以调高流量清洗阈值，具体操作请参考**配置Anti-DDoS防护策略**。

2.4.3 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

如果您不需要接收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 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“告警通知”页签，单击  ，关闭告警通知。

图 2-5 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2-6所示。

图 2-6 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。

2.4.4 如何开启 Anti-DDoS 封堵通知?

问题描述

Anti-DDoS控制台中的告警通知仅能开启流量清洗通知，如果您需要及时收到EIP遭到封堵的通知，请参考下文中的操作步骤。

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，单击页面左上方的 ☰，选择“管理与监管 > 云监控服务 CES”。

步骤3 在左侧导航栏选择“事件监控”，进入“事件监控页面”。

步骤4 单击右上角的“创建告警规则”，进入“创建告警规则”页面。

步骤5 配置EIP封堵告警关键参数：

- 告警类型：事件
- 事件类型：系统事件

- 事件来源：弹性公网IP
- 触发规则：自定义创建
- 告警策略：需要选择EIP封堵，并且选择需要提示的“告警级别”。
- 通知方式：根据实际设置。

图 2-7 EIP 封堵告警关键参数

步骤6 单击“立即创建”，完成封堵告警通知创建。

----结束

2.5 业务故障类

2.5.1 网络流量异常的原因?

为了保障华为云网络的整体可用性，华为云采用黑洞封堵，对遭受大流量攻击的云主机在一定时间内限制外网通信。

华为云为普通用户免费提供2Gbps的DDoS攻击防护，最高可达5Gbps（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5Gbps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。

2.5.2 DDoS 攻击导致客户端禁止访问，怎么办?

您可以通过“Anti-DDoS监控报表”，查看单个公网IP 24小时的异常事件，或查看Anti-DDoS拦截报告查看所有公网IP的防护统计信息、TOP10被攻击公网IP等，判断您的业务是否是遭受DDoS攻击，导致IP被黑洞封堵，从而引发客户端被禁止访问。

如果确认是遭受DDoS攻击导致IP被黑洞封堵，那么当您的云主机进入黑洞24小时后，黑洞会自动解封。

2.5.3 遭受流量攻击，如何查询公网 IP 的具体防护信息?

您可以通过“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。

2.5.4 没有受到攻击，触发了流量清洗?

Anti-DDoS检测到IP的入流量超过流量清洗阈值时，触发流量清洗。如果不想被清洗，可以调高流量清洗阈值，具体操作请参考“配置Anti-DDoS防护策略”。

3 DDoS 原生高级防护常见问题

3.1 功能咨询

3.1.1 什么是全力防护?

全力防护是DDoS原生高级防护提供的防护能力，指华为云根据当前区域下DDoS本地清洗中心的网络和资源能力，调用所有可用资源对攻击进行全力防护，其防护能力随着华为云网络能力的不断提升而相应提升。

全力防护当前提供2种版本：DDoS原生防护-全力防基础版、DDoS原生防护-全力防高级版。

3.1.2 DDoS 原生高级防护可以防护非华为云和云下的 IP 吗?

DDoS原生高级防护支持对华为云公网IP资源，例如ECS、ELB、WAF、EIP等进行防护，不支持对非华为云和云下的资源进行防护。

3.1.3 DDoS 原生高级防护可以防护 IPv6 吗?

DDoS原生高级防护可以为华为云公网IP（IPv6和IPv4两种类型）提供防护，满足您对IPv6和IPv4类型业务防护需求。

3.1.4 DDoS 原生高级防护中防护 IP 被黑洞了，如何处理?

对进入封堵状态的防护IP，您可以使用自助解封功能提前解封黑洞。

3.1.5 DDoS 原生高级防护的防护对象有哪些?

DDoS原生高级防护支持对华为云上的公网IP资源进行防护，例如华为云ECS、ELB、WAF、EIP等。

3.1.6 DDoS 原生高级防护能够防护几层攻击?

DDoS原生高级防护可以防御三层和四层流量型攻击。如果您需要防护七层流量攻击，需要和独享WAF联动防护。

3.1.7 DDoS 原生高级防护的流量回切时间是多久?

DDoS原生高级防护的流量回切时间约5~10分钟。

DDoS原生高级防护流量切换到DDoS高防的过程，根据DNS域名生效时间和用户本地的递归DNS生效时间，大概需要5~10分钟。在此期间，整体流量可能同时在DDoS原生高级防护IP和高防IP中存在。

3.1.8 DDoS 原生高级防护可以跨区域使用吗?

DDoS原生高级防护中仅原生防护2.0支持跨区域使用，其他版本暂不能跨区域防护。

3.1.9 什么是专属 EIP

专属EIP是指DDoS防护专属EIP，普通EIP在华为云本地机房进行攻击防御，专属EIP是在DDoS清洗中心进行攻击防御，具备T级带宽，防护能力强大。

为ECS服务器绑定专属EIP后，可添加到全力防高级版和原生防护2.0进行防护。

3.2 计费问题

3.2.1 DDoS 原生高级防护如何计费?

价格体系

使用DDoS原生高级防护需要购买DDoS原生高级防护实例。

计费方式

DDoS原生高级防护提供DDoS原生标准版、DDoS原生防护-全力防基础版、DDoS原生防护-全力防高级版三种服务版本，根据您选择的版本和规格参数计费。

- DDoS原生标准版、DDoS原生防护-全力防高级版提供包周期预付费计费模式，使用越久越便宜。包周期计费按照订单的购买周期来进行结算。
- DDoS原生防护-全力防基础版提供按需和包周期的计费模式。

表 3-1 计费项信息

版本	计费项目	计费方式	说明
DDoS原生防护-全力防基础版	实例	按购买的实例数量计费。	-
	防护IP数	每个DDoS原生防护-全力防基础版实例防护的IP个数。	取值范围为50～500，且防护IP数必须设置为5的倍数。
	防护次数	每个DDoS原生防护-全力防基础版实例防护的次数。	防护次数：无限次

版本	计费项目	计费方式	说明
	购买时长	提供包月和包年的购买模式。	支持“3个月”、“6个月”或“1年”。
DDoS原生防护-全力防高级版	实例	按购买的实例数量计费。	-
	防护IP数	每个DDoS原生防护-全力防高级版实例防护的IP个数。	取值范围为50～500，且防护IP数必须设置为5的倍数。
	防护次数	每个DDoS原生防护-全力防高级版实例防护的次数。	防护次数：无限次
	购买时长	提供包月和包年的购买模式。	支持“3个月”、“6个月”或“1年”。

3.2.2 DDoS 原生高级防护的业务带宽需要计费吗?

DDoS原生高级防护提供DDoS原生防护-全力防基础版、DDoS原生防护-全力防高级版两种服务版本。

两种规格都需要支付业务带宽费用，只有DDoS原生标准版固定了带宽值，无法自选带宽大小。

相比DDoS高防（需要将流量引流到高防机房进行清洗，通过互联网产生额外业务带宽费用），DDoS原生防护-全力防基础版和DDoS原生防护-全力防高级版直接在华为云内进行回源，不产生通过互联网的额外业务带宽费用。

3.2.3 如何退订 DDoS 原生高级防护?

包年月购买的DDoS原生高级防护不支持无理由退订。如果满足可退订条件，可以联系客服申请退订。

可退订条件

在购买或使用过程中发现无法与业务匹配，可联系客服申请退订。

已经正常使用的DDoS原生高级防护实例无法退订。通过DDoS原生高级防护服务后台，如判断出实例已经正常使用过，此种情况无法退订。

4 DDoS 高防常见问题

4.1 功能规格

4.1.1 DDoS 高防支持哪些业务端口?

背景信息

当您的域名需要业务接入DDoS高防场景，在配置防护域名时，如果“源站类型”选择“源站IP”，需要配置“转发协议”和“源站端口”。

- 转发协议：DDoS高防转发客户端（例如浏览器）请求的协议类型。
- 源站端口：DDoS高防转发客户端请求到服务器的业务端口。

图 4-1 配置源站端口

DDoS 高防支持防护的业务端口

- 四层防护
  DDoS高防四层防护支持的端口范围为：**80~65535**。
- 七层防护

表 4-1 DDoS 高防七层防护支持的端口

转发协议	源站端口
HTTP	80、81、82、83、84、85、88、133、134、140、141、144、151、881、1135、1139、7000、7001、8006、8078、8080、8087、8088、8089、8090、8093、8097、8100、8182、8200、8813、8814、8888、9000、9001、9002、9003、18080、19101、19501、21028、40010
HTTPS	443、882、1818、4006、4430、4443、5443、6443、7443、8033、8081、8082、8083、8443、8445、8553、8663、8750、8804、8805、9443、9999、13080、14443、18443、18980、20000、28443、30001、30003、30004、30005

4.1.2 DDoS 高防支持哪些转发协议?

DDoS高防支持的转发协议有：

- 四层协议：TCP、UDP
- 七层协议：HTTP/WebSocket、HTTPS/WebSockets

如何配置 HTTP/WebSocket 和 HTTPS/WebSockets 转发协议?

在“域名接入 > 添加域名”页面，转发协议选择“HTTP”或“HTTPS”，即可配置HTTP/WebSocket或HTTPS/WebSockets转发协议。

4.1.3 DDoS 高防是否支持修改防护带宽?

- DDoS高防允许升级扩容保底防护带宽。
- DDoS高防允许修改弹性防护带宽，每天允许修改3次弹性防护带宽，弹性防护带宽修改之后立即生效。

4.1.4 DDoS 高防源站域名是否支持 CDN CNAME?

DDoS高防源站域名当前仅支持华为云WAF CNAME，不支持其他CNAME。

4.1.5 购买高防实例时选定保底带宽 10G 弹性带宽 20G，最终获得最大防护能力是多少?

20G。用户最终获得的最大防护能力即是用户选定的弹性防护带宽，弹性防护带宽并不是在保底防护带宽之上的增量。而且当用户选定的弹性防护带宽和保底防护带宽相同时则不具备弹性防护能力。

例如，用户选定保底防护带宽50G和弹性防护带宽50G，则用户最大防护能力也是50G，不具备弹性防护能力。

4.1.6 DDoS 高防回源到云主机的是公网 IP 吗?

是。DDoS高防系统通过公网回源到源站，因此回源到云主机的源站IP为公网IP。

4.1.7 DDoS 高防最多支持多少个域名?

每个实例默认赠送50个域名（支持单域名和泛域名），可以付费增加，最多可支持200个，超过200个可以通过购买更多的高防实例解决。

须知

域名个数为一级域名（例如，example.com）、单域名/子域名（例如，www.example.com）和泛域名（例如，*.example.com）的总数。即每个DDoS高防实例可以防护50个单域名或泛域名，也可以防护1个一级域名和49个与其相关的子域名或泛域名。

4.1.8 配置 DDoS 高防后，平均时延会增加多少?

业务接入DDoS高防后，平均时延会增加30ms。业务实际时延根据业务情况有所不同。

4.1.9 DDoS 高防对并发数有限制吗?

并发数指系统同时能处理的请求数量，反映了系统的负载能力。对网站而言，并发数即网站并发用户数，指同时提交请求的用户数目。

DDoS高防对并发数没有限制。DDoS高防支持TCP/UDP/HTTP(s)/Websocket(s)等协议转发，默认不限制TCP连接，且对HTTP协议没有限制。

4.1.10 如何关闭 DDoS 高防服务?

DDoS高防不提供关闭功能。业务系统接入DDoS高防后，如果您不再使用DDoS高防，请先删除防护域名， 确保在不使用DDoS情况下业务无影响后，退订DDoS高防即可关闭DDoS高防服务。

4.2 接入配置

4.2.1 部署在华为云外的业务系统能否接入 DDoS 高防?

用户只要保证源站（用户业务系统）IP地址在公网可以访问即可，不区分云内云外。

4.2.2 接入防护域名后，如何测试防护域名是否配置正确?

步骤1 登录管理控制台。

步骤2 接入防护域名，详细操作请参考**如何将业务系统接入高防服务?** 。

步骤3 复制待测试的域名的“CNAME”值。

步骤4 ping“CNAME”值并记录“CNAME”对应的IP地址（例如：192.168.0.1）。

步骤5 在本地修改“hosts”文件，以Windows系统为例，进入“C:\Windows\System32\drivers\etc”，打开“hosts”文件，追加一条记录，如下图所示：

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      [redacted]                    # source server
#      [redacted]                    # x client host

# localhost name resolution is handled within DNS itself.
#   [redacted]       localhost
#   ::1              localhost

192.168.0.1    www.test.com
```

步骤6 清理浏览器缓存，在浏览器中输入域名即可测试域名业务是否正常。

----结束

4.2.3 如何解决上传 HTTPS/WebSockets 证书时出现“错误的请求”提示的问题?

上传HTTPS/WebSockets证书出现“错误的请求”提示的常见原因和解决方法如下：

- 证书名字过长。
  解决方法：修改证书文件名到10 个字符以内。
- 证书文件名包含特殊字符。
  解决方法：仅以英文字符和数字命名证书。
- 证书内容不规范。
  解决方法：**将非PEM格式的证书转换为PEM格式**。安装证书和私钥输入格式删除证书文件中不规范的内容。例如：删除“---BEGIN CERTIFICATE---”之前的内容。

4.2.4 如何将非 PEM 格式的证书转换为 PEM 格式?

- **CER/CRT格式证书转换为PEM格式**
  可通过修改证书文件扩展名的方式进行转换。
  例如，将“certificate.cer”证书文件重命名为“certificate.pem”即可。
- **PFX格式证书转换为PEM格式**
  可通过openssl工具进行转换。

```
#提取证书命令
openssl pkcs12 -in certificate.pfx -nokeys -out cert.pem
#提取私钥命令
openssl pkcs12 -in certificate.pfx -nocerts -out key.pem -nodes
```

- **P7B格式证书转换为PEM格式**

  可通过openssl工具进行转换。

  a. 执行转换命令

  ```
  openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
  ```

  b. 获取outcertificat.cer文件中证书文件的内容。

  c. 将证书内容保存为PEM格式。

- **DER格式证书转换为PEM格式**

  可通过openssl工具进行转换。

  ```
  #提取证书命令
  openssl x509 -inform der -in certificate.cer -out certificate.pem
  #提取私钥命令
  openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
  ```

4.2.5 DDoS 高防和 WAF 同时使用，怎么配置?

同时使用DDoS高防和WAF的配置步骤说明如下：

1. 在WAF管理控制台获取域名的CNAME值。
2. 将CNAME值配置到DDoS高防。
3. 修改DNS解析。

配置完成后，流量会先经过DDoS高防，再转发至WAF，实现联动防御。

4.2.6 如何将业务系统接入高防服务?

- 对于通过域名对外提供服务的系统，修改DNS配置，将对外提供的业务域名解析到华为云提供的CNAME。
- 对于通过IP对外提供服务的系统，将对外提供的业务IP变更为高防IP。

4.2.7 如何实现 CNAME 接入?

什么是CNAME?

CNAME就是DNS别名。DNS A记录是把域名直接解析到IP地址，而CNAME记录则是把域名解析到另外一个域名（别名）。例如，域名“www.abc.com”配置了CNAME别名“ccd01c25c8535fa4.huaweisafedns.com”。用户访问“www.abc.com”时，DNS通过第一次解析获得了CNAME别名后，自动对CNAME别名“ccd01c25c8535fa4.huaweisafedns.com”进行二次解析获得该CNAME对应的真实IP地址。解析过程由DNS协议自动完成。

使用CNAME接入方式有哪些优势?

- 简单方便

  用户只需要在域名解析服务商处（例如：华为云云解析服务。）修改一次解析配置即可。

  对于同一个域名，在多条线路中生成的CNAME记录是一致的。用户只需要配置一条CNAME解析即可，DDoS高防自动将CNAME记录配置到域名对应的多个高防

IP。当高防IP发生变化时，DDoS高防将自动更新CNAME映射，不需要手动修改DNS配置。

- 访问性能高

  当域名选择多条线路时，DDoS高防将根据实际访问用户的来源进行流量调度，选择合适线路以确保用户访问性能。

- 高可靠

  一个域名可以选择多条线路，当某条线路的高防IP出现异常时，CNAME可以自动将流量调度到其他可用线路，保证用户业务的持续性。

已配置分链路解析，使用CNAME接入后如何配置?

一般情况下需要一条默认线路的CNAME解析即可替换之前的分链路解析，智能解析的过程由华为云自动完成。

华为云提供的CNAME地址具备分链路解析的能力，会根据您购买的线路情况自动进行分链路解析。

4.2.8 DDoS 高防在配置多个源站时如何分发流量?

当用户配置多个源站IP时，DDoS高防采用轮询模式分发流量，业务流量将均匀地分发到各个源站IP。

4.2.9 用户在完成高防防护配置后，如何检查是否完成源站白名单添加了高防回源 IP 的配置?

对服务器和安全设备进行排查，确保高防回源IP加入到相应的白名单中、并不对回源流量设置过滤或者限制。例如：

- 如果用户源站在华为云上，则需要配置ACL和安全组，将回源IP在ACL和安全组中设置放行。
  a. 登录管理控制台。
  b. 单击管理控制台左上角的，选择区域或项目。
  c. 单击页面左上方的，选择“网络 > 虚拟私有云”。
  d. 参考**添加安全组规则**添加回源IP的安全组放行规则。
  e. 参考**创建网络ACL**添加回源IP的网络ACL放行规则。
- 如果源站有自设的安全策略，请确保生效。用户配置的有些安全策略可能需要重启才能生效。

4.2.10 如何修改已暴露的源站 IP?

操作场景

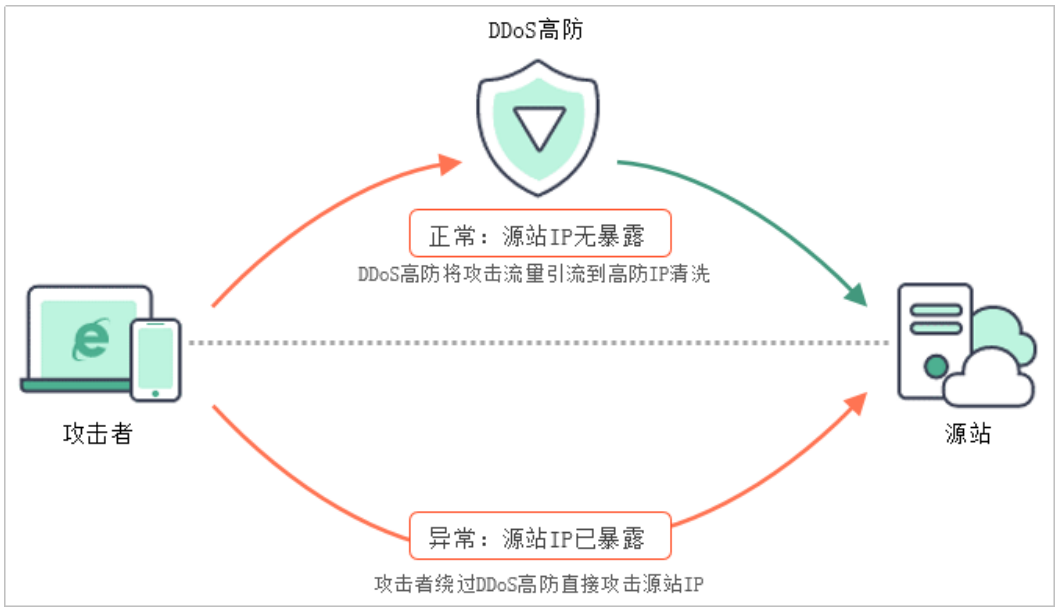
用户在完成高防防护配置后，源站IP仍被攻击，说明源站IP已经暴露，需要修改已暴露的源站IP。

该任务以弹性云服务器（Elastic Cloud Server，简称ECS）为例，介绍如何修改源站IP（例如弹性公网IP）的方法。

源站 IP 暴露典型原因

- 未配置DDoS高防服务时，源站IP受到过黑客攻击，说明源站IP已经暴露。
- 配置DDoS高防服务后，部分攻击者会记录源站使用过的IP，存在绕过高防直接攻击源站IP的情况，建议更换源站IP。

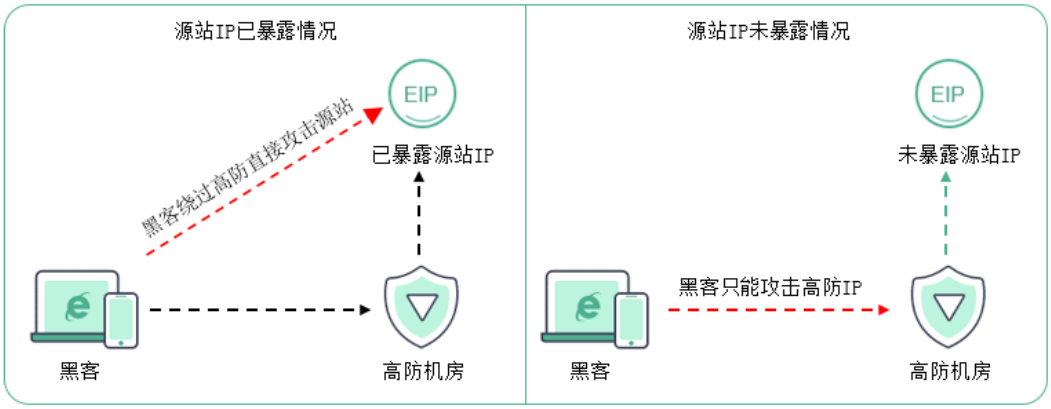
图 4-2 源站 IP 暴露典型原因



解决方案

以弹性云服务器为例，通过为弹性云服务器实例重新分配弹性公网IP（Elastic IP，简称EIP），将已暴露的EIP更换为未暴露的EIP，实现修改源站IP的目的。

图 4-3 原理说明



操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的 ☰，选择“网络 > 虚拟私有云”，进入虚拟私有云管理界面。

步骤4 在左侧导航树中，选择“弹性公网IP和带宽 > 弹性公网IP”，进入“弹性公网IP”界面。

步骤5 在需要修改的弹性公网IP所在行的“操作”列，单击“解绑”。

步骤6 单击“是”。

步骤7 为弹性云服务器实例重新分配IP，在需要绑定的弹性公网IP所在行的“操作”列，单击“绑定”。

步骤8 选择实例。

步骤9 单击“确定”。

----结束

4.2.11 如何查看高防回源 IP 段?

如果用户的源站已配置防火墙，为了防止高防回源IP被源站拦截或限速，需要将高防回源IP段的IP地址添加到源站的防火墙，或其它防护软件的白名单中。

该任务指导用户如何查看高防回源IP段，将高防回源IP段的IP地址添加到源站的防火墙，或其它防护软件的白名单中。

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，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

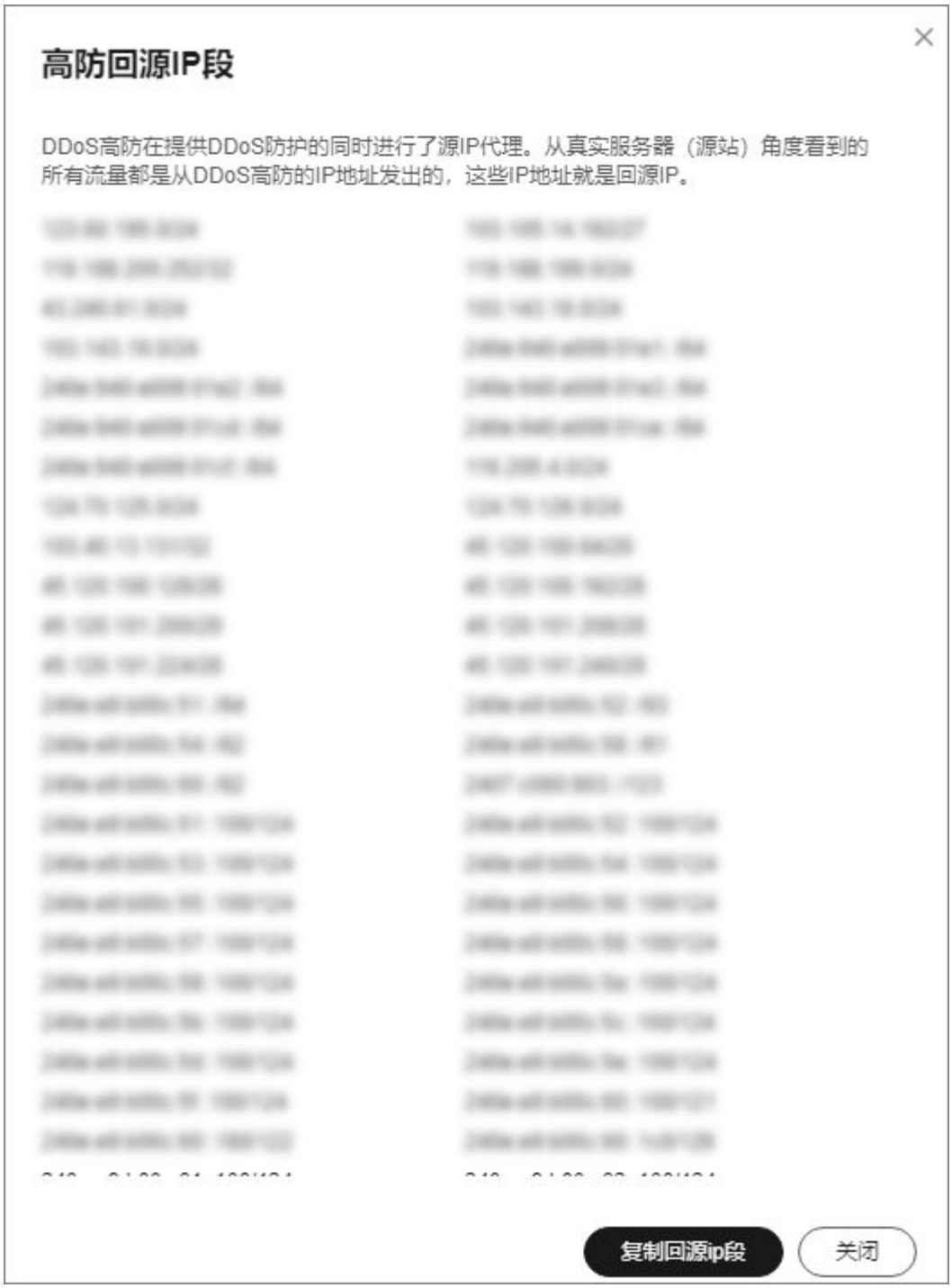
步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 4-4 域名接入页

步骤4 在域名列表左上角，单击“高防回源IP段”。

步骤5 在弹出的“高防回源IP段”对话框中，查看高防回源IP段信息，如图4-5所示。

图 4-5 查看高防回源 IP 段



步骤6 将高防回源IP段添加到源站的防火墙或其它防护软件的白名单中。

----结束

4.2.12 接入防护域名后，可以进行企业项目资源迁移吗?

DDoS高防支持多项目管理，企业可以按项目管理DDoS高防资源，支持企业项目资源迁移，但是配置了防护域名接入的高防实例无法更改所属企业项目。

4.2.13 能否在华为云服务器自行搭建 DDoS 防御?

可以。用户可以在华为云服务器为自身业务搭建DDoS防御体系。如果频繁遭遇大流量攻击，华为云会执行封堵策略或冻结，建议您购买DDoS高防产品来保障业务连续性。

4.2.14 高防配置黑白名单，如何设置保护客户的服务器?

DDoS高防服务支持对已接入防护的高防实例设置黑名单和白名单，通过设置，黑名单中的IP会被拦截，白名单中的IP会被放行。具体步骤请参考配置黑白名单，如果您需要防护源站服务器，请联系技术支持为您解决。

4.2.15 DDoS 防护策略中配置黑白名单后，还需要在 WAF 防护策略里配置吗?

DDoS防护策略里配置的白名单会自动同步到WAF防护策略里，用户无需在WAF防护策略里再次配置。

在DDoS防护策略里配置黑名单后，业务流量经过DDoS防护设备会自动拦截，无需在WAF防护策略里再次配置。如果域名绑定了多个实例，需要在多个实例上配置黑名单。

4.2.16 一个域名如何同时接入 IPv4 和 IPv6?

DDoS高防国内版支持源站域名同时接入IPv4和IPv6，具体方法如下：

步骤1 参考**购买DDoS高防实例**分别购买一个IPv4和IPv6实例。

步骤2 参考**配置防护域名**将域名接入DDoS高防，选择实例线路时，同时勾选购买的IPv4实例和IPv6实例。

- “源站类型”：选择“源站域名”。
- “选择实例与线路”：同时勾选IPv4和IPv6实例。

图 4-6 选择实例与线路

----结束

4.2.17 域名接入失败，提示“域名已存在”等信息

请根据提示信息内容进行排查：

- 提示“域名已存在”：在接入域名时，提示域名已存在，一般情况是该域名客户已接入过，或客户的其他账号下接入过相同域名。如需重新接入，找到相同域名或老账号下的相同域名删除后重新接入即可。如域名客户没有接入过也提示存在，可提工单联系后端研发协助排查。
- 提示“此域名已存在相同的域名或者其他用户已使用”：在接入域名时，如图提示此域名已存在相同的域名或其他用户已使用，一般是已有用户接入过与当前域名相同二级域名的其他域名。高防服务默认二级域名的归属权只属于一个租户，如能证明二级域名的归属，可提工单联系后端进行白名单处理。

4.3 故障反馈

4.3.1 高防 IP 卡顿、延迟、访问不通等问题排查

问题描述

客户端访问高防IP异常卡顿，出现较大延迟、丢包现象。

排查方案

- **业务本身存在跨网访问**

  产生原因：华为云高防服务支持电信、联通、移动及BGP四种线路。DNS侧配置导致的跨网解析和高防侧源站IP配置导致的跨网回源都会造成一定的延迟和丢包。

  解决方案：

  - DNS侧：检查DNS配置是否有错误。

    如果使用华为云提供的CNAME解析不会产生此问题；如果使用A记录解析，请根据访问来源的运营商配置对应的高防IP，BGP高防IP则配置为默认。如果用户由于DNS配置错误造成丢包或延迟，由此带来的后果华为云无法承担。

  - 高防侧：检查源站IP配置是否有错误。

    如果源站业务单独使用某个运营商，那么跨站访问天然会产生延迟与丢包，由此带来的后果华为云无法承担。

    如果源站使用多个运营商的IP地址，请根据高防IP的运营商添加相对应的源站IP，例如将电信的高防IP与电信的源站IP绑定。如果用户由于回源线路配置错误造成丢包或延迟，由此带来的后果华为云无法承担。

- **后端服务器异常**

  根据出现异常的高防IP配置的源站类型进行排查。

  - 源站是负载均衡

    参照以下步骤进行排查。

    i. 针对负载均衡IP和端口，通过运行tcping工具，查看记录是否有异常。

    ii. 查看负载均衡服务器状态（如连接数情况、后端服务器）是否有异常状态。

    iii. 查看负载均衡是否设置黑、白名单，或者其他的访问控制策略，确认放行高防本身回源IP段。

    iv. 查看负载均衡后端主机和网络，确认是否有防火墙IP封禁策略。

  - 源站是服务器

    参照以下步骤进行排查。

    i. 针对服务器IP和端口，通过运行tcping工具查看记录是否有异常。

    ii. 查看后端服务器是否有异常事件，如服务器本身黑洞及清洗事件、CPU高、数据库请求慢、出方向带宽满等。

    iii. 查看服务器本身是否设置黑、白名单，或者其他的访问控制策略，确认放行高防本身回源IP段。

    iv. 查看服务器或网络，确认是否有安全软件或其它IP封禁策略阻断高防回源IP。

- **高防IP是否有清洗事件**

  - 高防IP有清洗事件

    参照以下步骤进行排查。

    i. 针对受攻击端口，通过运行tcping工具查看是否有延迟和丢包，并记录。

    ii. 针对未被攻击端口，通过运行tcping工具查看是否有延迟和丢包，并记录。

    根据记录结果，对照下表查看问题原因。

表 4-2 记录结果

受攻击端口是否有延时、丢包	未被攻击端口是否有延时、丢包	问题原因分析
是	否	说明清洗策略未误杀，查看后端服务器状态是否异常，确认后端服务器抗攻击性能。如果服务器抗攻击能力较弱，则需要收紧防御策略。
是	是	清洗策略误杀导致。请提交工单，需要进行后端排查。
否	否	非清洗策略原因。
否	是	一般不存在这种情况。

上述前两种情况，建议您通过**提交工单**说明情况来处理。如果需要收紧防御策略，您需要提供服务器抗攻击能力的详细参数，包括：

- 正常用户访问情况
- 业务主要交互过程
- 应用对外服务能力

– 高防IP没有清洗事件

说明问题非攻击导致。

- **高防IP有黑洞事件**

  被攻击超过弹性峰值的高防IP会触发黑洞事件，请确认产生丢包的IP是否被黑洞。

  建议购买更大带宽的弹性峰值，并且调整业务系统，使其具备切换能力。当线路被黑洞时，可切换至正常线路。

4.3.2 配置高防后访问网站提示 504 错误

问题描述

配置高防IP服务后，网站执行某些POST请求时，长时间等待后返回504错误，执行不成功。

问题原因

此问题是由于请求处理时间过长，已超过高防IP服务的连接阈值，高防IP服务主动断开连接。

- TCP默认连接超时时间为900s。
- HTTP/WebSocket、HTTPS/WebSockets默认连接超时时间为120s。

解决方法

建议您在应用层面部署长时间任务执行的心跳机制，确保在请求等待的过程中保持该连接活跃。

对于非常规偶发性任务请求，您可以绕过高防IP直接访问后端ECS云服务器执行该任务。

4.3.3 如何判断遭受的攻击类型?

您可以在DDoS高防概览界面，通过查看相应的流量报表信息，判断遭受的攻击类型为CC攻击还是DDoS攻击。

判断方法

如果您的DDoS高防同时遭受到CC攻击和DDoS攻击时，可参照以下方法快速判断遭受的攻击类型：

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航树，选择“DDoS高防 > 概览”。

步骤4 单击“DDoS攻击防护”、“CC攻击防护”，通过查看相应的流量报表信息，判断攻击类型：

攻击类型	DDoS攻击防护流量报表信息	CC攻击防护流量报表信息
DDoS攻击	• 报表中有攻击流量的波动。 • 已触发流量清洗。	• 报表中没有相关联的流量波动。
CC攻击	• 报表中有攻击流量的波动。 • 已触发流量清洗。	• 报表中有相关联的流量波动。

----结束

4.3.4 防护域名开启“WEB 基础防护”之后，如何排查500/502/504 错误?

防护域名开启“WEB基础防护”之后，访问网站如果出现“500 ”，“502”，“504”等报错，并且显示“Web应用防火墙”和“网站”连接失败，如图4-7所示。

图 4-7 502 报错

可能的原因比较多，如防火墙拦截、源站配置错误、HTTPS/WebSockets采用不安全的协议版本、后端服务器性能问题等。

以下是可能的原因及解决方案：

- 防火墙、后端服务器安全防护软件、业务限速策略拦截。

  现象：防护域名开启“WEB基础防护”之后正常，但是一段时间后就报502，或者大概率出现502。

  解决方法：将高防的回源IP段添加到防火墙（硬件或软件）、安全防护软件、业务限速模块的白名单。
- 源站配置错误

  现象：防护域名开启“WEB基础防护”之后，访问页面返回502/500，或者大概率出现502/500（当后端配置了多个服务器的情况）。

  解决方法：在“域名接入”页面，防护域名列表中找到相应的域名记录，单击“操作”列中的“编辑”，确认转发协议、IP、端口等信息是否正确。

图 4-8 修改域名业务配置

如图4-8配置，可在浏览器访问http://xx.xx.xx.108:80 、https://xx.xx.xx.108:443来检查后端业务端口是否打开。

- HTTPS/WebSockets采用不安全的协议版本

  现象：防护域名开启“WEB基础防护”之后，HTTPS/WebSockets业务大概率返回502，而直接通过IP访问源站正常。

  解决方法：因为SSL低版本的协议存在严重的安全隐患，华为WAF防护支持TLS1.2及以上版本的协议。所以如果您的业务服务器的SSL版本较低，防护域名开启“WEB基础防护”之后则会出现502错误，需要您升级SSL版本解决问题。

  您可以通过访问“https://www.ssllabs.com/ssltest/index.html”检查网站服务的SSL版本信息：

  - 如果您的Web服务器是Windows 2008以前的版本，SSL协议不支持TLS1.2及以上。您需要将服务器版本升级到Windows 2008以上（或Linux较新版本的操作系统），并在IIS等服务中开启TLS1.2。
  - 如果您的Web服务是其他系统，请确认SSL协议是否是TLS1.2或以上。

- 后端服务器性能问题

  现象：防护域名开启“WEB基础防护”之后，业务正常。但业务量增加时，502/504比例增加。直接访问源站也有一定概率出现502/504的返回码。

  解决方法：

  - 优化服务器的相关配置，包括TCP网络参数的优化配置，Ulimit相关参数设置等。
  - 对后端ECS扩容来支撑业务增长，DDoS高防支持配置多个后端服务器。

4.3.5 配置转发规则失败原因排查

原因排查：

- 转发规则配置生效一般需要2-3分钟，处于“处理中”属于正常状态，请稍候刷新查看。
- 转发规则配置下发过程中，高防系统会检查您配置的源站IP和端口是否连通以及与现有转发规则是否冲突，如配置状态失败，请您检查源站是否工作正常或已有转发规则配置。

4.3.6 UDP 封禁原因排查

开启了“UDP流量封禁”的线路，会阻止UDP流量的访问，请查看高防防护策略下高防实例的线路状态，确认“UDP流量封禁”处于关闭。

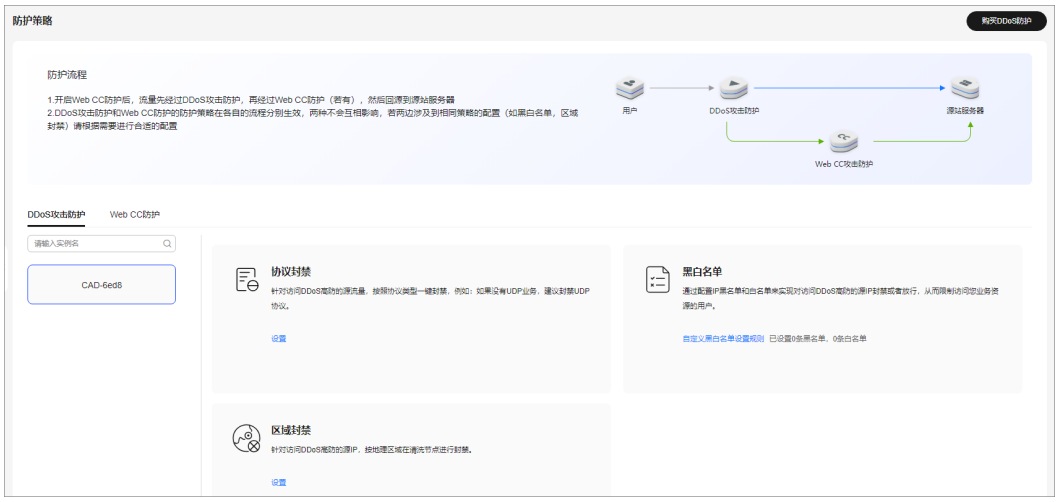
操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

图 4-9 DDoS 高防防护策略页面



步骤4 选择需要配置协议封禁的实例。

步骤5 在协议封禁配置框中单击“设置”。

步骤6 在弹出的对话框中选择需要配置协议封禁的路线，并且将开关调整至 ，打开协议禁用功能。

图 4-10 协议封禁设置

----结束

4.3.7 服务器 IP 流量过高被自动封堵后，如何解封?

如果是运营商封堵，24小时后将自动解封。

DDoS高防服务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。

4.3.8 配置转发规则时为什么某些端口配置失败?

故障现象

添加转发规则时，“转发端口”和“源站端口”配置为某些特定端口时，转发规则配置失败。

说明

端口取值范围1～65535。

原因分析

DDoS高防判定表4-3中的端口为高危端口，禁止使用。

表 4-3 高危端口

协议	端口
TCP类	135、136、137、138、139、445、3333、4444、5554、6000、8090、9995、9996、25000、50050、53413、60000
UDP类	135、137、138、139、593、901、1027、1028、1068、2745、3127、3128、3333、5800、5900、6000、6129、6667、8090、8998、9996、25000、50050、5341、60000

处理建议

建议您将端口修改为其他非高危端口。

4.3.9 域名接入高防后出现“Received fatal alert”报错

故障现象

域名接入DDoS高防后出现“Received fatal alert: handshake_failure; nested exception is javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure”报错，不接入高防则正常。

原因分析

客户接入的回调平台客户端不支持SNI扩展。

解决方法

对于不支持SNI的客户端有以下建议：

1. 建议您升级或使用新版本的浏览器，如Chrome、Firefox等，以支持SNI扩展。
2. 升级客客户端的java版本和OpenSSL版本。
3. 升级客客户端JDK版本至1.8，支持TLSv1.2并向下兼容。
4. 如果是第三方回调，需要让其调用源站IP。

4.4 产品咨询

4.4.1 什么是被防护的 IP 地址?

源站IP是源站服务器所使用的公网IP，即被防护的IP地址。

高防IP是DDoS高防提供防护服务的IP地址。

DDoS高防服务通过高防IP代理源站IP对外提供服务，将所有的公网流量都引流至高防IP，进而隐藏源站，避免源站（用户业务）遭受大流量DDoS攻击。

4.4.2 DDoS 高防支持权重回源吗?

DDoS高防按照轮询机制回源，目前不支持按权重回源。您可以将高防回源到ELB公网IP，然后在ELB上使用按权重回源给ECS。

4.4.3 DDoS 高防可以跨区域使用吗?

DDoS高防是全局服务，不区分区域（Region），因此可以跨区域使用。多个Region使用一个DDoS高防，业务系统响应的性能不会降低。

4.4.4 什么是 CNAME?

CNAME就是DNS别名。DNS A记录是把域名直接解析到IP地址，而CNAME记录则是把域名解析到另外一个域名（别名）。例如，域名“www.abc.com”配置了CNAME别名“ccd01c25c8535fa4.huaweisafedns.com”。用户访问“www.abc.com”时，DNS通过第一次解析获得了CNAME别名后，自动对CNAME别名“ccd01c25c8535fa4.huaweisafedns.com”进行二次解析获得该CNAME对应的真实IP地址。解析过程由DNS协议自动完成。

4.4.5 什么是 BGP?

BGP（Border Gateway Protocol，边界网关协议）是运行于TCP上的一种自治系统（AS）的路由协议，是唯一能够妥善处理不相关路由域间的多路连接的协议。

4.4.6 什么是 DDoS 高防的源站端口?

用户的实际业务对外提供服务所使用的端口号。

4.4.7 什么是 DDoS 高防源站 IP?

用户的实际业务对外提供服务所使用的公网IP地址。

4.4.8 什么是需要防护的网站 IP 地址?

DDoS高防提供防护服务的IP地址是高防IP。源站服务器所使用的公网IP即源站IP是被防护的IP地址。高防IP代替源站IP向客户提供服务，使源站IP不直接暴露出去。DDoS高防服务通过高防IP代理源站IP对外提供服务，将所有的公网流量都引流至高防IP，进而隐藏源站，避免源站（用户业务）遭受大流量DDoS攻击。

4.4.9 什么是业务带宽?

业务带宽是高防机房清洗后回源给源站的业务流量带宽。当流量超过业务带宽时，可能会出现丢包的情况。

4.4.10 什么是转发协议?

用户的实际业务对外提供服务所使用的协议类型，例如TCP（Transmission Control Protocol）、UDP（User Datagram Protocol）。

4.4.11 接入 DDoS 高防时业务会中断吗?

业务接入高防时需要将域名解析从源站修改为高防IP。为避免域名解析生效过程中业务中断，建议您的源站继续提供服务，直到域名全部解析到高防IP，再将源站下线。

4.4.12 同一个域名可以绑定多个高防吗?

如果该域名目前已绑定的高防正在被使用，由于域名冲突的原因，无法再绑定高防。需先将该域名解析回源站，解绑目前已绑定的高防后，再使用该域名重新绑定到其他的高防。

4.4.13 客户端访问的 IP 为什么是华为的高防 IP?

您购买高防服务后，把域名解析到高防IP（Web业务把域名解析指向高防IP，非Web业务把业务IP替换成高防IP），接入高防IP后，所有访问经过高防IP过滤。

高防IP代替源站IP提供访问，客户端访问的IP即为华为的高防IP。

4.4.14 为什么接入 DDoS 高防后 IP 地址流量增长?

配置DDoS高防服务后，部分攻击者会记录源站使用过的IP，存在绕过高防直接攻击源站IP的情况，建议更换源站IP。

4.4.15 IP 流量增长是否会暴露源站 IP?

不会。当您把业务接入DDoS高防后，域名解析到高防IP（Web业务把域名解析指向高防IP，非Web业务把业务IP替换成高防IP），所有访问经过高防IP过滤，进而隐藏源站，避免源站遭受大流量DDoS攻击。

4.4.16 DDoS 高防如何防护业务?

DDoS高防服务通过高防IP代理源站IP对外提供服务，将所有的公网流量都引流至高防IP，进而隐藏源站，避免源站（用户业务）遭受大流量DDoS攻击。

- 对于通过域名对外提供服务的系统，修改DNS配置，将对外提供的业务域名解析到华为云提供的CNAME。
- 对于通过IP对外提供服务的系统，将对外提供的业务IP变更为高防IP。

4.4.17 DDoS 高防是否支持 SSL 双向认证?

不支持。

4.4.18 证书上传到 DDoS 高防后，可以编辑和删除吗?

网站类业务接入DDoS高防时，如果选择“HTTPS/WebSockets”协议并且“源站类型”选择“源站IP”时，您需要导入证书。

证书上传到DDoS高防后，您可以进入“域名配置”界面，在域名所在行的“业务类型”列中，单击“更换”来刷新证书。

DDoS高防暂不支持删除证书功能。

4.4.19 超过 DDoS 高防业务带宽会有什么影响?

如果您的业务流量超过购买的DDoS高防实例的业务带宽，将触发流量限速，可能导致随机丢包。

4.4.20 DDoS 高防是软件高防还是硬件高防?

DDoS高防为软件高防服务，与成本相对较高的传统硬件高防相比，DDoS高防部署更方便，业务接入DDoS高防后即可防护，且可以查看DDoS高防的防护日志，了解当前业务的网络安全状态。

相比传统硬件高防，DDoS高防在防护性能上有以下优势：

- **海量带宽**

  15T以上DDoS高防总体防御能力，单IP最高1000G防御能力，抵御各类网络层、应用层的DDoS攻击。

- **高可用服务**

  全自动检测和攻击策略匹配，实时防护；业务流量采用集群分发，性能高，时延低，稳定性好。

- **弹性防护**

  通过基础带宽+弹性带宽的购买方式，DDoS防护阈值支持弹性调整，可随时升级更高级别的防护。

4.4.21 DDoS 高防支持防护 IPv6 吗?

DDoS高防仅部分业务接入点支持防护IPv6。您也可以使用DDoS原生基础防护（Anti-DDoS流量清洗）和DDoS原生高级防护服务防护IPv6。

说明

网络请求在经过DDoS高防代理后，客户业务源站所见的源IP为高防的回源IP，客户可以通过TOA协议，从TCP报文中的tcp option字段获取真实源IP，支持获取IPv6真实访问源。

在开启了DDoS高防的Web基础防护或将源站配置为华为云WAF的场景，当前无法获取IPv6真实访问源。

4.4.22 为什么 DDoS 高防和 ELB 的流量不一致?

DDoS高防统计的是某段时间内的秒级流量峰值，单位是bps。ELB统计的是一段时间内的流量平均值，所以ELB的流量统计值会比DDoS高防的流量值小。

需要注意的是，入方向流量超过DDoS的业务带宽，会触发限流，业务带宽需要根据业务实际流量进行设置。

如果需要查看DDoS高防的业务带宽，建议通过DDoS高防Console控制台进行查看。

4.5 计费问题

4.5.1 DDoS 高防如何计费?

价格体系

DDoS高防服务需要购买高防实例。

计费方式

华为云DDoS高防根据您选择业务宽带、保底防护宽带和弹性防护宽带的规格计费。

表 4-4 计费项信息

计费项	计费方式	计费说明
业务带宽	预付费，按月/年付费。	高防机房将清洗后的干净流量，转发给源站所占用的带宽。 **说明** 高防机房在华为云外，建议购买的高防业务带宽规格大于或等于源站出口带宽。
保底防护带宽	预付费，按月/年付费。	用于防御攻击的保底带宽。如果攻击峰值小于等于客户购买的保底防护带宽，客户无需支付月/年费以外的额外费用。
弹性防护带宽	后付费，按天付费。	用于防御攻击的最大可用带宽。弹性防护带宽的具体价格请参考**价格计算器**中“价格详情”页签。

弹性防护宽带的计费详情：

- 计费标准：取决于当日发生的攻击峰值，即一天内发生多次攻击，仅峰值最高的攻击参与计费。
- 后付费：根据实际攻击峰值产生弹性防护费用。如果没有攻击，便不会产生弹性防护费用。
- 规格可调整：DDoS高防服务管理控制台支持调整弹性防护带宽，调整后新的弹性防护带宽可立即生效。
- 可避免付费：将弹性防护带宽设置为与基础防护带宽一致，则可避免产生弹性防护的后付费费用。

4.5.2 用户缴费后，缴费状态无法更新是什么原因?

用户缴费后，没有收到缴费信息，支付平台的缴费状态无法更新为“已缴费”，可能的原因和解决方法如下：

- 充错号码，请在交易记录中查看充值号码是否有误。
- 运营商下发缴费短信存在延迟，请联系运营商或华为技术支持查询缴费状态。

4.5.3 如果购买弹性防护，一个月都没有攻击，不需要任何费用吗?

这种情况下，仅需要支付基础防护带宽的包月费用，不产生其它额外的费用。

4.5.4 攻击超过弹性防护能力上限会怎样?

如果攻击流量超过防护能力，该IP会强制进入黑洞，阻断全部流量。

4.5.5 当前选择的弹性防护带宽是 100G，发现不够用，可以改成 200G 吗?

可以。DDoS高防服务管理控制台支持调整弹性防护带宽，调大或者调小都可以。

须知

调整后新的弹性防护带宽可立即生效，但计费标准取决于当日发生的攻击峰值。

4.5.6 一个 IP 一天内被攻击多次，费用该怎么计算?

以当天（0:00-24:00）攻击的峰值为准，只收取一次。例如某IP一天内分别遭到50G、100G、200G共三次攻击，则当天的弹性防护付费账单按照200G攻击的弹性计费标准收取。

4.5.7 购买了高防实例，如何停止使用弹性防护能力，避免产生弹性防护的后付费费用?

可将购买的高防实例的弹性防护带宽设置为与基础防护带宽一致，当遭受超出基础防护带宽流量的攻击时，将不会启用弹性防护带宽进行防护。

4.5.8 如何为 DDoS 高防续费?

您可以在DDoS高防管理控制台中，进行高防IP服务的续费。

须知

请确认续费的账号同时具有“CAD Administrator”和“BSS Administrator”角色，或者该账号具有“Tenant Administrator”角色。

- BSS Administrator：费用中心、资源中心、账号中心的所有执行权限。项目级角色，在同项目中勾选。
- Tenant Administrator：除统一身份认证服务外，其他所有服务的所有执行权限。

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 单击实例下的“续费”。

步骤5 在续费页面选择续费时长，单击“去支付”，完成相应支付流程。

----结束

4.5.9 如何退订 DDoS 高防?

DDoS高防不支持无理由退订。如果满足可退订条件，可以联系客服申请退订。

可退订条件

在购买或使用过程中发现无法与业务匹配，可联系客服申请退订。例如：您的业务服务器部署在海外，而您购买了DDoS高防大陆站，导致DDoS高防服务无法使用。

已经正常使用的高防实例无法退订。通过DDoS高防服务后台，如判断出高防实例已经正常使用过，此种情况无法退订。

4.5.10 如何开通自动续费?

您可以为购买的DDoS高防实例开通自动续费功能，当购买的服务期满时，系统会按照续费周期进行续费。

须知

请确认开通自动续费的账号同时具有“CAD Administrator”和“BSS Administrator”角色，或者该账号具有“Tenant Administrator”角色。

- BSS Administrator：费用中心、资源中心、账号中心的所有执行权限。项目级角色，在同项目中勾选。
- Tenant Administrator：除统一身份认证服务外，其他所有服务的所有执行权限。

如果您当前正在购买DDoS高防，可参考如下开通方式：

1. 在购买DDoS高防时，可以勾选“自动续费”选项，完成自动续费。
   具体操作如下：
   选择“购买DDoS防护 > 购买时长 > 自动续费”。

图 4-11 购买时长

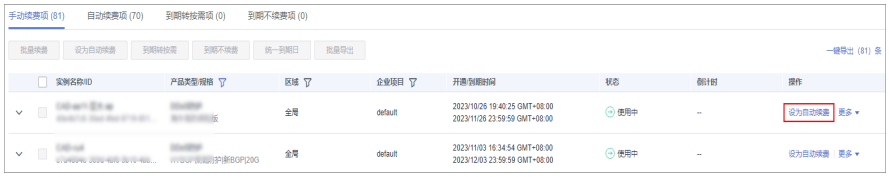
如果您当前已经购买DDoS高防，可参考如下开通方式：

在“续费管理”界面，完成自动续费。

具体操作如下：

1. 登录管理控制台，单击右上方的“费用”。
   系统进入“费用中心”页面。
2. 在左侧导航栏，选择“订单管理 > 续费管理”。
3. 选择对应高防实例进行自动续费开通操作。

图 4-12 自动续费



4.5.11 退订后重新购买 AAD，原配置数据可以保存吗？

不能保存。当您退订AAD后，AAD将不会保存配置数据。因此，重新购买AAD后，您需要重新将业务接入AAD。

有关退订AAD的详细操作，请参见**如何退订DDoS高防？**。

有关业务接入AAD的详细操作如下：

- 对于通过域名对外提供服务的系统，修改DNS配置，将对外提供的业务域名解析到华为云提供的CNAME。
- 对于通过IP对外提供服务的系统，将对外提供的业务IP变更为高防IP。

4.5.12 DDoS 高防弹性带宽具体怎么计费？

计费说明

DDoS高防实例的弹性带宽计费取当日多次DDoS攻击的峰值作为计费依据，不同场景费用说明如下：

- 当日DDoS攻击峰值≤保底防护带宽：不会产生弹性防护带宽费用。

- 保底防护带宽＜当日DDoS攻击峰值＜弹性防护带宽：会产生弹性防护带宽费用。
- 当日DDoS攻击峰值≥弹性防护带宽：会产生弹性防护带宽费用。

计费示例

- 保底防护带宽＜攻击峰值＜弹性防护带宽：**弹性防护带宽用量（计费）=当日攻击峰值－保底防护带宽**
- 攻击峰值≥弹性防护带宽：**弹性防护带宽用量（计费）=弹性防护带宽－保底防护带宽**

例如：三个DDoS高防实例，保底防护带宽均为20Gbps，弹性防护带宽规格为100Gbps。三个实例当日遭受多次DDoS攻击，弹性防护带宽计费规则如下。

表 4-5 计费规则

实例	攻击峰值	是否产生费用	说明
实例A	20Gbps	否	攻击峰值未超过保底防护带宽，不计费。
实例B	80Gbps	是	计费防护带宽：80Gbps-20Gbps=60Gbps。
实例C	120Gbps	是	120Gbps大于弹性防护带宽100Gbps。 计费防护带宽：100Gbps-20Gbps=80Gbps。