DDoS 防护

产品介绍

文档版本 02

发布日期 2023-08-31

华为技术有限公司

版权所有 © 华为技术有限公司 2024。 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


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

 版权所有 © 华为技术有限公司

目 录

 版权所有 © 华为技术有限公司

 版权所有 © 华为技术有限公司

1 了解 DDoS 攻击

1.1 什么是 DDoS 攻击

拒绝服务（Denial of Service，简称DoS）攻击也称洪水攻击，是一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，服务暂时中断或停止，导致合法用户不能够访问正常网络服务的行为。当攻击者使用网络上多个被攻陷的电脑作为攻击机器向特定的目标发动DoS攻击时，称为分布式拒绝服务攻击（Distributed Denial of Service Attack，简称DDoS）。常见DDoS攻击类型如表1-1所示。

表 1-1 常见 DDoS 攻击类型

攻击类型	说明	举例
网络层攻击	通过大流量拥塞被攻击者的网络带宽，导致被攻击者的业务无法正常响应客户访问。	NTP Flood攻击。
传输层攻击	通过占用服务器的连接池资源，达到拒绝服务的目的。	SYN Flood攻击、ACK Flood攻击、ICMP Flood攻击。
会话层攻击	通过占用服务器的SSL会话资源，达到拒绝服务的目的。	SSL连接攻击。
应用层攻击	通过占用服务器的应用处理资源，极大消耗服务器处理性能，达到拒绝服务的目的。	HTTP Get Flood攻击、HTTP Post Flood攻击。

1.2 遭受 DDoS 攻击后如何向网监报案?

当业务遭受大量DDoS攻击时，首先可以采用DDoS高防服务来保障业务的稳定，另一方面建议立即向网监部门进行报案。

版权所有 © 华为技术有限公司

报案流程

1. 遭受DDoS攻击后，您应该尽快向当地网监部门进行报案，并根据网监部门的要求提供相关信息。
2. 网监部门判断是否符合立案标准，并进入网监处理流程。

   说明

   具体立案标准请咨询当地的网监部门。
3. 正式立案后，华为云会配合网监部门负责人提供攻击取证。

华为云能提供什么相关证据?

您的报案在网监部门立案后，华为云将配合网监部门提供以下协助：

- 华为云会配合网监部门，向网监负责人提供您在华为云平台上的业务的流量日志、遭受攻击信息等。

  说明

  由于相关数据将作为法律证据，因此无法直接提供给您。您可以在华为云管理控制台中自行查看攻击流量的相关信息。
- 华为云不能对流量日志和攻击信息等进行分析，直接给出谁是攻击者的结论。

  说明

  由于华为云不是法官，无法判定谁有罪；不具有执法权，不能进行立案调查；华为云只能作为证据的提供者和证人。
- 华为云会及时响应网监部门的协助调查要求，配合开展工作。

  建议您在遭受安全攻击时，参考当地网监部门的立案调查标准，积极请求网警进行立案调查。

自主查看攻击流量的相关信息：

您可以在华为云管理控制台查看流量、攻击事件等。

1.3 华为云黑洞策略

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

版权所有 © 华为技术有限公司

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1-2进行处理。

表 1-2 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。

黑洞阈值

黑洞阈值指华为云为客户提供的基础防御阈值，当流量超过限定的阈值时，华为云会采取黑洞策略封堵IP。

清洗原理

系统对业务攻击流量进行实时检测，一旦发现针对云主机的攻击行为，将把业务流量从原始网络路径引流到华为云DDoS清洗系统。通过华为云DDoS清洗系统对该IP的流量进行识别，丢弃攻击流量，将正常流量转发至目标IP，减缓攻击对服务器造成的损害。

自助解封规则说明

说明

购买了DDoS防护（**DDoS原生高级防护**）的用户，每个月将免费赠送三次自助解封配额，解封配额当月如果未用完将在月底清零。

- 对于同一防护IP，当日首次解封时间必须大于封堵时间30分钟以上才能解封。解封时间=$2^{(n-1)}$*30分钟（n表示解封次数）。

  例如，当日第一次解封需要封堵开始后30分钟，第二次解封需要封堵开始后60分钟，第三次解封需要封堵开始后120分钟。

版权所有 © 华为技术有限公司

- 对于同一防护IP，如果上次解封时间和本次封堵时间间隔小于30分钟，则本次解封时间的间隔=2^n*30分钟（n表示解封次数）。

  例如，该IP已解封过一次，上次解封时间为10:20，本次发生封堵时间为10:40，两者时间间隔小于30分钟，则本次需要封堵开始后120分钟才能解封，即12:40可以解封（本次发生封堵时间10:40后120分钟）。

  须知

  如果您在30分钟内解封过其他任一IP，即使满足以上条件，也不能对该IP进行解封。

- DDoS防护会根据风控自动调整自助解封次数和间隔时长。

版权所有 © 华为技术有限公司

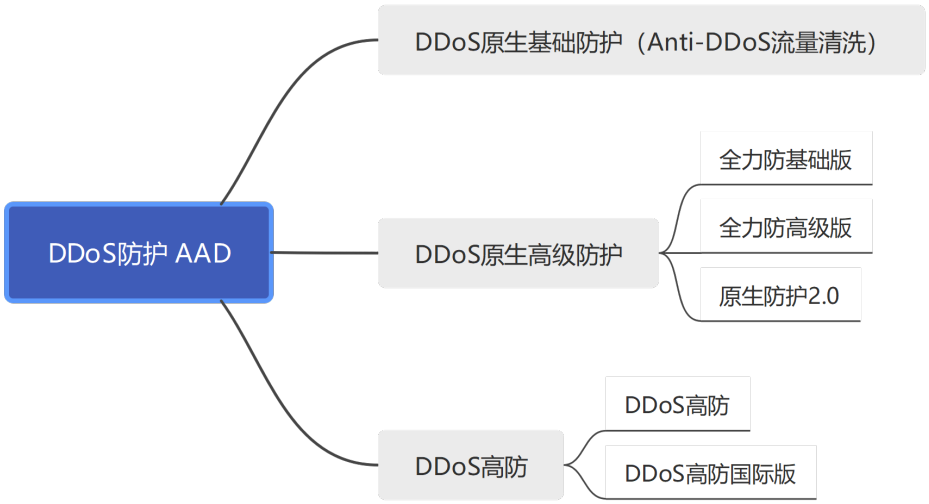
2 了解 DDoS 防护 AAD

2.1 如何选择 DDoS 防护产品

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。

图 2-1 DDoS 防护分支介绍



各服务防护方案说明

各子服务详细介绍如**表2-1**所示。

版权所有 © 华为技术有限公司

表 2-1 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。

版权所有 © 华为技术有限公司

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。	如果您的业务服务器部署在中国内地，且业务主要用户来自中国内地，不能保障中国内地以外的用户的访问质量（有可能出现网络访问质量问题）。 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。	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。	如果您的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，不能保障中国内地用户的访问质量（存在约300毫秒的平均访问延时）。 **说明** 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。

各服务支持的 DDoS 攻击类型

表 2-2 DDoS 防护支持的业务类型

DDoS攻击类型	DDoS原生基础防护（Anti-DDoS流量清洗）	DDoS原生高级防护	DDoS高防
畸形报文	√	√	√

版权所有 © 华为技术有限公司

DDoS攻击类型	DDoS原生基础防护（Anti-DDoS流量清洗）	DDoS原生高级防护	DDoS高防
传输层DDoS攻击	√ SYN Flood攻击（小包攻击）防御效果一般，推荐使用DDoS原生高级防护或DDoS高防。	√	√
DNS DDoS攻击	×	×	√
连接型DDoS攻击	×	仅全力防高级版支持	√
Web应用层DDoS攻击	×	×	√

说明

- √：表示支持。
- ×：表示不支持。

2.2 DDoS 原生基础防护

2.2.1 什么是 DDoS 原生基础防护

什么是 DDoS 原生基础防护?

DDoS原生基础防护（Anti-DDoS流量清洗）服务（以下简称Anti-DDoS）免费为华为云内公网IP资源（弹性云服务器、弹性负载均衡），提供网络层和应用层的DDoS攻击防护（如泛洪流量型攻击防护、资源消耗型攻击防护），并提供攻击拦截实时告警，有效提升用户带宽利用率，保障业务稳定可靠。

功能特性

Anti-DDoS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。

Anti-DDoS可以帮助用户缓解以下攻击：

- Web服务器类攻击
  SYN Flood攻击。
- 游戏类攻击

 版权所有 © 华为技术有限公司

UDP（User Datagram Protocol ） Flood攻击、SYN Flood、TCP（Transmission Control Protocol ）类攻击、分片攻击等。

Anti-DDoS还提供以下功能：

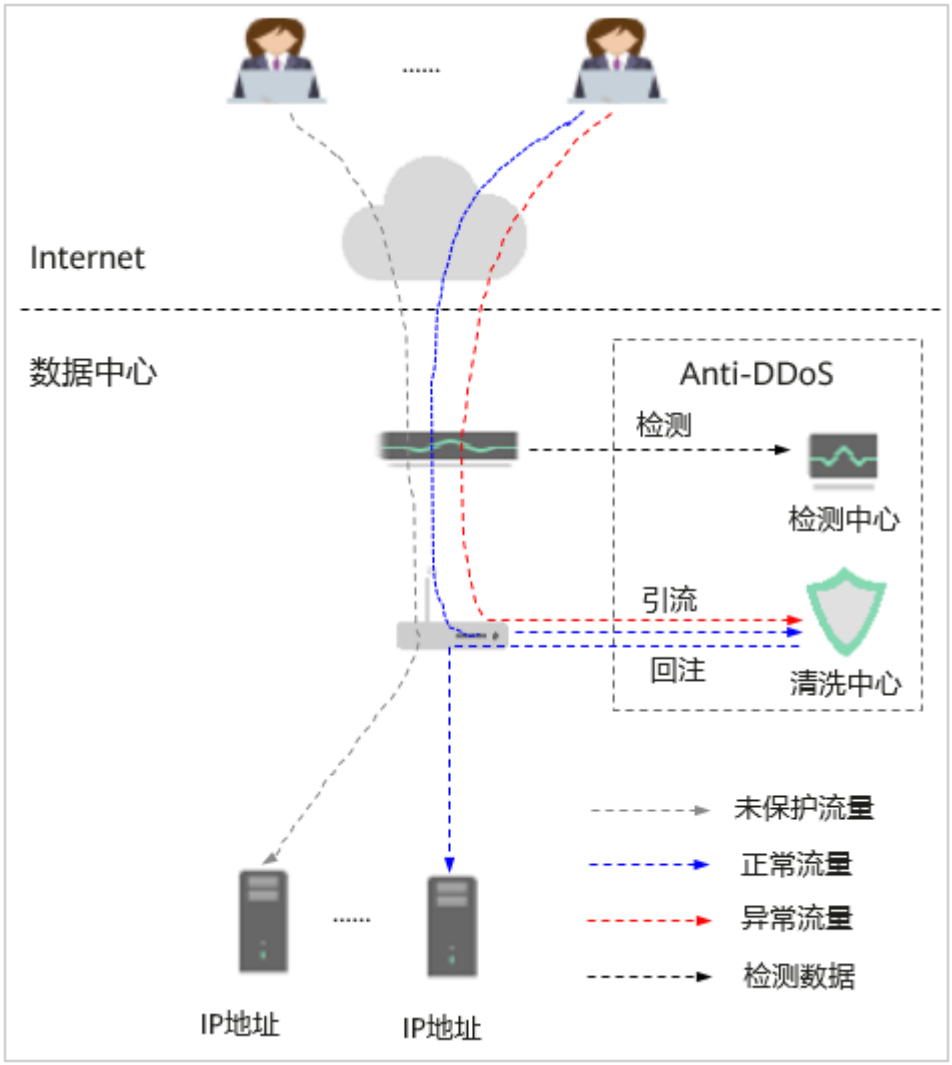
- 为单个公网IP地址提供监控记录，包括当前防护状态、当前防护配置参数、24小时内流量情况、24小时内异常事件。
- 为用户所有进行防护的公网IP地址提供拦截报告，支持查询攻击统计数据，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10和共拦截攻击次数等。

2.2.2 应用场景

Anti-DDoS仅对公有云内的公网IP提供DDoS攻击防护。

Anti-DDoS设备部署在机房出口处，网络拓扑架构如图2-2所示。

图 2-2 网络拓扑架构图



检测中心根据用户配置的安全策略，检测网络访问流量。当发生攻击时，将数据引流到清洗设备进行实时防御，清洗异常流量，转发正常流量。

版权所有 © 华为技术有限公司

Anti-DDoS流量清洗服务提供最高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。

2.2.3 产品优势

DDoS原生基础防护（Anti-DDoS流量清洗）为华为云用户提供DDoS攻击防护，其产品优势如下：

- 优质防护

  实时监测，及时发现DDoS攻击，丢弃攻击流量，将正常流量转发至目标IP。

  提供优质带宽，保证业务连续性和稳定性，保障用户访问速度。
- 全面精准

  海量IP黑名单库，精准有效；七层过滤的手术刀式清洗机制，动态流量基线智能学习。
- 秒级响应

  先进的逐包检测机制，各类攻击威胁秒级响应；强大的清洗设备性能，极低的清洗时延。
- 自动开启

  本服务在购买EIP时自动开启防护，无需采购昂贵清洗设备，无需安装。
- 免费使用

  本服务是免费服务，使用时不需要购买资源，不产生任何费用，用户可放心使用。

2.3 DDoS 原生高级防护

2.3.1 什么是 DDoS 原生高级防护

什么是 DDoS 原生高级防护?

DDoS原生高级防护（Cloud Native Anti-DDoS，CNAD）是华为云推出的针对华为云ECS、ELB、WAF、EIP等云服务直接提升其DDoS防御能力的安全服务。DDoS原生高级防护对华为云上的IP生效，通过简单的配置，DDoS原生高级防护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，确保云服务上的业务安全、可靠。

功能特性

DDoS原生高级防护支持以下防护功能：

- 透明接入

  无需修改域名解析、设置源站保护，可以直接对华为云上公网IP资源进行防护。
- 全力防护

  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，尽可能帮助您防御DDoS攻击。全力防护的防护能力随着华为云网络能力的不断提升而相应提升。
- 联动防护

 版权所有 © 华为技术有限公司

开启联动防护后，可自动联动调度DDoS高防对DDoS原生高级防护对象中的云资源进行防护。

- IPv4/IPv6双协议防护

  支持同时为IPv6和IPv4两种类型的IP提供防护，满足您对IPv6类型业务防护需求。

- 流量清洗

  DDoS原生高级防护检测到IP的入流量超过设置的阈值时，触发流量清洗。

- IP黑白名单

  通过配置IP黑名单或IP白名单来封禁或者放行访问DDoS原生高级防护的源IP，从而限制访问您业务资源的用户。

- 协议封禁

  根据协议类型一键封禁访问DDoS原生高级防护的源流量。例如，访问DDoS原生高级防护的源流量如果没有UDP（User Datagram Protocol，用户数据报协议）业务，建议封禁UDP协议。

业务规格

各版本每个实例支持的业务规格说明如表2-3所示。

须知

DDoS原生高级防护只能防护相同区域的云资源，不能跨区域（Region）防护。

表 2-3 DDoS 原生高级防护业务规格

规格	DDoS原生防护-全力防基础版	DDoS原生防护-全力防高级版	原生防护2.0
计费模式	包年包月	包年包月	包年包月+按需计费
带宽类型	云原生网络，全动态BGP（不支持静态BGP）。	云原生网络，多线BGP。	云原生网络，全动态BGP（不支持静态BGP）。
防护能力	共享全力防护，不低于20G。	共享全力防护，最高可达1T。	中国大陆：共享全力防护，不低于20G。 中国大陆外：运营商跨境防护。
防护IP数	范围为50～500，且防护IP数必须设置为5的倍数。	范围为50～500，且防护IP数必须设置为5的倍数。	50-1000个，，且防护IP数必须设置为50的倍数。
防护次数	不限次数	不限次数	不限次数

版权所有 © 华为技术有限公司

规格	DDoS原生防护-全力防基础版	DDoS原生防护-全力防高级版	原生防护2.0
IP更换次数	不支持	不支持	不支持
业务带宽	最低100M，最大支持上限20,000Mbps。	最大支持40,000Mbps。	最大支持20,000Mbps。

2.3.2 应用场景

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：

- 业务部署在华为云服务上，且云服务能提供公网IP资源
- 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

2.3.3 产品优势

DDoS原生高级防护为软件DDoS防护服务，与成本相对较高的传统硬件防护相比，可一键提升华为云ECS、ELB、WAF、EIP等云服务的DDoS防御能力，具有以下优势：

- 快速接入

  无需配置转发规则，快速接入服务即可直接提升华为云上EIP的防护能力。

  说明

  DDoS原生高级防护-全力防高级版只能防护专属EIP。
- 弹性防护能力

  遭受大规模攻击时自动调用当前区域华为云最大DDoS防护能力提供全力防护。
- 海量清洗带宽

  拥有多线BGP防护带宽，轻松抵御DDoS攻击，可以满足活动大促、活动上线等重要业务的安全稳定性保障需求。
- 卓越清洗能力

  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。
- 丰富的防护报表

  提供多维度统计报表，通过查看流量信息，了解当前网络安全状态。

版权所有 © 华为技术有限公司

2.4 DDoS 高防

2.4.1 什么是 DDoS 高防

DDoS高防（Advanced Anti-DDoS）是企业重要业务连续性的有力保障。当您的服务器遭受大流量DDoS攻击时，DDoS高防可以保护用户业务持续可用。DDoS高防通过高防IP代理源站IP对外提供服务，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。可服务于华为云、非华为云及IDC的互联网主机。

说明

DDoS高防实例到期≥30个自然日时，DDoS高防将停止转发业务流量，实例将被释放。如果您不需要继续使用DDoS高防，请务必在到期30个自然日之前，将业务流量从高防切换到源站服务器。

- 未接入DDoS高防

  未接入高防时，源站直接对互联网暴露，一旦发生DDoS攻击，很容易导致源站瘫痪。

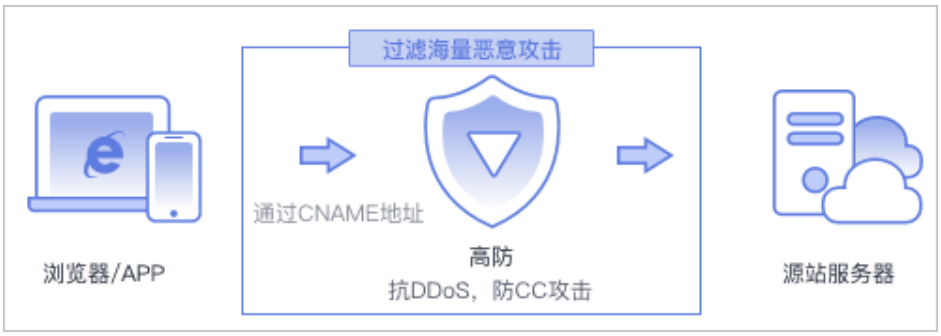
  图 2-3 未接入 DDoS 高防示意图

- 接入DDoS高防

  当您购买DDoS高防并将业务接入DDoS高防后，网站类业务把域名解析指向高防IP，非网站类的业务IP将替换成高防IP，DDoS高防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。

  图 2-4 接入 DDoS 高防示意图

版权所有 © 华为技术有限公司

DDoS 高防工作原理

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。DDoS高防引流和转发原理示意图如下：

- 客户

  访问源站（用户业务）的客户。
- 源站IP

  源站服务器所使用的公网IP，也是被防护的IP地址，应避免对外暴露（泄露）。
- 高防IP

  与源站IP相对应，用于代替源站IP来面向客户提供服务，使源站IP不直接暴露出去。
- 回源IP

  是高防机房代替客户去和源站服务器通信的若干个IP地址（高防机房会将客户的IP随机转换成某个回源IP，并由这个回源IP代替客户IP去和源站服务器通信）。

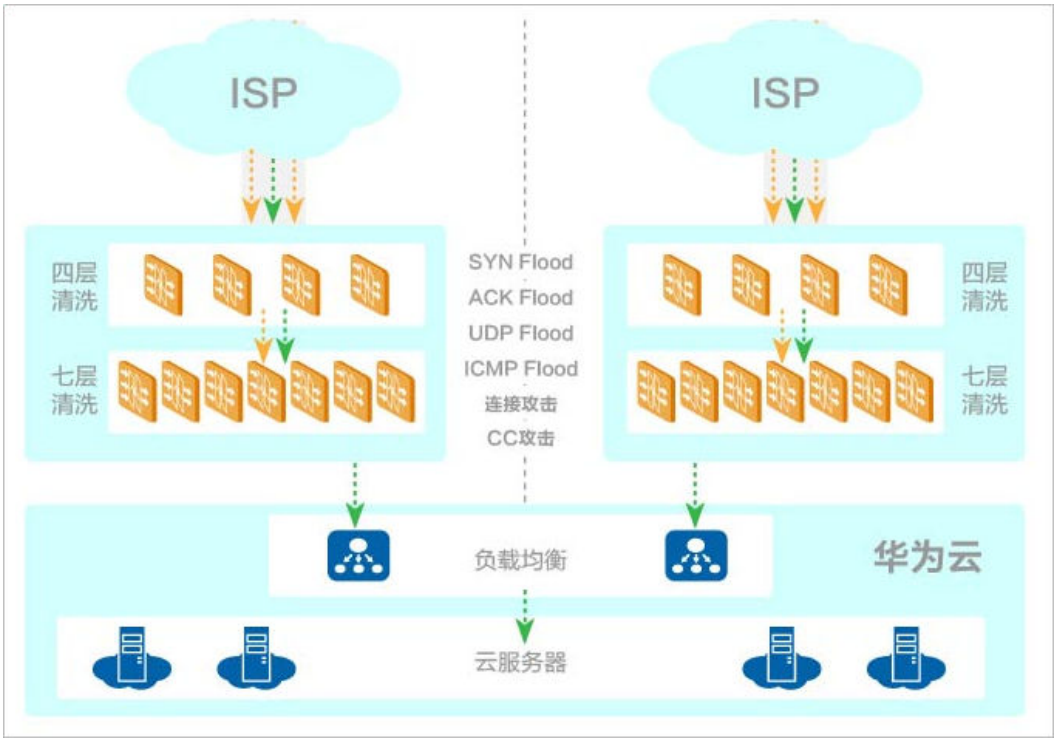
DDoS高防为用户提供DDoS防护服务，可以防护SYN Flood、UDP Flood、ACK Flood、ICMP Flood、DNS Query Flood、NTP reply Flood、CC攻击等各类网络层、应用层的DDoS攻击。

版权所有 © 华为技术有限公司

业务架构

DDoS高防服务采用分层防御、分布式清洗，通过精细化多层过滤防御技术，可以有效检测和过滤攻击流量。网络拓扑示意图如图2-5所示。

图 2-5 网络拓扑示意图



2.4.2 功能规格

DDoS高防的功能规格说明如表2-4所示，套餐内的功能规格不能降低。

表 2-4 DDoS 高防功能规格

参数	说明
接入类型	提供两种接入方式：“网站类”和“IP接入”。 **说明** 网站类：华为云通过智能算法为您选择最佳接入点，并且不再提供固定的高防IP。推荐使用“域名接入”的用户购买并使用。 IP接入：仅提供IP端口防护，提供固定的高防IP。推荐使用“四层转发规则”的用户购买并使用。
实例	每个用户默认最多可以购买5个实例。
线路	线路选择：“BGP”。
业务接入点	提供以下三种选择，请根据您业务的地理位置自行选择： • 华北1：线路支持中国移动、中国电信、中国联通、北京教育网、鹏博士、河北广电、重庆广电。 • 华东2：支持中国移动、中国电信、中国联通。

版权所有 © 华为技术有限公司

参数	说明
IP类型	● IPv4：防护IPv4源站需要选择IPv4实例。 ● IPv6：防护IPv6源站需要选择IPv6实例。
防护域名数（仅选择“网站类”接入时可选择）	每个实例免费提供50个域名防护数量。可以付费增加，最多可支持200个。 **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。
保底防护带宽	保底防护带宽支持配置的范围说明如下： 10Gbps、20Gbps、30Gbps、60Gbps、100Gbps、300Gbps、400Gbps、500Gbps、600Gbps、800Gbps、1000Gbps。 如果需要提升防护性能，可以设置“弹性防护带宽”。
弹性防护带宽	每个实例的弹性防护带宽每天可以修改3次。弹性防护带宽支持配置的范围说明如下： 10Gbps、20Gbps、30Gbps、40Gbps、50Gbps、60Gbps、70Gbps、80Gbps、100Gbps、200Gbps、300Gbps、400Gbps、500Gbps、600Gbps、700Gbps、800Gbps、1000Gbps。 当攻击超过保底防护带宽时扣费，无攻击或者攻击未超过保底防护带宽时不会产生扣费。 攻击峰值大于所选的弹性防护带宽，则高防IP会被黑洞，在购买高防实例后，可以根据业务实际情况，修改弹性防护带宽。 **说明** 弹性防护带宽不能小于保底防护带宽。如果用户选择的弹性防护带宽等于保底防护带宽，则弹性防护功能不生效。
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。 每个实例免费赠送100Mbps业务带宽，可以付费增加，最大支持2Gbps。即从DDoS高防到源站的回源过程会产生业务流量，如果访问流量在100Mbps以内，可以直接免费使用。
转发协议	● 四层协议：TCP、UDP。 ● 七层协议：HTTP/WebSocket、HTTPS/WebSockets。
接入方式	● 网站类业务接入 用于网站业务，客户通过把高防CNAME配置到DNS的方式接入高防IP。 ● 非网站类业务接入 用于APP、PC客户端类业务，客户通过把高防CNAME配置到DNS或者把高防IP直接配置到客户端的方式将流量接入高防。
黑洞解封时间	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。 **说明** 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。

版权所有 © 华为技术有限公司

参数	说明
防护对象	支持华为云、非华为云及IDC的互联网主机。

DDoS 高防 IPv4 和 IPv6 的差异

DDoS高防实例支持IPv4高防IP和IPv6高防IP，查看下表方便您了解两者的功能差异。

⚠ 注意

防护IPv4源站需要选择IPv4实例，防护IPv6源站需要选择IPv6实例。请您在购买实例的时候注意您要防护的IP类型。

功能	IPv4高防IP	IPv6高防IP
黑白名单	√	√
区域流量封禁	√	×
协议流量封禁	√	√
CC防护	√	√
Web基础防护	√	√
更新域名证书	√	√
更新域名的高防IP解析线路	√	√
修改源站IP	√	√
CNAME自动调度	√	√
查看攻击事件	√	√
查看攻击类型分布	√	√
查看CC攻击防护情况	√	√
获取客户真实源IP	√	×

2.4.3 应用场景

DDoS高防服务的主要使用场景包括：娱乐（游戏）、金融、政府、电商、媒资、教育（在线）等行业：

版权所有 © 华为技术有限公司

- 娱乐（游戏）

  娱乐（游戏）行业是DDoS攻击的重灾区，高防IP能保证游戏的可用性和持续性，提高用户体验，在商家活动、节日游戏等旺季时段提供防护。

- 金融

  满足金融行业的合规性要求，保证线上交易的实时性、安全稳定性。

- 政府

  满足国家政务云建设标准的安全需求，为重大会议、活动、敏感时期提供安全保障，确保民生服务正常可用，维护政府公信力。

- 电商

  为用户访问互联网提供防护，使业务正常不中断，在电商大促等活动时段提供防护功能。

- 企业

  保证企业站点服务持续可用，避免DDoS攻击造成经济和企业形象损失问题，降低维护费用，节省安全成本。

2.4.4 产品优势

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，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。

DDoS高防可以防护海量DDoS攻击，具备精准、弹性、高可靠、高可用等优势。

- **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。

- **专业运营团队**

  7*24小时运营团队随时应对；专业的运营人员随时解答您的疑问，为您的业务保驾护航。

版权所有 © 华为技术有限公司

3 服务版本差异

部署方式以及其区别

华为云DDoS防护服务有两种部署方式。

- 透明模式：可以直接提升您在华为云上资产的DDoS防护能力。

- 代理模式：通过将您的服务器IP隐藏在DDoS高防IP之后，由DDoS高防IP为您的服务器抵御DDoS攻击，从而达到防护您的业务连续，不受DDoS攻击影响目的。

表 3-1 透明模式和代理模式的区别

项目	透明模式	代理模式
计费方式	包年包月	包年包月

版权所有 © 华为技术有限公司

项目	透明模式	代理模式
服务版本	DDoS原生基础防护（免费） DDoS原生高级防护全力防-基础版 DDoS原生高级防护全力防-高级版	DDoS高防 DDoS高防国际版
使用场景	业务服务器部署在华为云上，华为云上可访问的公网IP	业务服务器部署在华为云、非华为云上，通过公网可访问
防护对象	IP	IP、域名
优势	透明接入，直接防护服务器地址 华为云原生网络防护，时延低	对外隐藏服务器地址 高防清洗中心防护，防护强 可以防护华为云和非华为云场景

各版本支持的规格

表 3-2 各版本支持的规格

项目	DDoS原生基础防护	DDoS原生高级防护全力防-基础版	DDoS原生高级防护全力防-高级版	DDoS原生高级防护-原生防护2.0	DDoS高防-网站防护
计费类型	免费	包年包月	包年包月	实例为包年包月计费；业务带宽支持包年包月和按需计费。	包年包月
接入模式	透明接入	透明接入	透明接入	透明接入	DNS解析牵引
网络类型	原生网络	云原生网络，全动态BGP（不支持静态BGP）	云原生网络，多线BGP	云原生网络，全动态BGP（不支持静态BGP）	多线BGP

版权所有 © 华为技术有限公司

项目	DDoS原生基础防护	DDoS原生高级防护全力防-基础版	DDoS原生高级防护全力防-高级版	DDoS原生高级防护-原生防护2.0	DDoS高防-网站防护
防护对象	华为云内EIP	华为云内EIP	华为云专属EIP	华为云内EIP	互联网上可访问的域名（华为云上+华为云下）
支持协议	IPv4、IPv6	IPv4、IPv6	IPv4	IPv4、IPv6	IPv4、IPv6
对象数量	无限制	50-500个	50-500个	50-1000个	50-200个
业务带宽	不涉及	100Mbps-20Gbps	100Mbps-40Gbps	100Mbps-20Gbps	100Mbps-2Gbps

须知

同一个DDoS高防实例只能支持一种IP协议（IPv4或IPv6），如您需要多个协议，请购买多个高防实例。

各版本支持的防护能力

表 3-3 各版本支持的防护能力

项目	DDoS原生基础防护（免费）	DDoS原生高级防护全力防-基础版	DDoS原生高级防护全力防-高级版	DDoS高防-网站防护	DDoS高防-IP防护
防护能力	• 中国大陆Region：不高于5G • 非中国大陆Region：不高于500M	共享全力防护，不低于20G	共享全力防护，最高可达1T	1T（可多个实例叠加）	1T

版权所有 © 华为技术有限公司

项目	DDoS原生基础防护（免费）	DDoS原生高级防护全力防-基础版	DDoS原生高级防护全力防-高级版	DDoS高防-网站防护	DDoS高防-IP防护
DDoS防护	清洗阈值	• 黑白名单 • 清洗阈值 • 协议封印 • 水印防护	• 黑白名单 • 清洗阈值 • 协议封印 • 水印防护 • 连接防护	• 黑白名单 • 海外封禁 • UDP封禁 **须知** 国际版当前仅支持线下配置	• 黑白名单 • 海外封禁 • UDP封禁 **须知** 国际版当前仅支持线下配置
应用防护	不涉及	联动独享WAF支持	联动独享WAF支持	• 默认3000 QPS • 大于3000QPS需联动华为云WAF、独享WAF支持	联动独享WAF支持

版权所有 © 华为技术有限公司

4 安全

4.1 责任共担

华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

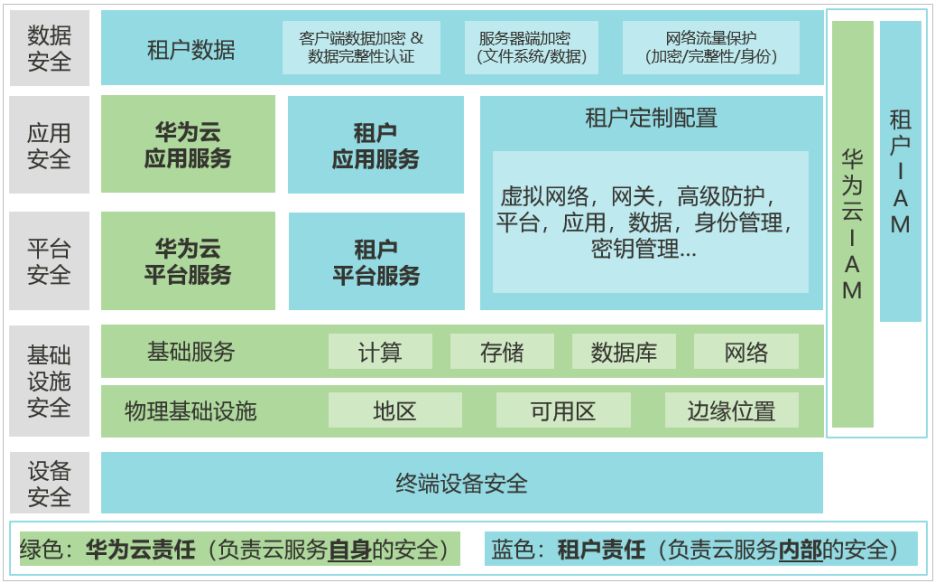
安全性是华为云与您的共同责任，如**图4-1**所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

版权所有 © 华为技术有限公司

图 4-1 华为云安全责任共担模型



4.2 身份认证与控制

身份认证

无论用户通过DDoS控制台还是API访问DDoS，都会要求访问请求方出示身份凭证，并进行身份合法性校验，同时提供登录保护和登录验证策略加固身份认证安全。DDoS服务基于统一身份认证服务（IAM），支持三种方式身份认证方式：**用户名密码**、**访问密钥**、**临时访问密钥**。同时还提供**登录保护**及**登录验证策略**。

访问控制

DDoS防护服务基于统一身份认证服务（IAM）通过IAM系统角色和IAM细粒度授权来进行访问控制。详细如下：

- **DDoS原生基础防护权限管理**

4.3 数据保护技术

DDoS不存储用户敏感数据，并且对用户数据传输进行加密保护，以防止个人数据泄露，保证您的个人数据安全。

数据保护手段	简要说明
传输加密（HTTPS）	用户个人敏感数据（如证书）将通过TLS 1.2进行传输中加密，所有华为云DDoS的API调用都支持 HTTPS 来对传输中的数据进行加密。
个人数据保护	用户在DDoS上的配置，由DDoS通过控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露或防止别的用户修改您的配置，保证您的个人数据安全。

版权所有 © 华为技术有限公司

数据保护手段	简要说明
隐私数据保护	DDoS会对存储的用户审计数据进行敏感数据脱敏。
数据销毁	DDoS在用户主动删除实例，或用户销户的情况下，会删除对应用户的审计实例。

4.4 审计与日志

云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

CTS支持配置关键操作通知。用户可将与DDoS相关的高危敏感操作，作为关键操作加入到CTS的实时监控列表中进行监控跟踪。当用户使用DDoS服务时，如果触发了监控列表中的关键操作，那么CTS会在记录操作日志的同时，向相关订阅者实时发送通知。

4.5 服务韧性

华为云数据中心按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减小由硬件故障、自然灾害或其他灾难带来的服务中断，华为云为所有数据中心提供灾难恢复计划。

4.6 监控安全风险

DDoS通过多种方式提供监控数据。

查看 DDoS 数据报表

DDoS控制台提供防护监控数据。用户可以通过DDoS控制台查看防护资源的监控信息。详细如下：

子服务	监控对象	监控内容
DDoS原生基础防护	公网IP	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。
DDoS原生高级防护	防护对象	包括实例的接收流量、攻击流量，以及DDoS防护趋势图、清洗流量峰值、攻击类型分布、TOP10被攻击IP等信息

版权所有 © 华为技术有限公司

子服务	监控对象	监控内容
DDoS高防	高防IP 防护域名	DDoS攻击防护 可以查看高防实例线路的高防入流量峰值、攻击流量峰值和DDoS攻击次数信息，以及流量和报文两个维度的攻击类型分布、DDoS攻击事件、TOP5攻击类型流量清洗等信息。 CC攻击防护 可以查看防护域名请求与攻击次数、攻击类型分布、TOP5攻击源IP的次数等信息。

通过 CES 服务查看 DDoS 监控

DDoS防护同时也提供基于云监控服务CES的资源和操作监控能力，帮助用户监控账号下的防护资源，执行自动实时监控、告警和通知操作。用户可以实时掌握防护资源所产生的信息。

4.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 4-2 合规证书下载

版权所有 © 华为技术有限公司

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 4-3 资源中心

版权所有 © 华为技术有限公司

5 权限管理

5.1 DDoS 原生基础防护

如果您需要对华为云上创建的DDoS原生基础防护（Anti-DDoS）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制他们对云上资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有Anti-DDoS的使用权限，但是不希望他们拥有删除Anti-DDoS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用Anti-DDoS，但是不允许删除Anti-DDoS的权限，控制他们对Anti-DDoS资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用Anti-DDoS服务的其它功能。

Anti-DDoS 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

Anti-DDoS部署时通过物理区域划分，为项目级服务，授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问Anti-DDoS时，需要先切换至授权区域。

如表5-1所示，包括了Anti-DDoS的所有系统角色。由于云上各服务之间存在业务交互关系，Anti-DDoS服务的角色依赖其他服务的角色实现功能。因此给用户授予Anti-DDoS服务的角色时，需要同时授予依赖的角色，Anti-DDoS服务的权限才能生效。

 版权所有 © 华为技术有限公司

表 5-1 Anti-DDoS 系统角色

策略名称	描述	依赖关系
Anti-DDoS Administrator	Anti-DDoS服务的管理员权限。	依赖Tenant Guest角色。 Tenant Guest：全局级角色，在全局项目中勾选。
Anti-DDoS FullAccess	Anti-DDoS流量清洗服务所有权限	-
Anti-DDoS ReadOnlyAccess	Anti-DDoS流量清洗服务只读权限	-

5.2 DDoS 原生高级防护

如果您需要对华为云上购买的CNAD资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制员工对云上资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这些员工拥有CNAD的使用权限，但是不希望这些员工拥有删除CNAD资源等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CNAD，但是不允许删除CNAD资源的权限，控制员工对CNAD资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CNAD的其它功能。

CNAD 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CNAD部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问CNAD时，不需要切换区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对CNAD服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如表5-2所示，包括了CNAD的所有系统角色。

版权所有 © 华为技术有限公司

表 5-2 CNAD 系统角色

系统角色/策略名称	描述	类别	依赖关系
CNAD FullAccess	DDoS原生高级防护所有权限。	系统策略	进行付费操作（例如，购买DDoS原生高级防护实例）时需要同时具有CNAD FullAccess和BSS Administrator角色，或者具有Tenant Administrator角色。
CNAD ReadOnlyAccess	DDoS原生高级防护只读权限。	系统策略	无。

CNAD FullAccess 策略内容

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cnad:*:*"
            ]
        }
    ]
}
```

CNAD ReadOnlyAccess 策略内容

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cnad:*:get*",
                "cnad:*:list*"
            ]
        }
    ]
}
```

5.3 DDoS 高防

如果您需要对云上购买的AAD资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制员工对云上资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这些员工拥有AAD的使用权限，但是不希望这些员工拥有删除AAD等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用AAD，但是不允许删除AAD的权限，控制员工对AAD资源的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用AAD的其它功能。

版权所有 © 华为技术有限公司

AAD 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

AAD部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问AAD时，不需要切换区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对AAD服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如表5-3所示，包括了AAD的所有系统角色。

表 5-3 AAD 系统角色

系统角色/策略名称	描述	类别	依赖关系
CAD Administrator	DDoS高防服务的管理员权限。	系统角色	进行付费操作（例如，购买DDoS高防实例、升级规格）时需要同时具有CAD Administrator和BSS Administrator角色，或具有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。 **须知** CAD Administrator系统角色即将下线，为了确保正常使用AAD，建议您尽快授予用户AAD FullAccess或AAD ReadOnlyAccess系统策略。
AAD FullAccess	DDoS高防服务所有权限。	系统策略	进行付费操作（例如，购买DDoS高防实例、升级规格）时需要同时具有AAD FullAccess和BSS Administrator角色，或具有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。

版权所有 © 华为技术有限公司

系统角色/策略名称	描述	类别	依赖关系
AAD ReadOnlyAccess	DDoS高防服务只读权限，拥有该权限的用户仅能查看DDoS高防。	系统策略	无。

AAD FullAccess 策略内容

```
{
        "Version": "1.1",
        "Statement": [{
            "Action": [
                "aad:*"
            ],
          "Effect": "Allow"
        }]
}
```

AAD ReadOnlyAccess 策略内容

```
{
        "Version": "1.1",
        "Statement": [{
            "Action": [
                "aad:*:get",
                "aad:*:list"
            ],
          "Effect": "Allow"
        }]
}
```


版权所有 © 华为技术有限公司

A 修订记录

发布日期	修改说明
2023-08-31	第二次正式发布。 ● 调整了目录结构。 ● **如何选择DDoS防护产品**，优化内容描述。
2022-07-01	第一次正式发布。

版权所有 © 华为技术有限公司