Anti-DDoS 流量清洗

产品介绍

文档版本 08

发布日期 2021-08-06

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。

目 录

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。

2 基本概念

2.1 华为云黑洞策略

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。

什么是黑洞?

黑洞是指云主机受攻击流量超过防护黑洞阈值时，华为云屏蔽云主机的外网通信。当云主机进入黑洞24小时后，黑洞会自动解封。若解封之后，系统监控到流量仍然超过防护的黑洞阈值，则再次触发黑洞。

由于黑洞是华为云向运营商购买的服务，而运营商对黑洞解除时间和频率都有严格的限制，所以黑洞状态无法人工解除，需耐心等待系统自动解封。

为什么需要黑洞，为什么华为云不能免费帮用户无限防御 DDoS 攻击?

DDoS防御需要成本，其中最大的成本就是带宽费用。带宽是华为云向运营商购买，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。华为云在控制成本的前提下，会尽量为用户免费防御DDoS攻击，但当攻击流量超出阈值时，会进行拉黑。因此，为保障业务连续性，需要您购买DDoS高防产品，以提升DDoS防御能力。

2.2 清洗原理、黑洞阈值

华为云Anti-DDoS流量清洗服务默认开启，为用户提供DDoS攻击防御功能。

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中引流到华为云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。

黑洞阈值

黑洞阈值指华为云为客户提供的基础攻击防御范围，当攻击超过限定的阈值时，华为云会采取黑洞策略封堵IP。

Anti-DDoS流量清洗免费防护的黑洞触发阈值为500Mbps。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。

2.3 Anti-DDoS 流量清洗与高防区别

Anti-DDoS流量清洗为用户提供基本防御，高防为付费增值服务，提供专家贴身保障，详见表2-1。

表 2-1 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	• 防护策略固定 • 全局通用策略	• 防护策略丰富 • 专业CC防护能力 • 定制化策略
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

2.4 常见 DDoS 攻击类型

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攻击类型见表2-2所示。

表 2-2 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。

攻击类型	说明	举例
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。
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。

3 功能特性

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、HTTP Flood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。

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。

4 产品优势

Anti-DDoS流量清洗服务为华为云用户提供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，每日特征库更新；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

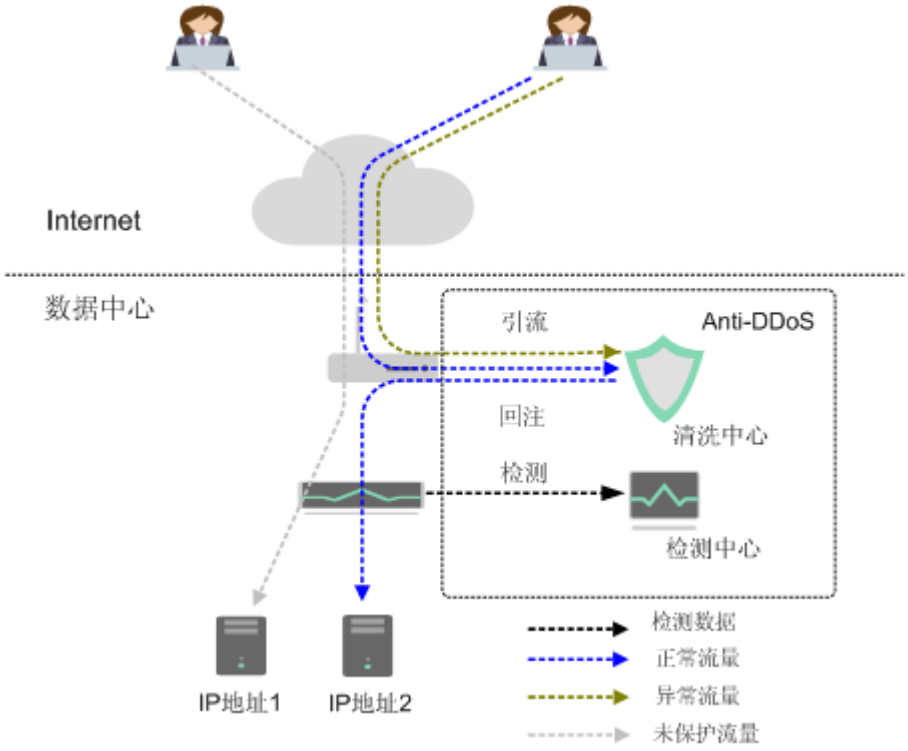
  本服务是免费服务，使用时不需要购买资源，不产生任何费用，用户可放心使用。

5 使用场景

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5-1所示。

图 5-1 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。

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。

6 计费说明

Anti-DDoS流量清洗服务为用户免费提供最高500Mbps的DDoS攻击防护。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。

7 访问与使用

7.1 如何访问

公有云提供了Web化的服务管理平台，即管理控制台管理方式和基于HTTPS请求的API（Application Programming Interface）管理方式。

- 管理控制台管理方式

  如果用户已注册华为云，可登录管理控制台，单击管理控制台左上角的 ，选择区域和项目，在主页选择“安全与合规 > Anti-DDoS流量清洗”，访问Anti-DDoS服务。

- 基于HTTPS请求的API管理方式

  用户可通过接口方式访问Anti-DDoS，具体操作请参见《Anti-DDoS流量清洗API参考》。

7.2 如何使用

Anti-DDoS使用说明如下：

- 为IP地址开启Anti-DDoS防护后，即可对其提供DDoS攻击保护。
  - Anti-DDoS已实现自动开启防护的功能。
  - 购买弹性公网IP前，您可以在“Anti-DDoS流量清洗服务”的“公网IP”页签下，单击“设置默认防护策略”，为新购买的弹性公网IP设置“默认防护策略”。购买弹性公网IP后，自动开启Anti-DDoS的“默认防护策略”的DDoS攻击防护，如图7-1所示。

图 7-1 设置默认防护策略

- 如果在购买弹性公网IP前，您没有设置“默认防护策略”，那么新购买的弹性公网IP，自动开启Anti-DDoS的“默认防护”模式的DDoS攻击防护，如图7-2所示。

  “默认防护”模式：当实际业务的UDP（User Datagram Protocol）流量大于120Mbps或者TCP（Transmission Control Protocol）流量大于35000pps时，将触发流量清洗，Anti-DDoS将拦截攻击流量。

图 7-2 默认防护模式

说明

- Mbps=Mbit/s即兆比特每秒（1,000,000bit/s），Million bits per second的缩写，是一种传输速率单位，指每秒传输的位（比特）数量。
- PPS是Packets Per Second的简称，是常用的网络吞吐率的单位，即每秒发送多少个分组数据包，网络的性能通常用吞吐率（throughput）这个指标来衡量。

– 如果您删除了公网IP，则会自动关闭Anti-DDoS防护，并在CTS里可以查询到该事件。

- 当IP地址受到DDoS攻击时，如果需要接收提醒信息（短信或Email），可开启告警通知。
- 在防护过程中，用户可根据业务实际情况，及时调整防护策略。
- 开启防护后，可通过查看监控报告和拦截报告，了解详细网络安全状况。
- 开启Anti-DDoS防护后，不允许关闭防护。

7.3 与其他云服务的关系

与云审计服务的关系

云审计服务（Cloud Trace Service，简称CTS）记录Anti-DDoS相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

表 7-1 CTS 支持的 Anti-DDoS 操作列表

操作名称	事件名称
开启Anti-DDoS防护	openAntiddos
关闭Anti-DDoS防护	deleteAntiddos
调整Anti-DDoS安全设置	updateAntiddos

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为Anti-DDoS提供了权限管理的功能。需要拥有Anti-DDoS Administrator权限的用户才能使用Anti-DDoS服务。如需开通该权限，请联系拥有Security Administrator权限的用户，详细内容请参见《统一身份认证服务用户指南》。

与消息通知服务的关系

消息通知服务（Simple Message Notification，简称SMN）提供消息通知功能。Anti-DDoS开启告警通知后，如果IP地址受到DDoS攻击时用户会收到消息通知（通知方式由用户设置，短信、邮件等）。

有关SMN的详细内容，请参见《消息通知服务用户指南》。

7.4 Anti-DDoS 权限管理

如果您需要对华为云上创建的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，您可以在华为云帐号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。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。

如果华为云帐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。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

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”，然后在指定区域对应的项目中设置相关权限，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7-2**所示，包括了Anti-DDoS的所有系统角色。由于华为云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。

表 7-2 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。

- **IAM产品介绍**
- **创建用户组并授予Anti-DDoS权限**

A 修订记录

发布日期	修改说明
2022-05-19	第九次正式发布。 CC防护功能下架。
2021-08-06	第八次正式发布。 修改管理控制台入口描述。
2020-05-27	第七次正式发布。 新增**计费说明**。
2020-01-07	第六次正式发布。 **如何使用**，增加了默认防护功能的相关说明。
2019-12-16	第五次发布。 国际站域名切换。
2019-12-04	第四次发布。 **与其他云服务的关系**，优化相关描述。
2019-11-21	第三次发布。 图片增加图标题及固定文档ID。
2018-05-28	第二次正式发布。 **与其他云服务的关系**，新增通过云审计服务查看Anti-DDoS的审计日志的操作步骤。
2017-12-31	第一次正式发布。