Anti-DDoS 流量清洗

用户指南

文档版本 03

发布日期 2021-09-30

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 产品介绍 1
1.1 什么是 Anti-DDoS 流量清洗? 1
1.2 基本概念 1
1.2.1 清洗原理、黑洞阈值 1
1.2.2 常见 DDoS 攻击类型 1
1.3 功能特性 2
1.4 产品优势 3
1.5 使用场景 3
1.6 访问与使用 4
1.6.1 如何访问 4
1.6.2 如何使用 4
1.6.3 与其他云服务的关系 5
1.6.4 Anti-DDoS 权限管理 5
2 查看公网 IP 7
3 开启告警通知 9
4 配置 Anti-DDoS 防护策略 11
5 查看监控报表 14
6 查看拦截报告 17
7 常见问题 19
7.1 产品咨询类 19
7.1.1 什么是 Anti-DDoS 流量清洗? 19
7.1.2 什么是 SYN Flood 攻击和 ACK Flood 攻击? 19
7.1.3 什么是 CC 攻击? 19
7.1.4 什么是慢速连接攻击? 20
7.1.5 什么是 UDP 攻击和 TCP 攻击? 20
7.1.6 如何理解“百万级的 IP 黑名单库”? 20
7.1.7 Anti-DDoS 的触发条件是什么? 20
7.1.8 Anti-DDoS 流量清洗进行防御时对正常业务有影响吗? 20
7.1.9 Anti-DDoS 清洗机制是怎样的? 20
7.1.10 Anti-DDoS 流量清洗服务有何使用限制? 20
7.2 基本功能类 20

7.2.1 Anti-DDoS 流量清洗服务能帮助缓解哪些类型的攻击？ 20
7.2.2 ELB 防护和 ECS 防护有什么区别？ 21
7.2.3 为什么同一个公网 IP 地址的清洗次数和攻击次数不一致？ 21
7.3 告警通知类 21
7.3.1 攻击事件能否及时通知？ 21
7.3.2 用户收到告警通知，是否正常？ 21
A 修订记录 22

1 产品介绍

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。

1.2 基本概念

1.2.1 清洗原理、黑洞阈值

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DDoS清洗系统，通过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

黑洞阈值是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，系统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300Mbps。

1.2.2 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。
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。

1.3 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、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。

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。

1.4 产品优势

Anti-DDoS流量清洗服务为用户提供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

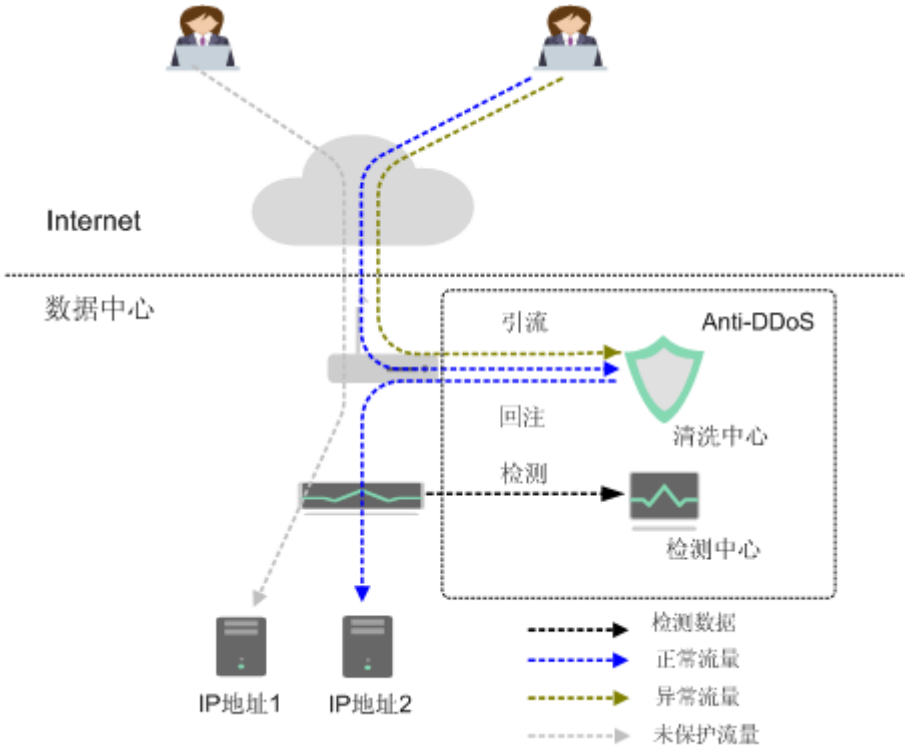
  自动开启防护，无需安装。
- 免费使用

  本服务是免费服务，用户可放心使用。

1.5 使用场景

Anti-DDoS设备部署在机房出口处，网络拓扑架构如**图1-1**所示。

图 1-1 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300Mbps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。

1.6 访问与使用

1.6.1 如何访问

- 管理控制台管理方式

  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 > Anti-DDoS流量清洗”，访问Anti-DDoS。
- 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》。

1.6.2 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。
- 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。

1.6.3 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 1-2 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》。

1.6.4 Anti-DDoS 权限管理

如果您需要对云上创建的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云资源的访问。

通过IAM，您可以在帐号中给员工创建IAM用户，并授权控制他们对云资源的访问范围。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。

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1-3所示，包括了Anti-DDoS的所有系统角色。由于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 1-3 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。

2 查看公网 IP

操作场景

该任务指导用户查看公网IP。

须知

- 自动开启Anti-DDoS“默认防护”。
- 开启Anti-DDoS防护后，不允许关闭。

前提条件

- 已获取管理控制台的登录帐号与密码。

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，选择“安全 > Anti-DDoS流量清洗”，进入Anti-DDoS服务管理界面。

步骤4 选择“公网IP”页签，查看公网IP，参数说明如表2-1所示。

图 2-1 查看公网 IP

说明

- 全部开启防护：单击“全部开启防护”，为当前区域下所有未开启防护的公网IP开启Anti-DDoS防护。
- 开启Anti-DDoS“默认防护”后，当检测到报文总流量达到120Mbps时，触发流量清洗功能。如果需要配置Anti-DDoS的防护策略，可以修改防护参数，详细操作请参见**配置Anti-DDoS防护策略**。
- Anti-DDoS最高提供300Mbps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。
- 在“所有防护状态”搜索框中选择防护状态，“公网IP”界面将只显示对应状态的公网IP。
- 在搜索框中输入公网IP或公网IP的关键字，单击 或 ，可以搜索指定的公网IP。

表 2-1 参数说明

参数名称	说明
公网IP	Anti-DDoS防护的公网IP地址。 **说明** 如果公网IP已开启Anti-DDoS防护，单击公网IP，可以跳转至该公网IP的“监控报表”页面。
防护状态	公网IP的防护状态，包括： • 正常 • 设置中 • 未开启 • 清洗中 • 黑洞中

----结束

3 开启告警通知

操作场景

为Anti-DDoS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、邮件等）。否则，无论DDoS攻击流量多大，用户都只能登录管理控制台自行查看，无法收到报警信息。

前提条件

- 已获取管理控制台的登录帐号与密码。

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，选择“安全 > Anti-DDoS流量清洗”，进入Anti-DDoS服务管理界面。

步骤4 选择“告警通知”页签，设置告警通知，如图3-1所示，相关参数说明如表3-1所示。

图 3-1 设置告警通知

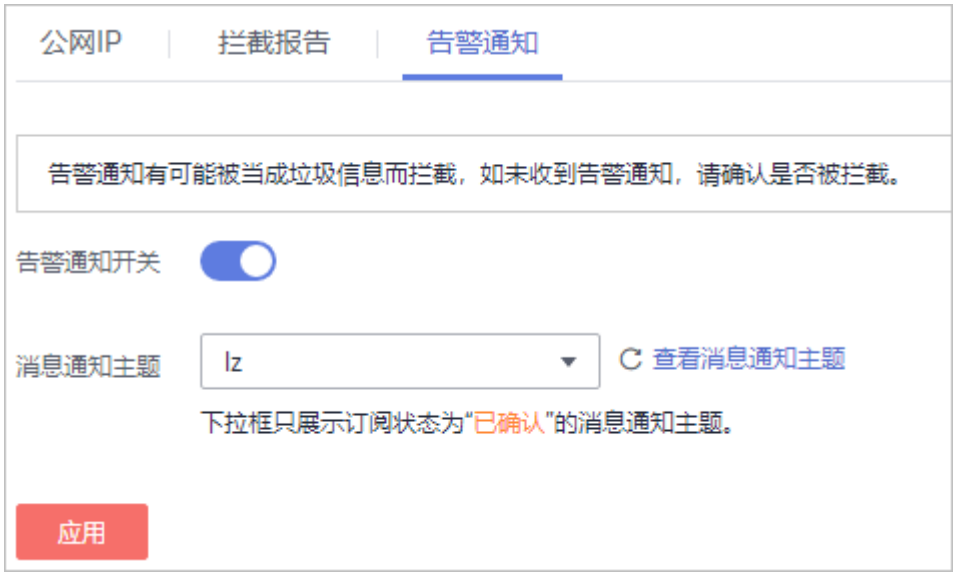


表 3-1 设置告警通知

参数名称	说明	示例
告警通知开关	开启或关闭告警通知，说明如下： •  ：开启状态。 •  ：关闭状态。 如果告警通知为关闭状态，单击  ，将告警通知状态设置为  。	
消息通知主题	可以选择使用已有的主题，或者单击“查看消息通知主题”创建新的主题。 更多关于主题的信息，请参见《消息通知服务用户指南》。	-

步骤5 单击“应用”，开启告警通知。

----结束

4 配置 Anti-DDoS 防护策略

操作场景

开启Anti-DDoS防护后，用户在使用过程中可以根据实际情况调整Anti-DDoS防护策略。

前提条件

已获取管理控制台的登录帐号与密码。

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，选择“安全 > Anti-DDoS流量清洗”，进入Anti-DDoS服务管理界面。

步骤4 选择“公网IP”页签，在待配置Anti-DDoS防护策略的公网IP地址所在行，单击“防护设置”。

图 4-1 防护设置

步骤5 在“防护设置”对话框中，修改相应的参数，如图4-2所示，参数说明如表4-1所示。

图 4-2 防护设置

表 4-1 参数说明

参数	说明
防护设置	• 默认防护：此模式下，“流量清洗阈值”默认为“120Mbps”，即当实际业务的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。 • 手动设置：此模式下，可按照实际业务流量设置“流量清洗阈值”和开启“CC防护”。 **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（Packets Per Second，简称PPS），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。

参数	说明
流量清洗阈值	Anti-DDoS检测到IP的入流量超过该阈值时，触发流量清洗。 ● 当“防护设置”为“默认防护”时，“流量清洗阈值”默认为“120Mbps”。 ● 当“防护设置”为“手动设置”时，“流量清洗阈值”可按照实际业务流量进行设置，建议设置为与所购买带宽最接近的数值，但不超过购买带宽。 **说明** 当实际业务流量触发流量清洗阈值时，Anti-DDoS仅拦截攻击流量；当实际业务流量未触发流量清洗阈值时，无论是否为攻击流量，都不会进行拦截。 请按照实际业务访问流量选择参数。建议选择与所购买带宽最接近的数值，但不超过购买带宽。
CC防护	● 关闭：关闭CC防护。 ● 开启：开启CC防护。 **说明** 有Web业务且支持完整HTTP协议栈的客户端才能使用CC防护。因为CC防护采用“重定向”或“重定向+验证码”模式。如果客户端不支持，建议关闭CC防护。
HTTP请求速率	仅当“CC防护”为“开启”时，需要设置此参数。单位为“qps”，即每秒查询率（Query Per Second），是对一个特定的查询服务器在规定时间内所处理流量多少的衡量标准，在因特网上，作为域名系统服务器的机器的性能经常用每秒查询率来衡量。 该参数用于防御对网站的大量恶意请求，当网站HTTP请求速率达到所设参数时触发CC防护。一般情况下，如果防护弹性IP地址，建议该参数值不大于5000，如果防护弹性负载均衡，则可以选择较大的值。 建议设置为所部署业务平均每秒能处理的HTTP请求个数。Anti-DDoS检测到的总请求数量超过设置的“HTTP请求速率”时，会自动开启流量清洗。参数值过大会导致CC防护不能及时触发。 ● 实际HTTP请求速率低于设置的数值时，用户所部署的业务能够处理所有的HTTP请求，不需要Anti-DDoS的参与。 ● 实际HTTP请求速率等于或高于设置的数值时，Anti-DDoS会触发CC防护，对每个请求进行分析检查，会影响正常请求的响应速度。

步骤6 单击“确定”，保存配置。

----结束

5 查看监控报表

操作场景

用户可以查看单个公网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。

前提条件

已获取管理控制台的登录帐号与密码。

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，选择“安全 > Anti-DDoS流量清洗”，进入Anti-DDoS服务管理界面。

步骤4 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 5-1 查看监控报表

步骤5 在“监控报表”页面，可以查看该公网IP报表的详细指标，如图5-2和图5-3所示。

- 可查看包括当前防护状态、当前防护配置参数、24小时流量情况、24小时异常事件等信息。
- 24小时防护流量数据图，以5分钟一个数据点描绘的流量图，主要包括以下方面：
  - 流量图展示所选云服务器的流量情况，包括服务器的正常入流量以及攻击流量。

  - 报文速率图展示所选云服务器的报文速率情况，包括正常入报文速率以及攻击报文速率。
- 近1天内攻击事件记录表：近1天内云服务器的DDoS事件记录，包括清洗事件和黑洞事件。

图 5-2 查看流量监控报表

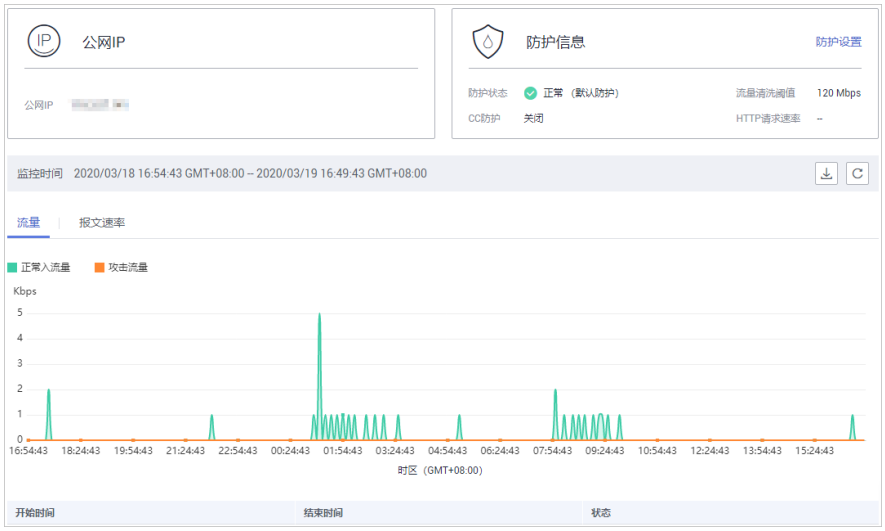
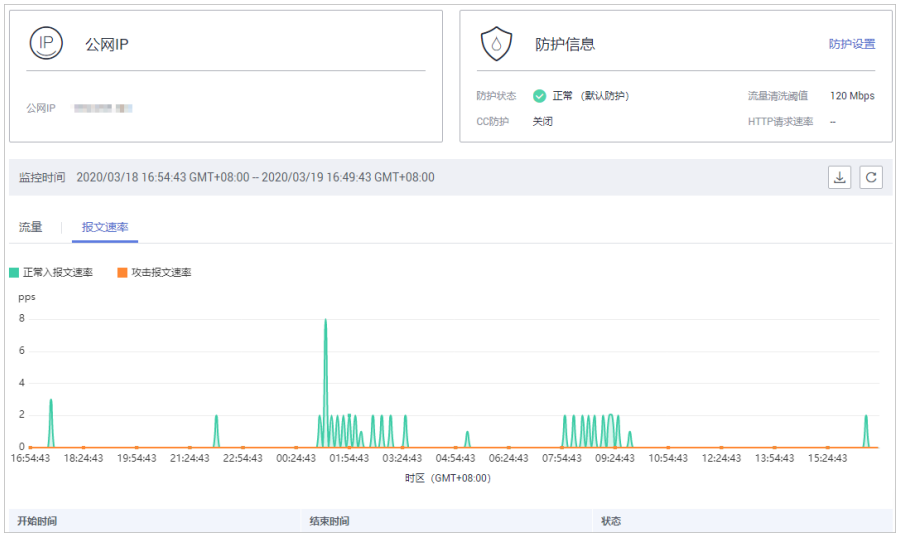


图 5-3 查看报文速率监控报表



说明

- 单击  ，可以将监控报表下载到本地，查看公网IP报表的详细指标信息。
- 在流量监控报表页面，单击 攻击流量 或 正常入流量，报表中将只显示“攻击流量”或“正常入流量”信息。
- 在报文速率监控报表页面，单击 攻击报文速率 或 正常入报文速率，报表中将只显示“攻击报文速率”或“正常入报文速率”信息。

----结束

6 查看拦截报告

操作场景

查看用户所有公网IP地址的防护统计信息，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10和共拦截攻击次数。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤1 登录管理控制台。

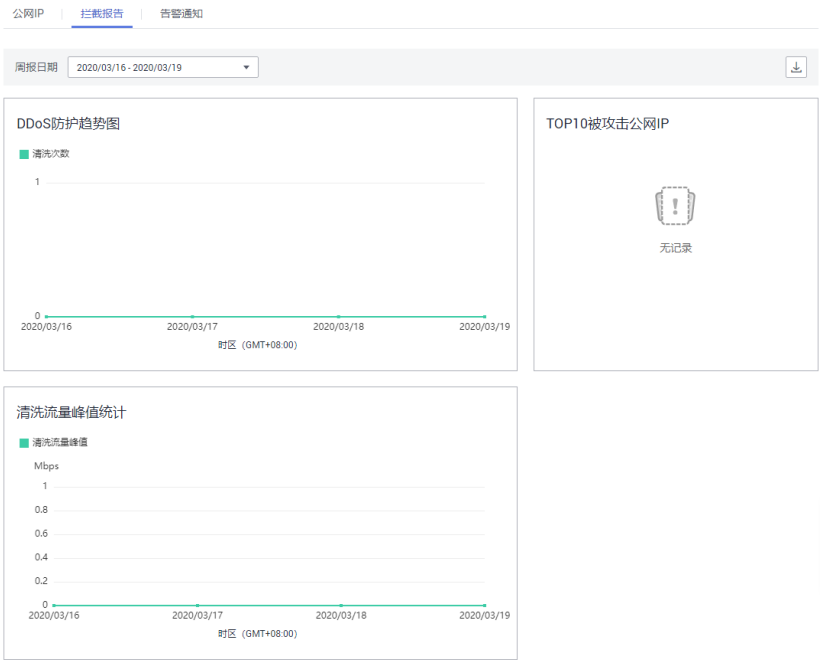
步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击，选择“安全 > Anti-DDoS流量清洗”，进入Anti-DDoS服务管理界面。

步骤4 选择“拦截报告”页签，可以查看用户所有公网IP地址的防护统计信息，如图6-1所示。

可通过选择“周报日期”来查看固定日期内的安全报告，查看时间范围为一周，支持查询前四周统计数据，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。

图 6-1 查看拦截报告



说明

单击 ，可以将拦截报表下载到本地，查看固定日期内的防护统计信息。

----结束

7 常见问题

7.1 产品咨询类

7.1.1 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。

7.1.2 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。

7.1.3 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。

7.1.4 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。

7.1.5 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。

7.1.6 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。

7.1.7 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。

7.1.8 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。

7.1.9 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。

7.1.10 Anti-DDoS 流量清洗服务有何使用限制?

提供的DDoS攻击防护取决于用户的网络出口带宽。

7.2 基本功能类

7.2.1 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。

7.2.2 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。

7.2.3 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。

7.3 告警通知类

7.3.1 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**。

7.3.2 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。

A 修订记录

发布日期	修改说明
2021-09-30	第三次正式发布。 • **清洗原理、黑洞阈值**，修改黑洞触发阈值参数。 • **配置Anti-DDoS防护策略**，更新界面截图。
2021-07-31	第二次正式发布。 **Anti-DDoS权限管理**，优化内容描述。
2020-11-06	第一次正式发布。