

Anti-DDoS 流量清洗

# 用户指南

文档版本 09  
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 设置默认防护策略.....	1
2 查看公网 IP.....	5
3 开启告警通知.....	7
4 配置 Anti-DDoS 防护策略.....	9
5 查看监控报表.....	13
6 查看拦截报告.....	16
7 权限管理.....	18
7.1 创建用户并授权使用 Anti-DDoS.....	18
A 修订记录.....	20

# 1 设置默认防护策略

您可以通过在“设置默认防护策略”窗口中，勾选“手动设置”，设置默认防护策略，新购买的公网IP均会按照已设置的默认防护策略开启DDoS攻击防护。

如果需要关闭设置的默认防护策略，您可以在“设置默认防护策略”窗口中将“防护设置”勾选为“默认防护”，关闭手动设置的默认防护策略。

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。“默认防护”模式的“流量清洗阈值”为“120Mbps”，“CC防护”为“关闭”状态。

## 前提条件

已获取管理控制台的登录帐号与密码。

## 手动设置默认防护策略

**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“安全与合规 > 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，单击“设置默认防护策略”，如图1-1所示。

图 1-1 设置默认防护策略



**步骤5** 在弹出的设置默认防护策略窗口中，勾选“手动设置”，如图1-2所示。

图 1-2 配置默认防护策略



步骤6 配置“流量清洗阈值”和“CC防护”。

表 1-1 参数说明

参数	说明
流量清洗阈值	<p>Anti-DDoS检测到IP的入流量超过该阈值时，触发流量清洗。</p> <p>“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。</p> <p><b>说明</b> 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。</p>
CC防护	<ul style="list-style-type: none"> <li>● 关闭：关闭CC防护。</li> <li>● 开启：开启CC防护。</li> </ul> <p><b>说明</b> 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。</p>
HTTP请求速率	<p>仅当“CC防护”为“开启”时，需要设置此参数。</p> <p>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。</p> <p>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。</p>


**步骤7** 单击“OK”，完成默认防护策略的设置。

默认防护策略设置完成后，新购买的公网IP均按照默认防护策略启动防护。若需要调整防护策略，请参见[配置Anti-DDoS防护策略](#)。

----结束

## 关闭手动设置的默认防护策略

若新购买的公网IP不需要按照手动设置的默认防护策略开启防护，您可以关闭手动设置的默认防护策略。关闭后，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。

**步骤1** 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。

**步骤2** 选择“公网IP”页签，单击“设置默认防护策略”，如[图1-3](#)所示。

**图 1-3** 设置默认防护策略



**步骤3** 在弹出的设置默认防护策略窗口中，勾选“手动设置”，关闭手动设置的默认防护策略，如[图1-4](#)所示。

当“防护设置”勾选为“默认防护”时，“流量清洗阈值”默认为“120Mbps”，“CC防护”为“关闭”状态。

**图 1-4** 关闭手动设置的默认防护策略



**步骤4** 单击“确定”，关闭手动设置的默认防护策略。

关闭手动设置的默认防护策略后，新购买的公网IP按照“默认防护”开启DDoS攻击防护。

----**结束**

# 2 查看公网 IP

## 操作场景

该任务指导用户查看公网IP。

### 须知


- 购买了公网IP后，自动开启Anti-DDoS“默认防护”。开启Anti-DDoS防护后，即可对开启防护的IP地址提供DDoS攻击保护。
- 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。
- 登录帐号已购买公网IP。

## 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“安全与合规 > Anti-DDoS流量清洗”，进入Anti-DDoS服务管理界面。

图 2-1 Anti-DDoS 流量清洗





**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 2-2 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。
- 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。 <b>说明</b> 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： <ul style="list-style-type: none"> <li>● 正常</li> <li>● 设置中</li> <li>● 未开启</li> <li>● 清洗中</li> <li>● 黑洞中</li> </ul>

----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。
- 登录帐号已购买公网IP。

## 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“安全与合规 > Anti-DDoS流量清洗”，进入Anti-DDoS服务管理界面。

图 3-1 Anti-DDoS 流量清洗








**步骤4** 选择“告警通知”页签，设置告警通知，如[图3-2](#)所示，相关参数说明如[表3-1](#)所示。

图 3-2 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	<p>开启或关闭告警通知，说明如下：</p> <ul style="list-style-type: none"> <li>：开启状态。</li> <li>：关闭状态。</li> </ul> <p>如果告警通知为关闭状态，单击 ，将告警通知状态设置为 。</p>	
消息通知主题	<p>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。</p> <p>更多关于主题的信息，请参见《<a href="#">消息通知服务用户指南</a>》。</p>	-

**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

已获得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 4-2 防护设置



公网IP	防护状态	防护设置	操作
[Redacted]	正常	流量清洗阈值 300 Mbps CC防护 开启 HTTP请求速率 100 qps	查看日志报表 防护设置
[Redacted]	正常	流量清洗阈值 100 Mbps CC防护 关闭 HTTP请求速率 --	查看日志报表 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4-3所示，参数说明如表4-1所示。

图 4-3 防护设置



**防护设置**

公网IP [Redacted]

防护设置  默认防护  手动设置

流量清洗阈值 ② 300 Mbps

CC防护 ②  开启  关闭

HTTP请求速率 ② 100 qps

请根据网站正常访问量选择参数。参数过大会导致CC防护不能及时触发。

确定 取消

表 4-1 参数说明

参数	说明
防护设置	<ul style="list-style-type: none"> <li>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。</li> <li>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”。</li> </ul> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
流量清洗阈值	<p>Anti-DDoS检测到IP的入流量超过该阈值时，触发流量清洗。</p> <ul style="list-style-type: none"> <li>当“防护设置”为“默认防护”时，“流量清洗阈值”默认为“120Mbps”。</li> <li>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。</li> </ul> <p><b>说明</b></p> <p>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。</p> <p>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。</p>
CC防护	<ul style="list-style-type: none"> <li>关闭：关闭CC防护。</li> <li>开启：开启CC防护。</li> </ul> <p><b>说明</b></p> <p>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。</p>

参数	说明
HTTP请求速率	<p>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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"><li>• 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。</li><li>• 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。</li></ul>

**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

已获得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 5-1 Anti-DDoS 流量清洗



**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 5-2 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5-3和图5-4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 5-3 查看流量监控报表

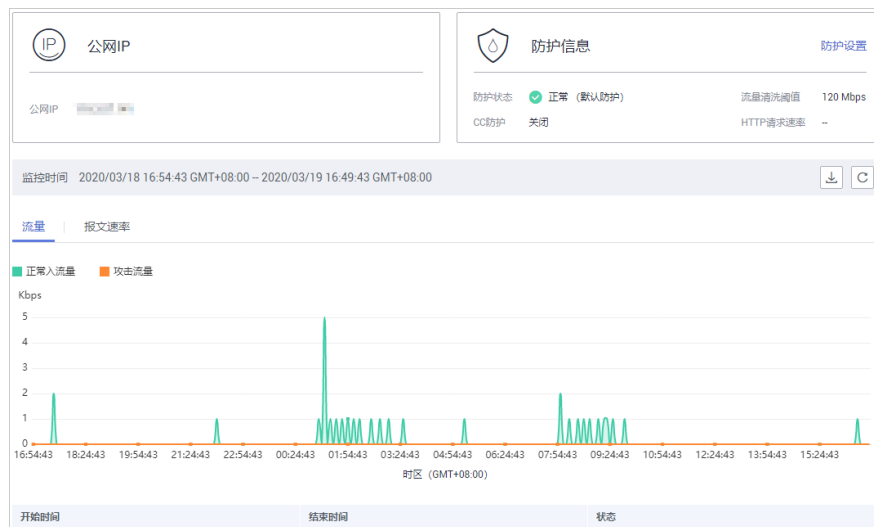
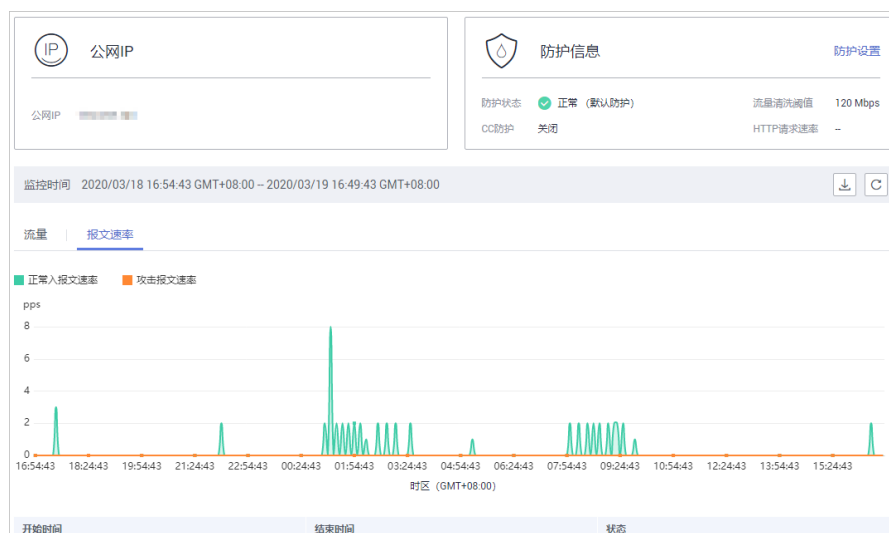







图 5-4 查看报文速率监控报表



### 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 6-1 Anti-DDoS 流量清洗



**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6-2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 6-2 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 权限管理

## 7.1 创建用户并授权使用 Anti-DDoS

如果您需要对您所拥有的Anti-DDoS进行精细的权限管理，您可以使用[统一身份认证服务](#)（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云帐号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用Anti-DDoS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将Anti-DDoS资源委托给更专业、高效的其他华为云帐号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

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，您可以跳过本章节，不影响您使用Anti-DDoS服务的其它功能。

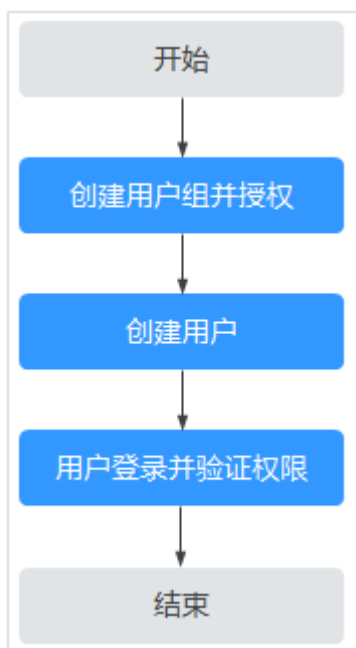
本章节为您介绍对用户授权的方法，操作流程如[图7-1](#)所示。

### 前提条件

给用户组授权之前，请您了解用户组可以添加的Anti-DDoS权限，并结合实际需求进行选择，Anti-DDoS支持的系统权限，请参见：[Anti-DDoS系统权限](#)。

## 示例流程

图 7-1 给用户授权服务权限流程



1. **创建用户组并授权。**  
在IAM控制台创建用户组，并授予Anti-DDoS服务的管理员权限“Anti-DDoS Administrator”。
2. **创建用户并加入用户组。**  
在IAM控制台创建用户，并将其加入1中创建的用户组。
3. **用户登录并验证权限。**  
新创建的用户登录控制台，切换至授权区域，验证权限：  
在“服务列表”中选择除Anti-DDoS服务外的任一服务，若提示权限不足，表示“Anti-DDoS Administrator”已生效。

# A 修订记录

发布日期	修改说明
2021-10-09	第九次正式发布。 <a href="#">配置Anti-DDoS防护策略</a> ，更新界面截图。
2021-08-06	第八次正式发布。 修改管理控制台入口描述。
2020-08-25	第七次正式发布。 新增 <a href="#">设置默认防护策略</a> 。
2020-04-08	第六次正式发布。 更新界面截图。
2020-01-07	第五次正式发布。 <a href="#">配置Anti-DDoS防护策略</a> ，补充参数说明。
2019-12-16	第四次发布。 国际站域名切换。
2019-11-21	第三次发布。 图片增加图标题及固定文档ID。
2018-01-19	第二次正式发布。 <a href="#">开启告警通知</a> ，告警通知界面优化。
2017-12-31	第一次正式发布。