



# 天翼云·Anti-DDoS 流量清洗

## 用户使用指南

天翼云科技有限公司

---

# 目 录

---

<b>1 产品简介</b> .....	<b>4</b>
1.1 产品定义.....	4
1.2 产品优势.....	4
1.3 功能特性.....	4
1.4 应用场景.....	5
1.5 术语解释.....	6
1.6 使用限制.....	7
1.7 该产品与其他服务的关系.....	8
<b>2 计费说明</b> .....	<b>9</b>
<b>3 用户指南</b> .....	<b>10</b>
3.1 开启 Anti-DDoS 防护.....	10
3.2 关闭 Anti-DDoS 防护.....	12
3.3 调整安全设置.....	13
3.4 查看监控报表.....	15
3.5 查看拦截报告.....	16
3.6 开启告警通知.....	17
3.7 关闭告警通知.....	19
<b>4 常见问题</b> .....	<b>21</b>
4.1 计费类.....	21
4.1.1 Anti-DDoS 如何计费? .....	21
4.2 概念类.....	21
4.2.1 什么是 SYN Flood 攻击和 ACK Flood 攻击? .....	21
4.2.2 什么是 CC 攻击? .....	21
4.2.3 什么是慢速连接攻击? .....	21
4.2.4 什么是 UDP 攻击和 TCP 攻击? .....	22
4.2.5 如何理解“百万级的 IP 黑名单库”? .....	22
4.3 功能类.....	22
4.3.1 Anti-DDoS 有何使用限制? .....	22
4.3.2 哪些服务可以使用 Anti-DDoS? .....	22

---

4.3.3 如何使用 Anti-DDoS? .....	22
4.3.4 Anti-DDoS 能阻止哪些类型的攻击? .....	22
4.3.5 攻击事件能否及时通知? .....	23
4.3.6 当业务经常被 DDoS 攻击时如何处理? .....	23
4.3.7 ELB 防护和 EIP 防护有什么区别? .....	23
4.3.8 为什么同一个公网 IP 地址的清洗次数和攻击次数不一致? .....	23
4.3.9 用户注销帐号是否需要清理 Anti-DDoS 服务的资源? .....	23

# 1 产品简介

## 1.1 产品定义

Anti-DDoS 流量清洗服务（以下简称 Anti-DDoS）为弹性公网 IP 提供网络层和应用层的 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 通过对互联网访问弹性公网 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 产品优势

### 极速

秒级的攻击响应延迟（<3 秒），清洗时网络延迟 30ms 以内。

### 专业

专业优质防护线路，专业防 DDoS 设备，TCP/UDP 清洗零误杀；百万级 IP 黑名单库，精准有效；覆盖所有防护类型，防护类型包括 SYN flood、UDP flood 等所有 DDoS 攻击方式。

### 无成本

天翼云以免费方式向用户提供防 DDoS 服务，用户可以在管理控制台开启并配置云主机的防 DDoS 能力。

### 可视化管理

以图形方式提供 DDoS 防护日志，方便用户掌握 DDoS 攻击趋势以及云主机被攻击的情况。

## 1.3 功能特性

提供四到七层的 DDoS 攻击防护能力

Anti-DDoS 流量清洗服务提供四到七层的 DDoS 攻击防护，包括 SYN flood、UDP flood 等所有 DDoS 攻击方式。

#### **支持通过 Web 页面设置参数**

提供针对公网 IP 配置和修改 Anti-DDOS 相关参数的能力，参数包括每秒请求量、单一源 IP 连接数。

#### **提供 DDoS 防护监控**

提供查看单个公网 IP 的监控能力，包括当前防护状态、当前防护配置参数、24 小时前到现在的流量情况、24 小时的异常事件（清洗和黑洞）。

#### **提供安全能力报告**

提供查看安全报告能力，查看区间为一周，支持查询前四周统计数据，包括防护流量、攻击次数、攻击 top10 排名。

## 1.4 应用场景

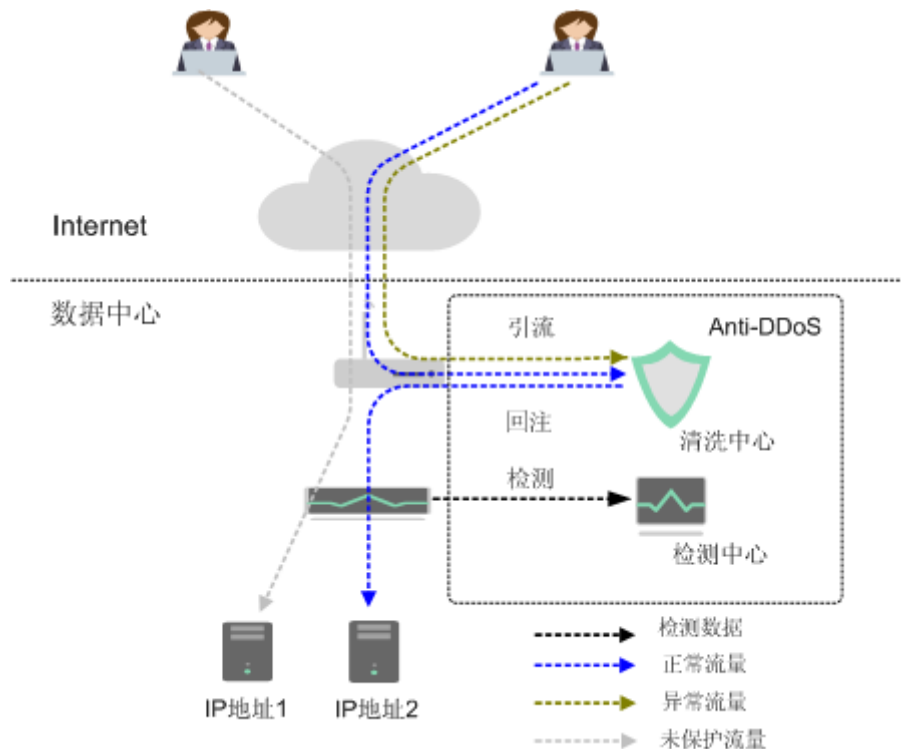
Anti-DDoS 对公网 IP 提供不超过 5Gbps 流量的 DDoS 攻击防护。

对大于 5Gbps 的流量，系统会进行自动限流措施（正常访问流量会丢失）；对于正常业务流量超过 5Gbps 流量的应用，建议用户自主购买第三方清洗中心服务，从第三方获取报表。

Anti-DDoS 设备部署在机房出口处，网络拓扑架构如图 1-1 所示。

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。

图1-1 网络拓扑结构



## 1.5 术语解释

### CC 攻击

CC 攻击是针对 Web 服务器或应用程序的攻击，利用获取信息的标准的 GET/POST 请求，如请求涉及数据库操作的 URI（Universal Resource Identifier）或其他消耗系统资源的 URI，造成服务器资源耗尽，无法响应正常请求。

### 带宽

通过带宽展示网络的使用情况，作为服务计费的依据。

### 分布式拒绝服务攻击

拒绝服务攻击（Denial of Service Attack，缩写：DoS）亦称洪水攻击，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。

### 黑洞状态

黑洞状态是指服务器的外网访问被屏蔽，从服务器内部看到访问流量为零的状态。

## 流量清洗

流量清洗是用于准确识别网络中的异常流量并将其丢弃，保证正常流量通行的网络安全服务。流量清洗的主要对象是 DDoS 攻击。

## SYN Flood 攻击

SYN Flood 攻击是指通过伪造的 SYN 报文（其源地址是伪造地址或不存在的地址），向目标服务器发起连接，目标服务器用 SYN-ACK 应答，而此应答不会收到 ACK 报文，导致目标服务器保持了大量的半连接，直到超时。这些半连接可以耗尽服务器资源，使目标服务器无法建立正常 TCP 连接，从而达到攻击的目的。

## 实例

实例是 Kubernetes 部署应用或服务的最小的基本单位。

## 弹性公网 IP

弹性公网 IP 可以绑定到用户帐户下的任何弹性云服务器上，而不需要是特定的弹性云服务器。与传统静态 IP 地址不同，当弹性云服务器或者区 Region 不可用时，弹性公网 IP 地址可以快速重定向到用户帐户下的任何弹性云服务器的公网 IP 地址上。

## 弹性云主机

弹性云主机（Elastic Cloud Server, ECS）是由 CPU、内存、操作系统、云硬盘组成的基础的计算组件。弹性云主机创建成功后，您就可以像使用自己的本地 PC 或物理服务器一样，在云上使用弹性云主机。

## UDP Flood 攻击

UDP Flood 攻击是指攻击者通过僵尸网络向目标服务器发送大量的 UDP 报文，这种 UDP 报文通常为大包，且速率非常快，从而造成服务器资源耗尽，无法响应正常的请求。

## 云主机

参见[弹性云主机](#)。云主机是具有完整硬件、操作系统、网络功能，并且运行在一个完全隔离环境中的计算机系统。云主机具有弹性、按需获取的特点。

## 1.6 使用限制

Anti-DDoS 提供不超过 5Gbps 流量的 DDoS 攻击防护。对大于 5Gbps 的流量，系统会自动限流措施（正常访问流量会丢失）；对于正常业务流量超过 5Gbps 流量的应用，建议用户自主购买第三方清洗中心服务，从第三方获取报表。

## 1.7 该产品与其他服务的关系

### 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》。



# 2 计费说明

---

Anti-DDoS 流量清洗为免费服务。但与 Anti-DDoS 流量清洗关联的天翼云产品，按正常相关云产品对应的价格收费。

# 3 用户指南

## 3.1 开启 Anti-DDoS 防护


开启 Anti-DDoS 防护后，即可对开启防护的实例 IP 地址提供 DDoS 攻击保护。

### 前提条件

- 已获取管理控制台的登录帐号与密码。
- 实例未开启 Anti-DDoS 防护。

### 操作步骤

步骤 1 登录管理控制台。

步骤 2 单击管理控制台上方的 ，选择区域或项目。

步骤 3 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“实例列表”页签，在需要开启防护的实例 IP 所在行的“操作”列，单击“开启防护”，如图 3-1 所示。

图3-1 开启防护

实例IP ▲	实例类型 ▼	DDoS防护状态 ▼	操作
弹性IP地址 7	弹性IP地址	未开启	开启防护
弹性IP地址 2	弹性IP地址	未开启	开启防护
弹性IP地址 9	弹性IP地址	未开启	开启防护

步骤 5 根据实际配置防护参数，参数说明如表 3-1 所示。

图3-2 配置防护参数

开启防护
✕

最大业务流量:  ▼ ?

请按照实际业务流量选择参数，建议不超过购买带宽。

CC防护:  关闭

开启 HTTP请求速率:  ▼ ?

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。

表3-1 防护参数说明

参数名称	说明
最大业务流量	<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>当实际业务流量触发流量清洗时，Anti-DDoS 仅拦截攻击流量；当实际业务流量未触发流量清洗时，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>说明</p> <p>只有支持完整 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> <ul style="list-style-type: none"> <li>• HTTP 请求速率：开启 CC 防护时该参数才能生效。建议选择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此阈值后，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。                         <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> </li> </ul>

步骤 6 单击“确定”，保存配置，开启防护。

----结束

## 3.2 关闭 Anti-DDoS 防护


开启 Anti-DDoS 防护后，即可对开启防护的实例 IP 地址提供 DDoS 攻击保护。如果不需要使用 Anti-DDoS 防护功能，可以关闭 Anti-DDoS。

### 前提条件

- 已获取管理控制台的登录帐号与密码。
- 实例已开启 Anti-DDoS 防护。

### 操作步骤

步骤 1 登录管理控制台。

步骤 2 单击管理控制台上方的 ，选择区域或项目。

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

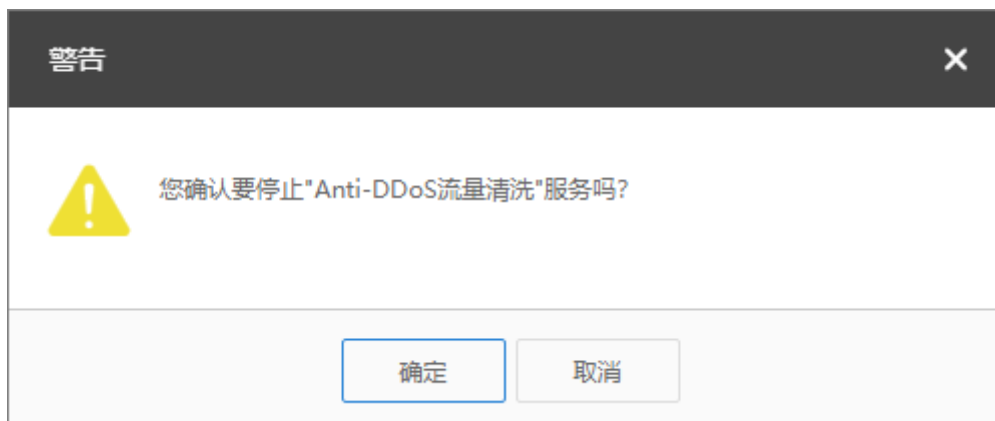
步骤 4 选择“实例列表”页签，在需要关闭防护的实例 IP 所在行的“操作”列，单击“停止防护”，如图 3-3 所示。

图3-3 停止防护

实例IP ▲	实例类型 ▼	DDoS防护状态 ▼	操作
10.10.10.17	弹性IP地址	正常	<a href="#">查看监控报表</a> <a href="#">安全设置</a> <a href="#">停止防护</a>
10.10.10.2	弹性IP地址	未开启	<a href="#">开启防护</a>
10.10.10.9	弹性IP地址	未开启	<a href="#">开启防护</a>

步骤 5 在弹出的窗口中，单击“确定”，关闭防护，如图 3-4 所示。

图3-4 确认信息



----结束

### 3.3 调整安全设置

用户为实例开启 Anti-DDoS 防护后，可以再次调整安全策略。

#### 前提条件

- 已获取管理控制台的登录帐号与密码。
- 实例已开启 Anti-DDoS 防护。

#### 操作步骤

步骤 1 登录管理控制台。

步骤 2 单击管理控制台上方的 ，选择区域或项目。

步骤 3 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“实例列表”页签，在需要调整安全设置的实例 IP 所在行的“操作”列，单击“停止防护”，如图 3-5 所示。

图3-5 调整安装设置

实例IP	实例类型	DDoS防护状态	操作
弹性IP地址 7	弹性IP地址	正常	<a href="#">查看监控报表</a> <a href="#">安全设置</a> <a href="#">停止防护</a>
弹性IP地址 2	弹性IP地址	未开启	<a href="#">开启防护</a>
弹性IP地址 9	弹性IP地址	未开启	<a href="#">开启防护</a>

步骤 5 根据实际修改防护参数，参数说明如表 3-2 所示。

图3-6 修改防护参数

安全设置
✕

最大业务流量:  ?

请按照实际业务流量选择参数，建议不超过购买带宽。

CC防护:  关闭

开启 HTTP请求速率:  ?

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。

表3-2 防护参数说明

参数名称	说明
最大业务流量	<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>当实际业务流量触发流量清洗时，Anti-DDoS 仅拦截攻击流量；当实际业务流量未触发流量清洗时，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>说明</p> <p>只有支持完整 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> <ul style="list-style-type: none"> <li>• HTTP 请求速率：开启 CC 防护时该参数才能生效。建议选择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此阈值后，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。                         <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> </li> </ul>

步骤 6 单击“确定”，完成修改，配置生效。

----结束

## 3.4 查看监控报表


用户为实例开启 Anti-DDoS 防护后，可以查看实例的监控详情，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。
- 实例已开启 Anti-DDoS 防护。

### 操作步骤

步骤 1 登录管理控制台。

步骤 2 单击管理控制台上方的 ，选择区域或项目。

步骤 3 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“实例列表”页签，在需要查看的实例 IP 所在行的“操作”列，单击“查看监控报表”，如图 3-7 所示。

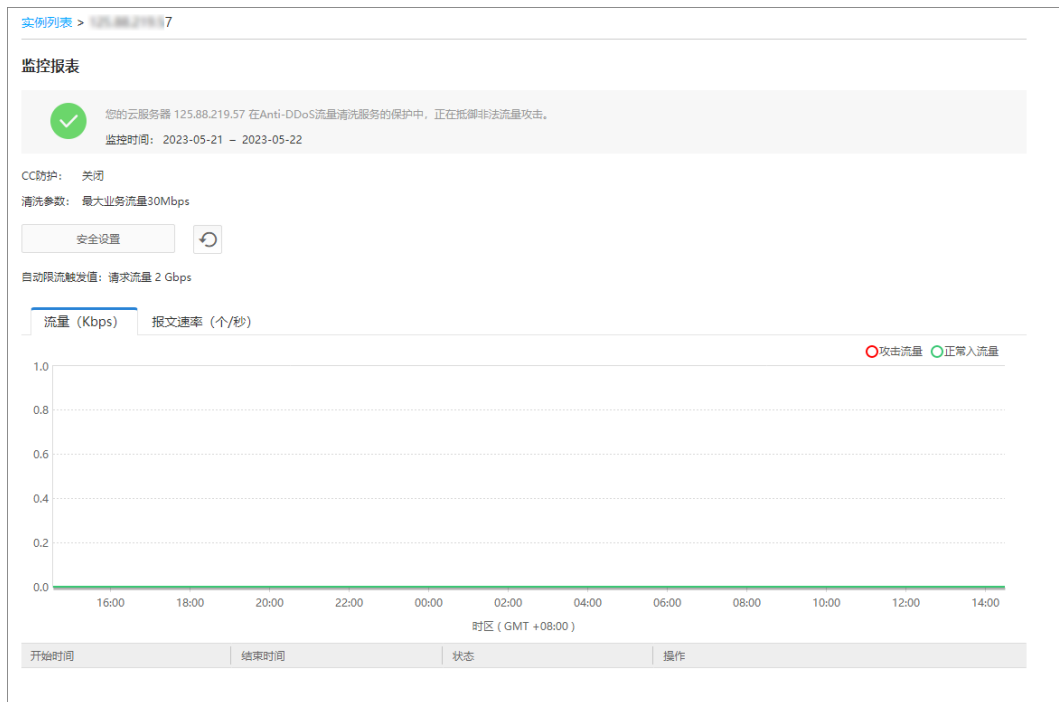
图3-7 查看监控报表

实例IP	实例类型	DDoS防护状态	操作
弹性IP地址	弹性IP地址	正常	<a href="#">查看监控报表</a> <a href="#">安全设置</a> <a href="#">停止防护</a>
弹性IP地址	弹性IP地址	未开启	<a href="#">开启防护</a>
弹性IP地址	弹性IP地址	未开启	<a href="#">开启防护</a>

步骤 5 在“监控报表”界面，可以查看实例 IP 报表的详细指标，如图 3-8 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，以五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3-8 监控报表



---结束

## 3.5 查看拦截报告

用户开启 Anti-DDoS 防护后, 系统将以一周为一个时间段生成拦截报告。用户可以通过拦截报告获取所有实例 IP 的防护统计信息, 包括清洗次数、清洗流量, 以及实例 IP 被攻击次数 Top10 排名和当周的拦截攻击次数。

### 前提条件

已获取管理控制台的登录帐号与密码。

### 操作步骤


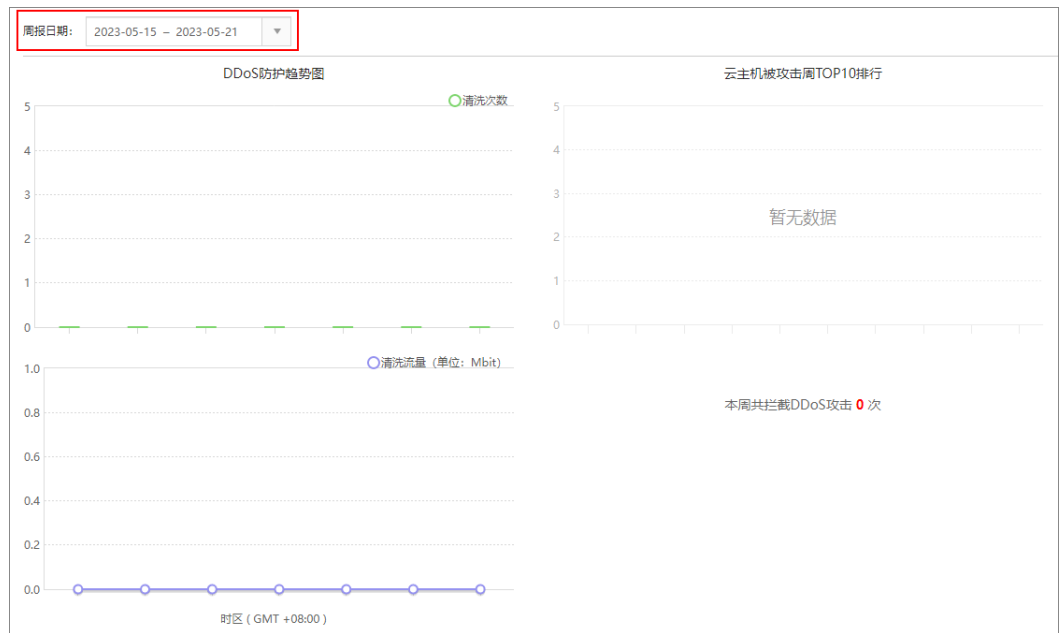
- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台上方的 , 选择区域或项目。
- 步骤 3 选择“安全 > Anti-DDoS 流量清洗”, 进入 Anti-DDoS 服务管理界面。
- 步骤 4 选择“拦截报告”页签, 选择需要查看的“周报日期”, 即可查看当周的拦截报告。



图3-9 拦截报告



----结束

## 3.6 开启告警通知

为 Anti-DDoS 开启告警通知以后，当实例受到 DDoS 攻击时，您会收到提醒消息（短信或 Email）。否则，无论 DDoS 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。

### 前提条件

已获取管理控制台的登录帐号与密码。

### 操作步骤


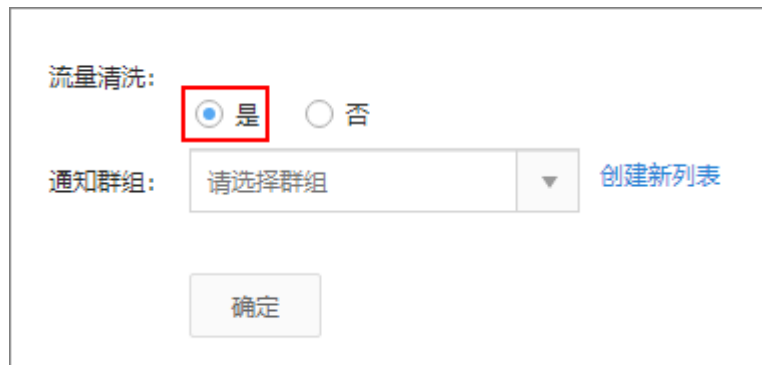
- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台上方的 ，选择区域或项目。
- 步骤 3 选择“安全 > Anti-DDoS 流量清洗”，进入 Anti-DDoS 服务管理界面。
- 步骤 4 选择“告警通知设置”页签，进入告警通知配置页面。
- 步骤 5 在“流量清洗”参数后，勾选“是”，开启告警通知。

图3-10 开启告警通知



流量清洗： 是  否

通知群组：请选择群组 创建新列表

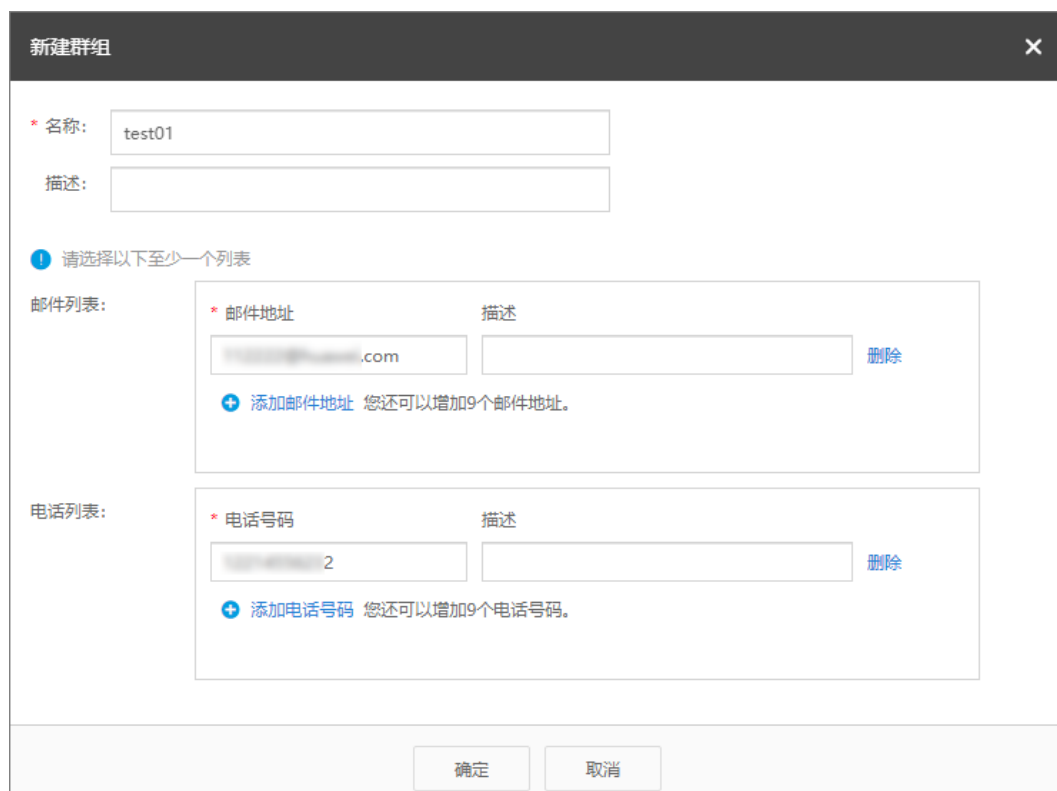
确定

步骤 6（可选）在“通知群组”参数后，单击“创建新列表”，根据实际配置需要接收告警通知的“邮件地址”和“电话号码”后，单击“确定”，如图 3-11 所示。

### 说明

若已有通知群组，可跳过此步骤。

图3-11 创建通知群组



新建群组 ×

\* 名称: test01

描述:

① 请选择以下至少一个列表

邮件列表:

* 邮件地址	描述	
xxxxxx@xxxx.com		删除

+ 添加邮件地址 您还可以增加9个邮件地址。

电话列表:

* 电话号码	描述	
xxxxxx 2		删除

+ 添加电话号码 您还可以增加9个电话号码。

确定 取消

步骤 7 选择需要接收告警通知的群组，单击“确定”，如图 3-12 所示。

图3-12 选择群组

流量清洗：  
 是  否

通知群组：  
topic-test 创建新列表

确定

----结束

## 3.7 关闭告警通知

关闭告警通知后，无论 DDoS 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。

### 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 单击管理控制台上方的 ，选择区域或项目。
- 步骤 3 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“告警通知设置”页签，进入告警通知配置页面。
- 步骤 5 在“流量清洗”参数后，勾选“否”，单击“确定”，关闭告警通知。

图3-13 关闭告警通知

流量清洗：  
 是  否

通知群组：  
topic-test 创建新列表

确定

----结束

# 4 常见问题

## 4.1 计费类

### 4.1.1 Anti-DDoS 如何计费？

Anti-DDoS 流量清洗为免费服务。但与 Anti-DDoS 流量清洗关联的天翼云产品，按正常相关云产品对应的价格收费。

## 4.2 概念类

### 4.2.1 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。

### 4.2.2 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。

### 4.2.3 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。

#### 4.2.4 什么是 UDP 攻击和 TCP 攻击？

UDP 攻击和 TCP 攻击的基本原理说明如下：

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。

#### 4.2.5 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。

### 4.3 功能类

#### 4.3.1 Anti-DDoS 有何使用限制？

提供不超过 5Gbps 流量的 DDoS 攻击防护。

对大于 5Gbps 的流量，系统会自动限流措施（正常访问流量会丢失）；对于正常业务流量超过 5Gbps 流量的应用，建议用户自主购买第三方清洗中心服务，从第三方获取报表。

#### 4.3.2 哪些服务可以使用 Anti-DDoS？

Anti-DDoS 流量清洗服务的防护对象为用户购买的公网 IP，不区分服务。

#### 4.3.3 如何使用 Anti-DDoS？

购买了弹性公网 IP 后，即可自动开启 Anti-DDoS 防护。如果您有未开启 Anti-DDoS 防护的弹性公网 IP，请参考 3.1 开启 Anti-DDoS 防护开启防护。

#### 4.3.4 Anti-DDoS 能阻止哪些类型的攻击？

Anti-DDoS 可以轻松应对流量拥塞型攻击，精确识别连接耗尽型、慢速攻击，帮助用户防护以下攻击：

- 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。

### 4.3.5 攻击事件能否及时通知？

可以。在 Anti-DDoS 界面，单击“告警通知”页签，开启告警通知。

告警通知开启后，在受到 DDoS 攻击时，用户会收到报警信息（短信或 Email）。

### 4.3.6 当业务经常被 DDoS 攻击时如何处理？

当业务经常被 DDoS 攻击时，除了使用 Anti-DDoS 对 DDoS 攻击进行防护外，用户还可以参照以下处理方法进一步提高网络的安全性：

- 及时安装系统补丁。
- 建立并完善备份机制，定期备份系统的重要信息（例如，系统配置信息）。设置复杂度高的特权帐号密码（例如，管理员帐号密码），降低攻击的可能性。
- 定期检查系统的物理环境，禁止不必要的网络服务。
- 建立并完善网络边界安全防护策略，防护来自网络外部的威胁。
- 定期检查系统配置信息，查看每天的安全日志，及时排查安全隐患。
- 使用网络安全设备（例如，防火墙）加固网络安全，配置网络安全设备的安全规则，过滤网络中所有可能的伪造数据包。
- 联系网络服务提供商实现路由的访问控制和对带宽总量的限制。

### 4.3.7 ELB 防护和 EIP 防护有什么区别？

EIP 指绑定到弹性云服务器的弹性 IP 地址，ELB 指绑定弹性负载均衡的弹性 IP 地址。对于 Anti-DDoS 来说，ELB 防护和 EIP 防护都是对 IP 地址进行 DDoS 攻击防护，两者没有区别。

### 4.3.8 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。

### 4.3.9 用户注销帐号是否需要清理 Anti-DDoS 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，注销帐号时不需要清理资源。
- 本服务在购买 EIP 时自动开启防护，不产生任何费用，用户可放心使用。