天翼云 3.0 •Anti-DDoS 流量清洗

用户使用指南

中国电信股份有限公司云计算分公司

目 录

1 产品概述

1.1 产品定义

Anti-DDoS 流量清洗（CT-AntiDDoS ，Anti-DDoS ）通过专业的 DDoS 防护设备来为用户互联网应用提供精细化的抵御 DDOS 攻击能力，如 UDP Flood 攻击、SYN Flood 攻击和 CC 攻击等。用户可业务模型配置流量参数阀值，可监控攻防状态，并查看每日或每周报告。

1.2 功能介绍

Anti-DDoS 流量清洗为用户提供了自助配置和监控流量清洗服务的能力，配套提供一个高度管控、灵活使用的管理平台，达到配置简单、服务资源监控方便的目标。通过主备部署模式，提供高可靠性。

天翼云 Anti-DDoS 流量清洗具有以下功能：

提供针对公网 IP 配置和修改 Anti-DDoS 相关参数的能力。

提供针对弹性云主机和负载均衡型设备的公网 IP 的防护能力。

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）。

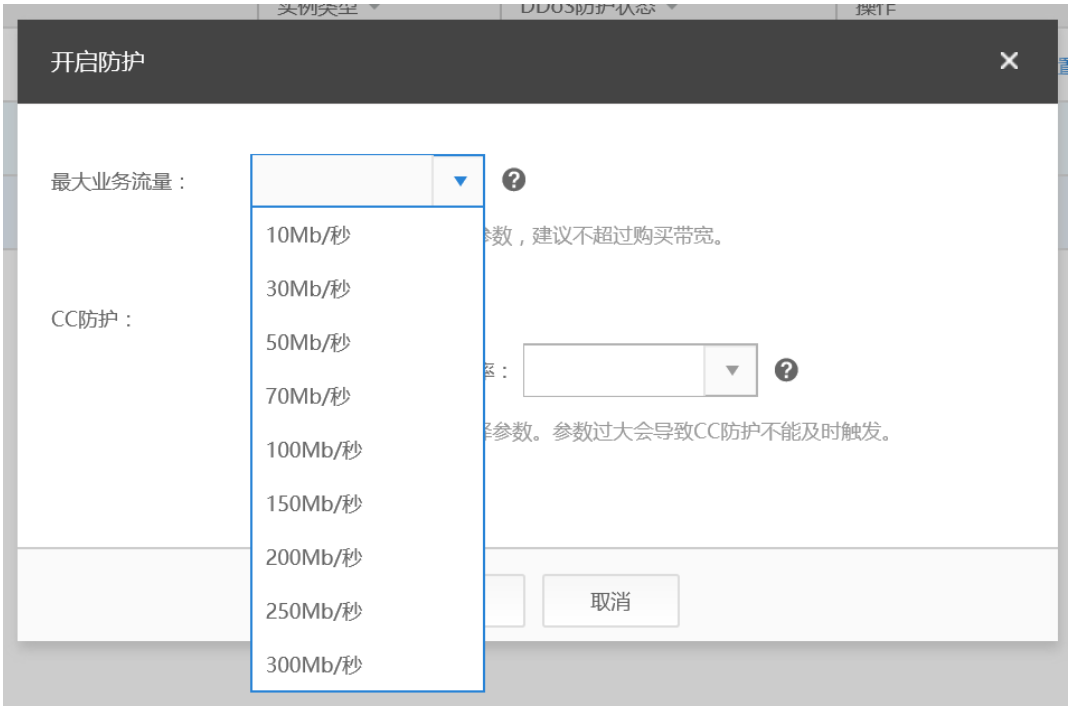
提供查看安全报告能力，查看区间为一周，支持查询前四周统计数据，包括防护流量、攻击次数、攻击 Top10 排名。

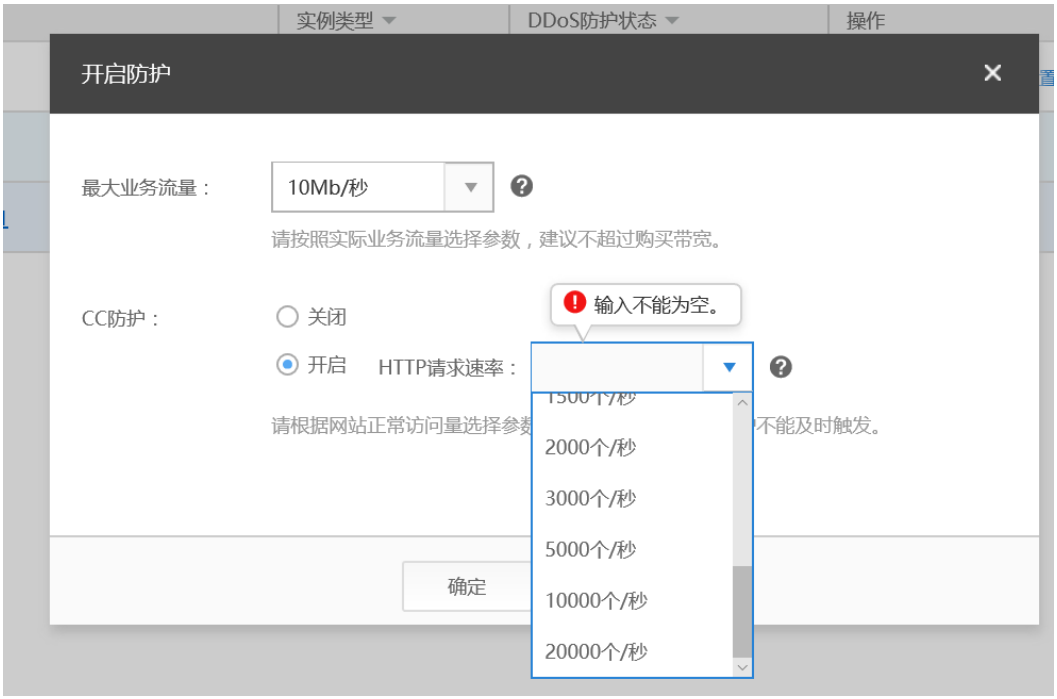
提供接收并分析 Anti-DDoS 设备上报日志的能力，将结果输出在界面上呈现给用户。

2 快速入门

2.1 开启防护

- 注册并登录天翼云管理控制台。
- 单击【安全】【Anti-DDoS 流量清洗】。
- 在【Anti-DDoS】【实例列表】界面待开启防护的实例所在行，单击【开启防护】。
- 在【开启防护】界面，根据界面提示配置参数





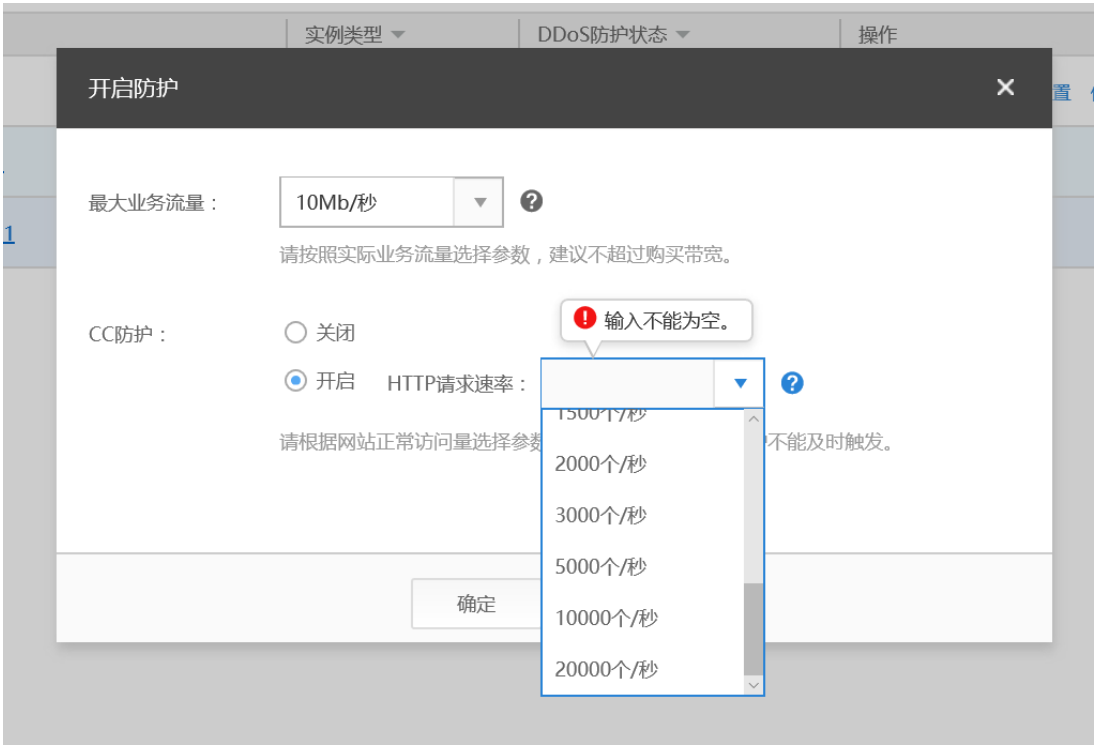
- 每秒请求数：Anti-DDoS 设备检测到总的入流量超过此阀值后，便会开启流量清洗。
- 建议和弹性 IP 的带宽保持一致，如果网站在做推广或者活动时适当调大。
- 每秒 HTTP 请求数：Anti-DDoS 设备检测到总的请求数量超过此阀值后，便会开启流量清洗
- 单一源 IP 连接数：Anti-DDoS 设备会监控发送到用户 IP 地址的连接数，当超过该连接数时、会对发起连接数过多的源 IP 地址进行限制。
- 单击“确定”。

3 配置管理

3.1 配置管理

开启防护

- 登录天翼云管理控制台。
- 单击【安全】【Anti-DDoS 流量清洗】。
- 在【Anti-DDoS】【实例列表】界面待开启防护的实例所在行，单击【开启防护】。
- 在【开启防护】界面，根据界面提示配置参数，在此可以开启 CC 防护，设置每秒 HTTP 请求数清洗阀值。

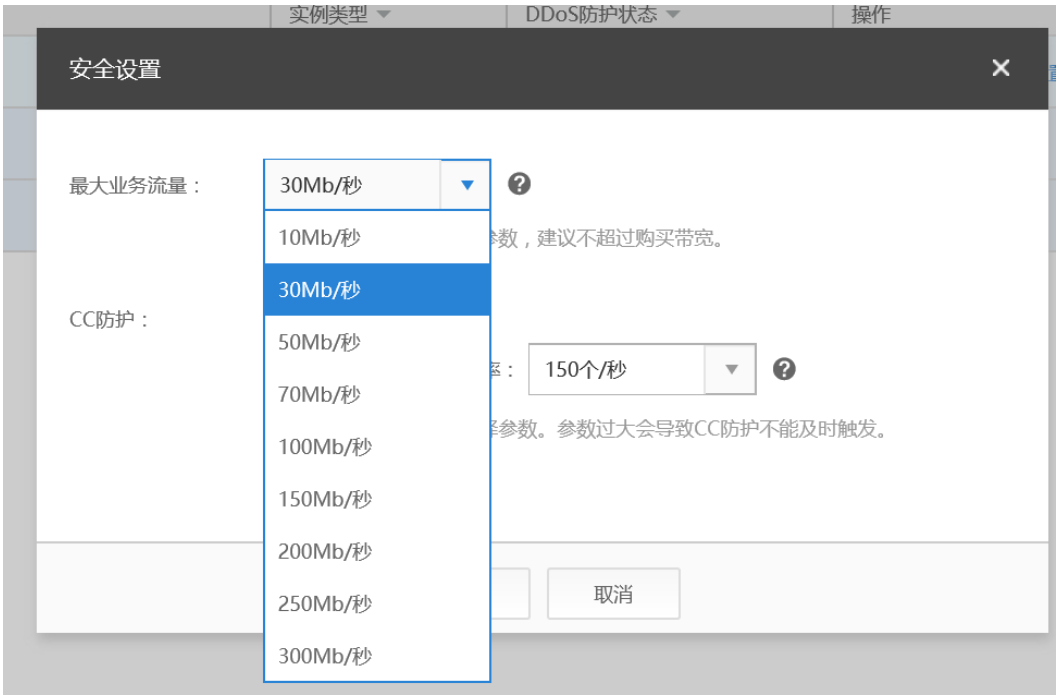


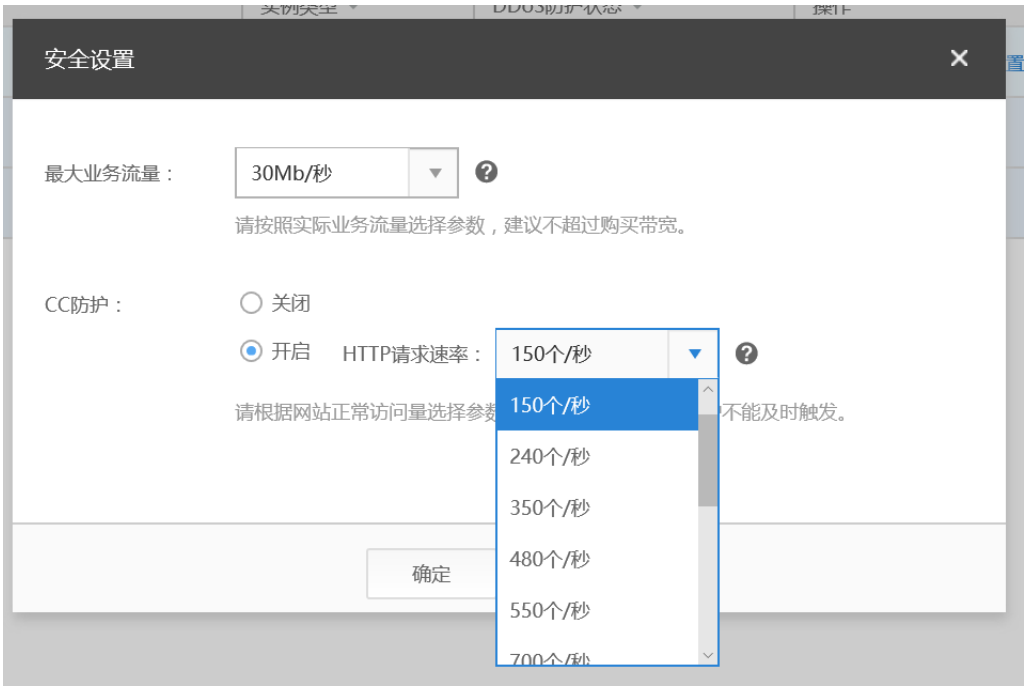
- 每秒请求数：Anti-DDoS 设备检测到总的入流量超过此阀值后，便会开启流量清洗。
- 建议和弹性 IP 的带宽保持一致，如果网站在做推广或者活动时适当调大。
- 每秒 HTTP 请求数：Anti-DDoS 设备检测到总的请求数量超过此阀值后，便会开启流量清洗。
- 单一源 IP 连接数：Anti-DDoS 设备会监控发送到用户 IP 地址的连接数，当超过该连接数时、会对发起连接数过多的源 IP 地址进行限制。

- 单击【确定】。

安全设置

- 在【Anti-DDoS】【实例列表】界面实例所在行，单击【安全设置】。
- 在【安全设置】界面，根据界面提示配置参数





- 单击【确定】。

停止防护

在【Anti-DDoS】【实例列表】界面待停止防护的实例所在行，单击【停止防护】。

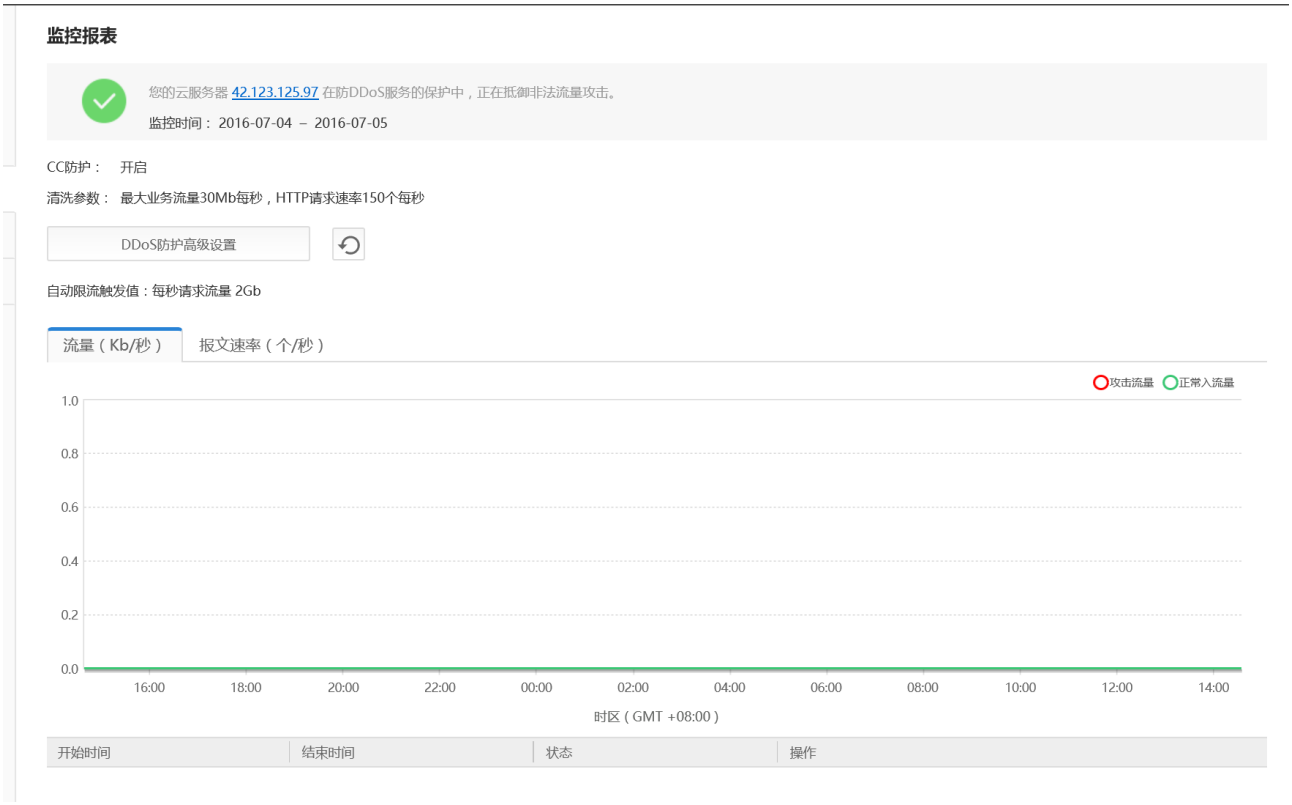
3.2 监控管理

针对云主机，可以查看具体的 Anti-DDoS 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。

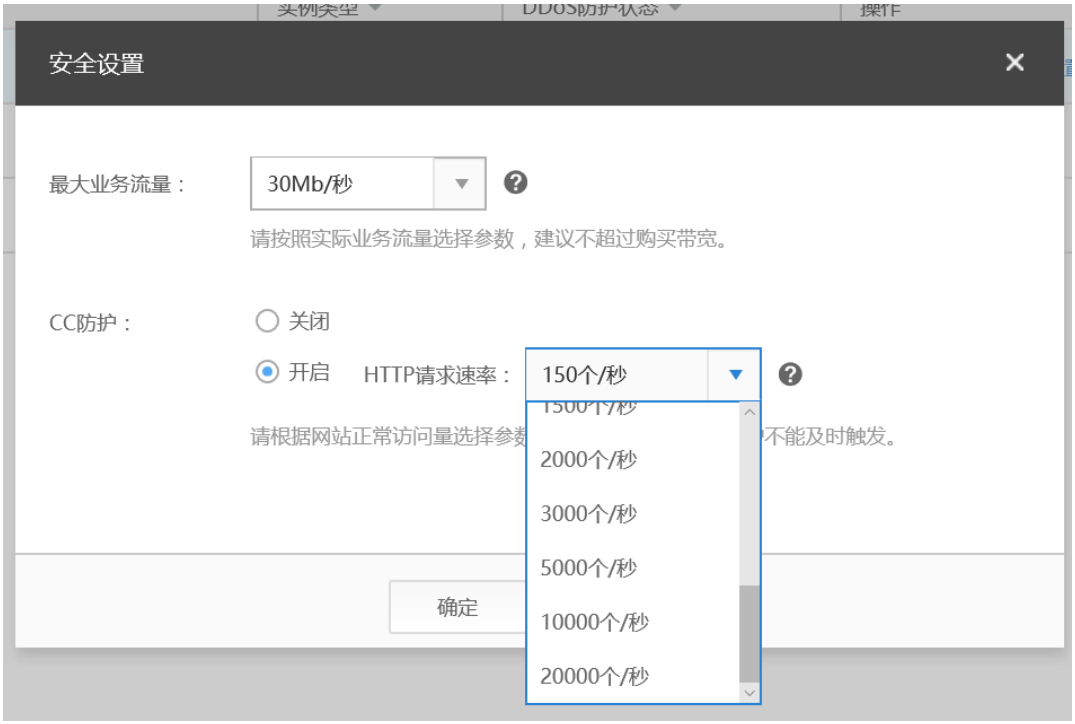
查看监控报表

- 注册并登录天翼云管理控制台。
- 单击【安全】【Anti-DDoS 流量清洗】。
- 在【Anti-DDoS】【实例列表】界面实例所在行，单击实例 IP 地址或【查看监控报表】。

- 在【监控报表】界面，可以查看该实例报表的详细指标

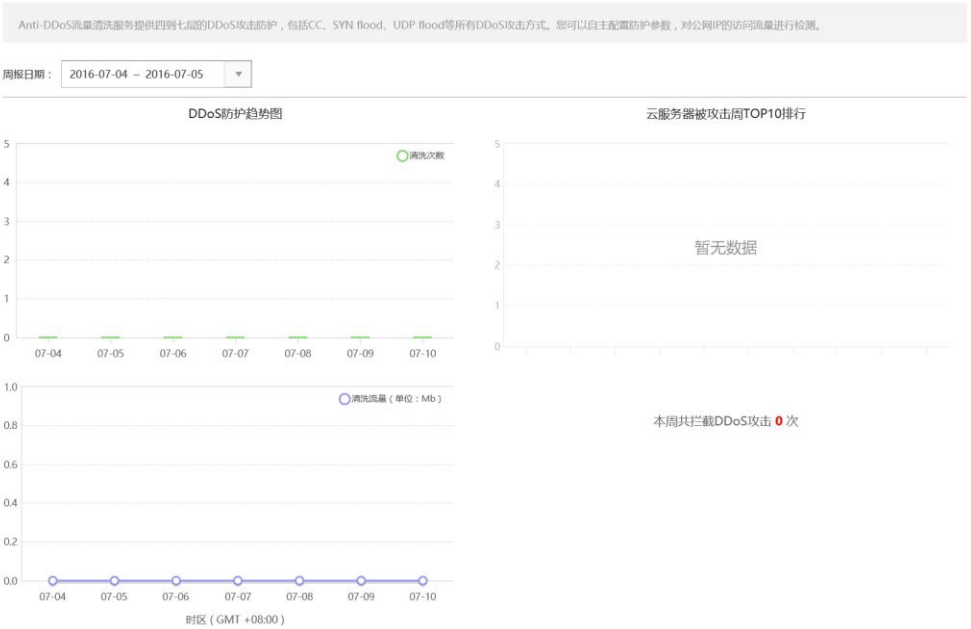


- 当前的 DDoS 现状：展示当前所选云服务器的 DDoS 攻击现状，在防护中/未开启防护。
- CC 防护：当前 CC 防护状态。
- 清洗触发值：开启防护或者安全配置时设置的各项清洗阈值。
- 黑洞触发值：当前系统默认的黑洞触发值，5Gbit/s。
- 24 小时防护流量数据图：以五分钟一个数据点描绘的流量图，主要包括以下方面：
  - ✓ 流量图：展示所选云服务器的流量情况，主要包括服务器的正常出入流量以及总入流量，当基于流量的 DDoS 攻击发生时，总入流量将大于正常入流量。
  - ✓ 报文速率图：展示所选云服务器的报文速率 PPS 情况，主要包括正常出 / 入报文速率以及总入报文速率，当基于 PPS 的 DDoS 攻击发生时，总入 PPS 将大于正常入 PPS。
- 近 1 天内攻击事件记录表：近 1 天内云主机的 DDoS 事件记录，包括清洗事件和黑洞事件。
  - ✓ 当需要设置安全配置时，可单击“DDoS 防护高级设置”。



查看安全报告

- 登录天翼云管理控制台。
- 单击【安全】【Anti-DDoS 流量清洗】。
- 在【Anti-DDoS】【拦截报告】界面，可以查看该实例报表的详细指标
- 可通过选择周报日期来查看固定日期内的安全报告，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。


Anti-DDoS流量清洗服务提供四到七层的DDoS攻击防护，包括CC、SYN flood、UDP flood等所有DDoS攻击方式。您可以自主配置防护参数，对公网IP的访问流量进行检测。
周报日期：
2016-07-04 – 2016-07-05
DDoS防护趋势图
清洗次数
5
4
3
2
1
0
07-04
07-05
07-06
07-07
07-08
07-09
07-10
清洗流量（单位：Mb）
1.0
0.8
0.6
0.4
0.2
0.0
时区（GMT +08:00）
云服务器被攻击周TOP10排行
暂无数据
本周共拦截DDoS攻击 0 次

4 常见问题

4.1 什么是 Anti-DDoS 流量清洗？

Anti-DDoS 流量清洗（以下简称 Anti-DDoS）引导用户针对 5G 以下的流量自主配置防护参数，通过调用天翼云 Anti-DDoS 管理中心的能力在网络出口对访问流量进行检测和清洗，通过调用天翼云 Anti-DDoS 管理中心提供的 API 下发策略到检测中心；按用户生成报表，并呈现给用户。

对大于 5G 的流量，设置为黑洞状态或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。

4.2 Anti-DDoS 服务是付费的吗？

Anti-DDoS 服务作为安全服务的基础服务，目前属于免费服务。

4.3 Anti-DDoS 的服务方式是什么？

表1-1 服务方式

服务名称	面向的产品	检测方式	是否默认开通
Anti-DDoS 服务	• 弹性云主机 • 弹性负载均衡	实时	否

Anti-DDoS 实时地对您在天翼云服务中购买并且使用中的弹性 IP 地址进行流量的检测和清洗，从而保护了和弹性 IP 地址绑定的弹性云主机或者负载均衡器不受攻击。

4.4 如何开启 Anti-DDoS 防护？

1. 登录天翼云管理控制台。
2. 单击“安全 > Anti-DDoS 流量清洗”。
3. 在“Anti-DDoS > 实例列表”界面待开启防护的实例所在行，单击“开启防护”。

4. 在“开启防护”界面，根据界面提示配置参数，在此可以开启 CC 防护，设置每秒 HTTP 请求数清洗阀值，0 所示。

图 4-1 开启防护

- 每秒请求数：Anti-DDoS 设备检测到总的入流量超过此阀值后，便会开启流量清洗。
- 建议和弹性 IP 的带宽保持一致，如果网站在做推广或者活动时适当调大。
- 每秒 HTTP 请求数：Anti-DDoS 设备检测到总的请求数量超过此阀值后，便会开启流量清洗。
- 单一源 IP 连接数：Anti-DDoS 设备会监控发送到用户 IP 地址的连接数，当超过该连接数时、会对发起连接数过多的源 IP 地址进行限制。

5. 单击“确定”。

4.5 如何进行阈值调整？

1. 注册并登录天翼云管理控制台。
2. 单击“安全 > Anti-DDoS 流量清洗”。
3. 在“Anti-DDoS > 实例列表”界面实例所在行，单击“安全设置”。
4. 在“安全设置”界面，根据界面提示配置参数，如 0 所示。

安全设置

- 每秒请求数：Anti-DDoS 设备检测到总的入流量超过此阀值后，便会开启流量清洗。
- 建议和弹性 IP 的带宽保持一致，如果网站在做推广或者活动时适当调大。
- 每秒 HTTP 请求数：Anti-DDoS 设备检测到总的请求数量超过此阀值后，便会开启流量清洗。
- 单一源 IP 连接数：Anti-DDoS 设备会监控发送到用户 IP 地址的连接数，当超过该连接数时、会对发起连接数过多的源 IP 地址进行限制。

5. 单击“确定”。