Anti-DDoS 流量清洗

用户使用指南

天翼云科技有限公司

目 录

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；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

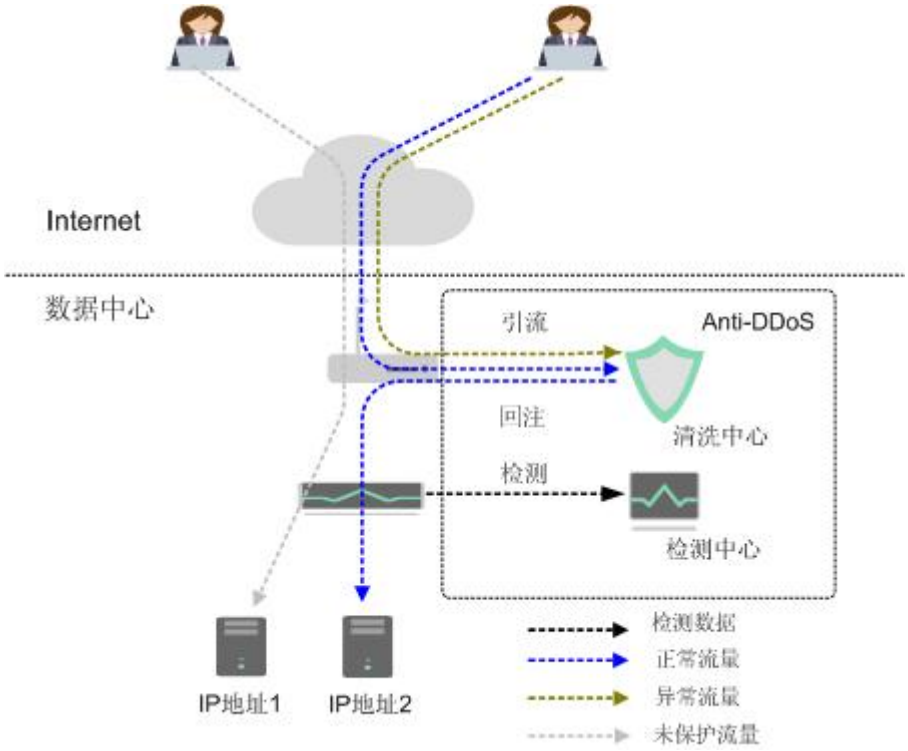
Anti-DDoS 对公网 IP 提供不超过 5Gbps 流量的 DDoS 攻击防护。

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，简称 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（Distributed Denial of Service Attack，简称 DDoS）。

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。

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。

1.7 该产品与其他服务的关系

Anti-DDoS 可以为弹性云主机、弹性负载均衡、Web 应用防火墙、弹性 IP 等服务的公网 IP 资源提供防护能力。此外，与其他云服务之间还存在以下关系。

表 1-1 与其他云服务的关系

服务名称	与其他服务的关系	主要交互功能
云审计服务	开通云审计服务后，云审计服务会记录Anti-DDoS 相关的操作事件，方便用户日后的查询、审计和回溯。	查看云审计日志
消息通知服务	消息通知服务提供消息通知功能。Anti-DDoS 开启告警通知后，如果 IP 地址受到 DDoS 攻击时用户会收到短信或邮件的提醒信息。	开启告警通知
云日志服务	将攻击日志记录到云日志服务（Log Tank Service，简称 LTS）中，通过 LTS 记录 Anti-DDoS 日志，可以高效地进行实时决策分析、设备运维管理以及业务趋势分析。	配置 Anti-DDoS 日志
云监控服务	云监控服务可以监控 Anti-DDoS 相关的指标，用户可以通过指标及时了解防护状况，并通过这些指标设置防护策略。	设置事件告警通知
统一身份认证服务	统一身份认证服务（Identity and Access Management，简称 IAM）为 Anti-DDoS 提供权限管理的功能，拥有对应权限的用户才能使用 Anti-DDoS 服务。	-

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 查看公网 IP 防护状态

购买了公网 IP 后，自动开启 Anti-DDoS“默认防护”，即自动对公网 IP 地址提供 DDoS 攻击保护。

使用限制

开启 Anti-DDoS 防护后，不允许关闭。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

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 在“公网 IP”页签，在公网 IP 列表中查看防护状态。

说明：

- 在“所有防护状态”搜索框中选择防护状态，“公网 IP”界面将只展示对应状态的公网 IP。
- 在搜索框中输入公网 IP 或公网 IP 的关键字，单击搜索或刷新图标，可以搜索指定的公网 IP。

公网 IP 列表参数说明：

参数名称	说明

参数名称	说明
公网 IP	Anti-DDoS 防护的公网 IP 地址。 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
资产类型	NetInterFace
防护设置	当前公网 IP 的流量清洗阈值。

3.2 设置流量清洗阈值

用户为公网 IP 开启 Anti-DDoS 防护后，默认流量清洗阈值为 120Mbps，请根据业务实际进行修改。

前提条件

- 已获取管理控制台的登录账号与密码。
- 公网 IP 已开启 Anti-DDoS 防护。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

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 在“公网 IP”页签，根据实际选择设置方法。

- 为多个公网 IP 设置防护策略：勾选多个公网 IP 后，单击页面上方“防护设置”。
- 为单个公网 IP 设置防护策略：在需要设置防护策略的公网 IP 所在行，单击“防护设置”。

步骤 5 根据实际修改防护参数，参数说明如表 3-1 所示。

表 3-1 防护参数说明

参数名称	说明

参数名称	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。 “默认防护”为“120Mbps”，“手动设置”支持更多档位。 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。 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。

步骤 6 单击“确定”。

----结束

3.3 查看监控报表

用户为公网 IP 开启 Anti-DDoS 防护后，可以查看公网 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账号与密码。
- 公网 IP 已开启 Anti-DDoS 防护。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

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“公网 IP”页签，在需要查看的公网 IP 所在行的“操作”列，单击“查看监控报表”。

步骤 5 在“监控报表”界面，可以查看公网 IP 报表的详细指标。

- 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。

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。

----结束

3.4 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公网 IP 的防护统计信息，包括清洗次数、清洗流量，以及 TOP10 被攻击公网 IP 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账号与密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

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。

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

3.5 开启告警通知

为 Anti-DDoS 开启告警通知以后，当公网 IP 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。

告警通知默认关闭，用户可以根据实际情况手动开启告警通知。

前提条件

已获取管理控制台的登录账号与密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

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”页签，进入告警通知配置页面。

步骤 5 打开告警通知开关。

步骤 6 选择需要接收消息通知主题。

说明

如需创建新的消息通知主题，请单击“查看消息通知主题”，根据提示进行创建。

步骤 7 单击“应用”。

----结束

相关操作

关闭告警通知：在告警通知配置页面，将告警通知状态参数置为关闭状态，即可关闭告警通知。

说明：

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。

3.6 设置事件告警通知

操作场景

通过云监控服务，对防护的弹性公网 IP 启用事件监控，当出现清洗、封堵、解封等事件时进行告警，方便您及时了解防护情况。

开启事件告警通知后，出现相关事件时，即可在云监控服务的事件监控页面查看事件详情。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

步骤 3 选择“管理与部署 > 云监控服务”。

步骤 4 根据实际选择方式。

- 方法一：在左侧导航树，单击“事件监控”，进入“事件监控”页面。

- 方法二：在左侧导航树，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤 5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”页面。

步骤 6 参考表 3-2 配置告警参数。

表 3-2 参数说明

参数	说明
名称	系统会随机产生一个名称，您也可以进行修改。
描述	告警规则描述。
告警类型	选择“事件”。
事件类型	选择“系统事件”。
事件来源	选择“弹性公网 IP”。
监控范围	告警规则适用的资源范围，根据需要选择。
触发规则	选择“自定义创建”。
告警策略	推荐选择“EIP 封堵”、“EIP 解封”、“EIP 开始 DDoS 清洗”、“EIP 结束 DDoS 清洗”。

步骤 7 根据实际需要，选择是否发送通知。

说明

告警消息由消息通知服务 SMN 发送，可能产生少量费用。

表 3-3 通知参数

参数	说明
发送通知	根据实际需要设置。
通知对象	在下拉框选择已有主题，或单击“新建主题”创建新的通知主题。

步骤 8 单击“立即创建”。

----结束

3.7 开启日志记录

操作场景

启用 Anti-DDoS 防护功能后，您可以将攻击日志记录到云日志服务（Log Tank Service，简称 LTS）中，通过 LTS 记录的 Anti-DDoS 日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。

前提条件

已开通云日志服务。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

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“日志”页签，进入日志配置页面。

步骤 5 开启日志  ，并选择日志组和日志流，相关参数说明如表 3-4 所示。

表 3-4 日志配置参数

参数	参数说明
选择日志组	选择已创建的日志组，或者单击“查看日志组”，跳转到 LTS 管理控制台创建新的日志组。
记录攻击日志	选择已创建的日志流，或者单击“查看日志流”，跳转到 LTS 管理控制台创建新的日志流。 攻击日志记录每一个攻击告警信息，包括攻击事件类型、防护动作、攻击源 IP 等信息。

步骤 6 单击“确定”，日志配置成功。

您可以在云日志服务 LTS 控制台查看 Anti-DDoS 的防护日志。

----结束

日志字段说明

表 3-5 全量日志字段说明

字段	说明
logType	日志类型。默认为“ip_attack_sum”，攻击日志。
deviceType	上报日志的设备类型。默认为“CLEAN”，清洗设备。
inKbps	入流量（单位：kbps）。
maxPps	入流量峰值（单位：pps）。
dropPps	丢弃的流量均值（单位：pps）。
maxAttackInBps	攻击流量峰值时刻的入流量值（单位：bps）。
currentConn	当前连接数。
zoneIP	防护的 IP。
logTime	日志产生的时间。
attackType	攻击类型，对应的攻击类型请参考表 3-6。
inPps	入流量（单位：pps）。
maxKbps	入流量峰值（单位：kbps）。
dropKbps	丢弃的流量均值（单位：kbps）。
startTime	攻击开始时间。
endTime	攻击结束时间，为空时则表示攻击还未结束。
maxAttackInConn	攻击流量峰值时刻的连接数。
newConn	新建连接数。

表 3-6 攻击类型说明

数值	攻击类型
0-9	自定义服务攻击
10	Syn Flood 攻击
11	Ack Flood 攻击
12	SynAck Flood 攻击

数值	攻击类型
13	Fin/Rst Flood 攻击
14	并发连接数超过阈值
15	新建连接数超过阈值
16	TCP 分片报文攻击
17	TCP 分片 BandWidth limit 攻击
18	TCP BandWidth limit 攻击
19	UDP flood 攻击
20	UDP 分片攻击
21	UDP 分片 BandWidth limit 攻击
22	UDP BandWidth limit 攻击
23	ICMP BandWidth limit 攻击
24	Other BandWidth limit 攻击
25	总流量限流
26	HTTPS Flood 攻击
27	HTTP Flood 攻击
28	保留
29	DNS Query Flood 攻击
30	DNS Reply Flood 攻击
31	Sip Flood 攻击
32	黑名单丢弃
33	HTTP URL 行为异常
34	TCP 分片 abnormal 丢弃流量
35	TCP abnormal 丢弃流量
36	UDP 分片 abnormal 丢弃流量
37	UDP abnormal 丢弃流量
38	ICMP abnormal 攻击
39	Other abnormal 攻击
40	Connection Flood 攻击
41	域名劫持攻击

数值	攻击类型
42	DNS 投毒攻击报文
43	DNS 反射攻击
44	超大 DNS 报文攻击
45	DNS 源请求速率异常
46	DNS 源回应速率异常
47	DNS 域名请求速率异常
48	DNS 域名回应包速率异常
49	DNS 请求报文 TTL 异常
50	DNS 报文格式异常
51	DNS Cache 匹配丢弃攻击
52	端口扫描攻击
53	TCP Abnormal 攻击(tcp 报文标记位异常)
54	BGP 攻击
55	UDP 关联防范异常
56	DNS NO such Name 异常
57	Other 指纹攻击
58	防护对象限流攻击
59	HTTP 慢速攻击
60	恶意软件防范
61	域名阻断
62	FILTER 过滤
63	Web 攻击抓包
64	SIP 源限速攻击

3.8 查看审计日志

3.8.1 云审计服务支持的 Anti-DDoS 操作列表

云审计服务记录了 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。

云审计服务支持的 Anti-DDoS 操作列表如表 3-7 所示。

表 3-7 支持审计的 Anti-DDoS 操作列表

操作名称	事件名称
开启 Anti-DDoS 防护	OPEN_ANTIDDOS
修改 Anti-DDoS 防护配置	UPDATE_ANTIDDOS
设置 LTS 全量日志配置	UPDATE_LTS_CONFIG
更新租户的告警提醒配置情况	UPDATE_ALERT_CONFIG
修改流量清洗阈值默认档位	UPDATE_DEFAULT_CONFIG
删除流量清洗阈值默认档位	DELETE_DEFAULT_CONFIG

3.8.2 查看云审计日志

开启了云审计服务后，系统开始记录 Anti-DDoS 资源的操作。云审计服务管理控制台保存最近 7 天的操作记录。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

步骤 3 选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。

步骤 4 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤 5 在下拉框中选择“云服务”，输入“Anti-DDoS”，按“Enter”。

步骤 6 在查询结果中单击事件名称，查看事件详情。

事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：

- 事件名称、资源名称、资源 ID、事件 ID：需要输入某个具体的名称或 ID。
  - 资源名称：当该事件所涉及的云资源无资源名称或对应的 API 接口操作不涉及资源名称参数时，该字段为空。
  - 资源 ID：当该资源类型无资源 ID 或资源创建失败时，该字段为空。

- 云服务、资源类型：在下拉框中选择对应的云服务名称或资源类型。
- 操作用户：在下拉框中选择一个或多个具体的操作用户。
- 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
  - normal：表示操作成功。
  - warning：表示操作失败。
  - incident：表示比操作失败更严重的情况，如引起其他故障等。
- 时间范围：可选择查询最近 1 小时、最近 1 天、最近 1 周的操作事件，也可以自定义最近 1 周内任意时间段的操作事件。

----结束

4 最佳实践

4.1 设置 DDoS 攻击告警通知

为 Anti-DDoS 开启告警通知以后，当公网 IP 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账号与密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

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”页签，进入告警通知配置页面。

步骤 5 打开告警通知开关。

步骤 6 选择需要接收消息通知主题。

说明

如需创建新的消息通知主题，请单击“查看消息通知主题”，根据提示进行创建。

步骤 7 单击“应用”。

----结束

4.2 连接已被黑洞的服务器

操作场景

当服务器遭受大流量攻击时，Anti-DDoS 将调用运营商黑洞，屏蔽该服务器的外网访问。对于黑洞的服务器，您可以通过弹性云主机连接该服务器。

前提条件

- 登录账号已购买公网 IP。
- 已获取弹性云主机的登录账号与密码。
- 已获取被黑洞的服务器的登录账号与密码。

约束条件

弹性云主机与被黑洞的服务器同地域且可正常访问。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择区域。

步骤 3 单击页面左上方的 ☰，选择“计算 > 弹性云主机”，进入弹性云主机管理界面。

步骤 4 登录与被黑洞的服务器同地域且可正常访问的弹性云主机。

步骤 5 连接黑洞状态的服务器，连接方式说明如表 4-1 所示。

表 4-1 连接黑洞服务器说明

弹性云服务器的操作系统	黑洞服务器的操作系统	连接方式
Windows	Windows	使用 **mstsc** 方式登录黑洞状态的服务器。 1. 在弹性云主机中输入“mstsc”，单击 mstsc 打开远程桌面连接工具。 2. 在“远程桌面连接”的对话框中，单击“选项”。 3. 输入待登录的云主机的公网 IP 和用户名，默认为“Administrator”。 4. 单击“确定”，根据提示输入密码，登录服务器。
	Linux	使用 PuTTY、Xshell 等远程登录工具登录服务器。

弹性云服务器的操作系统	黑洞服务器的操作系统	连接方式
Linux	Windows	1. 安装远程连接工具（例如 rdesktop）。 2. 执行以下命令，登录黑洞状态的服务器。 **rdesktop -u** *用户名* **-p** *密码* **-g** *分辨率* *黑洞服务器绑定的公网 IP 地址*
	Linux	执行以下命令，登录黑洞状态的服务器。 **ssh** *黑洞服务器绑定的公网 IP*

----结束

后续操作

通过弹性云主机成功连接该服务器后，您可以将处于黑洞状态的服务器上的文件转移至已登录的弹性云主机，您也可以通过这种方式变更该服务器上的配置文件等。

4.3 提升 DDoS 防护能力

天翼云 Anti-DDoS 流量清洗服务为普通用户免费提供 2Gbps 的 DDoS 攻击防护，最高可达 5Gbps，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。

如果急需恢复业务，建议您购买 DDoS 高防服务，提升 DDoS 防护能力。

5 常见问题

5.1 计费类

5.1.1 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。

5.2 概念类

5.2.1 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。ACK Flood 攻击的原理非常简单，黑客向目标服务器发送大量带有 ACK 标记的数据包。由于 ACK 包是确认数据包的标记，服务器在收到 ACK 包后会向发送端返回确认信息，从而消耗服务器的资源。如果攻击量足够大，服务器将不得不忙于处理这些恶意请求，从而无法响应正常用户请求。

5.2.2 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。

5.2.3 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。

5.2.4 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。

5.2.5 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。

5.2.6 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。

5.2.7 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。

5.2.8 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。

您可以通过拦截报告页面，查看所有公网 IP 的防护统计信息，包括清洗次数、清洗流量以及 TOP10 被攻击公网 IP。

5.2.9 Anti-DDoS 流量清洗可以提供哪些数据？

- 您可以查看监控报表，查看单个公网 IP 的监控详情，包括防护状态、流量清洗阈值、24 小时的流量情况、24 小时的异常事件等。
- 您可以查看拦截报告，查看所有公网 IP 的防护统计信息，包括清洗次数、清洗流量以及 TOP10 被攻击公网 IP。

- 您可以为 Anti-DDoS 开启告警通知，当公网 IP 遭受攻击时，您可以及时收到通知。否则，无论攻击流量多大，您都只能登录管理控制台自行查看，无法收到报警信息。

5.2.10 如何判断是否有攻击发生？

- 您可以登录控制台查看监控报表，查看 24 小时的流量情况和 24 小时的异常事件。
- 您可以登录控制台查看拦截报告，查看流量清洗信息。
- 如果您已经开启告警通知，发生攻击事件时，您可以及时收到通知。

5.3 功能类

5.3.1 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。

5.3.2 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。

5.3.3 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。

5.3.4 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。

5.3.5 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）。

5.3.6 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账号密码（例如，管理员账号密码），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。

5.3.7 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。

5.3.8 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。

5.3.9 用户注销账号是否需要清理 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，注销账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。

5.3.10 当遭受超过 5Gbps 的攻击时如何处理？

Anti-DDoS 为普通用户免费提供 2Gbps 的 DDoS 攻击防护，最高可达 5Gbps（视天翼云可用带宽情况）。系统会对超过 5Gbps 的受攻击公网 IP 进行黑洞处理。

5.3.11 Anti-DDoS 防护是一个区域，还是用户的单个 IP？

Anti-DDoS 防护的是用户的单个 IP。

5.3.12 如何查看 Anti-DDoS 流量清洗次数？

您可以通过查看拦截报告，查看指定时间段的流量清洗次数。

5.3.13 如何查看 Anti-DDoS 防护统计信息？

您可以通过查看拦截报告，查看所有公网 IP 的防护统计信息，包括清洗次数、清洗流量以及 TOP10 被攻击公网 IP。

5.3.14 是否能彻底关闭流量清洗功能？

不能。为保护天翼云平台的安全，所有进入天翼云的流量必须开启防护策略。

5.3.15 如何判断入网流量是否经过了 Anti-DDoS 流量清洗服务？

Anti-DDoS 仅对天翼云内的公网 IP 提供 DDoS 攻击防护。

- 若您从外网访问公网 IP，入网流量会先经过公网路由。您可以在公网 IP 所在的云主机上查看访问的路由，若有经过公网路由，则经过了 Anti-DDoS 流量清洗服务。

  若经过了 Anti-DDoS 流量清洗服务，当公网 IP 受到 DDoS 攻击时，会有以下信息：

  - Anti-DDoS 流量清洗服务控制台会有流量清洗记录。
  - 您会收到告警提醒消息（短信或 Email）。
- 若您从内网访问公网 IP，入网流量不会经过公网路由，不经过公网路由，则不经过 Anti-DDoS 流量清洗服务。

  例如：您在天翼云两个不同的区域分别申请了一个公网 IP，那么两个公网 IP 之间相互访问，则不经过 Anti-DDoS 流量清洗服务。

5.4 阈值及黑洞类

5.4.1 Anti-DDoS 流量清洗阈值指什么？

流量清洗阈值是触发 DDoS 防御动作生效的阈值，触发防御后，攻击流量将被拦截，业务流量会被正常放行。

您可以根据实际业务带宽情况调整 Anti-DDoS 流量清洗阈值，具体操作请参考设置流量清洗阈值。

5.4.2 Anti-DDoS 流量清洗阈值如何设置？

您可以根据实际业务带宽情况调整 Anti-DDoS 流量清洗阈值，具体操作请参考设置流量清洗阈值。

5.5 告警通知类

5.5.1 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，例如短信或 Email），属正常现象。

您可以登录控制台查看公网 IP 的防护状态。如果不想被清洗，可以调高流量清洗阈值，具体操作请参考设置流量清洗阈值。

5.5.2 如何取消 Anti-DDoS 告警通知？

当消息订阅者不需要接收“消息通知服务”推送的告警通知时，您可以参考关闭告警通知关闭告警通知。

5.6 业务故障类

5.6.1 公网 IP 流量低的原因？

天翼云为普通用户免费提供 2Gbps 的 DDoS 攻击防护，最高可达 5Gbps（视天翼云可用带宽情况），当攻击超过限定的阈值时，天翼云会采取黑洞策略封堵 IP。

5.6.2 网络流量异常的原因？

为了保障网络的整体可用性，天翼云采用黑洞封堵，对遭受大流量攻击的云主机在一定时间内限制外网通信。

天翼云为普通用户免费提供 2Gbps 的 DDoS 攻击防护，最高可达 5Gbps（视天翼云可用带宽情况），当攻击超过限定的阈值时，天翼云会采取黑洞策略封堵 IP。

5.6.3 监控显示流量平稳，触发流量清洗是什么原因？

Anti-DDoS 检测到 IP 的入流量超过流量清洗阈值时，触发流量清洗。如果不想被清洗，可以调高流量清洗阈值，具体操作请参考设置流量清洗阈值。

5.6.4 DDoS 攻击导致客户端禁止访问，怎么办？

您可以参考查看监控报表和查看拦截报告，判断您的业务是否是遭受 DDoS 攻击，导致 IP 被黑洞封堵，从而引发客户端被禁止访问。

如果确认是遭受 DDoS 攻击导致 IP 被黑洞封堵，请等待自动解封。

5.6.5 遭受流量攻击，如何查询公网 IP 的具体防护信息？

您可以通过查看监控报表，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。

A 修订记录

发布日期	修改说明
2024-11-21	第四次正式发布。 • 优化设置流量清洗阈值步骤描述。 • 优化查看监控报表步骤描述。 • 优化查看拦截报告步骤描述。
2023-12-20	第三次正式发布。 • 新增设置事件告警通知章节。 • 新增配置 Anti-DDoS 日志章节。 • 新增审计章节。 • 优化该产品与其他服务的关系描述。

发布日期	修改说明
2023-10-15	第二次正式发布。 • 新增 Anti-DDoS 的触发条件是什么？章节。 • 新增 Anti-DDoS 流量清洗进行防御时对正常业务有影响吗？章节。 • 新增 Anti-DDoS 清洗机制是怎样的？章节。 • 新增 Anti-DDoS 流量清洗可以提供哪些数据？章节。 • 新增 Anti-DDoS 流量清洗服务支持哪些地区的防护？章节。 • 新增如何判断是否有攻击发生？章节。 • 新增当遭受超过 5Gbps 的攻击时如何处理？章节。 • 新增 Anti-DDoS 防护是一个区域，还是用户的单个 IP？章节。 • 新增如何查看 Anti-DDoS 流量清洗次数？章节。 • 新增如何查看 Anti-DDoS 防护统计信息？章节。 • 新增是否能彻底关闭流量清洗功能？章节。 • 新增如何判断入网流量是否经过了 Anti-DDoS 流量清洗服务？章节。 • 新增阈值及黑洞类章节。 • 新增告警通知类章节。 • 新增业务故障类章节。 • 用户指南优化了操作描述。
2023-05-22	第一次正式发布。