DDoS 防护

快速入门

文档版本 01

发布日期 2023-08-07

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 如何使用 Anti-DDoS 流量清洗

- Anti-DDoS流量清洗服务（以下简称Anti-DDoS）为弹性公网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。
- 本指南通过查看公网IP、开启Anti-DDoS告警通知、配置Anti-DDoS防护策略，以及查看监控和拦截报告的方式，指导您快速上手Anti-DDoS流量清洗服务。

步骤一：准备环境

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“计算 > 弹性云服务器 ECS”。

步骤3 参考购买弹性云服务器创建一台弹性云服务器并绑定弹性公网IP。

说明

- ECS需要绑定一个弹性公网IP，具备外网访问权限。
- 如果用户已有ECS，可重复使用，无需多次创建。

----结束

步骤二：查看公网 IP

步骤1 单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”页面。

步骤2 在“公网IP”页签，查看**步骤一：准备环境**中准备的公网IP已开启默认防护。

图 1-1 查看公网 IP

----结束

步骤三：开启告警通知

步骤1 单击“告警通知”页签。

步骤2 打开告警通知开关，并设置消息通知主题，单击“应用”。

图 1-2 设置告警通知

说明

为Anti-DDoS开启告警通知以后，当弹性公网IP受到DDoS攻击时用户会收到提醒消息（短信或Email）。

----结束

步骤四：配置 Anti-DDoS 防护策略

步骤1 单击“公网IP”页签，在目标公网IP所在行，单击“防护设置”。

图 1-3 防护设置

步骤2 根据实际需要修改防护设置后，单击“确定”。

图 1-4 修改防护设置

说明

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。

----结束

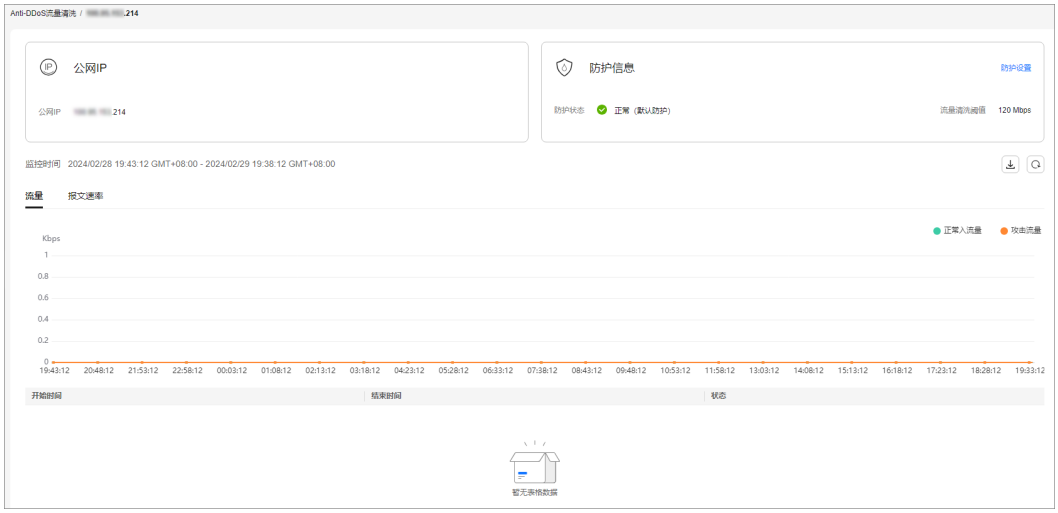
步骤五：查看监控报表

步骤1 单击“公网IP”页签，在目标公网IP所在行，单击“查看监控报表”。

图 1-5 查看监控报表

你可以查看公网IP的防护状态、24小时内流量详情和攻击事件等。

图 1-6 监控详情



----结束

2 快速接入 DDoS 原生高级防护-全力防基础版

DDoS原生高级防护（Cloud Native Anti-DDoS，CNAD）是华为云推出的针对华为云ECS、ELB、WAF、EIP等云服务直接提升其DDoS防御能力的安全服务。DDoS原生高级防护对华为云上的IP生效，通过简单的配置，DDoS原生高级防护提供的安全能力就可以直接加载到云服务上，提升云服务的安全防护能力，确保云服务上的业务安全可靠。

步骤一：购买全力防基础版实例

步骤1 登录管理控制台。

步骤2 单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”页面。

步骤3 在界面右上角，单击“购买DDoS防护”，进入“购买DDoS防护”页面。

步骤4 “实例类型”选择“DDoS原生防护”。

步骤5 “防护规格”选择“全力防基础版”。

步骤6 根据实际需要设置购买参数后，单击“立即购买”，根据提示完成支付。

图 2-1 设置 DDoS 原生防护-全力防基础版防护规格

----结束

步骤二：创建防护策略

步骤1 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤2 参考**添加防护策略**配置防护策略。

----结束

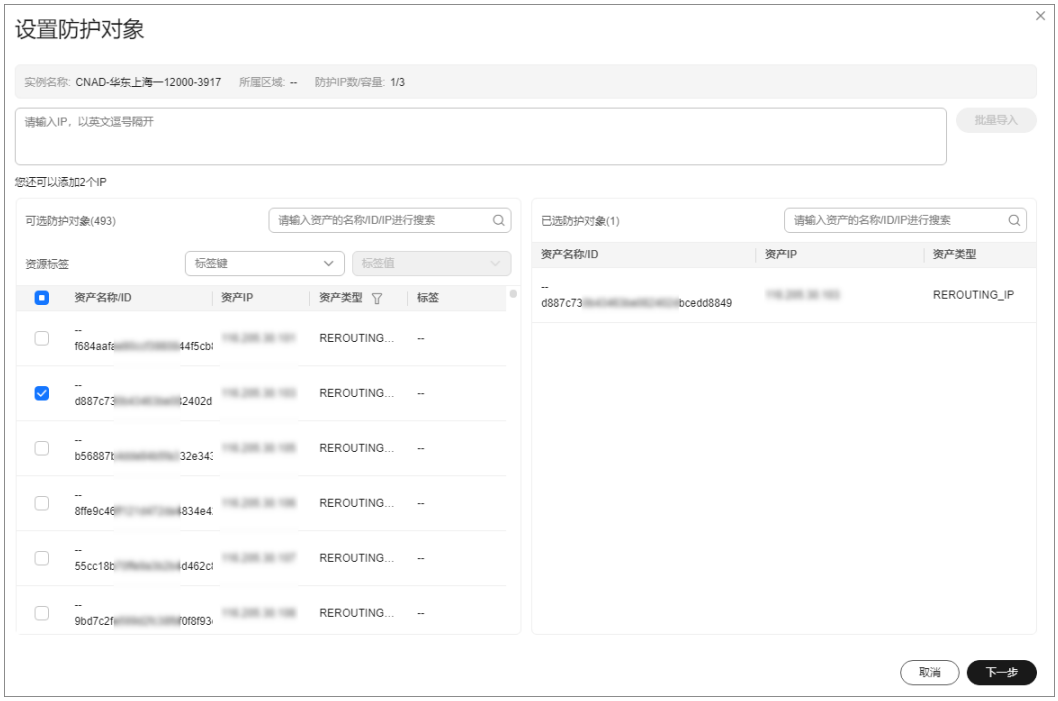
步骤三：添加防护对象

步骤1 在左侧导航栏选择“DDoS原生高级防护 > 实例列表”，进入DDoS原生高级防护“实例列表”页面。

步骤2 在目标实例所在框的右上方，单击“设置防护对象”。

步骤3 参考**添加防护对象**将需要防护的IP资源添加为防护对象。

图 2-2 设置防护对象



说明

添加的防护对象（例如ECS、ELB、WAF、EIP等）IP资源所在区域与购买的DDoS原生高级防护实例区域必须相同。

----结束

3 快速接入 DDoS 原生高级防护-全力防高级版

DDoS原生高级防护（Cloud Native Anti-DDoS，CNAD）是华为云推出的针对华为云ECS、ELB、WAF、EIP等云服务直接提升其DDoS防御能力的安全服务。DDoS原生高级防护对华为云上的IP生效，通过简单的配置，DDoS原生高级防护提供的安全能力就可以直接加载到云服务上，提升云服务的安全防护能力，确保云服务上的业务安全可靠。

步骤一：购买全力防高级版实例

步骤1 登录管理控制台。

步骤2 单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”页面。

步骤3 在界面右上角，单击“购买DDoS防护”，进入“购买DDoS防护”页面。

步骤4 “实例类型”选择“DDoS原生防护”。

步骤5 “防护规格”选择“全力防高级版”。

步骤6 根据实际需要设置购买参数后，单击“立即购买”，根据提示完成支付。

图 3-1 设置 DDoS 原生防护-全力防高级版防护规格

----结束

步骤二：购买专属 EIP 并绑定实例

步骤1 参考**申请弹性公网IP**购买专属EIP。

说明

购买全力防高级版后，专属EIP会在EIP购买页显示，例如“5_DDoSAlways1bgp”，以实际显示为准。

步骤2 参考**将弹性公网IP绑定至实例**将专属EIP绑定给全力防高级版实例。

----结束

步骤三：创建防护策略

步骤1 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤2 参考**添加防护策略**配置防护策略。

----结束

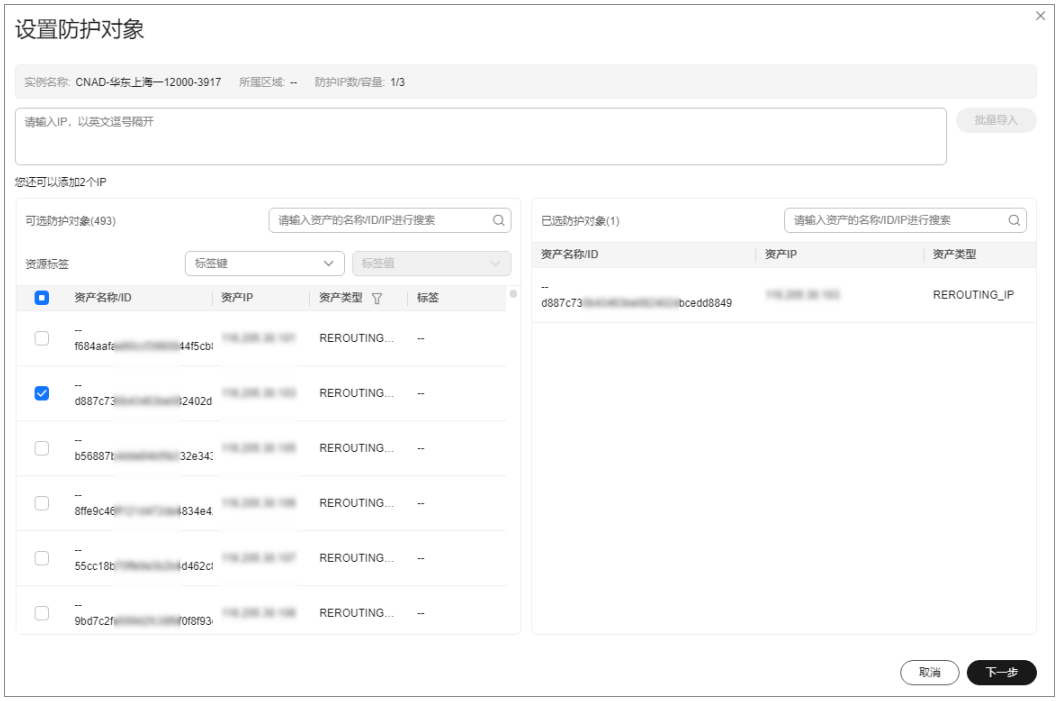
步骤四：添加防护对象

步骤1 在左侧导航栏选择“DDoS原生高级防护 > 实例列表”，进入DDoS原生高级防护“实例列表”页面。

步骤2 在目标实例所在框的右上方，单击“设置防护对象”。

步骤3 参考**添加防护对象**将专属EIP添加为防护对象。

图 3-2 设置防护对象



----结束

4 入门实践

当您成为华为云用户，即可免费使用DDoS原生基础防护（Anti-DDoS流量清洗）服务；如果您需要获得更好的防护能力，推荐购买更高版本的DDoS防护服务。

本文介绍不同版本DDoS防护服务的防护实践，帮助您更好地使用DDoS防护服务。

表 4-1 DDoS 防护

版本	实践		描述
DDoS原生基础防护（Anti-DDoS流量清洗）	使用流程	**如何使用Anti-DDoS流量清洗**	介绍如何快速使用Anti-DDoS流量清洗服务。
	日常维护	**设置DDoS攻击告警通知**	开启DDoS攻击告警通知。
		连接已被黑洞的服务器	通过弹性云服务器远程访问被黑洞的服务器。
	防护升级	**提升DDoS防护能力**	购买更高版本DDoS防护服务。
DDoS原生高级防护	联动防护	**华为云“DDoS原生高级防护+ELB”联动防护**	为部署在华为云ECS上的网站业务配置“DDoS原生高级防护+ELB”联动防护，进一步提升ECS防御DDoS攻击能力。
		华为云“DDoS原生高级防护+独享WAF”联动防护	为部署在华为云ECS上的网站业务配置“DDoS原生高级防护+WAF”联动防护，同时防御四层DDoS攻击和七层Web攻击、CC攻击等，大幅提升网站业务的安全性和稳定性。
DDoS高防	业务接入	**DDoS高防业务接入**	如何快速接入DDoS高防并开展日常维护。
	分析定位	**通过DDoS高防判断遭受的攻击类型**	DDoS高防同时遭受到CC攻击和DDoS攻击时，如何快速判断攻击类型。

版本	实践		描述
		如何获取真实源IP	源站服务器为CentOS7等Linux操作系统时，通过DDoS高防的TOA模块获取真实源IP。
	联动防护	华为云"DDoS高防+WAF"联动	介绍如何配置域名解析，实现华为云“DDoS高防+WAF（Web应用防火墙）”联动。
		华为云“DDoS高防+CDN”联动	当用户的视频、电商等业务系统可以通过域名区分动静态资源，使用“DDoS高防+CDN”联动提升防护。
	等保合规	等保合规安全解决方案	为客户提供一站式的安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保合规要求。
DDoS调度中心	联动防护	DDoS阶梯调度最佳实践	购买DDoS原生防护-全力防基础版时选择开启联动防护后，通过配置DDoS阶梯调度策略，可以自动联动调度DDoS高防对DDoS原生防护-全力防基础版防护的云资源进行防护，提升防护能力。