DDoS 防护

快速入门

文档版本01发布日期2023-08-07





版权所有 © 华为云计算技术有限公司 2024。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

NUAWE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: <u>https://www.huaweicloud.com/</u>

目录

1 如何使用 Anti-DDoS 流量清洗	1
2 快速接入 DDoS 原生高级防护-全力防基础版	5
3 快速接入 DDoS 原生高级防护-全力防高级版	8
4 入门实践	11

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。

- 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

公网IP 拦截报告 告	警通知 日志		
您还可以将345个IP从默认档位调整	到自定义档位		
设置默认防护策略 全部	防护设置		
Q 公网IP:	添加筛选条件		
✓ 公网IP	防护状态	资产类型防护设置	企业项目
214	📀 正常 (默认防护)	EIP 流量清洗調值 120 Mbps	default

----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

公网IP	拦截报告	告警通知	日志
 告答: 此处: 	通知有可能被当成 只能配置清洗告警	垃圾信息而拦截, ,如需配置黑洞封:	如未收到告警通知,请确认是否被拦截。 堵告警,请前往CES的事件监控配置。如何配置CES黑洞封堵事件告警?
清洗流量告警	音阈値 ⑦ 1	000	Kbps
SMN告警通领	ŧлтž 🧲	D	
消息通知主题	ā te	est001	✓ Q 查看消息通知主题
	t.T	立框只展示订阅状态	态为" 已确认 "的消息通知主题。
应用			

🗀 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

公网IP 拦截报告 告誓	嗵知 日志			
您还可以将345个IP从默认档位调整到	自定义档位			
设置默认防护策略 全部开	启防护 防护设置			
Q 公网IP: 214 ×	添加筛选条件			×
□ 公同IP 🔶	防护状态	资产类型 防护设置	企业项目	操作
214	📀 正常 (默认助护)	EIP 流量清洗调值 120 Mbps	default	查看监控报表 防护设置 设置标签
10 ~ 总条数: 1 〈 (1	1			

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

防护设置		×
公网IP	.214	
防护设置	🔵 默认防护 🛛 💿 手动设置	
流量清洗阈值 ⑦	150 Mbps ~	
		取消 确定

🛄 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

公网IP 拦截报告 告警递	劉知 日志			
您还可以将345个IP从默认档位调整到自知	理义档位			
设置默认防护策略 全部开启	助护设置			
Q 公网IP: 214 × ※	页加筛选条件			×
✓ 公同IP	防护状态	资产类型 防护设置	企业项目	操作
214	🥏 正常 (戦込防护)	EIP 流量清洗阀值 120 Mbps	default	查看监控报表 防护设置 设置标签

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

Anti-DDoS汽量清洗 /	
(P) (제제) (P)	◎ 防护信息 899 Km
公開中 214	和学校会 O 正常 (在以近3年) (高齢面内時間 120 Maps
証拠時期間 2024/02/25 19.43.12 GMT+06.00 - 2024/02/29 19.38.12 GMT+06.00	(D) (D)
Rops 1	 正常入流量 吹曲洗量
0.8	
0.4 0.2 1943113 204413 214513 224613 000513 010613 010613 021513 025613 042513 065813 065813 0	2981) 084117 084817 104317 114817 114817 140817 140817 141817 141817 141817 141817 172317 182817 183817
开始出间 机束时间	88
	・ / /

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。

实例类型	DDoS原生防护
计费模式 ⑦	包年包月
防护规格 🕝	全力防高级版 全力防基础版
	针对云上公网IP防护,云原生网络尽力防 接入描引 只能搭配独享WAF
规格描述	接入模式:透明接入 带宽英型:云原生网络,全动态BGP(不支持静态BGP) 防护能力:共享全力防护 ① 保护资源:云资源公网IP,包括ECS,ELB,EIP等
IP协议	IPv4, IPv6双线支持
资源所在地 🕐	华北北凉四 华东-上海一 华南-广州 西南-贵阳一
	注:原生防护实例只能防护相同区域的云资源,不能跨Region防护。
防护IP数 ⑦	- 50 +
	00 Mbps
业务带宽 🕜	
	100 2,500 3,000 7,500 10,000 12,500 15,000 17,500 20,000

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。

- 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

设置防护对象								×
实例名称: CNAD-华东上海一12000-3917	所属区域:	防护IP数/容量: 1/3						
请输入IP, 以英文逗号隔开								批星导入
您还可以添加2个IP								
可选防护对象(493)	请	输入资产的名称/ID/IP进行	搜索 Q		已远防护对象(1)		请输入资产的名称/ID/IP进行	ī搜索 Q
资源标签	建	▼ 标签值			资产名称/ID	资产	τlb	资产类型
■ 资产名称/ID	资产IP	资产类型 🖓	标签	0	 d887c73 bcedd8849		200.00.003	REROUTING_IP
	10.205.30.10	REROUTING	-					
✓ - d887c73 l2402d	10.200.30.10	REROUTING	-					
b56887t 32e34:	14.285.38.10	REROUTING						
	10.200.30.10	REROUTING	-					
	14.285.38.10	REROUTING						
9bd7c2fi 10f8f93	14.285.38.19	REROUTING	-					
								び消 下一步

🗀 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。

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。

实例类型	DDoS原生粉护
计费模式 ⑦	包年包月
防护规格 ⑦	全力防腐吸版 全力防基础版 针对DDos专属原生IP防护,防护带宽更大 专属池EIP受限销售。首次喝买全力防高级版成功后会自动为您开通专属EIP的购买权限。 接入指引 只能搭割换导WAF
规格描述	接入模式: 选明接入 带宽类型:云原生网络,多线BGP 防护能力: 共享全力防护 保护资源:DDoS防护专属EIP
IP协议	IPv4支持
资源所在地 📀	华北北京二 华北北京四 华东-上海一 华南·广州 注:原生防护实例只能防护相同区域的云资源,不能跨Region防护。
防护IP数⑦	- 50 + 100 Mbps
业务带宽 ⑦	III - 100 + 100 5,000 10,000 15,000 20,000 25,000 30,000 35,000 40,000 注: 此市党为高防机房清洗后回源给源站的干净业务流量带党;建议此业务带党规格大于或等于源站出口带党,否则可能会导致丢包或者影响业务。

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。

文档版本 01 (2023-08-07)

图 3-2 设置防护对象

设置防护对象				×
实例名称: CNAD-华东上海一12000-3917 所属的	区域: 防护IP数/容量: 1/3			
请输入IP, 以英文逗号稿开				批量导入
您还可以添加2个IP				
可选防护对象(493)	请输入资产的名称/ID/IP进行搜索 Q	已远防护对象(1)	请输入资产的名称/ID/IP进	行搜索 Q
资源标签	✓ 标签值 ∨	资产名称/ID	资产IP	资产类型
■ 资产名称/ID 资产IP	资产类型 🖓 标签	 d887c73 bcedd8849	10.205.30.003	REROUTING_IP
	REROUTING			
	REROUTING			
b56887t 32e34:	REROUTING			
	REROUTING			
55cc18b d462cl	REROUTING			
9bd7c2f 70f8f93	REROUTING			
			\subset	取消 下一步



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。

	þ	防扎	DoS	DI	4-1	表
--	---	----	-----	----	-----	---

版本	实践		描述
DDoS原生基 础防护 (Anti-DDoS 流量清洗)	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。