DDoS 防护

快速入门

文档版本06发布日期2024-12-31





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	如何免费使用 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	.6
3	快速接入 DDoS 原生高级防护-全力防高级版	13
4	快速接入 DDoS 原生防护 2.0	20
5	入门实践	27

▲ 如何免费使用 Anti-DDoS 流量清洗

购买了华为云弹性公网IP(以下简称EIP)的用户,可以免费使用Anti-DDoS流量清洗 服务(以下简称Anti-DDoS)。

Anti-DDoS为弹性公网IP提供四层的DDoS攻击防护和攻击实时告警通知,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。

Anti-DDoS会对**华为云上的EIP**自动开启防护,您只需要简单配置告警通知、防护策略,即可快速获得Anti-DDoS提供的防护能力。

操作流程

本章节介绍如何为EIP快速配置Anti-DDoS防护,流程如图1-1所示。

图 1-1 操作流程



操作步骤	说明
准备事项	注册华为账号、开通华为云、授予Anti-DDoS权限、准备 防护对象。
步骤一:查看公网IP状态	查看防护对象是否已同步到Anti-DDoS控制台并开启默认 防护。
步骤二:开启告警通知	为防护对象设置流量清洗告警通知。
步骤三:配置Anti- DDoS防护策略	为防护对象配置流量清洗策略。
步骤四:查看监控报表	查看防护对象的防护状态、流量详情。

准备事项

在使用Anti-DDoS流量清洗之前,请先注册华为账号并开通华为云。具体操作详见注册华为账号并开通华为云、实名认证。

如果您已开通华为云并进行实名认证,请忽略此步骤。

- 2. 请确保已为账号赋予相关权限。具体操作请参见创建用户并授权使用Anti-DDoS。
- 3. 参考购买弹性云服务器创建一台ECS服务器并绑定弹性公网IP。

门 说明

如果用户已有符合要求的ECS服务器,可重复使用,无需再次创建。

步骤一: 查看公网 IP 状态

- 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,确保准备事项中准备的公网IP已同步到Anti-DDoS并开启默认防护。

图 1-2 查看公网 IP

公网IP 拦截报告 行	音響通知 日志					
您还可以将345个IP从默认档位调整	您还可以將345个IP从默认档位调整到自定义档位					
设置默认防护策略	设置默认防护策略 全部开启防护 防护设置					
Q 公网IP:	Q 公网IP: 214 × 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 流量清洗阈值 120 Mbps	default			

----结束

步骤二: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,设置告警参数后,单击"应用"。

图 1-3 设置告警通知

公网IP	拦截报告	告警通知	日志
● 告答道 此处只	■知有可能被≦ R能配置清洗領	当成垃圾信息而拦截, 告警, 如需配置黑洞封	如未收到告警通知,请确认是否被拦截。 时堵告警,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	減值 ⑦	1000	Kbps
SMN告警通知	研关		
消息通知主题	I	test001	✓ Q 查看消息通知主题
		下拉框只展示订阅状	态为" 已确认 "的消息通知主题。
应用			

表 1-1 参数说明

参数	示例	说明
清洗流量告 警阈值	1000Кbр s	当清洗流量大小达到该阈值时,发送告警通知,请根据 实际需要设置阈值大小。
SMN告警通 知开关		将告警开关设置为了,打开告警。 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)。
消息通知主 题	-	可以选择使用已有的主题,或单击"查看消息通知主 题"创建新的主题。 主题创建方法请参考 <mark>创建主题</mark> 。

----结束

步骤三: 配置 Anti-DDoS 防护策略

图 1-4 防护设置

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"。

公网IP 拦截报告 告警测	通知 日志						
您还可以将345个IP从默认档位调整到自	通可以病345个19从患以無位満難到局定又無位						
设置默认防护策略	訪护 防护设置						
Q 公网IP: 214 × 第	Q 公務中: 244 × 諸加強恐怖				×		
□ 公同IP 争	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	流量清洗阈值 120 Mbps	default	查看些拉报表 防护设置 设置标签		
10 ~ 总条数: 1 〈 1	10 ~						

步骤2 根据实际需要修改防护设置后,单击"确定"。

图 1-5 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

表 1-2 参数说明

参数	示例	说明
防护设置	手动设置	默认防护为120Mbps,手动设置支持更多其他档 位。
流量清洗阈 值	150Mbps	建议选择与所购买带宽最接近的数值,但不超过购 买带宽。
		Anti-DDoS检测到IP的入流量超过该阈值时,触发流 量清洗。

----结束

步骤四: 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 1-6 查看监控报表

公网IP 拦	載报告 告警通知	日志				
您还可以将345个I	这可以将345个时代,就从他应该撤到自定义地位					
设置默认防护的	義略 全部开启防护	防护设置				
Q 公网IP:	214 × 添加筛选条	件				×
公司IP <	•	防护状态	资产类型	防护设置	企业项目	操作
	214	正常 (数认助护)	EIP	流量清洗阈值 120 Mbps	default	查看监控报表 防护设置 设置标签

您可以查看公网IP的防护状态、24小时内流量详情和攻击事件等。

图 1-7 监控详情

Anti-DDoS流量源	院 /214		
P	公网IP	⑦ 防护信息 □>>≤8	
公网IP	214	8))中华古 🕑 正架 (RKU25(P) 正路(RKU25(P) 120 Moo	3
监控时间	2024/02/28 19 43 12 GMT+08:00 - 2024/02/29 19:38 12 GMT+08:00	(±)	Q
Kbps 1		夏菜入民量 ● 校会)	后量
0.8			
0.2	2 204812 215312 225812 000312 010812 021312 031812 042312 052812 063312 0	Jariz 0842112 094812 1052112 115812 130312 140812 1512112 161812 172212 182812 193	3:12
开始时间	结束时间	17.25 17.25	

----结束

相关信息

- 如果您需要对防护的EIP启用事件监控,当出现清洗、封堵、解封等事件时都进行告警,请参考设置事件告警通知进行配置。
- 如果您的EIP被攻击导致黑洞,您可以使用自助解封功能提前解封黑洞,具体操作 参考自助解封封堵IP。
- 如果您需要对防护的EIP开启攻击日志记录,用于后续分析、运维,可开启LTS日志,具体参考请参考配置Anti-DDoS日志。

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-全力防基础版针对**华为云的全动态BGP EIP**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。

本章节以防护中国大陆的华北-北京四区域的EIP为例,指导您如何购买和使用全力防基础版。

操作流程

本章节介绍如何快速购买全力防基础版并开启防护,流程如图2-1所示。





操作步骤	说明	
准备事项	注册华为账号、开通华为云、为账户充值、授予DDoS原 生高级防护权限、准备防护对象。	
步骤一:购买全力防基 础版	在指定区域购买全力防基础版。	
步骤二:创建防护策略	为防护对象创建并配置防护策略。	
步骤三:添加防护对象	将防护对象添加到全力防基础版实例。	

准备事项

- 在使用全力防基础版之前,请先注册华为账号并开通华为云。具体操作详见注册 华为账号并开通华为云、实名认证。
 如果您已开通华为云并进行实名认证,请忽略此步骤。
- 请保证账户有足够的资金,防止购买全力防基础版失败。具体操作请参见账户充值。
- 3. 请确保已为账号赋予相关权限。具体操作请参见创建用户并授权使用CNAD。
- 4. 在华北-北京四区域参考购买弹性云服务器创建一台ECS服务器并绑定弹性公网 IP。

🛄 说明

如果用户已有符合要求的ECS服务器,可重复使用,无需再次创建。

步骤一:购买全力防基础版

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 设置购买参数后,单击"立即购买",根据提示完成支付。

表 2-1 参	褖数说明
---------	------

参数	示例	说明
实例类型	DDoS原生防护	需要购买的实例类型。
计费模式	包年包月	按订单的购买周期计费,需要用户预先支付一定 时长的费用。 全力防基础版只支持包年包月。
防护区域	中国大陆	 中国大陆:适用于业务服务器部署在中国大陆的场景(支持跨Region),仅支持全动态BGP EIP。 中国大陆外:适用于业务服务器部署在亚太地区(当前支持香港)的场景,仅支持优选BGP EIP。
防护规格	全力防基础版	需要购买的版本。
资源所在地	华北-北京四	防护的云资源所在区域。不能跨区域 (Region)防护。
防护IP数	50	防护IP数是指每个DDoS原生高级防护实例支持 防护的EIP数量,建议根据您的云资源拥有的EIP 数量进行评估。

参数	示例	说明
业务带宽	100Mbps	业务带宽是指高防机房清洗后回源给源站的干净 业务流量带宽。建议此业务带宽规格大于或等于 源站出口带宽,否则可能会导致丢包或者影响业 务。
实例名称	CNAD-test	购买的实例名称,自定义。
企业项目	-	仅当使用企业类型的账号购买时,会显示该参 数,请根据实际选择。
购买时长	-	购买的时长,请根据实际选择。
购买数量	-	购买的数量,请根据实际选择。

实例类型 DDoS原生防护 DDoS高防 DDoS高防国际版 DDoS调度中心
计费模式 ⑦ 包年包月
ペロノ国中
防护规格 ③
全力防高级版 全力防基础版 标准版 原生防护2.0
针对云上公网IP防护,云原生网络尽力防 接入指引 只能搭配独享WAF
规格描述
接入模式: 透明接入
带宽类型: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 ⑦
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 ⑦
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 ②
- 50 +
业务带竞 ②
100Mbps 1,000Mbps 5,000Mbps 10,000Mbps 20,000Mbps 自定义
实例名称
CNAD-e20c
一次创建多个实例时,系统会自动在实例名后增加后缀,例如:CNAD-0001。
购买时长
3个月 6个月 1年
自动续费 ②
购买数量

图 2-2 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

🛄 说明

DDoS原生高级防护支持的防护策略较多,此处以清洗策略为例进行介绍。

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

步骤2 单击"创建策略",创建一个策略。

表 2-2 参数说明

参数	示例	说明
策略名称	Policy01	防护策略的名称,自定义。
所属实例	选择 <mark>步骤</mark> 4中购买 的实例。	防护策略需要防护的目标实例。

步骤3 在创建的策略所在行,单击"配置策略",进入"策略内容"页面。

步骤4 在"基础防护"下方,单击"设置"。

图 2-3 基础防护

	基础防护
\otimes	DDoS防护检测到IP的入流量超过该阈值时,触发流量清洗。"流量清洗档位"可按照实际业务流量进行设置,建议设置为与 所购买带宽最接近的数值,但不超过购买带宽。每个档位提供三套基础防护策略,实现对常见网络层攻击的秒级阻断。
	设置 流量清洗阈值 300 Mbps 防御模式 正常

步骤5 在弹出的"基础防护设置"对话框中,设置流量清洗档位和防御模式。

图 2-4 基础防护设置

基础防护设置	×
流量清洗档位	
300 Mbps	~
请按照实际业务流量选择参数。建议设置为与所购买IF 宽。	带宽最接近的数值,但不超过购买带
防御模式	
🔵 宽松 (豆常 🗌 严格	
	取消 确定

表 2-3 参数说明

参数	示例	说明
流量清洗档位	300Mbps	当IP遭受的DDoS攻击带宽超过配置的清洗档位 时,触发DDoS原生高级防护对攻击流量进行清 洗。
		建议选择与已购买带宽最接近的数值,但不超过已 购买带宽。
防御模式	正常	流量达到设定的流量档位,将会触发流量清洗。
		• 宽松: 流量达到清洗档位的3倍后触发清洗。
		• 正常:流量达到清洗档位的2倍后触发清洗。
		 严格:流量达到清洗档位就触发流量清洗。

----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"选择实例"中,选择**步骤4**中购买的实例。
- 步骤3 单击"设置防护对象",进入"设置防护对象"界面。
- 步骤4 勾选准备事项中准备的弹性公网IP,单击"下一步"。

图 2-5 设置防护对象

文例名称 所置区域: 防分P取物容量: 45 環緒入P, 以英文運時隔开 ジZGQU版加4/NP 可透防炉対象(388) 博輸入资产的ID/P进行搜索 改振時座 必須時座 ご 強力D 資产IP 資产ID 資产IP 資产ID 資产IP ご 184 184 abfa9 - - - -	×
講報入IP, 以英文運写稿开 認述可以添加41/P 可透動炉対象(388) 講報入资产的ID/P进行搜索 资源标签 标签键 资源标D 资产IP 资产ID 资产IP 第 10	
ま な	批量导入
可透热炉对象(388) 请输入资产的DDIP进行搜索 Q 资源标签 标签键 新签值 资产D 资产P 资产型 資产 第2 标签 18 10 18 10	
	Q
淡戸D 淡戸契型 1 枝茎 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	类型
 • • 184 • sbfa9 • 10 •	0.750_F
 V 184 abfa9 .10 	
 ✓ 18. abfa9 10 	
· · · · · · · · · · · · · · · · · · ·	
ART/TENCHERNARDAREN THE DR IN . ARTICUTE.	
Inclusion considering inclusion and approximent and	
BARTANING AND AND A REALTAN	
antal-Assessment and as Assessment	

步骤5 单击"确定"。

----结束

相关信息

- 如果需要及时获取DDoS攻击信息,您可以设置告警通知,具体操作请参考设置告 警通知。
- DDoS原生高级防护支持查看流量趋势、攻击分布等信息,具体操作请参考查看数据报表。

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-全力防高级版针对**华为云的DDoS防护专属EIP**生效,通过简单的配置,DDoS 原生高级防护-全力防高级版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。

本章节以防护中国大陆的华北-北京四区域为例,指导您如何购买和使用全力防高级 版。

操作流程

本章节介绍如何快速购买全力防高级版并开启防护,流程如图3-1所示。

图 3-1 操作流程



操作步骤	说明
准备事项	注册华为账号、开通华为云、为账户充值、授予DDoS原 生高级防护权限、准备ECS服务器。
步骤一: 购买全力防高 级版	在指定区域购买全力防高级版。
步骤二:购买专属EIP 并绑定ECS	在指定区域购买DDoS防护专属EIP并绑定到ECS服务器。
步骤三: 创建防护策略	为防护对象创建并配置防护策略。
步骤四:添加防护对象	将防护对象添加到全力防高级版实例。

文档版本 06 (2024-12-31)

准备事项

- 在使用全力防高级版之前,请先注册华为账号并开通华为云。具体操作详见注册 华为账号并开通华为云、实名认证。
 如果您已开通华为云并进行实名认证,请忽略此步骤。
- 请保证账户有足够的资金,防止购买全力防高级版失败。具体操作请参见账户充值。
- 3. 请确保已为账号赋予相关权限。具体操作请参见创建用户并授权使用CNAD。
- 4. 在华北-北京四区域参考购买弹性云服务器创建一台ECS服务器。
- 步骤一:购买全力防高级版
 - 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 设置购买参数后,单击"立即购买",根据提示完成支付。

参数	示例	说明
实例类型	DDoS原生防护	需要购买的实例类型。
计费模式	包年包月	按订单的购买周期计费,需要用户预先支付一定 时长的费用。 全力防高级版只支持包年包月。
防护区域	中国大陆	 中国大陆:适用于业务服务器部署在中国大陆的场景(支持跨Region),仅支持全动态BGP EIP。 中国大陆外:适用于业务服务器部署在亚太地区(当前支持香港)的场景,仅支持优选BGP EIP。
防护规格	全力防高级版	需要购买的版本。
资源所在地	华北-北京四	防护的云资源所在区域。不能跨区域 (Region)防护。
防护IP数	50	防护IP数是指每个DDoS原生高级防护实例支持 防护的EIP数量,建议根据您的云资源拥有的EIP 数量进行评估。
业务带宽	100Mbps	业务带宽是指高防机房清洗后回源给源站的干净 业务流量带宽。建议此业务带宽规格大于或等于 源站出口带宽,否则可能会导致丢包或者影响业 务。
实例名称	CNAD-test	购买的实例名称,自定义。

表 3-1 参数说明

参数	示例	说明
企业项目	-	仅当使用企业类型的账号购买时,会显示该参 数,请根据实际选择。
购买时长	-	购买的时长,请根据实际选择。
购买数量	-	购买的数量,请根据实际选择。

图 3-2 全力防高级版

实例类型 DDoS原生防护 DDoS高防 DDoS高防国际版 DDoS调度中心
計要模式 ② 包年包月 防护区域 ③ 中国大陆 中国大陆外 防护规格 ③ 全力防高级版 全力防基础版 原生防护2.0 针对DDos专属原生IP防护,防护带宽更大 专属池EIP受限销售。首次购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 只能措面独享WAF
期格描述 発入機式: 瓷明接入 荒炭葉型: 完厚生四弦: 余线BGP 防护法: 芒夏全力防治: 保护资源: DDoS防护专属EIP Ph以 Pv4支持 愛願所在地 ⑦ 华北北京二 华东上海一 华北北京二 华东上海一 安康广州 注: 原生防护突侧只能防护相同区域的云资源, 不能劈Region防护 DipP数 ⑦ - 50 + 少年帝 ⑦ 100Mbps 500Mbps 1,000Mbps 百定义 注: 此带宽为高防机房清洗后回漂给漂站的干净业务流量带宽; 建议此业务带宽规格大于或等于漂站出口带宽, 否则可能会导致去包或者影响业务
自动续费 ⑦ 购买数量 - 1

----结束

步骤二: 购买专属 EIP 并绑定 ECS

步骤1 参考申请弹性公网IP在华北-北京四区域购买一个专属EIP。

🛄 说明

华北-北京四区域的EIP线路为"5_DDoSAlways1bgp",实际以控制台显示为准。

步骤2 参考将弹性公网IP绑定至实例将购买的专属EIP绑定到准备事项中的ECS服务器。

----结束

步骤三: 创建防护策略

🛄 说明

DDoS原生高级防护支持的防护策略较多,此处以清洗策略为例进行介绍。

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

步骤2 单击"创建策略",创建一个策略。

表 3-2 参数说明

参数	示例	说明
策略名称	Policy01	防护策略的名称,自定义。
所属实例	选择 <mark>步骤</mark> 4中购买 的实例。	防护策略需要防护的目标实例。

步骤3 在创建的策略所在行,单击"配置策略",进入"策略内容"页面。

步骤4 在"基础防护"下方,单击"设置"。

图 3-3 基础防护

		基础防护
	\otimes	DDoS防护检测到IP的入流量超过该阈值时,触发流量清洗。"流量清洗档位"可按照实际业务流量进行设置,建议设置为与 所购买带宽最接近的数值,但不超过购买带宽。每个档位提供三套基础防护策略,实现对常见网络层攻击的秒级阻断。
		设置 流星清洗阈值 300 Mbps 防御模式 正常

步骤5 在弹出的"基础防护设置"对话框中,设置流量清洗档位和防御模式。

图 3-4 基础防护设置

基础防护设置	×
流量清洗档位	
300 Mbps	~
请按照实际业务流量选择参数。建议设置为与所购买IF 宽。	P带宽最接近的数值,但不超过购买带
防御模式	
🔵 宽松 💿 正常 🕢 严格	
	取消 确定

表 3-3参数说明

参数	示例	说明
流量清洗档位	300Mbps	当IP遭受的DDoS攻击带宽超过配置的清洗档位 时,触发DDoS原生高级防护对攻击流量进行清 洗。 建议选择与已购买带宽最接近的数值,但不超过已 购买带宽。
防御模式	正常	流量达到设定的流量档位,将会触发流量清洗。 • 宽松:流量达到清洗档位的3倍后触发清洗。 • 正常:流量达到清洗档位的2倍后触发清洗。 • 严格:流量达到清洗档位就触发流量清洗。

----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"选择实例"中,选择**步骤4**中购买的实例。
- 步骤3 单击"设置防护对象",进入"设置防护对象"界面。
- 步骤4 勾选准备事项中准备的专属EIP,单击"下一步"。

图 3-5 设置防护对象

设置	防护对象									:	\times
实例名	称:		所属区域:	防护IP数/容量: 4/5							
清輸)	\IP,以英文逗号隔开									批量导入	
您还可以	↓添加4个IP										
可选助	前対象(388)		谱	输入资产的ID/IP进行搜	۲	Q		已远防护对象(1)	请输入资产的IC	D/IP进行搜索 Q	
资源标	筂	标签	键	▼ 标签值		~		资产ID	资产IP	资产类型	
0	资产ID		资产IP	资产类型 🖓	标签		0	18;	10	NENCLIPHE_P	
	00004441740.449	-	110,200,301	MERCUTIN.							
	1-1010/17-14-14050	who i	10.200.201	8050,751							
	18;	abfa9	.1	0							
	Resource concerned		110,200,30	8080174							
	801/10-040a/00	-		8050,751							
	DOM: NO PROPERTY AND INCOME.	-		4040474							
	an paraceter	-		8080179							
	10100000000000000000000000000000000000	-	10.200.00	8080174							
										取消 下一步	

步骤5单击"确定"。

----结束

相关信息

- 如果需要及时获取DDoS攻击信息,您可以设置告警通知,具体操作请参考设置告 警通知。
- DDoS原生高级防护支持查看流量趋势、攻击分布等信息,具体操作请参考查看数据报表。

4 快速接入 DDoS 原生防护 2.0

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-原生防护2.0针对华为云上的EIP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。

DDoS原生防护2.0中国大陆区域同时支持防护普通EIP和DDoS防护专属EIP,中国大陆 外区域同时支持防护优选BGP EIP和DDoS防护专属EIP。

本章节以防护中国大陆区域的普通EIP为例,指导您如何购买和使用原生防护2.0。

操作流程

本章节介绍如何快速购买原生防护2.0并开启防护,流程如图4-1所示。

图 4-1 操作流程



操作步骤	说明
准备事项	注册华为账号、开通华为云、为账户充值、授予DDoS原 生高级防护权限、准备防护对象。
步骤一: 购买原生防护 2.0	在指定区域购买原生防护2.0。
步骤二:创建防护策略	为防护对象创建并配置防护策略。
步骤三:添加防护对象	将防护对象添加到原生防护2.0实例。

准备事项

- 在使用全力防基础版之前,请先注册华为账号并开通华为云。具体操作详见注册 华为账号并开通华为云、实名认证。
 如果您已开通华为云并进行实名认证,请忽略此步骤。
- 2. 请保证账户有足够的资金,防止购买原生防护2.0失败。具体操作请参见<mark>账户充</mark> <u>值</u>。
- 3. 请确保已为账号赋予相关权限。具体操作请参见创建用户并授权使用CNAD。
- 4. 在参考购买弹性云服务器创建一台ECS服务器并绑定EIP。

步骤一:购买原生防护 2.0

- 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 设置购买参数后,单击"立即购买",根据提示完成支付。

参数	示例	说明
实例类型	DDoS原生防护	需要购买的实例类型。
计费模式	包年包月	按订单的购买周期计费,需要用户预先支付一定 时长的费用。当前只支持包年包月。
防护区域	中国大陆	 中国大陆:适用于业务服务器部署在中国大 陆的场景(支持跨Region),仅支持全动态 BGP EIP。
		 中国大陆外:适用于业务服务器部署在亚太 地区(当前支持香港)的场景,仅支持优选 BGP EIP。
防护规格	原生防护2.0	需要购买的版本。
防护IP数	50	防护IP数是指每个DDoS原生高级防护实例支持 防护的EIP数量,建议根据您的云资源拥有的EIP 数量进行评估。
公网线路计 费模式	按需计费	 包年包月:按订单的购买周期,需要用户预 先支付一定时长的费用,按照业务带宽计 费。
		 按需计费:按照每天实际产生的干净流量计费。
计量规则	干净流量	干净流量是指未被污染的正常业务流量,不包含 攻击流量。

表 4-1 参数说明

参数	示例	说明
业务带宽	100Mbps	业务带宽是指高防机房清洗后回源给源站的干净 业务流量带宽。建议此业务带宽规格大于或等于 源站出口带宽,否则可能会导致丢包或者影响业 务。
		公网线路计费模式为包年包月才有该参数。
实例名称	CNAD-test	购买的实例名称,自定义。
企业项目	-	仅当使用企业类型的账号购买时,会显示该参 数,请根据实际选择。
购买时长	-	购买的时长,请根据实际选择。
购买数量	-	购买的数量,请根据实际选择。

图 4-2 原生防护 2.0

实例类型
DDoS原生防护 DDoS高防 DDoS高防国际版 DDoS调度中心
包牛包月
防护区域 ⑦
中国大陆中国大陆外
防护规格 ⑦
全力防高级版 全力防基础版 标准版 原生防护2.0
规格描述
接入模式: 透明接入
带宽类型:云原生网络,多线BGP 防护能力:共享全力防护(⑦
保护资源:全动态BGP EIP, DDoS防护专属EIP
IP协议
IPv4, IPv6双线支持
资源所在地
中国大陆Region(支持多Region防护,包括北京四、上海一、华南广州等)
防护IP数 ③
- 50 +
公网线路计费模式 ⑦
包年包月 按需计费
计量规则 ⑦
干净流量
按照每天实际产生的干净流量计费产品价格详情 [2]
实例名称
CNAD-1410
一次创建多个实例时,系统会自动在实例名后增加后缀,例如:CNAD-0001。
企业项目 ②
default ~
购买时长
1个月 3个月 6个月 1年
购买数量
- 1 +

----结束

步骤二: 创建防护策略

🛄 说明

DDoS原生高级防护支持的防护策略较多,此处以清洗策略为例进行介绍。

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

步骤2 单击"创建策略",创建一个策略。

表 4-2 参数说明

参数	示例	说明
策略名称	Policy01	防护策略的名称,自定义。
所属实例	选择 <mark>步骤</mark> 4中购买 的实例。	防护策略需要防护的目标实例。

步骤3 在创建的策略所在行,单击"配置策略",进入"策略内容"页面。

步骤4 在"基础防护"下方,单击"设置"。

图 4-3 基础防护

	基础防护					
\otimes	DDoS防护检测到IP的入流量超过该阈值时,触发流量清洗。"流量清洗档位"可按照实际业务流量进行设置,建议设置为与 所购买带宽最接近的数值,但不超过购买带宽。每个档位提供三套基础防护策略,实现对常见网络层攻击的秒级阻断。					
	设置 流量清洗阈值 300 Mbps 防御模式 正常					

步骤5 在弹出的"基础防护设置"对话框中,设置流量清洗档位和防御模式。

图 4-4 基础防护设置

基础防护设置	\times
流量清洗档位	
300 Mbps ~	
请按照实际业务流量选择参数。建议设置为与所购买IP带宽最接近的数值,但不 宽。	超过购买带
防御模式	
○ 宽松 (● 正常 ○ 严格	
取消	确定

表 4-3 参数说明

参数	示例	说明		
流量清洗档位	300Mbps	当IP遭受的DDoS攻击带宽超过配置的清洗档位 时,触发DDoS原生高级防护对攻击流量进行清 洗。		
		建议选择与已购买带宽最接近的数值,但不超过已 购买带宽。		
防御模式	正常	流量达到设定的流量档位,将会触发流量清洗。		
		• 宽松:流量达到清洗档位的3倍后触发清洗。		
		• 正常:流量达到清洗档位的2倍后触发清洗。		
		 严格:流量达到清洗档位就触发流量清洗。 		

----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"选择实例"中,选择**步骤4**中购买的实例。
- 步骤3 单击"设置防护对象",进入"设置防护对象"界面。
- 步骤4 勾选准备事项中准备的EIP,单击"下一步"。

图 4-5 设置防护对象

实例系称 所属区域 防护P数容量 415							
请输入IP,以英文运号隔开 就是马入							
您还可以添加	思述可以添加4个IP						
可选防护对	寸象(388)	请辅	入资产的ID/IP进行搜索	Q	已选防护对象(1)	请输入资产的ID/IP进行	ī搜索 Q
资源标签		标签键	 「标签值 	~	资产ID	资产IP	资产类型
资	产ID	资产IP	资产类型 🍸 🛛 标签	•	18;	10	10101710.0
	Contract Charlos		880,78				
	1011/11/14/14/00/1	10.200.001	800.75				
18	3i at	bfa9 .10	8080278				
0	NAME AND ADDRESS		8980,798				
\Box	0.7360404000	10.25.2	885.75				
	0.0000000000000000000000000000000000000	192 10.200.00	8880,751				
	- 24000-24000	10.200.30	80804798				
	1	10.26.0	800.010				
							取消下一步

步骤5单击"确定"。

----结束

相关信息

- 如果需要及时获取DDoS攻击信息,您可以设置告警通知,具体操作请参考设置告 警通知。
- DDoS原生高级防护支持查看流量趋势、攻击分布等信息,具体操作请参考查看数据报表。



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 5-1 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	如何免费使用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	通过ECS访问被黑洞 的服务器	通过弹性云服务器远程访问被黑洞 的服务器。	
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。	
DDoS高防	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。	