DDoS 防护 AAD

用户指南

文档版本 09

发布日期 2025-02-08

华为技术有限公司

版权所有 © 华为技术有限公司 2025。 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


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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

 版权所有 © 华为技术有限公司

目 录

 版权所有 © 华为技术有限公司

 版权所有 © 华为技术有限公司

 版权所有 © 华为技术有限公司

1 DDoS 原生基础防护操作指南

1.1 Anti-DDoS 流量清洗概述

EIP加入DDoS原生基础防护（Anti-DDoS流量清洗）的进行防护的流程如图1-1所示。

图 1-1 Anti-DDoS 使用流程

表 1-1 流程说明

序号	流程	说明
1	开启防护	Anti-DDoS流量清洗为免费服务，购买EIP时自动开启防护。
2	通过IAM授予使用Anti-DDoS的权限	通过统一身份认证服务（Identity and Access Management，简称IAM）为用户授予精细的Anti-DDoS服务权限。
3	设置EIP防护策略	为防护的EIP设置流量清洗阈值，当实际业务流量触发流量清洗阈值时，Anti-DDoS将对流量进行清洗，缓解DDoS攻击。

版权所有 © 华为技术有限公司

序号	流程	说明
4	常用安全操作	• **设置告警通知实现DDoS攻击预警**：为Anti-DDoS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。 • **开启DDoS事件告警通知**：通过云监控服务，对防护的EIP启用事件监控，当出现清洗、封堵、解封等事件时进行告警。 • **为EIP添加标签**：可以使用标签对云资源进行分类，方便管理。 • **查看EIP监控报表**：查看指定公网IP的监控详情，包括、防护状态、防护参数、24小时的流量情况和异常事件等。 • **查看拦截报告**：查看用户所有公网IP地址的防护统计信息，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10等。 • **查询审计日志**：通过云审计服务查看历史Anti-DDoS的操作记录。

说明

DDoS原生基础防护暂不支持GEIP、GA类型的公网IP的攻击告警通知和防护策略定制。

1.2 通过 IAM 授予使用 Anti-DDoS 的权限

1.2.1 创建用户并授权使用 Anti-DDoS

如果您需要对您所拥有的Anti-DDoS进行精细的权限管理，）您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用Anti-DDoS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将Anti-DDoS资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用Anti-DDoS服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图1-2**所示。

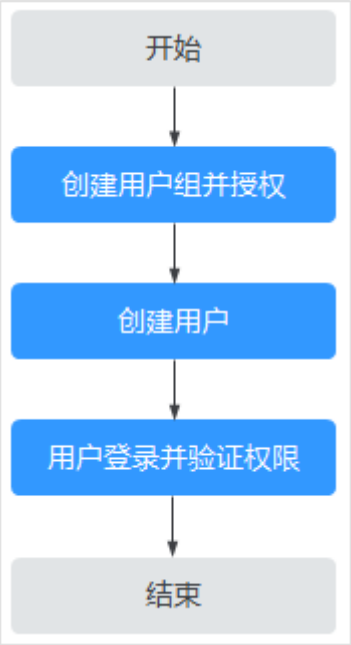
前提条件

给用户组授权之前，请您了解用户组可以添加的Anti-DDoS权限，并结合实际需求进行选择，Anti-DDoS支持的系统权限，请参见：**Anti-DDoS系统权限**。如果您需要对除Anti-DDoS之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

版权所有 © 华为技术有限公司

示例流程

图 1-2 给用户授权服务权限流程



1. **创建用户组并授权**。

   在IAM控制台创建用户组，并授予Anti-DDoS服务的管理员权限“Anti-DDoS Administrator”。

2. **创建用户并加入用户组**。

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限。

   新创建的用户登录控制台，切换至授权区域，验证权限：

   单击页面左上方的 ☰，选择除Anti-DDoS服务外的任一服务，如果提示权限不足，表示“Anti-DDoS Administrator”已生效。

1.2.2 Anti-DDoS 自定义策略

如果系统预置的Anti-DDoS权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见**Anti-DDoS权限及授权项**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的Anti-DDoS自定义策略样例。

 版权所有 © 华为技术有限公司

Anti-DDoS 自定义策略样例

- 示例1：授权用户查询Anti-DDoS默认防护策略

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "anti-ddos:defaultDefensePolicy:get"
                        ]
        }
    ]
}
```

1.2.3 Anti-DDoS 权限及授权项

如果您需要对您所拥有的Anti-DDoS进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用Anti-DDoS的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

权限	授权项	依赖关系说明
查询Anti-DDoS默认防护策略	anti-ddos:defaultDefensePolicy:get	-
配置Anti-DDoS默认防护策略	anti-ddos:defaultDefensePolicy:create	-
删除Anti-DDoS默认防护策略	anti-ddos:defaultDefensePolicy:delete	-
查询Anti-DDoS配置可选范围	anti-ddos:optionalDefensePolicy:list	-

版权所有 © 华为技术有限公司

权限	授权项	依赖关系说明
查询Anti-DDoS服务	anti-ddos:ip:getDefensePolicy	vpc:publicIps:list
更新Anti-DDoS服务	anti-ddos:ip:updateDefensePolicy	-
开通Anti-DDoS服务	anti-ddos:ip:enableDefensePolicy	-
查询周防护统计情况	anti-ddos:ip:getWeeklyReport	-
查询指定EIP防护流量	anti-ddos:ip:getDailyTrafficReport	-
查询指定EIP异常事件	anti-ddos:ip:getDailyEventReport	-
查询指定EIP防护状态	anti-ddos:ip:getDefenseStatus	-
查询EIP防护状态列表	anti-ddos:ip:listDefenseStatuses	-
查询Anti-DDoS任务	anti-ddos:task:list	-
查询告警配置信息	anti-ddos:alertConfig:get	smn:topic:list
更新告警配置信息	anti-ddos:alertConfig:update	-
查询云日志服务配置	anti-ddos:logConfig:get	-
更新云日志服务配置	anti-ddos:logConfig:update	-
查询配额	anti-ddos:quota:list	-
查询资源标签列表	anti-ddos:ip:listTagsForResource	-
批量添加标签	anti-ddos:ip:tagResource	-
批量删除标签	anti-ddos:ip:untagResource	-

1.2.4 控制台的权限依赖

DDoS原生基础防护对其他云服务有诸多依赖关系，因此在您开启IAM系统策略授权后，在Console控制台的各项功能需要配置相应的服务权限后才能正常查看或使用，依

版权所有 © 华为技术有限公司

赖服务的权限配置均基于您已设置了IAM系统策略授权的Anti-DDoS Administrator策略权限，详细设置方法请参见**创建用户并授权使用Anti-DDoS**。

依赖服务的权限设置

如果IAM用户需要在Console控制台拥有相应功能的查看或使用权限，请确认已经对该用户所在的用户组设置了Anti-DDoS Administrator策略的集群权限，再按如下**表1-2**增加依赖服务的角色或策略。

表 1-2 Console 中依赖服务的角色或策略

控制台功能	依赖服务	需配置角色或策略
开启Anti-DDoS告警通知	消息通知服务 SMN	需要增加SMN ReadOnlyAccess的系统策略，才能获取消息通知服务的主题群组。
设置标签	标签管理服务 TMS	需要增加TMS FullAccess的系统策略，才能创建标签键。

1.3 设置流量清洗阈值拦截攻击流量

Anti-DDoS为华为云上的EIP资源自动开启DDoS攻击防护，即Anti-DDoS对华为云上购买的EIP自动开启DDoS攻击防护。

Anti-DDoS防护策略支持以下两种设置方法：

- 设置默认防护策略

  默认防护策略作为系统初始策略，对所有新购买的EIP生效，不影响存量EIP的流量清洗阈值。策略默认的“流量清洗阈值”为120Mbps，支持修改。
- 为指定EIP设置防护策略

  手动为公网IP设置特定的防护策略，支持批量操作和单个操作。手动设置了防护策略的公网IP将不再使用默认防护策略。

须知

档位选择和业务不匹配，可能导致攻击漏防或业务流量误清洗，请选择与所购买带宽最接近的数值，但不超过购买带宽。

设置默认防护策略

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“公网IP”页签，单击“设置默认防护策略”。

步骤4 根据实际设置“流量清洗阈值”，如**图1-3**所示。

版权所有 © 华为技术有限公司

图 1-3 配置默认防护策略

表 1-3 参数说明

参数	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。 **说明** • 流量清洗阈值需要根据业务带宽进行选择，与具体防御策略无关。当流量清洗阈值远低于实际业务带宽时，可能引发误告警；当流量清洗阈值远高于实际业务带宽时，可能导致攻击漏防。因此建议选择与实际业务带宽最接近的数值，但不超过购买带宽。 • 当实际业务流量触发流量清洗阈值时，Anti-DDoS仅拦截攻击流量；当实际业务流量未触发流量清洗阈值时，无论是否为攻击流量，都不会进行拦截。

步骤5 单击“确定”，完成默认防护策略的设置。

说明

默认防护策略设置完成后，新购买的公网IP均按照默认防护策略启动防护。

----结束

为指定 EIP 设置防护策略

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 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”。

版权所有 © 华为技术有限公司

图 1-4 批量设置防护策略

- 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”。

图 1-5 单个公网 IP 设置防护策略

步骤4 根据实际设置“流量清洗阈值”。

图 1-6 设置防护策略

表 1-4 参数说明

参数	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。 **说明** • 流量清洗阈值需要根据业务带宽进行选择，与具体防御策略无关。当流量清洗阈值远低于实际业务带宽时，可能引发误告警；当流量清洗阈值远高于实际业务带宽时，可能导致攻击漏防。因此建议选择与实际业务带宽最接近的数值，但不超过购买带宽。 • 当实际业务流量触发流量清洗阈值时，Anti-DDoS仅拦截攻击流量；当实际业务流量未触发流量清洗阈值时，无论是否为攻击流量，都不会进行拦截。

 版权所有 © 华为技术有限公司

步骤5 单击“确定”，完成设置。

----结束

查看 EIP 防护状态

设置了流量清洗阈值后，可以查看防护的EIP状态和防护信息。

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“公网IP”页签，查看公网IP。

图 1-7 查看公网 IP

说明

- 支持防护IPv4和IPv6环境下发起的流量攻击。
- 全部开启防护：单击“全部开启防护”，为当前区域下所有未开启防护的公网IP开启Anti-DDoS防护。
- 开启Anti-DDoS“默认防护”后，当检测到报文总流量达到120Mbps时， 触发流量清洗功能。如果需要配置Anti-DDoS的防护策略，可以修改防护参数，详细操作请参见**设置流量清洗阈值拦截攻击流量**。
- Anti-DDoS最高提供500Mbps的DDoS攻击防护。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；对于可能会遭受超过500Mbps流量攻击的应用，建议您购买华为云DDoS高防服务，提升防护能力。
- 在“所有防护状态”搜索框中选择防护状态，“公网IP”界面将只显示对应状态的公网IP。

表 1-5 参数说明

参数名称	说明
公网IP	Anti-DDoS防护的公网IP地址。 **说明** 如果公网IP已开启Anti-DDoS防护，单击公网IP，可以跳转至该公网IP的“监控报表”页面。

 版权所有 © 华为技术有限公司

参数名称	说明
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	防护对象的类型。 • EIP：弹性公网IP。 • ELB：弹性负载均衡。 • NetInterFace • VPN：虚拟专用网络。 • NAT：NAT网关。 • VIP：高可用虚拟IP。 • CCI：云容器实例。 • SubEni
防护设置	当前公网IP的流量清洗阈值。
企业项目	当前公网IP所属的企业项目。

----结束

1.4 设置告警通知实现 DDoS 攻击预警

为Anti-DDoS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）。否则，无论DDoS攻击流量多大，用户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

已创建消息通知主题，具体操作，请参见《消息通知服务用户指南》。

开启 Anti-DDoS 告警通知

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“告警通知”页签，设置告警通知，相关参数说明如表1-6所示。

版权所有 © 华为技术有限公司

图 1-8 设置告警通知

表 1-6 设置告警通知

参数名称	说明
清洗流量告警阈值	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	开启或关闭告警通知，说明如下： •  ：开启状态。 •  ：关闭状态。
消息通知主题	可以选择使用已有的主题，或者单击“查看消息通知主题”创建新的主题。 更多关于主题的信息，请参见**《消息通知服务用户指南》**。

步骤4 单击“应用”，开启告警通知。

----结束

1.5 开启 DDoS 事件告警通知

通过云监控服务，对防护的EIP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。

开启事件告警通知

步骤1 **登录管理控制台**。

 版权所有 © 华为技术有限公司

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的 ，选择“管理与监管 > 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1-7配置告警参数。

图 1-9 告警参数

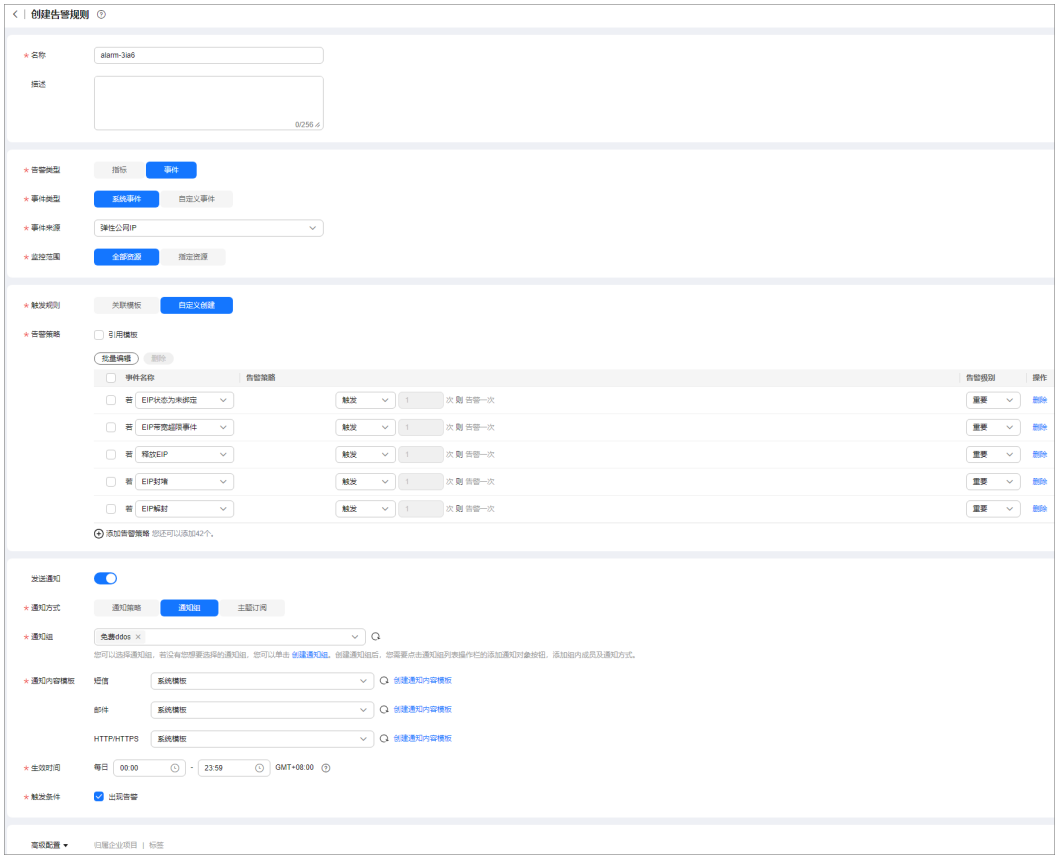


表 1-7 参数说明

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”。

 版权所有 © 华为技术有限公司

参数	说明
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	默认为“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”。 当流量大于10000kps时，系统会在开始清洗和结束清洗各发送一次告警通知；流量小于10000kps不会发送告警通知。
通知方式	根据实际选择进行配置。 **说明** 告警消息由消息通知服务SMN发送，可能产生少量费用。

步骤7 单击“立即创建”，在弹出的窗口中单击“确定”，告警通知创建成功。

----结束

1.6 开启日志记录

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

已创建LTS日志组和日志流，具体操作请参考**管理日志组**和**管理日志流**。

开启 LTS 日志

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“日志”页签，开启日志  ，并选择日志组和日志流，相关参数说明如**表1-8**所示。

版权所有 © 华为技术有限公司

图 1-10 配置日志

表 1-8 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，包括攻击类型、防护的IP等信息。

步骤4 单击“确定”，日志配置成功。

您可以在LTS管理控制台查看Anti-DDoS的防护日志。

----结束

日志字段说明

本章节介绍了AntiDDoS日志包含的日志字段。

表 1-9 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）。

 版权所有 © 华为技术有限公司

字段	说明
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1-10**。
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 1-10 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
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

版权所有 © 华为技术有限公司

数值	攻击类型
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
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

版权所有 © 华为技术有限公司

数值	攻击类型
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

1.7 为 EIP 添加标签

标签由标签键和标签值组成，用于标识云资源。当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。DDoS原生基础防护支持为防护的公网IP配置标签，方便管理。

设置标签

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 单击“公网IP”页签。

步骤4 在需要设置标签的公网IP所在行，单击“设置标签”。

图 1-11 设置标签

步骤5 在标签添加页面，单击“添加标签”。

步骤6 选择“标签键”和“标签值”。

版权所有 © 华为技术有限公司

- 手动设置标签：手动输入标签键和标签值。
- 选择已有标签：选择已有的标签。

图 1-12 添加标签

说明

如您的组织已经设定本服务的相关标签策略，则需按照标签策略规则为资源添加标签。标签如果不符合标签策略的规则，则可能会导致标签添加失败，请联系组织管理员了解标签策略详情。

步骤7 单击“确定”。

----结束

1.8 查看 EIP 监控报表

用户可以通过Anti-DDoS控制台查看指定EIP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。

查看监控报表

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“公网IP”页签，在待查看监控报表的公网IP地址所在行，单击“查看监控报表”。

图 1-13 查看监控报表

 版权所有 © 华为技术有限公司

步骤4 在“监控报表”页面，可以查看该公网IP报表的详细指标，如图1-14和图1-15所示。

- 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5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。

图 1-14 查看流量监控报表

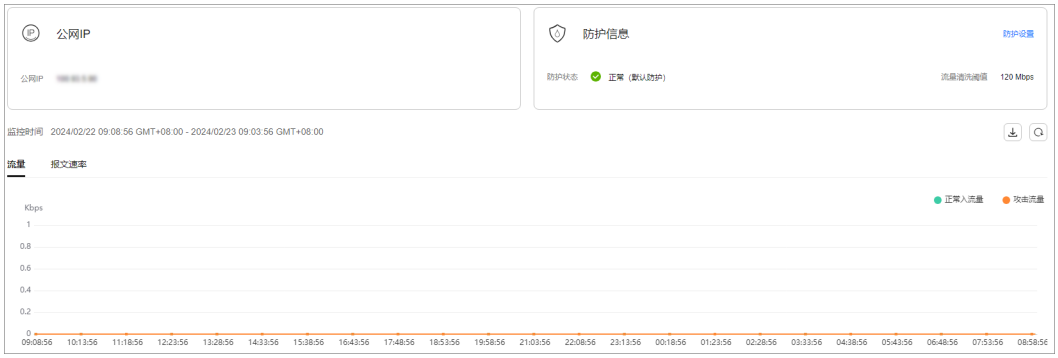
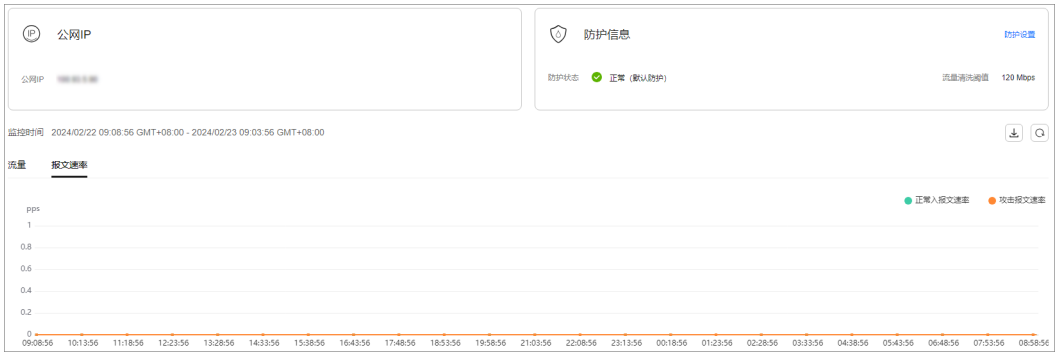


图 1-15 查看报文速率



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

1.9 查看拦截报告

Anti-DDoS控制台按周生成拦截报告，用户可以查看EIP的防护统计信息，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10和共拦截攻击次数。

 版权所有 © 华为技术有限公司

查看 Anti-DDoS 拦截报告

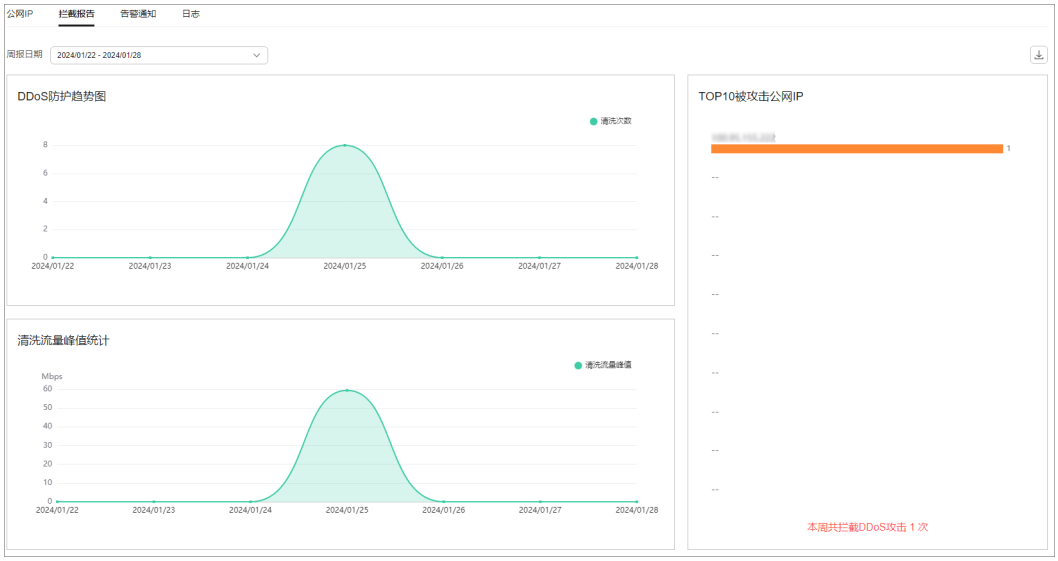
步骤1 登录管理控制台。

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

步骤3 选择“拦截报告”页签，可以查看用户所有公网IP地址的防护统计信息，如图1-16所示。

可通过选择“周报日期”来查看固定日期内的安全报告，查看时间范围为一周，支持查询前四周统计数据，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10和共拦截攻击次数。

图 1-16 查看拦截报告



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

1.10 查询审计日志

1.10.1 云审计服务支持的 Anti-DDoS 操作

云审计服务（Cloud Trace Service，CTS）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1-11所示。

版权所有 © 华为技术有限公司

表 1-11 CTS 支持的 Anti-DDoS 操作列表

操作名称	事件名称
修改Anti-DDoS防护配置	UPDATE_ANTIDDOS
设置LTS全量日志配置	UPDATE_LTS_CONFIG
批量添加/编辑TMS资源标签	UPDATE_RESOURCE_TAGS
批量删除TMS资源标签	DELETE_RESOURCE_TAGS
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
查询任务列表	QUERY_TASK_LIST
查询告警配置详情	QUERY_ALERT_CONFIG
查询IP的防护配置	QUERY_IP_DEFENSE_POLICY
查询Anti-DDoS防护配置列表	QUERY_DEFENSE_POLICY_LIST
查询IP的防护状态	QUERY_IP_DEFENSE_STATUS
批量查询IP的防护状态	QUERY_IP_LIST_DEFENSE_STATUS
查询IP的日流量详情	QUERY_IP_DAILY_TRAFFIC_REPORT
导出IP的日流量详情	EXPORT_IP_DAILY_TRAFFIC_REPORT
查询IP的日异常事件列表	QUERY_IP_DAILY_EVENT_REPORT
查询IP的周防护统计情况	QUERY_IP_WEEKLY_REPORT
导出IP的周防护统计情况	EXPORT_IP_WEEKLY_REPORT
查询配置状态	QUERY_CONFIG_STATUS
查询信誉信息	QUERY_CREDIT_INFO
查询流量清洗阈值默认档位	QUERY_DEFAULT_CONFIG
查询配额	QUERY_QUOTA
查询全量日志配置	QUERY_LOG_CONFIG
查询资源实例	QUERY_TMS_RESOURCE_INSTANCE
查询资源实例个数	QUERY_TMS_RESOURCE_COUNT
查询IP的资源标签	QUERY_IP_RESOURCE_TAG
查询资源标签列表	QUERY_RESOURCE_TAG_LIST

版权所有 © 华为技术有限公司

1.10.2 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。

用户可以通过云审计服务查看历史Anti-DDoS的操作记录。

前提条件

已开通云审计服务，具体操作请参考**开通云审计服务**。

查看 Anti-DDoS 审计日志

步骤1 **登录管理控制台**。

步骤2 单击页面左侧的 ☰，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 在下拉框中选择“云服务”，输入“Anti-DDoS”，按“Enter”。

步骤5 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

版权所有 © 华为技术有限公司

2 DDoS 原生高级防护操作指南

2.1 DDoS 原生高级防护概述

EIP接入DDoS原生高级防护进行防护的流程如所示。

图 2-1 接入流程

表 2-1 流程说明

序号	流程	说明
1	**通过IAM授予使用DDoS原生高级防护的权限**	通过统一身份认证服务（Identity and Access Management，简称IAM）为用户授予精细的DDoS原生高级防护服务权限。
2	**购买实例**	根据业务需求购买DDoS原生高级防护实例。
3	**添加防护策略**	DDoS原生高级防护提供了丰富全面的防护规则，您可以根据业务需求配置相应的防护策略。
4	**添加防护对象**	将需要防护的EIP添加到DDoS原生高级防护实例。

版权所有 © 华为技术有限公司

序号	流程	说明
5	常用安全操作	• **开启DDoS攻击告警通知**：开启告警通知后，当EIP遭受DDoS攻击时，您可以第一时间接收告警通知。 • **开启日志记录**：通过LTS记录的日志数据，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。 • **查看数据报表**：可查看指定时间范围内的访问与攻击统计次数等信息。 • **实例管理**：开通续费、升级规格、配置标签等常用实例管理操作。 • **防护对象管理**：查看防护对象信息、移除防护对象等。 • **查看监控指标**：通过云监控服务，对防护的EIP启用事件和指标监控。 • **查询审计日志**：通过云审计服务查看DDoS原生高级防护的历史操作记录。

2.2 通过 IAM 授予使用 DDoS 原生高级防护的权限

2.2.1 创建用户并授权使用 CNAD

如果您需要对您所拥有的CNAD进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

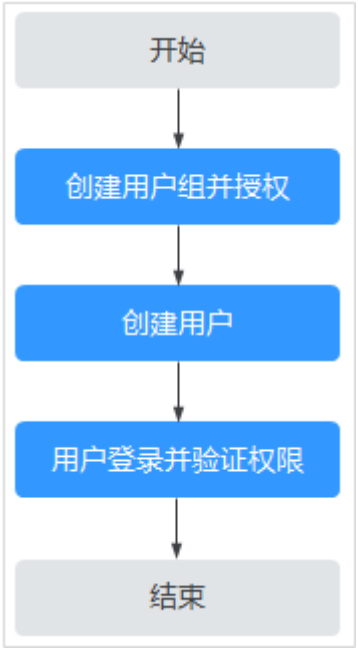
- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用CNAD资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将CNAD资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用CNAD服务的其它功能。

版权所有 © 华为技术有限公司

示例流程

图 2-2 给用户授权服务权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予DDoS原生高级防护权限“CNAD FullAccess”。

2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

   在页面左上方的 ☰，选择除DDoS原生高级防护外（假设当前策略仅包含“CNAD FullAccess”）的任一服务，如果提示权限不足，表示“CNAD FullAccess”已生效。

2.2.2 CNAD 自定义策略

如果系统预置的CNAD权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见**CNAD权限及授权项**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的CNAD自定义策略样例。

版权所有 © 华为技术有限公司

CNAD 自定义策略样例

- 示例1：授权用户查询防护IP列表

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cnad:protectedIpDropList:list"
                        ]
        }
    ]
}
```

- 示例2：拒绝用户删除IP黑白名单规则

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予“CNAD FullAccess”的系统策略，但不希望用户拥有“CNAD FullAccess”中定义的删除IP黑白名单规则的权限（cnad:blackWhiteIpList:delete），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为“Deny”，然后同时将“CNAD FullAccess”和拒绝策略授予用户，根据Deny优先原则用户可以对CNAD执行除了删除IP黑白名单规则的所有操作。以下策略样例表示：拒绝用户删除IP黑白名单规则。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "cnad:blackWhiteIpList:delete"
            ]
        },
    ]
}
```

2.2.3 CNAD 权限及授权项

如果您需要对您所拥有的CNAD进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用CNAD的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

版权所有 © 华为技术有限公司

权限	授权项	依赖关系说明
查询配额	cnad:quota:get	-
查询单个防护策略详情	cnad:policy:get	-
查询统计数据	cnad:countReport:get	-
查询资产安全状态	cnad:securityStatusReport:get	-
查询每周安全统计数据	cnad:weekStatisticsReport:get	-
创建告警通知	cnad:alarmConfig:create	如果授予用户告警通知权限，需要同时授予用户“cnad:alarmConfig:create”授权项和“中国-香港”的“SMN Administrator”权限。
删除告警通知	cnad:alarmConfig:delete	如果授予用户告警通知权限，需要同时授予用户“cnad:alarmConfig:delete”授权项和“中国-香港”的“SMN Administrator”权限。
查询告警通知	cnad:alarmConfig:get	如果授予用户告警通知权限，需要同时授予用户“cnad:alarmConfig:get”授权项和“中国-香港”的“SMN Administrator”权限。
更新实例	cnad:package:put	-

版权所有 © 华为技术有限公司

权限	授权项	依赖关系说明
绑定防护IP到实例	cnad:protectedIp:create	如果授予用户为CNAD实例绑定对象的权限，需要同时授予用户“cnad:protectedIp:create”授权项和实例所属区域的“vpc:publicIps:list”（查询弹性公网IP）授权项。 例如，用户在“中国-香港”购买了一个CNAD实例。如果授予用户为CNAD实例绑定对象的权限，则需要授予该用户“cnad:protectedIp:create”授权项和“中国-香港”的“vpc:publicIps:list”授权项，使该用户只能操作“中国-香港”实例上绑定的防护对象。
创建防护策略	cnad:policy:create	-
更新防护策略	cnad:policy:put	-
删除防护策略	cnad:policy:delete	-
绑定防护策略到防护IP	cnad:bindPolicy:create	-
移除防护IP的防护策略	cnad:unbindPolicy:create	-
创建IP黑白名单	cnad:blackWhiteIpList:create	-
删除IP黑白名单	cnad:blackWhiteIpList:delete	-
更新防护IP标签	cnad:ipTag:put	-
查询清洗范围	cnad:cleanScaleDropList:list	-
查询实例列表	cnad:packageDropList:list	-
查询防护策略列表	cnad:policyDropList:list	-
查询防护IP列表	cnad:protectedIpDropList:list	-
查询实例详情	cnad:package:list	-
查询防护策略详情	cnad:policy:list	-
查询防护IP列表	cnad:protectedIp:list	-
查询总流量数据	cnad:trafficTotalReport:list	-

版权所有 © 华为技术有限公司

权限	授权项	依赖关系说明
查询攻击流量	cnad:trafficAttackReport:list	-
查询总数据包	cnad:packetTotalReport:list	-
查询攻击数据包	cnad:packetAttackReport:list	-
查询DDoS防护趋势	cnad:cleanCountReport:list	-
查询清洗流量峰值统计数据	cnad:cleanKbpsReport:list	-
查询攻击类型分布	cnad:attackTypeReport:list	-
查询攻击事件	cnad:attackReport:list	-
查询Top10被攻击IP	cnad:attackTop:list	-
创建实例	cnad:package:create	如果授予用户购买CNAD权限，需要同时授予用户“cnad:package:create”授权项和所有区域以下BSS授权项： • bss:order:update 操作订单权限 • bss:contract:update 修改合同商务 • bss:balance:view 查看账户 • bss:order:pay 支付权限

2.2.4 控制台的权限依赖

DDoS原生高级防护对其他云服务有诸多依赖关系，因此在您开启IAM系统策略授权后，在Console控制台的各项功能需要配置相应的服务权限后才能正常查看或使用，依赖服务的权限配置均基于您已设置了IAM系统策略授权的CNAD FullAccess或CNAD ReadOnlyAccess策略权限，详细设置方法请参见**创建用户并授权使用CNAD**。

依赖服务的权限设置

如果IAM用户需要在Console控制台拥有相应功能的查看或使用权限，请确认已经对该用户所在的用户组设置了CNAD FullAccess或CNAD ReadOnlyAccess策略的集群权限，再按如下**表2-2**增加依赖服务的角色或策略。

版权所有 © 华为技术有限公司

表 2-2 Console 中依赖服务的角色或策略

控制台功能	依赖服务	需配置角色或策略
开启LTS日志	云日志服务 LTS	需要增加LTS ReadOnlyAccess的系统策略，才能选择在云日志服务中创建的日志组和日志流名称。
开启告警通知	消息通知服务 SMN	需要增加SMN ReadOnlyAccess的系统策略，才能获取消息通知服务的主题群组。
配置实例标签	标签管理服务 TMS	需要增加TMS FullAccess的系统策略，才能创建标签键。
购买实例	企业项目管理服务 EPS	需要增加EPS ReadOnlyAccess的系统策略后，才能在购买实例时选择该企业项目。

2.3 购买实例

在使用DDoS原生高级防护前，您需要购买DDoS原生高级防护实例。

有关DDoS原生高级防护各版本详细的功能规格介绍，请参见表2-3，请您根据业务需求购买对应版本。

表 2-3 各版本支持的规格

项目	全力防基础版	全力防高级版	原生防护2.0
计费类型	包年包月	包年包月	• 实例为包年包月计费。 • 业务带宽支持包年包月和按需计费。
防护对象	华为云EIP	DDoS防护专属EIP	• 中国大陆：全动态BGP EIP、DDoS防护专属EIP • 中国大陆外：优选BGP EIP、DDoS防护专属EIP
防护区域	单区域防护	单区域防护	• 中国大陆：支持多区域防护。 • 中国大陆外：当前仅支持香港、新加坡。
支持协议	IPv4、IPv6	IPv4	IPv4、IPv6
对象数量	50-500个	50-500个	50-1000个
业务带宽	100Mbps-20Gbps	100Mbps-20Gbps	100Mbps-20Gbps

版权所有 © 华为技术有限公司

项目	全力防基础版	全力防高级版	原生防护2.0
防护能力	共享全力防护，不低于20G，最高可达数百G。	共享全力防护，最高可达1T。	• 中国大陆：共享全力防护，不低于20G。 • 中国大陆外：运营商跨境防护。

说明

- 使用DDoS防护专属EIP的场景下，如果出现网络波动等极端场景，流量可能会调度到防护能力较小的备用机房，导致防护能力降低。
- 优选BGP EIP加入原生防护2.0后，新增支持防护来自国内的攻击，仍不支持防护来自海外的攻击。优选BGP EIP海外攻击的黑洞阈值较低，当海外攻击超过黑洞阈值时，优选BGP EIP将会被封堵。如需防护海外攻击，请购买DDoS防护专属EIP搭配原生防护2.0使用。

前提条件

- 账号需要拥有“CNAD FullAccess”和“BSS Administrator”角色权限。
- 购买DDoS原生防护前，已成功申请开通服务版本。

说明

进入“购买DDoS防护”界面，“实例类型”选择“DDoS原生防护”后，在界面右下角单击“立即申请”，按界面提示信息，申请开通。

购买 DDoS 原生高级防护实例

您可以根据业务需求购买不同版本的实例。

购买原生防护 2.0

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“安全与合规 > DDoS防护AAD”，进入“Anti-DDoS流量清洗”界面。

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 根据实际选择防护区域。

注意

中国大陆外区域的原生防护2.0只能防护49.0.236.0/22、49.0.234.0/23和49.0.233.0/24的优选BGP IP。

步骤6 “防护规格”选择“原生防护2.0”。

步骤7 设置规格参数，相关参数说明如表2-4所示。

版权所有 © 华为技术有限公司

图 2-3 原生防护 2.0

表 2-4 参数说明

参数	说明
防护IP数	取值范围为50～1000，且防护IP数必须设置为50的倍数。

版权所有 © 华为技术有限公司

参数	说明
公网线路计费模式	根据实际选择。 • 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。只有中国大陆才支持该模式。 • 按需计费：按照每天实际产生的干净流量计费。
业务带宽	“公网线路计费模式”选择“包年包月”才有该参数。
计量规则	“公网线路计费模式”选择“按需计费”才有该参数。 干净流量是指未被污染的正常业务流量，不包含攻击流量。

步骤8 设置“实例名称”，选择“购买时长”和“购买数量”后，在界面右下角单击“立即购买”。

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤9 在“订单详情”页面，如果您确认订单无误，单击“去支付”。

步骤10 在“购买DDoS防护”的支付界面，单击“确认付款”，完成订单支付。

付款成功后，系统跳转至DDoS防护实例列表界面。当实例状态为“正常”时，说明实例创建成功。

步骤11 （可选）请参考**申请弹性公网IP**在所需的区域购买DDoS防护专属EIP。

说明

- 相对于普通EIP，DDoS防护专属EIP是在DDoS清洗中心进行攻击防御，具备T级带宽，防护能力特别强。
- 如果您需要申请DDoS防护专属EIP，请参考此步骤购买。
- 以下区域线路名称仅供参考，实际以控制台为准。

表 2-5 专属 EIP 线路

区域	DDoS防护专属EIP线路名称
华南-广州	5_ddosalways1bgp
华北-北京二	5_DDoSAlways1bgp
华北-北京四	5_DDoSAlways1bgp
华东-上海一	5_ddosalways1bgp
华东-上海二	5_DDoSAlways1bgp
中国-香港	5_DDoSAlways2bgp
亚太-新加坡	5_DDoSAlways1bgp

----结束

版权所有 © 华为技术有限公司

购买全力防基础版

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

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 “防护区域”选择“中国大陆”。

步骤6 “防护规格”选择“全力防基础版”。

步骤7 设置规格参数，如图2-4所示，相关参数说明如表2-6所示。

版权所有 © 华为技术有限公司

图 2-4 设置 DDoS 原生防护-全力防基础版防护规格

表 2-6 全力防基础版参数说明

参数	说明
防护区域	全力防基础版当前只支持中国大陆区域。
资源所在地	选择防护资源所在的区域。 **须知** DDoS原生防护实例只能防护相同区域的云资源，不能跨Region防护。例如，华东-上海一的云原生防护实例只能防护华东一上海一的云资源。

版权所有 © 华为技术有限公司

参数	说明
防护IP数	取值范围为50～500，且防护IP数必须设置为5的倍数。
业务带宽	业务带宽是高防机房清洗后回源给源站的业务流量带宽。

步骤8 设置“实例名称”，选择“购买时长”和“购买数量”后，在界面右下角单击“立即购买”。

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤9 在“订单详情”页面，如果您确认订单无误，单击“去支付”。

步骤10 在“购买DDoS防护”的支付界面，单击“确认付款”，完成订单支付。

付款成功后，系统跳转至DDoS防护实例列表界面。当实例状态为“正常”时，说明实例创建成功。

----结束

购买全力防高级版

说明

购买DDoS原生防护-全力防高级版前请确认已知晓全力防高级版只能防护专属EIP。

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

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 根据实际选择防护区域。

步骤6 “防护规格”选择“全力防高级版”。

步骤7 设置规格参数，相关参数说明如表2-7所示。

版权所有 © 华为技术有限公司

图 2-5 设置 DDoS 原生防护-全力防高级版防护规格

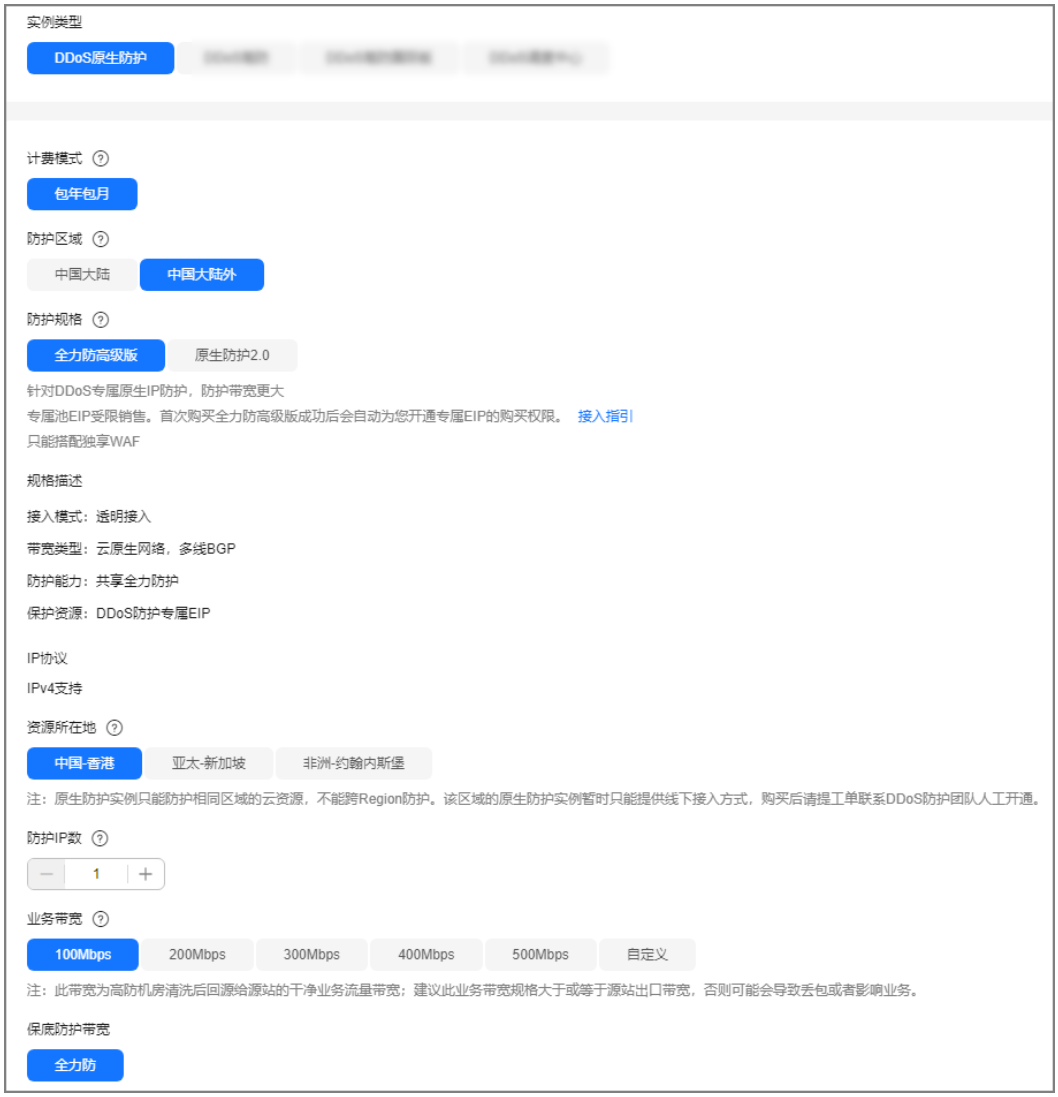


表 2-7 全力防高级版参数说明

参数	说明
防护区域	• 中国大陆：适用于业务服务器部署在中国大陆的场景，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的场景，仅支持优选BGP EIP。
资源所在地	选择防护资源所在的区域。 **须知** DDoS原生防护实例只能防护相同区域的云资源，不能跨Region防护。例如，华东-上海一的云原生防护实例只能防护华东一上海一的云资源。
防护IP数	取值范围为50～500，且防护IP数必须设置为5的倍数。

版权所有 © 华为技术有限公司

参数	说明
业务带宽	业务带宽是高防机房清洗后回源给源站的业务流量带宽。 取值范围：100M~40,000M

步骤8 设置“实例名称”，选择“购买时长”和“购买数量”后，在界面右下角单击“立即购买”。

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤9 在“订单详情”页面，如果您确认订单无误，单击“去支付”。

步骤10 在“购买DDoS防护”的支付界面，单击“确认付款”，完成订单支付。

付款成功后，系统跳转至DDoS防护实例列表界面。当实例状态为“正常”时，说明实例创建成功。

步骤11 请参考**申请弹性公网IP**在所需的区域购买DDoS防护专属EIP。

表 2-8 专属 EIP 线路

区域	DDoS防护专属EIP线路名称
华南-广州	5_ddosalways1bgp
华北-北京二	5_DDoSAlways1bgp
华北-北京四	5_DDoSAlways1bgp
华东-上海一	5_ddosalways1bgp
华东-上海二	5_DDoSAlways1bgp
中国-香港	5_DDoSAlways2bgp
亚太-新加坡	5_DDoSAlways1bgp

说明

以上区域线路名称仅供参考，实际以控制台为准。

----结束

2.4 添加防护策略

2.4.1 防护策略概述

DDoS原生高级防护提供了丰富的防护策略，购买实例后，您可以根据业务需要选择适合的防护策略，如**表2-9**所示。

版权所有 © 华为技术有限公司

须知

防护策略设置错误可能导致攻击漏防或流量误清洗，请根据业务实际谨慎操作。

表 2-9 防护策略

防护策略	章节	说明
基础防护	**设置基础防护策略拦截攻击流量**	为防护对象设置基础防护策略，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，保障业务可用。
IP黑白名单	**通过黑白名单拦截/放行指定IP的流量**	通过配置IP黑名单或IP白名单来封禁或者放行访问DDoS防护的源IP，从而限制访问您业务资源的用户。
指纹过滤	**通过指纹特征设置流量处理策略**	通过配置指纹过滤防护规则，对数据包中指定位置的内容进行特征匹配，根据匹配结果设置处理动作，比如丢弃、通过、限速等。
端口封禁	**封禁指定端口的流量**	当某个目的端口不需要被访问时，为降低DDoS攻击风险，您可以通过端口封禁策略，阻止流量对该端口的访问。
协议封禁	**封禁指定协议的流量**	根据协议类型一键封禁访问DDoS防护对象的源流量，支持封禁UDP/TCP/ICMP等协议。
水印防护	**通过水印防护抵御CC攻击**	通过在业务端共享水印算法和关键字，客户端发出的报文都镶嵌入水印特征，能有效抵御四层CC攻击。
高级防护	**通过高级防护策略限制异常连接**	如果同一个源站IP短时间内频繁发起大量异常连接状态的报文时，您可以通过配置高级防护策略，将该源站IP纳入黑名单中进行封禁惩罚，等封禁结束后可恢复访问。
区域封禁	**封禁指定区域的流量**	DDoS原生高级防护支持封禁指定区域的流量，策略生效后，来自该区域的访问流量将被丢弃。

2.4.2 设置基础防护策略拦截攻击流量

业务接入DDoS原生高级防护后，您可以为防护对象设置基础防护策略。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，保障您的业务可用。

须知

档位选择和业务不匹配，可能导致攻击漏防或业务流量误清洗，请选择与所购买带宽最接近的数值，但不超过购买带宽。

版权所有 © 华为技术有限公司

约束与限制

已有定制策略的用户无法直接修改流量清洗档位，需要**提交工单**联系华为技术支持修改。

开启基础防护

步骤1 **登录管理控制台**。

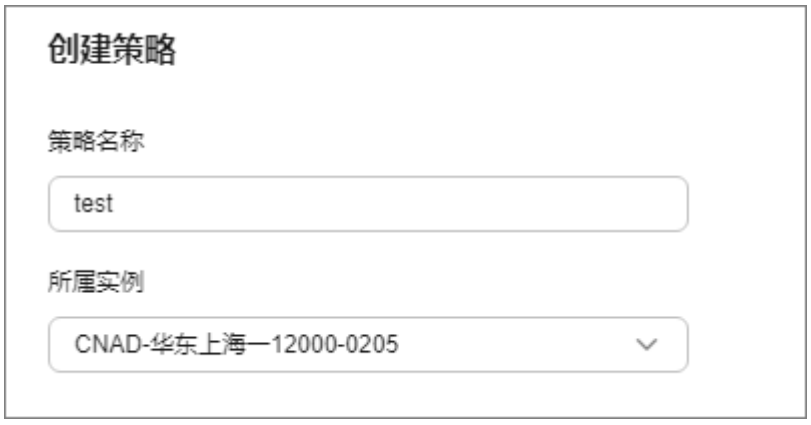
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 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4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

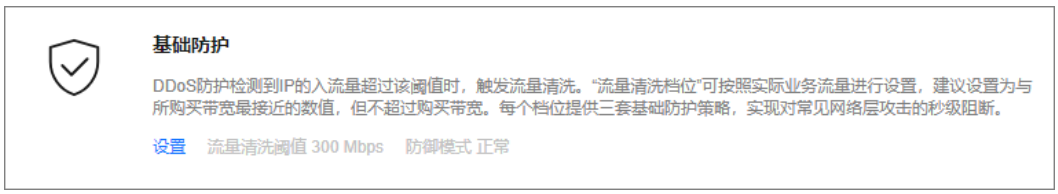
图 2-6 创建策略



步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“基础防护”配置框中，单击“设置”。

图 2-7 基础防护



步骤8 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。

版权所有 © 华为技术有限公司

图 2-8 基础防护设置

表 2-10 参数说明

参数	说明
流量清洗档位	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。 **说明** 流量清洗阈值需要根据业务带宽进行选择，与具体防御策略无关。当流量清洗阈值远低于实际业务带宽时，可能引发误告警；当流量清洗阈值远高于实际业务带宽时，可能导致攻击漏防。因此建议选择与实际业务带宽最接近的数值，但不超过购买带宽。
防御模式	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，出现流量误清洗时建议使用该模式缓解对业务的影响。 • 正常：流量达到清洗档位的2倍后触发清洗，默认防御策略推荐该模式。 • 严格：流量达到清洗档位就触发流量清洗，出现攻击漏防时建议使用该模式加强防御。

步骤9 单击“确定”，完成基础防护策略配置。

----结束

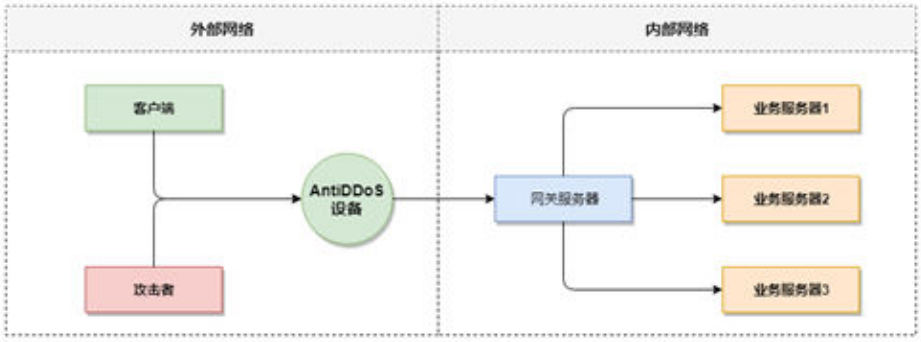
2.4.3 通过水印防护抵御 CC 攻击

通过在业务端共享水印算法和关键字，客户端发出的报文都镶嵌入水印特征，能有效抵御四层CC攻击。

通常UDP Flood的防御方式有两种，一种是动态指纹学习，一种是UDP限流，前者可能会将正常的业务载荷学习成攻击指纹，容易造成误杀，后者会将正常流量和攻击流量一起进行阻断，影响您的正常业务使用。

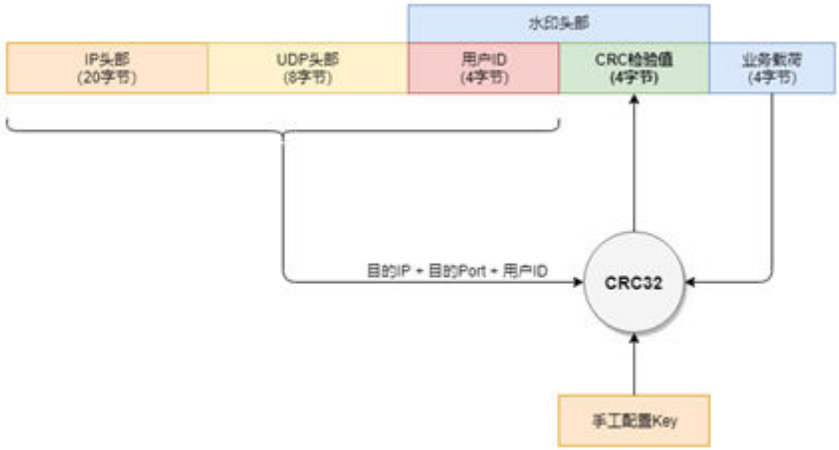
版权所有 © 华为技术有限公司

图 2-9 设备防护原理图



如图2-10所示，华为云解决方案通过在UDP报文中增加水印头部信息，用以标识正常的业务报文，线下DDoS防护设备在接收到UDP报文后，通过检查UDP水印的正确性，可以高效准确放行正常的业务报文，阻断攻击报文。

图 2-10 水印解决方案



客户端和DDoS防护设备需要使用相同的信息结构和计算规则，其中计算规则是指计算水印值的哈希因子和哈希算法，在本方案中，哈希因子使用了目的IP、目的端口、用户标识和水印关键字，哈希算法使用CRC32。

约束与限制

- 该功能需要客户端同步开发，如果需要使用，请提交工单申请开通。
- 一个水印最多可以配置两条关键字。

开启水印防护

您可以通过控制台设置水印防护策略，并在客户端配置水印。

设置水印防护策略

步骤1 登录管理控制台。

 版权所有 © 华为技术有限公司

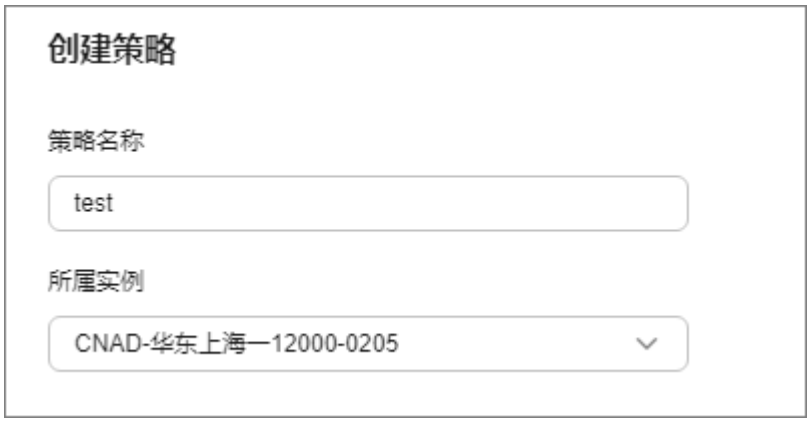
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 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4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

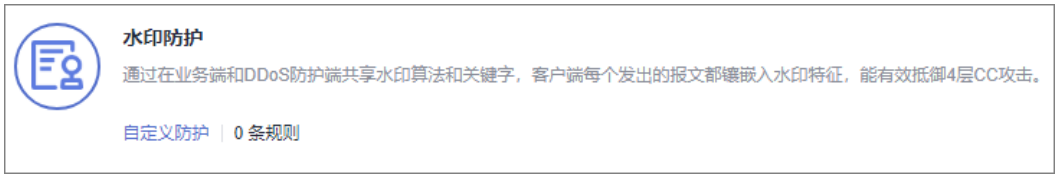
图 2-11 创建策略



步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“水印防护”配置框中，单击“自定义防护”。

图 2-12 水印防护配置框



步骤8 在弹出的“水印防护设置”页面中，单击“新建水印”。

步骤9 在“新建水印”对话框中，设置水印参数。

版权所有 © 华为技术有限公司

图 2-13 新建水印

表 2-11 水印参数说明

参数	说明
水印名称	输入水印名称。
协议	当前仅支持UDP协议。
关键字	输入关键字，最多可输入两个关键字。
端口范围	支持的端口范围为1~65535。

步骤10 单击“确定”，水印添加成功。

----结束

在客户端配置水印

本节主要以C语言进行示例，指导**客户端开发人员**如何在客户端实现UDP水印的计算和添加，开发人员可以根据实现开发平台进行代码调整。

步骤1 初始化CRC表：

```
unsigned int g_szCRCTable[256];
void CRC32TableInit(void)
{
    unsigned int c;
    int n, k;
    for (n = 0; n < 256; n++) {
        c = (unsigned int)n;
        for (k = 0; k < 8; k++) {
            if (c & 1) {
                c = 0xedb88320 ^ (c >> 1);
            }
            else {
```

 版权所有 © 华为技术有限公司

```
            c = c >> 1;
        }
    }
    g_szCRCTable[n] = c;
  }
}
```

步骤2 计算CRC哈希值的接口，其中第一个参数crc默认使用0即可。

```
unsigned int CRC32Hash(unsigned int crc, unsigned char* buf, int len)
{
  unsigned int c = crc ^ 0xFFFFFFFF;
  int n;
  for (n = 0; n < len; n++) {
    c = g_szCRCTable[(c ^ buf[n]) & 0xFF] ^ (c >> 8);
  }
  return c ^ 0xFFFFFFFF;
}
```

步骤3 计算报文的水印值示例代码。计算水印信息结构如图2-14所示。

图 2-14 计算水印信息结构图

- 水印数据结构定义如下代码所示：

  注意

  - 字节序需要使用网络序。
  - 业务载荷不满4字节的，使用0进行填充。

```
typedef struct {
    unsigned int   userId;    /* 用户标识ID */
    unsigned int   payload;   /* 业务载荷 */
    unsigned short destPort;  /* 业务目的端口 */
    unsigned short rsv;       /* 保留字段，2字节填充 */
    unsigned int   destIp;    /* 业务目的IP */
    unsigned int   key;       /* 水印关键字 */
} UdpWatermarkInfo;
```

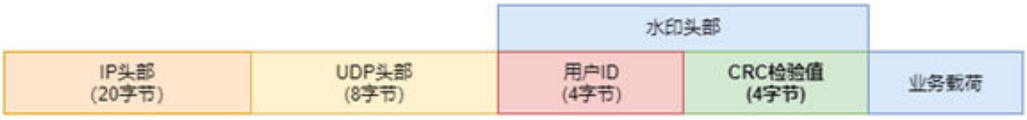
- 计算CRC哈希值可以使用CPU硬件加速接口进行替换，以提升处理性能。

```
unsigned int UdpFloodWatermarkHashGet(unsigned int userId, unsigned int payload, unsigned short
destPort, unsigned int destIp, unsigned int key)
{
    UdpWatermarkInfo stWaterInfo;

    stWaterInfo.destIp   = destIp;
    stWaterInfo.destPort = destPort;
    stWaterInfo.userId   = userId;
    stWaterInfo.payload  = payload;
    stWaterInfo.key      = key;
    stWaterInfo.rsv      = 0;

    return CRC32Hash(0, (UCHAR *)&stWaterInfo, sizeof(stWaterInfo));
}
```

步骤4 将计算出的CRC哈希值，按图2-15结构填充到报文中，然后发送出去。

版权所有 © 华为技术有限公司

图 2-15 填充报文 UDP 水印



----结束

2.4.4 通过黑白名单拦截/放行指定 IP 的流量

通过配置IP黑名单或IP白名单来封禁或者放行访问DDoS防护的源IP，从而限制访问您业务资源的用户。

约束与限制

每条规则最多可以添加200条黑/白名单IP。

添加 IP 到黑白名单

步骤1 登录管理控制台。

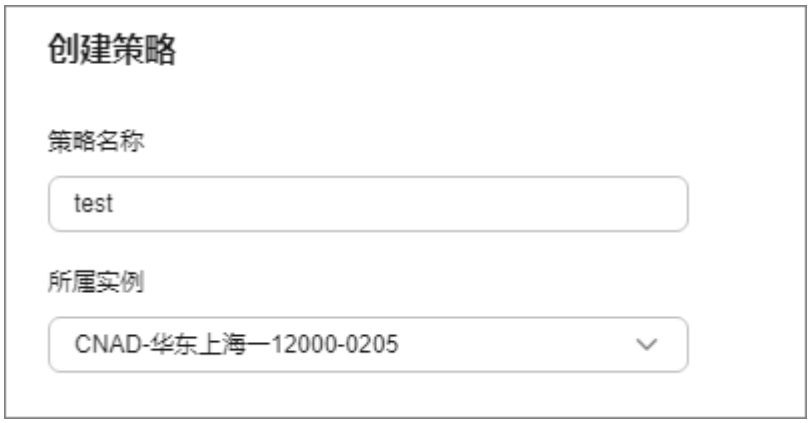
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 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4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-16 创建策略



步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“IP黑白名单”配置框中，单击“自定义防护”，如图2-17所示。

版权所有 © 华为技术有限公司

图 2-17 IP 黑白名单配置框

步骤8 在弹出的“IP黑白名单设置”页面中，选择“黑名单”或“白名单”页签后，单击“添加”。

图 2-18 添加 IP

步骤9 在弹出的对话框中，输入黑名单IP/IP段（需要拦截的IP）或白名单IP/IP段（需要放行的IP）后，单击“确定”，如图2-19和图2-20所示。

图 2-19 添加黑名单 IP

版权所有 © 华为技术有限公司

图 2-20 添加白名单 IP

----结束

相关操作

- 选择“黑名单”页签，单击操作列的“删除”或批量勾选要删除的黑名单，在列表左上方单击“删除”，被删除的黑名单IP，设备将不再拦截其访问流量。
- 选择“白名单”页签，单击操作列的“删除”或批量勾选要删除的白名单，在列表左上方单击“删除”，被删除的白名单IP，设备将不再直接放行其访问流量。

2.4.5 封禁指定端口的流量

当某个目的端口不需要被访问时，为降低DDoS攻击风险，您可以通过端口封禁策略，阻止流量对该端口的访问。

开启端口封禁

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

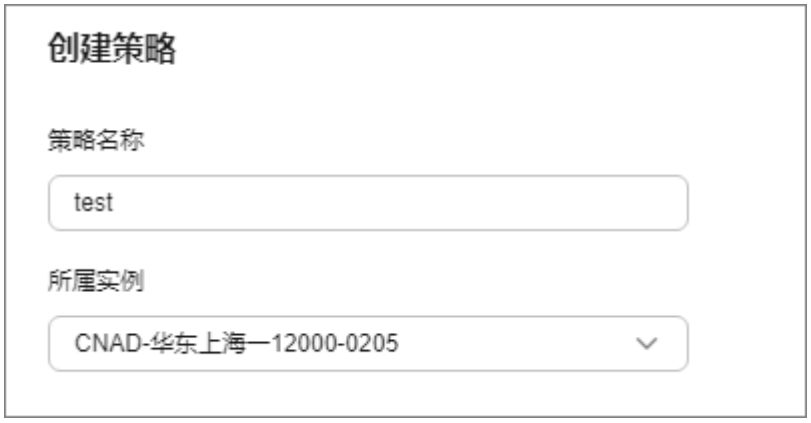
步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

版权所有 © 华为技术有限公司

图 2-21 创建策略



步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“端口封禁”配置框中，单击“自定义防护”。

图 2-22 端口封禁配置框

步骤8 在弹出的“端口封禁设置”对话框中，单击“新建端口ACL”。

步骤9 在弹出的对话框中，设置端口ACL。

版权所有 © 华为技术有限公司

图 2-23 新建端口 ACL

表 2-12 端口 ACL 参数说明

参数	说明
端口规则名称	输入规则名称。
协议	设置封禁端口的协议。支持TCP、UDP。
端口类型	只支持“目的端口”。
开始端口-结束端口	设置封禁端口的范围。
匹配后动作值	封禁端口匹配后的防护动作。 “丢弃”：丢弃访问该端口的流量。

步骤10 单击“确定”。

----结束

后续处理

- 在目标端口所在行“操作”列，单击“删除”可以删除封禁端口规则。
- 在目标端口所在行“操作”列，单击“编辑”可以修改封禁端口规则信息。

2.4.6 封禁指定协议的流量

开启协议封禁后，系统将根据协议类型对访问DDoS防护对象的流量进行限速，支持UDP/TCP/ICMP等协议。

版权所有 © 华为技术有限公司

不同协议的限速阈值如表2-13所示。

表 2-13 限速阈值

协议类型	限速阈值
UDP	10Mbps
TCP	10Mbps
ICMP	100pps
Other（其他协议）	10Mbps

开启协议封禁

步骤1 登录管理控制台。

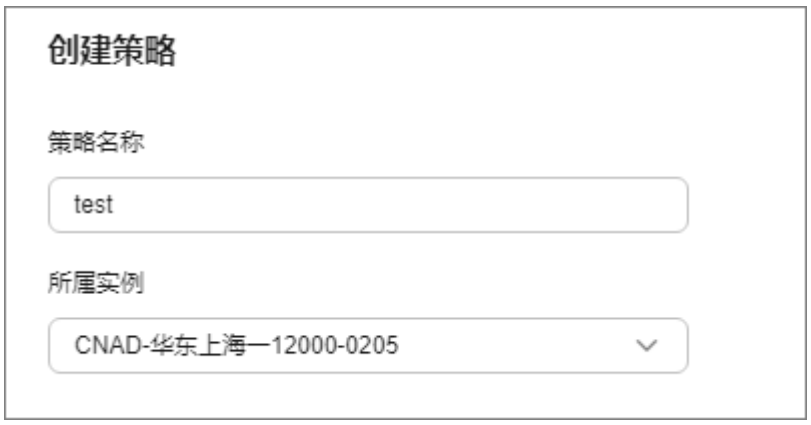
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 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4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-24 创建策略



步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“协议封禁”配置框中，单击“设置”，如图2-25所示。

图 2-25 协议封禁配置框

版权所有 © 华为技术有限公司

步骤8 在弹出的“协议封禁设置”对话框中，选择开启或关闭封禁的协议，单击“确定”。

图 2-26 设置协议封禁

-  ：开启封禁，可以阻止目标协议的流量访问。
-  ：关闭封禁，允许目标协议的流量访问。

----结束

2.4.7 通过指纹特征设置流量处理策略

您可以通过配置指纹过滤防护规则，对数据包中指定位置的内容进行特征匹配。

特征匹配后的流量，可以进行动作设置，比如丢弃、通过、限速等。

开启指纹过滤

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

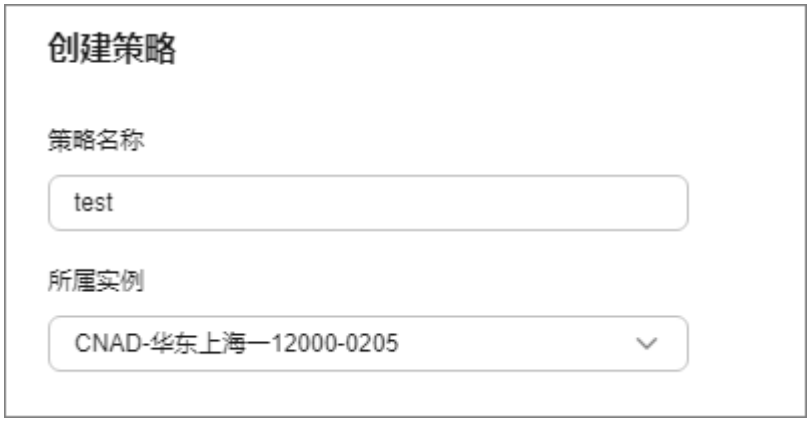
步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

版权所有 © 华为技术有限公司

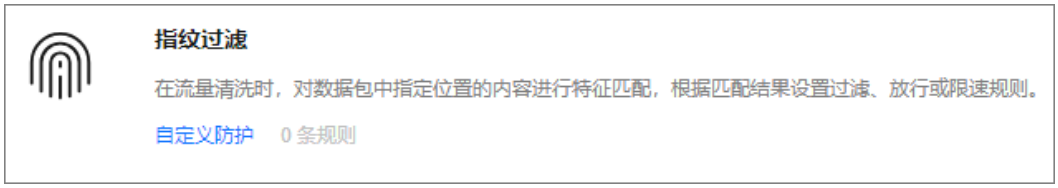
图 2-27 创建策略



步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“指纹过滤”配置框中，单击“自定义防护”。

图 2-28 指纹过滤配置框



步骤8 在弹出的“指纹过滤设置”对话框中，单击“新建指纹”。

步骤9 在弹出的对话框中，设置指纹参数。

版权所有 © 华为技术有限公司

图 2-29 新建指纹

表 2-14 指纹参数说明

参数	说明
指纹名称	输入指纹规则名称。
协议	设置指纹的协议，支持UDP和TCP协议。
源端口	指纹源端口的范围。
目的端口	指纹目的端口的范围。
包长过滤	需要过滤出的流量包长度。

版权所有 © 华为技术有限公司

参数	说明
报文载荷特征	• 检测载荷：设置检测载荷的十六进制值。 • 偏移量：设置指纹的偏移量。 例如：检测载荷为“1234afee”，“偏移量”为20，当数据区的第21个字节到第32个字节的内容匹配“1234afee”时，则认为此报文命中指纹。
匹配后动作	设置指纹匹配后的动作。 • 通过：放行流量。 • 丢弃：丢弃流量。 • 源限速：对源端限速，如某IP（或用户）的访问频率超过限速频率，就会对该IP（或用户）的访问限速。 • 通过&白名单：放行流量并将该指纹特征加入白名单。 • 丢弃&黑名单：丢弃流量并将该指纹特征加入黑名单。 • 限速：限制流量的访问速率。

步骤10 单击“确定”。

----结束

后续处理

- 在目标端口所在行“操作”列，单击“删除”可以删除指纹过滤规则。
- 在目标端口所在行“操作”列，单击“编辑”可以修改指纹过滤规则的信息。

2.4.8 通过高级防护策略限制异常连接

如果同一个源站IP短时间内频繁发起大量异常连接状态的报文时，您可以通过配置高级防护策略，将该源站IP纳入黑名单中进行封禁惩罚，等封禁结束后可恢复访问。

约束与限制

高级防护功能目前处于公测阶段，仅DDoS原生高级防护-全力防高级版部分区域支持该功能，如果您需要此项功能请**提交工单**开通。

开启高级防护

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“安全与合规 > DDoS防护AAD”，进入“Anti-DDoS流量清洗”界面。

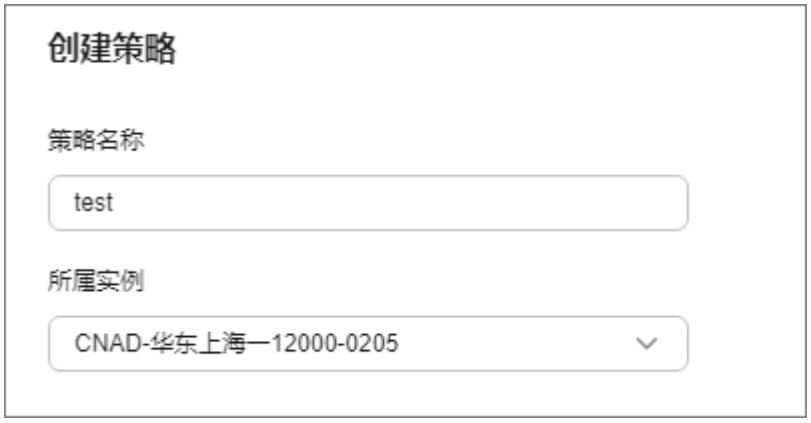
步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

版权所有 © 华为技术有限公司

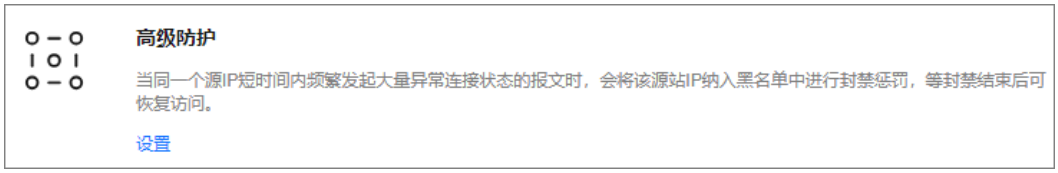
图 2-30 创建策略



步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“高级防护”配置框中，单击“设置”。

图 2-31 高级防护



步骤8 根据实际设置防护参数。

版权所有 © 华为技术有限公司

图 2-32 连接防护设置

表 2-15 连接防护设置参数说明

类别	参数	说明
检测阈值	目的IP地址并发连接数检查	当目的IP地址的TCP并发连接数大于“连接数阈值”时，启动针对TCP连接耗尽攻击的防御。防御启动后，开始对源IP地址进行检查。
	目的IP地址新建连接速率检查	当目的IP地址每秒新增加的TCP连接数大于“连接速率阈值”时，启动针对TCP连接耗尽攻击的防御。防御启动后，开始对源IP地址进行检查。

版权所有 © 华为技术有限公司

类别	参数	说明
防护动作	TCP连接耗尽防御	开启“TCP连接耗尽防御”后可设置： • “源IP新建连接检查”：按照设定周期检查源IP地址的新建连接数，当新建连接数大于设定值时，将该源站IP纳入黑名单中进行封禁惩罚，等封禁结束后可恢复访问。 • “源IP并发连接检查”：当源IP地址的TCP并发连接数大于设定值，将该源站IP纳入黑名单中进行封禁惩罚，等封禁结束后可恢复访问。
	应用层空连接防御	开启“应用层空连接防御”后可设置： • **HTTP**：按照设定周期检查源IP地址的HTTP异常连接，当异常连接数大于设定值时，将该源站IP纳入黑名单中进行封禁惩罚，等封禁结束后可恢复访问。 • **HTTPS**：按照设定周期检查源IP地址的HTTPS异常连接，当异常连接数大于设定值时，将该源站IP纳入黑名单中进行封禁惩罚，等封禁结束后可恢复访问。

步骤9 单击“确定”。

----结束

2.4.9 封禁指定区域的流量

DDoS原生高级防护支持封禁海外流量策略配置，策略生效后，来自海外的访问流量将被丢弃。

不同产品版本的策略生效条件不一样，具体请参见**表2-16**。

表 2-16 区域封禁生效条件

产品版本	区域封禁生效条件
全力防基础版	开启策略并触发攻击时生效。
全力防高级版	开启策略后生效。
原生防护2.0	• 接入DDoS防护专属EIP：开启策略后生效。 • 接入普通EIP：开启策略并触发攻击时生效。

约束与限制

- 该功能目前处于内测阶段，仅部分用户可以试用，其他用户需要**提交工单**申请开通。
- 当前DDoS原生高级防护仅支持“海外地区”封禁。

版权所有 © 华为技术有限公司

开启区域封禁

步骤1 登录管理控制台。

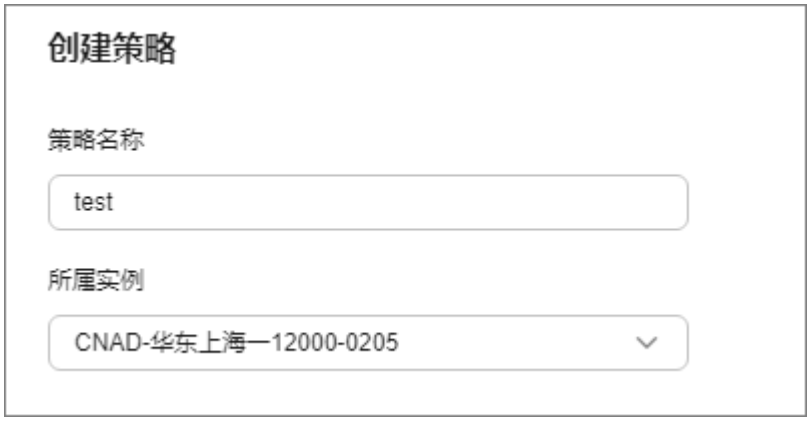
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 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4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

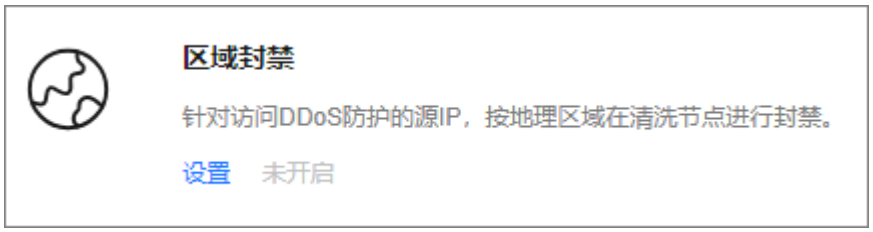
图 2-33 创建策略



步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“区域封禁”配置框中，单击“设置”。

图 2-34 区域封禁设置



步骤8 在弹出的对话框中勾选需要封禁的区域。

图 2-35 选择封禁区域

版权所有 © 华为技术有限公司

步骤9 单击“确定”，完成区域封禁设置。

----结束

2.5 添加防护对象

开通DDoS原生高级防护后，您需要将华为云上的公网IP资源添加为防护对象，才能为公网IP资源开启DDoS原生高级防护。

约束与限制

- 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相同。
- 全力防高级版只能防护专属EIP，原生防护2.0既能防护普通EIP也能防护专属EIP。
- 中国大陆外区域的原生防护2.0只能防护49.0.236.0/22、49.0.234.0/23和49.0.233.0/24的优选BGP IP。

前提条件

已创建防护策略，具体操作请参考**添加防护策略**。

添加防护对象到实例

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

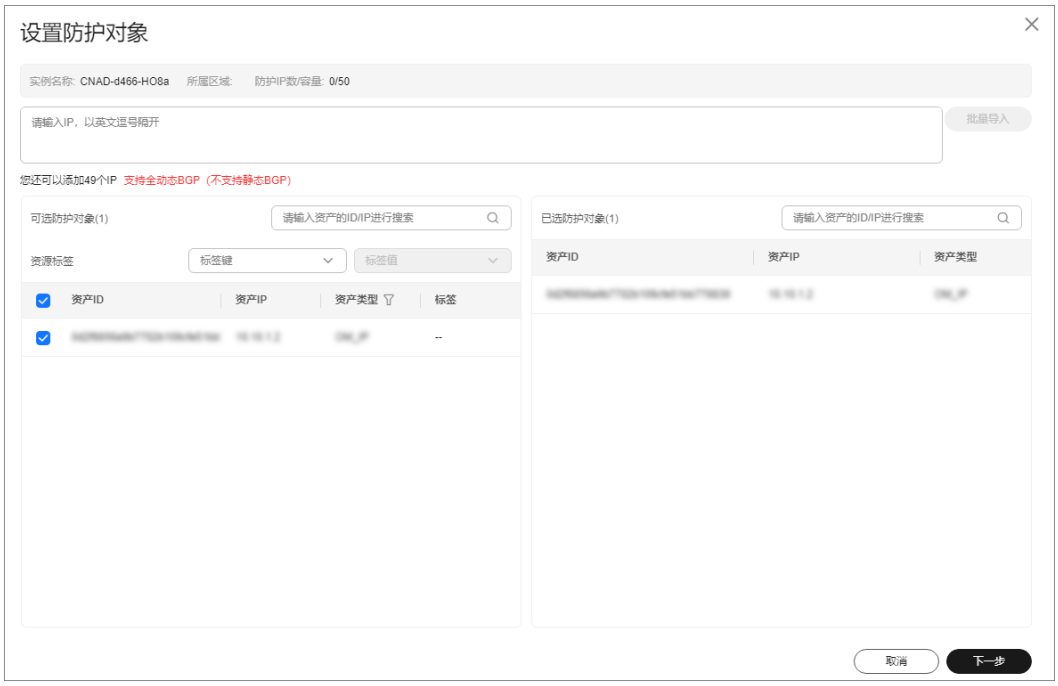
步骤3 在左侧导航栏选择“DDoS原生高级防护 > 实例列表”，进入DDoS原生高级防护“实例列表”页面。

步骤4 在目标实例中，单击“设置防护对象”。

步骤5 在弹出的“设置防护对象”对话框中，勾选需要防护的IP后，单击“下一步”。

版权所有 © 华为技术有限公司

图 2-36 设置防护对象



说明

- “可选防护对象”中为未添加到DDoS原生高级防护的IP。
- 支持批量导入防护IP。

步骤6 确认防护对象的设置，并且在下方选择IP防护策略，单击“确定”完成防护对象的设置。

图 2-37 确认防护对象设置

说明

防护策略的设置详见**添加防护策略**。

----结束

相关操作

- **查看实例防护对象**：您可以在实例区域框中，在“防护IP数”行后单击“查看”，查看当前实例的防护对象。

版权所有 © 华为技术有限公司

- **删除防护对象**：在设置防护对象页面，取消勾选防护对象即可。
- **配置标签**：在目标防护对象所在行的“标签”列中，单击。输入标签名称后，单击“确定”。

2.6 开启 DDoS 攻击告警通知

开启告警通知后，当IP遭受DDoS攻击时，您将接收到告警通知信息（接收消息方式由您设置）。

约束与限制

通知主题只支持在华北-北京四、中国-香港创建的主题。

前提条件

在开启告警通知前，建议您在“消息通知服务”**创建主题**并**添加订阅**。

说明

消息通知服务为付费服务，价格详情请参见**SMN价格详情**。

开启告警通知

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 告警通知”，进入“告警通知设置”页面。

步骤4 在“告警通知”页面，设置告警通知，相关参数说明如**表2-17**所示。

图 2-38 设置告警

版权所有 © 华为技术有限公司

表 2-17 设置告警通知

参数名称	说明
清洗流量告警阈值	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	开启或关闭告警通知，说明如下： •  ：开启状态。 •  ：关闭状态。
消息通知主题	可以选择使用已有的主题，或者单击“查看消息通知主题”创建新的主题。 更多关于主题的信息，请参见**《消息通知服务用户指南》**。

步骤5 单击“应用”，告警通知设置完成。

----结束

相关操作

如需关闭告警通知，在**图2-38**中，关闭告警通知，即将告警通知开关设置为  。

2.7 开启日志记录

启用DDoS原生高级防护功能后，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CNAD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，具体操作请参考**管理日志组**和**管理日志流**。

开启 LTS 日志

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏，选择“DDoS原生高级防护 > 概览”，进入“数据报表”页面。

步骤4 选择“日志”页签，开启日志  ，并选择日志组和日志流，相关参数说明如**图2-39**所示。

版权所有 © 华为技术有限公司

图 2-39 配置日志

表 2-18 全量日志配置参数

参数	参数说明
选择企业项目	选择已创建的企业项目。
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	开启后可设置： 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，包括攻击类型、防护的IP等信息。

步骤5 单击“确定”，全量日志配置成功。

您可以在LTS管理控制台查看DDoS原生高级防护的防护日志。

----结束

日志字段说明

本章节介绍了DDoS原生高级防护日志包含的日志字段。

表 2-19 关键字段说明

字段	说明
currentConn	当前连接数。
maxInPps	入报文峰值（单位：pps）。
newConn	新建连接数。
deviceType	上报日志的设备类型。默认为“CLEAN”，清洗设备。

版权所有 © 华为技术有限公司

字段	说明
attackTypes	攻击类型，具体请参考表2-20。
zoneIP	防护的IP。
logType	日志类型。默认为“ip_attack_sum”，攻击日志。
maxDropPps	攻击报文峰值（单位：pps）。
maxInKbps	入流量峰值（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。
maxDropKbps	攻击流量峰值（单位：kbps）。
attackStatus	攻击状态。 ● ATTACK：攻击状态。 ● NORMAL：正常状态。

表 2-20 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
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

版权所有 © 华为技术有限公司

数值	攻击类型
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
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

版权所有 © 华为技术有限公司

数值	攻击类型
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

2.8 查看数据报表

DDoS原生高级防护从流量趋势和报文速率两个维度展示正常流量和攻击流量信息，您可以通过查看正常流量和攻击流量的信息，了解当前网络安全状态。

在“数据报表”页面，您可以查看实例的攻击源、接收流量、攻击流量，以及DDoS防护趋势图、清洗流量峰值、攻击类型分布、TOP10被攻击IP等信息。

查看 DDoS 原生高级防护数据报表

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 概览”，进入DDoS原生高级防护“数据报表”页面。

版权所有 © 华为技术有限公司

图 2-40 数据报表页面

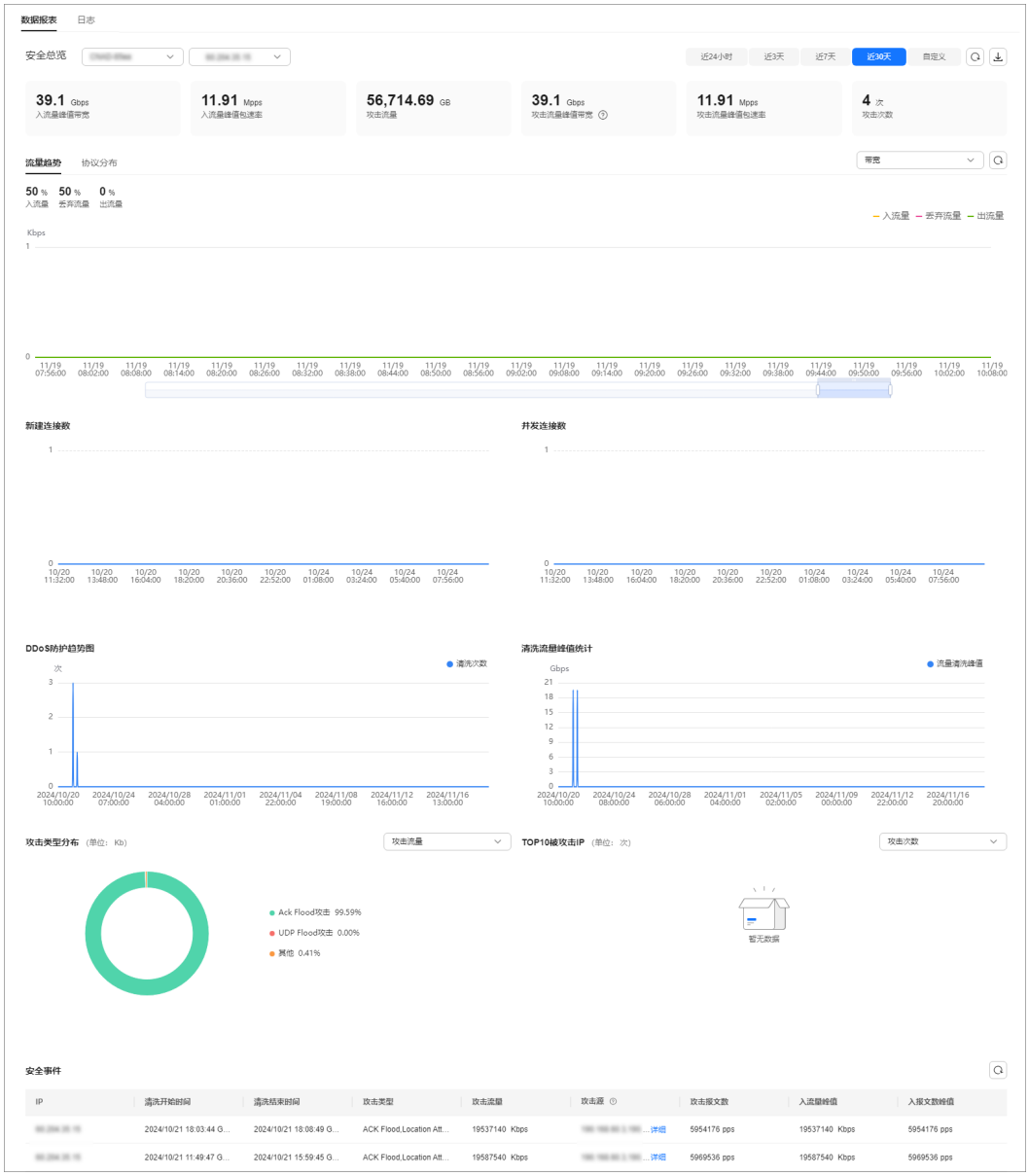


表 2-21 参数说明

参数	说明
入流量峰值带宽	每秒访问指定实例指定IP的最高流量。
入流量峰值包速率	入方向流量每秒流入数据包的最大值。
攻击流量峰值带宽	每秒攻击指定实例指定IP的最高流量。此处特指攻击生成了安全事件的防护过程中产生的攻击流量。
攻击流量峰值包速率	攻击流量每秒流入数据包的最大值。

版权所有 © 华为技术有限公司

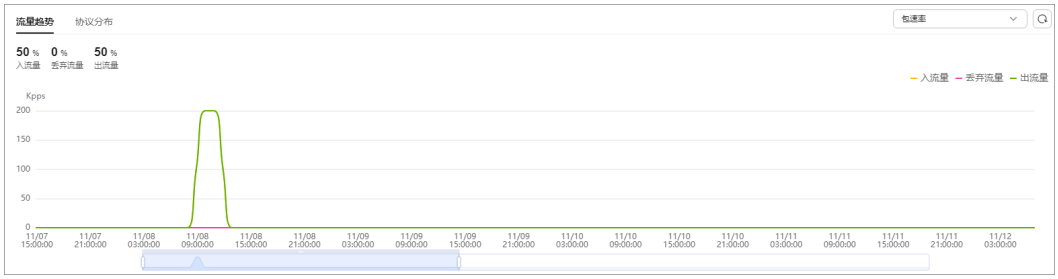
参数	说明
攻击次数	DDoS攻击指定实例指定IP的次数。
流量趋势	入流量、出流量、丢弃流量的占比及分布趋势。
协议分布	流量中TCP、UDP、ICMP等协议的占比及分布趋势。
并发连接数	查看同时访问的连接数。
新建连接数	查看新建访问的连接数。
DDoS防护趋势图	清洗次数的分布趋势。
清洗流量峰值统计	清洗流量峰值的分布趋势。
攻击类型分布	查看攻击事件类型。支持按“攻击次数”和“攻击流量”查看。
TOP10被攻击IP	被攻击次数最多的10个IP排行。支持按“攻击次数”和“带宽”查看。
安全事件	查看DDoS攻击事件。 单击攻击源IP后的“详细”，可以查看完整的攻击源IP列表。

说明

- 单击攻击源IP后的“详细”，可以查看完整的攻击源IP列表。
- 攻击中的事件，单击“查看动态黑名单”，可以查看攻击中的黑名单列表。
- 进行中的攻击事件可能不展示攻击源。
- 一些只包含部分攻击类型的攻击事件不含攻击源。
- 攻击源随机采样，不是全量的攻击源信息。

步骤4 选择“流量趋势”页签，查看流量趋势防护信息。

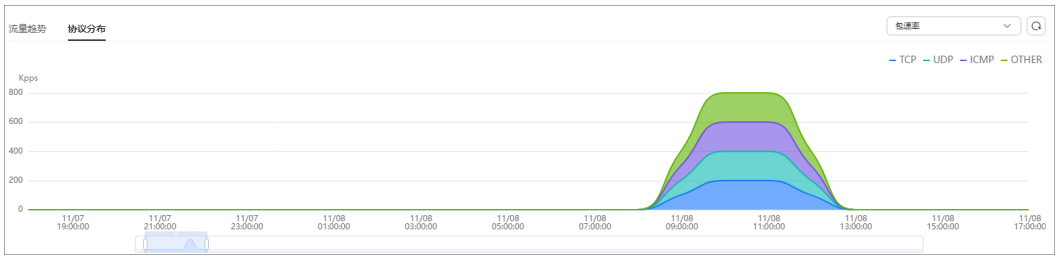
图 2-41 流量趋势



步骤5 选择“协议分布”页签，查看协议分布信息。

版权所有 © 华为技术有限公司

图 2-42 协议分布



----结束

相关操作

下载报表：在界面右上角单击，可以将数据报表下载到本地。

2.9 实例管理

2.9.1 查看实例信息

开通DDoS原生高级防护后，您可以通过实例列表查看已购买的实例信息，确保实例状态正常。

查看 DDoS 原生高级防护实例信息

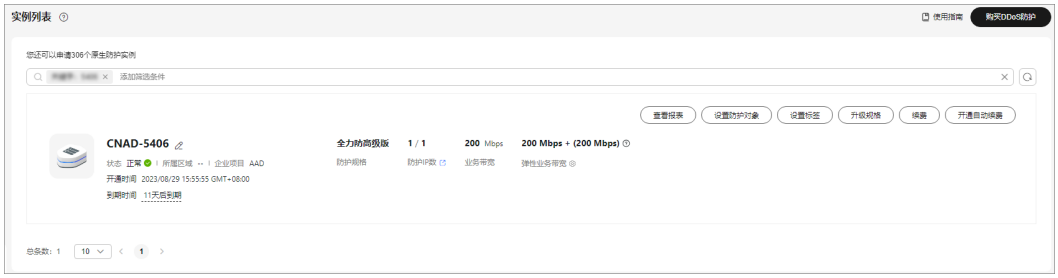
步骤1 登录管理控制台。

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

步骤3 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4 查看实例信息。

图 2-43 实例页面



----结束

版权所有 © 华为技术有限公司

2.9.2 配置实例标签

标签由标签键和标签值组成，用于标识云资源。当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。DDoS实例支持配置标签，方便管理实例。

设置实例标签

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 实例列表”，进入“实例列表”页面。

步骤4 在目标实例所在行，单击“设置标签”。

图 2-44 设置标签

步骤5 在标签添加页面，单击“添加标签”。

步骤6 选择“标签键”和“标签值”。

- 手动设置标签：手动输入标签键和标签值。
- 选择已有标签：选择已有的标签。

图 2-45 添加标签

版权所有 © 华为技术有限公司

说明

如您的组织已经设定本服务的相关标签策略，则需按照标签策略规则为资源添加标签。标签如果不符合标签策略的规则，则可能会导致标签添加失败，请联系组织管理员了解标签策略详情。

步骤7 单击“确定”。

----结束

2.10 防护对象管理

2.10.1 查看防护对象信息

添加防护对象后，您可以定期查看防护对象的防护状态、攻击统计等详细信息，及时调整防护策略，提高业务安全性。

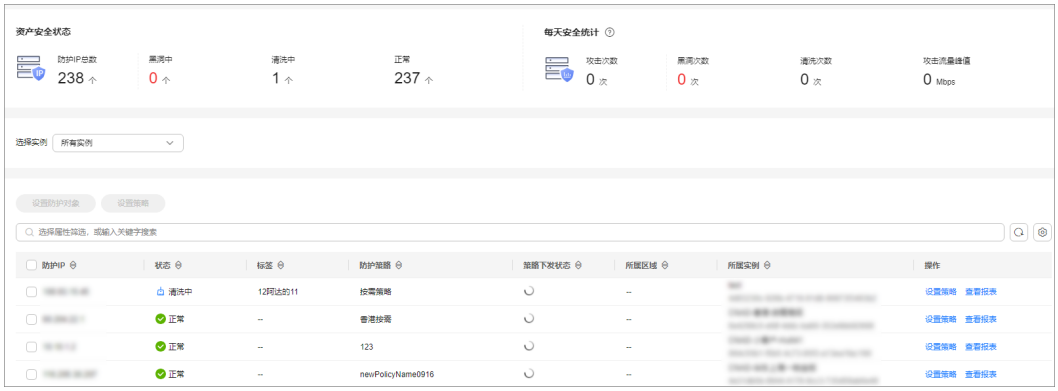
查看防护对象

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护对象”，进入“防护对象”页面。

图 2-46 防护对象



步骤4 查看防护对象信息，相关参数说明如表2-22所示。

表 2-22 防护对象相关参数说明

参数	说明
防护IP	CNAD防护的IP资源。
标签	防护IP设置的标签信息。

版权所有 © 华为技术有限公司

参数	说明
状态	防护IP的防护状态。 • 正常 • 清洗中
防护策略	防护IP所配置的防护策略。
策略下发状态	防护策略的下发状态。 • 策略下发中 • 策略下发成功
所属区域	防护IP所在的区域。
所属实例	防护IP所在的实例。
操作	• 单击“查看报表”，跳转到数据报表页面，查看防护数据信息。 • 防护IP未配置防护策略时，单击设置策略，可以为防护IP选择防护策略。

----结束

2.10.2 为防护对象设置防护策略

您需要为添加的防护对象选择防护策略，防护对象才能使用DDoS原生高级防护策略，抵御DDoS攻击。

设置防护策略

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“安全与合规 > DDoS防护AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护对象”，进入“防护对象”页面。

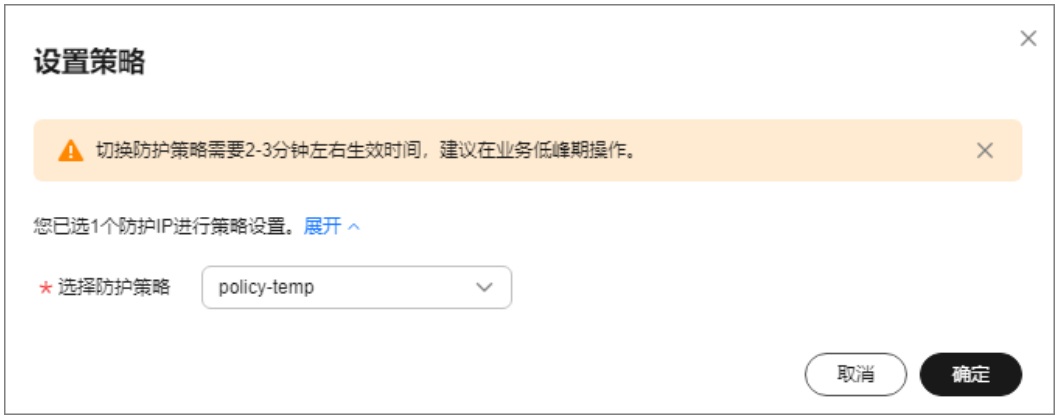
图 2-47 防护对象

 版权所有 © 华为技术有限公司

步骤4 在目标防护对象所在行的“操作”列中，单击“设置策略”。

步骤5 在弹出的对话框中，选择防护策略后，单击“确定”，如图2-48所示。

图 2-48 设置策略



说明

单击“展开”，可以查看防护IP的详细信息。

----结束

批量设置防护策略

勾选需要设置防护策略的防护对象，在列表左上角单击“设置策略”，根据提示选择防护策略，单击“确定”。

说明

批量设置方法只能用于同一实例下的多个防护对象。

2.10.3 移除防护对象

当您的业务不需要DDoS原生高级防护时，可以移除防护对象。

绑定在DDoS原生高级防护-全力防基础版上的EIP，在移除后**自动纳入DDoS原生基础防护**中防护。

绑定在DDoS原生高级防护-全力防高级版上的DDoS防护专属EIP，**在移除后不可再被互联网访问**。请谨慎选择后再移除防护对象。

须知

防护对象移除后，将失去DDoS防护能力，导致资源面临安全风险，请谨慎操作。

移除防护对象

步骤1 登录管理控制台。

版权所有 © 华为技术有限公司

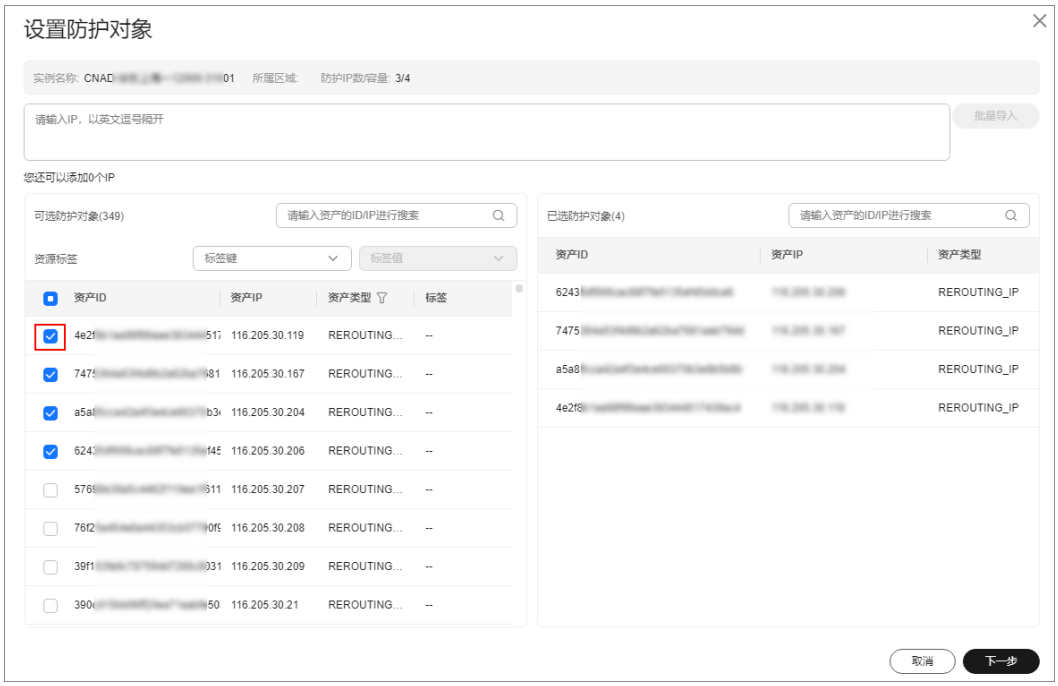
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 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4 找到需要移除防护对象的实例，单击“设置防护对象”。

步骤5 在弹出的对话框中，取消勾选需要移除的防护对象，单击“下一步”。

图 2-49 移除防护对象



步骤6 确认移除的防护对象，单击“确定”，完成移除防护对象。

图 2-50 确认移除防护对象

----结束

2.11 查看监控指标

版权所有 © 华为技术有限公司

2.11.1 DDoS 原生高级防护监控指标说明

功能说明

本节定义了DDoS原生高级防护上报云监控服务的监控指标的命名空间和监控指标列表，用户可以通过云监控服务提供管理控制台来检索DDoS原生高级防护产生的监控指标和告警信息。

命名空间

SYS.DDOS

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

监控指标

表 2-23 DDoS 原生高级防护服务支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
ip_drop_rate	丢弃流量	IP丢弃流量带宽	≥0kb/s	DDoS原生高级防护	60秒
instance_drop_rate	丢弃流量	实例丢弃流量带宽	≥0kb/s	DDoS原生高级防护	60秒
ip_back_to_source_rate	回源带宽	IP回源流量带宽	≥0kb/s	DDoS原生高级防护	60秒
instance_back_to_source_rate	回源带宽	实例回源流量带宽	≥0kb/s	DDoS原生高级防护	60秒
ip_internet_in_rate	入流量	IP入流量带宽	≥0kb/s	DDoS原生高级防护	60秒
instance_internet_in_rate	入流量	实例入流量带宽	≥0kb/s	DDoS原生高级防护	60秒
ip_new_connection	新建连接	IP新建连接数	≥0count/s	DDoS原生高级防护	60秒
instance_new_connection	新建连接	实例新建连接数	≥0count/s	DDoS原生高级防护	60秒
ip_concurrent_connection	并发连接	IP并发连接数	≥0count/s	DDoS原生高级防护	60秒

版权所有 © 华为技术有限公司

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
instance_concurrent_connection	并发连接	实例并发连接数	≥0count/s	DDoS原生高级防护	60秒

维度

Key	Value
package	防护包
package_ip	防护包-防护IP

2.11.2 查看监控指标

您可以通过管理控制台，查看DDoS原生高级防护的相关指标，及时了解DDoS原生高级防护的防护状况，并通过指标设置防护策略。

前提条件

已在云监控页面设置监控告警规则。有关设置监控告警规则的详细操作，请参见**设置监控告警规则**。

查看监控指标

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的 ，选择“管理与监管 > 云监控服务 CES”。

步骤4 选择“云服务监控 > DDoS服务 DDoS”。

版权所有 © 华为技术有限公司

图 2-51 选择服务

步骤5 在“云服务监控详情”页面，选择“DDoS服务 > 防护包”。

步骤6 在需要查看的目标所在行，单击“查看监控指标”，查看对象的指标详情。

----结束

2.11.3 设置监控告警规则

通过设置DDoS告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解DDoS原生高级防护的防护状况，从而起到预警作用。

为多个实例或实例防护的IP设置监控告警请参考**批量设置监控告警规则**；为某个指定实例或实例防护的IP设置监控告警请参考**为单个指定资源设置监控告警规则**。

如果您需要自主定义更多的监控指标，可通过API请求上报至云监控服务，具体操作请参考**添加监控数据**和**DDoS原生高级防护监控指标说明**。

批量设置监控告警规则

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

版权所有 © 华为技术有限公司

步骤3 单击页面左上方的 ☰，选择“管理与监管 > 云监控服务 ”。

步骤4 在左侧导航树栏，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”界面。

步骤6 填写告警规则信息，如图2-52所示，填写规则如表2-24所示。

图 2-52 设置监控告警规则

 版权所有 © 华为技术有限公司

表 2-24 告警规则参数说明

参数名称	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	选择告警类型。
云产品	在下拉列表框中选择“DDoS服务-防护包”。
资源层级	选择需要监控的资源维度。
监控范围	告警规则适用的资源范围，可选择资源分组或指定资源。
触发规则	可选择“关联模板”和“自定义创建”。 创建自定义模板的具体操作请参考**创建自定义告警模板**。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。
模板	选择关联或导入的模板。
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	需要发送告警通知的对象，根据实际选择。

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

为单个指定资源设置监控告警规则

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务 ”。

步骤4 选择“云服务监控 > DDoS服务 DDoS”。

 版权所有 © 华为技术有限公司

图 2-53 选择服务

步骤5 在“云服务监控详情”页面，选择“DDoS服务 > 防护包”。

步骤6 在需要监控的对象所在行，选择“更多 > 创建告警规则”。

步骤7 填写告警规则信息，如图2-54所示，填写规则如表2-25所示。

图 2-54 设置监控告警规则

表 2-25 告警规则参数说明

参数名称	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。

版权所有 © 华为技术有限公司

参数名称	参数说明
描述	告警规则描述。
告警类型	保持默认。
资源类型	保持默认。
维度	保持默认。
监控范围	保持默认。
监控对象	保持默认。
触发规则	可选择“关联模板”和“自定义创建”。 创建自定义模板的具体操作请参考**创建自定义告警模板**。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。
模板	选择关联或导入的模板。
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	根据实际选择通知方式。

步骤8 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

2.11.4 设置事件告警通知

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DDoS原生高级防护的防护情况。

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。

说明

设置事件告警通知时，如果开启了“发送通知”，会使用消息通知服务（SMN）并产生相关费用。

开启事件告警通知

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 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。

版权所有 © 华为技术有限公司

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2-26配置告警参数。

图 2-55 告警参数

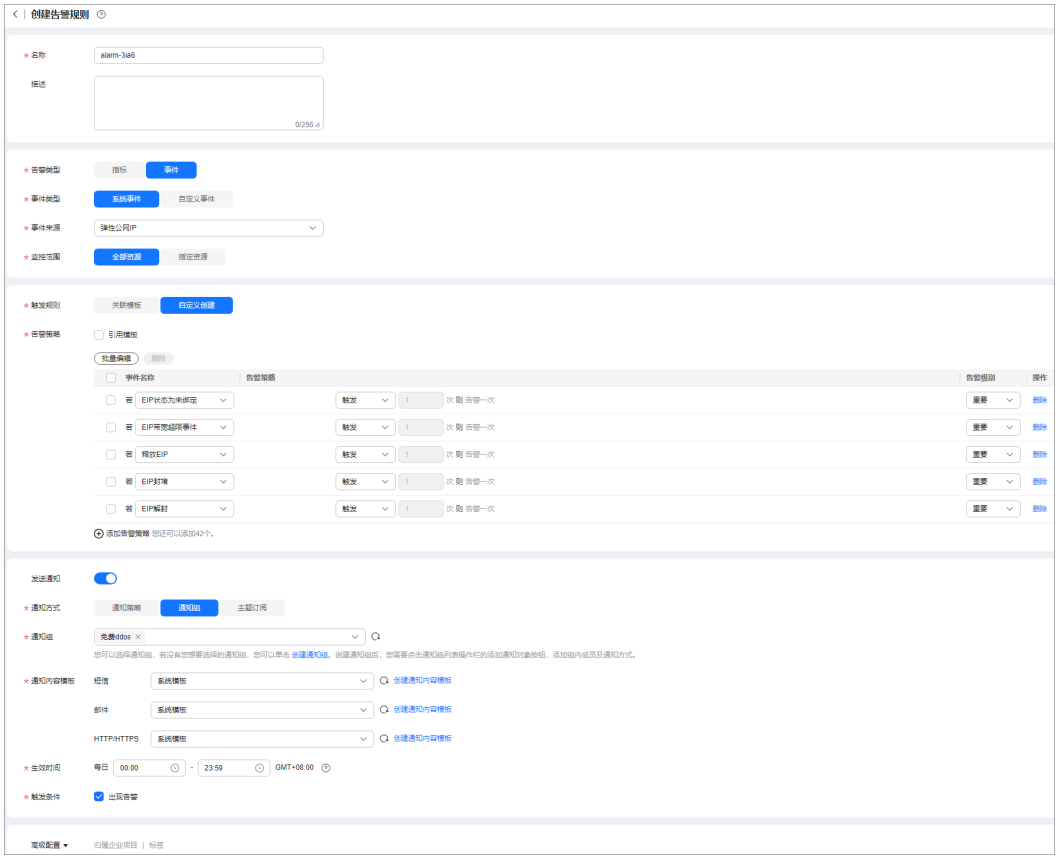


表 2-26 参数说明

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	默认为“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”。 当流量大于10000kps时，系统会在开始清洗和结束清洗各发送一次告警通知；流量小于10000kps不会发送告警通知。

 版权所有 © 华为技术有限公司

参数	说明
通知方式	根据实际选择进行配置。 **说明** 告警消息由消息通知服务SMN发送，可能产生少量费用。

步骤7 单击“立即创建”，在弹出的窗口中单击“确定”，告警通知创建成功。

----结束

2.12 查询审计日志

2.12.1 云审计服务支持的 DDoS 原生高级防护操作

云审计服务（Cloud Trace Service，CTS）记录了DDoS防护相关的操作事件，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DDoS防护操作列表如**表2-27**所示。

表 2-27 云审计支持的 DDoS 防护操作列表

操作名称	事件名称
更新告警通知配置	updateAlarmConfig
删除告警通知配置	deleteAlarmConfig
创建防护包	createPackage
更新防护包	updatePackage
绑定IP到防护包	bindIpToPackage
从防护包上解绑IP	unbindIpToPackage
删除防护包	DeletePackage
创建策略	createPolicy
更新策略	updatePolicy
绑定IP到策略	bindIpToPolicy
从策略中解绑IP	unbindIpToPolicy
添加黑白名单	addblackWhiteIpList
删除黑白名单	deleteblackWhiteIpList
删除策略	deletePolicy
配置全量日志的日志组和日志流	updateLogConfig

版权所有 © 华为技术有限公司

操作名称	事件名称
关闭全量日志的日志组和日志流	deleteLogConfig
给防护IP打标签	updateTagForIp
设置连接防护策略	updateConnectionProtection
新增端口封禁	addPortBlock
更新端口封禁	updatePortBlock
删除端口封禁	deletePortBlock
新增指纹过滤	createFingerprint
更新指纹过滤	updateFingerprint
删除指纹过滤	deleteFingerprint
添加IP黑白名单	addBlackWhiteIpList
删除IP黑白名单	deleteBlackWhiteIpList
新增水印	createWatermark
修改水印	updateWatermark
删除水印	deleteWatermark

2.12.2 查看云审计日志

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

前提条件

已开通云审计服务，具体操作请参考**开通云审计服务**。

查看 DDoS 原生高级防护审计日志

步骤1 **登录管理控制台**。

步骤2 单击页面左侧的 ☰，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 在下拉框中选择“云服务”，输入“CNAD”，按“Enter”。

步骤5 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：

版权所有 © 华为技术有限公司

- 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

版权所有 © 华为技术有限公司

3 DDoS 高防操作指南

3.1 DDoS 高防概述

购买DDoS高防实例，业务接入DDoS高防后即可防护，通过丰富全面的防护规则帮助您防护海量DDoS攻击。

业务接入DDoS高防的流程如图3-1所示。

图 3-1 接入流程

表 3-1 流程说明

序号	流程	说明
1	通过IAM授予使用DDoS高防的权限	通过统一身份认证服务（Identity and Access Management，简称IAM）为用户授予精细的DDoS高防服务权限。
2	购买实例	根据业务需求购买DDoS高防实例。
3	接入DDoS高防	将域名或IP接入DDoS高防。
4	配置防护策略	DDoS高防提供了丰富全面的防护规则，您可以根据业务需求配置相应的防护策略。

版权所有 © 华为技术有限公司

序号	流程	说明
5	常用安全操作	• **开启DDoS攻击告警通知**：开启告警通知后，遭受DDoS攻击时，您可以第一时间接收告警通知。 • **开启日志记录**：通过LTS记录的日志数据，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。 • **查看数据报表**：查看DDoS攻击防护数据报表和CC攻击防护数据报表，了解当前业务的网络安全状态。 • **实例管理**：查看高防实例信息、修改实例规格和配置等。 • **域名管理**：查看域名信息、修改解析线路、和域名配置等。 • **证书管理**：查看证书信息，进行证书的更新和删除等管理。 • **转发规则管理**：查看转发规则、修改源站IP、导出转发规则等。 • **查看监控指标**：通过云监控服务，查看DDoS高防的相关指标，及时了解DDoS高防的防护状况，及时调整防护策略。 • **查询审计日志**：通过云审计服务查看DDoS高防的历史操作记录。

3.2 通过 IAM 授予使用 DDoS 高防的权限

3.2.1 创建用户并授权使用 AAD

如果您需要对您所拥有的AAD进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用AAD资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将AAD资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用AAD服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图3-2**所示。

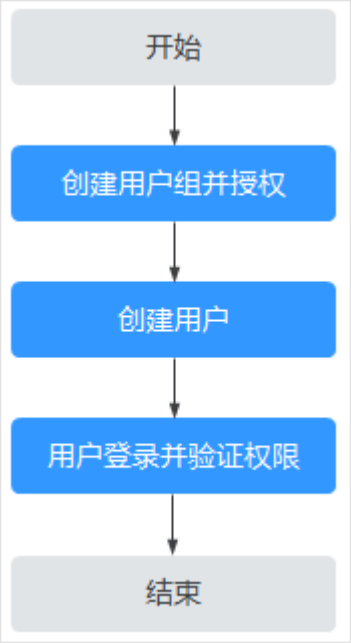
前提条件

给用户组授权之前，请您了解用户组可以添加的AAD权限，并结合实际需求进行选择。

版权所有 © 华为技术有限公司

示例流程

图 3-2 给用户授权服务权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予DDoS高防服务权限“AAD FullAccess”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，验证权限：

   单击页面左上方的 ☰，选择除DDoS高防服务外（假设当前策略仅包含“AAD FullAccess”）的任一服务，如果提示权限不足，表示“AAD FullAccess”已生效。

3.2.2 AAD 自定义策略

如果系统预置的AAD权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见**AAD权限及授权项**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的AAD自定义策略样例。

AAD 自定义策略样例

- 示例1：授权用户查询防护策略

版权所有 © 华为技术有限公司

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aad:policy:get"
                                ]
        }
    ]
}
```

- 示例2：拒绝用户删除IP黑白名单规则

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予“AAD FullAccess”的系统策略，但不希望用户拥有“AAD FullAccess”中定义的删除IP黑白名单规则的权限（aad:whiteBlackIpRule:delete），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为“Deny”，然后同时将“AAD FullAccess”和拒绝策略授予用户，根据Deny优先原则用户可以对AAD执行除了删除IP黑白名单规则的所有操作。以下策略样例表示：拒绝用户删除IP黑白名单规则。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aad:whiteBlackIpRule:delete"
            ]
        },
    ]
}
```

3.2.3 AAD 权限及授权项

如果您需要对您所拥有的AAD进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用AAD的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

版权所有 © 华为技术有限公司

权限	授权项
查询实例详情	aad:instance:get
查询实例列表	aad:instance:list
创建实例	aad:instance:create
修改实例	aad:instance:put
查询证书列表	aad:certificate:list
上传证书	aad:certificate:create
删除证书	aad:certificate:delete
获取域名详情	aad:domain:get
获取域名列表	aad:domain:list
添加域名	aad:domain:create
编辑域名	aad:domain:put
删除域名	aad:domain:delete
查询防护策略	aad:policy:get
查询开启防护策略的域名列表	aad:policy:list
创建防护策略	aad:policy:create
更新防护策略	aad:policy:put
删除防护策略	aad:policy:delete
创建黑白名单规则	aad:whiteBlackIpRule:create
删除黑白名单规则	aad:whiteBlackIpRule:delete
查询黑白名单规则列表	aad:whiteBlackIpRule:list
查询配额	aad:quotas:get
查询转发规则	aad:forwardingRule:get
导出转发规则	aad:forwardingRule:list
添加转发规则	aad:forwardingRule:create
修改转发规则	aad:forwardingRule:put
删除转发规则	aad:forwardingRule:delete
查看数据报表	aad:dashboard:get
查询告警通知	aad:alarmConfig:get
创建告警通知	aad:alarmConfig:create

版权所有 © 华为技术有限公司

3.2.4 控制台的权限依赖

DDoS高防对其他云服务有诸多依赖关系，因此在您开启IAM系统策略授权后，在Console控制台的各项功能需要配置相应的服务权限后才能正常查看或使用，依赖服务的权限配置均基于您已设置了IAM系统策略授权的AAD FullAccess或AAD ReadOnlyAccess策略权限，详细设置方法请参见**创建用户并授权使用AAD**。

依赖服务的权限设置

如果IAM用户需要在Console控制台拥有相应功能的查看或使用权限，请确认已经对该用户所在的用户组设置了CAD Administrator、AAD FullAccess或AAD ReadOnlyAccess策略的集群权限，再按如下**表3-2**增加依赖服务的角色或策略。

表 3-2 Console 中依赖服务的角色或策略

控制台功能	依赖服务	需配置角色或策略
添加域名	云证书管理服务 CCM	源站使用HTTPS转发协议时，自动拉取证书需要授予SCM ReadOnlyAccess权限。
配置DDoS高防日志	云日志服务 LTS	需要增加LTS ReadOnlyAccess的系统策略，才能选择在云日志服务中创建的日志组和日志流名称。
开启告警通知	消息通知服务 SMN	需要增加SMN ReadOnlyAccess的系统策略，才能获取消息通知服务的主题群组。
配置实例标签	标签管理服务 TMS	需要增加TMS FullAccess的系统策略，才能创建标签键。
购买实例	企业项目管理服务 EPS	需要增加EPS ReadOnlyAccess的系统策略后，才能在购买实例时选择该企业项目。

3.3 购买实例

3.3.1 购买 DDoS 高防实例

当您的服务器频繁遭受DDoS攻击，尤其是大流量DDoS攻击时，DDoS高防可以提供持续性的防护，保障业务的连续性。

购买后，您只需要进行简单的配置接入，即可获得强大的防护能力，适用于服务器部署在中国大陆和亚太地区的业务。

须知

- DDoS高防购买后，不支持退款。
- DDoS高防实例到期≥30个自然日时，DDoS高防将停止转发业务流量，实例将被释放。如果您不需要继续使用DDoS高防，请务必在到期30个自然日之前，将业务流量从高防切换到源站服务器。

版权所有 © 华为技术有限公司

约束与限制

- 每个用户默认最多可以购买5个实例。如果配额不足，您可以**提交工单**申请扩大配额。
- 业务服务器在中国内地，推荐购买DDoS高防。使用DDoS高防，域名必须经过ICP备案，未备案域名将无法正常访问。
- 业务服务器在中国内地以外的地域，推荐购买DDoS高防国际版。

前提条件

账号需要拥有“CAD Administrator”和“BSS Administrator”角色权限。

购买 DDoS 高防

步骤1 **登录管理控制台**。

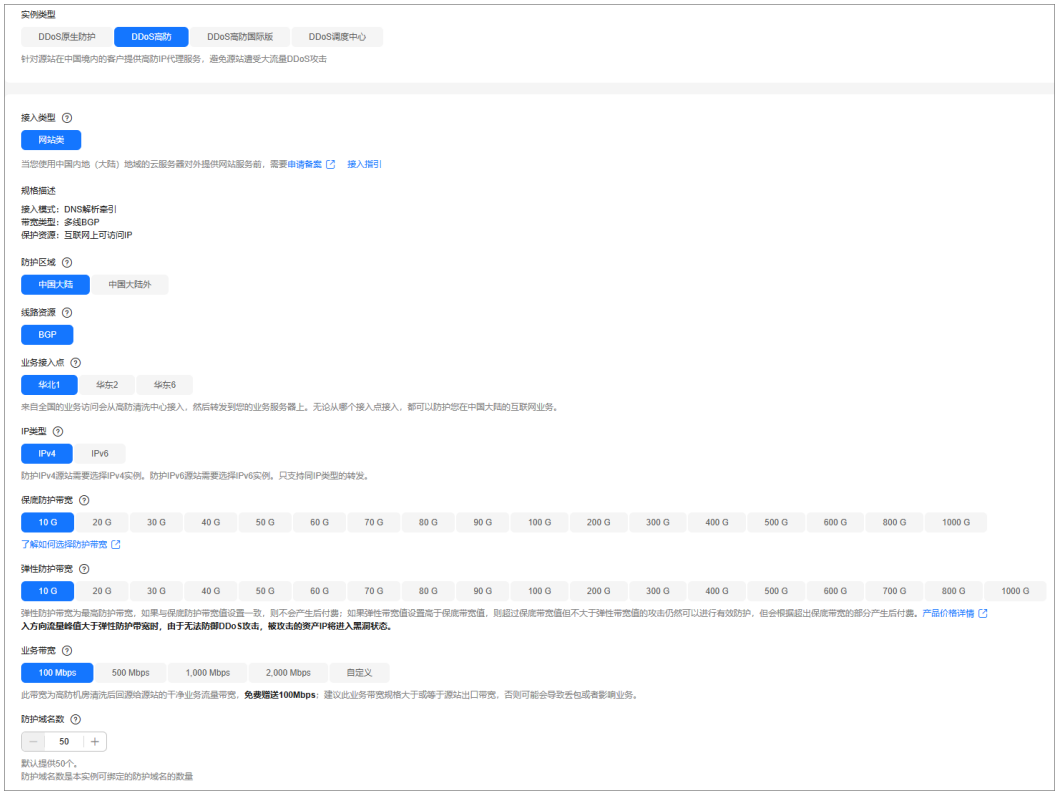
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

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 在“购买DDoS防护”界面，“实例类型”选择“DDoS高防”。

步骤5 设置DDoS高防实例规格，如**图3-3**所示，相关参数说明如**表3-3**所示。

图 3-3 购买 DDoS 高防



 版权所有 © 华为技术有限公司

表 3-3 参数说明

参数	说明
接入类型	● 网站类：华为云通过智能算法为您选择最佳接入点，并且不再提供固定的高防IP。推荐使用“域名接入”的用户购买并使用。 ● IP接入：仅提供IP端口防护，提供固定的高防IP。
防护区域	● 中国大陆：适用于业务服务器部署在中国大陆的场景。 ● 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、新加坡）的场景。 业务服务器部署在其他地域的场景，推荐购买DDoS高防国际版。
线路资源	● 中国大陆：仅支持“BGP”。 ● 中国大陆外：仅支持AnyCast。
业务接入点	中国大陆提供以下接入点，请根据您业务的地理位置自行选择： ● 华北1：线路支持中国移动、中国电信、中国联通、北京教育网、鹏博士、河北广电、重庆广电。 ● 华东2：支持中国移动、中国电信、中国联通。 ● 华东6：支持中国移动、中国电信、中国联通。 中国大陆外仅支持亚太接入点，该线路适用于业务服务器部署在亚太地区（当前支持香港、新加坡）的场景。
IP类型	● IPv4：防护IPv4源站需要选择IPv4实例。 ● IPv6：防护IPv6源站需要选择IPv6实例。 中国大陆外只支持防护IPv4。
防护套餐	中国大陆外区域才有此参数。 ● 保险防护：提供每月2次高级防护，适用于防护有低DDoS攻击风险的服务。 ● 全力防护：提供不限次数的高级防护，适用于防护有高DDoS攻击风险的服务。
保底防护带宽	保底防护带宽是指用于防御攻击的保底带宽。如果攻击峰值小于等于客户购买的保底防护带宽，客户无需支付额外费用。 如果需要提升防护性能，可以设置“弹性防护带宽”。
弹性防护带宽	攻击峰值超过保底防护带宽时产生弹性防护费用，后扣费。 在购买高防实例后，可以根据业务实际情况，修改弹性防护带宽。 **说明** 弹性防护带宽不能小于保底防护带宽。如果用户选择的弹性防护带宽等于保底防护带宽，则弹性防护功能不生效。
防护域名数	仅接入类型为“网站类”时可选择。默认提供50个，可以付费增加，最多可支持200个。

版权所有 © 华为技术有限公司

参数	说明
转发规则数	仅接入类型为“IP接入”时有此参数。 ● 中国大陆：默认提供50个，可以付费增加，最多可支持500个。 ● 中国大陆外：默认提供5个，可以付费增加，最多可支持200个。
业务带宽	高防实例的回源业务带宽，从高防实例转发回源站的干净流量带宽。业务带宽支持配置的范围为100Mbps～5000Mbps。 请您统计将要接入华为云DDoS高防实例的所有业务日常入方向和出方向总流量的峰值，您选择的最大业务带宽应大于这些业务的网络入、出方向总流量峰值中较大的值。 **注意** 如果您购买的实例业务带宽低于上述中的峰值流量大小，可能会丢包或者影响业务，在这种情况下请及时升级业务带宽。升级规格请参见**升级实例规格**。 假如，您有两个业务（业务A和业务B）需要接入DDoS高防服务，业务A正常业务流量峰值均不超过50 Mbps，业务B正常业务流量峰值均不超过70 Mbps，业务流量总和不超过120Mbps。在这种情况下，您只需要确保购买的实例的最大业务带宽大于120Mbps即可保证业务的正常运行。

步骤6 选择“购买时长”和“购买数量”，如**图3-4**所示，相关参数说明如**表3-4**所示。

图 3-4 选择购买时长和购买数量

表 3-4 购买参数说明

参数	说明	取值样例
实例名称	高防实例名称。 ● 名称长度小于等于32个字符。 ● 名称只能由中文字符、大小写英文字母、数字、下划线和中划线组成。	CAD-0001

版权所有 © 华为技术有限公司

参数	说明	取值样例
企业项目	企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请**开通企业管理功能**。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **说明** • “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。 • 只有注册的华为云账号购买实例时，“企业项目”下拉列表中才可以选择到“default”。	-
购买时长	根据实际选择。	-
购买数量	选择购买的实例个数，每个用户默认最多可以购买5个实例。	1

说明

“自动续费”为可选项。勾选“自动续费”后，系统将在产品到期前自动续费。

步骤7 单击“立即购买”。

步骤8 在“订单详情”页面，勾选协议后，单击“去支付”。

说明

中国大陆外区域需要等待审批后才能进行支付。

步骤9 在支付界面完成订单支付。

----结束

3.3.2 购买 DDoS 高防国际版实例

当您的服务器频繁遭受DDoS攻击，尤其是大流量DDoS攻击时，DDoS高防国际版可以提供持续性的防护，保障业务的连续性。

购买后，您只需进行简单的配置接入，即可获得强大的防护能力，适用于服务器部署在中国内地以外的业务。

须知

- DDoS高防购买后，不支持退款。
- DDoS高防实例到期≥30个自然日时，DDoS高防将停止转发业务流量，实例将被释放。如果您不需要继续使用DDoS高防，请务必在到期30个自然日之前，将业务流量从高防切换到源站服务器。

版权所有 © 华为技术有限公司

约束与限制

- 每个用户默认最多可以购买5个实例。如果配额不足，您可以**提交工单**申请扩大配额。
- 业务服务器在中国内地，推荐购买DDoS高防。使用DDoS高防，域名必须经过ICP备案，未备案域名将无法正常访问。
- 业务服务器在中国内地以外的地域，推荐购买DDoS高防国际版。
- DDoS高防国际版实例当前只支持在控制台进行实例购买、实例续费和域名接入管理，不支持配置防护策略、告警通知等操作。

前提条件

账号需要拥有“CAD Administrator”和“BSS Administrator”角色权限。

购买 DDoS 高防国际版

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

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 在“购买DDoS防护”界面，“实例类型”选择“DDoS高防国际版”。

步骤5 设置DDoS高防实例规格，如**图3-5**所示，相关参数说明如**表3-5**所示。

版权所有 © 华为技术有限公司

图 3-5 购买 DDoS 高防国际版

表 3-5 参数说明

参数	说明
线路资源	当前支持“亚太”。
IP个数	多个：为用户的每个业务系统单独提供高防IP，上限为所选规格内包含的防护域名与防护端口的总和。
防护带宽	50G：提供最高50Gbit/s防护。 全力防：DDoS高防集群将使用所有可用资源进行全力防护，但如果攻击超过集群可用的防护能力，依然存在黑洞风险。
转发规则数	默认提供5个，最多可选50个。
防护域名数	默认提供5个，最多可选50个。
业务带宽	业务带宽指高防机房将清洗后的干净流量，转发给源站所占用的带宽。 • 业务带宽支持范围：10Mbps～5000Mbps。 • 高防机房在华为云外，建议购买的高防业务带宽规格大于或等于源站出口带宽。

版权所有 © 华为技术有限公司

步骤6 选择“购买时长”和“购买数量”，如图3-6所示，相关参数说明如表3-6所示。

图 3-6 选择购买时长和购买数量

表 3-6 购买参数说明

参数	说明	取值样例
实例名称	高防实例名称。 ● 名称长度小于等于32个字符。 ● 名称只能由中文字符、大小写英文字母、数字、下划线和中划线组成。	CAD-0001
企业项目	企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请开通企业管理功能。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **说明** ● “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。 ● 只有注册的华为云账号购买实例时，“企业项目”下拉列表中才可以选择到“default”。	-
购买时长	可以选择3个月～1年的时长。	3
购买数量	选择购买的实例个数，每个用户默认最多可以购买5个实例。	1

说明

“自动续费”为可选项。勾选“自动续费”后，系统将在产品到期前自动续费。

步骤7 单击“立即购买”。

步骤8 待订单完成审批后，在“订单详情”页面，单击“去支付”。

 版权所有 © 华为技术有限公司

步骤9 在支付界面完成订单支付。

----结束

3.4 接入 DDoS 高防

3.4.1 业务接入 DDoS 高防概述

DDoS高防支持接入域名和IP，两种接入方式的主要差异如下：

表 3-7 接入方式说明

接入类型	适用场景	主要差异
域名接入	业务通过域名对外提供服务，域名已通过ICMP备案，您可以将域名接入DDoS高防。	华为云通过智能算法为您选择最佳接入点，并且不再提供固定的高防IP。推荐使用“域名接入”的用户购买并使用。
IP接入	业务没有域名，仅通过公网IP对外提供服务，您可以通过配置转发规则将业务接入DDoS高防。	仅提供IP端口防护，提供固定的高防IP。推荐使用“四层转发规则”的用户购买并使用。

须知

- 业务接入过程中配置错误可能导致防护失效或业务中断，建议离线配置，避免业务在线时操作。配置成功，验证通过之后再将业务接入。
- 如果无法评估场景风险，请**提交工单**咨询。

3.4.2 域名网站类业务接入 DDoS 高防

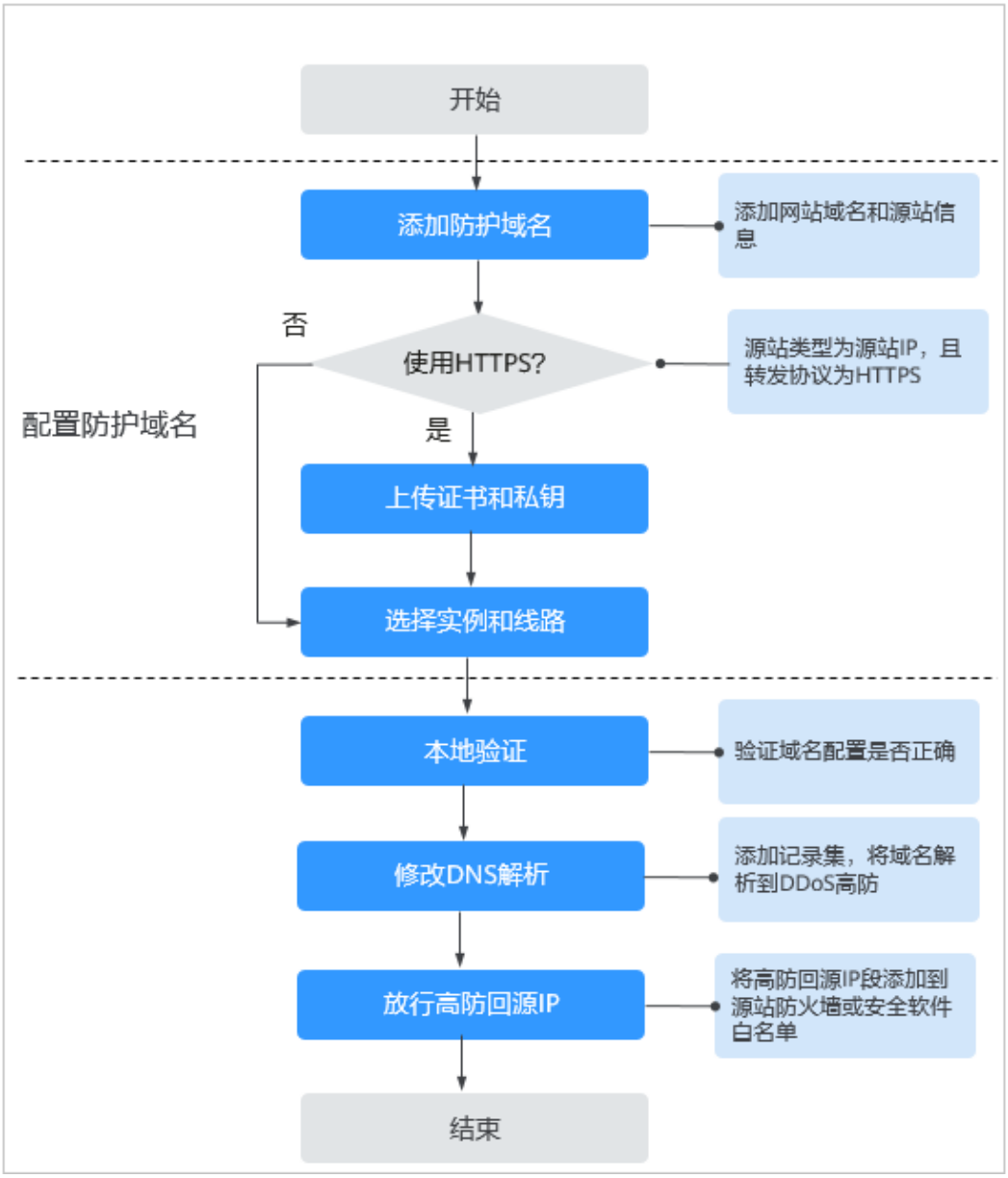
如果您的业务通过域名对外提供服务，域名已通过ICMP备案，您可以将域名接入DDoS高防，获得大流量DDoS攻击防护能力。

域名接入流程

网站类业务接入DDoS高防流程如**图3-7**所示。

版权所有 © 华为技术有限公司

图 3-7 网站类业务接入 DDoS 高防流程



约束与限制

- 服务器协议为HTTPS时，需要上传证书，DDoS高防当前仅支持PEM格式证书。
- CNAME值是根据域名生成的，对于同一个域名，其CNAME值是一致的。
- 源站域名为CNAME时，只支持华为云WAF的CNAME。
- 一个域名可以选择多条线路（高防IP），选择多个高防IP时请确保各高防IP所配置的转发规则个数以及转发规则的转发协议、转发端口和业务类型保持一致。

步骤一：添加防护域名

步骤1 登录管理控制台。

 版权所有 © 华为技术有限公司

步骤2 在页面上方选择“区域”后，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”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-8 域名接入页

步骤4 在域名列表左上方，单击“添加域名”。

步骤5 在添加域名界面配置域名信息，如图3-9所示，相关参数说明如表3-8所示。

图 3-9 配置网站类域名信息

 版权所有 © 华为技术有限公司

表 3-8 域名配置参数说明

参数名称	说明	示例
防护域名	用户的实际业务对外提供服务所使用的域名。 ● 单域名：输入防护的单域名。例如：www.example.com。 ● 泛域名 – 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。 – 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。	单域名：www.example.com 泛域名：*.example.com
源站类型	待添加防护域名的源站的类型。 ● 源站IP：真实服务器的公网IP地址，最多可输入20个IP地址，IP地址间以“,”分隔。 ● 源站域名 当前仅支持华为云WAF CNAME。 ● 转发协议 DDoS高防转发客户端（例如浏览器）请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。 ● 源站端口 DDoS高防转发客户端请求到服务器的业务端口。 **须知** ● 如果待添加域名与其它域名使用同一个高防IP（高防线路）与协议/端口，待添加域名和其它域名的“源站类型”必须保持一致，且注意： – 如果其他域名的“源站类型”为“源站IP”，请确保其它域名已开启Web攻击防护，详细操作请参考**开启WEB基础防护**。 – **如果其他域名的“源站类型”为“源站域名”，请确保其它域名与待添加域名是在同一个WAF区域接入的WAF防护。** – 不要在WAF侧修改或删除接入的第一个源站CNAME信息，如需修改或删除，应先在高防侧删除相应域名信息后，再修改或删除WAF侧的域名信息。 ● 如果“源站类型”选择“源站域名”，请确保您的业务在接入WAF时选择了使用代理，否则接入高防后会导致业务不通。 ● 华为云WAF接入DDoS高防后，如果后续您的业务需要拆除WAF防护，请首先把业务从DDoS高防拆除。	源站IP：XXX.XXX.1.1 转发协议：HTTP 源站端口：80

版权所有 © 华为技术有限公司

参数名称	说明	示例
证书	“源站类型”选择“源站IP”且“转发协议”选择“HTTPS”时，需要上传证书。有关上传证书的详细操作，请参见步骤6。	-

步骤6 （可选）上传证书。

“源站类型”选择“源站IP”且“转发协议”选择“HTTPS”时，您需要导入证书。

您可以在“证书”下拉列表框中选择已有证书，或上传新证书。

上传新证书的操作步骤如下。

1. 单击“上传”，在弹出的“上传证书”对话框中，选择证书上传方式。
   - 手动上传：输入证书名称，粘贴证书和私钥文本内容，如图3-10所示，相关参数说明如表3-9所示。
   - 自动拉取：选择已签发的证书。

须知

建议证书名称长度不超过10个字符，且不包括特殊字符。

图 3-10 上传证书

 版权所有 © 华为技术有限公司

说明

- 当前只支持TLS 1.0、TLS 1.1、TLS 1.2版本证书的上传。
- 当前仅支持PEM格式证书。
- 同一用户的证书名不可重复。

表 3-9 证书参数说明

参数名称	说明
证书文件	- 证书输入格式如下： -----BEGIN CERTIFICATE----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYD VQQGEwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3 ZWkxDzANBgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZz ZXJ2ZXIxIjAgBgkqhkiG9w0BCQEWE3p3YW5nd2VpZGtkQDE2My5jb20wHhcNMTUw MzE4MDMzNjU5WhcNMjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNV BAgTAlpKMQswCQYDVQQHEwJIWjEPMA0GA1UEChMGaHVhda2VpMQ8wDQY..... -----END CERTIFICATE----- - 证书文件内容的复制方法： ▪ PEM格式证书：用文本编辑器直接打开进行复制。 ▪ 非PEM格式证书：先转换成PEM格式，再用文本编辑器直接打开进行复制。
私钥文件	私钥输入格式如下： -----BEGIN RSA PRIVATE KEY----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYDVQQG EwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3ZWkxDzAN BgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZzZXJ2ZXIxIjAg BgkqhkiG9w0BCQEWE3poYW5nd2VpZGtkQDE2My5jb20wHhcNMTUwMzE4MDMzNjU5WhcN MjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAlpKMQswCQYDVQQH EwJIWjEPMA0GA1UEChMGaHVhd2VpMQ8wDQYDVQQLEwZ -----END RSA PRIVATE KEY----- - 私钥文件内容的复制方法： ▪ PEM格式证书：用文本编辑器直接打开进行复制。 ▪ 非PEM格式证书：先转换成PEM格式，再用文本编辑器直接打开进行复制。

2. 单击“确定”。

步骤7 单击“下一步”，选择高防实例与线路，如图3-11所示。

图 3-11 选择高防实例与线路

 版权所有 © 华为技术有限公司

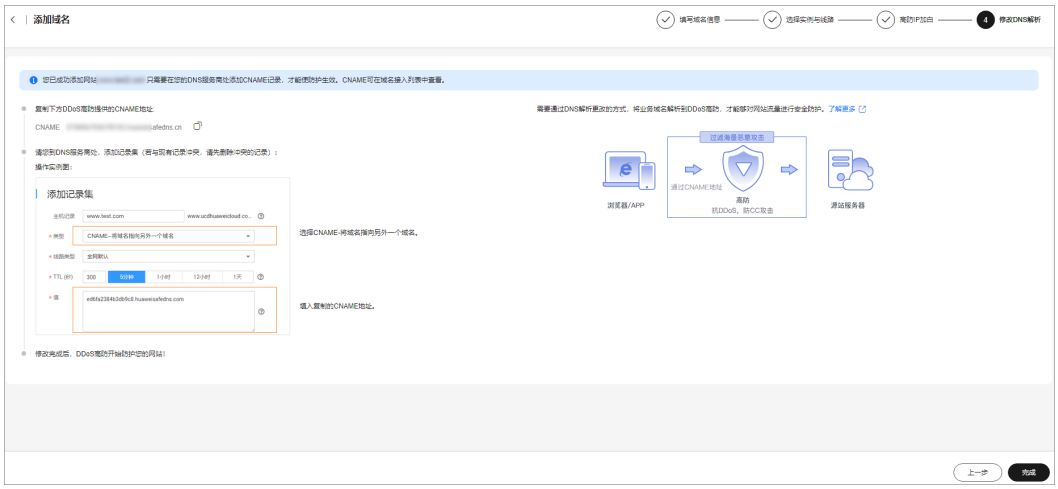
须知

- 一个域名可以选择多条线路（高防IP），选择多个高防IP时请确保各高防IP所配置的转发规则个数以及转发规则的转发协议、转发端口和业务类型保持一致。

步骤8 单击“提交并继续”，弹出如图3-12所示界面。

建议您单击“下一步”，跳过本步骤，后续参照**步骤四：修改DNS解析**完成DNS解析配置。

图 3-12 修改 DNS 解析

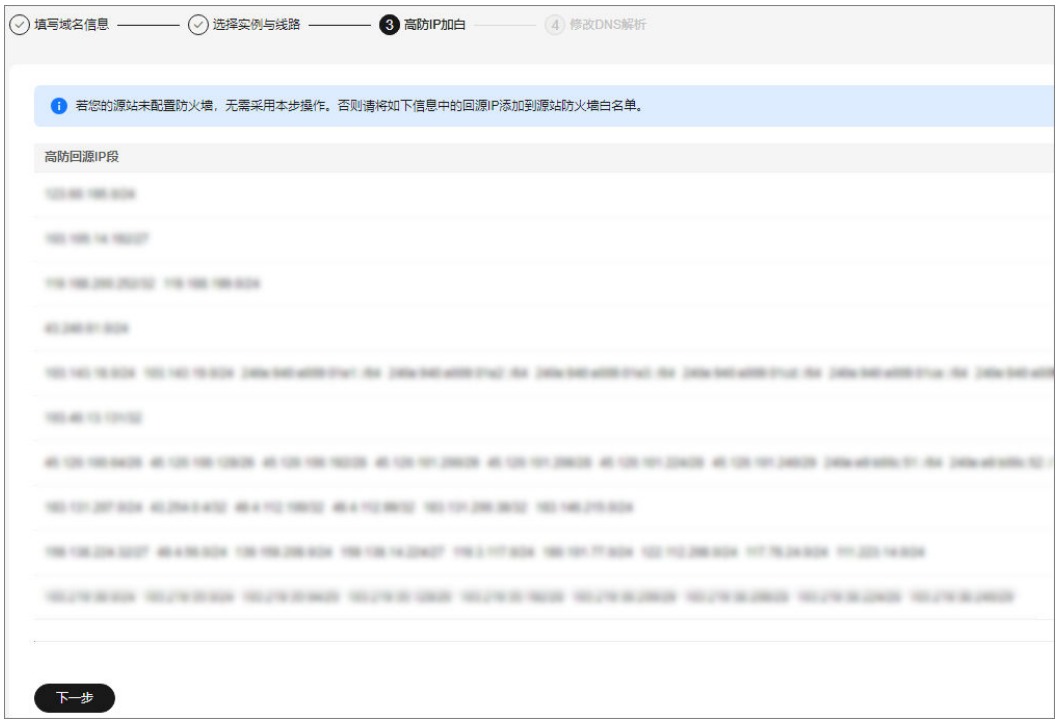


步骤9 单击“完成”，完成防护域名配置。

域名配置完成，系统跳转至“域名接入”界面，您可以在域名列表中查看添加的防护域名。

版权所有 © 华为技术有限公司

图 3-13 高防回源 IP 段



如果源站已配置防火墙或安装安全软件，请将高防回源IP地址段添加到源站的防火墙、ACL或者其他任何安全软件，即对回源IP段设置为放行，以确保高防的回源IP不受源站安全策略影响。有关放行回源IP的详细操作，请参见**步骤二：放行高防回源IP段**。

须知

DDoS高防会替换真实用户IP并且将客户业务的访问流量汇聚到高防回源IP。

- 在没有启用DDoS高防时：对于源站来说真实客户端的地址是非常分散的，且正常情况下每个源IP的请求量都不大。
- 在启用DDoS高防后：由于高防回源的IP段固定且有限，对于源站来说所有的请求都是来自高防回源IP段，因此分摊到每个回源IP上的请求量会增大很多（可能被误认为回源IP在对源站进行攻击）。此时，如果源站有其它防御DDoS的安全策略，很可能对回源IP进行拦截或者限速。例如，最常见的502错误。

----结束

步骤二：放行高防回源 IP 段

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

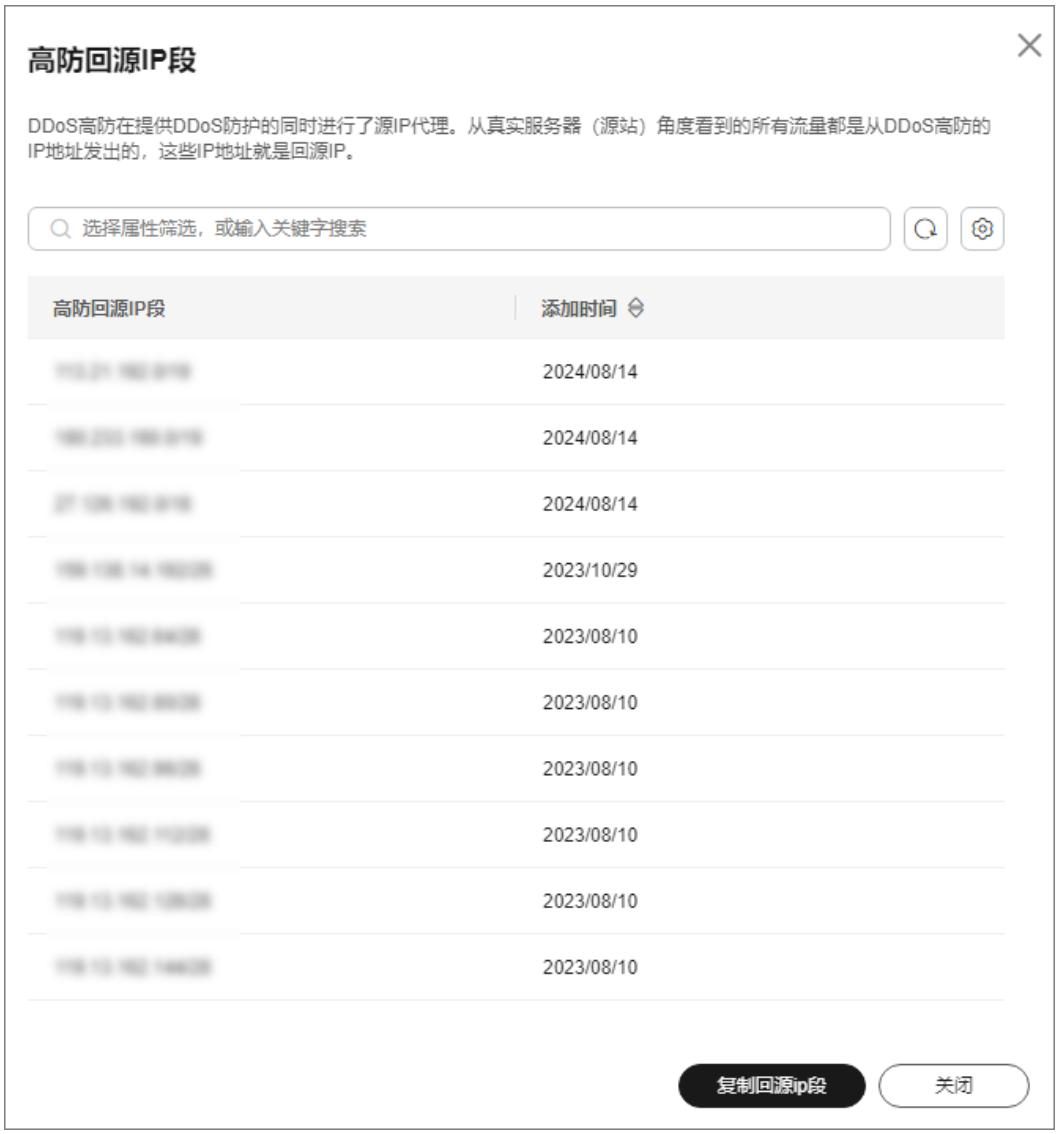
 版权所有 © 华为技术有限公司

图 3-14 域名接入页

步骤4 在域名列表左上角，单击“高防回源IP段”。

步骤5 在弹出的“高防回源IP段”对话框中，查看高防回源IP段信息。

图 3-15 查看高防回源 IP 段



步骤6 将高防回源IP段添加到源站的防火墙或其它防护软件的白名单中。

----结束

 版权所有 © 华为技术有限公司

步骤三：验证域名接入状态

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-16 域名接入页

步骤4 在目标域名的“CNAME”列，单击 ，复制域名的CNAME值。

步骤5 打开Telnet，执行以下命令，测试已接入DDoS高防的源站IP是否能成功建立连接。

telnet *源站IP* 80

以源站IP对外开放的80端口为例。

- 如果可以连通，则说明Telnet公网地址在本机网络环境可用。
- 如果无法连通，则需要更换本地测试机网络环境，因为某些企业网有可能配置过内部网络限制。例如连接手机Wi-Fi热点以切换为运营商网络。

步骤6 执行以下命令，测试域名接入DDoS高防配置是否正确。

telnet *在目标域名的“CNAME”列，单击，复制域名的C...中的CNAME值* 80

- 如果可以连通，说明配置成功。
- 如果无法连通，请确认域名参数是否配置正确。

说明

如您需验证WAF基础防护是否正确开启，请参见：**WAF本地验证**。

----结束

步骤四：修改 DNS 解析

获取防护域名的高防CNAME后，您需要将该CNAME值添加到在云解析服务的记录集中。

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

版权所有 © 华为技术有限公司

图 3-17 域名接入页

步骤4 在目标域名的“CNAME”列，单击 ，复制域名的CNAME值。

步骤5 单击页面左上方的 ，选择“网络 > 云解析服务 DNS”。

步骤6 参考**添加CNAME类型记录集**完成CNAME接入。

----结束

3.4.3 非域名类业务接入 DDoS 高防

如果您的业务没有域名，仅通过公网IP对外提供服务，您可以通过配置转发规则将业务接入DDoS高防。配置转发规则后，高防IP会自动将流量转发到源站IP。进而隐藏源站，避免源站遭受大流量DDoS攻击。

约束与限制

- 同一个源站IP可以添加到多个转发规则中。
- 每个转发规则的“转发协议”和“转发端口”参数是唯一的，不能配置相同的参数。
- 批量配置转发规则，导入文件仅支持“.txt”格式文件。文件中添加的转发规则条目数不允许超过当前配额限制。在配额限制内，单次最大导入条目为200条。

IP 接入 DDoS 高防

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏，选择“DDoS高防 > 转发配置”。

步骤4 选择需要添加转发规则的实例和线路，单击“添加”。

图 3-18 选择实例和线路

步骤5 根据实际填写转发信息。

版权所有 © 华为技术有限公司

表 3-10 参数说明

参数	说明
转发协议	该参数表示用户的实际业务对外提供服务所使用的协议类型，包含： • tcp：是一种面向连接的、可靠的、基于字节流的传输层通信协议。 • udp：是一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。
转发端口	该参数表示用户的实际业务对外提供服务时用于引流的端口。
源站端口	该参数表示用户的实际业务对外提供服务所使用的端口。

版权所有 © 华为技术有限公司

参数	说明
源站IP	该参数表示用户实际业务对外提供服务所使用的公网IP。 • 配置转发规则后，用户需要根据实际的接入方式修改域名，修改完成后高防IP会自动将流量转发到源站IP。 • 最多可输入20个IP地址，IP地址间以“,”分隔。 • 请填写真实有效的公网IP地址。

⚠ 注意

出于安全因素考虑，部分运营商会对下列端口进行拦截，导致无法访问。建议避免使用下列端口：

- TCP：42、135、137-139、444、445、593、1025、1068、1434、3127-3130、3332、4444、4789、4790、5554、5800、5900、6669、9996。
- UDP：135-139、445、593、1026-1028、1068、1433、1434、4444、4789、4790、5554、9996、17185。

步骤6 确认信息无误后，单击“确定”。

----结束

相关操作

- 如果不需要某条转发规则，参考**删除转发规则**。
- 如果需要备份转发规则或者快速修改转发规则的配置信息，参考**导出转发规则**。

3.4.4 接入 DDoS 高防后的防护建议

当业务接入DDoS高防服务后，保障访问安全是非常重要的，因为这关系到源站的安全和业务的连续性。

以下是一些具体的建议，用于保护源站服务器并提升业务的可用性。

防护建议

在不同环节，您可以采取以下措施来降低业务遭受DDoS攻击的风险，提升源站服务器的安全性。主要方法如**表3-11**和**表3-12**所示。

版权所有 © 华为技术有限公司

图 3-19 业务架构示意图

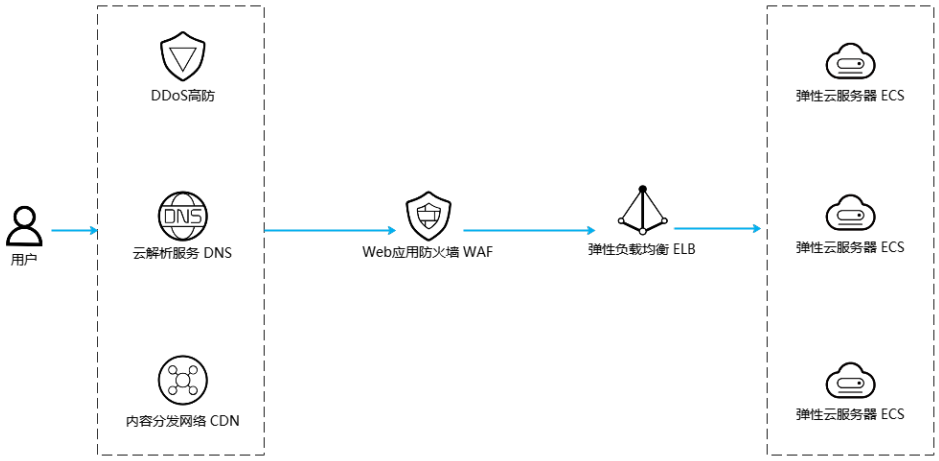


表 3-11 优化安全配置

加固操作	加固说明
配置安全组	将ECS加入安全组，能有效减少无关的访问请求，降低被攻击风险，具体操作请参考**加入安全组**。
使用虚拟私有云	使用虚拟私有云（Virtual Private Cloud，VPC）对ECS进行网络隔离，能有效防止内网的攻击，具体操作请参考**创建虚拟私有云和子网**。
开启弹性伸缩	通过弹性伸缩（Auto Scaling，AS）自动调整ECS资源，可以在受到攻击时自动增加ECS实例，提升处理性能，缓解攻击影响。具体方案请参考**什么是弹性伸缩**。
加强业务监控	通过设置DDoS告警规则，用户可自定义监控目标与通知策略，帮助您及时了解DDoS高防防护状况，从而起到预警作用，具体操作请参考**设置监控告警规则**。
开启CDN调度	使用DDoS调度中心实现DDoS高防和CDN调度，业务正常访问期间，流量就近接入CDN节点加速；仅在业务受到攻击时，流量切换到DDoS高防进行清洗，确保业务稳定，缓解DDoS攻击。具体操作请参考**配置CDN调度策略**。
开启Web应用防护墙	将网站类应用接入Web应用防火墙（WAF），和DDoS高防进行联动防护。流量会先经过DDoS高防，再转发至WAF，实现联动防御，具体操作请参考**使用WAF和DDoS高防实现域名防护**。
开启主机防护	将主机接入企业主机安全（Host Security Service，HSS）进行，实时监测主机中的风险并阻止非法入侵行为，降低主机的主要安全风险。具体操作请参考**接入HSS**。
优化DNS解析	将业务托管到多个DNS服务商，并优化DNS解析策略，能有效缓解流量攻击。业务接入华为云DNS的方法请参考**快速添加网站域名解析**。

版权所有 © 华为技术有限公司

表 3-12 加固源站服务器

类别	业务场景	加固说明
业务部署在华为云ECS	DDoS高防→华为云ECS	在ECS中放行所有DDoS高防的回源IP段，具体操作**配置安全组规则**。 查看DDoS回源IP段的方法请参考**步骤二：放行高防回源IP段**。
	DDoS高防→华为云ELB→华为云ECS	在ELB中设置访问控制策略，具体操作请参考**访问控制管理**。
	DDoS高防→华为云WAF→华为云ECS	在源站ECS中设置访问控制策略，只放行WAF的回源IP段，拒绝其他非WAF回源IP段的访问，具体操作请参考**配置安全组规则**。 查看WAF回源IP段的方法请参考**如何放行云模式WAF的回源IP段**。
业务部署在华为云外的服务器	DDoS高防→华为云外源站服务器	在源站服务器的安全软件中，设置源站保护策略，只放行DDoS高防的回源IP段，拒绝其他非DDoS高防回源IP段的访问。 查看DDoS回源IP段的方法请参考**步骤二：放行高防回源IP段**。

3.5 配置防护策略

3.5.1 防护策略概述

DDoS高防提供了丰富的防护策略，购买实例后，您可以根据业务需要选择适合的防护策略，如**表3-13**所示。

须知

防护策略设置错误可能导致攻击漏防或流量误清洗，请根据业务实际谨慎操作。

表 3-13 防护策略

防护场景	防护策略	章节	说明
基础攻击防护	WEB基础防护	**开启WEB基础防护**	开启后您可以使用高防提供的部分七层CC防护能力，如果您需要通过源站IP方式接入多个不同域名，也依赖该能力的开启。

版权所有 © 华为技术有限公司

防护场景	防护策略	章节	说明
DDoS攻击防护	黑白名单	通过黑白名单拦截/放行指定IP的流量	通过配置IP黑名单和白名单来实现对访问DDoS高防的源IP封禁或者放行，从而限制访问您业务资源的用户。
	协议封禁	封禁指定协议的流量	您可以通过UDP流量封禁功能，一键放行或阻止协议流量访问DDoS高防实例。
	区域封禁	封禁指定区域的流量	DDoS高防支持封禁指定区域的流量，策略生效后，来自该区域的访问流量将被丢弃。
Web CC防护	智能CC	通过智能CC策略防御CC攻击	针对CC攻击场景，自动感知源站压力并生成防护策略。启用特性后，需要10~15分钟进行流量基线学习。
	频率控制	通过频率控制策略缓解CC攻击	通过设置频率控制策略，限制单个IP/Cookie/Referer访问者对防护网站上源端的访问频率，有效缓解CC攻击。

3.5.2 开启 WEB 基础防护

接入防护域名后，可以为域名的源站IP开启WEB基础防护，开启后您可以使用高防提供的部分七层CC防护能力。

须知

- 开启或关闭Web基础防护可能导致业务中断，建议离线配置，避免业务时在线操作。
- 如果无法评估场景风险，请提交工单咨询。

约束与限制

WEB基础防护仅对“网站类”业务且源站类型为“源站IP”的转发规则生效。

开启 WEB 基础防护

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-20 域名接入页

版权所有 © 华为技术有限公司

步骤4 将“WEB基础防护”的状态设置为  ，开启WEB基础防护。

说明

系统默认开启“流量攻击防护”。

----结束

3.5.3 封禁指定区域的流量

DDoS高防支持封禁指定区域的流量，策略生效后，来自该区域的访问流量将被丢弃。

约束与限制

只支持一键放行或阻止海外流量访问， 不支持对某个国家或地区配置流量封禁。

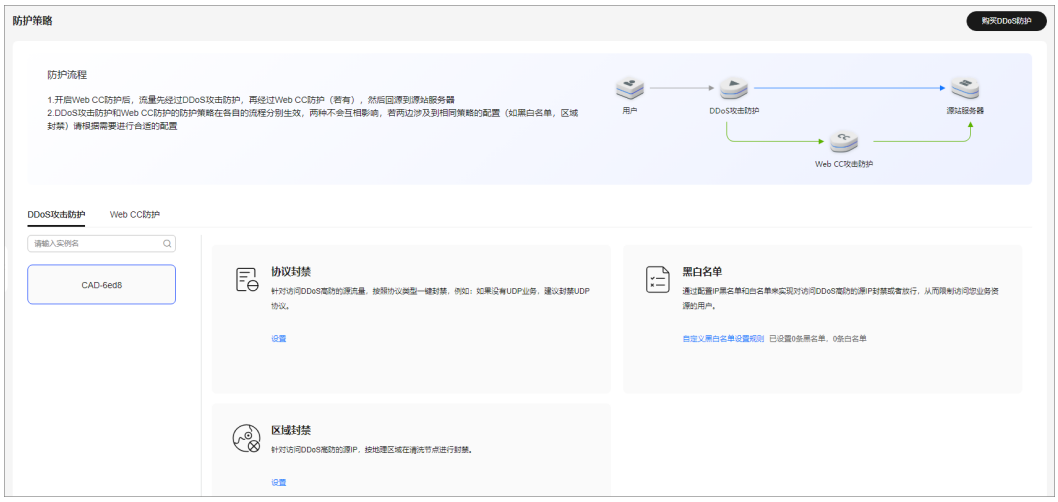
开启区域封禁

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

图 3-21 DDoS 高防防护策略页面



步骤4 选择需要配置区域封禁的实例。

步骤5 在区域封禁配置框中单击“设置”。

步骤6 在弹出的对话框中，选择需要设置区域封禁的路线，并且勾选需要封禁的区域。

版权所有 © 华为技术有限公司

图 3-22 区域封禁设置

步骤7 单击“确定”，完成区域封禁设置。

----结束

3.5.4 封禁指定协议的流量

针对访问DDoS高防的流量，按照协议类型一键封禁。如果没有UDP业务，建议封禁UDP协议。

开启UDP协议封禁后，当访问流量超过2Mbps，将对UDP协议的访问流量进行限速。

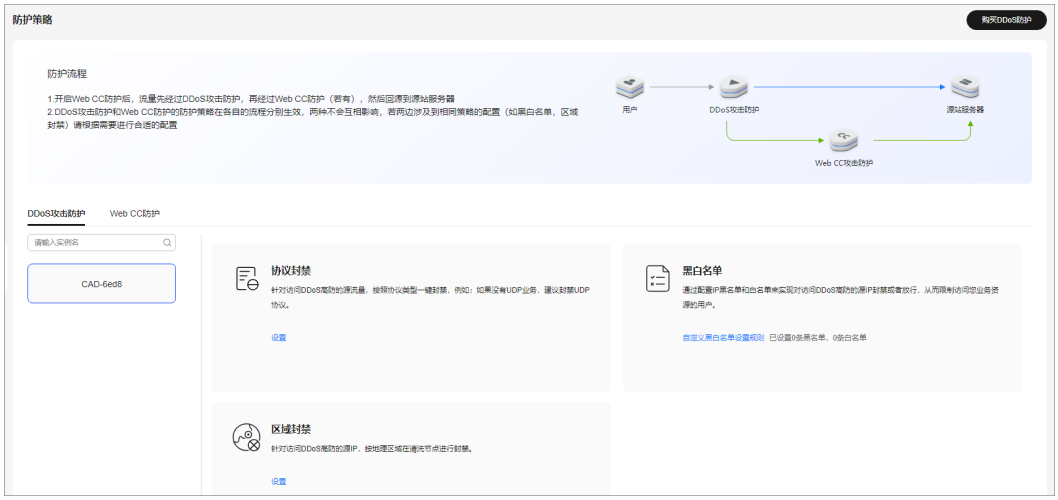
开启协议封禁

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

图 3-23 DDoS 高防防护策略页面



步骤4 选择需要配置协议封禁的实例。

步骤5 在协议封禁配置框中单击“设置”。

 版权所有 © 华为技术有限公司

步骤6 在弹出的对话框中选择需要配置协议封禁的路线，并且将开关调整至，打开协议禁用功能。

图 3-24 协议封禁设置

----结束

3.5.5 通过黑白名单拦截/放行指定 IP 的流量

通过配置IP黑名单和白名单来实现对访问DDoS高防的源IP封禁或者放行，以拦截或放行指定IP的访问请求。

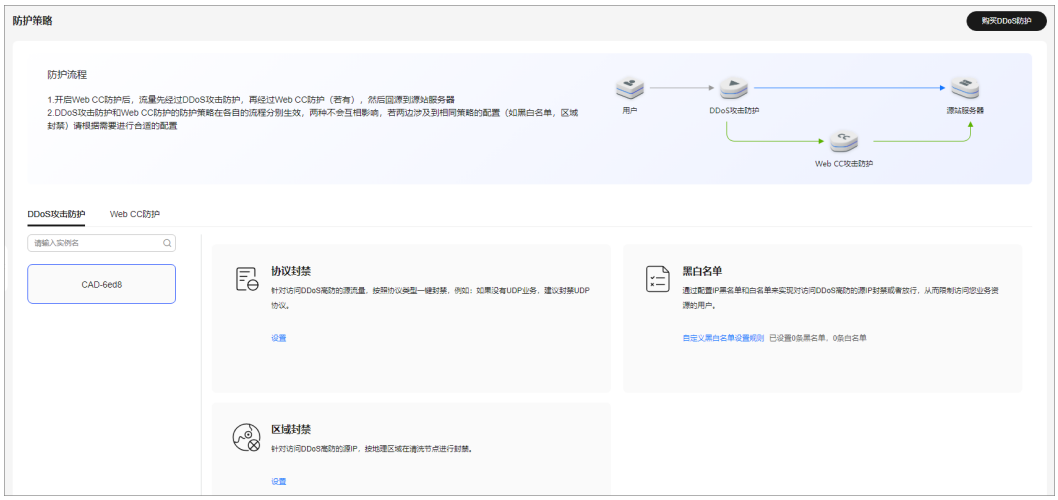
配置黑白名单

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

图 3-25 DDoS 高防防护策略页面



步骤4 选择需要配置黑名单或白名单的实例。

步骤5 配置黑白名单。

版权所有 © 华为技术有限公司

- 配置黑名单
  a. 在“黑白名单”配置框中，单击“自定义黑白名单设置规则”。
  b. 选择“黑名单”页签，单击“添加”。
  c. 在弹出的对话框中，输入需要进行拦截的IP或IP/掩码，如图3-26所示。

  图 3-26 添加黑名单 IP

  说明

  每个实例可添加100个黑名单IP，黑名单中的IP会被拦截。

  d. 单击“确定”。
  在“黑名单IP”界面，单击操作列的“删除”或选择要删除的黑名单执行“批量删除”，被删除的黑名单IP，设备将不再拦截其访问流量。
- 配置白名单
  a. 选择“白名单IP”页签，单击“添加”。
  b. 在弹出的对话框中，输入需要被放行的IP或IP/掩码，如图3-27所示。

版权所有 © 华为技术有限公司

图 3-27 添加白名单 IP

说明

- IP地址/范围以英文逗号隔开，不可重复，个数不能超过剩余配额数。
- 单条规则的掩码范围IPv4不能小于16，IPv6不能小于64，一次只能配置一个子网段。

c. 单击“确定”。

在“白名单IP”界面，单击操作列的“删除”或选择要删除的白名单执行“批量删除”，被删除的白名单IP，设备将不再直接放行其访问流量。

----结束

3.5.6 通过频率控制策略缓解 CC 攻击

您可以通过设置频率控制策略，限制单个IP/Cookie/Referer访问者对防护网站上源端的访问频率，同时支持策略限速、域名限速和URL限速，精准识别CC攻击以及有效缓解CC攻击。

前提条件

网站类业务已开启“WEB基础防护”，具体操作请参考**开启WEB基础防护**。

开启频率控制策略

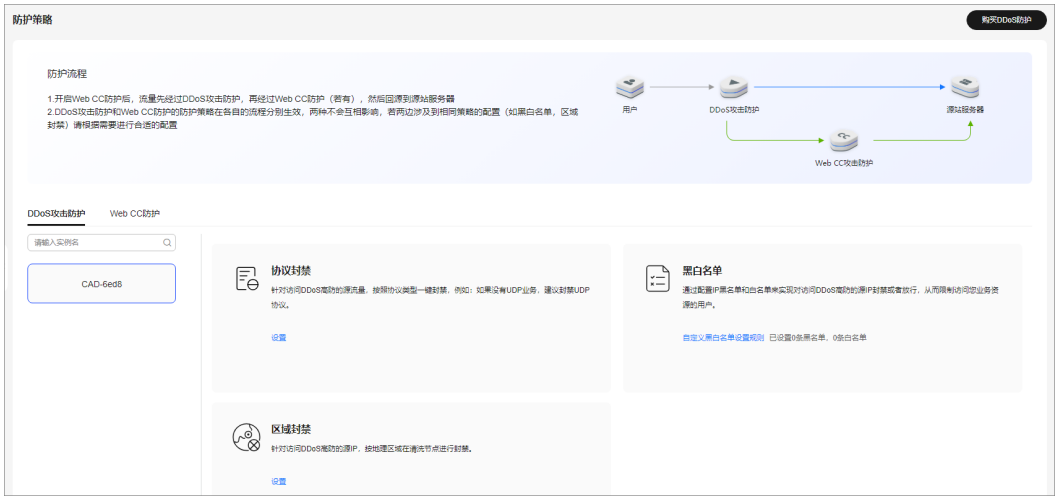
步骤1 **登录管理控制台**。

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

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

版权所有 © 华为技术有限公司

图 3-28 DDoS 高防防护策略页面



步骤4 单击“Web CC防护”页签。

步骤5 选择需要防护的区域和对象后，在“频率控制”下方单击“自定义频率控制规则”。

图 3-29 频率控制

步骤6 单击“添加规则”。

步骤7 配置频率控制规则，如**图3-30**所示。

 版权所有 © 华为技术有限公司

图 3-30 添加频率控制规则

表 3-14 参数说明

参数	说明
规则名称	自定义规则名称。

版权所有 © 华为技术有限公司

参数	说明
限速模式	● “源限速”：对源端限速，如某IP（或用户）的访问频率超过限速频率，就会对该IP（或用户）的访问限速。 – “IP限速”：根据IP区分单个Web访问者。 – “用户限速”：根据Cookie键值或者Header区分单个Web访问者。 – “其他”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。 **说明** 选择“其他”时，“Referer”对应的“内容”填写为包含域名的完整URL链接，仅支持前缀匹配和精准匹配的逻辑，“内容”里不能含有连续的多条斜线的配置，如“///admin”，引擎会将“///”转为“/”。 例如：如果用户不希望访问者从“www.test.com”访问网站，则“Referer”对应的“内容”设置为“http://www.test.com”。 ● “目的限速”：对目的端限速。 – “策略限速”：当多个域名共用一个策略时，该策略下对应的所有域名请求次数合并限速(不区分访问IP)；泛域名防护场景时，该泛域名对应的所有子域名的请求次数合并限速(不区分访问IP)。 – “域名限速”：每个域名单独统计总请求次数，超过设定值则触发防护动作(不区分访问IP)。 – “URL限速”：每个URL请求单独统计请求次数，超过设定值则触发防护动作(不区分访问IP)。
域名聚合统计	“限速模式”选择“目的限速 > 策略限速”时，不需要配置此参数。 默认关闭，开启后，泛域名对应的所有子域名的请求次数合并限速(不区分访问IP)。例如，配置的泛域名为“*.a.com”，会将所有子域名（b.a.com，c.a.com等）的请求一起聚合统计。
用户标识	“限速模式”选择“源限速 > 用户限速”时，需要配置此参数： ● 选择“Cookie”时，设置Cookie字段名，即用户需要根据网站实际情况配置唯一可识别Web访问者的Cookie中的某属性变量名。用户标识的Cookie，不支持正则，必须完全匹配。例如：如果网站使用Cookie中的某个字段name唯一标识用户，那么可以用name字段来区分Web访问者。 ● 选择“Header”时，设置需要防护的自定义HTTP首部，即用户需要根据网站实际情况配置可识别Web访问者的HTTP首部。
限速条件	单击“添加”增加新的条件，至少配置一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。 ● “字段”：根据实际选择。 ● “子字段”：当“字段”选择IPv4、IPv6、Cookie、Header、Params时，请根据实际需求配置子字段。 ● “逻辑”：在下拉列表中选择需要的逻辑关系。 ● “内容”：输入或者选择条件匹配的内容。

版权所有 © 华为技术有限公司

参数	说明
限速频率	单个Web访问者在限速周期内可以正常访问的次数，如果超过该访问次数，系统将根据配置的“防护动作”来处理。 “全局计数”：根据不同的限速模式，将已经标识的请求在一个或多个节点上的计数聚合。默认为每节点单独计数，开启后本区域所有节点合并计数。“IP限速”不能满足针对某个用户进行限速，需要选择“用户限速”或“其他”的Referer限速，此时标识的请求可能会访问到不同的节点，开启全局计数后，将请求访问的一个或多个节点访问量聚合，达到全局统计的目的。
防护动作	当访问的请求频率超过“限速频率”时，可设置以下防护动作： ● “人机验证”：表示超过“限速频率”后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。人机验证目前支持英文。 ● “阻断”：表示超过“限速频率”将直接阻断。 ● “动态阻断”：上一个限速周期内，请求频率超过“限速频率”将被阻断，那么在下一个限速周期内，请求频率超过“放行频率”将被阻断。 ● “仅记录”：表示超过“限速频率”将只记录不阻断。 ● “JS挑战”：表示DDoS高防向客户端返回一段正常浏览器可以自动执行的JavaScript代码。如果客户端正常执行了JavaScript代码，则DDoS高防在一段时间（默认30分钟）内放行该客户端的所有请求（不需要重复验证），否则拦截请求。
锁定验证	当“防护动作”选择“人机验证”时，需要配置该参数。 当人机验证未通过时，在设定时间内的访问都要进行验证。
放行频率	当“防护动作”选择“动态阻断”时，可配置放行频率。 如果在一个限速周期内，访问超过“限速频率”触发了拦截，那么，在下一个限速周期内，拦截阈值动态调整为“放行频率”。 “放行频率”需要小于等于“限速频率”。
生效时间	默认为“立即生效”。
阻断时长	当“防护动作”选择“阻断”时，可设置阻断后恢复正常访问页面的时间。
阻断页面	当“防护动作”选择“阻断”时，需要设置该参数，即当访问超过限速频率时，返回的错误页面。 ● 当选择“默认设置”时，返回的错误页面为系统默认的阻断页面。 ● 当选择“自定义”，返回错误信息由用户自定义。
页面类型	当“阻断页面”选择“自定义”时，可选择阻断页面的类型“application/json”、“text/html”或者“text/xml”。
页面内容	当“阻断页面”选择“自定义”时，可设置自定义返回的内容。

版权所有 © 华为技术有限公司

步骤8 单击“确定”。

----结束

后续操作

- 开启频率控制防护：在“Web CC防护”页面，将“频率控制”状态设置为 。
- 关闭频率控制防护：在“Web CC防护”页面，将“频率控制”状态设置为 。

3.5.7 通过智能 CC 策略防御 CC 攻击

开启智能CC防护后，DDoS高防中的压力学习模型会根据源站返回的HTTP状态码和时延等来实时地感知源站的压力，从而识别源站是否被CC攻击了，DDoS高防再根据异常检测模型实时地检测源站在HTTP协议上的特征的异常行为，然后基于这些异常特征，使用AI算法生成精准防护规则和CC防护规则，来防御CC攻击。

约束与限制

该功能目前处于内测阶段，仅部分用户可以试用，其他用户需要**提交工单**申请开通。

前提条件

网站类业务已开启“WEB基础防护”，具体操作请参考**开启WEB基础防护**。

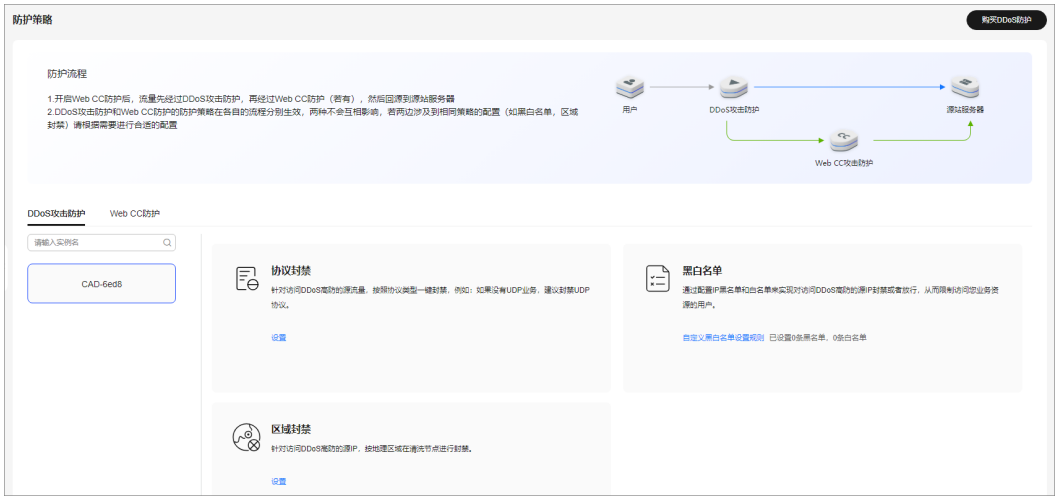
开启智能 CC

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

图 3-31 DDoS 高防防护策略页面

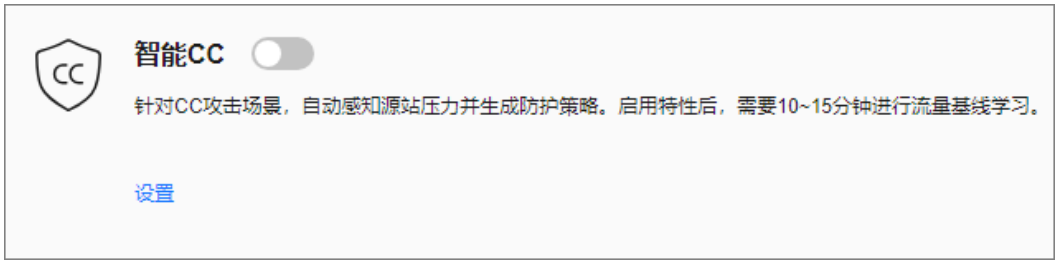


 版权所有 © 华为技术有限公司

步骤4 单击“Web CC防护”页签。

步骤5 选择需要防护的区域和对象后，在“智能CC”下方单击“设置”。

图 3-32 智能 CC



步骤6 根据实际设置防护策略，如表3-15所示。

图 3-33 智能 CC 设置

表 3-15 参数说明

参数	说明
模式	• 预警：仅记录日志，不进行阻断。 • 防护：阻断恶意请求，并记录日志。
等级	• 宽松：仅拦截已知的特定恶意攻击，适合于比较大型的网站，对正常请求不会造成误杀。 • 正常：适合请求量平稳，服务器处理性能有一定冗余的场景。检测待恶意攻击时，开启智能防御，对正常业务影响极低，推荐使用该等级。 • 严格：适合网站性能差，防护效果不佳的情况下开启，可能存在部分误杀。

步骤7 在“Web CC防护”页面，将“智能CC”状态设置为  ，开启防护。

----结束

3.6 开启 DDoS 攻击告警通知

开启DDoS高防告警通知后，当出现以下情况时，您将接收到告警通知信息（接收消息方式由您设置）：

版权所有 © 华为技术有限公司

- IP遭受DDoS攻击。
- DDoS攻击峰值超过保底防护带宽而产生弹性计费。

如果您需要详细地监控服务各项指标，推荐您使用云监控服务设置监控告警规则和事件告警通知，具体操作请参考**查看监控指标**。

前提条件

- 消息通知服务为付费服务，价格详情请参见**SMN价格详情**。
- 在开启告警通知前，建议您先以管理员身份在“消息通知服务”中创建“消息主题”，详细操作请参见。

开启告警通知

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 告警通知”，进入“告警通知”页面。

步骤4 在“告警通知设置”页面，选中“DDoS攻击”。

图 3-34 “告警通知设置”对话框

单击下拉列表选择已创建的主题或者单击“查看消息通知服务主题”创建新的主题，用于配置接收告警通知的终端。

说明

只支持在华北-北京四、中国-香港创建的主题。

单击“查看主题”创建新主题的操作步骤如下：

1. 参见**创建主题**创建一个主题。
2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。

版权所有 © 华为技术有限公司

3. 确认订阅。添加订阅后，完成订阅确认。

更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。

步骤5 单击“确定”，告警通知设置完成。

说明

如需关闭告警通知，在图3-34中，取消勾选“DDoS攻击”后，单击“确定”。

----结束

3.7 开启日志记录

启用DDoS高防功能后，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AAD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，具体操作请参考**管理日志组**和**管理日志流**。

开启 DDoS 高防日志

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“安全与合规 > DDoS防护AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 概览”，进入“概览”页面。

步骤4 单击“日志”，开启全量日志  ，并选择日志组和日志流，相关参数说明如图3-35所示。

 版权所有 © 华为技术有限公司

图 3-35 配置 DDoS 高防日志

表 3-16 日志配置参数

参数	参数说明
企业项目	选择已创建的企业项目。
日志组Region	选择日志组所属的Region
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。
实例攻击日志	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。 实例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，字段说明如**表3-17**所示。
实例攻击详情	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。 实例攻击详情记录攻击开始时间、结束时间、攻击状态、攻击类型等信息，字段说明如**表3-18**所示。

步骤5 单击“确定”，日志配置成功。

您可以在LTS管理控制台查看防护日志。

----结束

日志字段说明

本章节介绍了DDoS高防日志包含的日志字段。

 版权所有 © 华为技术有限公司

表 3-17 实例攻击日志字段说明

字段	说明
ip	被攻击IP。
ip_id	被攻击IP的ID。
attack_type	攻击的类型。
attack_protocol	该字段尚未使用，默认是0。
attack_start_time	攻击开始时间，毫秒级时间戳。
attack_status	攻击状态。 ● ATTACK：攻击中。 ● NORMAL：攻击结束。
drop_kbits	分钟级别的最大攻击流量，单位“bit”。
attack_pkts	分钟级别的最大攻击报文数。
duration_elapse	已结束安全事件的持续时间，单位“秒”。
end_time	攻击结束时间，毫秒级时间戳。未结束的安全事件，该字段为0。
max_drop_kbps	攻击流量的峰值，单位“kbps”。
max_drop_pps	攻击报文的峰值，单位“pps”。

表 3-18 实例攻击详情字段说明

字段	说明
attackStatus	攻击状态。
attackType	攻击状态。 ● ATTACK：攻击中。 ● NORMAL：攻击结束。
attackTypeDescCn	攻击类型（中文）。
attackTypeDescEn	攻击类型（英文）。
attackUnit	攻击单位。
attacker	攻击来源。
attackerKbps	攻击流量峰值，单位“kbps”。
attackerPps	攻击流量峰值，单位“pps”。

版权所有 © 华为技术有限公司

字段	说明
direction	日志方向。 ● inbound：入方向。 ● outbound：出方向。
dropKbits	丢弃的流量总数，单位“kbits”。
dropPackets	丢弃的报文总数。
duration	攻击持续时间，单位“秒”。
handleTime	处理日志时间。
logTime	日志时间。
logType	日志类型。
maxDropKbps	IP丢弃流量峰值，单位“kbps”。
maxDropPps	IP丢弃流量峰值，单位“pps”。
port	端口号。
startTimeAlert	异常开始时间。
timeScale	时间标识（处理分钟级或小时级数据的标识）。
valid	是否成功解析到日志。
writeTime	持久化时间。
zoneIP	防护IP。
startTimeAttack	攻击开始时间。
startTimeKey	对于同一个攻击不同时间的唯一标识。

3.8 查看数据报表

业务接入DDoS高防后，您可以通过查看DDoS攻击防护数据报表和CC攻击防护数据报表，了解当前业务的网络安全状态。

在“概览”页面，您可以查看以下数据信息：

- DDoS攻击防护

  可以查看指定时间段的安全总览信息、流量趋势、协议分布、连接数、攻击分布、安全事件、黑洞事件等信息。
- CC攻击防护

  可以查看指定时间段的请求次数、攻击次数、带宽、攻击分布、攻击源、攻击事件等信息。

版权所有 © 华为技术有限公司

查看 DDoS 攻击防护报表

步骤1 登录管理控制台。

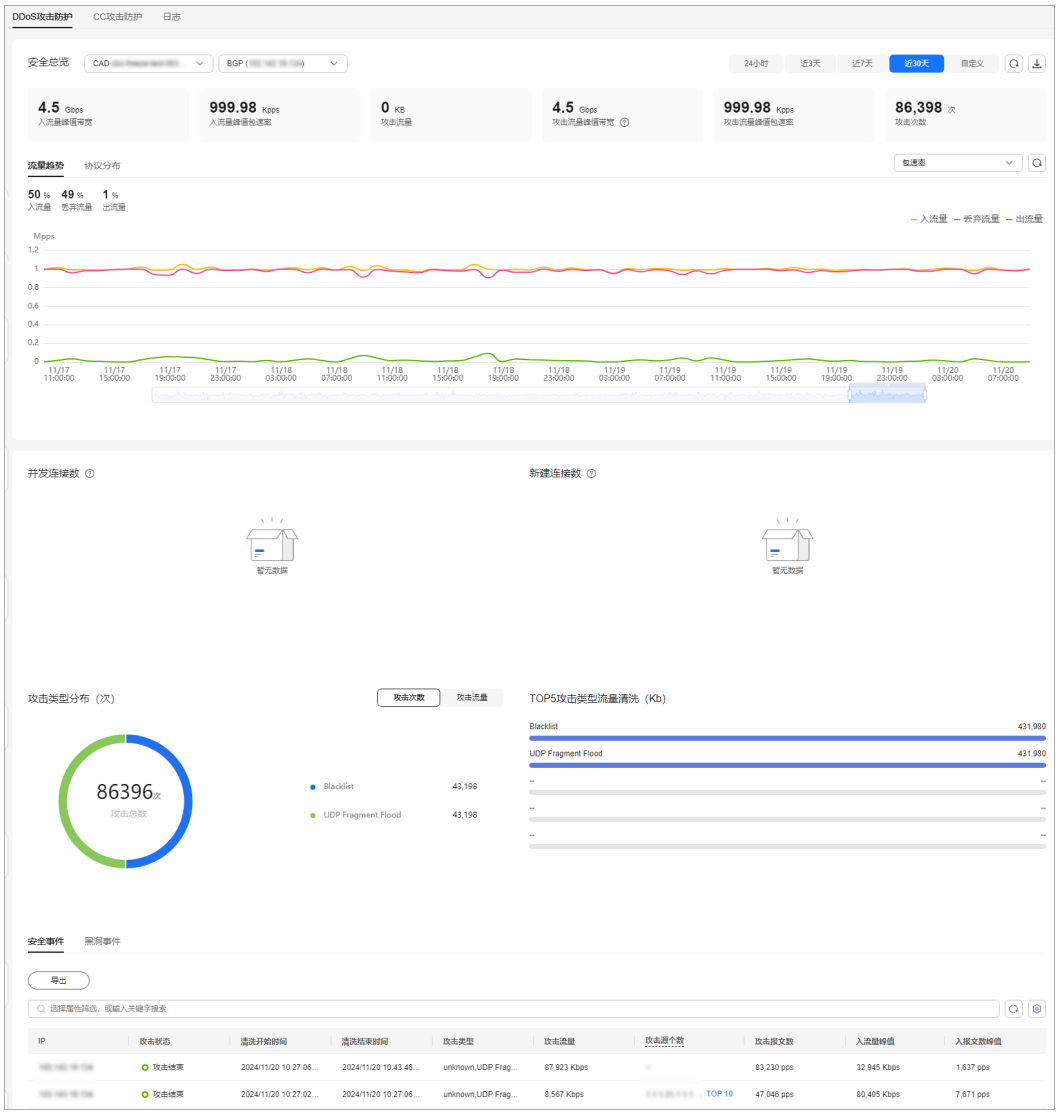
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 概览”，进入“概览”页面。

步骤4 单击“DDoS攻击防护”页签。

步骤5 选择待查看的实例名称、线路地址和历史时间段（24小时、近3天、近7天、近30天、自定义，其中，自定义可以查看90天内的防护日志），相关参数说明如表3-19所示。

图 3-36 DDoS 攻击防护



 版权所有 © 华为技术有限公司

表 3-19 DDoS 攻击参数说明

参数	说明
入流量峰值带宽	每秒访问指定实例指定IP的最高流量。
入流量峰值包速率	入方向流量每秒流入数据包的最大值。
攻击流量峰值带宽	每秒攻击指定实例指定IP的最高流量。此处特指攻击生成了安全事件的防护过程中产生的攻击流量。
攻击流量峰值包速率	攻击流量每秒流入数据包的最大值。
攻击次数	DDoS攻击指定实例指定IP的次数。
流量趋势	入流量、出流量、丢弃流量的占比及分布趋势。
协议分布	流量中TCP、UDP、ICMP等协议的占比及分布趋势。
并发连接数	查看同时访问的连接数。
新建连接数	查看新建访问的连接数。
攻击类型分布	查看攻击事件类型。 ● 选择“攻击次数”，可查看指定域名被攻击的类型、攻击的次数、以及攻击占比。 ● 单击“攻击流量”中的其中一个颜色区域，可查看指定域名被攻击的类型、攻击的流量、以及流量占比。
TOP5攻击类型流量清洗	TOP5攻击类型次数统计。
安全事件	查看DDoS攻击事件。 ● 单击攻击源IP后的“详细”，可以查看完整的攻击源IP列表。 ● 攻击中的事件，单击“查看动态黑名单”，可以查看攻击中的黑名单列表。 ● 单击“导出”，可导出安全事件报告。 **说明** 关于DDoS攻击事件报表中攻击源的字段，请您注意以下几点说明： ● 进行中的攻击事件可能不展示攻击源。 ● 一些只包含部分攻击类型的攻击事件不含攻击源。 ● 攻击源随机采样，不是全量的攻击源信息。
黑洞事件	查看被封堵的IP、状态，封堵开始和结束的时间。 单击“导出”，可导出黑洞事件报告。

版权所有 © 华为技术有限公司

说明

在防护日志页面的流量或报文的图表中，不同的查询时间间隔对应的展示粒度不同，具体如下：

- 查询时间＜20分钟：展示粒度为1分钟。
- 20分钟＜查询时间＜40分钟：展示粒度为2分钟。
- 40分钟＜查询时间＜60分钟：展示粒度为3分钟。
- 1小时＜查询时间≤6小时：展示粒度为5分钟。
- 6小时＜查询时间≤24小时：展示粒度为10分钟。
- 1天＜查询时间≤7天：展示粒度为30分钟。
- 7天＜查询时间≤15天：展示粒度为1小时。
- 15天＜查询时间≤30天：展示粒度为14小时。

----结束

查看 CC 攻击防护报表

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 概览”，进入“概览”页面。

步骤4 单击“CC攻击防护”页签。

步骤5 选择需要查看域名和时间范围，相关参数说明如表3-20所示。

版权所有 © 华为技术有限公司

图 3-37 CC 攻击防护

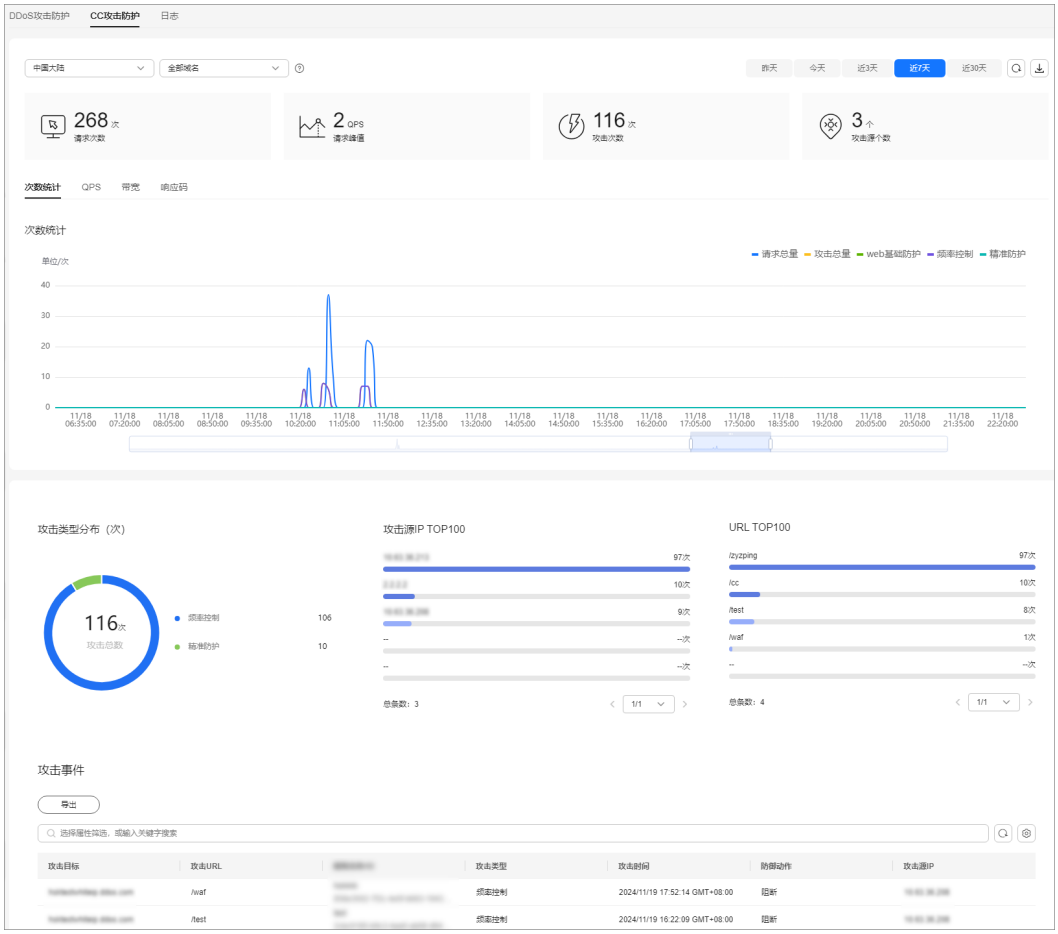


表 3-20 CC 攻击防护参数说明

参数	说明
请求次数	访问者访问指定域名的总次数。 如果“全部域名”下拉列表中选择的是“全部域名”，则统计的是访问全部已开启WAF的域名的总次数。
请求峰值	每秒访问指定域名的最高次数。 如果“全部域名”下拉列表中选择的是“全部域名”，则统计的是每秒访问全部已开启WAF的域名的最高次数。
攻击次数	攻击指定域名的次数。
攻击源个数	攻击指定域名的攻击源个数。
次数统计	按照次数统计的请求趋势图，包括请求总量、攻击总量、不同攻击的次数分布。

版权所有 © 华为技术有限公司

参数	说明
QPS	QPS（Queries Per Second）即每秒钟的请求量，例如一个HTTP GET请求就是一个Query。 平均值：域名平均每秒钟的请求量。 峰值：域名每秒请求的最大值。
带宽	平均值：查看出带宽和入带宽的平均值。 峰值：查看出带宽和入带宽的峰值。
响应码	• DDoS高防响应：DDoS高防返回给客户端的响应码以及响应次数。 • 源站响应：源站返回给DDoS高防的响应码以及响应次数。
攻击类型分布	查看不同攻击的次数及占比。 • 单击“攻击类型分布”中的其中一个颜色区域，可查看指定域名被攻击的类型、攻击的次数、以及攻击占比。 • 当不需要展示某种类型的攻击时，单击事件分布图右侧攻击类型对应的颜色方块，取消在事件分布圆环中的展示。
攻击源IP TOP100	排名前100的攻击源IP数据。
URL TOP100	排名前100的攻击URL数据。
攻击事件	攻击事件具体参数请参考**表3-21**。 单击“导出”，可导出攻击事件报告。

表 3-21 攻击事件参数说明

参数	说明
攻击目标	被攻击的域名。
攻击URL	攻击的防护域名的URL，如“/4b87ef”。
攻击类型	发生攻击的类型，如“频率控制”。
攻击时间	本次攻击发生的时间。
防御动作	防护配置中设置的防护动作。 • 阻断 • 仅记录 • 人机验证
攻击源IP	攻击者的IP地址。

----结束

版权所有 © 华为技术有限公司

3.9 实例管理

3.9.1 查看实例信息

开通DDoS高防后，您可以通过实例列表查看已购买的实例信息，确保实例状态正常。

查看 DDoS 高防实例信息

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在实例列表界面，查看高防实例信息，相关参数说明如表3-22所示。

图 3-38 实例信息

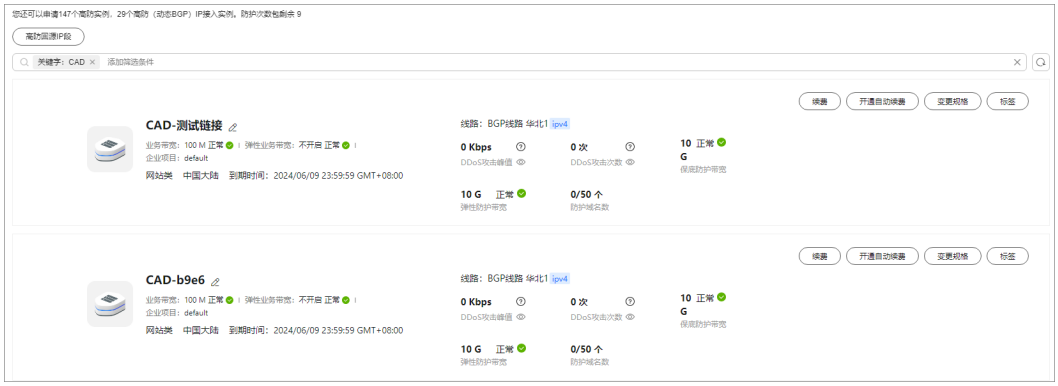


表 3-22 实例参数说明

参数名称	说明
实例名称	高防实例的名称，单击名称右边的，可以更改实例名称。
业务带宽	实例的业务带宽和状态。
企业项目	实例所属的企业项目。
接入类型	接入实例的防护对象类型。
防护区域	实例防护的区域范围。
线路	线路接入资源、业务接入点和IP类型。
DDoS攻击峰值	当日的DDoS攻击峰值。
DDoS攻击次数	当日的DDoS攻击次数。
实例规格信息	保底防护带宽、弹性防护带宽、防护域名数。

版权所有 © 华为技术有限公司

----结束

3.9.2 升级实例规格

购买实例后，如果您的业务有变化，对实例规格有更高要求，您可以通过升级规格操作，以满足更大的DDoS攻击防护需求。

费用说明

变更规格会引起费用的变化，详细的费用说明请参见**变更资源费用说明**。

约束与限制

- 如果客户购买的是非BGP线路的三线实例（当前已不售卖），不提供升级规格功能，需要修改弹性带宽值请**提交工单**进行调整。
- 不支持升级时更换线路。
- 已到期的实例不支持升级。
- 已冻结的实例不支持升级。

升级 DDoS 高防实例规格

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在目标实例“实例名称”所在行，单击“变更规格”。

步骤5 在“DDoS高防变更规格”界面，调整实例规格。

图 3-39 域名接入类型实例

版权所有 © 华为技术有限公司

图 3-40 IP 接入类型实例

表 3-23 参数说明

参数	说明
保底防护带宽	保底防护带宽是指用于防御攻击的保底带宽。如果攻击峰值小于等于客户购买的保底防护带宽，客户无需支付额外费用。
弹性防护带宽	弹性防护带宽是用于防御攻击的最大可用带宽。弹性防护带宽并不是在保底防护带宽之上的增量，当用户选定的弹性防护带宽和保底防护带宽相同时则不具备弹性防护能力。
业务带宽	业务带宽是指为高防机房清洗后回源给源站的干净业务流量带宽。每个实例免费赠送100Mbps业务带宽，可以付费增加，如果高防机房在华为云外，建议购买的高防业务带宽规格大于或等于源站出口带宽。
防护域名数	实例为域名接入类型时，才有该参数。
转发规则数	实例为IP接入类型时，才有该参数。

步骤6 单击“提交”，界面会判断选择的规格是否有变化，如果没有变化则弹出提示“规格无变化，无需升级”。否则跳转到下一步的确认界面。

步骤7 单击“去支付”，付款成功后，系统跳转至“支付成功”的界面。

----结束

3.9.3 开通自动续费

如果您购买实例时，开通了自动续费功能。当服务期满时，系统会自动按照购买的实例周期进行续费。您可以根据业务需求，选择开通自动续费功能。

说明

开通自动续费的资源可随时进行手动续费，手动续费成功后自动续费依然有效，系统将在资源新的到期时间前的第7天开始扣款。有关自动续费的详细介绍，请参见**续费规则说明**。

版权所有 © 华为技术有限公司

前提条件

请确认开通自动续费的账号同时具有“AAD FullAccess”和“BSS Administrator”角色权限。

开通自动续费

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在需要开通自动续费的实例所在行，单击“开通自动续费”，进入“设为自动续费”页面。

步骤5 选择续费时长和自动续费次数。

图 3-41 开通自动续费

步骤6 单击“开通”，按界面提示信息开通自动续费。

----结束

3.9.4 配置实例标签

标签由标签键和标签值组成，用于标识云资源。当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。DDoS实例支持配置标签，方便管理实例。

配置 DDoS 高防实例标签

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在目标实例所在行，单击“标签”。

版权所有 © 华为技术有限公司

图 3-42 设置标签

步骤5 在标签添加页面，单击“添加标签”。

步骤6 选择“标签键”和“标签值”。

- 手动设置标签：手动输入标签键和标签值。
- 选择已有标签：选择已有的标签。

图 3-43 添加标签

说明

如您的组织已经设定本服务的相关标签策略，则需按照标签策略规则为资源添加标签。标签如果不符合标签策略的规则，则可能会导致标签添加失败，请联系组织管理员了解标签策略详情。

步骤7 单击“确定”。

----结束

3.10 域名管理

3.10.1 查看域名信息

域名接入DDoS高防后，您可以通过域名接入列表查看已接入的域名信息，确保防护状态正常。

查看域名信息

步骤1 登录管理控制台。

 版权所有 © 华为技术有限公司

步骤2 在页面上方选择“区域”后，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”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-44 域名接入页

步骤4 查看域名信息。

表 3-24 参数说明

参数名称	说明
域名	防护的域名，单击域名可查看域名的Web CC防护详情。
CNAME	• 域名通过CNAME解析的CNAME信息。 • 单击，可以复制“CNAME”。
实例与线路	• 域名的CNAME接入状态。 • 域名的实例线路信息，单击“查看详情”，可以查看域名配置的实例线路的详细信息。 • 开启“CNAME自动调度”，高防IP被黑洞时将自动进行DNS调度来保证业务的可用性。
源站IP/域名	填写的源站IP/域名。
业务类型	• 域名的业务类型。 • “HTTPS/WebSockets”证书的“更换”，单击“更换”，可以更新域名绑定的证书。详细操作，请参见**更新证书**。
安全防护	域名的流量攻击防护、WEB基础防护和CC防护开启状态。 • 对于配置了“源站IP”的“网站类”业务，用户可以为域名开启网站防护功能。 • 对于配置了“源站域名”的“网站类”业务，无需为域名开启网站防护功能。 • 对于“非网站类”业务，系统只提供默认开启的流量攻击防护。
企业项目	实例所属的企业项目。

----结束

 版权所有 © 华为技术有限公司

3.10.2 修改域名的高防 IP 解析线路

业务接入DDoS高防后，如果您需要将域名切换到其他解析线路进行防护，可以通过修改域名的高防IP解析线路实现。

须知

- 修改高防IP解析线路可能导致防护失效或业务中断，建议在新线路验证通过之后再进行线路解析修改。
- 如果无法评估场景风险，请**提交工单**咨询。

约束与限制

域名的高防IP解析线路修改后约5分钟后才能生效。

修改域名解析线路

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-45 域名接入页

步骤4 在域名所在行的“实例与线路”列，单击“查看详情”。

步骤5 修改域名的高防IP解析线路，操作步骤如下：

- 关闭域名的高防IP解析线路。

  在线路详情页面，将需要关闭的线路的“线路解析开关”变更为 ，关闭该高防实例和线路下高防IP的域名解析功能。域名解析功能关闭后，用户仍然可以使用该高防IP的A记录方式。

- 新增域名的高防解析线路。

  a. 在线路详情页面，单击“新增实例线路”。

  b. 在“新增实例线路”对话框中，勾选新增的实例和线路，单击“确定”。

  c. 将“线路解析开关”变更为 ，开启新增的高防实例和线路下高防IP的域名解析功能。

- 删除域名的高防解析线路。

  a. 关闭待删除的线路。

版权所有 © 华为技术有限公司

b. 在关闭后的线路所在行，单击“删除线路”。

c. 单击“确定”。

- 全量规则导出。

  在线路详情页面，单击“全量规则导出”，即可导出该域名的所有线路转发规则。

----结束

3.10.3 修改域名业务配置

域名接入DDoS高防后，如果源站信息发生变更，可通过域名接入列表修改接入的源站信息。

须知

- 修改源站IP等信息可能导致防护失效或业务中断，请谨慎操作。
- 如果无法评估场景风险，请**提交工单**咨询。

约束与限制

- 如果要与其它域名复用同一个高防IP与端口，请确保其它域名与当前域名的“源站类型”相同。
- 如果要将域名的“源站类型”从“源站IP”改为“源站域名”时，请确保当前域名的“WEB基础防护”处于关闭状态。

修改域名业务配置

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-46 域名接入页

步骤4 在需要修改域名业务配置的域名所在行的“操作”列，单击“编辑”。

步骤5 在弹出的对话框“域名业务配置编辑”中，修改域名业务配置。

版权所有 © 华为技术有限公司

图 3-47 修改域名业务配置

步骤6 单击“确定”。

----结束

3.10.4 修改 TLS 配置

域名接入DDoS高防后，您可以通过域名接入列表，修改HTTPS证书配套的最低TLS版本和加密算法。

说明

低于最低TLS版本的请求将无法正常访问。

修改 TLS 配置

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

版权所有 © 华为技术有限公司

图 3-48 域名接入页

步骤4 在目标域名的“TLS配置”后，单击“编辑”。

步骤5 选择TLS版本和加密套件后，单击“确认”。

图 3-49 配置字段

----结束

3.10.5 设置 HTTP2 协议

如果您的域名支持HTTP2协议，您可以通过域名接入页面开启HTTP2防护。

约束与限制

- 只有转发协议为HTTPS且开启了WEB基础防护的域名才能设置HTTP2协议。
- 当客户端TLS版本不高于TLS 1.2时，HTTP2才生效。

前提条件

接入域名已开启WEB基础防护，具体操作请参考**开启WEB基础防护**。

版权所有 © 华为技术有限公司

开启 HTTP2 协议

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-50 域名接入页

步骤4 在目标域名的“HTTP2协议”后，单击“编辑”。

步骤5 根据实际设置HTTP2协议。

图 3-51 HTTP2 协议

步骤6 单击“确定”。

----结束

3.10.6 设置字段转发

DDoS高防支持为接入的域名配置header字段转发，将添加的字段插入到header中转给源站。

通过在回源请求中添加header字段，可以标记经过DDoS高防的请求，用于服务统计分析。

约束与限制

- 最多支持配置8个Key/Value值。
- 配置的Key值不能跟nginx原生字段重复。
- Value值可以自定义一个字符串，也可以配置为以$开头的变量。以$开头的变量仅支持配置如下字段：

```
$time_local
$request_id
```


版权所有 © 华为技术有限公司

```
$connection_requests
$tenant_id
$project_id
$remote_addr
$remote_port
$scheme
$request_method
$http_host
$origin_uri
$request_length
$ssl_server_name
$ssl_protocol
$ssl_curves
$ssl_session_reused
```

设置字段转发

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-52 域名接入页

步骤4 在目标域名所在行的“高级配置”列，单击“编辑”。

步骤5 输入Key/Value值，单击“添加”。

 版权所有 © 华为技术有限公司

图 3-53 配置字段

步骤6 单击“确认”。

----结束

3.10.7 批量接入域名

如果您有多个域名需要接入DDoS高防，可以通过xml批量添加域名到DDoS高防。

批量接入域名到 DDoS 高防

步骤1 根据以下样例，提前准备需要批量接入的“.xml”域名文件。

```
<DomainList>
 <DomainConfig>
  <Domain>example.domain.com</Domain>
  <InstanceConfig>
   <InstanceList>CAD-159</InstanceList>
  </InstanceConfig>
  <RealServerConfig>
   <ServerPortList>80,443</ServerPortList>
   <ServerList>xx.xx.xx.xx</ServerList>
  </RealServerConfig>
  <CertificateConfig>
   <Certificate>certificateName</Certificate>
  </CertificateConfig>
 </DomainConfig>
 <DomainConfig>
  <Domain>demo.domain.com</Domain>
  <InstanceConfig>
   <InstanceList>CAD-169,CAD-179</InstanceList>
  </InstanceConfig>
  <RealServerConfig>
   <ServerPortList>80,443</ServerPortList>
   <ServerList>learn.domain.com</ServerList>
```

 版权所有 © 华为技术有限公司

```
  </RealServerConfig>
 </DomainConfig>
</DomainList>
```

表 3-25 参数说明

参数	说明
<Domain>***example.domain.com***</Domain>	***example.domain.com***为待接入域名，该字段只能设置1个域名。
<InstanceList>***CAD-159***</InstanceList>	***CAD-159***为域名接入的DDoS高防实例ID，多个实例以英文逗号隔开。
<Certificate>***certificateName***</Certificate>	***certificateName***为HTTPS端口使用的证书，如果没有HTTPS端口可以不填写该字段。
<RealServerConfig><ServerPortList>***80,443***</ServerPortList><ServerList>***xx.xx.xx.xx***</ServerList></RealServerConfig>	源站信息： • ***80,443***为源站端口，多个端口以英文逗号隔开。 • ***xx.xx.xx.xx***为源站地址，多个地址以英文逗号隔开。 • 支持源站IP或源站域名，两者不能同时存在。

步骤2 登录管理控制台。

步骤3 在页面上方选择“区域”后，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”界面。

步骤4 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

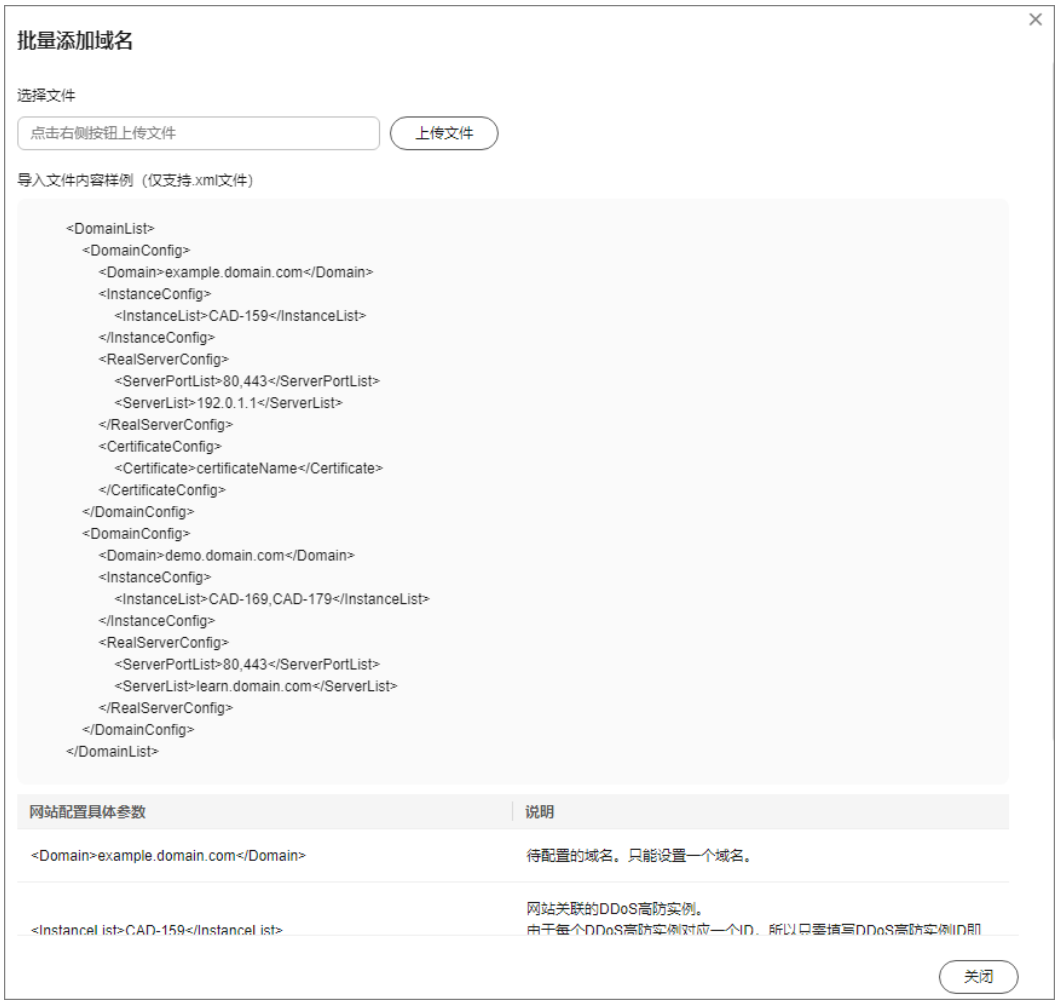
图 3-54 域名接入页

步骤5 单击“批量添加”。

步骤6 单击“上传文件”，选择本地“.xml”域名文件。

 版权所有 © 华为技术有限公司

图 3-55 上传文件



步骤7 单击“关闭”。

----结束

3.10.8 删除域名

如果您的业务发生变化，不需要防护某个域名时，可以在域名接入页面删除该域名。

须知

删除域名前，用户需要确认DNS域名服务商处已将CNAME记录修改为CNAME对应的真实的IP地址，确认该域名解析不经过高防。否则，直接删除域名将导致业务中断或服务不可用。

删除域名

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

 版权所有 © 华为技术有限公司

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-56 域名接入页

步骤4 根据实际需要选择删除方式。

- 删除单个域名：在需要删除的域名所在行的“操作”列，单击“删除”。
- 批量删除域名：勾选需要删除的域名，单击“批量删除”。

步骤5 在弹出的对话框中，单击“确定”。

----结束

3.11 证书管理

3.11.1 更新证书

如果您购买的证书即将到期，为了不影响域名的使用，建议您在到期前重新购买证书，并在DDoS高防上同步更新域名绑定的证书。

如果您需要更新域名绑定证书的信息，可以在DDoS高防上为域名绑定新的证书。

须知

- 证书更新1分钟后生效，为避免影响业务，建议您在业务量较少的时段进行更新操作。
- 证书过期后，对源站的影响极大，建议您在证书到期前及时更新证书。
- 域名和证书需要一一对应，泛域名只能使用泛域名证书。如果您没有购买泛域名证书，只有单域名对应的证书，则只能在DDoS高防中按照单域名的方式逐条添加域名进行防护。

更新证书

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

版权所有 © 华为技术有限公司

图 3-57 域名接入页

步骤4 在目标域名所在行的“业务类型”列，单击“更换”。

步骤5 在弹出的“更换证书”对话框中，上传新证书或者选择已有证书。

- 手动上传：输入证书名称，粘贴证书和私钥文本内容。当前仅支持PEM格式证书，非PEM格式的证书请参考**表3-26**转换。
- 自动拉取：选择已签发的证书。
- 选择已有证书：选择当前已使用的证书。

图 3-58 更换证书

表 3-26 证书转换命令

格式类型	转换方式
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	通过openssl工具进行转换。 提取私钥命令，以“cert.pfx”转换为“cert.key”为例。 **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes** 提取证书命令，以“cert.pfx”转换为“cert.pem”为例。 **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**

 版权所有 © 华为技术有限公司

格式类型	转换方式
P7B	通过openssl工具进行转换。 1. 执行转换命令。**openssl pkcs7 -print_certs -in incertificat.p7b -out cert.cer** 2. 获取“cert.cer”文件中证书文件的内容。 3. 将证书内容保存为PEM格式。
DER	通过openssl工具进行转换。 1. 提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** 2. 提取证书命令，以 “cert.cer”转换为“cert.pem”为例。 **openssl x509 -inform der -in cert.cer -out cert.pem**

说明

在Windows操作系统上执行openssl命令，请确保您已安装openssl工具。

步骤6 单击“确定”，证书更新完成。

----结束

3.11.2 查看证书

域名绑定证书后，您可以通过证书管理页面定期查看证书信息，及时更新，防止证书到期后业务无法访问。

查看证书信息

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-59 域名接入页

步骤4 单击“证书管理”，即可查看证书信息。

版权所有 © 华为技术有限公司

图 3-60 查看证书

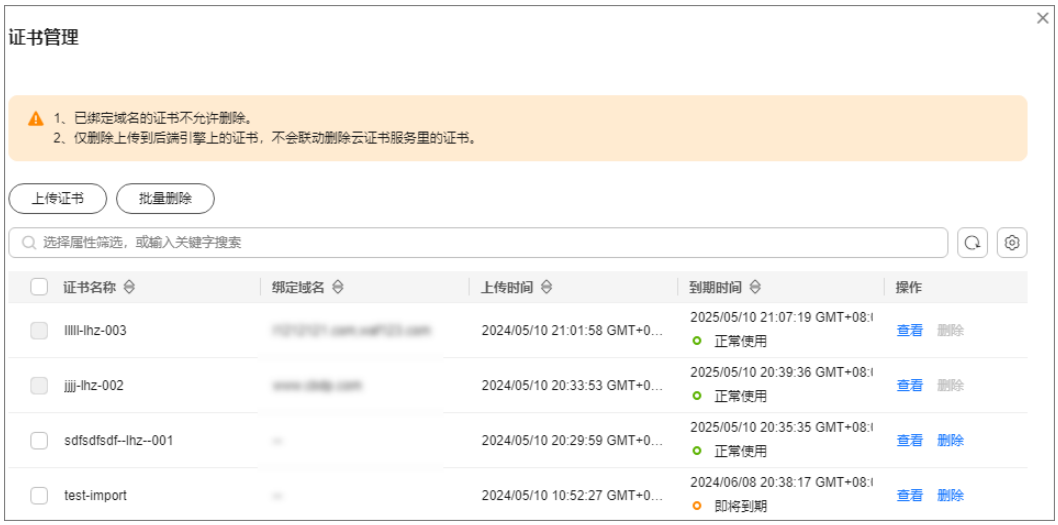


表 3-27 参数说明

参数名称	说明
证书名称	证书的名称。
绑定域名	证书已绑定的域名。
上传时间	上传证书的时间。
到期时间	证书到期的时间。

说明

在证书所在行，单击“查看”，可以查看证书的内容。

----结束

3.11.3 上传证书

源站类型为IP且转发协议为HTTPS时，需要为防护域名绑定证书。您可以在绑定证书前，通过证书管理页面提前上传需要的证书。

上传证书

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

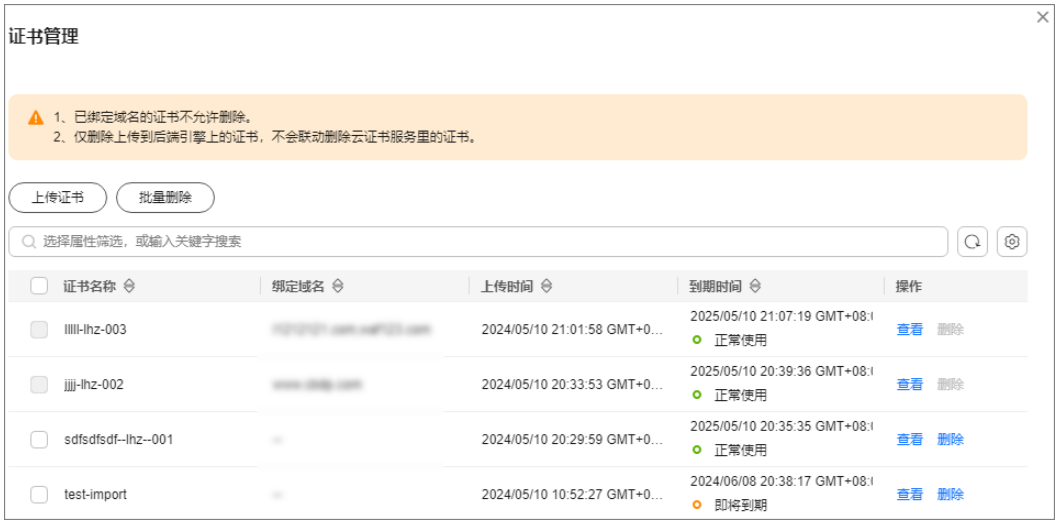
步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

版权所有 © 华为技术有限公司

图 3-61 域名接入页

步骤4 单击“证书管理”，进入证书列表。

图 3-62 查看证书



步骤5 单击“上传证书”。

步骤6 输入证书名称，粘贴证书和私钥文本内容。当前仅支持PEM格式证书，非PEM格式的证书请参考**表3-28**转换。

 版权所有 © 华为技术有限公司

图 3-63 上传证书

表 3-28 证书转换命令

格式类型	转换方式
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	通过openssl工具进行转换。 提取私钥命令，以“cert.pfx”转换为“cert.key”为例。 **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes** 提取证书命令，以“cert.pfx”转换为“cert.pem”为例。 **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	通过openssl工具进行转换。 1. 执行转换命令。**openssl pkcs7 -print_certs -in incertificat.p7b -out cert.cer** 2. 获取“cert.cer”文件中证书文件的内容。 3. 将证书内容保存为PEM格式。

版权所有 © 华为技术有限公司

格式类型	转换方式
DER	通过openssl工具进行转换。 1. 提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** 2. 提取证书命令，以 “cert.cer”转换为“cert.pem”为例。 **openssl x509 -inform der -in cert.cer -out cert.pem**

说明

在Windows操作系统上执行openssl命令，请确保您已安装**openssl**工具。

步骤7 单击“确定”，证书上传完成。

----结束

3.11.4 删除证书

已上传DDoS高防的证书，如果不需要再使用，可以通过证书管理页面进行删除。

约束与限制

已经绑定域名的证书无法删除，请参考**更新证书**修改域名的证书。

删除证书

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

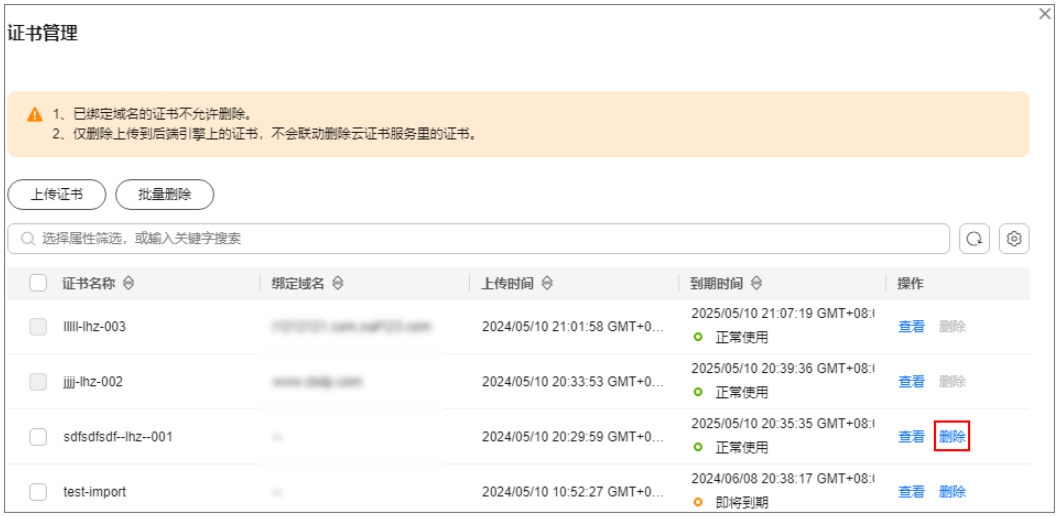
步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-64 域名接入页

步骤4 单击“证书管理”，进入证书列表。

 版权所有 © 华为技术有限公司

图 3-65 证书列表



步骤5 在需要删除的证书所在行，单击“删除”。

步骤6 在弹窗中，单击“确定”。

----结束

3.12 转发规则管理

配置转发规则后，您可以查看转发规则信息、修改源站IP、批量导出转发规则以及删除转发规则。

须知

删除转发规则可能导致业务中断，删除前请确认该转发规则没有被使用。

查看转发规则信息

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 转发配置”，进入“转发配置”页面。

步骤4 查看转发规则信息。

表 3-29 参数说明

参数名称	说明
转发协议/端口	转发规则的转发协议和转发端口。
状态	转发规则当前运行的状态。

版权所有 © 华为技术有限公司

参数名称	说明
转发模式	LVS（Linux Virtual Server）的转发规则模式。
源站区域	转发规则添加的源站区域。
源站IP	转发规则添加的源站IP。 如果需要修改源站IP，可以单击“编辑”，修改源站IP。
权重	转发规则的权重
操作	单击“删除”，删除转发规则。

----结束

修改源站 IP

步骤1 登录管理控制台。

步骤2 在左侧导航栏，选择“DDoS高防 > 转发配置”。

步骤3 在待修改源站IP的转发规则所在行，单击“编辑”。

步骤4 在弹出的“修改源站IP”对话框中，修改该转发规则的源站IP。

须知

请您填写真实有效的公网IP地址。

步骤5 单击“确定”。

----结束

导出转发规则

导出转发规则后，您可以快速修改转发规则的配置信息，再批量添加转发规则。

步骤1 在转发规则列表上方，单击“规则导出”。

步骤2 查看导出的转发规则文件“rules.txt”。

----结束

删除转发规则

当实例不需要某个转发规则时，您可以删除该转发规则。

版权所有 © 华为技术有限公司

- 单个删除转发规则：
  a. 在待删除的转发规则所在行的“操作”列，单击“删除”。
  b. 在弹出的对话框中，单击“确定”。
- 批量删除转发规则：
  a. 勾选需要删除的转发规则，单击“批量删除”。

  说明

  单次最多删除50条转发规则（由页面限制， Console单页最多展示50条转发规则）。
  b. 在弹出的对话框中，单击“确定”。

3.13 查看监控指标

3.13.1 DDoS 高防监控指标说明

功能说明

本节定义了DDoS高防上报云监控服务的监控指标的命名空间和监控指标列表，用户可以通过云监控服务提供管理控制台来检索DDoS高防产生的监控指标和告警信息。

命名空间

SYS.DDOS

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

监控指标

表 3-30 DDoS 高防服务支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
ip_drop_rate	丢弃流量	该指标为高防IP丢弃流量宽带	≥0kb/s	DDoS高防	5分钟
instance_drop_rate	丢弃流量	该指标为高防实例丢弃流量宽带	≥0kb/s	DDoS高防	5分钟
ip_back_to_source_rate	回源带宽	该指标为高防IP回源流量带宽	≥0kb/s	DDoS高防	5分钟
instance_back_to_source_rate	回源带宽	该指标为高防实例回源流量带宽	≥0kb/s	DDoS高防	5分钟

版权所有 © 华为技术有限公司

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
ip_internet_in_rate	入流量	该指标为高防IP入流量带宽	≥0kb/s	DDoS高防	5分钟
instance_internet_in_rate	入流量	该指标为高防实例入流量带宽	≥0kb/s	DDoS高防	5分钟
ip_new_connection	新建连接	该指标为高防IP新建连接数	≥0count/s	DDoS高防	5分钟
instance_new_connection	新建连接	该指标为高防实例新建连接数	≥0count/s	DDoS高防	5分钟
ip_concurrent_connection	并发连接	该指标为高防IP并发连接数	≥0count/s	DDoS高防	5分钟
instance_concurrent_connection	并发连接	该指标为高防实例并发连接数	≥0count/s	DDoS高防	5分钟
ip_service_bandwidth_usage	业务带宽利用率	该指标为高防IP业务带宽利用率	≥0%	DDoS高防	5分钟
instance_service_bandwidth_usage	业务带宽利用率	该指标为高防实例业务带宽利用率	≥0%	DDoS高防	5分钟

维度

Key	Value
zone_ip	实例 - 防护IP
instance_id	实例ID

3.13.2 查看监控指标

您可以通过管理控制台，查看DDoS高防的相关指标，及时了解DDoS高防的防护状况，并通过指标设置防护策略。

前提条件

已在云监控页面设置监控告警规则。有关设置监控告警规则的详细操作，请参见**设置监控告警规则**。

版权所有 © 华为技术有限公司

查看监控指标

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务 CES”。

步骤4 在左侧导航树，选择“云服务监控 > DDoS服务”。

图 3-66 选择服务

步骤5 在“云服务监控详情”页面，选择“DDoS服务 > 实例ID”。

步骤6 在需要查看的目标所在行，单击“查看监控指标”，查看对象的指标详情。

----结束

3.13.3 设置监控告警规则

通过设置DDoS告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解DDoS高防防护状况，从而起到预警作用。

为多个实例或实例防护的IP设置监控告警请参考**批量设置监控告警规则**；为某个指定实例或实例防护的IP设置监控告警请参考**为单个指定资源设置监控告警规则**。

版权所有 © 华为技术有限公司

如果您需要自主定义更多的监控指标，可通过API请求上报至云监控服务，具体操作请参考**添加监控数据**和**DDoS高防监控指标说明**。

批量设置监控告警规则

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务 ”。

步骤4 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”界面。

步骤6 填写告警规则信息，如**图 设置AAD监控告警规则**所示，填写规则如**表3-31**所示。

图 3-67 设置 AAD 监控告警规则

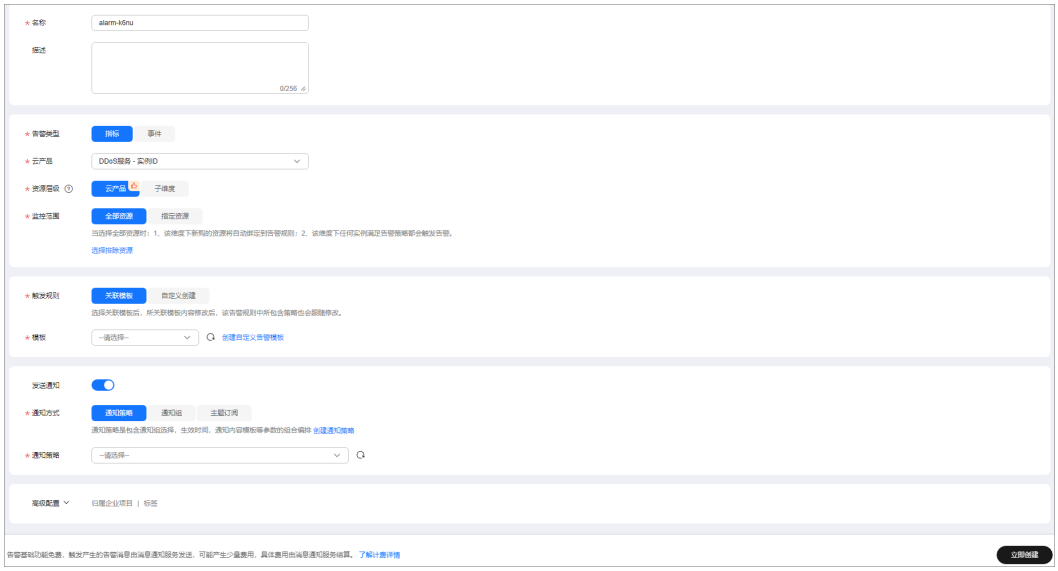


表 3-31 DDoS 高防告警规则参数说明

参数名称	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	选择告警类型。
云产品	在下拉列表框中选择“DDoS服务-实例ID”。
资源层级	选择需要监控的资源维度。
监控范围	告警规则适用的资源范围，可选择资源分组或指定资源。

 版权所有 © 华为技术有限公司

参数名称	参数说明
触发规则	可选择“关联模板”、“导入已有模板”和“自定义创建”。创建自定义模板的具体操作请参考**创建自定义告警模板**。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。
模板	选择关联或导入的模板。
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	根据实际选择通知策略。

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

为单个指定资源设置监控告警规则

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的 ，选择“管理与监管 > 云监控服务 ”。

步骤4 在左侧导航树，选择“云服务监控 > DDoS服务”。

 版权所有 © 华为技术有限公司

图 3-68 选择服务

步骤5 在“云服务监控详情”页面，选择“DDoS服务 > 实例ID”。

步骤6 在需要监控的对象所在行，选择“更多 > 创建告警规则”。

步骤7 填写告警规则信息，如**图 设置AAD监控告警规则**所示，填写规则如**表3-32**所示。

 版权所有 © 华为技术有限公司

图 3-69 设置 AAD 监控告警规则

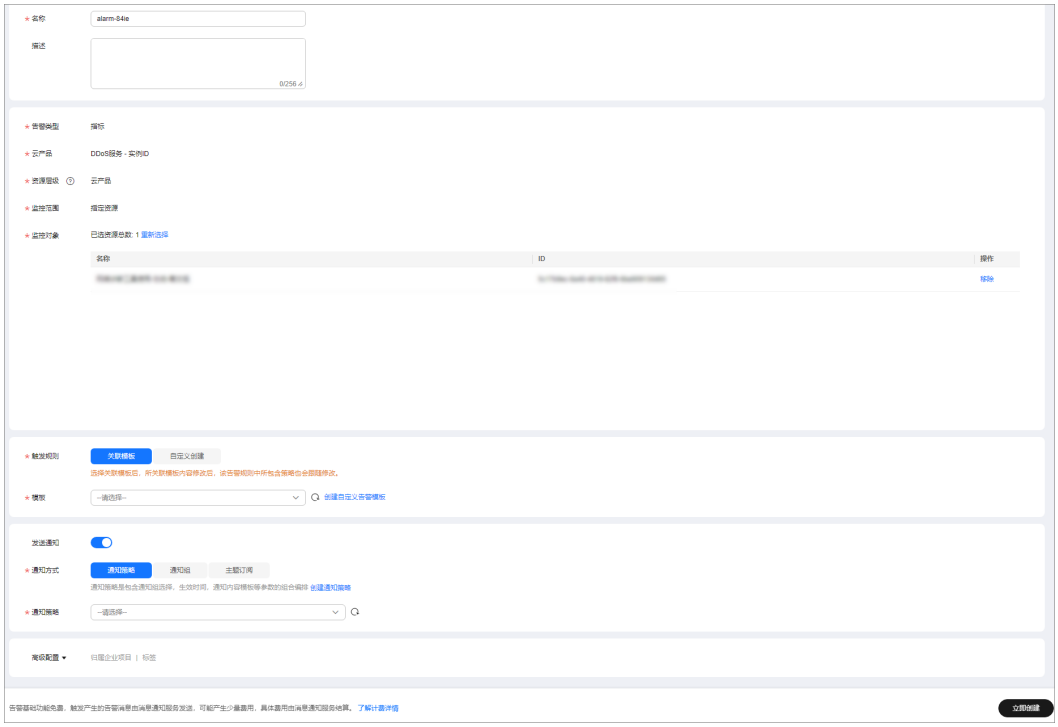


表 3-32 DDoS 高防告警规则参数说明

参数名称	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	保持默认。
云产品	保持默认。
资源层级	保持默认。
监控范围	保持默认。
监控对象	保持默认。
触发规则	可选择“关联模板”、“导入已有模板”和“自定义创建”。创建自定义模板的具体操作请参考**创建自定义告警模板**。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。
模板	选择关联或导入的模板。
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	根据实际选择需要的通知方式。

版权所有 © 华为技术有限公司

步骤8 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

3.13.4 设置事件告警通知

通过云监控服务，对DDoS高防启用事件监控，当出现黑洞、调度、攻击等事件时进行告警，方便您及时了解DDoS高防的防护情况。

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。

约束与限制

攻击流量超过10Mbps才会触发事件告警通知。

设置 DDoS 高防事件告警通知

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的 ，选择“管理与监管 > 云监控服务”。

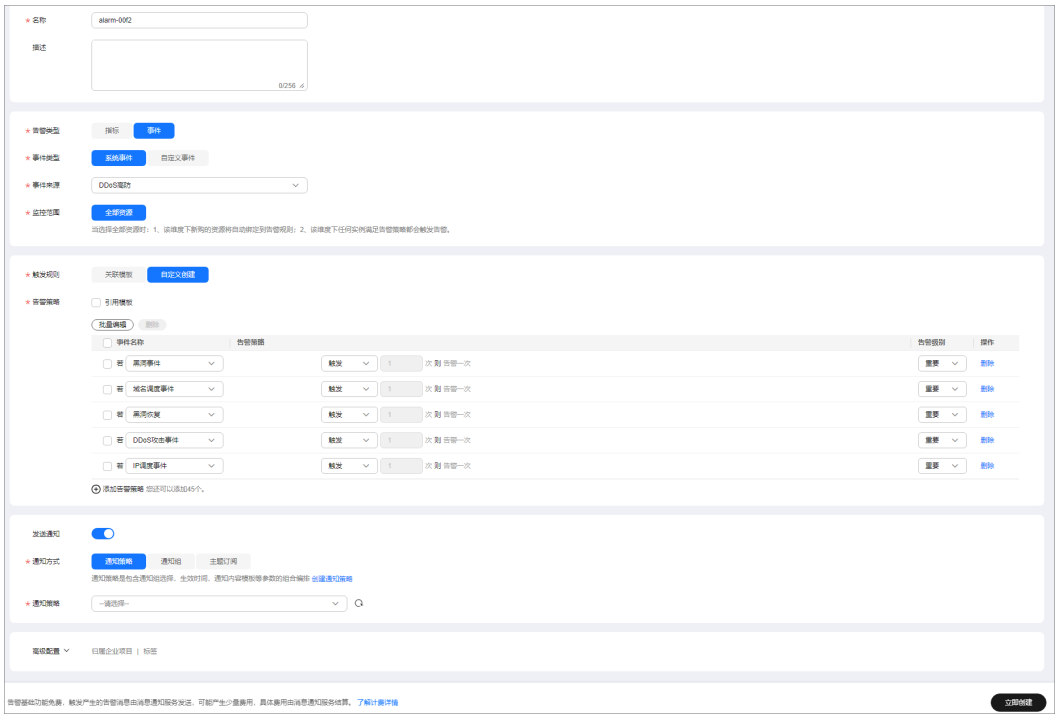
步骤4 根据实际选择方式。

- 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3-33配置告警参数。

图 3-70 告警参数



 版权所有 © 华为技术有限公司

表 3-33 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“DDoS高防”。
监控范围	选择“全部资源”。
触发规则	默认为“自定义创建”。
事件名称	推荐选择“IP调度事件”、“黑洞事件”、“黑洞恢复”、“域名调度事件”、“DDoS攻击事件”。
通知方式	根据实际选择通知方式。

说明

告警消息由消息通知服务SMN发送，可能产生少量费用。

步骤7 单击“立即创建”，在弹出的窗口中单击“确定”，告警通知创建成功。

----结束

3.14 查询审计日志

3.14.1 云审计服务支持的 DDoS 高防操作

云审计服务（Cloud Trace Service，CTS）记录了DDoS高防相关的操作事件，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DDoS防护操作列表如**表3-34**所示。

表 3-34 云审计支持的 DDoS 高防操作列表

操作名称	事件名称
上传/修改证书	domainCert
删除证书	delCertificate
新增域名、域名接入、创建域名	domainDns
导入域名	importDomain
修改域名配置	domainConfigEdit

版权所有 © 华为技术有限公司

操作名称	事件名称
设置Web基础防护/CC防护开关	domainSwitch
删除域名	deleteDomain
域名线路解析开关	cnameSwitch
新增字段转发、修改TLS配置、修改HTTP2协议	setDomainWafConfig
添加转发规则	addProtocolRule
导入、批量添加转发规则	importProtocolRule
批量删除转发规则	batchDelProtocolRule
修改转发规则中的回源IP	modifyIpInRule
开通实例	openInstance
更新实例规格	csbUpgrade
删除实例	deleteInstance
修改实例名称	modifyInstanceName
修改高防实例弹性带宽	modifyElasticBandwidth
设置实例PP协议开关	instancePpSwitch
开通实例（Console调用）	cadOpen
开通实例（CBC调用）	csbOpen
升级规格（Console调用）	cadUpgrade
修改用户当前LTS配置	updateLtsConfig
删除当前LTS配置	deleteLtsConfig
添加黑白名单	addBlackWhiteList
删除黑白名单	delBlackWhiteList
开启海外流量封禁	openForeignFlowBlock
关闭海外流量封禁	closeForeignFlowBlock
开启UDP流量封禁	openUDPFlowBlock
关闭UDP流量封禁	closeUDPFlowBlock
创建频率控制规则	addCCPolicy
更新频率控制规则	setCCPolicy
删除频率控制规则	deleteCCPolicy
配置WEB防护策略	updateWafPolicy

版权所有 © 华为技术有限公司

操作名称	事件名称
修改CC规则	updateIntelligentCc
添加区域封禁规则	addWafGeoIpRule
删除区域防护规则	deleteWafGeoIpRule
更新区域防护规则	updateWafGeoIpRule
创建CC黑白名单规则	addWafWhiteIpRule
删除CC黑白名单规则	deleteWafWhiteIpRule
创建精准防护规则	addWafCustomRule
更新精准防护规则	updateWafCustomRule
删除精准防护规则	deleteWafCustomRule
设置告警配置	setAlarmConfig
批量添加或删除资源标签	tmsResourceTagsAction
CNAME自动调度开关	cnameDispatchSwitch
修改智能CC规则	updateIntellingentCc

3.14.2 查看云审计日志

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

前提条件

已开通云审计服务，具体操作请参考**开通云审计服务**。

查看 DDoS 高防审计日志

步骤1 **登录管理控制台**。

步骤2 单击页面左侧的 ☰，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 在下拉框中选择“云服务”，输入“AAD”，按“Enter”。

步骤5 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。

版权所有 © 华为技术有限公司

  - 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

 版权所有 © 华为技术有限公司

4 DDoS 调度中心防护配额

4.1 购买 DDoS 调度中心防护

DDoS调度中心支持DDoS原生防护（或CDN服务）与DDoS高防进行联动防护，业务正常访问期间，流量正常接入DDoS原生防护（或CDN服务）；在业务受到海量攻击时，流量切换到DDoS高防服务进行清洗，确保重要业务不被攻击中断。

购买调度规则

步骤1 登录管理控制台。

步骤2 在服务列表选择“安全与合规 > DDoS防护”，进入DDoS防护服务界面。

步骤3 在左侧导航栏选择“DDoS调度中心 > 阶梯调度”。

步骤4 单击界面右上角的“购买DDoS防护”。

- 实例类型：选择“DDoS调度中心”。
- 规则数量：单个规则支持10个IP调度，购买多个规则可扩容IP调度总数。
- 购买时长：根据实际选择。
- 自动续费：是否自动续费。

版权所有 © 华为技术有限公司

图 4-1 购买调度规则

步骤5 确认规格无误后单击右下角“立即购买”，根据提示完成支付。

----结束

4.2 配置 DDoS 阶梯调度策略

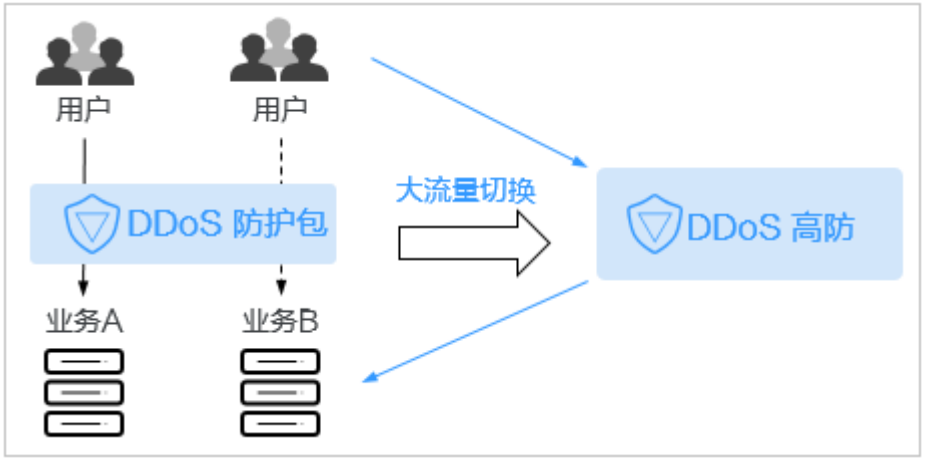
购买DDoS原生防护-全力防基础版后，通过配置DDoS阶梯调度策略，可以自动联动调度DDoS高防对DDoS原生防护-全力防基础版防护的云资源进行防护，防御海量攻击。

工作原理

DDoS原生高级防护自动联动调度DDoS高防的流程如图4-2所示。

版权所有 © 华为技术有限公司

图 4-2 联动调度流程图



约束与限制

- DDoS高防仅支持对DDoS原生高级防护对象中的云资源进行联动防护。
- DDoS原生高防和DDoS高防需要配置不同的源站IP。
- DDoS调度中心暂不支持添加IPv6 IP。

配置阶梯调度策略

步骤1 登录管理控制台。

步骤2 在服务列表选择“安全与合规 > DDoS防护”，进入DDoS防护服务界面。

步骤3 在左侧导航栏选择“DDoS调度中心 > 阶梯调度”。

步骤4 在阶梯调度列表框左上角，单击“添加规则”。

步骤5 在弹出的对话框中，设置调度规则参数，如图4-3所示，相关参数说明如表4-1所示。

图 4-3 添加调度规则

版权所有 © 华为技术有限公司

表 4-1 调度规则参数说明

参数	说明
规则名称	输入调度规则名称。 **说明** 一个规则可添加10个云资源IP，购买N个规则可添加的云资源IP总数为N*10个。
分组调度	填写局点、IP和调度分组。IP解析从1组开始依据分组进行。处于同一组的IP将同时发布解析。 默认分组：1。 **说明** • 当分组中存在被封禁的IP时，将跳过该IP对其他IP进行解析。 • 当前分组中所有IP被封堵后自动切换到下个分组，所有分组都无可用IP后进入联动调度。 • 仅支持DDoS原生防护对象中的云资源（ECS、EIP、ELB和WAF等）。
联动调度	• 不联动：只进行原生资源内的分组调度，不联动到高防DDoS防护。 • 联动到高防：调度到高防防护，需要提前购买并完成高防配置。 **注意** DDoS高防中配置的源站IP和阶梯调度分组中的IP不可重复，否则当阶梯调度分组中IP被封堵时，调度中心调度到高防后，高防回源被封堵的IP依旧异常，业务仍然无法恢复。

步骤6 单击“确定”完成配置。

----结束

相关操作

- 在目标调度规则所在行“操作”列，单击“删除”，可以删除该调度规则。
- 在目标调度规则所在行“操作”列，单击“查看详情”后，在弹出的页面中，可以查看调度规则的详细信息和添加的云资源信息。
  - 在基本信息后，单击，可以修改调度规则名称和是否联动调度。
  - 单击“添加资源”，在弹出的“添加联动资源”对话框中，修改、添加或删除云资源IP。
  - 在目标资源所在行的“操作”列，单击“删除”可以删除联动防护的云资源；或者勾选待删除的云资源后，在列表左上角单击“删除”，批量删除云资源。

4.3 开启阶梯调度告警通知

DDoS调度中心开启告警通知后，当防护IP发生以下事项时，您将接收到告警通知信息（接收消息方式由您设置）：

- 阶梯调度规则中的IP被封堵。

 版权所有 © 华为技术有限公司

- 阶梯调度规则中的IP被解封。
- 某条阶梯调度规则中所有的IP被封堵后调度。
- 某条阶梯调度规则中所有的IP被封堵后，有一个IP被解封恢复调度。

前提条件

- 在开启告警通知前，建议您在“消息通知服务”中**创建主题**并**添加订阅**。
- 创建的主题需要订阅者确认，具体操作请参考**请求订阅**。
- 已成功配置DDoS阶梯调度策略，具体操作请参考**配置DDoS阶梯调度策略**。

开启阶梯调度告警通知

步骤1 **登录管理控制台**。

步骤2 在服务列表选择“安全与合规 > DDoS防护”，进入DDoS防护服务界面。在左侧导航栏选择“DDoS调度中心 > 告警通知”。

步骤3 在“告警通知”页面中，开启告警通知，即将告警通知开关设置为  。

步骤4 在“通知主题”下拉列表选择已创建的主题，如**图4-4**所示。

图 4-4 “告警通知设置”对话框

说明

- 只有订阅状态为“已确认”的主题才能显示在下拉框。
- 只有和DDoS调度中心相同区域的主题才能显示在下拉框。
- 消息通知服务为付费服务，价格详情请参见**SMN价格详情**。

步骤5 单击“应用”，告警通知设置完成。

----结束

相关操作

如需关闭告警通知，在**图4-4**中，关闭告警通知，即将告警通知开关设置为  。

版权所有 © 华为技术有限公司

4.4 配置 CDN 调度策略

通过DDoS调度中心的自定义规则，联动使用DDoS高防和华为云CDN服务，从而实现在业务正常访问期间，流量就近接入CDN节点加速；在业务受到攻击时，流量切换到DDoS高防服务进行清洗。

前提条件

- 已购买和使用CDN服务，具体操作请参考**开通CDN服务**。
- 已购买DDoS高防服务，具体操作请参考**购买实例**。

约束与限制

您需要**提交工单**联系DDoS防护团队开通CDN调度功能权限。

开启 CDN 调度

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“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS调度中心 > CDN调度”。

步骤4 在“CDN调度”页面中，单击上方的“添加规则”。

图 4-5 添加 CDN 调度规则

步骤5 在弹出的对话框中添加相关内容，具体填写规则见**表4-2**。

 版权所有 © 华为技术有限公司

图 4-6 规则详情

表 4-2 规则填写详情

参数	说明
规则名称	输入CDN调度的自定义规则名称。
CDN域名	输入CDN域名（域名只能由字母、数字、-和.组成，且不能超过64个字符长度）。
CDN服务范围	添加的CDN域名的服务范围，需和CDN页面上配置一致，支持“中国大陆”、“中国大陆境外”、“全球”。
CDN CNAME	输入CDN CNAME（只能由小写字母、数字和.组成，且不能超过128个字符长度）。
高防CNAME	输入高防CNAME（只能由小写字母、数字和.组成，且不能超过128个字符长度）。
CDN切换高防规则	根据实际设置CDN切换到高防的触发规则。
高防切换CDN规则	根据实际设置切回CDN的策略规则。

版权所有 © 华为技术有限公司

步骤6 单击“确定”完成规则添加。

----结束

相关操作

- 编辑规则：在待编辑的规则所在行的“操作”列单击“编辑”，在弹出的对话框中修改相关参数。
- 删除规则：在待删除的规则所在行的“操作”列单击“删除”，在弹出的对话框中单击“确定”。

 版权所有 © 华为技术有限公司