DDoS 防护 AAD

最佳实践

文档版本 13

发布日期 2024-01-18

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为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

产品生命周期政策

华为公司对产品生命周期的规定以“产品生命周期终止政策”为准，该政策的详细内容请参见如下网址：
https://support.huawei.com/ecolumnsweb/zh/warranty-policy

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

华为初始证书权责说明

华为公司对随设备出厂的初始数字证书，发布了“华为设备初始数字证书权责说明”，该说明的详细内容请参见如下网址：
https://support.huawei.com/enterprise/zh/bulletins-service/ENEWS2000015766

华为企业业务最终用户许可协议(EULA)

本最终用户许可协议是最终用户（个人、公司或其他任何实体）与华为公司就华为软件的使用所缔结的协议。最终用户对华为软件的使用受本协议约束，该协议的详细内容请参见如下网址：
https://e.huawei.com/cn/about/eula

产品资料生命周期策略

华为公司针对随产品版本发布的售后客户资料（产品资料），发布了“产品资料生命周期策略”，该策略的详细内容请参见如下网址：
https://support.huawei.com/enterprise/zh/bulletins-website/ENEWS2000017760

目 录

1 DDoS 原生基础防护（Anti-DDoS 流量清洗）最佳实践

1.1 设置 DDoS 攻击告警通知

操作场景

开启DDoS攻击告警通知，当公网IP受到DDoS攻击时用户会收到提醒消息（接收消息方式由您设置）。

前提条件

- 已购买消息通知服务。
- 登录账号已购买公网IP。

约束条件

- 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，建议您在“消息通知服务”已**创建主题**并**添加订阅**。

操作步骤

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，如**图1-1**所示，相关参数说明**表1-1**所示。

图 1-1 设置告警通知

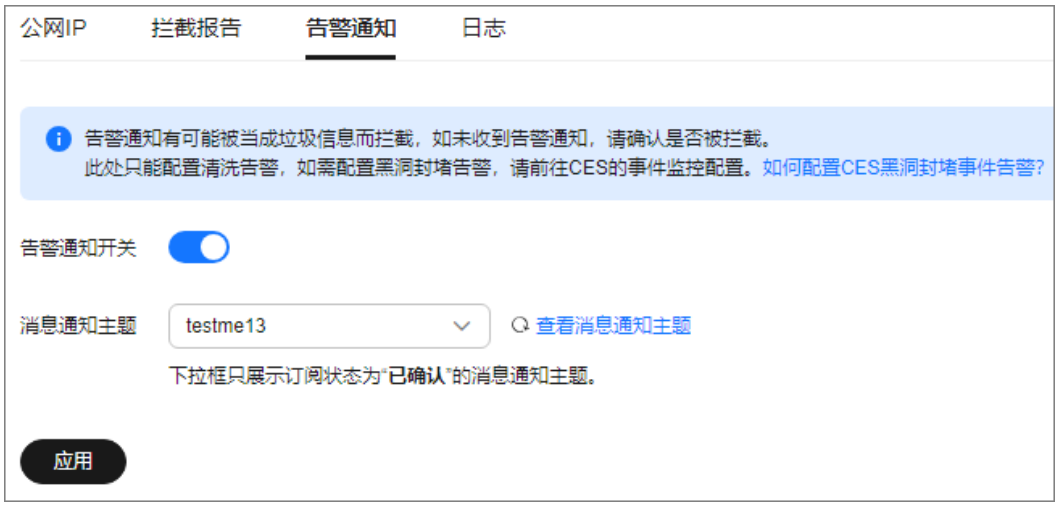


表 1-1 设置告警通知

参数名称	说明
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。

您可以单击“查看消息通知主题”创建新的主题，用于配置接收告警通知的终端。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. 参见**添加订阅**配置接收告警通知的手机号码、邮件地址等终端，即为创建的主题添加一个或多个订阅。

更多关于主题和订阅的信息，请参见**消息通知服务**。

步骤4 单击“确定”，开启告警通知。

----结束

1.2 连接已被黑洞的服务器

操作场景

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

前提条件

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

约束条件

弹性云服务器与被黑洞的服务器同地域且可正常访问。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“计算 > 弹性云服务器”，进入弹性云服务器管理界面。

步骤4 登录与被黑洞的服务器同地域且可正常访问的弹性云服务器。

弹性云服务器提供多种登录方式，请根据需要选择登录方式。

- 登录Windows弹性云服务器的详细介绍，请参见**Windows弹性云服务器登录方式概述**。
- 登录Linux弹性云服务器的详细介绍，请参见**Linux弹性云服务器登录方式概述**。

步骤5 连接黑洞状态的服务器，连接方式说明如**表1-2**所示。

表 1-2 连接黑洞服务器说明

弹性云服务器的操作系统	黑洞服务器的操作系统	连接方式
Windows	Windows	使用**mstsc**方式登录黑洞状态的服务器。 1. 在弹性云服务器中输入“mstsc”，单击mstsc打开远程桌面连接工具。 2. 在“远程桌面连接”的对话框中，单击“选项”。 3. 输入待登录的云服务器的弹性公网IP和用户名，默认为“Administrator”。 4. 单击“确定”，根据提示输入密码，登录服务器。
	Linux	使用PuTTY、Xshell等远程登录工具登录服务器。
Linux	Windows	1. 安装远程连接工具（例如**rdesktop**）。 2. 执行以下命令，登录黑洞状态的服务器。 **rdesktop -u** *用户名* **-p** *密码* **-g** *分辨率* *黑洞服务器绑定的弹性公网IP地址*

弹性云服务器的操作系统	黑洞服务器的操作系统	连接方式
	Linux	执行以下命令，登录黑洞状态的服务器。 **ssh** *黑洞服务器绑定的弹性公网IP*

----结束

后续操作

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

1.3 提升 DDoS 防护能力

华为云Anti-DDoS流量清洗服务为普通用户免费提供2Gbps的DDoS攻击防护，最高可达5Gbps，系统会对超过黑洞阈值的受攻击公网IP进行黑洞处理，正常访问流量会丢弃。

如果急需恢复业务，建议您购买华为云DDoS高防服务，提升DDoS防护能力。

2 DDoS 原生高级防护最佳实践

2.1 华为云“DDoS 原生高级防护+ELB”联动防护

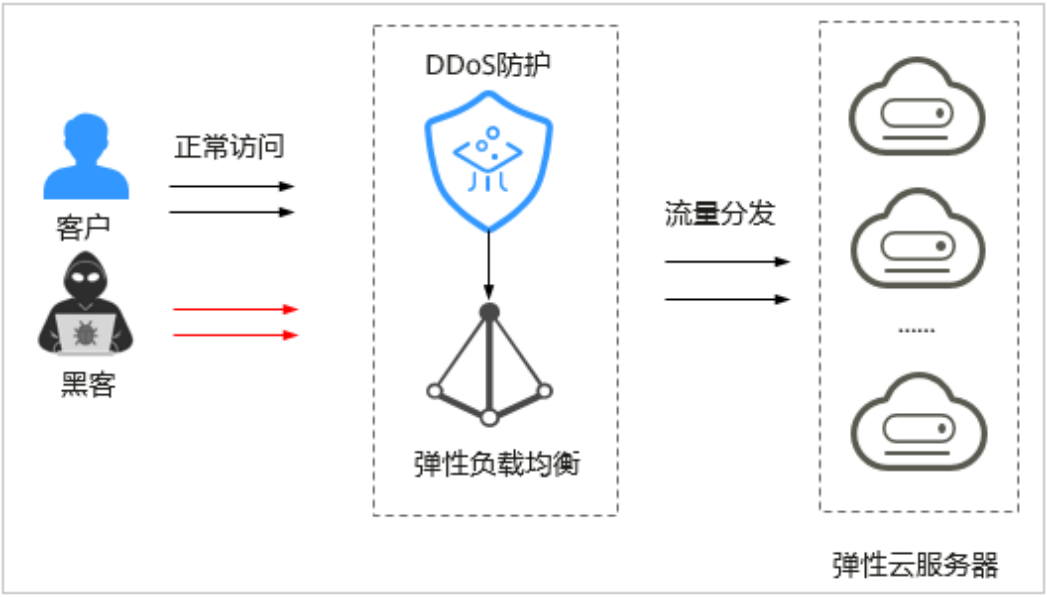
DDoS原生高级防护可以提升华为云弹性云服务器（Elastic Cloud Server，ECS）、弹性负载均衡（Elastic Load Balance，ELB）、Web应用防火墙（Web Application Firewall，WAF）、弹性公网IP（Elastic IP，EIP）等云服务的DDoS防御能力，确保云服务上的业务安全。ELB可以将访问流量根据分配策略分发到后端多台服务器，扩展应用系统对外的服务能力，消除单点故障提升应用系统的可用性。

应用场景

当您的网站类业务部署在华为云ECS上时，您可以为网站业务配置“DDoS原生高级防护+ELB”联动防护，即ECS源站服务器部署ELB后将ELB的公网IP添加到DDoS原生高级防护实例进行防护，进一步提升ECS防御DDoS攻击能力。

相比直接为ECS开启DDoS原生高级防护，“DDoS原生高级防护+ELB”联动防护通过ELB丢弃未监听协议和端口的流量，对不同类型的DDoS攻击（例如，SSDP、NTP、Memcached等反射型攻击、UDP Flood攻击、SYN Flood大包攻击）有更好的防御效果，可以大幅度提升ECS防御DDoS攻击能力，确保用户业务安全、可靠。

图 2-1 华为云“DDoS 原生高级防护+ELB”联动防护



约束条件

- DDoS原生高级防护只能防护购买区域的公网IP资源，不能跨区域防护。
- ELB不支持跨地域部署，需要选择与后端服务器相同的区域，并选择公网实例类型。

前提条件

已创建ECS实例（在支持购买DDoS原生高级防护实例的区域。例如，华北-北京四）并部署网站类业务。

操作步骤

步骤1 **创建负载均衡实例**。

创建负载均衡实例时请注意：

- 区域：选择与ECS实例相同的区域（例如，华北-北京四）
- 网络类型：选择“公网”。

步骤2 **为ELB实例绑定公网IP**。

步骤3 获取创建的负载均衡实例的公网IP地址，如**图2-2**所示。

图 2-2 ELB 实例公网 IP

步骤4 **购买DDoS原生高级防护实例**。

区域：选择与ECS实例相同的区域（例如，华北-北京四）

步骤5 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。

图 2-3 实例列表

步骤6 在目标实例所在框的右上方，单击“设置防护对象”。

步骤7 在弹出的“设置防护对象”对话框中，勾选**步骤3**中ELB的EIP后，单击“确定”。

成功添加防护对象后，您可以为防护对象配置防护策略。DDoS原生高级防护将为ECS源站服务器提供DDoS攻击全力防护能力，在业务遭受DDoS攻击时，自动触发流量清洗。

有关配置防护策略的详细操作，请参见**配置防护策略**。

----结束

2.2 华为云“DDoS 原生高级防护+独享 WAF”联动防护

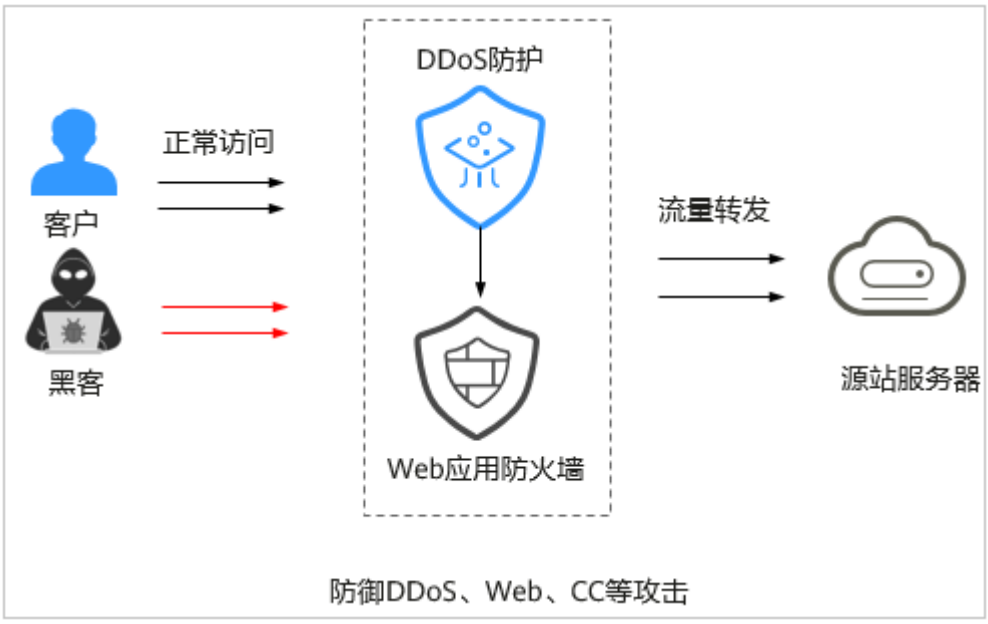
DDoS原生高级防护可以提升华为云弹性云服务器（Elastic Cloud Server，ECS）、弹性负载均衡（Elastic Load Balance，ELB）、Web应用防火墙（Web Application Firewall，WAF）、弹性公网IP（Elastic IP，EIP）等云服务的DDoS防御能力，确保云服务上的业务安全。WAF通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

应用场景

当您的网站类业务部署在华为云ECS上时，您可以为网站业务配置“DDoS原生高级防护+独享WAF”联动防护，即网站业务接入独享模式WAF后将WAF独享引擎的ELB绑定的公网IP添加到DDoS原生高级防护实例进行防护，实现DDoS原生高级防护和独享WAF双重防护，同时防御四层DDoS攻击和七层Web攻击、CC攻击等，大幅提升网站业务的安全性和稳定性。

网站业务部署“DDoS原生高级防护+独享WAF”联动防护后，所有业务流量经过WAF独享引擎进行安全清洗后，攻击流量（包括DDoS攻击、Web攻击、CC攻击等）被丢弃，正常的业务流量被WAF转发到源站服务器。

图 2-4 华为云“DDoS 原生高级防护+WAF”联动防护



约束条件

- DDoS原生高级防护只能防护购买区域的公网IP资源，不能跨区域防护。
- DDoS原生高级防护仅支持与WAF独享模式联动防护。

前提条件

网站已**接入WAF独享模式**。

操作步骤

步骤1 获取ELB的弹性公网IP。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目。
3. 单击页面左上方的，选择“网络 > 弹性负载均衡 ELB”，进入“负载均衡器”页面。
4. 在WAF独享模式绑定的负载均衡器所在行，获取ELB的弹性公网IP。

图 2-5 复制弹性公网 IP

步骤2 在ELB的弹性公网IP所在的区域**购买DDoS原生高级防护实例**。

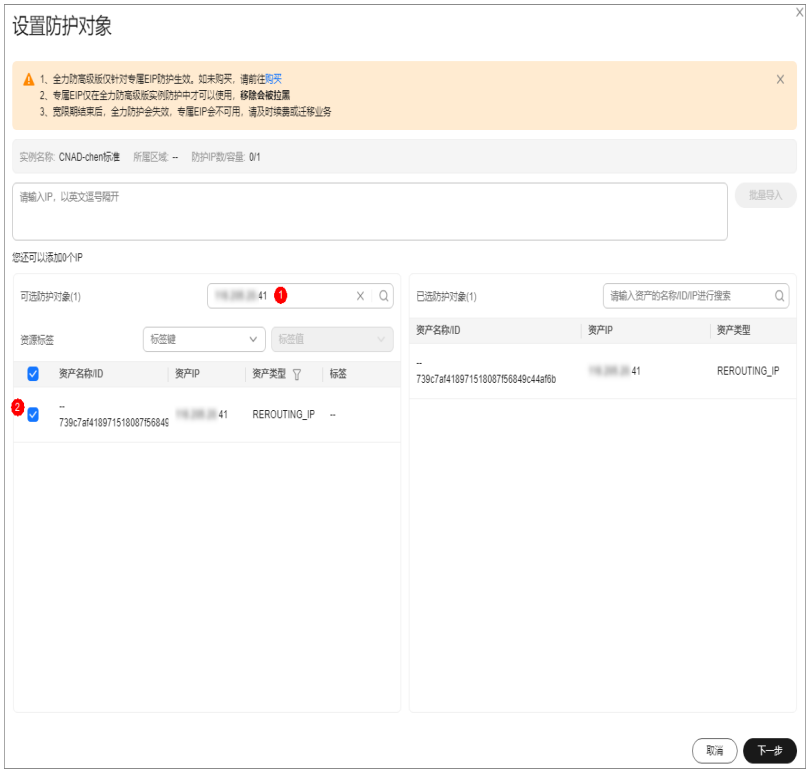
步骤3 添加ELB的弹性公网IP到DDoS原生高级防护。

1. 单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”。
2. 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。
3. 在目标实例所在框的右上方，单击“设置防护对象”。

图 2-6 设置防护对象

4. 搜索**步骤1**中ELB的弹性公网IP，将其设置为防护对象，单击“下一步”。

图 2-7 添加防护对象



5. 为新增的防护IP选择防护策略后，单击“确定”。

图 2-8 选择防护策略

成功添加防护对象后，您可以为防护对象配置防护策略，具体操作请参见**添加防护策略**。

----结束

3 DDoS 高防最佳实践

3.1 DDoS 高防业务接入

3.1.1 准备阶段

在业务接入DDoS高防前，建议您对业务情况进行全面梳理并完成接入前准备工作，以获取业务状况和业务接入信息，为业务接入DDoS高防提供依据。

网站业务梳理

建议您参照**表3-1**对业务情况进行全面梳理，了解当前业务状况和具体数据，为后续使用DDoS高防的防护功能提供指导依据。

表 3-1 网站业务梳理

梳理项	说明
网站和业务信息	
域名是否完成ICP备案	查询域名是否备案，域名如果没有备案无法接入DDoS高防。
网站/应用业务每天的流量峰值情况，包括Mbps、QPS	判断风险时间点，作为选择DDoS高防实例的业务带宽和业务QPS规格的依据。
业务的主要用户群体（例如，访问用户的主要来源地域）	方便业务接入后配置DDoS高防的海外/UDP流量封禁策略。
源站是否部署在非中国内地地域	源站部署在非中国内地地域时，建议购买DDoS高防（国际版）服务。
源站服务器的操作系统（Linux、Windows）和所使用的Web服务中间件（Apache、Nginx、IIS等）	判断源站是否存在访问控制策略，避免源站误拦截DDoS高防回源IP转发的流量。如果有，需要在源站上设置放行DDoS高防的回源IP。有关放行DDoS高防回源IP的详细操作，请参见**放行高防回源IP段**。

梳理项	说明
业务是否需要支持IPv6协议	如果您的业务需要支持IPv6协议，建议您使用DDoS原生高级防护。有关DDoS原生高级防护的详细介绍，请参见**什么是DDoS原生高级防护?** 。
业务使用的协议类型	用于后续业务接入DDoS高防时配置网站信息，选择对应的协议。
业务端口	判断源站业务端口是否在DDoS高防的支持端口范围内。有关DDoS高防支持的业务端口说明，请参加**DDoS高防支持哪些业务端口?** 。
请求头部（HTTP Header）是否带有自定义字段且服务端拥有相应的校验机制	判断DDoS高防是否会影响自定义字段导致服务端业务校验失败。如果有，请**提交工单**联系技术支持人员协助分析。
业务是否有获取并校验真实源IP机制	接入DDoS高防后，真实源IP会发生变化。请确认是否要在源站上调整获取真实源IP配置，避免影响业务。 如果需要请提前部署TOA模块或从x-forwarded-for获取真实源IP。
（针对HTTPS业务）服务端是否使用双向认证	DDoS高防暂不支持双向认证，需要变更认证方式。
（针对HTTPS业务）是否存在会话保持机制	如果您的业务有上传、登录等长会话需求，建议您使用基于七层的Cookie会话保持功能。
业务是否存在空连接	例如，服务器主动发送数据包防止会话中断，这类情况下接入DDoS高防后可能会对正常业务造成影响。
业务是否使用了CDN	如果业务使用了CDN，请确保业务支持以下两种方案： • 动态资源引流到DDoS高防，静态资源引流到CDN • 无法分离发生攻击时手动切换到DDoS高防
业务是否要求使用专线回源	DDoS高防不支持专线回源。
业务使用的域名个数及转发规则个数	有关DDoS高防规格的详细介绍，请参见**功能规格**。
业务及攻击情况	
用户遭受的历史TOP攻击类型和流量大小	• UDP带宽型攻击+数值 • HTTP CC攻击+数值 • TCP连接类攻击+数值
业务类型及业务特征（例如，游戏、棋牌、网站、App等业务）	便于在后续攻防过程中分析攻击特征。

梳理项	说明
业务流量（入方向）	帮助后续判断是否包含恶意流量。例如，日均访问流量为100 Mbps，则超过100 Mpbs时可能遭受攻击。
业务流量（出方向）	帮助后续判断是否遭受攻击，并且作为是否需要扩展业务带宽的参考依据。
单用户、单IP的入方向流量范围和连接情况	帮助后续判断是否可针对单个IP制定限速策略。
业务是否遭受过大流量攻击及攻击类型	根据历史遭受的攻击类型，设置针对性的DDoS防护策略。
业务遭受过最大的攻击流量峰值	根据攻击流量峰值判断DDoS高防功能规格的选择。
业务是否遭受过CC攻击（HTTP Flood）	通过分析历史攻击特征，配置预防性策略。
业务遭受过最大的CC攻击峰值QPS	通过分析历史攻击特征，配置预防性策略。
用户群体属性	例如，个人用户、网吧用户、通过代理访问的用户。用于判断是否存在单个出口IP集中并发访问导致误拦截的风险。
当前业务是否正在受DDoS攻击	如果业务正在遭受DDoS攻击，接入DDoS高防需要更换源站IP。

准备工作

业务接入DDoS高防前，请您根据实际的业务类型完成如**表3-2**所示准备工作。

须知

业务接入DDoS高防时，建议您先使用测试业务环境进行测试，测试通过后再正式接入生产业务环境。

表 3-2 接入 DDoS 高防前准备工作

业务类型	准备工作
网站业务	• 获取需要接入的网站域名信息，包含网站的源站服务器IP（仅支持公网IP的防护）、端口信息等。 • 确认所接入的网站域名已完成ICP备案。 • 如果您的网站支持HTTPS协议访问，您需要准备相应的证书和私钥信息，一般包含格式为“.crt”的公钥文件或格式为“.pem”的证书文件、格式为“.key”的私钥文件。 • 具有网站DNS域名解析管理员的账号，用于修改DNS解析记录，将网站流量切换至DDoS高防。 • 检查网站业务是否已有信任的访问客户端（例如监控系统、通过内部固定IP或IP段调用的API接口、固定的程序客户端请求等）。 业务接入DDoS高防后，需要将这些信任的客户端IP加入白名单。
非网站业务	获取业务对外提供服务的端口、协议类型。 如果业务通过域名访问，需要准备DNS域名解析管理员账号，用于修改DNS解析记录将网站流量切换至DDoS高防。

3.1.2 业务接入 DDoS 高防

当您将业务接入DDoS高防后，网站类业务把域名解析指向高防IP，DDoS高防将所有的公网流量都引流至高防IP，进而隐藏源站，避免源站（用户业务）遭受大流量DDoS攻击。

图 3-1 接入 DDoS 高防示意图

紧急接入场景说明

如果您的业务在接入DDoS高防前已经遭受攻击或源站IP已被黑洞，建议您在业务接入DDoS高防时参照**表3-3**进行处理。

如果在接入DDoS高防前业务已遭受攻击，建议您更换源站服务器IP。更换IP前，请务必确认是否在客户端或App端中通过代码直接指向源站IP，在这种情况下，请先更新客户端或App端代码后再更换源站IP，避免影响业务正常访问。具体操作请参见**更换源站ECS公网IP**。

表 3-3 紧急接入场景说明

业务场景	使用说明
业务已经遭受DDoS攻击	一般情况下，业务接入DDoS高防后，采用默认防护配置。
源站IP已被黑洞	如果在接入DDoS高防前，业务源站服务器已被攻击且触发黑洞策略，请及时更换源站IP。 如果您的源站为华为云ELB实例，请更换ELB实例公网IP，详细操作请参见**更换ECS IP**。 **须知** • 更换源站IP后，请尽快将业务接入DDoS高防进行防护，避免源站IP暴露。 • 如果您的业务部署在华为云上，而您不希望更换源站IP，或者已经更换源站IP但仍存在IP暴露的情况，建议您在源站ECS服务器前部署弹性负载均衡（ELB）实例，并将ELB实例的公网IP作为源站IP接入DDoS高防。

前提条件

- 已完成业务情况进行梳理和接入前准备工作。
- 域名类业务已接入WAF。

操作步骤

步骤1 **购买DDoS高防实例**。

- 如果您的业务服务器部署在中国内地，请购买DDoS高防实例。

  须知

  - DDoS高防实例不支持接入未经ICP备案的域名。如果您需要使用DDoS高防防护网站业务，请确认网站域名已经完成ICP备案。
  - DDoS高防实例默认提供IPv4高防IP。如果您需要IPv6高防IP，请选择购买DDoS原生防护实例。

- 如果您的业务服务器部署在中国内地以外地域，且业务主要用户来自中国内地，由于单独使用DDoS高防（国际版）不能保障中国内地用户的访问质量（存在约300毫秒的平均访问延时），建议您考虑以下方案：

  如果只需要保障中国内地电信、联通和非移动线路用户的业务访问速度和稳定性，您可以单独购买DDoS高防和优选线路（无防护）。

步骤2 参考**域名类业务接入DDoS高防**，将业务接入DDoS高防。

步骤3 为避免恶意攻击者绕过DDoS高防直接攻击源站服务器，建议您设置源站保护。

有关源站保护的详细操作，请参见**设置源站保护**。

步骤4 配置CC攻击防护策略。

- 业务正常时

网站业务接入DDoS高防后，建议您在业务运行一段时间后（两、三天左右），通过分析业务应用日志数据（包括URL、单一源IP平均访问QPS等），评估正常情况下单访问源IP的请求QPS情况并相应配置频率控制自定义规则限速策略，避免遭受攻击后的被动响应。

- 正在遭受CC攻击时

  通过查看DDoS高防防护日志，获取域名请求TOP URL、IP地址、访问来源IP、User-Agent等参数信息，根据实际情况配置频率控制自定义规则，并观察防护效果。

  有关配置频率自定义规则的详细操作，请参见**自定义频率控制防护规则**。

  如果实际防护效果不佳，建议您购买**MDR服务**，协助您进一步分析日志并制定防护策略。

步骤5 本地检查测试配置准确性。

配置完DDoS高防防护策略后，建议参照**表3-4**和**表3-5**检查测试DDoS高防配置是否正确。

有关本地验证的详细操作，请参见**本地验证**。

表 3-4 业务检查项说明

业务类型	检查项说明
域名类业务	接入配置域名是否填写正确。
	域名是否备案。
	接入配置协议是否与实际协议一致。
	接入配置端口是否与实际提供的服务端口一致。
	源站填写的IP是否是真实服务器IP，而不是错误填写为其他IP。
	证书信息是否正确上传。
	证书是否合法（例如，加密算法不合规、错误上传其他域名的证书等）。
	证书链是否完整。
	是否已了解DDoS高防实例的弹性防护计费方式。
	协议类型是否启用WebSocket、WebSockets协议。

表 3-5 业务可用性验证项

验证说明	验证项
必检项	测试业务是否能够正常访问。
必检项	测试业务登录会话保持功能是否正常。

验证说明	验证项
必检项	（域名类业务）观察业务返回4XX和5XX响应码的次数，确保回源IP未被拦截。
建议项	是否配置后端服务器获取真实访问源IP。
建议项	（域名类业务）是否配置源站保护，防止攻击者绕过DDoS高防直接攻击源站。
必检项	测试TCP业务的端口是否可以正常访问。

步骤6 切换业务流量。

本地检查验证通过后，建议采用测试的方式逐个修改DNS解析记录，将网站业务流量切换至DDoS高防，避免批量操作导致业务异常。如果切换流量过程中出现异常，请快速恢复DNS解析记录。

须知

- 修改DNS解析记录后，需要10分钟左右生效。
- 真实业务流量切换后，您需要再次根据上述业务可用性验证项进行测试，确保业务正常运行。

步骤7 **开启告警通知**。

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），及时发现业务异常现象：

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

  您将在次日上午收到告警通知信息。

----结束

接入后日常维护事项说明

业务接入DDoS高防后，建议您参照**表3-6**例行维护业务。

表 3-6 日常维护事项

维护事项	说明
弹性防护后付费	如果需要启用DDoS高防的弹性防护能力，请务必先查看DDoS高防的计费方式，避免实际产生的弹性防护费用超出预算。有关DDoS高防详细的服务资费和费率标准，请参见**产品价格详情**。

维护事项	说明
判断攻击类型	当DDoS高防同时遭受CC攻击和DDoS攻击时，您可以**查看DDoS高防防护日志**，根据攻击流量信息判断遭受的攻击类型。 • DDoS攻击类型：在实例防护报表中有攻击流量的波动，且已触发流量清洗，但在域名防护报表中不存在相关联的波动。 • CC攻击类型： 在实例防护报表中有攻击流量的波动，已触发流量清洗，且在域名防护报表中有相关联的波动。
业务访问延时或丢包	针对源站服务器在中国内地以外地域、主要访问用户来自中国内地地域的情况，如果用户访问网站时存在延时高、丢包等现象，主要访问用户来自非中国内地地域的情况，可能存在跨网络运营商导致的访问链路不稳定，建议您购买DDoS高防（国际版）实例并选择加速线路。
删除域名或端口转发配置	如果需要删除已防护的域名端口转发配置记录，请您确认业务是否已正式接入DDoS高防。 • 如果尚未正式切换业务流量，直接删除域名或端口转发配置记录。 • 如果已完成业务流量切换，删除域名或端口转发配置前务必前往域名DNS解析服务控制台，修改域名解析记录将业务流量切换回源站服务器。 **说明** • 删除转发配置前，请务必确认域名的DNS解析或业务访问已经切换至源站服务器。 • 删除域名配置后，DDoS高防将无法再为您的业务提供专业级安全防护。

3.2 通过 DDoS 高防判断遭受的攻击类型

DDoS攻击指主要作用于四层流量的攻击。此种攻击可在“DDoS攻击防护”报表中查看防护结果。CC攻击指主要作用于七层网站连接数的攻击。此种攻击可在“CC攻击防护”报表中查看防护结果。

判断方法

如果您的DDoS高防同时遭受到CC攻击和DDoS攻击时，可参照以下方法快速判断遭受的攻击类型：

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 单击“DDoS攻击防护”、“CC攻击防护”，通过查看相应的流量报表信息，判断攻击类型：

攻击类型	DDoS攻击防护流量报表信息	CC攻击防护流量报表信息
DDoS攻击	• 报表中有攻击流量的波动。 • 已触发流量清洗。	• 报表中没有相关联的流量波动。
CC攻击	• 报表中有攻击流量的波动。 • 已触发流量清洗。	• 报表中有相关联的流量波动。

----结束

3.3 如何获取真实源 IP

业务接入DDoS高防后，经过高防转发的流量到服务端之后真实源IP将被隐藏，在业务应用开发中，通常需要获取客户端真实的IP地址。例如，投票系统为了防止刷票，需要通过获取客户端真实IP地址，限制每个客户端IP地址只能投票一次。

本章节介绍如何通过安装DDoS高防提供的TOA模块获取真实源IP。

约束条件

源站服务器为以下Linux操作系统时，您可以通过安装DDoS高防提供的TOA模块获取高防转发后流量的真实源IP。

- CentOS6.5（对应Linux内核版本2.6.X）
- CentOS7（对应Linux内核版本3.10.X）
- toa_common（通用版本toa，一般针对Linux内核3.0及其以上的系统，如Ubuntu 14/16 、Suse 11/42等）
- toa_linux-2.6.32-220.23.1.el6.x86_64.rs（对应指定的版本：linux-2.6.32-220.23.1.el6.x86_64.rs）

须知

- DDoS高防仅支持IPv4，获取真实源IP时请确保TOA在IPv4端口输出。
- DDoS高防+Web源站场景下，如果DDoS高防关闭了Web基础防护，则需要在源站安装TOA以获取真实源IP；如果DDoS高防开启了Web基础防护，则流量路径是高防->集群小WAF->Web源站，不需要安装TOA获取真实源IP，可从xff，x-real等7层请求头部获取真实源IP。
- 如果源站服务器使用了其他操作系统（Ubuntu、SUSE等），请参考**TOA插件配置**定制编译安装TOA插件以获取真实源IP。

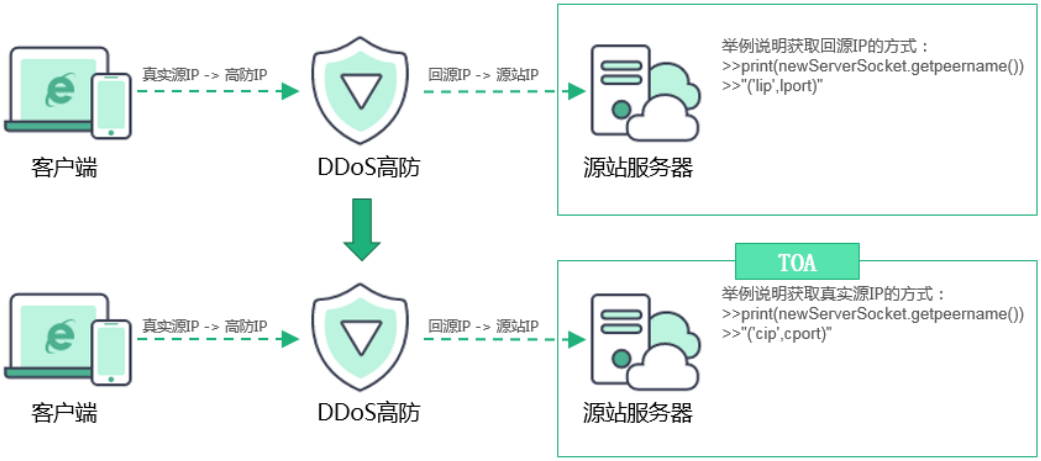
应用场景

安装高防TOA插件是基于四层协议（TCP）获取真实源IP的方法。如果您的业务部署场景为DDoS+WAF，请参考**如何在启用Web应用防火墙后获取访问者真实IP**获取七层协议（HTTP）真实源IP。

原理说明

通常情况下，经过高防的流量会修改真实源IP与高防IP（由真实源IP->高防IP转换为回源IP->源站IP），用户在自己的源站服务器上看到的流量源IP是回源IP，如**图3-2**所示。

图 3-2 原理说明



- 高防IP：华为云为用户提供的IP，用来代理源站IP，确保源站的稳定可靠。
- 回源IP：用户在自己的源站服务器上看到的所有流量的源IP就是回源IP。
- 源站IP：用户的实际业务对外提供服务所使用的公网IP地址。

操作步骤

步骤1 请参考**TOA模块的开源代码**编译安装TOA模块。

说明

挂载内核模块过程中，不影响服务器现有业务，不用修改原有服务器进程即可获取真实源IP。

步骤2 验证TOA内核模块。

可以参考**TOA插件配置**获取真实源IP，或参考**原理说明**如下示例获取源站IP。

```
>>print(newServerSocket.getpeername())
>>"('cip',cport)"
```

----结束

3.4 华为云"DDoS 高防+云模式 WAF"联动

操作场景

该任务指导用户如何配置域名解析，实现华为云“DDoS高防+WAF（Web应用防火墙）”联动。

DDoS高防和云模式WAF联动后，流量会先经过DDoS高防，再转发至WAF，实现联动防御。

图 3-3 联动原理

注意

如果您在DDoS高防防护的多个WAF CNAME使用的是同一个高防IP和端口。后续您在WAF控制台将该域名工作模式切换为“Bypass”模式时，会导致DDoS高防所有绑定相同高防IP和端口的域名不可用。

前提条件

- 已成功购买高防实例。
- 已购买Web应用防火墙，并且已配置防护域名。

约束条件

- “DDoS高防+WAF”联动仅支持域名防护。

须知

例如，example.com和www.example.com是两个不同的域名，在配置“DDoS高防+WAF”时，需要分别进行配置。

- 同一个高防IP+端口只能配置一种源站类型，若您配置过源站域名后，无法再配置源站IP。

操作步骤

步骤1 获取WAF CNAME值。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目。

3. 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。
4. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
5. 在“域名”列，单击要获取CNAME值的域名。
6. 在“基本信息”界面，单击“是否已使用代理”后的。

图 3-4 基本信息

7. 在弹出的“是否已使用代理”界面，选择“四层代理”，单击“确认”。
8. 在“基本信息”界面，复制CNAME。

图 3-5 复制 CNAME

步骤2 把WAF CNAME值配置到DDoS高防。

说明

配置WAF联动后，网站类业务不需要上传证书。

1. 单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”。
2. 选择“DDoS高防 > 域名接入”，进入“域名接入”页面。
3. 根据实际选择“中国大陆”或“中国大陆外”。
4. 单击“添加域名”。
5. 填写域名信息，单击“下一步”。

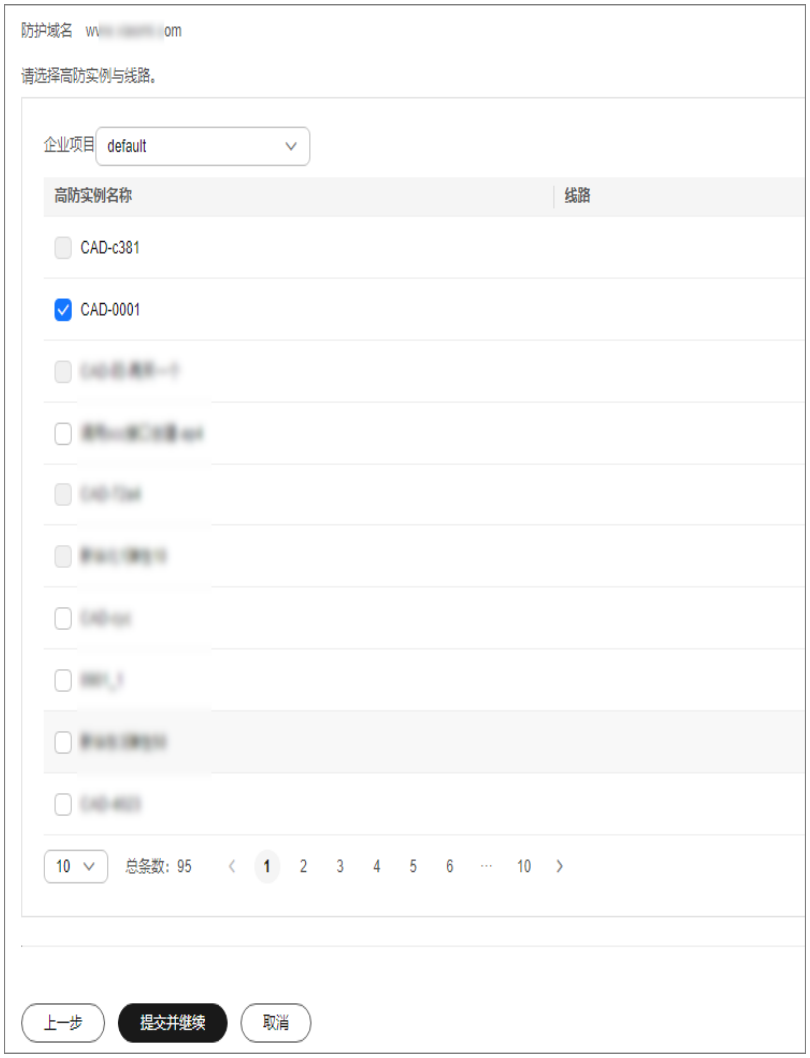
图 3-6 配置网站类域名信息

表 3-7 参数说明

参数	说明
防护域名	用户的实际业务对外提供服务所使用的域名。域名填写支持泛域名，例如 *.domain.com。
源站类型	- 选择“源站域名”。 - 填写源站域名的转发协议和源站端口。 - 填写复制的WAF CNAME。

6. 在“选择实例与线路”界面，选择需要使用的高防实例和对应的高防IP，单击“提交并继续”。

图 3-7 选择实例与线路



步骤3 单击“下一步”。

步骤4 在“修改DNS解析”页面，复制DDoS高防的CNAME，单击“完成”。

图 3-8 复制 DDoS 高防 CNAME

步骤5 修改DNS解析。

1. 单击页面左上方的 ☰，选择“网络 > 云解析服务 DNS”，进入云解析服务管理控制台。
2. 单击“公网域名”。
3. 在目标域名所在行，单击“管理解析”。
4. 单击“添加记录集”，添加CNAME记录集。

图 3-9 添加 CNAME 记录集

表 3-8 关键参数

参数	说明
主机记录	填写DDoS高防中配置的域名。
类型	选择“CNAME-将域名指向另外一个域名”。
线路类型	选择“全网默认”。

参数	说明
TTL（秒）	指解析记录在本地DNS服务器的缓存时间。如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。
值	填写复制的DDoS高防CNAME地址。

须知

DNS解析发布需要一定时间，大部分域名在5分钟内可以切换完成。

----结束

3.5 华为云“DDoS 高防+CDN”联动

操作场景

如果您的业务（如视频、电商平台）有大量图片或视频等资源需要为用户展示，且希望这些资源可以被用户快速获取。您可以使用华为云“DDoS高防+CDN”联动方案，使这些资源快速被用户获取，同时提高用户登录平台和支付能力等业务系统的网络能力，保证平台稳定运行。

约束限制

- 当用户的视频、电商等业务系统可以通过域名区分动静态资源，可以使用“DDoS高防+CDN”联动方案，动静态资源相关说明如表3-9所示。
- 部分平台业务系统的动静态资源采用一套域名，没有做动静态资源分离，这种情况无法使用“DDoS高防+CDN”联动方案，请参考备选方案进行处理。

图 3-10 “DDoS 高防+CDN”联动方案原理说明

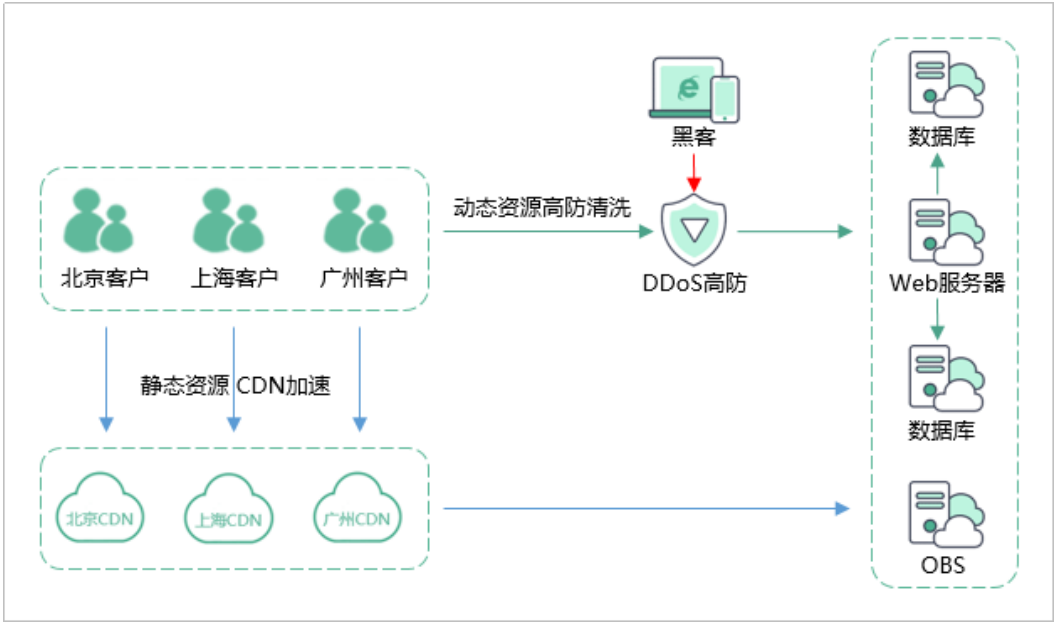


表 3-9 动态资源与静态资源

类别	定义	举例	解决办法
动态资源	服务器端在应答客户请求前需要和数据库进行交互的业务。	• 支付 • 登录	动态资源的域名解析到高防的CNAME。高防防护能够保证登录、支付等功能平台稳定运行不中断。
静态资源	客户可以直接在对象存储中获取的固定资源。	• 图片 • 视频	静态资源的域名解析到CDN的CNAME。CDN加速使客户能够快速获取视频、图片等资源，提升客户体验。

说明

- 如果是静态资源，例如图片业务的域名是image.abc.com，DNS将image.abc.com解析到CDN的CNAME，即可以获取静态资源CDN加速能力。
- 如果是动态资源，例如登录业务的域名是login.abc.com，DNS将login.abc.com解析到高防的CNAME，高防防护保证登录功能稳定运行。

备选方案

不需要动静态分离，用户业务遭受大流量DDoS攻击时，可以通过配置高防IP，将攻击流量引流到高防IP清洗，确保源站业务稳定可靠。没有攻击时，可以通过CDN加速提高客户使用体验。

流量能否直接先过 CDN 再过高防，或先过高防再过 CDN?

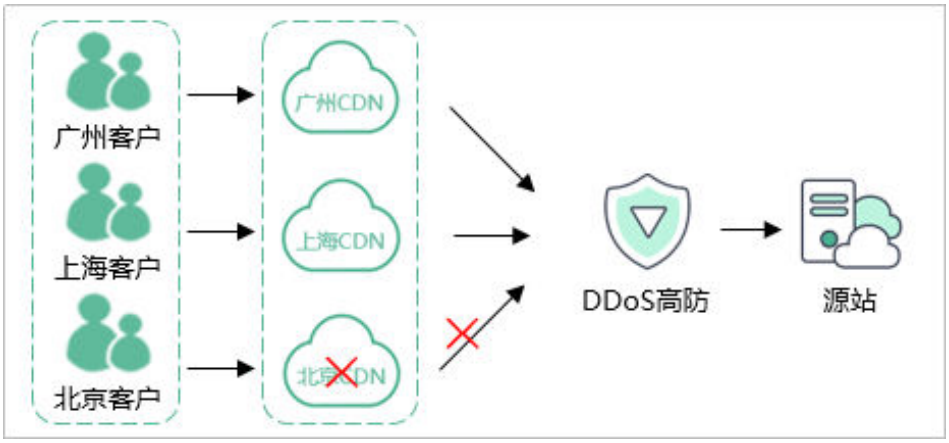
以下两种均不可以。

- 第一种情况：流量先经过CDN再经过高防，即高防串联在CDN后面。

  结果：高防的DDoS防护功能失去意义。

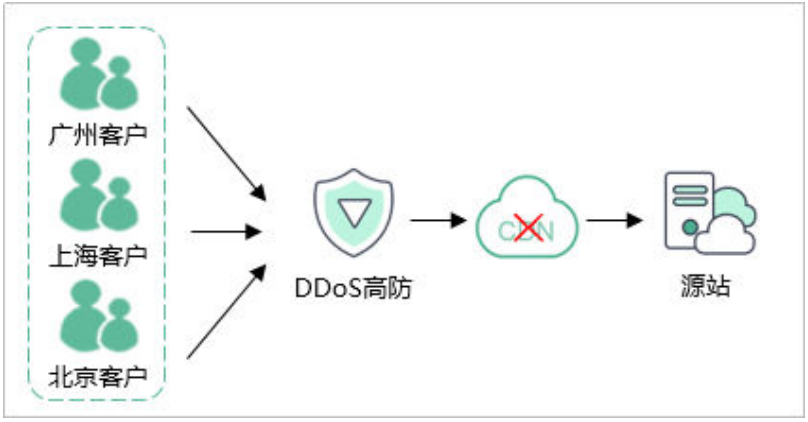
  原因：攻击流量先到达CDN，CDN被攻击用户无法访问，攻击流量不会到达高防，高防没有做流量清洗的机会。

图 3-11 流量先经过 CDN 再经过高防原理说明



- 第二种情况：流量先经过高防再经过CDN，即CDN串联在高防后面。
  结果：CDN的加速功能失去意义。
  原因：CDN加速能力的工作原理是使用户可以就近访问分散在各地的CDN节点，客户直接访问高防则无法使用CDN就近访问的加速能力。

图 3-12 流量先经过高防再经过 CDN 原理说明



操作步骤

静态资源接入，请参考**添加CDN加速域名**。

动态资源接入，请参考**域名网站类业务接入DDoS高防**。

3.6 华为云“DDoS 高防+DDoS 调度中心+CDN”联动

操作场景

CDN联动调度通过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；仅在业务受到攻击时，流量切换到DDoS高防服务进行清洗。

约束限制

您需要**提交工单**联系DDoS防护团队开通CDN调度功能权限。

切换条件

- CDN切换到高防
  连续3分钟内3次触发QPS超过阈值或连续10分钟内出现6次以上，并且CDN/DCDN上流量不超过10Gbps，触发切换流程。
- 高防回切到CDN
  连续12小时以上，域名QPS低于QPS阈值的80%，触发回切流程。回切时间8-23点，其他时间不触发回切。

操作步骤

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 在左侧导航树，选择“DDoS调度中心 > CDN调度”，进入“CDN调度”页面。

步骤4 单击“添加规则”。

图 3-13 添加规则

表 3-10 参数说明

参数	说明
规则名称	自定义的规则名称。
CDN域名	需要防护和加速的域名。
CDN服务范围	CDN域名的服务范围，需和CDN页面上配置一致。
CDN CNAME	CDN加速域名的CNAME。
高防CNAME	DDoS防护域名的CNAME。
切换条件	设置触发切换到DDoS高防的最小QPS值，输入范围100-10000。

步骤5 确认配置无误后，单击“确定”并记录下“调度CNAME”的值。

图 3-14 添加规则

步骤6 单击页面左上方的 ☰，选择“网络 > 云解析服务 DNS”。

步骤7 单击“公网域名”。

步骤8 在目标域名所在行，单击“管理解析”。

步骤9 单击“添加记录集”，添加CNAME记录集。

图 3-15 添加记录集

表 3-11 关键参数

参数	说明
主机记录	填写CDN域名。
类型	选择“CNAME-将域名指向另外一个域名”。
线路类型	选择“全网默认”。
TTL (秒)	指解析记录在本地DNS服务器的缓存时间。如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。
值	填写**步骤5**中的调度CNAME地址。

步骤10 确认配置无误，单击“确定”。

----结束

3.7 源站 IP 暴露的解决方法

在使用DDoS高防时，如果源站IP已暴露，可能存在绕过高防直接攻击源站IP的风险。建议用户更换源站IP。

在更换源站IP前，需要对暴露源站IP的可能因素进行检查，避免新更换的源站IP继续暴露。

DNS 解析记录检查

检查该遭到攻击的旧源站IP上所有DNS解析记录，确保域名全部解析到高防cname或高防IP，避免部分解析记录直接解析成新更换的源站IP。

信息泄露及命令执行类漏洞检查

检查网站或业务系统是否存在信息泄露的漏洞，如phpinfo()泄露、GitHub信息泄露等。

检查网站或业务系统是否存在命令执行类漏洞。

其他建议

建议不使用与旧源站IP相同或相近网段的IP作为新的源站IP，避免攻击者对C段或相近网段进行猜测和扫描。

建议提前准备备份链路和备份IP。

3.8 网站类业务实例迁移

网站类业务接入DDoS高防后，您可以通过修改域名的高防IP解析线路，将源站IP/源站域名切换到其他DDoS高防实例进行防护。

须知

修改域名的高防IP解析线路后约5分钟后生效。为了确保业务正常访问，建议您在业务量少时进行操作。

操作步骤

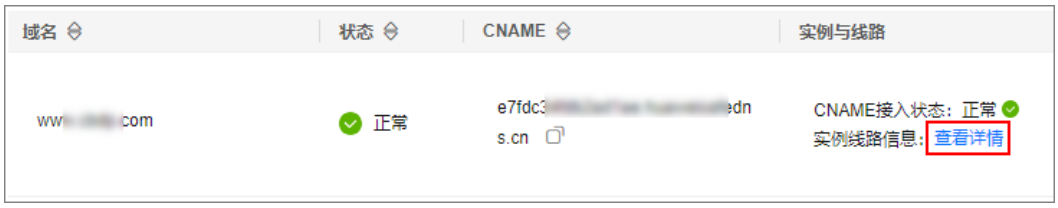
步骤1 登录管理控制台。

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 在左侧导航树，选择“DDoS高防 > 域名接入”。

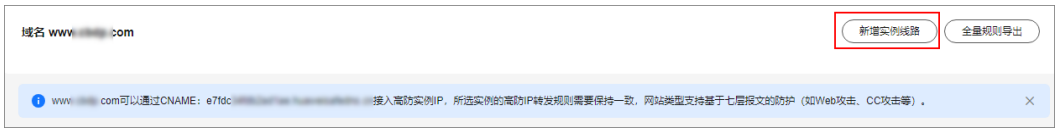
步骤4 在目标域名所在行的“实例与线路”列，单击“查看详情”。

图 3-16 查看详情



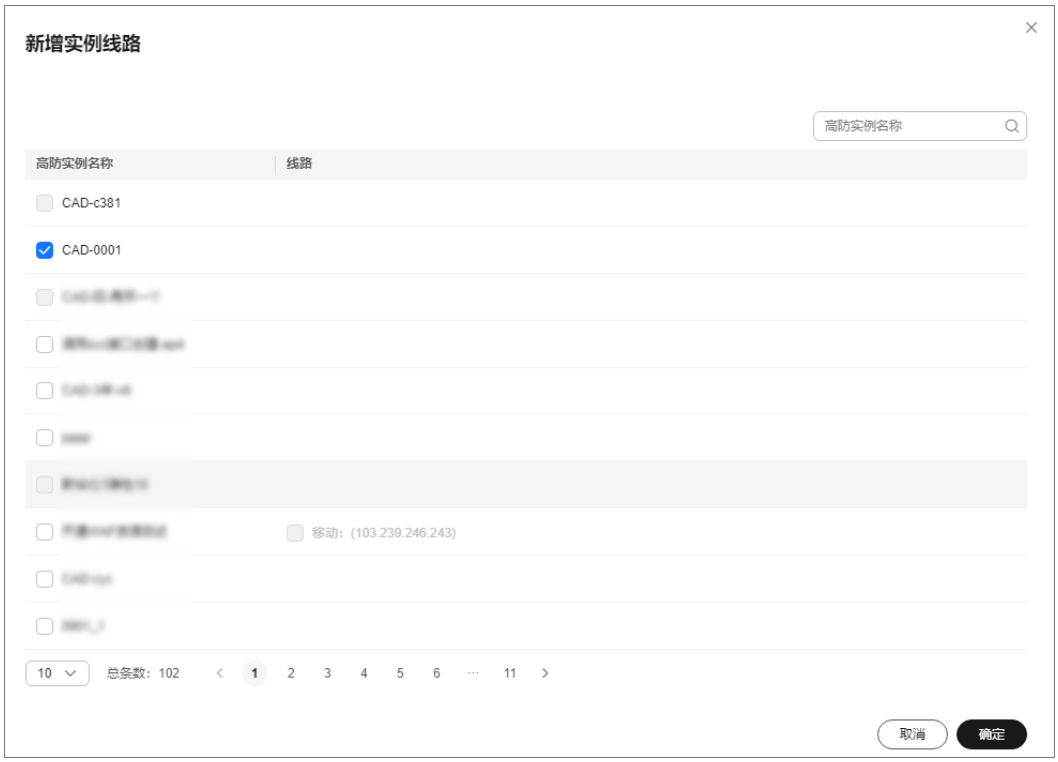
步骤5 在实例与线路列表右上方，单击“新增实例线路”。

图 3-17 新增实例线路



步骤6 在弹出的“新增实例线路”对话框中，选择需要切换到的新的DDoS高防实例和线路，单击“确定”。

图 3-18 选择线路



步骤7 将新添加的线路的“线路解析开关”设置为 。

图 3-19 域名解析

步骤8 将旧线路的“线路解析开关”状态变更为 ，关闭该高防实例和线路下高防IP的域名解析功能。

步骤9 单击“删除线路”，在弹出的提示框中，单击“确定”，删除该高防实例和线路下高防IP。

注意

不建议立即删除该线路，请在关闭旧高防实例和线路下高防IP的域名解析功能后24小时后删除。

----结束

4 DDoS 阶梯调度最佳实践

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

配置DDoS阶梯调度后，当发生海量攻击时，系统联动调度DDoS高防对DDoS原生高级防护对象中的华为云上云资源进行防护，业务流量经过DDoS高防转发。DDoS阶梯调度工作原理如图4-1所示。

- 当业务有正常访问/日常攻击时，DDoS原生高级防护提供DDoS攻击全力防护能力，在业务遭受DDoS攻击时，自动触发流量清洗。
- 当业务遭受海量流量攻击导致封堵时，DDoS阶梯调度自动调度高防CNAME，联动高防DDoS将恶意攻击流量引流到高防IP进行清洗，确保重要业务不被攻击中断。

图 4-1 DDoS 阶梯调度工作原理

本章节以网站类业务“www.example.com”域名为例，介绍如何配置DDoS阶梯调度。

约束条件

- DDoS原生高级防护只能防护购买区域的公网IP资源，不能跨区域防护。
- 防护域名（www.example.com）部署在华为云上，且部署在支持购买DDoS原生高级防护实例的区域（例如，华北-北京四）。

- 防护域名（www.example.com）未接入WAF。

前提条件

- 已购买“DDoS原生高级防护”，且购买时选择开启联动防护。
- 已获取防护域名（www.example.com）的源站公网IP地址。
- 如果防护域名（www.example.com）未部署在“华东-上海一”区域，则防护域名所在区域已准备了备用公网IP地址。
- 已成功购买DDoS原生高级防护实例。

  区域：选择防护域名（www.example.com）部署的区域（例如，华北-北京四）
- 已成功购买DDoS高防实例。

操作步骤

步骤1 登录管理控制台。

步骤2 添加防护对象。

1. 进入DDoS原生高级防护实例列表页面。
2. 在目标实例所在框的右上方，单击“设置防护对象”。
3. 在弹出的“设置防护对象”对话框中，勾选防护域名（www.example.com）的源站公网IP后，单击“确定”。

步骤3 创建防护策略。

1. 进入DDoS原生高级防护的防护策略页面。
2. 在防护策略列表的左上方，单击“创建策略”。
3. 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”。

步骤4 在**步骤4**中创建的防护策略所在行的“操作”列中，单击“配置策略”，配置防护策略。

有关配置防护策略的详细操作，请参见**配置防护策略**。

步骤5 将防护域名（www.example.com）接入DDoS高防。

1. 进入DDoS高防域名列表入口。
2. 在域名列表左上角，单击“添加域名”。
3. 填写域名信息，如**图4-2**所示，单击“下一步”。

图 4-2 配置网站类域名信息

须知

“源站类型”选择“源站IP”，源站IP配置说明如下：

- 如果防护域名部署在“华东-上海一”区域，源站IP配置为防护域名的源站公网IP地址。
- 如果防护域名未部署在“华东-上海一”区域，源站IP需要配置为防护域名所在区域同一网段准备的备用公网IP地址。

4. 在高防实例名称列表中选择实例与线路后，单击“提交并继续”。
5. 单击“下一步”后，单击“完成”。

防护域名接入DDoS高防，获取域名的CNAME值（12b6003fd3c2e618.huaweisafedns.com），如图4-3所示。

图 4-3 防护域名接入 DDoS 高防

步骤6 配置阶梯调度规则。

1. 进入阶梯调度页面。
2. 在阶梯调度列表框左上角，单击“添加规则”。
3. 在弹出添加规则对话框中，配置调度规则后，单击“确定”。
   - 分组调度：选择DDoS原生防护对象中的云资源。
   - 高防CNAME：填写为**步骤5.5**中的CNAME值。

   规则配置完成后，获取调度CNAME值，如**图4-4**所示。

图 4-4 获取调度 CNAME 值

步骤7 参考**添加CNAME类型记录集**添加DNS解析。

- “主机记录”：配置的域名。
- “类型”：选择“CNAME-将域名指向另外一个域名”。
- “线路类型”：全网默认。
- “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
- “值”：输入**步骤6.3**中的CNAME值。
- 其他的设置保持不变。

----结束

生效机制

DNS解析记录生效后，阶梯调度策略即可生效。

A 修订记录

发布日期	修改说明
2024-01-18	第十三次正式发布。 • 新增**源站IP暴露的解决方法**章节。 • 新增**华为云“DDoS高防+DDoS调度中心+CDN”联动**章节。
2023-11-28	第十二次正式发布。 • **华为云“DDoS原生高级防护+独享WAF”联动防护**，优化流程和截图。 • **华为云"DDoS高防+云模式WAF"联动**，优化流程和截图。
2023-08-28	第十一次正式发布。 新增**网站类业务实例迁移**章节。
2022-01-07	第十次正式发布。 新增“DDoS高防业务接入”章节。
2021-11-01	第九次正式发布。 **华为云"DDoS高防+云模式WAF"联动**，更新界面截图。
2021-10-12	第八次正式发布。 **华为云“DDoS原生高级防护+独享WAF”联动防护**，优化内容描述。
2021-09-10	第七次正式发布。 **DDoS阶梯调度最佳实践**，优化内容描述。
2021-08-27	第六次正式发布。 **DDoS阶梯调度最佳实践**，优化内容描述。
2021-07-14	第五次正式发布。 更新界面截图。

发布日期	修改说明
2021-06-17	第四次正式发布。 **设置DDoS攻击告警通知**，优化操作步骤。
2021-06-09	第三次正式发布。 **连接已被黑洞的服务器**，优化操作步骤。
2021-05-14	第二次正式发布。 • 新增**华为云“DDoS原生高级防护+ELB”联动防护**。 • 新增**华为云“DDoS原生高级防护+独享WAF”联动防护**。 • 新增**DDoS阶梯调度最佳实践**。
2021-02-01	第一次正式发布。