DDoS 防护 AAD

最佳实践

文档版本 17

发布日期 2025-01-26

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 最佳实践汇总 1
2 DDoS 原生基础防护（Anti-DDoS 流量清洗）最佳实践 2
2.1 通过 ECS 访问被黑洞的服务器 2
3 DDoS 原生高级防护最佳实践 4
3.1 使用 ELB 和 DDoS 原生高级防护提升 ECS 防御 DDoS 攻击能力 4
3.2 使用 WAF、ELB 和 DDoS 原生高级防护提升网站业务安全性 6
4 DDoS 高防最佳实践 10
4.1 使用 DDoS 高防识别攻击类型 10
4.2 使用 TOA 模块获取真实请求来源 IP 11
4.3 使用 WAF 和 DDoS 高防实现域名防护 12
4.4 使用 CDN 和 DDoS 高防防护动静态资源 19
4.5 网站业务迁移：从 DDoS 高防实例 A 到实例 B 21
5 通过 DDoS 调度中心实现流量的阶梯调度 24

1 最佳实践汇总

本文汇总了DDoS防护常见应用场景的操作实践，为每个实践提供详细的方案描述和操作指导，帮助用户轻松使用DDoS防护业务。

表 1-1 最佳实践一览表

分类	相关文档
被攻击后处理	通过ECS访问被黑洞的服务器
	使用DDoS高防识别攻击类型
	网站业务迁移：从DDoS高防实例A到实例B
源站IP相关	使用TOA模块获取真实请求来源IP
提升防护能力	通过DDoS调度中心实现流量的阶梯调度
联动防护	使用ELB和DDoS原生高级防护提升ECS防御DDoS攻击能力
	使用WAF、ELB和DDoS原生高级防护提升网站业务安全性
	使用WAF和DDoS高防实现域名防护
	使用CDN和DDoS高防防护动静态资源

2 DDoS 原生基础防护（Anti-DDoS 流量清洗）最佳实践

2.1 通过 ECS 访问被黑洞的服务器

应用场景

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ECS连接该服务器。

通过ECS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。

约束与限制

弹性云服务器需要与被黑洞的服务器同地域且可正常访问。

资源和成本规划

资源	资源说明	数量	成本说明
弹性云服务器 ECS	用于连接黑洞服务器。	1	ECS的计费方式及标准请参考**ECS计费说明**。

实施步骤

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2-1**所示。

表 2-1 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*
	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

3 DDoS 原生高级防护最佳实践

3.1 使用 ELB 和 DDoS 原生高级防护提升 ECS 防御 DDoS 攻击能力

应用场景

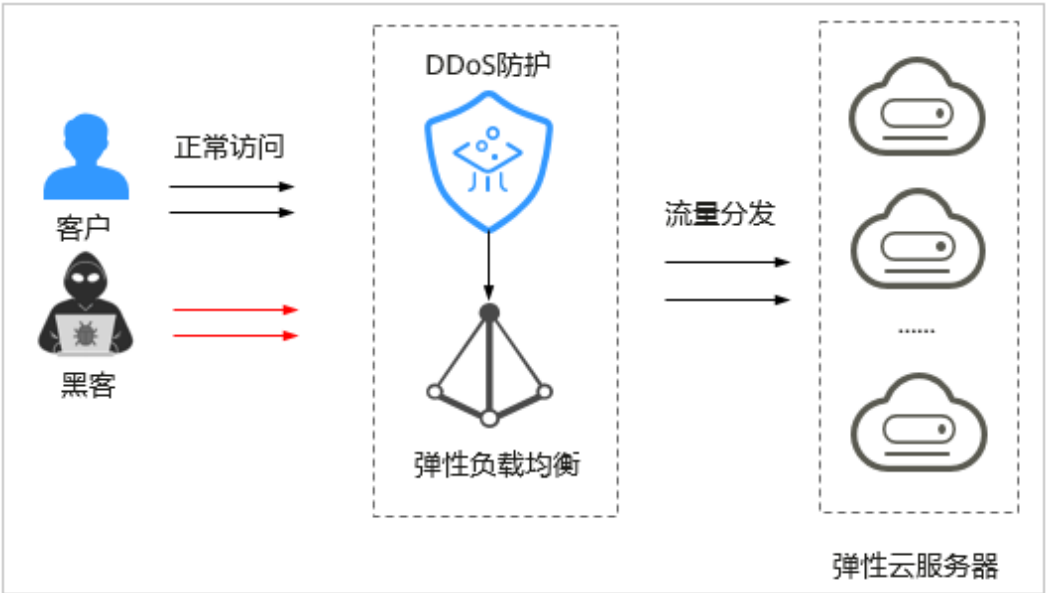
DDoS原生高级防护可以提升华为云弹性云服务器ECS、弹性负载均衡ELB等云服务的DDoS防御能力，确保云服务上的业务安全。

通过部署负载均衡ELB，并将ELB的公网IP地址接入DDoS原生高级防护，可以大幅度提高对不同类型DDoS攻击的防御能力。

方案架构

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。

图 3-1 华为云“DDoS 原生高级防护+ELB”联动防护



方案优势

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。

约束与限制

ELB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）。

资源和成本规划

资源	资源说明	数量	成本说明
弹性负载均衡 ELB	用于将访问流量分发到后端ECS服务器，缓解DDoS攻击造成的单点故障。	1	ELB的计费方式及标准请参考**ELB计费说明**。
DDoS原生高级防护	用于接入ELB的公网IP，防护DDoS攻击。	1	DDoS原生高级防护的计费方式及标准请参考**DDoS防护AAD计费说明**。

实施步骤

步骤1 创建一个负载均衡实例，具体操作请参考**创建负载均衡实例**。

表 3-1 关键参数说明

参数	说明
“区域”	选择与ECS实例相同的区域。
“弹性公网IP”	选择“现在购买”。
“线路”	选择“全动态BGP”。

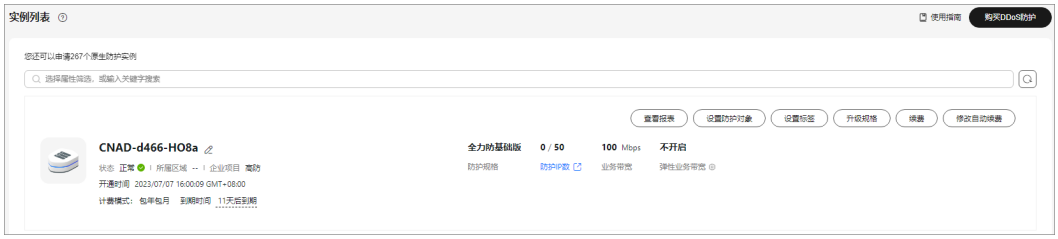
步骤2 获取创建的负载均衡实例的公网IP地址，如图3-2所示。

图 3-2 ELB 实例公网 IP

步骤3 在与ECS实例相同的区域购买DDoS原生高级防护实例。

步骤4 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 3-3 实例列表



步骤5 在目标实例所在框的右上方，单击“设置防护对象”。

步骤6 在弹出的“设置防护对象”对话框中，勾选步骤2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，请参见添加防护策略。

----结束

3.2 使用 WAF、ELB 和 DDoS 原生高级防护提升网站业务安全性

应用场景

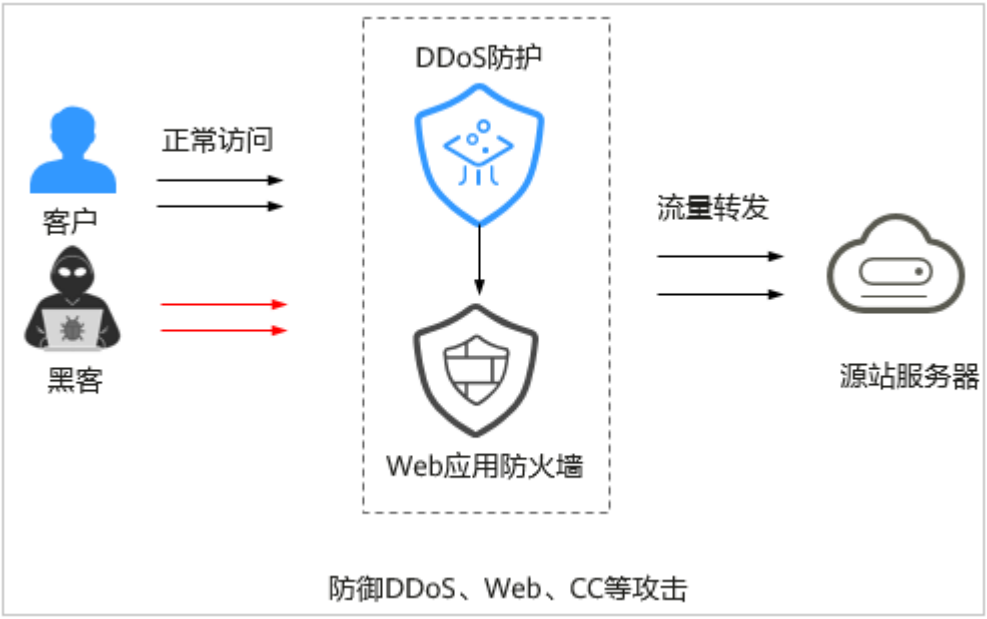
华为云Web应用防火墙（WAF）通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

DDoS原生高级防护可以为接入WAF（云模式-ELB接入）的网站类业务提供四层DDoS攻击防护，实现DDoS原生高级防护和云模式WAF（ELB接入）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。

方案架构

网站业务部署“DDoS原生高级防护+云模式WAF（ELB接入）”联动防护后，所有业务流量经过WAF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 3-4 华为云“DDoS 原生高级防护+WAF”联动防护



约束与限制

只支持已接入云模式WAF（ELB接入）的网站类业务，接入方法请参考**将网站接入WAF防护（云模式-ELB接入）**。

资源和成本规划

资源	资源说明	数量	成本说明
云模式WAF（ELB接入）	用于接入网站，提供Web、CC攻击防护。	1	WAF的计费方式及标准请参考**WAF计费说明**。
DDoS原生高级防护	用于防护接入WAF的网站类业务，提供DDoS攻击防护。	1	DDoS原生高级防护的计费方式及标准请参考**DDoS防护AAD计费说明**。

实施步骤

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“网络 > 弹性负载均衡 ELB”，进入“负载均衡器”页面。

步骤4 在WAF绑定的负载均衡器所在行，获取ELB的弹性公网IP。

图 3-5 复制弹性公网 IP

步骤5 在ELB的弹性公网IP所在的区域**购买DDoS原生高级防护实例**。

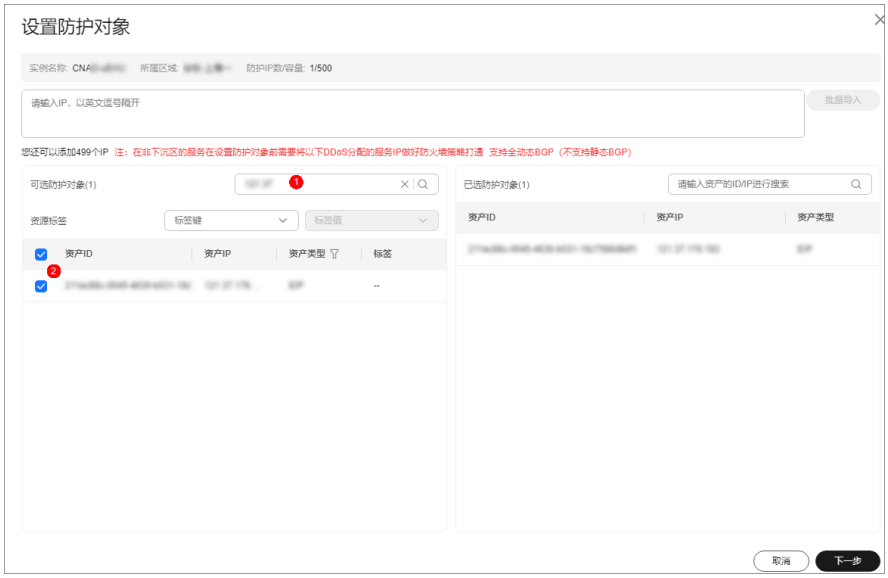
步骤6 单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”。

步骤7 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8 在目标实例所在框的右上方，单击“设置防护对象”。

步骤9 搜索**步骤4**中ELB的弹性公网IP，将其设置为防护对象，单击“下一步”。

图 3-6 添加防护对象



步骤10 为新增的防护IP选择防护策略后，单击“确定”。

图 3-7 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

4 DDoS 高防最佳实践

4.1 使用 DDoS 高防识别攻击类型

应用场景

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。

资源和成本规划

资源	资源说明	数量	成本说明
DDoS高防	用于提供DDoS攻击防护。	1	DDoS高防的计费方式及标准请参考**DDoS防护AAD计费说明**。

实施步骤

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 分别在“DDoS攻击防护”、“CC攻击防护”页面，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

4.2 使用 TOA 模块获取真实请求来源 IP

应用场景

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，客户业务源站所见的源IP为高防的回源IP，从tcp报文中的tcp option字段获取真实源IP，支持获取IPv6真实访问源。

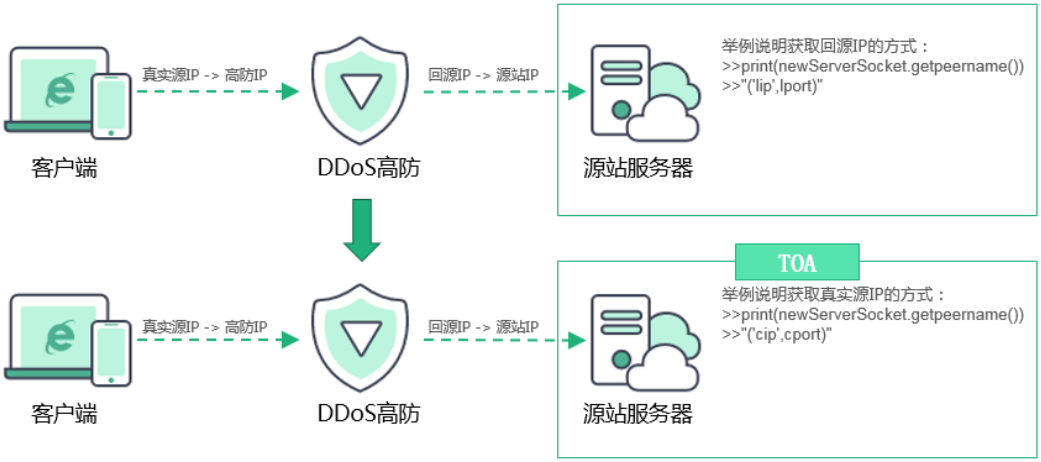
在业务应用开发中，通常需要获取客户端真实的IP地址。例如，投票系统为了防止刷票，需要通过获取客户端真实IP地址，限制每个客户端IP地址只能投票一次。

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。

方案架构

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4-1所示。

图 4-1 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。

约束与限制

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+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基础防护或源站配置为华为云WAF的场景，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，仅支持获取IPv4真实访问源。请参考**获取客户端真实IP**获取七层协议（HTTP）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。

实施步骤

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

4.3 使用 WAF 和 DDoS 高防实现域名防护

应用场景

华为云Web应用防火墙（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。

DDoS高防可以为域名提供连续性的有力保障，当服务器遭受大流量DDoS攻击时，DDoS高防可以保护用户业务持续可用。

通过WAF和DDoS高防双重防护，可以同时防御Web应用攻击和流量攻击，大幅提升域名的安全性和稳定性。

本实践建立在域名已接入了WAF，如何使网站流量同时经过DDoS高防和WAF进行防护，提升网站全面防护能力。

说明

域名接入WAF的方法请参考**将网站接入WAF防护**。

方案架构

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 4-2 联动原理

注意

如果您在DDoS高防使用同一实例和端口防护了多个域名，且域名源站为WAF CNAME时。当您在WAF侧的CNAME对应源站IP不同时，将WAF CNAME都Bypass后，会导致DDoS高防所有绑定相同高防IP和端口的域名不可用。

约束与限制

- “DDoS高防+云模式WAF”联动仅支持域名防护。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。

资源和成本规划

资源	资源说明	数量	成本说明
Web应用防火墙WAF	用于接入网站，提供Web、CC攻击防护。	1	WAF的计费方式及标准请参考**WAF计费说明**。
DDoS高防	用于防护接入WAF的域名，提供DDoS攻击防护。	1	DDoS高防的计费方式及标准请参考**DDoS防护AAD计费说明**。

实施步骤

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“是否使用七层代理”后的 。

图 4-3 基本信息

说明

如果WAF前使用的是华为云DDoS高防，要获取客户端真实IP，需要在域名基本信息页面的“流量标识”栏，将“IP标记”配置为“$remote_addr详细操作请参见”**配置攻击惩罚的流量标识**。

7. 在弹出界面，“是否使用七层代理”选择“是”，单击“确认”。
8. 在“基本信息”界面，复制CNAME。

图 4-4 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 4-5 配置网站类域名信息

表 4-1 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。
服务器配置	填写源站服务器使用的转发协议和端口。

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 4-6 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 4-7 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 4-8 添加记录集

表 4-2 关键参数

参数	说明
主机记录	填写DDoS高防中配置的域名。
记录类型	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。
记录值	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

4.4 使用 CDN 和 DDoS 高防防护动静态资源

应用场景

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。

方案架构

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图4-9所示。

- 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。

图 4-9 “DDoS 高防+CDN”联动方案原理说明

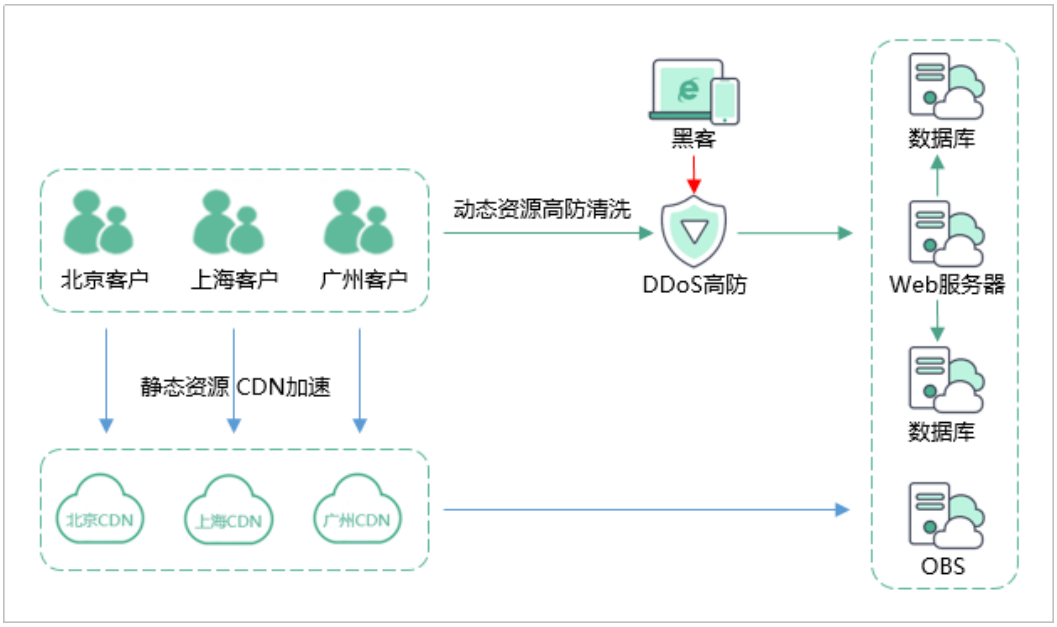


表 4-3 方案说明

类别	定义	举例	解决方案
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。

约束与限制

业务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。

资源和成本规划

资源	资源说明	数量	成本说明
内容分发网络CDN	用于加速静态资源。	1	CDN的计费方式及标准请参考**CDN计费说明**。
DDoS高防	用于防护动态资源。	1	DDoS高防的计费方式及标准请参考**DDoS防护AAD计费说明**。

实施步骤

步骤1 参考**添加CDN加速域名**完成静态资源接入。

步骤2 参考**域名网站类业务接入DDoS高防**完成动态资源接入。

----结束

4.5 网站业务迁移：从 DDoS 高防实例 A 到实例 B

应用场景

网站类业务接入DDoS高防后，如果您需要将源站IP/源站域名切换到其他DDoS高防实例进行防护，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。

资源和成本规划

资源	资源说明	数量	成本说明
DDoS高防实例	用于防护源站域名/源站IP。	2	DDoS高防的计费方式及标准请参考**DDoS防护AAD计费说明**。

实施步骤

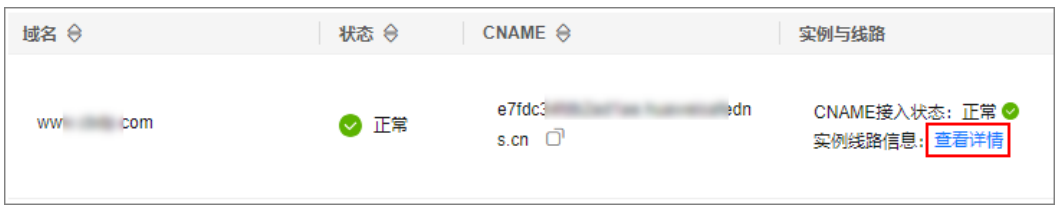
步骤1 登录管理控制台。

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 4-10 查看详情

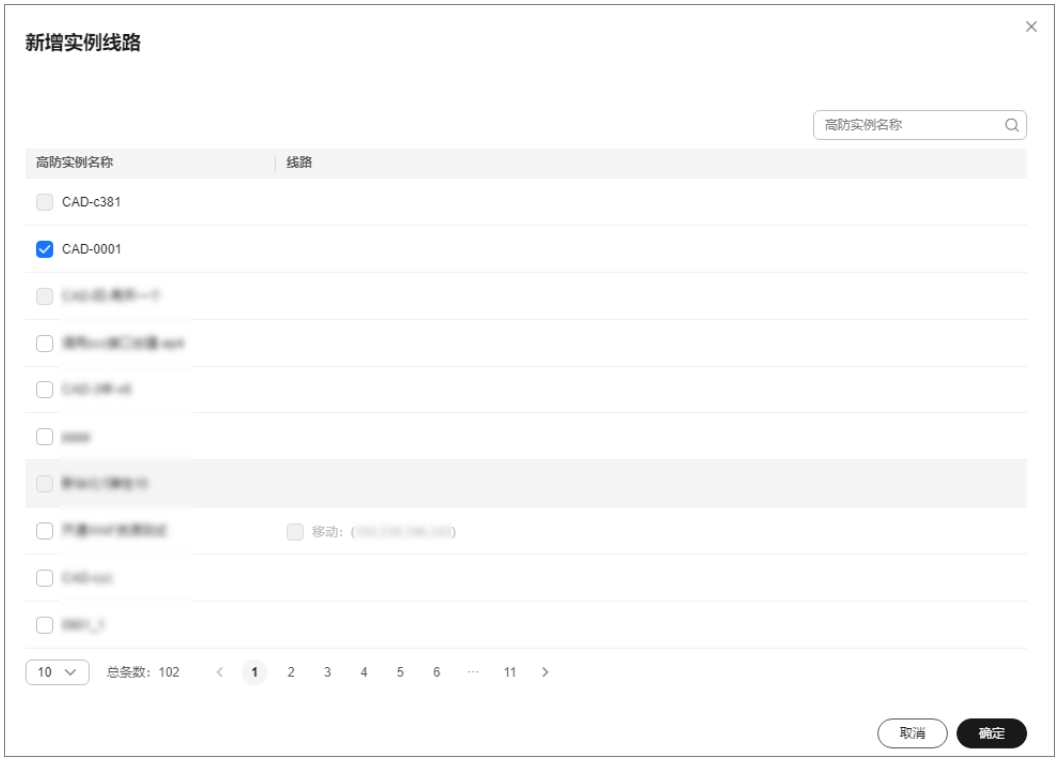


步骤5 在实例与线路列表右上方，单击“新增实例线路”。

图 4-11 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 4-12 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 4-13 线路解析

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

5 通过 DDoS 调度中心实现流量的阶梯调度

应用场景

如果您同时使用了DDoS原生防护全力防基础版和DDoS高防，您可以配置DDoS阶梯调度规则，系统联动调度DDoS高防对DDoS原生全力防基础版防护对象中的云资源进行防护，大幅提升DDoS攻击防护能力。

本章节以网站类业务“www.example.com”域名为例，介绍如何通过DDoS调度中心实现流量的阶梯调度。

方案架构

DDoS阶梯调度工作原理如图5-1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 5-1 DDoS 阶梯调度工作原理

方案优势

通过原生防护全力防基础版防御日常攻击，无需更换IP地址，业务流量直达源站服务器，不增加延迟。

发生海量攻击时，联动调度DDoS高防对DDoS原生全力防基础版防护对象中的云资源进行防护，业务流量经过DDoS高防转发。

约束与限制

- 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。

资源和成本规划

资源	资源说明	数量	成本说明
DDoS原生防护-全力防基础版	防御日常攻击，业务流量直达源站服务器。	1	计费方式及标准请参考**DDoS防护AAD计费说明**。
DDoS高防	防御海量攻击，业务流量经过DDoS高防转发。	1	

步骤一：购买并配置 DDoS 原生高级防护实例

步骤1 登录管理控制台。

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

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

步骤4 设置购买参数后，单击“立即购买”，根据提示完成支付。

- 实例类型：**DDoS原生防护**
- 计费模式：**包年包月**
- 防护区域：**中国大陆**
- 防护规格：**全力防基础版**
- 其他参数根据需要选择。

步骤5 选择“DDoS原生高级防护 > 实例列表”，进入实例列表页面。

步骤6 在目标实例所在行，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，勾选防护域名（www.example.com）的源站公网IP后，单击“下一步”。

步骤8 勾选需要的防护策略后，单击“确定”。

----结束

步骤二：购买并配置 DDoS 高防实例

步骤1 登录管理控制台。

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

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

步骤4 设置购买参数后，单击“立即购买”，根据提示完成支付。

- 实例类型：**“DDoS高防”**
- 接入类型：**“网站类”**
- 防护区域：**“中国大陆”**
- 其他参数根据需要选择。

步骤5 选择“DDoS高防 > 域名接入”，进入域名列表页面。

步骤6 在“中国大陆”页签，单击“添加域名”。

步骤7 填写域名信息后，单击“下一步”。

- 防护域名：需要防护的域名，如www.example.com。
- 源站类型：选择“源站IP”。
- 源站IP：填写防护域名的源站公网IP地址。
- 转发协议：源站服务器的转发协议。
- 源站端口：源站服务器使用的端口。

图 5-2 配置网站类域名信息

步骤8 选择高防实例与线路，单击“提交并继续”。

图 5-3 选择高防实例与线路

步骤9 单击“下一步”后，单击“完成”。

防护域名接入DDoS高防，获取高防实例的CNAME值，如图5-4所示。

图 5-4 防护域名接入 DDoS 高防

----结束

步骤三：配置阶梯调度

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。

- 规则名称：设置调度规则名称。
- 分组调度：选择要调度的DDoS原生高级防护实例所在**区域**、**源站IP**、**分组序号**。最多可添加10个IP。
- 联动调度：选择“联动到高防”。
- 高防CNAME：填写**步骤9**中获取的高防实例的CNAME值。

图 5-5 添加调度规则

步骤6 单击“确定”。

步骤7 在阶梯调度规则列表，获取调度CNAME。

图 5-6 调度 CNAME

----结束

步骤四：修改 DNS 解析

步骤1 登录管理控制台。

步骤2 在服务列表选择“网络 > 云解析服务 DNS”。

步骤3 在左侧导航栏选择“公网域名”。

步骤4 在防护域名（如www.example.com）所在行，单击“管理解析”。

步骤5 单击“添加记录集”，添加DNS解析。

- “记录类型”：选择“CNAME-将域名指向另外一个域名”。
- “线路类型”：全网默认。
- “记录值”：步骤7中获取的调度CNAME值。
- 其他参数根据需要选择。

----结束

