阿里云提供的DDoS防护解决方案包括免费的DDoS原生防护基础版服务和以下收费服务：DDoS原生防护企业版、DDoS高防（新BGP&国际）、游戏盾。下表描述了不同方案的具体说明。

**说明** 如果需要定制专属的安全解决方案，您可以通过电话咨询阿里云安全架构师，具体请联系[阿里云售前咨询](https://www.aliyun.com/support/95187" \t "_blank)。

| **名称** | **简介** | **应用场景** | **DDoS攻击防御能力** |
| --- | --- | --- | --- |
| [DDoS原生防护基础版](https://help.aliyun.com/document_detail/63643.html#section-y9w-gnp-17u) | 阿里云提供的基础服务，根据您所购买的阿里云产品（ECS、SLB、EIP、WAF）公网IP免费提供最大5 Gbps的DDoS防护能力。 | 购买阿里云产品即可获得基础的DDoS防护能力，仅可满足较低的安全需求，对于有最大安全防护需求的用户建议额外开通其他的安全方案。 | 支持防御不超过5 Gbps的DDoS攻击。  更多信息，请参见[DDoS原生防护套餐版本](https://help.aliyun.com/document_detail/63643.html#section-y9w-gnp-17u)。 |
| [DDoS原生防护企业版](https://help.aliyun.com/document_detail/63643.html#concept-63643-zh) | 阿里云提供的直接提升阿里云ECS、SLB、WAF、EIP等云产品DDoS防护能力的安全方案。  通过简单的配置，将DDoS原生防护企业版提供的安全能力直接加载到云产品上，提升其安全防护能力。 | * 在线视频、直播答题等对业务流畅要求比较高（低延迟）的DDoS攻击防护。 * 业务中存在大量端口、域名、IP的DDoS攻击防护。 | 支持[全力防护](https://help.aliyun.com/document_detail/40038.html?spm=a2c4g.11186623.2.14.3ac44f9fhHtYMm#section-iet-6rf-8p9)。 |
| [DDoS高防（新BGP、国际）](https://help.aliyun.com/document_detail/153308.html#concept-2417452) | 阿里云提供的解决互联网服务器（包括非阿里云主机）遭受大流量DDoS攻击的安全方案。  通过配置DDoS高防，将业务请求流量牵引至DDoS高防清洗，攻击流量被过滤，仅正常流量被转发到源站，确保源站服务器稳定可靠。 | * 金融、电商、门户类网站的DDoS攻击防护。 * 政府互联网出口、门户与开放平台的DDoS攻击防护。 * 重大线上直播、活动推广促销场景的DDoS攻击防护。 * 业务遭竞争对手恶意攻击、勒索场景的安全防护。 * 移动业务（App）遭恶意注册、刷单、刷流量场景的安全防护。 | * DDoS高防（新BGP）支持[弹性防护](https://help.aliyun.com/document_detail/40038.html" \l "section-y3t-edq-00t" \o ")。 * DDoS高防（国际）支持[高级防护](https://help.aliyun.com/document_detail/40038.html" \l "section-oum-a36-4bo" \o ")。 |
| [游戏盾](https://help.aliyun.com/document_detail/65033.html#concept-b3r-vc2-xdb) | 阿里云针对游戏行业面对的DDoS、CC攻击提供的行业针对性解决方案。  相比于DDoS高防，除有效防御大型DDoS攻击（T级别）外，游戏盾还具备彻底解决游戏行业特有的TCP协议的CC攻击问题的能力。 | * 游戏行业遭受大流量带宽压制场景的安全防护。 * 游戏行业遭受海量傀儡机长时间机器人攻击场景的安全防护。 | 支持防御Tbps级别的DDoS攻击。 |

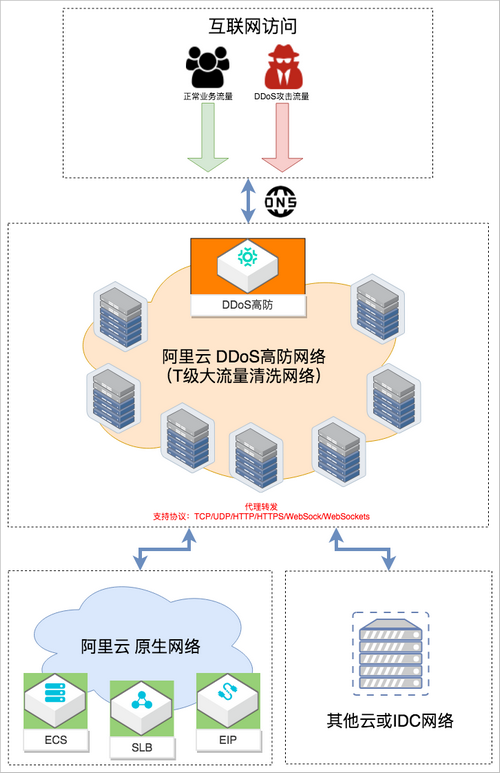
[上一篇：DDoS基础防护黑洞阈值](https://help.aliyun.com/document_detail/40033.html)

DDoS高防（Anti-DDoS）是阿里云提供的DDoS攻击代理防护服务。当您的互联网服务器遭受大流量的DDos攻击时，DDoS高防可以保护其应用服务持续可用。DDoS高防通过DNS解析调度流量到阿里云高防网络，代理接入阿里云DDoS防护系统，抵御流量型和资源耗尽型DDoS攻击。

## 工作原理

DDoS高防支持通过DNS解析和IP直接指向两种引流方式，实现网站域名和业务端口的接入防护。根据您在DDoS高防中为业务配置的转发规则，DDoS高防将业务的DNS域名解析或业务IP指向DDoS高防实例IP或CNAME地址进行引流。

来自公网的访问流量都将优先经过高防机房，恶意攻击流量将在高防流量清洗中心进行清洗过滤，正常的访问流量通过端口协议转发的方式返回给源站服务器，从而保障源站服务器的稳定访问。

[](http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/0690488951/p50168.png)

## DDoS高防服务类型

根据要接入DDoS高防进行防护的业务服务器部署地域的不同，DDoS高防提供新BGP（Anti-DDoS Pro）和国际（Anti-DDoS Premium）两种解决方案。

* [DDoS高防（新BGP）](https://help.aliyun.com/document_detail/69319.html#concept-69319-zh)：适用于业务服务器部署在**中国内地**地域的场景。采用中国内地独有的T级八线BGP带宽资源，为接入防护的业务防御超大流量的DDoS攻击。
* [DDoS高防（国际）](https://help.aliyun.com/document_detail/86301.html#concept-86301-zh)：适用于业务服务部署在**中国内地以外**地域的场景。依托世界领先的分布式近源清洗能力，为接入防护的业务提供不设上限的DDoS攻击全力防护能力。

更多信息，请参见[DDoS高防（新BGP）和DDoS高防（国际）的功能差异](https://help.aliyun.com/document_detail/153308.html?spm=a2c4g.11186623.6.590.46d5bdbbnsnWW8#section-kxj-agd-elk)。

## 产品优势

与传统DDoS攻击安全解决方案相比，阿里云DDoS高防具有部署简便、BGP网络质量高、防护能力大、系统稳定可用、防护精准，以及先进的AI智能防护技术等优势。

* 部署简便（5分钟完成部署）

根据您的业务特性，提供DNS解析和IP直接指向两种接入方式，实现网站域名和业务端口的接入防护。无需安装任何软硬件或调整路由配置，5分钟内即可完成部署和激活。

* 海量防御带宽资源

DDoS高防拥有中国内地超过8 Tbps、海外及港澳台地区超过2 Tbps的海量防御带宽资源，有效抵御所有各类基于网络层、传输层及应用层的DDoS攻击。

* 精准防护

针对交易类、加密类、七层应用、智能终端、在线业务攻击等实现精准防护，使得威胁无处可逃。

* AI智能防护

在流量清洗技术方面，分别针对网络流量型攻击和资源耗尽型DDoS攻击，通过自动优化防护算法和深度学习业务流量基线，达到精准识别攻击IP并自动过滤清洗的目的。

* 弹性防护

DDoS防护支持弹性调整防护带宽。您可在DDoS高防管理控制台自助升级，秒级生效，且无需新增任何物理设备。同时，业务上也无需进行任何调整，整个过程服务无中断。

* 保护源站安全

DDoS高防使用高防IP对您的业务站点进行隐藏，使攻击者无法找到您的源站地址，从而增加源站的安全性。

* 网络流量型DDoS攻击防护

大量针对网络传输层的攻击会使网络堵塞、机房不可用，而使您的网络业务中断或大面积瘫痪。在传统的代理、探测、反弹、认证、黑白名单、报文合规等标准技术的基础上，DDoS高防结合IP信誉、近源清洗，以及通过对网络指纹、用户行为、内容特征的深度包检测等多种技术的应用，可实现对威胁进行阻断和自定义过滤，并保证被防护的业务在遭受持续攻击时，仍可对外正常提供服务。

* 资源耗尽型DDoS攻击防护（CC攻击）

当攻击使网络应用层的服务器业务中断时，DDoS高防将对应用层的资源耗尽型DDoS攻击全面集成AI智能防护引擎，通过自定义过滤频率和精细至URL级别的过滤特征来提升防护效率和成功率，同时也大大降低了安全运维人员的工作难度。AI智能防护引擎基于以下特征进行防护：

* + 自学习用户业务流量和特征
  + 动态生成正常业务基线
  + 快速发现流量和特征异常
  + 自动介入分析攻击特征
  + 自动生成多维度组合策略
  + 动态执行或撤销防护策略指令
* 稳定、高可用
  + DDoS高防采用高可用网络防护集群，避免单点故障和冗余，且处理性能支持弹性扩展。全自动检测和攻击策略匹配，提供实时防护，清洗服务可用性达99.99%。
  + 对流量清洗机房的所有入流量、所有服务器CPU和内存进行监控，保障机房可用性。同时，针对服务器的引擎进行可用状态监控，并且具备自动下线和恢复机制。
  + 针对回源链路进行可用性监控，一旦发现不稳定，自动切换至备用链路，保障链路可用性。
  + 针对接入防护的源站服务器进行健康检查，一旦发现异常，自动切换。针对源站服务器的HTTP状态码进行监控，发现异常后自动启用回源或者切换等操作。
* 具备流量调度能力

DDoS高防服务可基于云产品的安全事件，通过DNS解析进行流量调度，实现在其他云产品未遭受DDoS攻击时不启用DDoS防护，而在遭受DDoS攻击时可以快速关联DDoS高防资源并启用DDoS防护功能。用户可根据自己的业务场景自定义配置调度模版，实现与云产品联动，自动化调度DDoS防护能力。

## 应用场景

阿里云DDoS高防适用于金融、电商、门户类网站，政府互联网出口、门户与开放平台，重大线上直播、活动推广促销的DDoS攻击防护场景，以及业务遭竞争对手恶意攻击、勒索，移动业务遭恶意注册、刷单、刷流量等安全防护场景。

在上述行业中，当业务存在以下安全风险时，推荐您使用DDoS高防：

* 遭受恶意攻击者的DDoS攻击勒索。
* DDoS攻击已经导致业务不可用，需要紧急恢复。
* 频繁遭受DDoS攻击，需要持续防护DDoS攻击，保护业务的稳定性。

## DDoS高防（新BGP）和DDoS高防（国际）的功能差异

下表罗列了只在DDoS高防（新BGP）或DDoS高防（国际）中支持的功能，方便您了解两者的功能差异。如果某个功能未在表中出现，则表示DDoS高防（新BGP）和DDoS高防（国际）均支持该功能。

**注意** 下表仅用于说明使用DDoS高防（新BGP）或DDoS高防（国际）服务过程中的具体功能点差异，并非作为您选择服务的依据。一般情况下建议您为部署在**中国内地**地域的业务开通DDoS高防（新BGP）服务，为部署在**中国内地以外**地域的业务开通DDoS高防（国际）服务。

标识释义：√表示支持，×表示不支持。

| **功能** | **描述** | **新BGP** | **国际** | **相关文档** |
| --- | --- | --- | --- | --- |
| 实例管理-  加速线路 | 加速线路必须与DDoS高防（国际）保险版或无忧版结合使用，用于实现中国内地用户对部署在非中国内地地域业务的访问加速。 | × | √ | [加速线路计费方式](https://help.aliyun.com/document_detail/106124.html#concept-dmb-1fg-4gb)  [配置DDoS高防（国际）加速线路](https://help.aliyun.com/document_detail/92502.html#task1328) |
| 实例管理-  安全加速线路 | 安全加速线路可以实现中国内地地区用户对非中国内地业务加速访问的同时，提供大流量DDoS攻击防护能力。 | × | √ | [安全加速线路计费方式](https://help.aliyun.com/document_detail/171811.html#concept-86324-zh)  [配置DDoS高防（国际）安全加速](https://help.aliyun.com/document_detail/171687.html#task-2537143) |
| 实例管理-  全局高级防护 | 全局高级防护需要与DDoS高防（国际）保险版结合使用，用于在DDoS高防（国际）保险版实例提供的每月两次高级防护次数耗尽时，获得更多的高级防护使用次数。 | × | √ | [全局高级防护计费方式](https://help.aliyun.com/document_detail/106119.html#concept-tzp-g2m-42b)  [购买全局高级防护](https://help.aliyun.com/document_detail/168964.html#task-1796740) |
| 域名接入-  启用HTTP2 | **填写网站信息**中支持**启用HTTP2.0**。 | √ | × | [添加网站](https://help.aliyun.com/document_detail/143347.html#task-2325689) |
| 域名接入-  Cname Reuse | **填写网站信息**中支持开启**Cname Reuse**。 | × | √ | [CNAME复用](https://help.aliyun.com/document_detail/130787.html#task-2323869) |
| 流量调度器-  出海加速 | **通用联动**规则中支持**出海加速**场景。 | × | √ | [概述](https://help.aliyun.com/document_detail/130783.html#task-2322746) |
| 流量调度器-  安全加速 | **通用联动**规则中支持**安全加速**场景。 | × | √ | [概述](https://help.aliyun.com/document_detail/130783.html#task-2322746) |
| 基础设施DDoS防护-  设置近源流量压制 | 针对访问DDoS高防实例的电信或联通线路的海外流量实行主动封禁。 | √ | × | [设置近源流量压制](https://help.aliyun.com/document_detail/95507.html#task799) |
| 基础设施DDoS防护-  黑洞解封 | 在DDoS高防控制台使用黑洞解封来快速恢复被攻击触发黑洞的业务。 | √ | × | [黑洞解封](https://help.aliyun.com/document_detail/95500.html#task664) |
| 调查分析-  操作日志 | 查看近30天的重要操作日志。 | √ | × | [查看操作日志](https://help.aliyun.com/document_detail/122475.html#task-2407471) |
| 调查分析-  高级防护日志 | 查看近30天的全局高级防护记录。 | × | √ | [查看高级防护日志](https://help.aliyun.com/document_detail/153141.html#task-2407471) |

## DDoS攻击损失保障

DDoS高防支持**DDoS攻击损失保障**服务，防止由于DDoS攻击导致您受DDoS高防保护的云服务器ECS、负载均衡SLB实例因使用量激增而产生额外的费用。如果为了响应DDoS攻击，这些受保护的实例产生了额外的后付费流量，您可以提交[工单](https://selfservice.console.aliyun.com/ticket/category/ddos/today)申请代金券补偿。