ALIBABA CLOUD

# 阿里云

## DDoS防护

## 阿里云DDoS防护产品介绍

文档版本：20220527

阿里云

# 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

| 格式 | 说明 | 样例 |
| --- | --- | --- |
| 危险 | 该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 危险<br>重置操作将丢失用户配置数据。 |
| 警告 | 该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 警告<br>重启操作将导致业务中断，恢复业务时间约十分钟。 |
| 注意 | 用于警示信息、补充说明等，是用户必须了解的内容。 | 注意<br>权重设置为0，该服务器不会再接受新请求。 |
| 说明 | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。 | 说明<br>您也可以通过按Ctrl+A选中全部文件。 |
| > | 多级菜单递进。 | 单击**设置**> **网络**> **设置网络类型**。 |
| **粗体** | 表示按键、菜单、页面名称等UI元素。 | 在**结果确认**页面，单击**确定**。 |
| Courier字体 | 命令或代码。 | 执行 `cd /d C:/window` 命令，进入Windows系统文件夹。 |
| *斜体* | 表示参数、变量。 | `bae log list --instanceid`<br>*Instance_ID* |
| [] 或者 [a\|b] | 表示可选项，至多选择一个。 | `ipconfig [-all\|-t]` |
| {} 或者 {a\|b} | 表示必选项，至多选择一个。 | `switch {active\|stand}` |

# 目录

# 1.概述

针对DDoS攻击的防护，阿里云提供多种安全解决方案，您可以根据实际业务场景和安全需求选择最合适的方案。本文介绍了不同DDoS防护解决方案的基本信息和适用场景。

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。

| 名称 | 简介 | 应用场景 | DDoS攻击防御能力 |
| --- | --- | --- | --- |
| DDoS原生防护基础版 | 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（含NAT）、轻量服务器、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。<br>更多信息，请参见DDoS原生防护套餐版本。 |
| DDoS原生防护企业版 | 阿里云提供的直接提升阿里云ECS、SLB、EIP（含NAT）、轻量服务器、WAF等云产品DDoS防护能力的安全方案。<br>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。<br>• 业务中存在大量端口、域名、IP的DDoS攻击防护。 | 支持全力防护。 |
| DDoS高防（新BGP、国际） | 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。<br>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。<br>• 政府互联网出口、门户与开放平台的DDoS攻击防护。<br>• 重大线上直播、活动推广促销场景的DDoS攻击防护。<br>• 业务遭竞争对手恶意攻击、勒索场景的安全防护。<br>• 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。<br>• DDoS高防（国际）支持高级防护。 |
| 游戏盾 | 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。<br>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。<br>• 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。 |

| 名称 | 简介 | 应用场景 | DDoS攻击防御能力 |
| --- | --- | --- | --- |

# 2.DDoS原生防护

## 2.1. 什么是DDoS原生防护

DDoS原生防护是一款针对阿里云ECS、SLB、EIP（含NAT）、轻量服务器、WAF等云产品直接提升DDoS防御能力的安全产品。相比于DDoS高防，DDoS原生防护可以直接把防御能力加载到云产品上，不需要更换IP，也没有四层端口、七层域名数等限制。DDoS原生防护部署简易，购买后只需要绑定需要防护的云产品的IP地址即可使用，几分钟内生效。

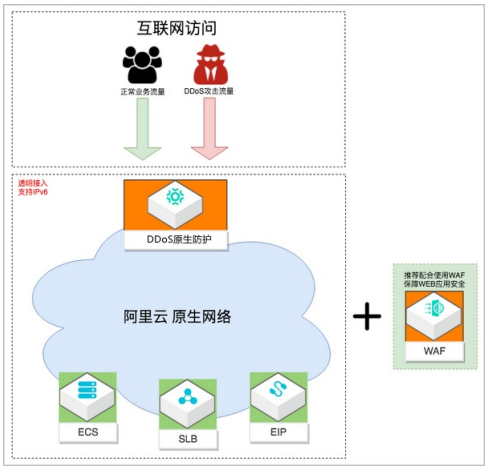
### 使用限制

DDoS原生防护企业版目前仅支持在中国内地地域直接开通。在中国内地以外地域开通原生防护企业版时，需要提交工单或者联系销售人员，通过审核后才能开通。

### 工作原理

DDoS原生防护直接为阿里云公网IP资源（包括ECS、SLB、EIP（含NAT）、轻量服务器、WAF）提升DDoS攻击防御能力，主要提供针对三层和四层流量型攻击的防御服务。当流量超出DDoS原生防护的默认清洗阈值后，自动触发流量清洗，实现DDoS攻击防护。

DDoS原生防护采用被动清洗方式为主、主动压制为辅的方式，针对DDoS攻击在反向探测、黑白名单、报文合规等标准技术的基础上，保证被防护用户在攻击持续状态下，仍可对外提供业务服务。DDoS原生防护通过在阿里云机房出口处建设DDoS攻击检测及清洗系统，采用旁路部署方式。




### 应用场景

DDoS原生防护适用于部署在阿里云上的业务，能够满足业务规模大、对网络质量要求高的用户。此类型用户虽然遭受DDoS攻击风险较低，但是一旦遭受DDoS攻击导致业务中断或受损，将会带来巨大的商业损失。阿里云DDoS原生防护可在最小接入成本的情况下提升DDoS防护能力，降低DDoS攻击对业务带来的潜在风险。

DDoS原生防护适用于具有以下特征的业务：

- 资源部署在阿里云上。
- 需要保护的公网IP数量多。
- 业务带宽或QPS较大。
- 具有IPv6访问流量的防护需求。

### DDoS原生防护套餐版本

DDoS原生防护提供基础版和企业版套餐。

- 基础版（DDoS基础防护）：默认为阿里云资源公网IP免费开启，无需购买。提供不超过5 Gbps的DDoS基础防护能力，具体请参见DDoS基础防护黑洞阈值。
- 企业版：购买后开启，提供全力防护能力。全力防护指阿里云根据当前机房网络的整体水位，尽可能帮助您防御DDoS攻击。随着阿里云网络能力的不断提升，全力防护的防护能力也会相应提升，而不需要您额外付出升级成本。
  - 支持防护阿里云资源公网IP，例如ECS、SLB、EIP、WAF。
  - 支持防护海外IDC服务器或云上按照网段去实现DDoS防护，提供代播实例。代播实例请联系销售人员购买。

  关于DDoS原生防护的详细计费说明，请参见DDoS原生防护计费方式。

### 产品优势

DDoS原生防护具有以下优势：

- 即刻购买，即刻生效。最短一分钟内即可完成DDoS原生防护的部署，直接把防御能力加载到云产品，免去部署和切换IP的烦恼。
- 具备弹性防护能力，遭受大规模攻击时调用当前地域阿里云最大DDoS防护能力提供全力防护。
- 采用阿里云BGP带宽，覆盖电信、联通、移动、教育网、长城宽带等不同的运营商，只需要一个IP，即可实现多个不同运营商的极速访问。
- 海量清洗带宽，满足活动大促、活动上线、重要业务的安全稳定性保障需求。
- 支持多个IP共享防护能力，满足多个IP地址都需要提升防御带宽的需求。
- 部分地域支持IPv6防护，具体请参见DDoS基础防护黑洞阈值。

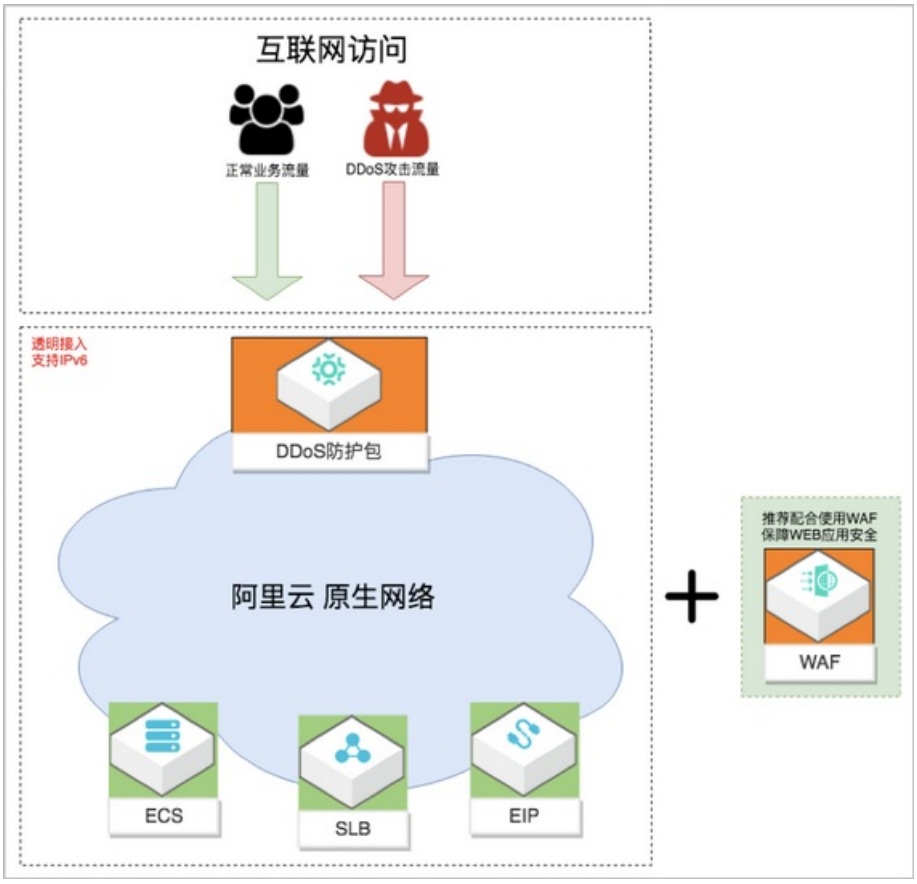
## 2.2. 应用场景

DDoS原生防护企业版主要提供针对三层和四层流量型攻击的防御服务。当流量超出DDoS原生防护企业版的默认清洗阈值后，自动触发流量清洗，实现DDoS攻击防护。

### 概述

DDoS原生防护企业版适用于部署在阿里云上的业务，能够满足业务规模大、对网络质量要求高的用户。此类型用户虽然遭受DDoS攻击风险较低，但是一旦遭受DDoS攻击导致业务中断或受损，将会带来巨大的商业损失。阿里云DDoS原生防护企业版可在最小接入成本的情况下提升DDoS防护能力，降低DDoS攻击对业务带来的潜在风险。DDoS原生防护企业版适用于具有以下特征的业务：

- 资源部署在阿里云上。
- 需要保护的公网IP数量多。
- 业务带宽或QPS较大。
- 具有IPv6访问流量的防护需求。




## 攻击类型适用性

下表描述了DDoS原生防护企业版适合防御的DDoS攻击类型。

| 攻击类型 | 是否适用 | 最佳防御配置 |
| --- | --- | --- |
| SSDP、NTP、Memcached等反射型攻击 | 是 | 推荐使用**DDoS原生防护企业版 > SLB > ECS**的部署方式，通过负载均衡丢弃未监听协议和端口的流量，获得更好的防护效果。 |
| UDP Flood攻击 | 是 | |
| SYN Flood攻击（大包攻击） | 是 | |
| SYN Flood攻击（小包攻击） | 是 | 推荐使用代理模式的DDoS高防服务。 |
| 连接数攻击 | 是 | 推荐使用代理模式的DDoS高防服务。 |
| CC攻击 | 否 | 推荐使用**DDoS原生防护企业版+Web应用防火墙**的部署方式，由Web应用防火墙防御CC攻击，DDoS原生防护企业版防御流量攻击，获得更好的防护效果。 |
| Web攻击 | 否 | |

## 业务场景适用性

下表描述了DDoS原生防护企业版适用的业务场景。

| 业务类型 | 是否适用 | 最佳防御配置 |
| --- | --- | --- |
| 网站类业务 | 是 | • 只需要防御DDoS攻击：<br>推荐使用**DDoS原生防护企业版 > SLB > ECS**的部署方式，通过负载均衡丢弃未监听协议和端口的流量，获得更好的防护效果。<br>• 需要防御DDoS攻击和CC攻击、Web攻击：<br>推荐使用**DDoS原生防护企业版+Web应用防火墙**的部署方式，由Web应用防火墙防御CC攻击，DDoS原生防护企业版防御流量攻击，获得更好的防护效果。 |
| 游戏类业务 | 否 | 推荐使用游戏盾服务进行防护。 |
| UDP服务类业务 | 否 | 推荐使用DDoS高防服务或游戏盾服务。 |
| App应用类业务 | 是 | 推荐使用**DDoS原生防护企业版 > SLB > ECS**的部署方式，通过负载均衡丢弃未监听协议和端口的流量，获得更好的防护效果。 |

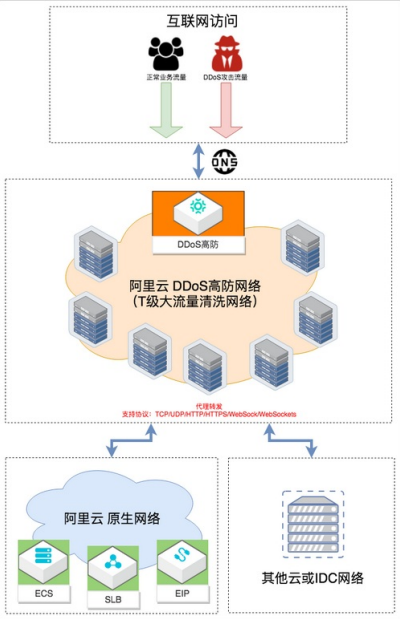
# 3.什么是DDoS高防（新BGP&国际）

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。




## 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）：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）：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。

## 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-<br>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<br>配置DDoS高防（国际）加速线路 |
| 实例管理-<br>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<br>配置DDoS高防（国际）安全加速 |
| 实例管理-<br>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。 | × | √ | 高级防护资源包计费方式<br>购买高级防护资源包 |
| 域名接入-<br>启用HTTP2 | **填写网站信息**中支持**启用HTTP2.0**。 | √ | × | 添加网站 |
| 域名接入-<br>Cname Reuse | **填写网站信息**中支持开启**Cname Reuse**。 | × | √ | CNAME复用 |
| 流量调度器-<br>出海加速 | **通用联动**规则中支持**出海加速**场景。 | × | √ | 概述 |

| 功能 | 描述 | 新BGP | 国际 | 相关文档 |
| --- | --- | --- | --- | --- |
| 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 |
| 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 |
| 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 |
| 调查分析-操作日志 | 查看近30天的重要操作日志。 | √ | × | 查询操作日志 |
| 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 |

## IPv4高防IP和IPv6高防IP的功能差异（DDoS高防（新BGP））

DDoS高防（新BGP）实例支持IPv4高防IP和IPv6高防IP，下表罗列了IPv4高防IP和IPv6高防IP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IPv4高防IP和IPv6高防IP均支持该功能。

标识释义：√表示支持，×表示不支持。

| 功能 | IPv4高防IP | IPv6高防IP | 相关文档 |
| --- | --- | --- | --- |
| 黑白名单 | √ | √ | 设置黑白名单（针对高防实例IP）<br>设置黑白名单（针对域名） |
| UDP反射攻击防护 | √ | × | 设置UDP反射攻击防护 |
| 近源流量压制 | √ | × | 设置近源流量压制 |
| 四层区域封禁 | √ | × | 设置区域封禁 |
| 区域封禁（针对域名） | √ | √ | 设置区域封禁（针对域名） |
| 黑洞解封 | √ | × | 黑洞解封 |
| 连接已被黑洞的服务器 | √ | √ | 连接已被黑洞的服务器 |
| AI智能防护 | √ | √ | 设置AI智能防护 |
| 精准访问控制 | √ | √ | 设置精准访问控制 |
| 频率控制 | √ | √ | 设置频率控制 |

| 功能 | IPv4高防IP | IPv6高防IP | 相关文档 |
| --- | --- | --- | --- |
| DDoS全局防护策略 | √ | √ | 设置DDoS全局防护策略 |
| 四层AI智能防护 | √ | × | 设置四层AI智能防护 |
| DDoS防护策略（虚假源和空连接检测、源限速、目的限速） | √ | √（不支持源限速功能，其余功能支持） | 设置DDoS防护策略 |
| 流量调度器 | √ | × | 概述 |
| 攻击分析 | √ | × | 攻击分析 |

## 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，您可以提交工单申请代金券补偿。

# 4.选型参考

阿里云基于多年的DDoS攻防经验和安全技术，提供多款正式商用的DDoS防护解决方案供您选择，满足您业务中对各类DDoS攻击安全防护场景的需求。本文介绍了在不同DDoS攻击防御场景下如何选择合适的DDoS防护产品或方案。

## 适合的防御场景

| 防御场景 | 场景特点 | 防护能力介绍 | 选择版本套餐 |
| --- | --- | --- | --- |
| 防御高风险DDoS攻击（推荐使用DDoS高防） | • 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。<br>• 遭受恶意攻击者的DDoS攻击勒索。<br>• DDoS攻击已经导致您的业务不可用，需要紧急恢复。<br>• 频繁遭受DDoS攻击，需要持续防护DDoS攻击，保护业务的稳定性。<br>• 移动业务遭恶意注册、刷单、刷流量等安全防护场景。 | 可以解决公有云上服务器（包括非阿里云主机）遭受大流量DDoS攻击的问题。通过DNS解析方式牵引流量到阿里云全球DDoS防护网络，清洗流量型和资源耗尽型DDoS攻击，隐藏被保护的源站服务器。 | 参考以下说明选择DDoS高防的版本套餐：<br>• 业务服务器部署在**中国内地**，且主要服务于**中国内地**的用户，推荐使用DDoS高防（新BGP）专业版。<br>• 业务服务器部署在**中国内地以外**，且主要服务于**中国内地以外**的用户，推荐使用DDoS高防（国际）保险版或无忧版。<br>• 业务服务器部署在**中国内地以外**，但主要服务于**中国内地**的用户，推荐使用DDoS高防（国际）出海套餐或DDoS高防（国际）安全加速线路。 |

| 防御场景 | 场景特点 | 防护能力介绍 | 选择版本套餐 |
| --- | --- | --- | --- |
| 防御（大规模业务）低风险DDoS攻击（推荐使用DDoS原生防护） | • 业务资源部署在阿里云环境。<br>• 业务规模较大。例如，业务带宽大于1 Gbps，HTTP和HTTPS业务QPS大于5,000。<br>• 需要保护的公网IP数量多。例如数十个甚至数千个IP需要防护。<br>• 需要防护的端口数量多。例如每个服务器上有数十个端口。<br>• 偶尔遭受DDoS攻击。<br>• 具有IPv6访问流量的防护需求。 | 直接提升阿里云ECS、SLB、EIP（含NAT）、轻量服务器、WAF等云产品公网IP的DDoS防护能力。基于阿里云原生防护网络，不改变源站服务器IP地址，透明防护流量型DDoS攻击。 | 参考以下说明选择DDoS原生防护的套餐版本：<br>• 基础版默认开启。<br>• 如果基础版提供的不超过5 Gbps的防御能力不能满足业务需求，推荐您使用DDoS原生防护企业版。<br>  ◦ 如果只需要防御DDoS攻击，推荐使用负载均衡+原生防护企业版的部署方式，由负载均衡丢弃未监听协议和端口的流量，获得更好的防护效果。<br>  ◦ 如果需要防御DDoS攻击和Web攻击、CC攻击，推荐使用Web应用防火墙+原生防护企业版的部署方式，由WAF防御CC攻击、DDoS原生防护企业版防御流量攻击，获得更好的防护效果。<br>• 如果需要Tbps级别原生防护能力，推荐使用具备DDoS防护（增强）功能的EIP和共享带宽包、共享流量包。 |
| 防御移动端业务为主的DDoS攻击（推荐使用游戏盾） | • 主要业务为移动端游戏业务。<br>• 具备集成阿里云SDK的能力。<br>• 业务实时性要求高，对自定义传输协议存在精细化防护需求。<br>• 具有网络传输加速需求。<br>• 具有网络加密传输需求。<br>• 需要追溯DDoS攻击的来源。 | 针对游戏行业面对的大规模DDoS、CC攻击提供防御能力。通过集成阿里云安全轻量级SDK，彻底解决App类业务的DDoS和CC攻击（包括游戏行业特有的TCP协议的CC攻击）问题。 | 无 |

## 适合的业务类型

| 业务类型 | DDoS高防 | DDoS原生防护 | 游戏盾 |
| --- | --- | --- | --- |
| 网站类业务 | ✓ | ✓ | × |
| UDP服务类业务 | ✓ | ✓ | ✓ |
| App应用类业务 | ✓ | ✓ | × |
| 游戏类业务 | ✓ | ✓ | ✓<br>（推荐） |

## 适合防御的DDoS攻击类型

下表中使用的符号说明如下：

- ✓：表示支持防御
- ×：表示不支持防御

| 攻击类型 | DDoS高防 | DDoS原生防护 | 游戏盾 |
| --- | --- | --- | --- |
| 畸形报文 | ✓ | ✓ | ✓ |
| 传输层DDoS攻击 | ✓ | ✓ | ✓ |
| DNS DDoS攻击 | ✓<br>支持针对DNS攻击进行清洗。如果需要保护NS服务，需要使用云解析抗DDoS服务。 | ✓<br>支持针对DNS攻击进行清洗。但如果需要保护NS服务，需要使用云解析抗DDoS服务。 | × |
| 连接型DDoS攻击 | ✓ | 即将发布。 | ✓ |
| Web应用层DDoS攻击 | ✓ | 即将发布。 | × |

# 5.DDoS应急防护方案

为帮助遭受DDoS攻击的企业快速止血，阿里云提供短期（一天）DDoS攻击应急防护方案，满足申请条件的用户可以申请该应急防护方案。长期防护DDoS攻击是降低被攻击风险的最佳途径，建议您考虑长期使用DDoS防护类服务。

## 一天应急服务

一天应急服务面向满足条件的企业用户免费开放，借助阿里云防护资源的优势，尽力帮助遭遇DDoS攻击的企业争取到应急时间，达到快速止血的目的。

**申请条件**

- 阿里云账号注册期和保有阿里云产品的时间超过三个月。
- 业务从未遭受过DDoS攻击或首次被攻击。
- DDoS攻击的带宽峰值小于100 Gbps。

**申请限制**

- 每个申请者每年最多可以申请一次一天应急服务。
- 提交申请时必须填写企业注册信息和联系人电话，并承诺一天应急服务的使用协议不可用于转售或者其他商业用途。

**申请入口**

单击前往一天应急服务申请页面。

**获取途径**

等待申请审核通过后，您可以在**DDoS高防**服务售卖页面开通免费的一天应急版本（**购买时长**配置为**1天**），如下图所示。

单击前往DDoS高防售卖页面。


## 长期防护服务

一天应急服务只用于暂时消除DDoS攻击带来的影响。长期防护DDoS攻击才是降低被攻击风险的最佳途径。建议您使用包年包月模式开通DDoS防护类服务，最大程度避免DDoS攻击给业务造成重大损失。

更多信息，请参见DDoS防护解决方案。

# 6.售前常见问题

本文列举了阿里云DDoS防护产品的售前常见问题。



## 阿里云DDoS防护是否提供免费服务？

提供。阿里云默认为每个阿里云用户开启免费的DDoS原生防护（即原生防护基础版），提供不超过5 Gbps的DDoS基础防护能力。免费的DDoS防护无需您购买、开通和配置。更多信息，请参见什么是DDoS原生防护。

另外，面向满足条件的企业用户，DDoS高防免费提供不超过1次/年的一天应急防护服务，支持防护不超过100 Gbps的DDoS攻击。更多信息，请参见一天应急服务。

阿里云不能免费帮助用户抵御无限的DDoS攻击。DDoS防御需要成本，其中最大的成本就是带宽费用。带宽由阿里云向电信、联通、移动等运营商购买，运营商在计算带宽费用时不会把DDoS攻击流量扣除掉，而是直接收取阿里云的带宽费用。阿里云DDoS防护为阿里云用户免费防御不超过5 Gbps的DDoS攻击流量，但是当攻击流量超出5 Gbps时，阿里云会屏蔽被攻击IP的流量，从而避免用户产生超额费用。

## 是否支持仅在业务被攻击时触发防护且收费，无攻击时不收费的DDoS高防服务？

目前不支持。DDoS高防采用包年包月的计费方式，您需要先购买DDoS高防实例并完成预付费，才能在实例有效期内使用DDoS高防服务。

## 阿里云DDoS防护产品是否支持试用？

- DDoS原生防护：您购买的阿里云公网IP资产默认开启了基础版防护（免费），享受不超过5 Gbps的DDoS基础防护能力；DDoS原生防护企业版为付费服务，暂不提供试用服务。

  > **注意** 企业版基于阿里云网络透明防护，且从基础版升级企业版，网络质量、延时和接入方式都不发生改变，因此建议您使用基础版进行网络测试。

- DDoS高防：由于DDoS高防服务依赖专用机房提供流量清洗服务，成本较高，因此不提供试用服务。但是支持在无DDoS攻击的情况下申请一天PoC试用，测试接入方法和网络效果。单击前往高防产品免费1天PoC测试申请页面。

## 非阿里云服务器是否能使用DDoS高防服务？

可以使用。DDoS高防（新BGP）和DDoS高防（国际）支持防护具有公网IP的服务器，只要您的业务使用的对外IP为公网IP，且与阿里云网络公网路由可达，都可以使用DDoS高防服务。更多信息，请参见什么是DDoS高防（新BGP&国际）。

## 服务器不在阿里云，域名在阿里云，是否能开通DDoS高防？

可以开通。如需开通DDoS高防（新BGP）防护该域名，必须保证域名已完成ICP备案。

## 使用阿里云DDoS高防是否需要完成域名备案？

如果您的域名要接入DDoS高防（新BGP）进行防护，则必须已经完成域名备案；接入DDoS高防（国际）进行防护时，不需要完成域名备案，但是业务必须合法合规。

关于域名备案的更多信息，请参见ICP备案流程概述。

## DDoS高防服务支持哪些地域？

- DDoS高防（新BGP）：适用于您的业务服务器部署在中国内地地域的场景。
- DDoS高防（国际）：适用于您的业务服务器部署在中国内地以外地域（包括中国香港等）的场景。

## DDoS高防是否限制接入域名的数量？

是，具体限制如下：

- 每个DDoS高防（新BGP）实例默认支持添加50个域名接入配置，且使用的不同一级域名（站点）数量不超过5个。
- 每个DDoS高防（国际）实例默认支持添加10个域名接入配置，且使用的不同一级域名（站点）数量不超过1个。

> **说明** 您可以在开通DDoS高防实例时扩展防护域名数规格，单个DDoS高防（新BGP）实例或DDoS高防（国际）实例最多支持添加200个域名接入配置。更多信息，请参见购买DDoS高防实例。

## DDoS高防是否支持泛域名？

支持。DDoS高防的**域名接入**配置中支持使用泛域名。更多信息，请参见添加网站。

泛域名解析指利用通配符（星号）作为次级域名，以实现所有的次级域名均指向同一个IP。例如，为www.aliyundoc.com配置泛域名解析后，访问*.aliyundoc.com都将解析到泛域名解析的IP。

## DDoS高防（新BGP）是否对接入端口有限制？

DDoS高防（新BGP）对接入端口没有限制，您可以将80~65535范围内任意端口的Web业务，接入**增强功能**的DDoS高防（新BGP）实例进行防护。更多信息，请参见自定义服务器端口。

但是，根据当前网络访问验证结果，互联网运营商侧或因部分高危端口存在安全隐患，会拦截针对高危端口的业务流量。相关的高危TCP端口包括：42、135、137、138、139、445、593、1025、1434、1068、3127、3128、3129、3130、4444、5554、5800、5900、9996。

如果您的Web业务使用了上述高危端口，则业务接入高防后，可能出现业务在部分地域无法被访问的问题。因此，建议您将业务接入高防前，确保Web业务使用其他非高危端口。

## 开通DDoS高防（国际）有什么要求吗？

开通DDoS高防（国际）防护网站业务时，您需要准备好域名（域名可以不用备案，但是业务要合规合法）；防护非网站业务时，您可以使用端口接入，无特殊要求。

## DDoS高防（新BGP）的保底带宽防护的是所有流量还是仅攻击流量？

DDoS高防（新BGP）的保底带宽防护所有接入DDoS高防（新BGP）实例的业务流量，包含正常业务流量和攻击流量。所有流量经过DDoS高防（新BGP）清洗后，正常的业务流量转发到您的源站服务器，攻击流量被直接拦截。