ALIBABA CLOUD

Alibaba Cloud

DDoS防护

产品定价

文档版本：20210120

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 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 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 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 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` *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

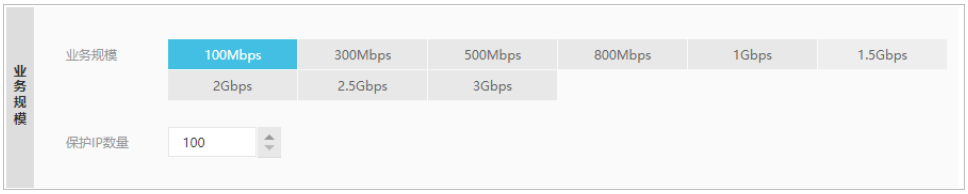
1.DDoS原生防护计费方式

DDoS原生防护提供基础版和企业版套餐。基础版默认开通，免费为您阿里云账号下的ECS、SLB、EIP、WAF实例提供不超过5 Gbps流量的DDoS攻击防御能力；企业版以包年方式计费，您必须通过预付费开通DDoS原生防护企业版实例，才能享受原生防护企业版提供的DDoS全力防护能力。

DDoS原生防护企业版实例规格

DDoS原生防护企业版实例默认提供DDoS共享全力防护能力。全力防护指根据当前机房网络和整体水位，尽可能对攻击进行防护，并且随着阿里云网络能力的不断提升，全力防护也会提升防护能力，不需要您额外付出升级成本。

DDoS原生防护企业版实例仅支持按年开通服务，订购时长包括1年、2年、3年。在创建DDoS原生防护企业版实例时，单个实例的包年单价由您选择的业务规模和保护IP数量决定。您只需选择与自身业务规模匹配的实例规格并完成一次性预付费，即可享用DDoS原生防护企业版服务。



- **业务规模**：指被防护业务的正常业务规模，以带宽来衡量，入方向或出方向流量按每月最大值95，可选规格：100 Mbps、300 Mbps、500 Mbps、800 Mbps、1 Gbps、1.5 Gbps、2 Gbps、2.5 Gbps、3 Gbps。 关于业务规模的估算方法，请参见估算业务规模。
- **保护IP数量**：需要DDoS原生防护实例保护的所有IP的数量，默认是100个，可选数量：100~255。

企业版计费规则

如果您需要保护的IP数量为100个，DDoS原生防护企业版套费用（单个地域）=业务规模月单价*12个月*订购年限。

如果您需要保护的IP数量超过100个，DDoS原生防护企业版套费用（单个地域）={业务规模月单价+（保护的IP数量-100）*30 USD/月}*12个月*订购年限。

业务规模月单价请参见下表。

> **说明** DDoS原生防护企业版套餐默认支持保护单个地域下的100个IP，每增加一个IP，其单价增加30 USD/月。如果您需要保护多个地域下的IP，则需要开通多个实例，或者提交工单申请定制。

下表描述了不同业务规模的DDoS原生防护实例每月的单价。如果以下价格信息与DDoS原生防护购买页存在差异，以DDoS原生防护购买页面上展示的实际价格为准。

> **说明** 需要防护的IP协议无论是IPV4或IPV6，DDoS原生防护实例每月价格没有差异。

业务规模	单价（USD/月）
100 Mbps	7,016
300 Mbps	9,025
500 Mbps	11,034

业务规模	单价（USD/月）
800 Mbps	14,047
1 Gbps	16,056
1.5 Gbps	21,079
2 Gbps	26,101
2.5 Gbps	31,124
3 Gbps	36,146

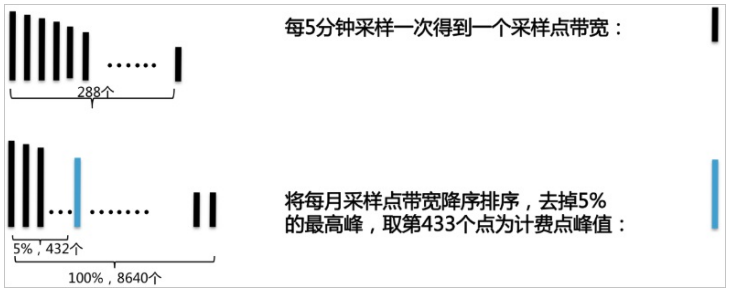
说明 默认100 Mbps业务规模起售，可选的最大业务规模为3 Gbps。如果您的业务规模超过3 Gbps，请提交工单申请定制。

估算业务规模

您可以按照以下方式估算业务规模（业务带宽）：

以5分钟为粒度采样，采集入方向和出方向的流量并计算入方向和出方向在5分钟内的平均带宽值，取入方向和出方向中较大的值作为采样点的带宽值。月底将所有的采样点按峰值从高到低排序，去掉5%的最高峰值采样点，以第95%个最高峰作为95计费点带宽。

下图是计费点带宽的示意图，以一个月30天为例。



如果实际业务带宽超过已购买的原生防护企业版实例的业务规模，会有什么影响？

原生防护企业版允许业务流量短期峰值超过购买的业务规模规格，但是如果一个月累计36小时超过规格，则全力防护会失效，仅保留原生防护的基础防护能力，正常业务带宽不会受到限制。

不支持退款

DDoS原生防护企业版实例不支持五天无理由退款。

联系我们

您可以通过工单或联系商务经理定制指定规格的DDoS原生防护企业版实例。

2.DDoS高防（新BGP）计费方式

本文介绍了DDoS高防（新BGP）服务的计费方式。

计费概述

DDoS高防（新BGP）为您部署在中国内地地域的业务提供针对DDoS攻击的**基础防护**和**弹性防护**服务。基础防护和弹性防护的具体计费方式如下：

- 基础防护：包年包月（按月-预付费）

  创建DDoS高防（新BGP）实例时，根据业务需要选择实例规格和购买时长，付费后开通实例。已开通的DDoS高防（新BGP）实例，在服务有效期内，为所有接入防护的业务提供保底防护能力。

  例如，创建实例时选择的保底防护带宽是30 Gbps，则接入防护的业务受到的DDoS攻击流量不超过30 Gbps时，可以直接防御，且不产生额外费用。

- 弹性防护：按量付费（按天-后付费）

  根据业务需要选择是否开启。如需开启，您只要将DDoS高防（新BGP）实例的弹性防护带宽设置为大于保底防护带宽的值，则接入防护的业务受到的DDoS攻击流量超过保底防护带宽但小于弹性防护带宽时，也可以防御，且产生发生攻击当日的弹性防护费用。

  例如，DDoS高防（新BGP）实例的保底防护带宽是30 Gbps，弹性防护带宽是100 Gbps，当接入防护的业务受到的DDoS攻击流量不超过30 Gbps或者大于100 Gbps时，不产生弹性防护费用，DDoS攻击流量在30~100 Gbps范围时，产生弹性防护费用。

更多关于DDoS高防（新BGP）的定价信息，请参见DDoS高防产品定价页。

基础防护（按月-预付费）

下表描述了默认规格下，不同DDoS防护能力（保底防护带宽）的DDoS高防（新BGP）实例的定价信息。根据实例支持的防护功能不同，DDoS高防（新BGP）实例分为标准功能和增强功能，两者的费用也有差别。关于标准功能和增强功能的更多信息，请参见DDoS高防（新BGP&国际）功能套餐。

> **说明** 如果下表描述的DDoS防护能力不能满足您的业务需求，您需要更高的DDoS防护能力，请提交工单联系我们。

DDoS防护能力	线路	标准功能费用	增强功能费用
30 Gbps	八线BGP	3,120美元/月	4,320美元/月
60 Gbps		7,020美元/月	8,220美元/月
100 Gbps		49,230美元/年（包年优惠价）	63,630美元/年（包年优惠价）
300 Gbps		79,260美元/年（包年优惠价）	93,660美元/年（包年优惠价）
400 Gbps		145,300美元/年（包年优惠价）	159,700美元/年（包年优惠价）
500 Gbps		563,430美元/年（包年优惠价）	577,830美元/年（包年优惠价）
600 Gbps		670,610美元/年（包年优惠价）	685,010美元/年（包年优惠价）

下表描述了DDoS高防（新BGP）实例的默认规格以及规格的扩展费用。如果您的实际业务需要超出实例的默认规格，您可以升级实例或在购买实例时对相应规格进行扩展。

名称	说明	默认情况	扩展单价
防护端口数	实例支持添加的TCP和UDP端口数量	50个	每5个端口：37.5美元/月
防护域名数	实例支持添加的HTTP和HTTPS域名数量	50个 **说明** 所有域名所属的一级域名总数不超过5个。	• 标准功能套餐：每10个域名45美元/月 • 增强功能套餐：每10个域名7.5美元/月 **说明** 每增加10个域名可增加一个一级域名。
业务带宽	实例支持处理的无攻击情况下最大业务流量	100 Mbps	每Mbps：15美元/月 **说明** 当实例的总业务带宽规格超出600Mbps时，超出部分的扩展业务带宽可享受优惠价（每Mbps：11美元/月）。
业务QPS	实例支持处理的无攻击情况下最大HTTP和HTTPS业务的并发请求速率	3,000 QPS	每100QPS：150美元/月

弹性防护（按天-后付费）

DDoS高防（新BGP）实例的弹性防护费用按照前一日实际发生的超出保底防护带宽的攻击流量部分的峰值（即选取当日内所遭受的DDoS攻击中的最大值后，扣除该实例的保底防护带宽值，得到超出部分的流量峰值）所对应的计费区间进行计算，生成后付费账单。

说明 如果您将DDoS高防（新BGP）实例的弹性防护带宽设置为与保底防护带宽一致，则不会产生任何后付费账单，但您的DDoS高防（新BGP）实例也将不具备弹性防护能力。

计费说明：

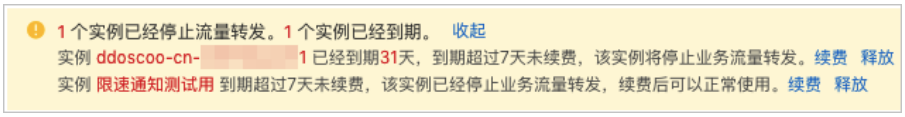
- 如果当日实际发生的DDoS攻击峰值不大于所购买的保底DDoS防护能力，则不会产生任何后付费。
- 当日实际发生的DDoS攻击峰值超过所设置的弹性防护带宽，则不会产生后付费账单。即如果当日实际遭受的DDoS攻击导致所防护的IP被黑洞，则不收取弹性防护费用。
- 当日的弹性防护费用账单一般在第二天上午八点至九点生成。

例如，您的DDoS高防（新BGP）实例的保底防护带宽规格是30 Gbps，弹性防护带宽规格是100 Gbps。当日该实例遭受两次DDoS攻击，其中一次攻击的峰值为80 Gbps，另一次攻击的峰值为40 Gbps，两次攻击均超过保底防护带宽。系统将选取当日所遭受的最大攻击峰值80 Gbps，并扣除实例的保底防护带宽30 Gbps，得到50 Gbps，按照“40 Gbps<攻击峰值≤50 Gbps”的计费区间计算当日所产生的弹性防护费用，即960美元。

下表描述了不同计费区间的弹性防护费用。

计费区间	弹性防护费用（单位：美元/天）
0 Gbps<攻击峰值≤5 Gbps	120
5 Gbps<攻击峰值≤10 Gbps	180
10 Gbps<攻击峰值≤20 Gbps	330
20 Gbps<攻击峰值≤30 Gbps	540
30 Gbps<攻击峰值≤40 Gbps	730
40 Gbps<攻击峰值≤50 Gbps	960
50 Gbps<攻击峰值≤60 Gbps	1,170
60 Gbps<攻击峰值≤70 Gbps	1,380
70 Gbps<攻击峰值≤80 Gbps	1,590
80 Gbps<攻击峰值≤100 Gbps	1,770
100 Gbps<攻击峰值≤150 Gbps	2,190
150 Gbps<攻击峰值≤200 Gbps	3,240
200 Gbps<攻击峰值≤300 Gbps	4,200
300 Gbps<攻击峰值≤400 Gbps	6,000
400 Gbps<攻击峰值≤500 Gbps	7,510
500 Gbps<攻击峰值≤600 Gbps	9,010
600 Gbps<攻击峰值≤700 Gbps	10,510
700 Gbps<攻击峰值≤800 Gbps	12,010
800 Gbps<攻击峰值≤900 Gbps	13,510
900 Gbps<攻击峰值≤1000 Gbps	15,010
1000 Gbps<攻击峰值≤1100 Gbps	16,510
1100 Gbps<攻击峰值≤1200 Gbps	18,010
1200 Gbps<攻击峰值≤1300 Gbps	19,510
1300 Gbps<攻击峰值≤1400 Gbps	21,010
1400 Gbps<攻击峰值≤1500 Gbps	22,520

实例到期说明

实例到期状态	说明
到期前	距离DDoS高防（新BGP）实例到期前的第7天、3天和1天，阿里云将会通过短信、邮件、站内信的形式提醒您实例即将到期，并提示您续费。
到期后7天内	• 对防护能力的影响： 如果DDoS高防（新BGP）实例在到期前没有续费，则实例到期后将停止提供DDoS防护服务，已接入防护的资产的DDoS防护能力会恢复到默认的免费防护能力（5 Gbps）且不再拥有弹性防护能力，但是实例仍可以维持业务流量转发。 • 通知： 实例到期后，阿里云将会通知您实例已到期且可用状态会保留7天，并提示您续费。
到期7天后	• 对业务流量转发的影响： DDoS高防（新BGP）实例到期7天后，将自动停止业务流量转发。如果这时正常续费，则业务流量转发自动恢复，您可以继续正常使用DDoS高防（新BGP）服务。 **说明** 建议您随时关注DDoS高防（新BGP）控制台上的已经到期的高防实例信息提示，并及时续费或设置自动续费，避免因停止业务流量转发影响业务。  1 个实例已经停止流量转发。1 个实例已经到期。 收起 实例 ddoscoo-cn-[redacted]1 已经到期31天，到期超过7天未续费，该实例将停止业务流量转发。续费 释放 实例 限速通知测试用 到期超过7天未续费，该实例已经停止业务流量转发，续费后可以正常使用。续费 释放 • 对实例配置的影响： 阿里云将定期进行资源回收。如果DDoS高防（新BGP）实例到期超过7天且未及时续费，则实例可能自动释放，原有实例配置也将释放。 • 通知： 实例到期7天后，阿里云将会通知您实例已经停止业务流量转发。

不支持退款

DDoS高防（新BGP）包年包月服务不支持提前退订，也不适用五天无理由退款。如果您已经完成创建DDoS高防（新BGP）实例，则一概不支持退款。

相关文档

- 创建DDoS高防（新BGP）实例
- 升级DDoS高防实例规格

3.DDoS高防（国际）计费方式

3.1. 保险版&无忧版计费方式

本文介绍了DDoS高防（国际）保险版和无忧版套餐的计费方式。

计费概述

DDoS高防（国际）为您部署在中国内地以外地域的业务提供针对DDoS攻击的**高级防护**①服务，并根据可使用的高级防护次数的不同，提供**保险版**②和**无忧版**③两种套餐版本供您选择。

DDoS高防（国际）仅支持**包年包月**（预付费）的计费方式。您必须先创建DDoS高防（国际）实例，根据业务需要选择套餐版本、实例规格和购买时长，付费后开通实例。已开通的DDoS高防（国际）实例，在服务有效期内，为所有接入防护的业务提供DDoS高级防护服务。

①高级防护

高级防护（即无上限全力防护）以成功防护每一次DDoS攻击为目标，整合阿里云海外地区所有高防清洗中心能力，全力保护您的业务。

大部分情况显示，持续使用DDoS高防服务并成功防护攻击的用户遭受攻击的风险将明显下降。一般来说，恶意攻击者发起攻击的目的是为了对目标业务造成损失。由于发起攻击本身也存在成本，如果攻击始终无法达到目的，攻击便会停止。

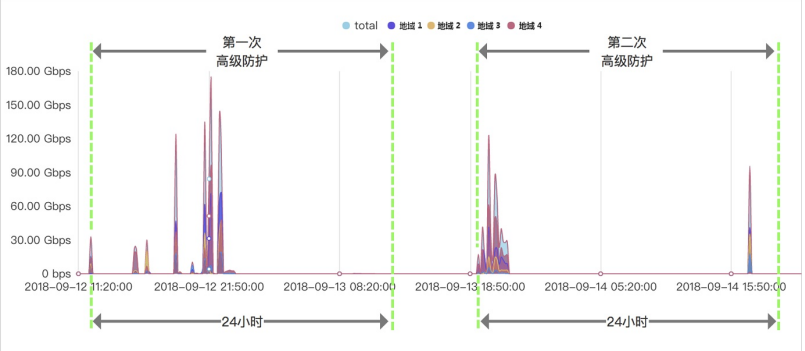
因此，DDoS高防（国际）的高级防护不设防护上限，调用阿里云海外地区所有高防清洗中心能力，全力保障您的业务。

> **注意** 如果您的业务遭受的攻击影响到阿里云海外高防清洗中心的基础设施，则阿里云保留压制流量的权利。DDoS高防（国际）实例受到流量压制时，可能对您的业务造成一定影响，例如业务访问流量可能会被限速，甚至被黑洞。

②保险版

DDoS高防（国际）保险版作为DDoS高防（国际）的入门方案，提供每月两次的高级防护，适用于受攻击风险较低的用户。接入防护的业务自遭受流量攻击起24小时内，将自动触发高级防护，并消耗一次高级防护使用次数。每月初DDoS高防（国际）保险版实例的高级防护使用次数将自动重置为两次。

例如，自9月12日11:20:00起所防护的IP遭到流量攻击，触发高级防护，24小时内DDoS高防（国际）为该业务提供无上限全力防护。9月13日18:50:00该业务再次遭受流量攻击并触发高级防护，24小时后无上限全力防护结束，且9月两次高级防护使用次数全部消耗。DDoS高防（国际）保险版实例的高级防护使用次数将在下月初（10月1日）自动重置。



> **说明** 如果每月两次的高级防护次数不能满足您的需求，您需要更多的高级防护（例如当月提供的两次高级防护次数已耗尽）或者使用时间更长（例如有效期一年）的高级防护，则可以额外购买全局高级防护。更多信息，请参见全局高级防护计费方式。

③无忧版

DDoS高防（国际）无忧版为您提供无限次高级防护。选购无忧版套餐后，您无需担心攻击大小和攻击次数，DDoS高防（国际）将全面为您的业务保驾护航。

实例定价

下表描述了默认规格下，不同**业务带宽**④的DDoS高防（国际）实例的定价信息。根据实例支持的防护功能不同，DDoS高防（国际）实例分为标准功能和增强功能，两者的费用也有差别。关于标准功能和增强功能的更多信息，请参见DDoS高防（新BGP&国际）功能套餐。

④业务带宽

业务带宽指无攻击情况下DDoS高防（国际）实例支持处理的最大正常业务带宽。请确保实例的业务带宽大于所需接入实例防护的所有业务的网络入方向总流量峰值、出方向总流量峰值中较大的值。

> **警告** 如果接入防护的正常业务带宽超出了DDoS高防（国际）实例的业务带宽规格，则会出现限流、随机丢包等现象，可能导致您的正常业务在一定时间内不可用、卡顿、延迟。

> **说明** 如果下表描述的业务带宽不能满足您的业务需求，您需要更高的业务带宽，请提交工单联系我们。

套餐类型	业务带宽	标准功能单价（美元/月）	增强功能单价（美元/月）
保险版 每月2次高级防护	100 Mbps	2,630	3,830
	150 Mbps	3,420	4,620
	200 Mbps	4,210	5,410
	250 Mbps	5,000	6,200
	300 Mbps	5,570	6,770
无忧版 无限次高级防护	100 Mbps	11,560	12,760
	150 Mbps	12,610	13,810
	200 Mbps	13,660	14,860
	250 Mbps	14,720	15,920
	300 Mbps	15,770	16,970

下表描述了DDoS高防（国际）实例的默认规格以及规格的扩展费用。如果您的实际业务需要超出实例的默认规格，您可以升级实例或在购买实例时对相应规格进行扩展。

名称	说明	默认情况	扩展单价
防护端口数	实例支持添加的TCP和UDP端口数量	5个	每5个端口：150 美元/月
防护域名数	实例支持添加的HTTP和HTTPS域名数量	10个 **说明** 最多涉及1个一级域名，即接入防护的域名所属的一级域名总数不超过1个。	• 标准功能套餐：每10个域名45美元/月 • 增强功能套餐：每10个域名75美元/月 **说明** 每增加10个域名可增加一个一级域名。
业务QPS	实例支持处理的无攻击情况下最大HTTP和HTTPS业务的并发请求速率	• 保险版：500 QPS • 无忧版：1,000 QPS	每100 QPS：150美元/月

实例到期说明

实例到期状态	说明
到期前	距离DDoS高防（国际）实例到期前的第7天、3天和1天，阿里云将会通过短信、邮件的形式提醒您实例即将到期，并提示您续费。
到期后30天内	• 对防护服务的影响： 如果DDoS高防（国际）实例在到期前没有续费，则实例到期后将停止提供DDoS防护服务，已接入防护的资产的DDoS防护能力会恢复到默认的免费防护能力。 • 对实例配置的影响： DDoS高防（国际）实例到期后，实例相关配置将会保留一个月（30天）。如果您在一个月内完成续费，则可以继续使用原有配置的DDoS高防（国际）实例。
到期30天后	DDoS高防（国际）实例到期30天后，实例将自动释放，实例相关配置也一并释放。如果这时您需要继续使用DDoS高防（国际）服务，则必须重新创建实例并完成相关配置。

不支持退款

DDoS高防（国际）包年包月服务不支持提前退订，也不适用五天无理由退款。如果您已经完成创建DDoS高防（国际）实例，则一概不支持退款。

相关文档

- 创建DDoS高防（国际）保险版或无忧版实例
- 升级DDoS高防实例规格

3.2. 加速线路计费方式

本文介绍了DDoS高防（国际）加速线路的计费方式。加速线路必须与DDoS高防（国际）服务搭配使用。如果您的业务部署在中国内地以外地域，您可以先为业务开启DDoS高防（国际）服务，防御DDoS攻击；在此基础上为业务开启加速线路服务，实现无攻击状态下中国内地用户对业务的访问加速。

计费概述

DDoS高防（国际）加速线路适用于您已经为部署在中国内地以外地域的业务开启DDoS高防（国际）服务后，帮助降低来自中国内地的用户对业务的访问延时，大幅提升在无攻击情况下的访问质量。

> **注意** 加速线路实例本身不具备任何防护能力，必须与DDoS高防（国际）保险版或无忧版实例搭配使用。

加速线路仅支持**包年包月**（预付费）的计费方式。您必须先创建加速线路实例，根据业务需要选择实例规格和购买时长，付费后开通实例。已开通的加速线路实例，在服务有效期内，为所有接入防护的业务提供访问加速服务。

实例定价

下表描述了不同**业务带宽**①的加速线路实例的定价信息。

① 业务带宽

业务带宽指无攻击情况下加速线路实例支持处理的最大正常业务带宽。请确保实例的业务带宽大于所需接入加速线路实例的所有业务的网络入方向流量峰值、出方向总流量峰值中较大的值。

> **警告** 如果接入防护的正常业务带宽超出了加速线路实例的业务带宽规格，则会出现限流、随机丢包等现象，可能导致您的正常业务在一定时间内出现不可用、卡顿、延迟等问题。

业务带宽	单价（美元/月）
10 Mbps	1,548
20 Mbps	3,096
30 Mbps	4,643
40 Mbps	6,191
50 Mbps	7,739
60 Mbps	9,287
70 Mbps	10,834
80 Mbps	12,382
90 Mbps	13,930
100 Mbps	15,478

实例到期说明

实例到期状态	说明
到期前	距离加速线路实例到期前的第7天、3天和1天，阿里云将会通过短信、邮件的形式提醒您实例即将到期，并提示您续费。
到期后30天内	• 对加速服务的影响： 如果加速线路实例在到期前没有续费，则实例到期后将停止提供访问加速能力。 • 对实例配置的影响： 加速线路实例到期后，实例相关配置将会保留一个月（30天）。如果您在一个月内完成续费，则可以继续使用原有配置的加速线路实例。
到期30天后	加速线路实例到期30天后，实例将自动释放，实例相关配置也一并释放。如果这时您需要继续使用加速线路服务，则必须重新创建实例并完成相关配置。

相关文档

- 创建DDoS高防（国际）加速线路
- 配置DDoS高防（国际）加速线路

3.3. 安全加速线路计费方式

本文介绍了DDoS高防（国际）安全加速线路的计费方式。

计费概述

DDoS高防（国际）安全加速线路仅支持**包年包月**（预付费）的计费方式。您必须先创建DDoS高防（国际）安全加速线路实例，根据业务需要选择套餐版本、实例规格和购买时长，付费后开通实例。已开通的DDoS高防（国际）安全加速线路实例，在服务有效期内，为所有接入防护的业务提供访问加速和DDoS防护服务。

实例定价

下表描述了默认规格下，不同**业务带宽**①的DDoS高防（国际）安全加速线路实例的定价信息。根据实例支持的防护功能不同，DDoS高防（国际）安全加速线路实例分为标准功能和增强功能，两者的费用也有差别。关于标准功能和增强功能的更多信息，请参见DDoS高防（新BGP&国际）功能套餐。

① 业务带宽

业务带宽指无攻击情况下DDoS高防（国际）安全加速线路实例支持处理的最大正常业务带宽。请确保实例的业务带宽大于所需接入实例防护的所有业务的网络入方向总流量峰值、出方向总流量峰值中较大的值。

> **警告** 如果接入防护的正常业务带宽超出了DDoS高防（国际）安全加速线路实例的业务带宽规格，则会出现限流、随机丢包等现象，可能导致您的正常业务在一定时间内不可用、卡顿、延迟。

> **说明** 如果下表描述的业务带宽不能满足您的业务需求，您需要更高的业务带宽，请提交工单联系我们。

业务带宽	标准功能单价（美元/月）	增强功能单价（美元/月）
10 Mbit/s	15,480	16,680
20 Mbit/s	17,028	18,228
30 Mbit/s	18,576	19,776
40 Mbit/s	20,124	21,324
50 Mbit/s	21,672	22,872
60 Mbit/s	23,220	24,420
70 Mbit/s	24,768	25,968
80 Mbit/s	26,316	27,516
90 Mbit/s	27,864	29,064
100 Mbit/s	29,412	30,612
150 Mbit/s	37,152	38,352
200 Mbit/s	44,892	46,092

下表描述了DDoS高防（国际）安全加速线路实例的默认规格以及规格的扩展费用。如果您的实际业务需要超出实例的默认规格，您可以升级实例或在购买实例时对相应规格进行扩展。

名称	说明	默认情况	扩展单价
防护端口数	实例支持添加的TCP和UDP端口数量	5个	每5个端口：150 美元/月
防护域名数	实例支持添加的HTTP和HTTPS域名数量	10个 **说明** 最多涉及1个一级域名，即接入防护的域名所属的一级域名总数不超过1个。	• 标准功能套餐：每10个域名45 美元/月 • 增强功能套餐：每10个域名75 美元/月 **说明** 每增加10个域名可增加一个一级域名。
业务QPS	实例支持处理的无攻击情况下最大HTTP和HTTPS业务的并发请求速率	500 QPS	每100 QPS：150 美元/月

实例到期说明

实例到期状态	说明
到期前	距离DDoS高防（国际）安全加速线路实例到期前的第7天、3天和1天，阿里云将会通过短信、邮件的形式提醒您实例即将到期，并提示您续费。
到期后30天内	• 对防护服务的影响： 如果DDoS高防（国际）安全加速线路实例在到期前没有续费，则实例到期后将停止提供访问加速和DDoS防护服务，已接入防护的资产的DDoS防护能力会恢复到默认的免费防护能力。 • 对实例配置的影响： DDoS高防（国际）安全加速线路实例到期后，实例相关配置将会保留一个月（30天）。如果您在一个月内完成续费，则可以继续使用原有配置的DDoS高防（国际）安全加速线路实例。
到期30天后	DDoS高防（国际）安全加速线路实例到期30天后，实例将自动释放，实例相关配置也一并释放。如果这时您需要继续使用DDoS高防（国际）安全加速线路服务，则必须重新创建实例并完成相关配置。

不支持退款

DDoS高防（国际）安全加速线路包年包月服务不支持提前退订，也不适用五天无理由退款。如果您已经完成创建DDoS高防（国际）安全加速线路实例，则一概不支持退款。

相关文档

- 创建DDoS高防（国际）安全加速线路
- 配置DDoS高防（国际）安全加速

3.4. 全局高级防护计费方式

本文介绍了DDoS高防（国际）全局高级防护的计费方式。全局高级防护与DDoS高防（国际）保险版搭配使用。如果DDoS高防（国际）保险版实例当月提供的两次高级防护次数已耗尽，您可以额外购买全局高级防护，获得更多高级防护（无上限全力防护）使用次数。

背景信息

DDoS高防（国际）保险版实例默认包含每月两次的高级防护，自遭受流量攻击起24小时内为您的业务提供无上限全力防护，并消耗一次高级防护使用次数。

如果所防护的业务遭受频繁的大流量攻击，保险版实例默认的两次高级防护可能无法完全保证业务的可用性，您可以购买全局高级防护补充您账号中所有DDoS高防（国际）保险版实例的高级防护使用次数。

下表描述了全局高级防护与DDoS高防（国际）实例的高级防护之间的区别。

类型	所属范围	有效期	使用次数
无忧版实例高级防护	实例	根据实例有效期	无限次

类型	所属范围	有效期	使用次数
保险版实例高级防护	实例	一个月 **说明** 当月未消耗的高级防护次数在下月初将被清空。	两次/月
全局高级防护	云账号	一年	单独购买

服务定价

下表描述了全局高级防护的具体定价信息。

定价参数	说明
付费方式	预付费
有效时长	1年
购买单价	1,580美元/次

不支持退款

全局高级防护经购买后，一概不支持退款。

相关文档

购买全局高级防护

4.DDoS高防（新BGP&国际）功能套餐

DDoS高防（新BGP&国际）提供标准功能和增强功能两种功能套餐。增强功能套餐在标准功能套餐的基础上，额外提供网站加速缓存、非标准业务端口、区域流量封禁等增强功能，增强DDoS高防的业务接入能力和DDoS攻击防护能力。您可以根据业务的情况和安全防护需求，选择合适的功能套餐。

购买DDoS高防（新BGP&国际）实例时，系统默认选择标准功能套餐，您可以选择增强功能套餐来获得更强大的业务接入能力和DDoS攻击防护能力。增强功能套餐的售价为1,145美元/月，即选择增强功能套餐将在标准功能套餐同规格实例的基础上增加1,145美元/月的增强功能费用。

对于已购买的标准功能套餐实例，您可以通过升级DDoS高防实例规格为该实例开通增强功能。更多信息，请参见升级DDoS高防实例规格。

> **说明** 新购或升级增强功能套餐后，对于已配置接入的网站域名业务，您需要编辑域名配置关联增强功能套餐的DDoS高防实例，为网站域名业务使用增强功能。

标准功能与增强功能套餐

下表描述了标准功能套餐和增强功能套餐在具体功能上的差异。

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
防护算法	流量型攻击防护	支持常见的流量型DDoS攻击防护，包括畸形报文攻击防护和各类流量型Flood攻击防护。	✓	✓
	资源耗尽型攻击防护	支持常见的网络四层/七层资源耗尽型CC攻击防护，例如HTTP GET Flood、HTTP POST Flood攻击等。 更多信息，请参见设置频率控制。	✓	✓
	AI智能防护	• 支持网络七层AI智能CC防护，缓解应用层精巧型CC攻击。 • 支持网络四层AI智能CC防护，缓解TCP连接耗尽型攻击。 更多信息，请参见设置AI智能防护。	✓	✓
	黑白名单	针对每个接入防护的域名业务支持配置最多200条访问IP白名单和200条访问IP黑名单规则。 更多信息，请参见设置黑白名单（针对域名）。	✓	✓

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
防护规则	精准访问控制	支持HTTP协议精准匹配防护规则。 更多信息，请参见设置精准访问控制。	针对每个接入防护的域名业务支持配置最多五条规则，且仅支持IP、URL、Referer、User-Agent字段	针对每个接入防护的域名业务支持配置最多十条规则
	区域IP封禁	针对每个接入防护的域名业务的访问流量支持按区域进行封禁。 更多信息，请参见设置区域封禁（针对域名）。	✗	✓
业务接入	HTTP（80/8080）、HTTPS（443/8443）标准端口转发	支持HTTP（80/8080）、HTTPS（443/8443）业务的DDoS攻击防护。	✓	✓
	HTTP、HTTPS非标准端口转发	支持HTTP、HTTPS非标准端口（不限于80、8080、443、8443端口）业务的DDoS攻击防护。 **说明** 每个实例支持配置最多10不同非标端口的转发。	✗	✓
其它	静态页面缓存	支持网站静态页面加速缓存。 **说明** 目前，自定义缓存规则处于公测阶段，每个接入防护的域名业务支持配置最多三条规则。 更多信息，请参见设置静态页面缓存。	✗	✓