ALIBABA CLOUD

阿里云

DDoS防护

常见问题

文档版本：20220317

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.常见问题概览

本文列举了阿里云DDoS防护产品相关的常见问题。

类型	问题列表
售前常见问题	• 阿里云DDoS防护是否提供免费服务？ • 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？ • 阿里云DDoS防护产品是否支持试用？ • 非阿里云服务器是否能使用DDoS高防服务？ • 服务器不在阿里云，域名在阿里云，是否能开通DDoS高防？ • 使用阿里云DDoS高防是否需要完成域名备案？ • DDoS高防服务支持哪些地域？ • DDoS高防是否限制接入域名的数量？ • DDoS高防是否支持泛域名？ • DDoS高防（新BGP）是否对接入端口有限制？ • 开通DDoS高防（国际）有什么要求吗？ • 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）弹性计费常见问题	• 如果开启了弹性防护，一个月都没有攻击，是否会产生弹性防护费用？ • 我购买了20 Gbps的保底防护、50 Gbps的弹性防护，最终我的防护能力是多大？ • 攻击流量超过弹性防护能力上限会怎样？ • 保底防护带宽30 Gbps，弹性防护带宽50 Gbps，实际攻击流量只有45 Gbps，如何收费？ • 当前选择的弹性防护带宽是100 Gbps，发现不够用，可以改成200 Gbps吗？ • 已购买30 Gbps保底防护带宽的DDoS高防（新BGP）实例，仍不够用，能否随时升级到更高的防护能力？ • 一个IP一天内被攻击多次，费用该怎么计算？ • 购买了DDoS高防（新BGP）实例，如何停止使用弹性防护能力，避免产生弹性防护的后付费费用？

类型	问题列表
DDoS原生防护常见问题	**基础版**（DDoS基础防护） • DDoS原生防护基础版可以防御SYN攻击吗？ • 我的ECS服务器被20 Mb的流量攻击了，DDoS原生防护基础版怎么不防护？ • 为什么使用DDoS原生防护基础版时，黑洞不能立即取消？ • 为什么云监控、云产品流量监控中的流量数据和DDoS防护的流量监控数据有差异？ • DDoS原生防护企业版的全力防护和DDoS高防（新BGP）的弹性防护的计费模式有什么区别？ • DDoS原生防护企业版所防护的IP被黑洞了该怎么办？ • 如果购买时选错了DDoS原生防护实例的地域该怎么办？ • 添加防护IP时收到“IP不属于你”的错误提示该怎么办？ **企业版** • DDoS原生防护企业版的全力防护和DDoS高防（新BGP）的弹性防护的计费模式有什么区别？ • DDoS原生防护企业版所防护的IP被黑洞了该怎么办？ • 如果购买时选错了DDoS原生防护实例的地域该怎么办？ • 添加防护IP时，企业版实例的防护IP容量已占满该怎么办？ • 添加防护IP时收到“IP不属于你”的错误提示该怎么办？

类型	问题列表
DDoS高防常见问题	• DDoS高防实例过期后会怎样？ • DDoS高防业务带宽说明 • 超过DDoS高防业务带宽会有什么影响？ • DDoS高防实例支持手动解除黑洞状态吗？ • DDoS高防的回源IP地址有哪些？ • DDoS高防是否会自动将DDoS高防的回源IP地址加入白名单？ • DDoS高防服务中的源站IP可以填写内网IP吗？ • 修改DDoS高防服务的源站IP是否有延迟？ • DDoS高防实例配置了多个网站业务，被攻击后如何查看是哪个网站受到攻击？ • DDoS高防是否支持健康检查？ • DDoS高防配置多个源站时如何进行负载均衡？ • DDoS高防服务是否支持会话保持？ • DDoS高防服务的会话保持是如何实现的？ • DDoS高防的四层TCP默认连接超时时间是多长？ • DDoS高防的HTTP或HTTPS默认连接超时时间是多久？ • DDoS高防服务是否支持IPv6协议？ • DDoS高防服务是否支持Websocket协议？ • DDoS高防服务是否支持HTTPS双向认证？ • 为什么老版本浏览器和安卓客户端无法正常访问HTTPS站点？ • DDoS高防支持的SSL协议和加密套件有哪些？ • DDoS高防如何保证上传证书及密钥的安全性？是否会解密HTTPS流量并记录访问请求的内容？ • DDoS高防支持的防护端口数和防护域名数有什么限制？ • 服务器的流量未达到清洗阈值，为何安全总览中会出现清洗流量？ • DDoS高防服务是否支持接入采用NTLM协议认证的网站？

类型	问题列表
DDoS高防热点问题	**配置类** • 不同的阿里云账号如何共享使用DDoS高防 • DDoS高防WebSocket配置 • DDoS高防健康检查的主动探测IP **业务异常** • 业务接入高防后存在卡顿、延迟、访问不通等问题 • 配置DDoS高防后访问网站提示502错误 • 启用DDoS高防后网站的某些请求返回“504 Gateway Time-out”错误 • Windows Server 2012系统实例由于ECN功能导致建立连接较慢 • 配置DDoS高防后访问业务缓慢 • 配置DDoS高防后不能实现会话保持的排查思路 • 业务接入DDoS高防后无法Ping高防IP • 业务添加DDoS高防后通过HTTP和HTTPS协议上传大文件失败 **防护分析** • 如何判断DDoS高防实例受到的攻击类型 • 如何预防或避免NTP服务的DDoS攻击 • 网站防护和非网站防护有什么区别？ **HTTPS业务** • DDoS高防上传HTTPS证书时出现“证书私钥不匹配”问题 • 不同格式的HTTPS证书转换成PEM格式 • 关于SNI在HTTPS通信中应用的介绍 • 证书与密钥不匹配问题排查

2.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。

3.DDoS原生防护常见问题

本文列举了DDoS原生防护（基础版&企业版）产品相关的常见问题。

基础版（DDoS基础防护）

- DDoS原生防护基础版可以防御SYN攻击吗？
- 我的ECS服务器被20 Mb的流量攻击了，DDoS原生防护基础版怎么不防护？
- 为什么使用DDoS原生防护基础版时，黑洞不能立即取消？
- 为什么云监控、云产品流量监控中的流量数据和DDoS防护的流量监控数据有差异？

企业版

- DDoS原生防护企业版的全力防护和DDoS高防（新BGP）的弹性防护的计费模式有什么区别？
- DDoS原生防护企业版所防护的IP被黑洞了该怎么办？
- 如果购买时选错了DDoS原生防护实例的地域该怎么办？
- 添加防护IP时，企业版实例的防护IP容量已占满该怎么办？
- 添加防护IP时收到“IP不属于你”的错误提示该怎么办？

DDoS原生防护基础版可以防御SYN攻击吗？

DDoS原生防护基础版服务可以防御SYN Flood攻击。

我的ECS服务器被20 Mb的流量攻击了，DDoS原生防护基础版怎么不防护？

DDoS原生防护基础版是公共的DDoS防护服务，不对很小的流量攻击（小于100 Mb）进行防护。建议您优化服务器性能，或者安装云锁等主机防火墙应对小于100 Mb的流量攻击。

为什么使用DDoS原生防护基础版时，黑洞不能立即取消？

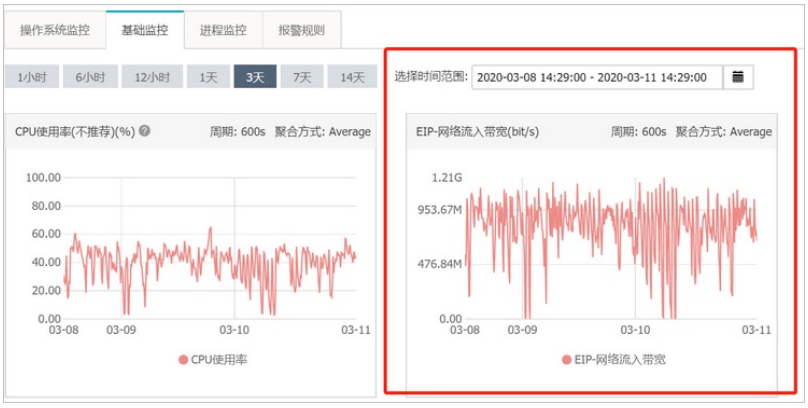
绝大多数用户的黑洞时间在30分钟到24小时之间。如果一个用户的攻击很频繁，阿里云可能通过增加黑洞时间采取惩罚措施。

黑洞是阿里云向运营商购买的服务，运营商有明确的黑洞解除时间限制，所以一般情况下黑洞不能立即取消。如果您需要黑洞解除功能，建议您购买DDoS原生防护企业版或者DDoS高防服务，这两种方案都支持手动解除黑洞的功能。更多信息，请参见什么是DDoS原生防护、什么是DDoS高防（新BGP&国际）。

为什么云监控、云产品流量监控中的流量数据和DDoS防护的流量监控数据有差异？

一般情况下，DDoS防护的流量监控数据大于您在云监控或具体云产品数据页面看到的流量数据。

示例：假设您的ECS实例遭受了DDoS攻击，触发流量清洗，您收到DDoS原生防护基础版的清洗通知，触发清洗时的流量为2.5 Gbps。但是，您在云监控中查询发现，流量清洗时ECS实例的弹性公网IP上的网络流入带宽约为1.2 Gbps。



出现上述情况，主要有以下几个原因：

- DDoS防护的流量监控数据来自流量清洗前，而云监控中的流量数据来自流量清洗后。
- DDoS防护的流量监控数据对应全部业务请求流量（包含攻击流量），而云监控中的流量数据只包含正常转发流量。
- 监控颗粒度不同。DDoS防护的监控颗粒度更精细，在判断攻击时，监控颗粒度是秒级。云监控的EIP流量图则是分钟级别的数据。
- 监控位置不同。DDoS防护在互联网和阿里云网络边界监控流量，而EIP的流量数据采集自转发设备。

> **说明** ECS、SLB、EIP、NAT等所有公网IaaS产品都可能会遇到上述问题。

DDoS原生防护企业版的全力防护和DDoS高防（新BGP）的弹性防护的计费模式有什么区别？

- DDoS原生防护企业版提供全力防护能力。当遭受攻击时，自动调度该企业版DDoS原生防护实例所在地域的阿里云最大DDoS防护能力提供全力防护。全力防护服务包含在企业版套餐中，不额外产生弹性防护费用。
- DDoS高防（新BGP）服务的弹性防护计费按照当日弹性带宽的流量峰值进行计费。更多信息，请参见弹性防护（按天后付费）。

DDoS原生防护企业版所防护的IP被黑洞了该怎么办？

DDoS原生防护企业版支持黑洞解除功能。

- 如果防护对象处于黑洞中状态，您可以使用手动解除黑洞功能，具体操作请参见解除黑洞。
- 您还可以参见黑洞自动解除最佳实践，实现已防护IP的黑洞自动化响应和快速解除。

如果购买时选错了DDoS原生防护实例的地域该怎么办？

如果您想要防护的IP与所购买的DDoS原生防护企业版实例的地域不一致，请提交工单申请退款，然后重新购买新的DDoS原生防护企业版实例。

添加防护IP时，企业版实例的防护IP容量已占满该怎么办？

如果您想要防护的IP数量超过了您购买的原生防护企业版实例的**保护IP数量**（即防护IP容量），您可以选择扩展当前实例的**保护IP数量**或者重新购买新的企业版实例，相关操作请参见升级实例规格和购买DDoS原生防护企业版实例。

添加防护IP时收到“IP不属于你”的错误提示该怎么办？

如果您在为DDoS原生防护企业版设置防护对象IP时，收到了**IP不属于你**的错误提示，请按照以下步骤进行排查：

1. 检查您所输入的IP地址，确认输入的IP地址正确无误。
2. 检查您想要添加的防护IP对应的云产品所属的地域，确认该地域与您所购买的DDoS原生防护企业版实例的所属地域一致。
3. 如果您想要添加的防护IP是WAF IP，检查该WAF实例的所属地域，确认DDoS原生防护企业版支持该地域。关于DDoS原生防护企业版支持的地域，请参见什么是DDoS原生防护。

4.DDoS高防常见问题

本文列举了DDoS高防（新BGP、国际）服务相关的常见问题。

DDoS高防实例过期后会怎样？

DDoS高防实例过期后无防御能力，具体说明如下：

- 过期7天内转发规则配置正常生效，流量超限将触发流量限速，可能导致随机丢包。
- 过期7天后将停止业务流量转发。这种情况下，如果您的业务访问地址仍解析到DDoS高防实例，则业务将无法被访问到。

更多信息，请参见实例到期说明。

DDoS高防业务带宽说明

DDoS高防实例的业务带宽指接入当前实例防护业务的正常业务流量，取入流量和出流量其中的较大值，单位：Mbps。

您可以在DDoS高防控制台的**实例管理**页面对实例进行升级，增大当前实例的**业务带宽**。具体操作，请参见升级实例。

超过DDoS高防业务带宽会有什么影响？

如果您的业务流量超过购买的DDoS高防实例的业务带宽，将触发流量限速，可能导致随机丢包。

DDoS高防实例支持手动解除黑洞状态吗？

DDoS高防（新BGP）和DDoS高防（国际）实例有区别，具体说明如下：

- DDoS高防（新BGP）实例：支持。

  每个阿里云账号每天共有五次手动解除黑洞状态的机会，每天零点自动恢复成五次。关于手动解除黑洞的具体操作，请参见黑洞解封。

- DDoS高防（国际）实例：暂不支持。

  与DDoS高防（新BGP）实例存在固定的防护带宽不同，DDoS高防（国际）实例提供不设上限的高级防护，正常情况下不需要手动解除黑洞。

> **说明** 如果您目前使用DDoS高防（国际）**保险版**实例，由于当月可用的高级防护次数已消耗完，导致业务被攻击后进入黑洞状态，建议您将保险版实例升级到无忧版实例（提供不限次数的高级防护）。DDoS高防（国际）保险版实例升级到无忧版实例后，可以自动解除原保险版实例的黑洞状态。

DDoS高防的回源IP地址有哪些？

您可以在DDoS高防控制台的**域名接入**页面查看DDoS高防的回源IP网段。更多信息，请参见放行DDoS高防回源IP。

DDoS高防是否会自动将DDoS高防的回源IP地址加入白名单？

不会。如果您的源站部署了防火墙或第三方的主机安全防护软件，您需要将DDoS高防的回源IP网段添加至相应的白名单中。更多信息，请参见放行DDoS高防回源IP。

DDoS高防服务中的源站IP可以填写内网IP吗？

不可以。DDoS高防通过公网进行回源，不支持直接填写内网IP。

修改DDoS高防服务的源站IP是否有延迟？

有延迟。修改DDoS高防服务已防护的源站IP后，需要大约五分钟生效，建议您在业务低峰期进行变更操作。相关操作，请参见更换源站ECS公网IP。

DDoS高防实例配置了多个网站业务，被攻击后如何查看是哪个网站受到攻击？

针对DDoS高防的大流量DDoS攻击行为，从数据包层面是无法分辨具体是哪个网站受到攻击。建议您使用多组DDoS高防实例，将您的网站分别部署在不同的DDoS高防实例上即可查看各个网站遭受攻击的情况。

DDoS高防是否支持健康检查？

支持。网站业务默认开启健康检查。非网站业务默认不开启健康检查，但可以通过DDoS高防控制台开启，具体操作，请参见配置健康检查。

关于健康检查的更多信息，请参见健康检查概述。

DDoS高防配置多个源站时如何进行负载均衡？

网站业务通过源地址HASH方式进行负载均衡。非网站业务可通过加权轮询的方式轮询转发。

DDoS高防服务是否支持会话保持？

支持。非网站业务可以通过DDoS高防控制台开启会话保持，具体操作，请参见配置会话保持。

DDoS高防服务的会话保持是如何实现的？

开启会话保持后，在会话保持的设定期间内，DDoS高防服务会把同一IP的请求持续发往源站中的一台服务器。但是，如果客户端的网络环境发生变化（例如，从有线切成无线、4G网络切成无线等），由于IP变化会导致会话保持失效。

DDoS高防的四层TCP默认连接超时时间是多长？

900秒。

DDoS高防的HTTP或HTTPS默认连接超时时间是多久？

120秒。

DDoS高防服务是否支持IPv6协议？

DDoS高防（新BGP）支持，DDoS高防（国际）暂不支持。

> **说明** DDoS高防（新BGP）实例支持IPv4高防IP和IPv6高防IP。IPv6高防IP支持转发来自IPv6客户端的请求，对接入业务有以下限制：域名接入只支持IPv4源站，端口接入支持IPv4或IPv6源站。当您的IPv6高防IP通过端口接入的是IPv6源站时，请提交工单或者联系销售人员，申请接入。

DDoS高防服务是否支持Websocket协议？

支持。更多信息，请参见DDoS高防WebSocket配置。

DDoS高防服务是否支持HTTPS双向认证？

网站接入方式不支持HTTPS双向验证。非网站接入且使用TCP转发方式时，支持HTTPS双向验证。

为什么老版本浏览器和安卓客户端无法正常访问HTTPS站点？

可能是因为客户端不支持SNI认证，请确认客户端是否支持SNI认证。关于SNI认证可能引发的问题，请参见SNI可能引发的HTTPS访问异常。

DDoS高防支持的SSL协议和加密套件有哪些？

支持的SSL协议包括：TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。

支持的加密套件包括：

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256

- ECDHE-RSA-AES256-SHA384
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256 AES256-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA
- AES128-SHA AES256-SHA
- DES-CBC3-SHA

更多信息，请参见自定义TLS安全策略。

DDoS高防如何保证上传证书及密钥的安全性？是否会解密HTTPS流量并记录访问请求的内容？

阿里云DDoS高防在防护HTTPS业务时，需要您上传对应的SSL证书及密钥，用于解密HTTPS流量并检测流量中的攻击特征。我们使用了专用的证书服务器（Key Server）来存储和管理密钥。Key Server依托于阿里云密钥管理系统KMS（Key Management Service），能够保护证书和密钥的数据安全性、完整性和可用性，符合监管和等保合规要求。关于KMS的详细介绍，请参见什么是密钥管理服务。

DDoS高防使用您上传的SSL证书及密钥解密HTTPS业务流量，只用于实时检测。我们只会记录包含攻击特征（payload）的部分请求内容，用于攻击报表展示、数据统计等，不会在您未授权的情况下，记录全量的请求或响应内容。

阿里云DDoS高防已通过ISO9001、ISO20000、ISO27001、ISO27017、ISO27018、ISO22301、ISO27701、ISO29151、BS10012、CSA STAR、等保三级、SOC1/2/3、C5、HK金融、菲律宾金融、OSPAR、ISO27001（印尼）、PCI DSS等多项国际权威认证，且作为标准的阿里云云产品，在云平台层面具备与阿里云同等水平的安全合规资质。详细内容，请参见阿里云信任中心。

> **说明** 使用DDoS高防防护HTTPS业务时，您也可以选择双证书方案，即在DDoS高防上使用一套证书及密钥，在源站服务器上使用另一套证书及密钥（两套证书及密钥必须都是合法的），以便将上传到DDoS高防的证书及密钥与源站服务器的证书及密钥分开管理。

DDoS高防支持的防护端口数和防护域名数有什么限制？

关于防护端口数、域名数的具体限制如下：

- 防护端口数：
  - 一个DDoS高防（新BGP）实例默认支持50个端口，支持扩展至400个。
  - 一个DDoS高防（国际）实例默认支持5个端口，支持扩展至400个。
- 支持域名数：
  - 一个DDoS高防（新BGP）实例默认支持50个域名配置，最大可扩展至200个。
  - 一个DDoS高防（国际）实例默认支持10个域名配置，最大可扩展至200个。

服务器的流量未达到清洗阈值，为何安全总览中会出现清洗流量？

对于已接入DDoS高防服务的业务，DDoS高防将自动过滤网络流量中存在的一些畸形包（例如，SYN小包、SYN标志位异常等不符合TCP协议的数据包），使您的业务服务器无需浪费资源处理这些明显的畸形包。这类被过滤的畸形包也将被计入清洗流量中，因此即使您的服务器流量未达清洗阈值，仍可能出现清洗流量。

DDoS高防服务是否支持接入采用NTLM协议认证的网站？

不支持。经DDoS高防转发的访问请求可能无法通过源站服务器的NTLM认证，客户端将反复出现认证提示。建议您的网站采用其他方式进行认证。

阿里云DDoS高防开放的端口是否对我的业务安全造成影响？

不会。DDoS高防（新BGP）和高防（国际）开放的端口都不会对您的业务造成影响。

高防对外提供流量接入转发服务，防护集群中会预定义一系列端口用于您的网站业务接入和防护服务。每个接入高防的域名或端口的业务流量只通过接入配置时设置的源站服务端口进行转发。任何未接入高防的源站服务端口上的访问请求是不会被转发到源站服务器的，因此未配置接入高防的端口开启不会对您的源站服务带来任何安全风险和威胁。

5.DDoS高防（新BGP）弹性计费常见问题

本文列举关于DDoS高防（新BGP）服务弹性计费的常见问题。

如果开启了弹性防护，一个月都没有攻击，是否会产生弹性防护费用？

不会。这种情况下，仅需要支付保底防护带宽的包月费用，不产生其他额外的费用。

我购买了20 Gbps的保底防护、50 Gbps的弹性防护，最终我的防护能力是多大？

最终实际防护能力是50 Gbps，以弹性防护能力为准。假如您选择20 Gbps的弹性防护能力，则最多只能提供20 Gbps的防护能力，相当于没有弹性防护功能。

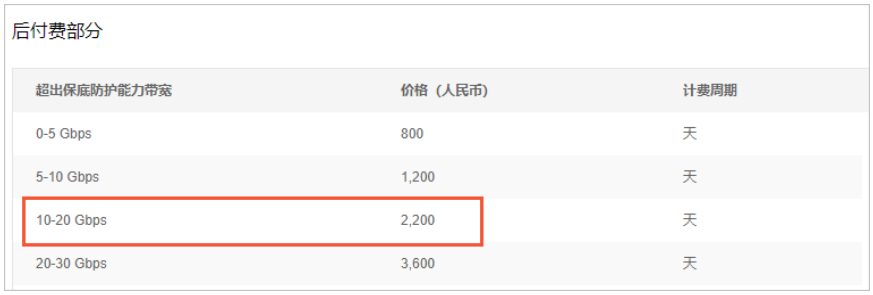
攻击流量超过弹性防护能力上限会怎样？

如果攻击流量超过弹性防护能力，则受到攻击的DDoS高防（新BGP）IP会强制进入黑洞，阻断全部流量。

保底防护带宽30 Gbps，弹性防护带宽50 Gbps，实际攻击流量只有45 Gbps，如何收费？

攻击流量小于30 Gbps（保底防护）的部分不会额外计费，只按照攻击峰值超出保底防护带宽的部分，即15 Gbps（45 Gbps-30 Gbps），收取弹性防护的费用。

您可以在DDoS防护产品定价页查询弹性后付费价格。例如，超出保底防护能力的攻击带宽为15 Gbps，对应的价格为2,200元/天。

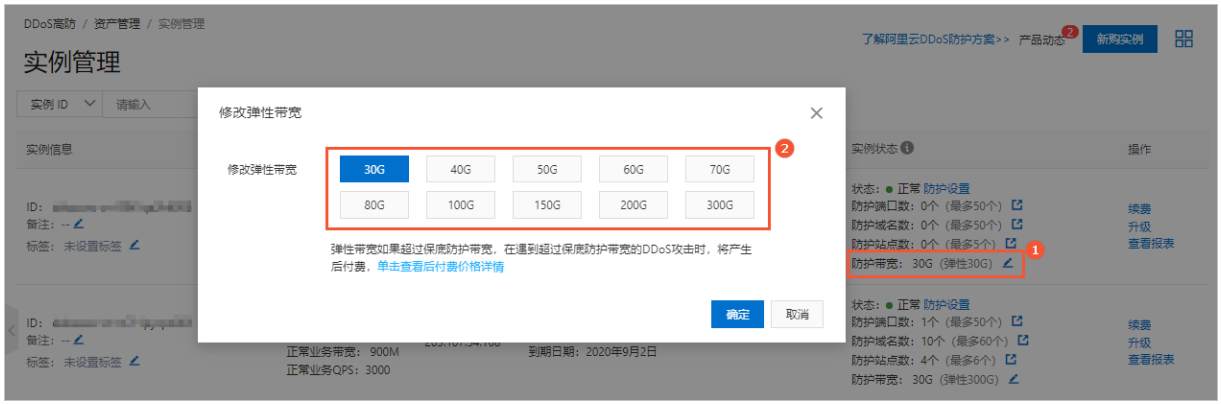

后付费部分

超出保底防护能力带宽	价格（人民币）	计费周期
0-5 Gbps	800	天
5-10 Gbps	1,200	天
10-20 Gbps	2,200	天
20-30 Gbps	3,600	天

当前选择的弹性防护带宽是100 Gbps，发现不够用，可以改成200 Gbps吗？

可以。

您可以在DDoS高防控制台（选择**中国内地**地域）的**实例管理**页面，调整DDoS高防（新BGP）实例的**防护带宽**。



说明 当日发生的攻击已经计费，修改后次日将以最新的弹性带宽进行计费。

已购买30 Gbps保底防护带宽的DDoS高防（新BGP）实例，仍不够用，能否随时升级到更高的防护能力？

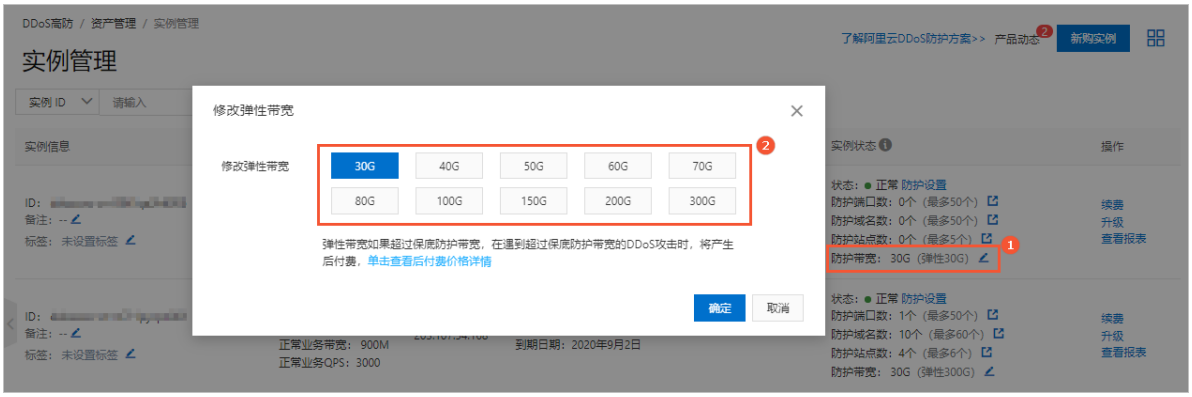
可以。您可以选择升级当前实例的保底防护带宽，或者增大其弹性防护带宽。

- 升级保底防护带宽

  您可以在DDoS高防控制台（选择**中国内地**地域）的**实例管理**页面对实例进行升级，增大当前实例的**保底防护带宽**，并完成付费。更多信息，请参见升级实例。

- 增大弹性防护带宽

  您可以在DDoS高防控制台（选择**中国内地**地域）的**实例管理**页面，调整DDoS高防（新BGP）实例的**防护带宽**，增大其弹性防护带宽。开启弹性防护无需您预付费，但会根据DDoS攻击的流量大小生成后付费账单。更多信息，请参见弹性防护（按天后付费）。



一个IP一天内被攻击多次，费用该怎么计算？

以当天（0:00~24:00）攻击的峰值为准，只产生一次弹性后付费账单。例如某个DDoS防护（新BGP）IP一天内分别遭到50 Gbps、100 Gbps、200 Gbps共三次攻击，则当天的弹性防护付费账单按照200 Gbps攻击的弹性计费标准收取。

购买了DDoS高防（新BGP）实例，如何停止使用弹性防护能力，避免产生弹性防护的后付费费用？

您可以将您购买的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，在遭受到超出保底防护带宽流量的攻击时，将不会启用弹性防护带宽进行防护。

您可以在DDoS高防控制台（选择**中国内地**地域）的**实例管理**页面，调整DDoS高防（新BGP）实例的**防护带宽**。