阿里云
DDoS高防IP

DDoS防护指南

文档版本：20190814

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

1 基本概念

1.1 什么是DDoS攻击

分布式拒绝服务（Distributed Denial of Service，简称DDoS）指借助于客户机/服务器模式，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。

通常，攻击者使用一个非法账号将DDoS主控程序安装在一台计算机上，并在网络上的许多计算机上安装了代理程序。在所设定的时间，主控程序将与大量代理程序进行通讯，代理程序收到指令时就发动攻击。利用客户机/服务器模式，主控程序能在几秒钟内激活成百上千次代理程序的运行。

畸形报文

畸形报文攻击指通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的报文时出现崩溃，从而达到拒绝服务的攻击目的。

畸形报文主要包括以下类型：Frag Flood、Smurf、Stream Flood、Land Flood、IP畸形报文、TCP畸形报文、UDP畸形报文。

传输层DDoS攻击

传输层DDoS攻击主要是指Syn Flood、Ack Flood、UDP Flood、ICMP Flood、RstFlood等攻击。

以Syn Flood攻击为例，它利用了TCP协议的三次握手机制，当服务端接收到一个Syn请求时，服务端必须使用一个监听队列将该连接保存一定时间。因此，通过向服务端不停发送Syn请求，但不响应Syn+Ack报文，从而消耗服务端的资源。当监听队列被占满时，服务端将无法响应正常用户的请求，达到拒绝服务攻击的目的。

DNS DDoS攻击

DNS DDoS攻击主要是指DNS Request Flood、DNS Response Flood、虚假源+真实源DNS Query Flood、权威服务器攻击和Local服务器攻击。

以DNS Query Flood攻击为例，其本质上执行的是真实的Query请求，属于正常业务行为。但如果多台傀儡机同时发起海量的域名查询请求，服务端无法响应正常的Query请求，从而导致拒绝服务。

连接型DDoS攻击

连接型DDoS攻击主要是指TCP慢速连接攻击、连接耗尽攻击、Loic、Hoic、Slowloris、Pyloris、Xoic等慢速攻击。

以Slowloris攻击为例，其攻击目标是Web服务器的并发上限，当Web服务器的连接并发数达到上限后，Web服务即无法接受新的请求。具体来说，Web服务接收到新的HTTP请求时，建立新的连接来处理请求，并在处理完成后关闭这个连接；如果该连接一直处于连接状态，收到新的HTTP请求时则需要建立新的连接进行处理；而当所有连接都处于连接状态时，Web将无法处理任何新的请求。

Slowloris攻击利用HTTP协议的特性来达到攻击目的。HTTP请求以`\r\n\r\n`标识Headers的结束，如果Web服务端只收到`\r\n`，则认为HTTP Headers部分没有结束，将保留该连接并等待后续的请求内容。

Web应用层DDoS攻击

Web应用层攻击主要是指HTTP Get Flood、HTTP Post Flood、CC等攻击。

通常应用层攻击完全模拟用户请求，类似于各种搜索引擎和爬虫一样，这些攻击行为和正常的业务并没有严格的边界，难以辨别。

Web服务中一些资源消耗较大的事务和页面。例如，Web应用中的分页和分表，如果控制页面的参数过大，频繁的翻页将会占用较多的Web服务资源。尤其在高并发频繁调用的情况下，类似这样的事务就成了早期CC攻击的目标。

由于现在的攻击大都是混合型的，因此模拟用户行为的频繁操作都可以被认为是CC攻击。例如，各种刷票软件对网站的访问，从某种程度上来说就是CC攻击。

CC攻击瞄准的是Web应用的后端业务，除了导致拒绝服务外，还会直接影响Web应用的功能和性能，包括Web响应时间、数据库服务、磁盘读写等。

1.2 阿里云黑洞策略

为了保障阿里云网络的整体可用性，阿里云采用黑洞策略，对遭受大流量攻击的服务器在一定时间内实行外网封禁。

什么是黑洞

黑洞是指服务器受攻击流量超过本机房黑洞阈值时，阿里云屏蔽服务器的外网访问。当服务器进入黑洞一段时间后，如果系统监控到攻击流量停止，黑洞会自动解封。

由于黑洞是阿里云向运营商购买的服务，而运营商对黑洞解除时间和频率都有严格的限制，所以黑洞状态无法人工解除，需耐心等待系统自动解封。

为什么需要黑洞策略？为什么阿里云不能免费帮用户无限抵御DDoS攻击？

DDoS 攻击不仅影响受害者，也会对整个云网络造成严重影响。

DDoS 防御需要成本，其中最大的成本就是带宽费用。带宽是阿里云向电信、联通、移动等运营商购买，运营商计算带宽费用时不会把 DDoS 攻击流量清洗掉，而是直接收取阿里云的带宽费用。阿里云云盾在控制成本的情况下会尽量为阿里云用户免费防御 DDoS 攻击，但是当攻击流量超出阈值时，阿里云会屏蔽被攻击 IP 的流量，从而避免超额费用的产生。

如果您的IP遭受的攻击流量超出阈值触发黑洞时，您可以通过购买DDoS防护包将防御能力提升至该IP所属地域的最高防御水平，同时您将获得立即解除黑洞的机会。

如何查看黑洞阈值和黑洞解除时间？

参见DDoS基础防护黑洞阈值，查看黑洞阈值。

参见查看黑洞时长，查看黑洞解除时间。

如何提升黑洞阈值？

免费加入安全信誉联盟，安全信誉联盟将综合多方面因素考量并计算动态黑洞阈值。

参见查看云盾安全信誉分计算依据，维护您的安全信誉分，获取更多免费加成的DDoS防护能力。

黑洞阈值不能满足要求该怎么办？

参见以下方案，轻松解决DDoS流量攻击困扰，保障服务器的正常运行。

- 购买DDoS防护包，获取最高可达100G防御能力且无需修改业务IP。
- 购买DDoS高防IP服务，获取最高可达T级别防御能力，需将流量切换至高防IP。

安全信誉提升阈值和购买高防提升防护量的区别？

安全信誉联盟主要帮助信誉好的用户提升首次被攻击的防护量，且黑洞阈值会随着信誉分变化而调整，不承诺固定的防护量。

高防IP服务用于帮助用户防护DDoS攻击，明确承诺防护量和防御效果。

各地域的黑洞触发阈值

云盾基础版各地域DDoS基础防护功能默认黑洞触发阈值（单位：bps）如下：

说明：

该触发阈值适用于阿里云 ECS、SLB、VPC、WAF等产品。

地区	1核CPU的经典网络ECS	2核CPU的经典网络ECS	4核以上CPU的经典网络ECS	SLB,VPC,WAF等
华东 1	500M	1G	5G	5G
华东 2	500M	1G	2G	2G
华北 1	500M	1G	5G	5G
华北 2	500M	1G	2G	2G
华北 3	500M	1G	2G	2G
华北 5	500M	1G	2G	2G
华南 1	500M	1G	2G	2G
中国香港	500M	500M	500M	500M
美西1	500M	1G	2G	2G
美东1	500M	500M	500M	500M
东京	500M	500M	500M	500M
新加坡	500M	500M	500M	500M
悉尼	500M	500M	500M	500M
吉隆坡	500M	500M	500M	500M
孟买	500M	1G	1G	1G
法兰克福	500M	500M	500M	500M
迪拜	500M	500M	500M	500M

黑洞时长

默认的黑洞时长是2.5小时，黑洞期间不支持解封。实际黑洞时长视攻击情况而定，从30分钟到24小时不等。黑洞时长主要受以下因素影响：

- 攻击是否持续。如果攻击一直持续，可能重新触发黑洞机制，黑洞时间将会延长。
- 攻击是否频繁，如果某用户是首次被攻击，黑洞时间会自动缩短；反之，频繁被攻击的用户被持续攻击的概率较大，黑洞时间会自动延长。

> **说明:**
> 针对个别黑洞过于频繁的用户，阿里云保留延长黑洞时长和降低黑洞阈值的权利，具体黑洞阈值和黑洞时长以控制台显示为准。

如果有疑问，请联系售后技术支持。

1.3 流量清洗、黑洞与阈值

阿里云服务器默认提供DDoS攻击防御功能。当网络流量超过清洗阈值时，阿里云会开始对攻击流量进行清洗，并尽可能保障您的业务可用；当网络流量超过弹性防护阈值时，则会触发黑洞机制，服务器的外网访问将被暂时屏蔽。

关于清洗

清洗是指将流量从原始网络路径中重定向到清洗设备上，通过清洗设备对该IP的流量成分进行正常和异常判断，丢弃异常流量，并对最终到达服务器的流量实施限流，减轻攻击对服务器造成的损害，但对流量中正常的部分可能造成损伤。

关于黑洞

如果云服务器遭受大量攻击，且超过免费防御的流量值时，进入黑洞。免费防御的流量值因不同的地区和不同的CPU配置而异，详情可参见云盾DDoS基础防护黑洞阈值。

触发黑洞后，会在一定时长内限制进入黑洞的服务器的外网通信，黑洞时长视攻击情况而定。

黑洞结束后自动进入清洗状态，核实攻击是否还存在。如果攻击依然存在，服务器会再次进入黑洞；如果攻击已经停止，系统会自动解封。如果被黑洞的服务器遭受的攻击量过大，会影响阿里云整个机房的网络稳定，所以不支持手动解除黑洞。

如果急需业务恢复，可以考虑购买阿里云DDoS高防IP服务 。

云盾DDoS高防IP服务是针对阿里云服务器在遭受大流量的DDoS攻击后导致服务不可用的情况下，推出的付费增值服务。您可通过配置高防IP，将攻击流量引流到高防IP，确保源站的稳定可靠。

2 通用DDoS防护方案

2.1 DDoS攻击缓解最佳实践

分布式拒绝服务攻击（DDoS攻击）是一种针对目标系统的恶意网络攻击行为，DDoS攻击经常会导致被攻击者的业务无法正常访问，也就是所谓的拒绝服务。

常见的DDoS攻击包括以下几类：

- 网络层攻击

  比较典型的攻击类型是UDP反射攻击，例如，NTP Flood攻击。这类攻击主要利用大流量拥塞被攻击者的网络带宽，导致被攻击者的业务无法正常响应客户访问。

- 传输层攻击

  比较典型的攻击类型包括SYN Flood攻击、连接数攻击等。这类攻击通过占用服务器的连接池资源从而达到拒绝服务的目的。

- 会话层攻击

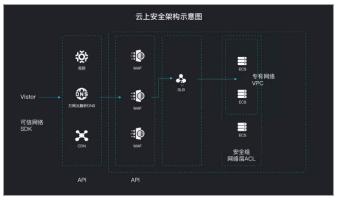
  比较典型的攻击类型是SSL连接攻击。这类攻击占用服务器的SSL会话资源从而达到拒绝服务的目的。

- 应用层攻击

  比较典型的攻击类型包括DNS flood攻击、HTTP flood攻击、游戏假人攻击等。这类攻击占用服务器的应用处理资源，极大地消耗服务器处理性能，从而达到拒绝服务的目的。

DDoS攻击缓解最佳实践

建议阿里云用户从以下几个方面着手缓解DDoS攻击的威胁：



- 缩小暴露面，隔离资源和不相关的业务，降低被攻击的风险。
  - 配置安全组

    尽量避免将非业务必须的服务端口暴露在公网上，从而避免与业务无关的请求和访问。通过配置安全组可以有效防止系统被扫描或者意外暴露。

    关于安全组的详细介绍，请查看安全组使用指南。
  - 使用专有网络（VPC，Virtual Private Cloud ）

    通过专有网络VPC实现网络内部逻辑隔离，防止来自内网肉鸡的攻击。

    关于专有网络VPC的详细介绍，请查看专有网络VPC使用指南。
- 优化业务架构，利用公共云的特性设计弹性伸缩和灾备切换的系统。
  - 科学评估业务架构性能

    在业务部署前期或运营期间，技术团队应该对业务架构进行压力测试，以评估现有架构的业务吞吐处理能力，为DDoS防御提供详细的技术参数指导信息。
  - 弹性和冗余架构

    通过负载均衡架构、或异地多中心的架构避免业务架构中出现单点故障。如果您的业务在阿里云上，可以灵活地使用负载均衡服务（SLB，Server Load Balancer）实现多台服务器

的多点并发处理业务访问，将用户访问流量均衡分配到各个服务器上，降低单台服务器的压力，提升业务吞吐处理能力，这样可以有效缓解一定流量范围内的连接层DDoS攻击。

关于负载均衡的详细介绍，请查看负载均衡使用指南。

- 部署弹性伸缩

  弹性伸缩（Auto Scaling）是根据用户的业务需求和策略，经济地自动调整弹性计算资源的管理服务。通过部署弹性伸缩，系统可以有效的缓解会话层和应用层攻击，在遭受攻击时自动增加服务器，提升处理性能，避免业务遭受严重影响。

  关于弹性伸缩的详细介绍，请查看弹性伸缩使用指南。

- 优化DNS解析

  通过智能解析的方式优化DNS解析，可以有效避免DNS流量攻击产生的风险。同时，建议您将业务托管至多家DNS服务商，并可以从以下方面考虑优化DNS解析。

  - 屏蔽未经请求发送的DNS响应信息
  - 丢弃快速重传数据包
  - 启用TTL
  - 丢弃未知来源的DNS查询请求和响应数据
  - 丢弃未经请求或突发的DNS请求
  - 启动DNS客户端验证
  - 对响应信息进行缓存处理
  - 使用ACL的权限
  - 利用ACL，BCP38及IP信誉功能

- 提供余量带宽

  通过服务器性能测试，评估正常业务环境下所能承受的带宽和请求数。在购买带宽时确保有一定的余量带宽，可以避免遭受攻击时带宽大于正常使用量而影响正常用户的情况。

- 服务器安全加固，提升服务器自身的连接数等性能。

  对服务器上的操作系统、软件服务进行安全加固，减少可被攻击的点，增大攻击方的攻击成本：

  - 确保服务器的系统文件是最新的版本，并及时更新系统补丁。
  - 对所有服务器主机进行检查，清楚访问者的来源。
  - 过滤不必要的服务和端口。例如，对于WWW服务器，只开放80端口，将其他所有端口关闭，或在防火墙上设置阻止策略。
  - 限制同时打开的SYN半连接数目，缩短SYN半连接的timeout时间，限制SYN/ICMP流量。
  - 仔细检查网络设备和服务器系统的日志。一旦出现漏洞或是时间变更，则说明服务器可能遭到了攻击。
  - 限制在防火墙外进行网络文件共享。降低黑客截取系统文件的机会，若黑客以特洛伊木马替换它，文件传输功能将会陷入瘫痪。
  - 充分利用网络设备保护网络资源。在配置路由器时应考虑针对流控、包过滤、半连接超时、垃圾包丢弃、来源伪造的数据包丢弃、SYN阀值、禁用ICMP和UDP广播的策略配置。
  - 通过iptable之类的软件防火墙限制疑似恶意IP的TCP新建连接，限制疑似恶意IP的连接、传输速率。

- 做好业务监控和应急响应。

  - 关注基础DDoS防护监控

    当您的业务遭受DDoS攻击时，基础DDoS默认会通过短信和邮件方式发出告警信息，针对大流量攻击基础DDoS防护也支持电话报警，建议您在接受到告警的第一时间进行应急处理。

    关于配置告警消息接收人和语音告警方式，请查看DDoS基础防护消息接收人设置。

  - 云监控

    云监控服务可用于收集、获取阿里云资源的监控指标或用户自定义的监控指标，探测服务的可用性，并支持针对指标设置警报。

    关于云监控的详细介绍，请查看云监控用户指南。

  - 建立应急响应预案

    根据当前的技术业务架构和人员，提前准备应急技术预案，必要时，可以提前进行技术演练，以检验应急响应预案的合理性。

- 选择合适的商业安全方案。阿里云既提供了免费的基础DDoS防护，也提供了DDoS防护包、高防IP、游戏盾等商业安全方案。
  - Web应用防火墙（WAF）

    针对网站类应用，例如常见的http Flood(CC攻击)攻击，可以使用WAF可以提供针对连接层攻击、会话层攻击和应用层攻击进行有效防御。

    关于WAF的详细介绍，请查看WAF功能使用概览。
  - DDoS防护包

    DDoS防护包为云产品IP提供防御100G以内的DDoS攻击的防护能力，即时生效。

    关于DDoS防护包的详细介绍，请查看DDoS防护包用户指南。
  - DDoS高级防护

    针对大流量DDoS攻击，建议使用阿里云高防IP服务。

    关于高防IP的详细介绍，请查看DDoS高防IP用户指南。
  - 游戏盾

    游戏盾是针对游戏行业常见的DDoS攻击、CC攻击推出的行业解决方案。相比于高防IP服务，游戏盾解决方案的针对性更强，针对游戏行业的攻击防御效果更好、成本更低。

    关于游戏盾的详细介绍，请查看游戏盾用户指南。

应当避免的事项

DDoS攻击是业内公认的行业公敌，DDoS攻击不仅影响被攻击者，同时也会对服务商网络的稳定性造成影响，从而对处于同一网络下的其他用户业务也会造成损失。

计算机网络是一个共享环境，需要多方共同维护稳定，部分行为可能会给整体网络和其他租户的网络带来影响，需要您注意：

- 避免使用阿里云产品机制搭建DDoS防护平台。
- 避免释放处于黑洞状态的实例。
- 避免为处于黑洞状态的服务器连续更换、解绑、增加SLB IP、弹性公网IP、NAT网关等IP类产品。
- 避免通过搭建IP池进行防御，避免通过分摊攻击流量到大量IP上进行防御。
- 避免利用阿里云非网络安全防御产品（包括但不限于CDN、OSS），前置自身有攻击的业务。
- 避免使用多个账号的方式绕过上述规则。

2.2 选择DDoS防护解决方案

阿里云基于多年的DDoS攻防经验和领先的安全技术，提供多款商业化安全解决方案供您选择，满足您业务中对各类DDoS攻击安全防护场景的需求。

高风险DDoS攻击防御场景

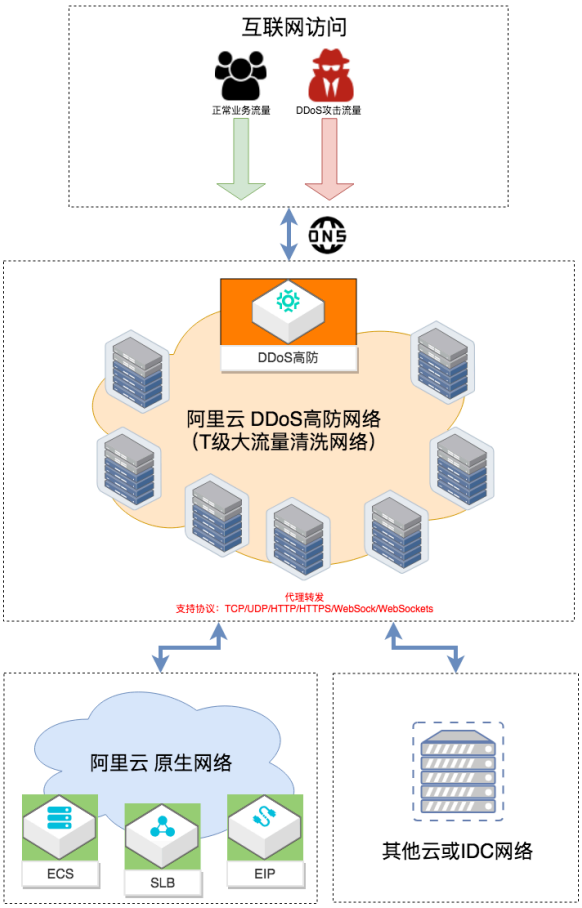
高风险DDoS攻击防御场景具体包含以下特点：

- 遭受恶意攻击者的DDoS攻击勒索
- DDoS攻击已经导致您的业务不可用，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

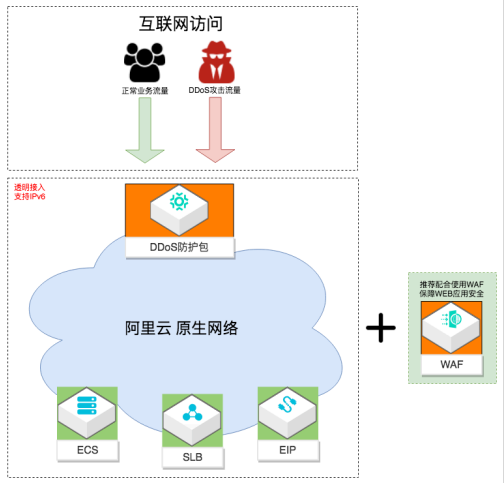
针对这些场景，推荐您根据业务的部署情况，选择以下阿里云DDoS防护安全解决方案：

- 业务部署在中国大陆地域，且业务的主要目标用户为中国大陆地区用户，推荐您选择新BGP高防服务。更多详情，请参见新BGP高防。
- 业务部署在非中国大陆地域，且业务的主要目标用户为非中国大陆地区用户，推荐您选择DDoS高防（国际）服务。更多详情，请参见DDoS高防（国际）。
- 业务部署在非中国大陆地域，且业务的主要目标用户为中国大陆地区用户，推荐您选择DDoS高防（国际）出海套餐。更多详情，请参见DDoS高防（国际）和加速线路。

DDoS高防安全解决方案架构



低风险DDoS攻击防御（大规模业务）场景

低风险DDoS攻击防御场景具体包含以下特点： · 业务资源部署在阿里云环境 · 业务规模较大。例如，业务带宽大于1 Gbps，HTTP/S业务QPS大于5,000 · 偶尔遭受DDoS攻击 · 具有IPv6访问流量的防护需求 针对这些场景，推荐您选择阿里云原生DDoS防护安全解决方案DDoS防护包。 更多详情，请参见DDoS防护包。	DDoS防护包安全解决方案架构 	

移动端业务为主的DDoS攻击防御场景

移动端业务DDoS攻击防御场景具体包含以下特点：

· 主要业务为移动端游戏业务
· 具备集成阿里云SDK的能力
· 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
· 具有网络传输加速需求
· 具有网络加密传输需求
· 需要追溯DDoS攻击的来源

针对这些场景，推荐您选择阿里云专为解决游戏行业面临的DDoS、CC攻击推出的针对性安全解决方案游戏盾。

阿里云DDoS防护解决方案

名称	简介	应用场景	可防御的攻击流量
DDoS基础防护	阿里云提供的基础服务，根据您所购买的阿里云产品免费提供最大5G的DDoS防护能力。同时，您还可以加入安全信誉联盟，根据您的安全信誉分获得更高的安全防护能力。	购买阿里云产品即可获得的基础DDoS防护能力，仅可满足最低的安全需求，对于有更高安全防护需求的用户建议额外选择其他安全方案。	支持防御不超过5G的DDoS攻击
DDoS防护包	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防护包提供的安全能力直接加载到云产品上，提升安全防护能力。	· 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	支持全力防御
新BGP高防 DDoS高防（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。通过配置DDoS高防，将攻击流量牵引至高防，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	支持全力防御
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安全解决方案。相比于高防IP，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 · 游戏行业遭受海量肉鸡长时间机器人攻击（Bot attack）场景的安全防护	支持全力防御

2.3 遭受DDoS攻击后如何向网监报案

如果您的业务遭受大量 DDoS 攻击，一方面您可以采用 DDoS 高防 IP 服务来保障您的业务稳定，另一方面建议您向网监部门进行报案。

报案流程

1. 遭受 DDoS 攻击后，您应该尽快向当地网监部门进行报案，并根据网监部门要求提供相关信息。
2. 网监部门判断是否符合立案标准，并进入网监处理流程。

> 说明:
> 具体立案标准请向您当地的网监部门进行咨询。

3. 正式立案后，阿里云配合网监部门接口人提供攻击取证。

阿里云能提供什么相关证据?

您的报案在网监部门立案后，阿里云将配合网监部门提供以下协助：

- 阿里云会配合网监部门，向网监接口人提供您在阿里云平台上的业务的流量日志、遭受攻击信息等。

> 说明:
> 由于相关数据将作为法律证据，因此无法直接提供给您。您可以在阿里云管理控制台中自行查看攻击流量的相关信息。

- 阿里云不能对流量日志和攻击信息等进行分析，直接给出谁是攻击者的结论。

> 说明:
> 由于阿里云不是法官，无法判定谁有罪；也不是具有执法权的警察，能够进行立案调查；阿里云只能作为证据的提供者和证人。

- 阿里云会及时响应网监部门的协助调查要求，配合开展工作。

建议您在遭受安全攻击时，参考当地网监部门的立案调查标准，积极请求公安网警进行立案调查。

> 说明:
> 您只需要向您当地的网监部门进行报案即可，您所在地的网监部门会直接联系杭州网监部门。阿里云将向杭州网监部门的接口人直接提供相关证据。

自主查看攻击流量的相关信息

您可以在DDoS基础防护控制台或态势感知控制台查看流量、攻击事件、抓包信息等。

说明:

受限于具体攻击情况，抓包信息无法确保每次都能抓取成功。建议您在攻击事件发生当天下载抓包文件。