DDoS攻击介绍

更新时间：2020-07-10 09:27:56

[**本页目录**](javascript:void(0))

* [攻击原理](https://help.aliyun.com/document_detail/28401.html?spm=a2c4g.11174283.6.578.7d3a6298Lx1C85#title-051-qr3-t2h)
* [DDoS攻击的危害](https://help.aliyun.com/document_detail/28401.html?spm=a2c4g.11174283.6.578.7d3a6298Lx1C85#title-u5u-ljf-yqm)
* [常见的DDoS攻击类型](https://help.aliyun.com/document_detail/28401.html?spm=a2c4g.11174283.6.578.7d3a6298Lx1C85#title-xnq-03p-8tr)
* [如何判断业务是否已遭受DDoS攻击？](https://help.aliyun.com/document_detail/28401.html?spm=a2c4g.11174283.6.578.7d3a6298Lx1C85#title-zif-3vy-b4o)

分布式拒绝服务（Distributed Denial of Service，简称DDoS）将多台计算机联合起来作为攻击平台，通过远程连接利用恶意程序，对一个或多个目标发起DDoS攻击，消耗目标服务器性能或网络带宽，从而造成服务器无法正常地提供服务。

**攻击原理**

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，并在网络上的多台计算机上安装代理程序。在所设定的时间内，主控程序与大量代理程序进行通讯，代理程序收到指令时对目标发动攻击，主控程序甚至能在几秒钟内激活成百上千次代理程序的运行。

**DDoS攻击的危害**

DDoS攻击会对您的业务造成以下危害：

* 重大经济损失

在遭受DDoS攻击后，您的源站服务器可能无法提供服务，导致用户无法访问您的业务，从而造成巨大的经济损失和品牌损失。

例如：某电商平台在遭受DDoS攻击时，网站无法正常访问甚至出现短暂的关闭，导致合法用户无法下单购买商品等。

* 数据泄露

黑客在对您的服务器进行DDoS攻击时，可能会趁机窃取您业务的核心数据。

* 恶意竞争

部分行业存在恶性竞争，竞争对手可能会通过DDoS攻击恶意攻击您的服务，从而在行业竞争中获取优势。

例如：某游戏业务遭受了DDoS攻击，游戏玩家数量锐减，导致该游戏业务几天内迅速彻底下线。

**常见的DDoS攻击类型**

| **DDoS攻击分类** | **攻击子类** | **描述** |
| --- | --- | --- |
| 畸形报文 | 畸形报文主要包括Frag Flood、Smurf、Stream Flood、Land Flood、IP畸形报文、TCP畸形报文、UDP畸形报文等。 | 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。 |
| 传输层DDoS攻击 | 传输层DDoS攻击主要包括Syn Flood、Ack Flood、UDP Flood、ICMP Flood、RstFlood等。 | 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攻击主要包括DNS Request Flood、DNS Response Flood、虚假源+真实源DNS Query Flood、权威服务器攻击和Local服务器攻击等。 | 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。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。 |

**如何判断业务是否已遭受DDoS攻击？**

出现以下情况时，您的业务可能已遭受DDoS攻击：

* 网络和设备正常的情况下，服务器突然出现连接断开、访问卡顿、用户掉线等情况。
* 服务器CPU或内存占用率出现明显增长。
* 网络出方向或入方向流量出现明显增长。
* 您的业务网站或应用程序突然出现大量的未知访问。
* 登录服务器失败或者登录过慢

DDoS攻击缓解最佳实践

更新时间：2020-07-08 11:27:03

[**本页目录**](javascript:void(0))

* [DDoS攻击缓解最佳实践](https://help.aliyun.com/document_detail/65932.html?spm=a2c4g.11186623.6.579.59837bfbcqPE9d#title-izu-78v-665)
* [应当避免的事项](https://help.aliyun.com/document_detail/65932.html?spm=a2c4g.11186623.6.579.59837bfbcqPE9d#title-bs1-6ik-5f8)

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。

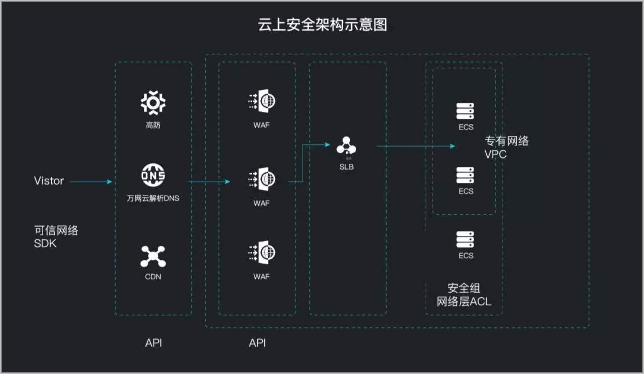
* 会话层攻击

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（即CC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，极大地消耗服务器计算资源，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：[](https://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/0288714951/p34235.png)

* 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，请参见[创建安全组](https://help.aliyun.com/document_detail/25468.html" \l "concept-ocl-bvz-xdb" \o "安全组是ECS实例的虚拟防火墙，用于设置单个或多个ECS实例的网络访问控制。本文介绍如何在ECS控制台上创建一个安全组。)。

* + 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，防止来自内网傀儡机的攻击。

关于专有网络VPC的详细介绍，请参见[什么是专有网络](https://help.aliyun.com/document_detail/34217.html" \l "concept-kbk-cpz-ndb" \o "专有网络是您自己独有的云上私有网络。您可以完全掌控自己的专有网络，例如选择IP地址范围、配置路由表和网关等，您可以在自己定义的专有网络中使用阿里云资源如云服务器、云数据库RDS版和负载均衡等。)。

* 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

通过负载均衡或异地多中心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，请参见[入门概述](https://help.aliyun.com/document_detail/86456.html#concept-ybd-pfl-vdb)。

* + 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，请参见[开通和授权服务](https://help.aliyun.com/document_detail/69789.html#concept-dnl-43m-qfb)。

* + 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阈值、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，请参见[设置黑洞告警通知](https://help.aliyun.com/document_detail/50426.html#task-1814028)。

* + 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，请参见[什么是云监控](https://help.aliyun.com/document_detail/35170.html#concept-2452587)。

* + 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，请参见[什么是Web应用防火墙](https://help.aliyun.com/document_detail/28517.html#concept-tzp-g2m-42b)。

* + DDoS原生防护

DDoS原生防护为云产品IP提供针对DDoS攻击的共享全力防护能力，即时生效。

关于DDoS原生防护的详细介绍，请参见[什么是DDoS原生防护（防护包）](https://help.aliyun.com/document_detail/63643.html#concept-63643-zh)。

* + DDoS高级防护

针对大流量DDoS攻击，建议使用阿里云DDoS高防服务。

关于DDoS高防的详细介绍，请参见[什么是DDoS高防](https://help.aliyun.com/document_detail/153308.html#concept-2417452)。

* + 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，请参见[什么是游戏盾](https://help.aliyun.com/document_detail/65033.html#concept-b3r-vc2-xdb)。

**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。