CLOUDFLARE

电子书

缓解 DDoS 攻击的五个关键考虑因素

如何以更好的 DDoS 防御保护您的组织

目录

概述

分布式拒绝服务（DDoS）攻击仍是网络犯罪分子用来对全球各类组织造成重大财务、运营及声誉损失的最有效手段之一。尽管这些攻击形式各异，但其目标始终是通过来自有组织的僵尸网络、被攻陷设备或网络的流量淹没目标服务器、服务或网络，从而使其陷入瘫痪。

随着各组织不断强化自身网络防御能力，犯罪分子也相应推出了针对多个应用和服务的新型攻击手段。其中，部分攻击以新方式瞄准网络层和传输层，导致网络流量峰值创下新高，达到每秒近 6 Tbps。另一些则是基于应用层的低速、低强度攻击，这类攻击旨在瞄准一个或多个服务网关，且设计得难以被检测到。

要应对 DDoS 攻击带来的挑战，需要采用全面的方法，以应对从网络层到应用层的所有威胁。

但增强安全性不应以牺牲性能为代价。虽然本地部署解决方案可作为部分应对之策，但更完善的解决方案会将性能与可扩展的、基于云的、尽可能接近攻击源的缓解措施相结合，这些措施在网络边缘发挥作用，能提供可扩展的最大灵活性和容量。

什么是 DDoS 攻击?

DDoS 攻击是一种恶意行为，旨在通过大量互联网流量冲击目标或其周围的基础设施，从而阻塞目标服务器、服务或网络的正常流量。

它们通过利用多个被入侵的计算机系统作为攻击流量的来源。利用的机器可以包括计算机，也可以包括其他联网资源（如 IoT 设备）。

总体而言，DDoS 攻击好比高速公路发生意外的交通堵塞，导致正常的车辆无法抵达预定目的地。

DDoS 攻击的类型

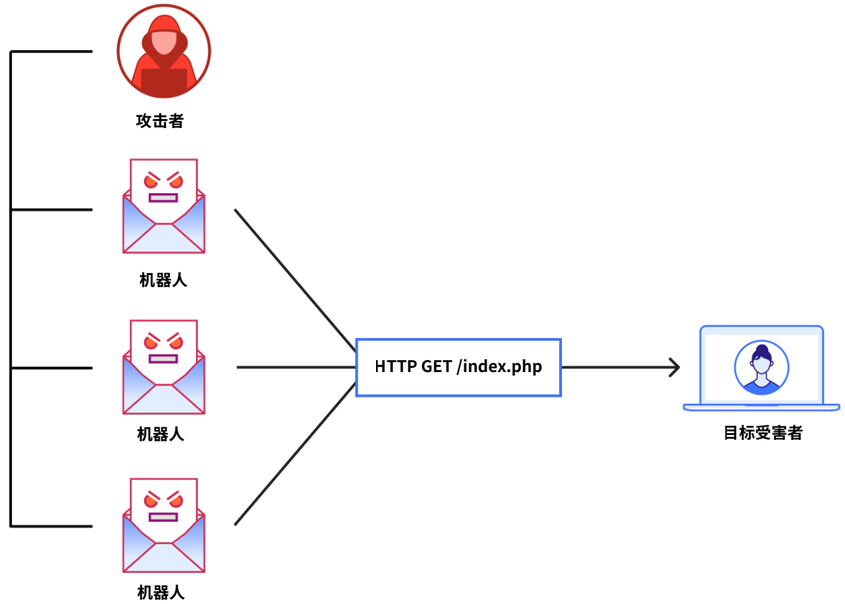
DDoS 攻击的目标可能是组织的应用、网络或源数据中心，这些目标涉及几个不同的层中。尽管所有这些攻击都会用恶意流量淹没目标，但它们可分为三个不同类别：

协议攻击：

协议攻击以网络和传输层中的漏洞为目标，旨在消耗 Web 服务器或其中间资源（包括防火墙和负载平衡器）的所有可用容量。这些攻击可能使用 SYN 洪水和碎片包攻击。这些攻击均以每秒数据包数（PPS）衡量。

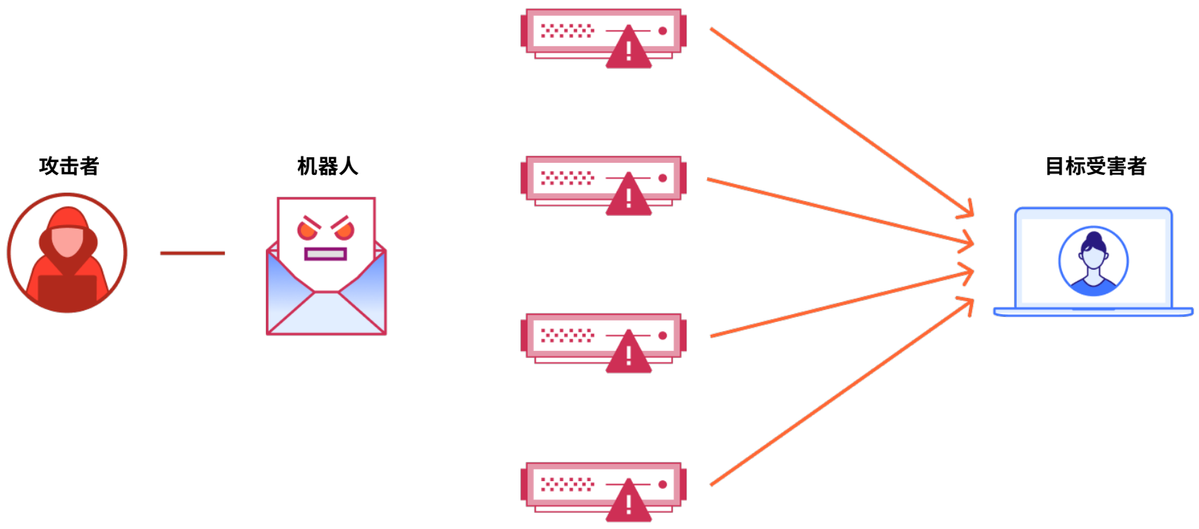
应用层攻击：

应用层攻击的目标是服务器上响应 HTTP 或 HTTPS 请求以生成网页并交付的层。这类攻击类似于在多台计算机上同时反复点击网页浏览器中的 “刷新” 按钮，由此产生的 HTTP/S 洪水可通过每秒请求数（RPS）来衡量。



容量耗尽型攻击：

这些容量耗尽攻击尝试耗尽目标与互联网之间的可用带宽，从而造成拥塞。运用某种放大方式或其他生成大量流量的手段（如僵尸网络请求），向目标发送大量数据。



为什么组织应该关注 DDoS 攻击?

如果遭遇 DDoS 攻击而下线，收入、客户服务和基本业务功能都会受到不利影响。在当今 “永远在线” 的世界，下线哪怕短短几分钟都有可能意味着失去宝贵客户、关键收入和来之不易的声誉。无论目的是破坏您的站点或网络，将流量转移到竞争对手，掩盖窃取企业数据的行为，还是仅仅导致最大程度的声誉损失，无论是对您的客户还是合作伙伴而言，DDoS 攻击都会造成同样程度的损害。

平均而言，严重中断通常持续 77 小时，并可能导致组织每小时损失高达 190 万美元。[1]这表明，影响企业收益的不仅是攻击的持续时间，还包括恢复和重新赢得客户信任所需的努力。

正如 “2025 年第一季度 DDoS 威胁报告” 中所述，Cloudflare 阻止了 2,050 万次 DDoS 攻击，相比 2024 年第一季度增长了 358%。超过 1 Tbps 的攻击数量也大幅增加。这些类型的超大容量攻击平均每天约 8 次，最大的一次攻击达到 6.5 太比特每秒 (Tbps)，与有史以来报告的最高带宽攻击相当。

一般而言，防范 DDoS 攻击需要具备以下能力：

- 分辨流量峰值源自于攻击还是高用户需求
- 阻止僵尸网络产生的流量，同时不中断合法流量
- 通过将剩余流量分成可管理的区块来智能路由，以防止拒绝服务
- 持续分析流量中的恶意攻击模式，以协助开发自适应、强化的安全防御措施

遭受攻击最多的十大行业：2025 年第一季度

1. 游戏与泛娱乐 — 季度环比：+4
2. 电信、服务提供商和运营商 — 季度环比：-1
3. 信息技术和服务 — 季度环比：+1
4. 互联网 — 季度环比：-2
5. 游戏 — 季度环比：+1
6. 银行和金融服务 — 季度环比：+2
7. 网络安全 — 季度环比：+37
8. 零售 — 季度环比：-1
9. 制造、技术和工程 — 季度环比：+28
10. 航空公司、航空、航天 — 季度环比：+40

想进一步了解 DDoS 攻击趋势？请查阅 Cloudflare 最新的 DDoS 威胁报告。

缓解 DDoS 攻击的五个关键考虑因素

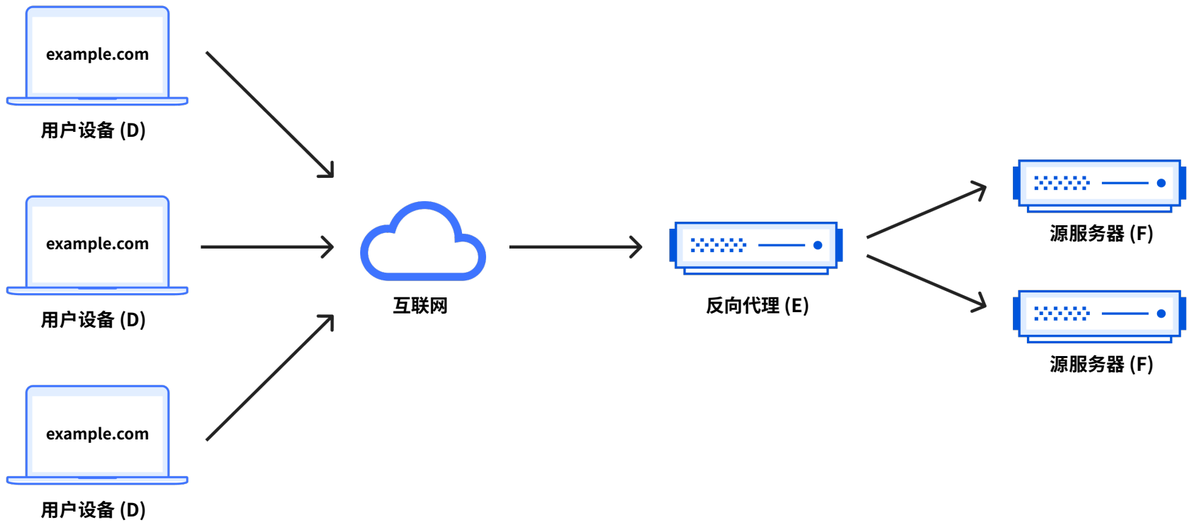
1

为每个资源量身定制方案

如果您的目标是保护 Web 服务器，添加反向代理可以为您的 Web 服务器打造一个“前门”，并带来诸多额外优势，例如负载平衡以及攻击防护 —— 这是因为 Web 服务器的 IP 地址会对潜在攻击者隐藏。本图展示了反向代理的工作原理。

对于更复杂的应用层攻击，Web 应用防火墙（WAF） 可充当反向代理，保护目标服务器免受某些类型的恶意流量攻击。

虽然有些组织选择自行构建或部署反向代理，但这需要大量的软件和工程资源，同时还需在硬件方面进行重大投资 —— 这些硬件平均每 3-5 年就需要更换。



2

优先考虑两个最重要的指标：容量与 TTM

评估现有容量，是否能在不影响站点功能的情况下缓解 DDoS 攻击。要吸收 DDoS 攻击所产生的流量激增，传统方式一直是建立本地服务器群。但这种做法的成本会迅速增加，而且在日益增大的容量耗尽攻击面前，即使最强大的企业级基础设施也可能不堪重负。速率限制能助一臂之力，但它会导致性能下降，而且一旦基础设施过载，仍有可能导致中断。

如果可用性短暂下降都会导致收入和生产力严重损失，缓解时间（TTM）就变得极其重要。为缩短 TTM，您需要确保流量可以在发生中断时转移到备用站点，但这只能在基础设施不堪重负之前起作用。

同样，更有效的方法是部署基于云的缓解解决方案，其提供无限的容量，防御任何规模或复杂性的 DDoS 攻击，并能在网络边缘提供服务，从而以最高灵活性缓解快速演变的 DDoS 攻击。

3

考虑始终在线还是按需保护

DDoS 缓解服务提供两种主要部署模式：按需部署和始终在线。

在按需模式下，正常流量直接流向应用，无需重定向，并仅在检测到攻击时，流量才会被转移到云清洗中心。这种方法通常需要客户干预来启动缓解，从而增加了攻击期间的响应时间。

始终在线方法会持续将所有流量通过提供商的数据中心进行路由，以进行威胁检查，即使在正常运行期间也是如此。这种方法可缩短检测到缓解的时间而不会导致服务中断，从而提供最全面的保护。它提供了一种无需动手的体验，在攻击期间客户不用采取任何行动。

虽然始终在线保护更全面，但也需要确保验证潜在供应商在通过其云基础设施转移所有流量时不会引入延迟。

4

绝不为安全而牺牲性能

DDoS 攻击会导致系统响应迟缓与服务中断，不仅降低性能，还会损害组织实现可持续增长的能力：

47%的用户不会等待加载超过两秒的网站[2]。换句话说，今天的消费者期望网站和应用能够瞬间加载，并且永远不会离线。

延迟也会损害生产力 —— 员工等待应用加载或网络响应所花费的时间会迅速累积。远程办公的兴起加剧了这个问题：一项远程办公调查结果中，89% 的受访者表示，由于互联网连接速度缓慢，他们平均每天损失的时间超过 30 分钟多。[3]

防御 DDoS 攻击而不降低性能需要细致的平衡。

如前所述，许多组织试图通过将流量重定向到通常远离流量源或源服务器的清洗中心来缓解 DDoS 攻击。这会造成瓶颈，导致延迟水平与遭受攻击时同样糟糕。因此，有限的清洗中心服务无法扩展以抵御可能来自任何地方的 DDoS 攻击。

相反，为了获得更快的响应时间，请考虑使用云交付的缓解服务，此类服务能够在全球任何地区靠近攻击来源的物理位置执行检测和缓解。

5

选择情报以领先于攻击者

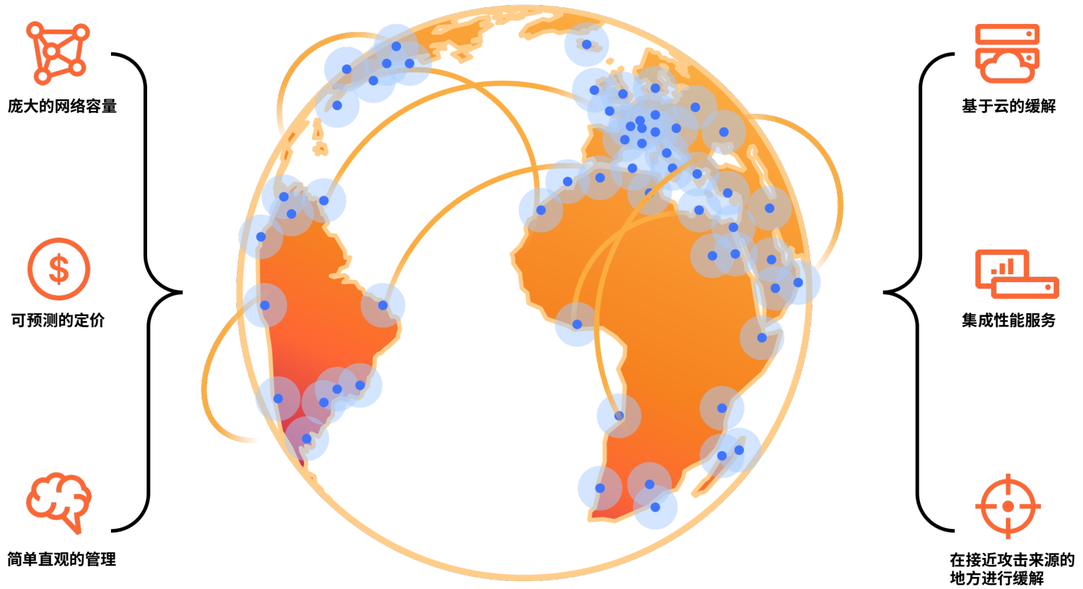
要抵御日益复杂的 DDoS 攻击，仅依靠分层防护策略并不足够。这需要持续分析流量中的恶意模式，以帮助您构建智能、自适应防御机制以有效防范未来攻击。

进行中的 DDoS 攻击正是抵御下一次攻击的关键所在：评估基于云的缓解服务时，重要的是不能只看防护容量、流量转发或过滤速度，还要关注其覆盖范围所提供的情报。

缓解网络规模越大、越强健，其针对不断演变的攻击模式所能提供的情报就越丰富，这些服务的预判性也就越强。

结语

应对 DDoS 攻击相关挑战，您需要采用全面的方法，以覆盖所有层级的各类威胁。尽管本地部署解决方案可作为部分应对方案，但它们很快会变得成本高昂且不切实际。更强大的解决方案将性能与可扩展的云端缓解相集成，可在网络边缘配置服务，提供最大的灵活性和无限的容量。这种解决方案有助于抵御任何规模或复杂程度的 DDoS 攻击。

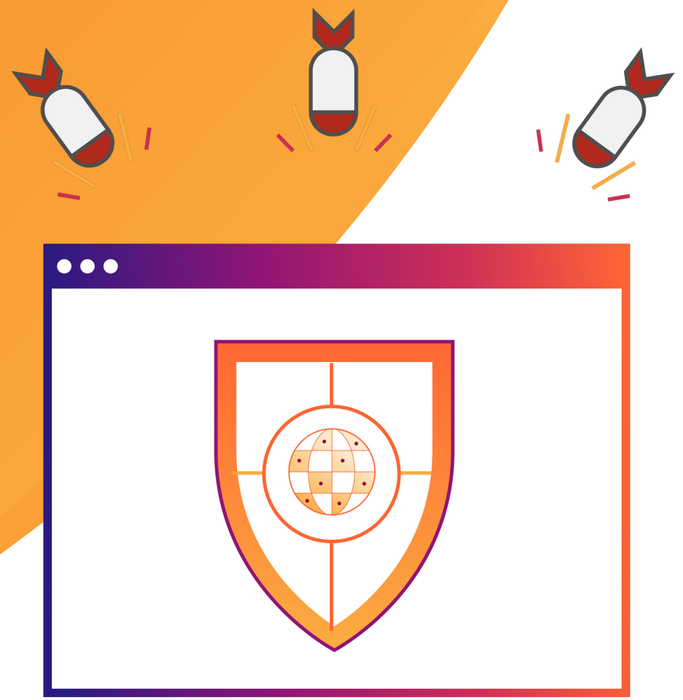


Cloudflare 如何帮助预防 DDoS 攻击

Cloudflare 提供集成的第 3-7 层 DDoS 防护，可帮助组织在攻击到达目标应用、网络和基础设施之前对其进行监控、阻止和缓解。我们的分层威胁防御具有以下主要优势：

- 全球 Anycast 网络，覆盖全球 335 个城市和 125 个国家/地区，能够吸收最大规模的 DDoS 攻击
- 流量路由和加速，帮助分散网络中的流量峰值，最大程度地减少延迟和拥塞
- 始终在线的自动 DDoS 缓解服务，可在三秒内检测并阻止恶意流量
- 下一代 WAF，提供先进的速率限制、定制规则集和灵活的威胁预防功能

了解 Zendesk、Shopify 和 Porsche Informatik 等组织如何借助 Cloudflare 阻止 DDoS 攻击。



参考资料

1. https://www.ciodive.com/news/it-tech-outages-cost-new-relic-report-crowdstrike/731100/
2. https://www.forbes.com/advisor/business/software/website-statistics/
3. https://www.computerweekly.com/news/252487354/Poor-connectivity-sees-home-workers-lose-over-half-an-hour-of-work-a-day

010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com/zh-cn/

REV:BDES-7230.2025MAY05