

缓解 DDoS 攻击的五种最佳实践

如何防御快速发展的分布式拒绝服务威胁，应对每一层上的漏洞



索引

内容摘要	3
第 1 部分: 什么是 DDoS 攻击?	4
DDoS 攻击的种类	5
DDoS 攻击的影响	8
第 2 部分: DDoS 攻击的新兴趋势	9
第 3 部分: DDoS 缓解的最佳实践	12
1. 加强保护策略	13
2. 优先考虑两个最重要的指标 — 容量和缓解时间	14
3. 考虑 永久在线 和 按需保护	15
4. 绝不安全而牺牲性能	16
5. 拥抱威胁情报以领先于 攻击者	17
Cloudflare 如何提供协助	18
总结	19

内容摘要

分布式拒绝服务 (DDoS) 攻击仍然是网络犯罪分子使用的最有效攻击方式之一，可对全球企业造成严重的财务、运营和声誉损害。尽管这些攻击会采取不同的形式，但目标始终是利用被入侵设备或网络的巨大流量，导致目标服务器、服务或网络瘫痪。

随着组织加强防御，网络犯罪分子转而发动新型攻击和更高容量的攻击。其中一些攻击采用全新的方式，将[开放系统互连 \(OSI\) 模型](#)的第 3 和第 4 层作为目标，产生的流量峰值可超过 1 Tbps。另一些则是基于第 7 层的低速度、低密度攻击，旨在避免引起注意，以一个或多个服务网关及应用程序层为目标。

应对 DDoS 攻击带来的挑战，需要一种全面的方法来解决所有层面的全部威胁。但是，增强安全性不应以牺牲性能为代价。虽然硬件设备工具可成为解决方案的一部分，但更健壮的解决方案将性能与可扩展的云端缓解相集成，并运行于网络边缘节点，从而提供最大的灵活性和无限的容量。

什么是 DDoS 攻击？

分布式拒绝服务 (DDoS) 攻击是一种恶意行为，利用大量互联网流量来淹没目标服务器、服务或网络，干扰其运行或使其下线。

DDoS 攻击者利用恶意软件控制在线计算机、路由器、物联网设备和其他设备，并将其作为攻击流量的来源。被感染的设备通常被称为机器人 (bot)，一组机器人则被称为“[僵尸网络 \(botnet\)](#)”。在攻击过程中，僵尸网络中的每台设备同时向目标发送请求，企图超过目标的流量上限，导致对正常流量的拒绝服务。

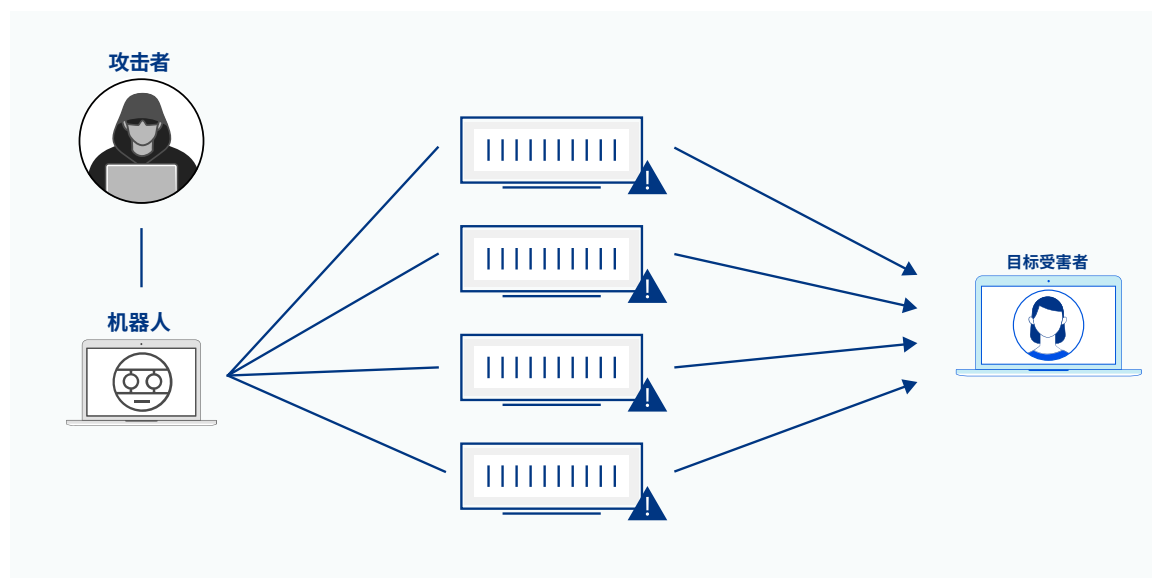
第 1 部分 – 什么是 DDOS 攻击

DDoS 攻击的种类

DDoS 攻击的目标可以是 OSI 模型中七“层”中的任何一个。虽然所有这些攻击都涉及用恶意流量淹没目标，但它们可以划分成三个不同的类别。这些类别描述了攻击发生的地点和方式。

容量耗尽攻击

这些攻击利用巨大的流量淹没目标站点和网络——流量远高于任何其他类型的攻击。这些攻击常常利用 [DNS 放大](#) 和其他暴力技术来产生巨大的流量激增，以比特率/秒 (bps) 来衡量。（在 DNS 放大攻击中，攻击者使用公开 DNS 解析器来以放大后的流量淹没目标。）

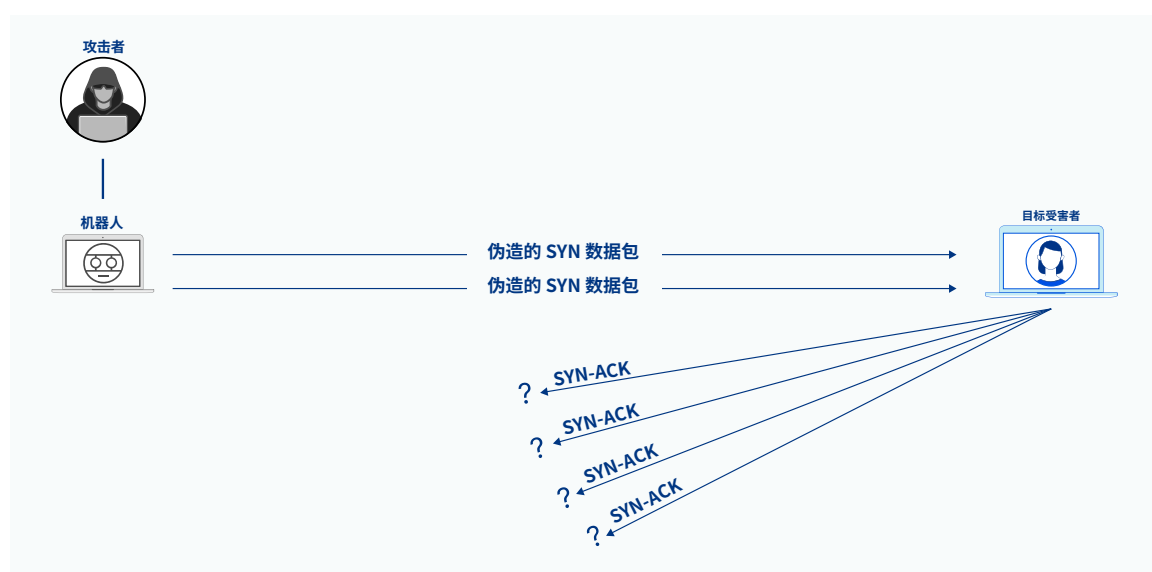


第 1 部分 – 什么是 DDOS 攻击

协议攻击

协议攻击以 OSI 模型的第 3 层（网络层）和第 4 层（传输层）中的漏洞为目标，旨在消耗 Web 服务器或其中间资源（包括防火墙和负载均衡器）的所有可用容量。这些攻击均以数据包/秒（pps）为单位衡量，包括：

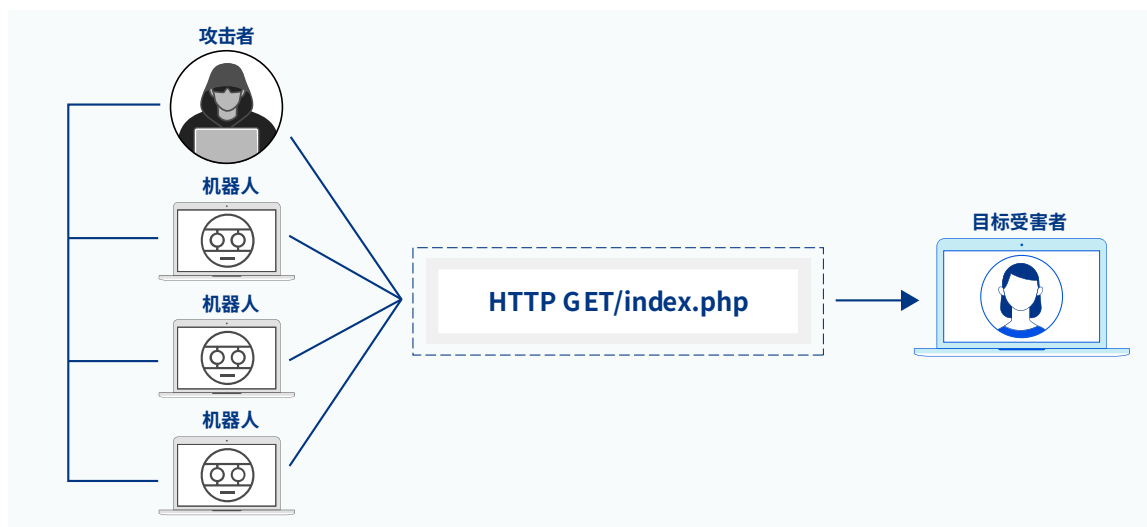
- [SYN 洪水](#)：这种攻击重复发送初始连接请求（SYN）包，以淹没目标服务器上所有可用的端口。
- [Ping of Death 攻击](#)：攻击者向目标发送超过最大允许大小的包，导致目标冻结或崩溃。
- [Smurf DDoS](#)：在这种攻击中，攻击者利用 [互联网控制消息协议 \(ICMP\)](#) 包来淹没服务器。



第 1 部分 – 什么是 DDOS 攻击

应用层攻击

这些攻击以 OSI 第 7 层为目标。在这一层，作为对 HTTP 或 HTTPS 请求的回应，服务器生成网页并发送出去。这些攻击相当于在许多计算机上同时反复刷新网页。因此，所产生的 HTTP/S 请求洪水以请求数/秒 (Rps) 来衡量。



这些类型的攻击之间存在一些重叠。例如，部分协议攻击可能属于容量耗尽型攻击。同时，还有多手段攻击，其中攻击者以协议堆栈的多层为目标，或同时发动，或作为对目标的反制措施的响应。

DDoS 攻击的影响

DDoS 攻击一旦成功，其直接影响是目标服务的性能下降或直接中断。目标服务的全部或部分可能无法访问。

这些性能上的挑战有更广泛的影响。对 web 应用而言，性能低下带来[一系列不利影响](#)，包括更高的跳出率，更低的转化率，以及品牌声誉受损。对企业网络而言，性能欠佳导致员工无法完成很多日常工作。

此外，一些 DDoS 攻击是掩盖其他攻击的烟幕，使安全团队分心应对，以便攻击者通过其他手段实现其最终目标。在这种情况下，目标组织有可能遭遇未经授权的应用访问、恶意软件感染、数据丢失或更糟的情况。

DDoS 攻击的新兴趋势

一般而言，企业需要若干核心能力来防御DDoS 攻击：

- 区分攻击流量和合法流量
- 在不影响合法用户流量的情况下检测不良机器人并阻止恶意机器人流量
- 分析流量并发现能有助于改善防御措施的恶意模式

然而，一些新兴趋势正在使 DDoS 安全变得更具挑战性。

第 2 部分— DDOS 攻击的新兴趋势



容量耗尽攻击依然存在, 且规模越来越大

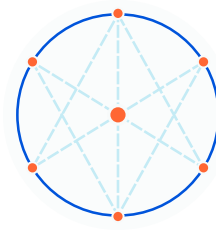
容量耗尽攻击可轻松压垮不受保护的组织。此类攻击的规模有增无减, 给企业带来更大压力。

2021 年 11 月, Cloudflare 自动阻止了一次创纪录的多维度 DDoS 攻击, 其峰值流量接近 2 Tbps。这是 Cloudflare 迄今为止观察到的最大攻击, 来自 1.5 万个运行 [Mirai 僵尸网络](#) 变种代码的机器人。不幸的是, 与著名的 Mirai 僵尸网络及其变种有关的攻击已经卷土重来。

例如, 在 2021 年夏季, 另一个 Mirai 变种僵尸网络发动了基于 UDP 和 TCP 的攻击, 流量多次超过 1 Tbps, 峰值达到 1.2 Tbps 左右。

除了 Mirai 相关攻击外, Cloudflare 网络数据显示, 大部分攻击依然在 500 Mbps 以下。尽管如此, [2021 年第三季度](#), 介于 500 Mbps 和 1 Gbps 的攻击较前一季度增长了 289%, 介于 1 Gbps 和 100 Gbps 的攻击环比增长了 126%。

取决于组织的规模和所用的应用程序, 网络带宽可能差异巨大。这意味着, 在未受保护的情况下, 某些组织很容易被相对较小的攻击击倒。因此, 随着容量耗尽攻击的规模增长, 企业应评估其 DDoS 缓解解决方案的容量。



攻击越来越复杂

多维度并行攻击大行其道, 表明 DDoS 攻击的复杂性日益增加。

近期[针对互联网语音协议 \(VoIP\) 提供商的攻击](#)激增就是多维度攻击的一个例子。VoIP 提供商专业从事利用语音、视频等在互联网通信的技术。这些攻击同时使用针对关键 HTTP 网站和 API 接口的第 7 层 (L7) 攻击和针对 VoIP 服务器基础设施的 L3/4 攻击。

在多维度攻击中, 攻击者 (通常是动态地) 使用多种攻击手段, 使得区分合法流量和恶意流量难上加难。不幸的是, 如果攻击者通过调整来规避应对措施, 则丢弃或限制流的做法将无济于事。

新攻击方式的出现, 或此前不常见的方式的兴起, 是 DDoS 攻击复杂性的另一个例子。例如, Cloudflare 发现, 2021 年第三季度, [DTLS](#) 放大攻击较前一个季度增加了 3,549%。同样, Cloudflare 网络数据显示, [2021 年第二季度](#), 滥用 [Quote of the Day \(QOTD\)](#) 的放大型 DDoS 攻击较前一季度增长了 123%。在同一季度, [利用 QUIC 协议的攻击](#)较前一季度增加了 109%。

随着攻击者不断寻找新方法发起更复杂的攻击, 组织在每个层面防御 DDoS 攻击变得至关重要。

第 2 部分 – DDOS 攻击的新兴趋势



勒索 DDoS 攻击日益增加

另一个重要趋势是勒索 DDoS 攻击增加。在勒索 DDoS 攻击中，攻击者向某个组织发出要进行 DDoS 攻击的威胁，以换取勒索金。某些情况下，攻击者将发动一次小型 DDoS 攻击，以证明其有能力并会实施攻击。攻击者通常要求以比特币或其他形式的加密货币来支付勒索金。

[2021 年上半年](#)，遭到 DDoS 攻击的受访 Cloudflare 客户中，有 11% 事前收到了勒索信。

例如，一家[财富 500 强公司](#)在 2020 年开始使用 Cloudflare Magic Transit (为本地网络提供 DDoS 保护等服务)。此前该公司收到一个网络犯罪团伙的勒索信，要求支付 20 个比特币。为了证明其意图，该团伙已经在台服务器上发动了 Gb 级攻击。

基于这些要求和发展趋势，组织应该优先考虑如下五种 DDoS 缓解实践。

DDoS 缓解最佳实践

- 加强保护策略
- 优先考虑两个最重要的指标——容量和缓解时间
- 考虑永远在线还是按需保护
- 绝不安全而牺牲性能
- 拥抱威胁情报以领先于攻击者

1. 加强保护策略



由于 DDoS 攻击可在 OSI 协议栈的多个层发生，采用全面的保护措施很重要。然而，传统的 DDoS 保护解决方案并非处理这个问题的唯一途径。如下策略可作为 DDoS 解决方案的补充并保护服务器和网络。

使用反向代理保护服务器

如果您的目的是保护 web 服务器，反向代理将防止攻击者识别您的服务器 IP 地址并将其作为目标。这样一来，攻击者将只能以反向代理为目标，从而保护了您的服务器。

一些公司构建或部署自己的反向代理，但这需要大量的软件和工程资源，以及对物理硬件的大量投资。

要实现反向代理的优势，最简单、最经济的方法之一是使用[内容分发网络 \(CDN\)](#)。CDN 是分布式的代理服务器网络，通过在更接近最终用户的地方缓存内容（或储存副本）来降低延迟。

寻找一个拥有[全球服务器负载均衡功能](#)的 CDN，以便您的站点能分布在全球各地的多个服务器上。这样一来，DDoS 攻击将能在更接近来源的地方被缓解，而不会影响到性能。（有关安全与性能权衡的更多信息，请参阅“提示 4”。）

保护网络

如果目标是保护网络基础设施，则可使用[边界网关协议 \(BGP\)](#) 重新路由，将流量重定向到可过滤掉恶意流量的清洗中心。但这样一来，所有流量都会被重新路由到数量有限、位置偏远的清洗中心，从而导致延迟明显增加。

因此，建议使用具有足够规模的云端 DDoS 缓解解决方案。使用基于云的缓解措施时，缓解服务提供商将公告自治系统编号 (ASN)，使流量直接路由到清洗服务器，而非前往源服务器。在这种配置中，流量在更接近攻击来源的地方被过滤，进一步降低了延迟。

2. 优先考虑两个最重要的指标——容量和缓解时间



DDoS 保护中最重要的因素是保护的强度（容量）和抵御攻击的速度（缓解时间）。

容量

为吸收 DDoS 攻击所产生的流量高峰，传统方法是投资购置本地硬件。但这样做成本很快就会变得昂贵起来，因为企业必须为应付孤立的攻击而并不常用的容量付费。此外，即使最健壮的企业级基础设施都有可能被最大规模的攻击所压垮。

[速率限制](#)，即限制服务器在一段时间内可接收的请求数量，会有帮助。然而，单纯使用速率限制会导致合法流量峰值期间性能下降，而且无法承受更复杂的攻击。

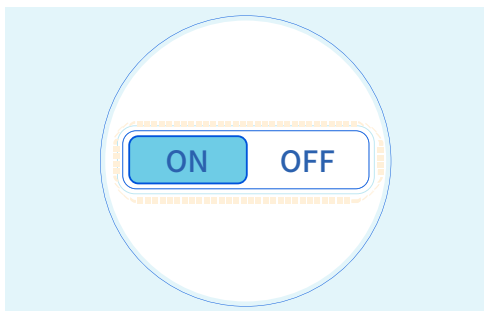
因此，优先使用高容量解决方案很重要。基于云且拥有可扩展资源的 DDoS 缓解甚至能吸收最大规模的攻击，使您的组织毫发无损。

缓解时间

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。要减少 TTM，您将需要确保流量能在发生中断时转移到替代站点——但这种方法仅在您的基础设施被压垮之前才有效。

相比之下，基于云且运行于边缘的 DDoS 保护在接近来源的地方缓解攻击，从而帮助减少 TTM。

3. 考虑永远在线和按需保护



使用按需缓解服务时，流量正常转发，直至检测到潜在的 DDoS 攻击。此时，流量将被重新路由到云端缓解服务，经过过滤并回传到源服务器。

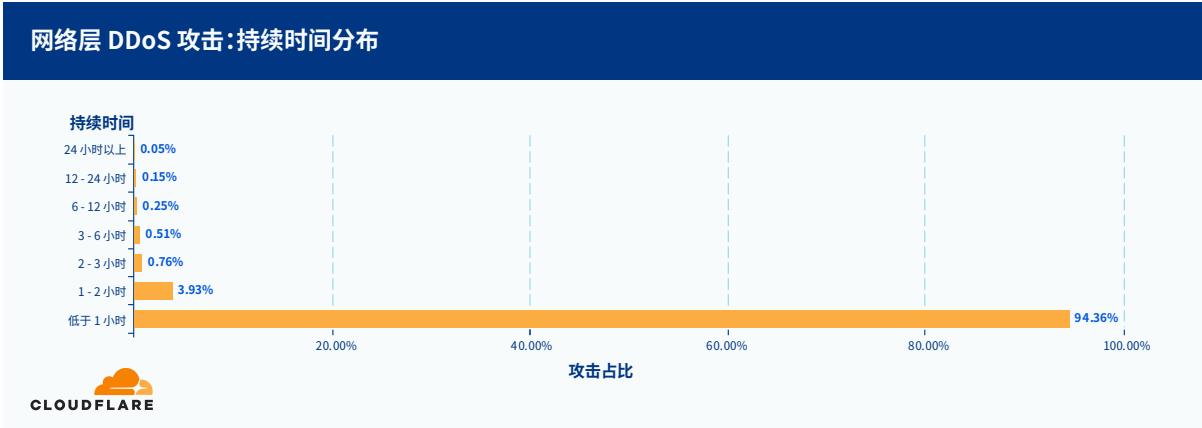
您仅在需要时为 DDoS 缓解付费，无需管理或额外资源。但这样也存在一些损失，尤其是在 TTM 方面。阻止攻击需要更长时间，这是因为，流量峰值必须达到特定的阈值，才会启动分析，并由人手动打开缓解服务。

按需解决方案不能很好地抵御短暂的攻击，而根据 Cloudflare 网络数据，大部分攻击都是短暂攻击。例如，[2021 年第三季度](#)，超过 94% 的网络层攻击持续时间不到一小时。短暂攻击也许听起来并不可怕，但如果未能及时启动按需保护，这些攻击也能产生巨大影响。更不用说，某些情况下，即使停机几分钟也可能造成损失。

攻击者也可能利用短暂攻击来测试某个组织的防御，然后再发动更大规模的攻击。

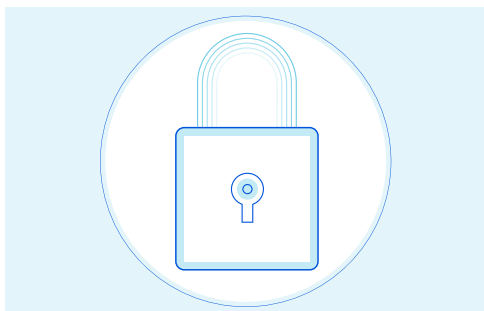
第 3 部分 - DDOS 缓解的最佳实践

相比之下，永远在线的缓解会持续路由和过滤所有站点流量。这样一来，只有干净的流量才会到达客户的服务器。虽然比按需服务更昂贵，但始终启用的缓解提供不间断的保护。这样做能减少 TTM，因为永远不需要手动打开服务。



来源: <https://radar.cloudflare.com/notebooks/ddos-2021-q3>

4. 绝不安全而牺牲性能

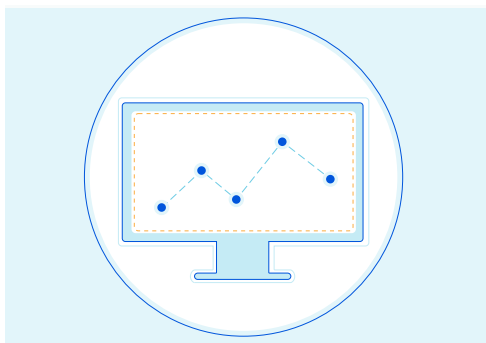


当今的数字消费者预期网站和应用能持续可用并快速加载。事实上，大多数人感知到的延迟仅为 [100-200 毫秒](#)。但延迟并不只是带来不便，因为[延迟每增加一秒，转化率就会降低 4.42%](#)。因此，在不降低影响的情况下防御 DDoS 攻击要求仔细的平衡。

为缓解攻击，很多组织尝试将流量重定向到清洗中心以过滤流量。然而，这些清洗中心往往远离流量来源或目的地网络，从而造成增加延迟的瓶颈。这迫使组织在性能和安全之间做出选择。

基于边缘的云缓解服务为这一平衡提供了解决方案。这些解决方案建立于分布式网络上，缓解在网络中的每一台服务器上运行，而非在集中式数据中心缓解攻击。这意味着，检测和缓解都在尽可能接近攻击来源的地方运行，从而减少 TTM。

5. 拥抱威胁情报以领先于攻击者



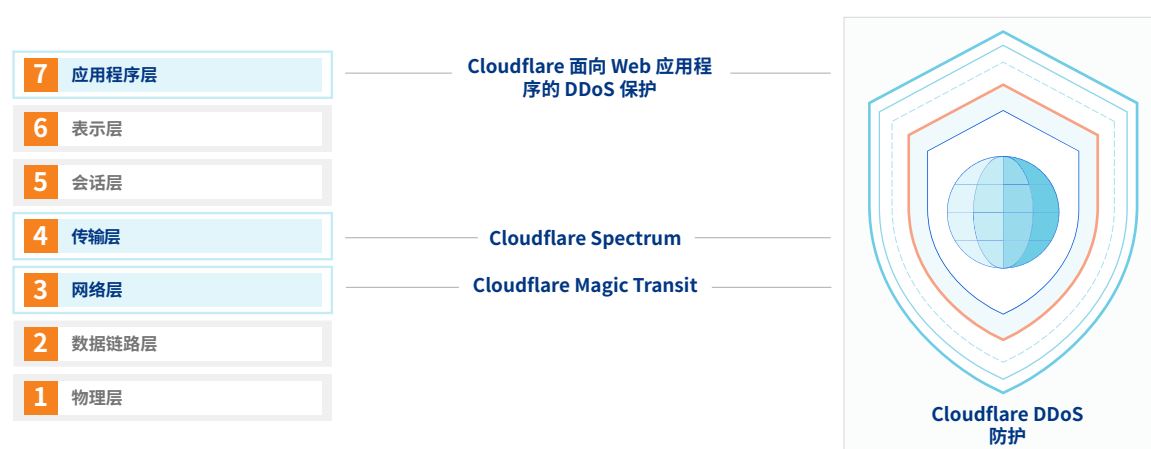
抵抗日益复杂的 DDoS 攻击不仅需要采用分层的方法。您还需要持续分析流量以识别恶意模式，以帮助您开发智能的自适应防御措施，以抵抗日后的攻击。

基于云的缓解系统往往采用机器学习，以便在新兴攻击出现前就予以检测和缓解。这就是所谓“威胁情报”。在评估基于云的缓解服务时，重要的一点是不仅考虑容量或传输和过滤速度，还要考虑网络情报。缓解网络规模越大、越健壮，它就能为不断演变的攻击模式提供更丰富的情报，从而提供更主动的保护。

Cloudflare 如何提供协助

Cloudflare 的分层安全防护方法将多种 DDoS 缓解能力整合到一个服务中，能够防止恶意流量造成的中断，并允许干净流量通过。我们使网站、应用程序、API 和整个网络维持正常运行，并提供高可用性和高性能。

Cloudflare 100 多个国家/地区超过 250 个城市设有数据中心，网络容量超过 100 Tbps，可在来源附近缓解 DDoS 攻击。



快速、自动缓解

与依赖于清洗中心的解决方案不同，Cloudflare 在我们网络上的每一台服务器上运行安全服务，能够抵御任何规模或复杂程度的 DDoS 攻击。

全面保护

Cloudflare DDoS 缓解在网络边缘缓解检测并阻止第 3、4 和 7 层攻击。此外，Cloudflare Spectrum 通过 Cloudflare 数据中心代理流量，保护 TCP/UDP 应用程序。

全球规模的威胁情报

Cloudflare 的全球网络保护着数百万个互联网资产，为 Cloudflare DDoS 提供情报。通过这些情报，我们能识别异常流量，防范复杂的新兴攻击。

高性价比的保护

所有 Cloudflare 计划都提供无限、不计量的 DDoS 缓解，无论攻击规模如何，无额外费用，也不会对攻击相关的流量激增进行惩罚。

第 3 部分 - DDOS 缓解的最佳实践

易于使用和管理

Cloudflare 始终启用的云 DDoS 保护提供直观的界面，用户仅需点击几下鼠标，即可快速、简单地保护其互联网资产，防御任何规模或复杂程度的 DDoS 攻击。

集成的安全和性能

Cloudflare 的 DDoS 保护可与其他安全和性能产品（包括 [web 应用程序防火墙](#)、[Cloudflare 机器人管理](#)、[Cloudflare Magic Transit](#)、[Cloudflare 负载均衡](#)、[Cloudflare CDN](#) 等）无缝集成、学习和操作。

以您的方式进行数据分析

[Cloudflare Analytics](#) 让您能够通过 Cloudflare 的集成仪表板或 GraphQL 分析 DDoS 事件。Cloudflare 日志也可与领先的第三方安全信息和事件管理 (SIEM) 工具集成。

总结

要制定行之有效有效的策略来应对 DDoS 攻击相关挑战，需要一种综合全面的方法来应对每个层面的所有威胁。本地解决方案可作为答案的一部分，但它们很快就变得代价高昂。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，确保能抵御任何规模或复杂程度的 DDoS 攻击。

© 2022 Cloudflare Inc.保留一切权利。Cloudflare 徽标是 Cloudflare 的商标。
所有其他公司和产品名称分别是与其关联的各自公司的商标。