白皮书

CLOUDFLARE

Cloudflare Magic Transit 既保护网络，又提升性能

Cloudflare Magic Transit 为本地、云和混合网络提供 DDoS 保护和流量加速。依托遍布 200 个城市的数据中心和超过 51 Tbps 的 DDoS 缓解容量，Magic Transit 能在接近源头的位置检测和缓解攻击，平均用时不足 3 秒，而且还附带了性能方面的效益。

本文将展示对我们网络运行的 Catchpoint 测试的结果，以量化 Magic Transit 对延迟的影响。测试结果表明，当流量通过 Cloudflare Magic Transit 路由时，试验客户的网络性能（延迟和数据包丢失）得以改善。具体而言，我们在测试结果中发现，流量通过 Magic Transit 路由时延迟缩短了 3 毫秒，数据包丢失则几乎为零。

Cloudflare Magic Transit 如何做到在不影响性能的前提下保护网络基础结构?

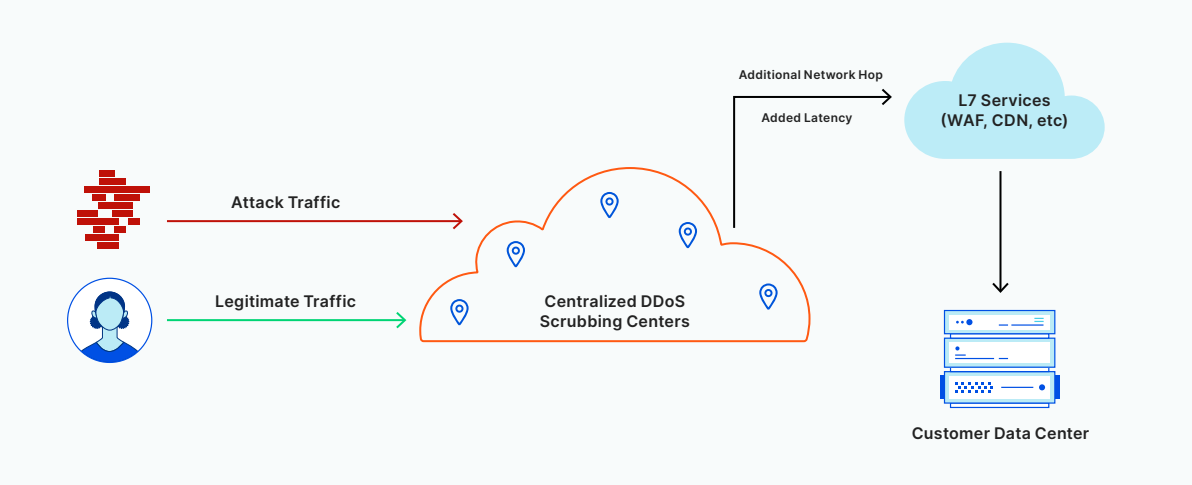
在 Magic Transit 诞生之前，保护网络基础结构免受 DDoS 攻击的策略主要有两种：本地硬件 DDoS 防护设备和云端清理解决方案。

在一定程度上，本地硬件设备可以很好地保护您的基础结构。这些设备的带宽有限，可能会被规模较大或同时发生的攻击压垮。硬件也需要大量前期投资，而且花费许多资源来进行管理和维护。

云端清理中心应运而生，提供一种更简单的替代选择：使流量经由清理中心进行传输，并在清理中心过滤掉攻击流量。这解决了本地硬件引起的财务负担和维护难题。

然而，这也造成了新的问题：显著的延迟。

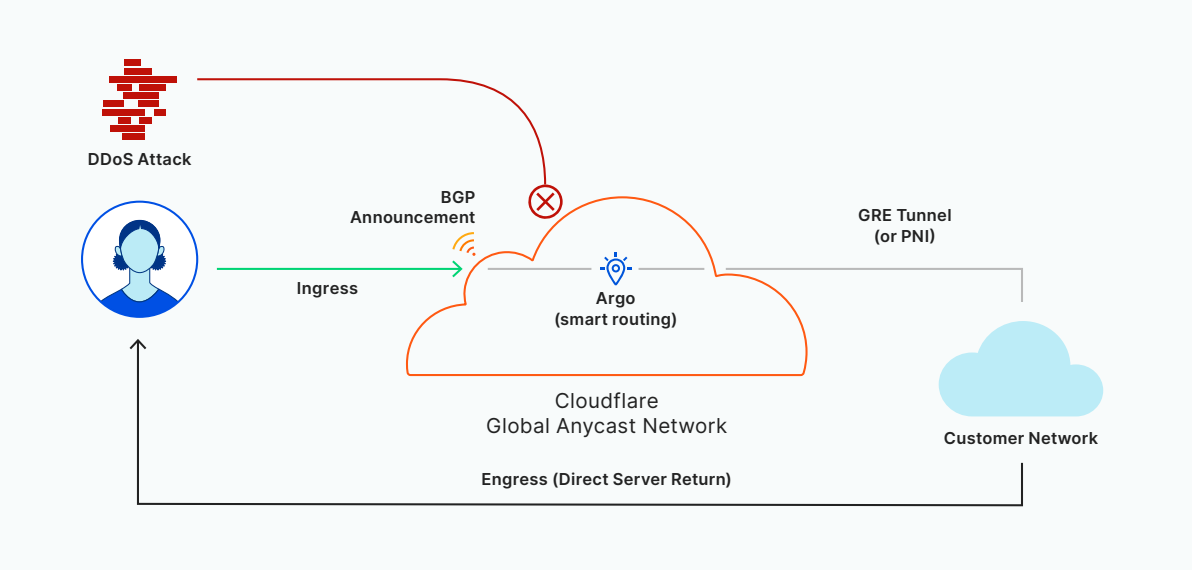
由于这些云提供商的清理中心数量有限，并且分散于不同的地理位置，因此流量可能必须传输很长距离以进行清理，然后才能到达最终目的地。云提供商通常只有屈指可数的清理中心，如果您或最终用户与所有清理中心相隔甚远，即使最终目的地就在附近，流量也必须传输很长一段距离。这是所谓的长号效应，通常会引起明显且恼人的延迟。（之所以称为“长号效应”，是因为如果您在地图上标出路途较长的往返路线，其形状类似于长号）。



“清理中心”距离远、数量少，专门用于缓解 DDoS。这需要网络流量传输到备用数据中心，以进行额外的 L4-7 处理，从而导致额外的延迟。

以上述情况为例，您需要在第 3-4 层以及第 7 层服务（例如 WAF 和 Bot Management 等）中处理流量。这时，您的流量首先到达遥远的 L3 清理中心以缓解 L3 DDoS，然后发送到辅助数据中心以进行任何其他 L7 处理，给端到端流量添加了网络跃点，引入了不必要的延迟。如果云供应商的清理中心数量有限，并且与网络流量的源头相距很远，那么延迟就会特别明显。

Magic Transit 带来了更好的解决方案。我们不使用专门的清理中心，而是让 Cloudflare 全球网络中的每个数据中心都能处理清理工作。 实际上，每个 Cloudflare 数据中心都运行完整的 Cloudflare 服务堆栈。这样一来，您的流量只需传到最近的 Cloudflare 数据中心便可；我们在 100 多个国家/地区的 200 多个城市设立了数据中心，因此距离有可能会很近。

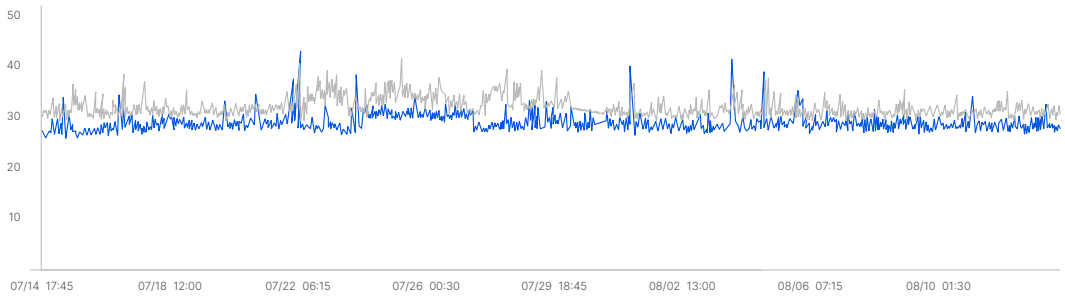


每个 Cloudflare 数据中心运行 L3-7 服务的完整堆栈，因此网络流量可在同一位置进行处理。

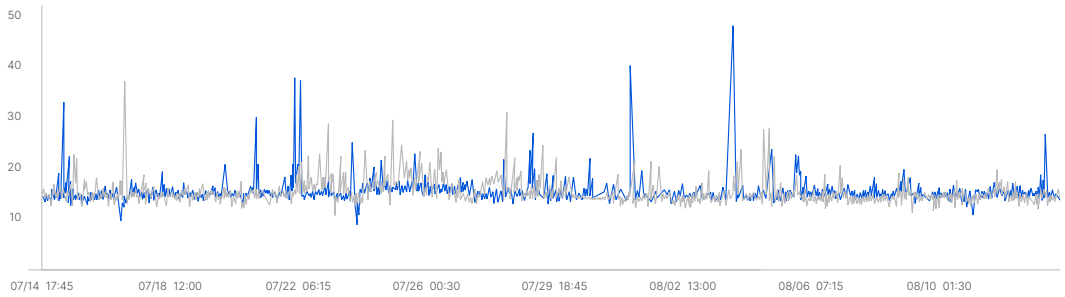
这意味着，没有长号效应，延迟也很短。网络性能是我们开发 Magic Transit 的首要关注点；我们想确保用户不会以性能为代价来获得安全性。

Catchpoint 测试

为了验证这一点，我们使用 Catchpoint 进行了一些测试，以判断使用 Magic Transit 对整体网络性能的影响。通过全局分布探针，我们对位于 Magic Transit 后方的 IP 地址和不用 Magic Transit 的另一个地址运行 ICMP ping 测试，这两个地址都托管在同一网络基础结构上。这样，我们能够同时测量延迟、数据包丢失和抖动，以查看性能差异。



使用 Magic Transit（蓝色）和不用 Magic Transit（灰色）时的延迟（ping 往返）性能（毫秒）



使用 Magic Transit（蓝色）和不用 Magic Transit（灰色）时的抖动性能（毫秒）

使用 Magic Transit（蓝色）和不用 Magic Transit（灰色）时的数据包丢失性能（百分比）

在上述测试中，蓝线代表使用 Magic Transit 时的性能，灰线则代表不用 Magic Transit 时的性能。

测试结果

性能	使用 Magic Transit（蓝色）	不用 Magic Transit（灰色）
延迟	28.96 毫秒	31.98 毫秒
抖动	15.61 毫秒	15.24 毫秒
丢包	0.52%	5.26%

这些测试的重点

- 使用 Magic Transit 时延迟缩短了 3 毫秒
- 使用 Magic Transit 时抖动增加了 0.36 毫秒
- 使用 Magic Transit 时数据包丢失几乎为零 (0.52%)，而不用 Magic Transit 时则为 5.26%

这些结果意味着什么?

延迟: 延迟是数据包从网络上的一个点传输到另一点所花费的时间。在我们的测试中，我们观察到 Cloudflare 网络的延迟较低。

Cloudflare 根据不同网络路径的状态不断优化流量路由，因此数据包从 Cloudflare 到客户网络的传出路径的效率通常要高于那些未经 Cloudflare 优化的数据包。

这可确保网络延迟不会延长，而且如我们的测试结果所示，许多情形中甚至可以缩短。这对于对延迟敏感 (实时) 的应用程序尤为重要，例如在线游戏和 IP 语音 (VoIP) 服务。

抖动: 网络抖动是指网络上数据包传递之间的延迟量。减少抖动对于 VoIP 等应用尤其重要。使用Magic Transit 时，抖动增加了 0.36 毫秒。即使对抖动敏感的应用，这也可以忽略不计。

数据包丢失: 网络传输中若有一个或多个数据包未能到达目的地，就会发生数据包丢失。根据具体的协议，数据包丢失可能会造成需要花费额外时间来重新传输，或者导致质量下降。对于像视频会议这样对时间极为敏感的传输，丢包率低于 1% 被认为可以接受*。在我们的测试中，我们观察到 Cloudflare 网络上的丢包率几乎降低到了零 (相比之下，不用 Magic Transit 时的丢包率超过了 5%)

总之，Magic Transit 对延迟、抖动和数据包丢失的影响不会损害用户体验，而且在许多情况下甚至还能改善体验。换而言之，Cloudflare 客户在使用 Magic Transit 时不必为网络性能“权衡取舍”而操心。

此外，Cloudflare Magic Transit 可与 Cloudflare 的所有安全性、性能和可靠性产品集成，进一步优化互联网资产的性能。

若要进一步了解 Cloudflare Magic Transit，请访问 www.cloudflare.com/magic-transit
或通过以下地址联系我们: sales@cloudflare.com

**https://web.archive.org/web/20131010010244/http://sdu.ictp.it/pinger/pinger.html*