白皮书

设计具有可用性和弹性的 DNS，充分应对 DDoS 攻击

简介

Edge DNS 为公司提供权威 DNS 服务，以将最终用户与其网站和其他应用程序连接起来。由于公司将大部分的注意力都集中在性能上，通常也就忽视了 DNS 在可用性和应变能力方面的重要性，尤其是针对企图中断服务并阻止用户进行连接的 DDoS 攻击。Akamai 对 Edge DNS 进行了专门设计，使其具有出色的全球规模、分段 IP Anycast 架构和多种 DDoS 控制措施（包括在必要时利用其他 Akamai 服务的能力），因此可以在面对大规模 DDoS 攻击时保持可用性。Edge DNS 以托管 DNS 服务的形式提供，它提供了性能和可用性的优化组合，从而始终将公司与最终用户连接起来。

统计数据备注

Akamai 最初构建 Edge DNS 的目的是提供权威 DNS 服务，以支持全球内容交付网络 (CDN) 解决方案。多年来，Akamai 在如何出色扩展大型 DNS 基础架构并维持可用性方面吸取了许多经验教训。右侧的高级统计数据可帮助读者笼统地了解平台的规模。但是，仅靠统计数据无法深入体现平台的可用性和恢复能力，还应结合考虑平台架构、特定 DDoS 缓解功能以及 Akamai 在保护平台抵御攻击时可用的整体容量。

平台统计数据

- 数千台名称服务器
- 1,000 多个入网点
- 超过 140 个城市
- 40 多个国家/地区

请注意，出于安全原因，Akamai 不会披露与名称服务器数量或入网点的数量、位置或规模有关的具体细节。此策略可保护 Akamai 和我们的客户抵御攻击者（可能会在规划攻击时尝试使用这些信息）。

架构

从上面的统计数据可以看出，Edge DNS 的规模比当今市场上其他最具竞争力的权威 DNS 服务更大。但是，有关服务器数量和入网点数量或总网络容量的高级统计数据不足以帮助读者全面了解这个全球化平台的可用性和恢复能力水平。与过去专门关注性能的其他 DNS 解决方案不同，Akamai 对 Edge DNS 进行了专门设计，除了兼顾性能之外，还提供了针对 DDoS 攻击的可用性和恢复能力，它具有多个级别的架构冗余，包括名称服务器、入网点、网络、甚至分段 IP Anycast 云。

IP Anycast

Edge DNS 包含数千个部署在 1,000 多个入网点的名称服务器，采用 IP Anycast 模型来响应 DNS 查询。IP Anycast 将来自最终用户的查询定向到最近的入网点以进行解析。除了更快的性能外，IP Anycast 还在可用性和恢复能力方面提供了几个基本优势，这也是大多数权威 DNS 服务使用它的原因：

- **可用性** - IP Anycast 允许不同网络位置的名称服务器响应针对单个 IP 地址的查询。通过利用 IP Anycast，Edge DNS 不仅在多个数据中心中为公司提供 DNS 解析，还通过全球分配负载来提高可用性。此外，单个物理服务器或整个入网点可以离线，而不会影响域名解析的总体能力。
- **规模** - Edge DNS 基础架构包含跨多个入网点的众多物理服务器，为公司提供了大量计算资源，在响应大量 DNS 请求时，公司可以始终依赖这些资源。Edge DNS 还可以在许多入网点访问大量额外的网络容量，因为它通常与其他 Akamai 服务共享容量。与独立 DNS 服务相比，这为 Edge DNS 提供了更大的规模来响应 DNS 泛洪攻击和其他形式的 DDoS 攻击。
- **分布** - 除了实现更大的规模之外，IP Anycast 还允许 Edge DNS 跨多个入网点和不同的网络位置分配流量。通过仔细考虑这些入网点的地理位置和网络部署，有助于控制较小的攻击对特定地理位置或网络的影响，并保持其他区域的客户端系统的可用性。

对 IP Anycast 的利用并非 Akamai 独有。通过允许多个名称服务器解析来自最终用户的 DNS 查询，IP Anycast 可提高任何 DNS 服务的域名解析可用性。但即使使用 IP Anycast，恢复能力仍受平台总规模的限制，大型 DDoS 攻击仍会使基于云的平台不堪重负。此外，如果没有多样化的架构，即使是较小的攻击，也有可能在特定地理区域击垮 DNS 服务，导致大量最终用户无法使用 DNS 服务，并影响这些用户连接到的任何网站的可用性。

Edge DNS 云

为了进一步提高针对攻击的恢复能力，Edge DNS 将其名称服务器和入网点分段到多个 IP Anycast 云中。Edge DNS 云由专用名称服务器和入网点以及关联的网络容量和连接组成。每个云都独立运行，因此 Edge DNS 在可用性、规模和分布性方面可以等同于多个独立的 DNS 提供商。

Edge DNS IP Anycast 云代表一组多样化的架构。虽然各个云之间不尽相同，但它们在性能和可用性这两大设计原则方面大体保持一致：

- **性能** - 高性能云可能在全球分布 100 多个入网点，每个都包含一组名称服务器。如图 1 所示，高性能云在靠近最终用户和本地互联网服务提供商 (ISP) 的许多位置部署小型名称服务器群集，以便提供更快的查询速度和更高的原始性能。从定义上来看，小的入网点对 DDoS 攻击的抵御能力较低，计算资源更少，网络容量更小，这是一种此消彼长的关系。
- **可用性** - Edge DNS 维护着许多高可用性云。如图 1 所示，高可用性云的入网点更少，但包括一个或多个锚点区域，这些锚点区域可以在集中式数据中心中包含数百个名称服务器，并通过多个网络提供大量专用网络容量和连接。锚点区域为高可用性云提供了相应的规模，以响应 DNS 请求和其他网络流量的巨大高峰。高可用性云通过少量较小的入网点来增强锚点区域，从而为全球用户维持可接受的性能水平。

图 1：Edge DNS 将多个 DNS 云与不同的架构相结合，从而提供性能、可用性和针对 DDoS 攻击的恢复能力的出色组合。

分段架构

与在单个 IP Anycast 云上运行权威 DNS 服务的其他提供商相比，Edge DNS 提供了截然不同的可用性水平。对于所有提供商而言，IP Anycast 允许服务在经历小型攻击（可能只影响特定地理位置，而不是整个平台）时，保持总体正常运行，从而提供了一些可用性优势。但是，即使是局部中断，也会对中断地区的最终用户以及依赖该服务与这些用户进行连接的公司造成影响。此外，通过攻击全球系统而产生流量的更大型的 DDoS 攻击可能会导致整个平台中断。

Edge DNS 拥有许多多样化的 IP Anycast 云，即使一个或多个云丢失，也可以继续运行。与单云架构相比，这可以提供更高程度的可用性和恢复能力来抵御 DDoS 攻击。此外，通过运行多个 IP Anycast 云，

可以在整个平台的各个子部分之间进行流量分段，从而缓解大规模 DDoS 攻击产生的影响。例如，针对单个 Edge DNS IP Anycast 云的攻击将定向到构成该特定云的物理名称服务器和入网点。分段架构将攻击造成的影响与其他 IP Anycast 云隔离开来，因此，即使单个云或客户可能受到 DDoS 攻击，Edge DNS 仍可在所有地理位置保持平台可用性。

图 2：每个 Edge DNS 客户都在高性能和高可用性云的唯一组合上获得名称服务器，从而尽可能减少针对其他客户的攻击造成的附带损害。

除了提高整体平台恢复能力之外，Edge DNS 分段架构还可在其他客户使用的名称服务器受到攻击时，降低对单个客户造成附带损害的风险。Edge DNS 为每位客户分配多个 Edge DNS 云，并提供高性能和高可用性云的独特组合（不被其他客户共享）。如图 2 所示，这种分配可尽可能减少任意两个客户之间名称服务器和 IP Anycast 云的重叠。即使分配给另一客户的 IP Anycast 云明确遭受大型 DDoS 攻击，它也可确保每个客户都拥有可用的名称服务器。

管理客户委托

针对单个公司的多个 DDoS 攻击通常在更长的时间内发生，Akamai 发现，广泛而持续的攻击活动曾持续数月或更长时间。在这种情况下，Edge DNS 的分段架构为 Akamai 提供了更大的灵活性，可进一步尽可能减少对非攻击目标的客户造成的影响。如图 3 所示，Akamai 可以重新分配单个客户的云，并在必要时进一步隔离攻击的影响。

图 3：Akamai 可以管理名称服务器委派，以进一步尽可能减少攻击的影响（与上面的图 2 对比），例如，将攻击目标客户从单个云中移出，并尽量减少非目标客户的重叠。

例如，Akamai 可以：

- **将攻击目标客户移离特定云** - 每个 Edge DNS 客户都与其他客户共享 IP Anycast 云。因此，针对一个客户的所有 Edge DNS 云的攻击可能会影响分配给其他客户的云的可用性。在正常情况下，递归解析程序会自动切换到性能更好的云，但对于持续的攻击活动，Akamai 可以重新分配攻击目标客户的 IP Anycast 云，以恢复非目标客户的可用性。
- **尽量减少非攻击目标客户的重叠** - 有时，多个 Edge DNS 客户共享的 Edge DNS 云数量可能高于正常数量。在这种情况下，针对单个客户的大规模攻击可能会对其他客户产生可观的性能影响，但总体服务仍然可用。如有必要，Akamai 可以为非攻击目标客户重新分配云，以减少或消除与攻击目标客户的重叠，并恢复其最终用户的性能。

多样化服务器部署

在每个 Anycast 云中，Akamai 在不同位置部署物理名称服务器，旨在提高该云的整体恢复能力。多样化 Edge DNS 云位置进一步在不同网络之间对流量进行分段，以便在不同情况下尽可能提高可用性。例如：

- **在具有多个网络的数据中心中** - 在考虑针对 DDoS 攻击的恢复能力时，网络连接的多样性与容量的大小一样重要。大型 DDoS 攻击可能会在到达数据中心之前就使上游 ISP 和其他网络不堪重负，从而导致网络拥塞和服务中断，即使数据中心本身不受影响也是如此。为了保持可用性，以及能够在攻击期间响应最终用户的 DNS 查询，Edge DNS 将名称服务器部署到大型数据中心（不仅具有大容量，而且还通过多个网络进行连接）。
- **ISP 隔离** - 在许多情况下，Edge DNS 直接在各个 ISP 的网络中部署名称服务器群集。这些名称服务器通常仅在这些网络中广播它们的 IP Anycast 流量，并仅为这些 ISP 的最终用户解析 DNS 查询。虽然这种安排限制了任何特定名称服务器群集可以服务的最终用户数量，但当 IP Anycast 云成为该 ISP 之外的攻击的目标时，此策略也可帮助这些用户维持可用性。攻击者必须在该特定 ISP 网络上拥有系统，才能看到这些名称服务器，即使如此，可用的容量通常足以为该云提供保护。
- **网络多样性** - 有意为客户分配不同的云 - 有些云的服务器位置是特定 ISP 所独有的，有些则连接了更广泛的计算机。此架构可确保，给定客户端的递归名称服务器始终能够连接到可用的 Edge DNS 云。

- **在与其他 Akamai 服务共享的数据中心中** - 通过运行权威 DNS 之外的许多不同服务，Akamai 可以将 Edge DNS 名称服务器部署到支持多种服务的数据中心中。如下文所述，这使 Edge DNS 在响应大型 DDoS 攻击时能够访问更大的网络容量，即专用网络容量，以及 Akamai 为其他服务部署的公用共享容量。

DDoS 控制

除了架构设计之外，Edge DNS 还包括多项控制措施，以帮助缓解 DNS 泛洪攻击等 DDoS 攻击造成的影响。许多 DDoS 攻击会使用大量流量来让网络链路不堪重负，而 DNS 泛洪攻击会生成大量合法 DNS 请求，以占用物理名称服务器上的计算和内存资源，并阻止它们响应实际最终用户的查询。Akamai 通过以下几种方式保护 Edge DNS 平台抵御 DNS 泛洪攻击：

- **规模** - Akamai 权威 DNS 服务的规模可能是其他竞品 DNS 解决方案的数倍。Edge DNS 利用了在全球 1,000 多个入网点部署的数千台名称服务器。虽然 IP Anycast 不是明确的 DDoS 控制措施，但它会将攻击流量分散到不同的地理位置和网络中，而物理名称服务器的数量为 Edge DNS 提供了足够的计算和内存资源，以吸收 DNS 请求的巨大高峰。
- **速率限制** - Edge DNS 包括速率限制功能，并且可以在请求量超过设置的阈值后自动丢弃来自各个 IP 地址的请求。速率限制可防止 DNS 请求中的巨大高峰占用物理名称服务器上的计算和内存资源，在应对生成大量请求但占用带宽相对较低的攻击时非常有用。请注意，Edge DNS 上的速率限制功能不可由客户配置，而是由 Edge DNS 平台独有的算法进行配置。
- **DNS 白名单** - 由于 Akamai 在互联网上的优势地位，它对递归解析程序的行为具有独特的可见性，这些解析程序负责处理互联网上大约 95% 的合法 DNS 查询。在重负载下，Edge DNS 可以在必要时采用正安全模型，并限制 DNS 请求发送到一组已知良好的 DNS 解析程序进行处理。

关于容量

虽然 DDoS 控制在缓解 DNS 泛洪攻击的影响时十分有用，但对于其他类型的网络层 DDoS 攻击，需要具备足够的可用网络容量来吸收大量流量。在过去几年中，容量耗尽攻击的风险大幅增加，最大的已知攻击现在的峰值带宽已远远超过 1 Tbps。

Akamai 不会披露 Edge DNS 平台的容量，以避免为攻击者提供可量化的目标。但是，Akamai 会持续投资增强平台规模的各个方面，不断发展 Edge DNS 基础架构，以满足新客户的要求，并妥善应对互联网上的流量增长。作为云服务提供商，Akamai 可以快速调整服务器的用途，并将 DNS 容量部署到新区域。Akamai 保留了大量可用容量以吸收巨大的流量高峰，而 Edge DNS 平台上的正常流量消耗的容量不到其总容量的 1%。如有必要，Edge DNS 还可以利用来自其他 Akamai 平台的资源以缓解 DDoS 攻击。

利用其他 Akamai 平台

传统方法（使用网络容量来估算抵御高带宽 DDoS 攻击的能力）不适用于 Edge DNS，主要因为，Edge DNS 可以利用来自其他 Akamai 平台的资源。Akamai 不仅仅是一家 DNS 公司，还运营着 Edge DNS 之外的许多服务。在 Akamai 运营的所有服务中，权威 DNS 对其他服务的运营至关重要，但整体流量仍然很小。这让我们有机会在需要时增加 Edge DNS 的可用容量：

- **从 CDN 借用容量** - 在许多情况下，Edge DNS 部署名称服务器的入网点与属于其他 Akamai 服务（在 Akamai CDN 上运行）的服务器相同。这些入网点通常要大得多，因为它们设计用于支持消耗更高带宽的服务。这还为 Akamai 提供了运营灵活性，使其可以在必要时从 CDN 借用容量，方法是：通过其他 Akamai 入网点转移其他服务，并将共享网络容量专门提供给 Edge DNS，以便它可以吸收大型 DDoS 攻击。
- **部署专用缓解容量** - 除了权威 DNS 和 CDN 之外，Akamai 还运营着具有专用缓解容量和功能的单独 DDoS 保护服务。当需要抵御大型 DDoS 攻击时，Akamai 可通过 Prolexic 清理中心分配各个名称服务器委派，以利用专用容量和 DDoS 抵御工具。这可以在 Edge DNS 前面有效地部署 Prolexic 平台的 DDoS 缓解功能，从而保留 Edge DNS 的资源以响应最终用户的合法查询。

多个 DNS 供应商

Edge DNS 提供了权威 DNS 服务（规模是许多竞品服务的数倍）、具有多个分段 IP Anycast 云的弹性架构，以及可利用其他 Akamai 服务的额外容量和功能抵御 DDoS 攻击的能力。凭借这些优势，Edge DNS 可以提供必要的可用性和恢复能力，以充当公司的唯一权威 DNS 提供商。但是，一些公司可能会选择将 Edge DNS 与其现有解决方案一起部署。多供应商部署允许公司保留现有的 DNS 记录管理做法，同时通过 Edge DNS 的额外可用性和冗余对其主要的 DNS 解决方案进行补充。

部署选项

Edge DNS 支持通过多种方式在多供应商环境中部署 Edge DNS：

- **传统辅助服务** - 拥有现有 DNS 提供商的公司可以将 Edge DNS 部署为辅助服务，以增强其主要的 DNS 解决方案。公司继续通过他们的主要提供商管理 DNS 记录，并使用区域转移或 Edge DNS API 自动更新 Edge DNS。主要和辅助解决方案都可以响应最终用户的查询，从而提供额外的可用性。
- **隐藏的主服务** - 对于希望继续在内部 DNS 解决方案上管理 DNS 记录的公司，Akamai 建议使用此部署选项。隐藏的主服务允许 Edge DNS（作为唯一的辅助 DNS 提供商或多个提供商之一）响应最终用户查询，使得内部解决方案不会遭受 DDoS 攻击。公司继续通过他们的主要提供商管理 DNS 记录，并使用区域转移或 Edge DNS API 自动更新 Edge DNS。
- **双重主服务** -“隐藏的主服务”概念的变种。某些云服务提供商不再采用传统的区域转移功能，并要求客户使用他们的 API 或其他用户接口进行区域记录更改。在这种方法中也可以利用 Edge DNS，方法是在主模式下配置 Edge DNS，并将 Edge DNS 云添加为权威 DNS。

以辅助服务的形式维持可用性

部署为辅助 DNS 解决方案时，Edge DNS 依赖主 DNS 解决方案中的区域更新，以确保它正确响应最终用户查询。通常，在有效期 (TTL) 内，区域文件在辅助 DNS 解决方案上保持有效，该期限受 Start of Authority（授权开始）记录中的到期字段控制。一旦中断时长超过 TTL 值，导致主解决方案中断的 DDoS 攻击也可能导致辅助解决方案停止响应查询。Edge DNS 通过以下方式防止出现这种情况：(1) 在 TTL 到期后，区域文件仍保持有效，以及 (2) 只要 DNS 注册表指向 Edge DNS，就继续响应 DNS 查询。这有助于以辅助 DNS 解决方案的形式提供额外的可用性（即使主解决方案不可用）。

结论

目前，最大的已知 DDoS 攻击的峰值带宽超过 1 Tbps。在这种规模下，将无法通过计算云服务可用的总带宽来准确评估针对此类攻击的恢复能力，即使是较小的攻击也可能导致出现区域级别的中断。Edge DNS 采用多层可用性方法为客户提供 100% 的可用性，该方法结合了：

- 覆盖全球的庞大规模，包括比许多竞品服务多出数倍的名称服务器和入网点
- 弹性架构，具有多个分段 IP Anycast 云，可隔离攻击的影响并防止对其他客户和整个平台造成附带损害
- 针对 DDoS 攻击的托管式响应，包括部署 DDoS 控制措施或根据需要重新分配客户委派的能力
- 利用其他 Akamai 服务的能力，包括 Akamai CDN 和 Prolexic DDoS 保护，可增强容量并抵御大型和小型 DDoS 攻击

权威 DNS 是一项任务关键型服务，它将全球最终用户与公司的在线业务连接到一起。无论是部署为唯一的权威 DNS 提供商，还是与现有 DNS 解决方案相结合，Edge DNS 都能为公司提供所需的可用性，使全球用户能够顺利访问公司的网站和其他面向互联网的应用程序。

Akamai