Akamai

白皮书

如何利用正确的应用层 DDoS 平台

规避“不速之客”

如今，应用层 DDoS 对我们意味着什么

世界各地的安全专家都非常清楚，DDoS（即分布式拒绝服务）是一种网络攻击，此类攻击会尝试用恶意流量淹没网站或网络资源，从而导致其无法正常运行。DDoS 攻击仍是攻击者最常用的攻击技术，而且过去五年中一直呈上升趋势。例如，最近的一次大规模攻击（以每秒数据包 [PPS] 计）在大约两分钟内峰值便达到了 809 MPPS。

从攻击数量的增加程度中，我们不难看出这样一个趋势，即应用层 DDoS 攻击的实例越来越多。这类攻击也称为第 7 层 DDoS 攻击，针对并破坏特定的网络应用程序，而不是整个网络。因此，不仅防御者很难去防范和抵御此类攻击，而且随着自动化和云服务等技术的大量采用，攻击者能够轻松获得发动这些攻击所需的工具，从而让入侵应用层变得前所未有的简单。

实际情况中，这类攻击中使用的请求看上去就像是正常的最终用户请求，因此很难去衡量攻击的复杂程度。由于能够更有效地侵袭目标服务器和网络，这意味着攻击以更少的总带宽就能造成更大的破坏。总之，应用层攻击易于实施，但难以减缓或阻止，而且特定于某个目标。

为了解应用层 DDoS 攻击如何对我们企业产生特别影响，我们需要了解所有类型的 DDoS 攻击如何影响我们。我们可以把 DDoS 攻击类型比做举办一场聚会时可能面临的危机。例如，您可能会邀请几个客人来家中举办庆祝活动或欢度周末。但是，可能会出现以下几个场景：

DDoS 攻击类型

场景 1
容量耗尽攻击

您的客人在听到您要聚会的消息后感到非常兴奋，因此对外（或许是在社交媒体上）分享了太多信息。此次聚会的消息不胫而走，大家都觉得您的聚会不容错过，所以在聚会当天，来了许多陌生面孔。这就是容量耗尽 DDoS 攻击，因为您所有的资源都被不请自来的人消耗掉了。

场景 2
协议攻击

有一位您特别信任的客人没有保住秘密！想被邀请参加您聚会（却没有受到邀请）的人，对您的某位客人软磨硬泡，以期探知聚会活动的细节内容。这位客人最终妥协了，于是一群不请自来的人闯入了您的聚会。这就是协议 DDoS 攻击，因为本应为您的聚会保守秘密的人却没有做到。

场景 3
应用程序攻击

一个心怀不轨的人听说您要举办聚会，所以决定伪装成受邀参加聚会的客人来到您的家中，并计划实施盗窃或抢劫活动。这就是应用程序 DDoS 攻击，因为此人伪装成了经身份验证的客人。

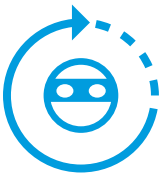
在所有这些场景中，都有一个共同漏洞，即您因聚会活动而打开了家门。这是应用层 DDoS 攻击可以利用且无法避免的漏洞，因为企业就在这一层与用户进行交互。此外，由于这一层直接服务用户，您对该层的控制力较弱，因此应用层 DDoS 攻击更加难以抵御。

另外，如果出现任何问题，都将让您付出额外的代价。无论是为更多的食物和饮料买单，被陌生人发现您的个人信息，还是致使您家中遭袭，聚会一旦出现问题，都会造成不菲的代价。

许多安全解决方案愈加注重防范应用层 DDoS 攻击，保护您的系统、资源以及敏感信息不受此类攻击的侵扰。应用层 DDoS 攻击现已越发常见，而且防范难度居高不下。您信任这些解决方案会保护您提供的服务。因此，归根究底，您的 DDoS 防护效果取决于您使用的防护平台。让我们来了解一下寻找应用层 DDoS 防护平台时需要注意的最新变化和趋势。

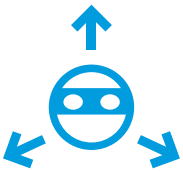
趋势和变化

一如既往，当我们针对特定攻击制定防御之道时，黑客就会调整策略以寻求破解之术。
我们一直在监测这种竞争，以下为我们目前观察到的四种趋势和变化：



1. 转向重复的短时攻击

对于 DDoS 攻击，攻击者逐渐很少使用长时攻击，而是更加注重攻击的规模和频率。Akamai 已监测到使用 9 种以上不同攻击媒介的复杂攻击，例如 ARM、SYN 泛洪、UDP 反射（DNS、WS-Discovery 等）、HTTP 泛洪等。

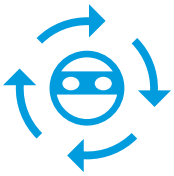


2. 更频繁地使用多媒介攻击

超过 20% 的攻击者在使用多媒介 DDoS 攻击，即将不同的 DDoS 攻击方法组合成一次短时攻击，然后在不久后再次重复。根据 Link11 的研究，同时使用的攻击媒介数量最多为 18 个，比 2021 年增加了 50%。

3. 规避检测以及后续抵御能力越来越强

攻击流量和正常流量非常难以区分，尤其是在应用层中更是如此。例如，僵尸网络会对受害人的服务器实施 HTTP 泛洪攻击。由于僵尸网络中的每个爬虫程序都能发出看似合法的网络请求，因此这种流量好像“正大光明”，并且来源可能看上去也是“规规矩矩”。



4. 先发起自动攻击，后定制攻击手段

随着云平台和 IaaS/PaaS 的普及，攻击者可轻而易举地获得自动化和计算能力，很容易发起自动攻击，并快速发起大规模攻击。因此，这些攻击不仅仅会导致容量耗尽，而且分布更广泛、更随机、设计更巧妙（在请求中使用随机化参数等）。

正如聚会场景中说明的那样，您家会受到三种方式的威胁，分别为资源消耗、不善保守秘密的客人或伪装的攻击者。伴随着应用层攻击的变化和发展趋势，可能会有很多不速之客想要瞒过“雷达”，进入您的房子。其实，在这三类场景中，为了增加隐蔽性，一切都经过精心的安排。例如，攻击者会事先踩点，看看您的房子有几个入口；提前了解聚会着装要求；或创建虚假的社交媒体个人资料来了解您的更多信息，从而骗过聚会上的所有客人，让他们以为攻击者是您的好朋友。

由于应用层 DDoS 攻击的复杂性在不断攀升，因此您最好采用比以往更全面的防护策略。过去，任何 Web 应用程序和 API 保护 (WAAP) 都能满足您的需求，甚至是内部构建的 WAAP 也不例外。如今，应用层攻击更加复杂，您的 WAAP 也需要做好应对准备。

全面的应用层 DDoS 防护方法

应用层 DDoS 攻击之所以难以检测，在于尽管多媒介攻击具有易被识别的特征，但是，处心积虑的攻击者会监测攻击响应，然后做出相应调整，以巧妙地避开意志坚定的防御者。为更连贯、更准确地化解这一挑战，您需要提高 WAAP 在检测、抵御和自助服务功能方面的能力。

毕竟，您不会希望 WAAP 只保护您家的正门。您希望它能够防御每个入口点，清楚如何识别伪装成客人的攻击者，并且在您同时面临多种攻击时能够进行扩展。好消息是：采用正确的平台可以抵御应用层 DDoS 攻击导致的危机，使您能够保持业务正常地持续运营。您的 DDoS 缓解策略必须更加全面，并侧重于以下方面：

平台的可扩展性

不论您的 WAAP 日常运行得多么出色，但如果它无法扩展以防范容量耗尽攻击，那么它将很快被攻破。正因如此，WAAP 下方的平台与 WAAP 自身一样重要。或许，您还想知道平台在何处运行。例如，Akamai 拥有遍布全球的边缘位置，通常都位于攻击的发源地。如果能够在 DDoS 攻击开始的地方加以抵御，那么阻止该攻击将变得更加容易。此外，可扩展性还能让速率限制和自定义规则等防御手段变得更加容易。

为您的防护措施提供信息的数据资源和输出

虽然任何 WAAP 都可监测流量和报告您生成的数据，但请考虑使用一种能够从全局视角汇总数据的解决方案。如果您的解决方案供应商能够监测成千上万家企业的流量，那么您生成的数据可在结合面临相同威胁的企业的背景信息下进行分析，并且能够更好地为您解决方案中的机器学习系统提供信息。然后，您自己的内部团队可获得这些数据，并用它们来为您迭代和自定义解决方案。

您解决方案的监测能力和准确性

一些检测方法（包括基于行为或异常的检测）是默认存在的，它们不仅监测传入的客户端流量，还会监测源站连接速率和服务器性能参数。但是，如果您拥有一款由强大的数据集提供信息支持的可扩展解决方案，那么您的 WAAP 将更具有针对性和准确性。另外，由于该解决方案具有自适应能力，能够发现有没有隐匿的攻击（比如隐藏在互联网开放代理后的攻击），让您可以对流量情况了如指掌。所有这一切都有助于确保正确的人获得通知，同时大幅减少误报。

因此，综上所述，如果您要筹办一场不会人满为患的聚会，您会希望自己的房子足够大（可扩展性），能够容纳可能不请自来的客人。您会希望从其他拥有糟糕聚会经验的人（数据资源）那里取取经，这样您便可提前了解您应该采取哪些防护措施。此外，您还会想要提前共享宾客名单，迎接每位客人进入房子（监测能力和准确性），从而确保每个人都安全可靠。

如果您不想亲自完成所有这些工作，您可雇佣值得信赖的增援人员来为您完成这些任务。托管服务可监测您为了区分普通客人与心怀不轨的客人而不得不高度关注的所有信号。此外，您还卸下了压力，不必再将员工的时间和专业知识专门用来全天候防范攻击，尤其是这种越发常见但却难以检测的攻击类型。

一谈到应用层 DDoS，往往就会提到应用层中与生俱来的变数和漏洞。这一话题至关重要，因为应用层 DDoS 攻击可能给企业造成极大的破坏。但是，应对这类攻击的防御措施却不必复杂或繁琐。只需一款具有策略性、可扩展性的数据驱动型解决方案，您便可轻松举办聚会。

详细了解 Akamai 如何通过第 7 层 DDoS 防护为您提供支持。