Akamai

白皮书

有关 DDoS 防御的 9 大误区

近两年来，分布式拒绝服务 (DDoS) 攻击规模翻了一番，攻击媒介的数量和组合也显著增加。2020 年，曾有企业遭遇过每秒 8.09 亿个数据包 (Mpps) 的攻击，这一事件成为有史以来规模最大的一次 PPS 攻击。尽管有些企业可能自认为遭到 DDoS 攻击的风险较低，但各行各业的关键业务服务和应用程序都会形成大量目标，如果基础架构得不到保护，所有业务都将面临停机和性能下降的风险。

企业必须将 DDoS 防护视为整体安全战略的关键要素，因此，了解相关误区对企业 DDoS 防御态势而言至关重要。

有关 DDoS 防护的观念存在很多误区，其中一些甚至源自安全供应商的鼓吹。

误区 1：总容量代表着可用的缓解资源

单看一个网络容量数据，往往会忽略掉重要细节。需回答的问题包括：有多少网络容量专门耗用在攻击流量方面？又有多少缓解系统资源专用于阻止攻击？有多少网络和系统资源可用于向该平台上的所有客户群传送安全流量？容量不仅仅局限于技术层面。从某种程度上说，如果技术无法有效发挥作用或优化缓解措施，那在升级、处理事件响应和微调缓解措施方面，还能求助于哪些专业人力资源？

提示：深入了解各提供商之间网络总容量和平台稳定性、可用于缓解攻击的容量以及安全流量交付利用率之间的差异。

误区 2：所有缓解时间 SLA 都是一样的

缓解时间意味着停止或阻止恶意流量的响应速度，且不会对合法流量和用户造成影响。单从时间上看，这存在很大的解读空间。例如，某些供应商可能要到流量持续激增 5 分钟以上，才会将其视为 DDoS 攻击行为。因此，SLA 计时器可能要到攻击开始 5 分钟后才会启动。这就意味着，广告中所说的 10 秒缓解时间实际上可能为 5 分钟或更长时间。其他一些供应商则将缓解时间定义为部署缓解措施规则所需的响应速度。归根到底，用户关心的是使面向互联网的资产恢复正常运行所需的时间。请务必仔细阅读供应商 SLA 的详细说明。

提示：深入研究 SLA 中所列缓解措施的时间细节。具体算法应如下所示：检测到攻击的时间 + 施行缓解管控措施的时间 + 阻止攻击的时间 + 缓解措施的效果 = 停止攻击的真实时间。

误区 3：吸入黑洞和速率限制都是可以接受的防御措施

吸入黑洞是一些 DDoS 缓解服务提供商常采取的防御措施。如有某项资产受到攻击并使其他客户面临风险，提供商可能会尝试通过将该资源的流量丢到虚拟黑洞中来防止继发损失。但这真的有用吗？从攻击者角度来看，吸入黑洞意味着任务完成，即致使目标资产有效离线。视提供商的基础架构而定，其他客户可能最终也会离线或遭遇到性能下降。作为另一种响应措施，许多提供商还将限制客户流量作为共享环境中的一种对策。但为了让客户感觉到资产或服务仍在运行而减少 20%-40% 的合法流量，这对遭受攻击的客户来说并非一种成功的局面。

提示：询问提供商平时或在受到攻击时，多久会发生一次吸入黑洞或速率限制流量的情况。弄清楚在何种情况下，提供商会屏蔽流量，以及需要满足哪些条件，您的服务才能得以恢复。

误区 4：跟谁共享云平台并不重要

所有企业都需要安全保障。即便是经常受到攻击的争议型企业（如赌博和色情网站等灰色产业）也需要安全防御。甚至某些推动犯罪活动和恐怖袭击的组织也从合法云供应商处购买了网络安全方案。很容易就认为这对您来说不重要。但如果您的企业与非法企业或经常受到攻击的企业共享云安全平台，则遭遇间接损害的可能性会大大提高。供应商的资源可能已被占用或不堪重负，致使您的企业面临风险。

如果您的企业与非法或经常受到攻击的企业共享云安全平台，遭遇间接损害的可能性会大大提高。

提示：仔细研读云安全供应商可接受的使用政策，确保您不会跟高风险目标共享安全平台资源。

误区 5：一体式安全平台 = 更好的安全体验

部分提供商通过单一云平台提供多种服务，这可能意味着就短期而言，能够降低部署和集成安全管控措施的技术复杂性。但共享同一后端基础架构和网络的多种服务，在环境的其他部分遭遇中断时，很容易受到平台中断、间接损害和恢复能力问题的影响。通常，由于设计单一平台法所存在的局限性，一站式供应商会选择某些功能折中措施。专门构建的 CDN、DNS 和 DDoS 净化云方案采用透明网络，旨在应对特定技术和安全挑战，也意味着能提供更高品质的缓解措施及大规模性能改善，进而优化防御态势。

提示：请记住，不必共享同一基础架构来实现一致化的安全体验。不同底层架构可以提供无缝的用户体验以及高水平的缓解措施。

误区 6：本地解决方案能提供更多管控措施

虽然本地解决方案能让企业通过自行调节的方式来管控风险，但其实这有点不太实际。对任何本地解决方案来说，最薄弱环节往往在于互联网链路的规模。随着 DDoS 攻击日渐强大并复杂化（多种媒介），即便是 4 Gbps 以下的典型攻击也会致使互联网链路饱和，甚至导致配备上乘内部硬件的数据中心发生拒绝服务的情况。对于本地部署方案，用户基本上需要好几分钟时间才能将严重攻击缓解措施转移到云端。由于安全人才稀缺而且不堪重负，各大企业都选择将 DDoS 缓解措施外包给基于云的平台，而不是开发内部 DDoS 防御专业技术。

提示：一旦网络、IT、事件响应人员不堪重负，后果将无法控制。DDoS 是一种应由防御专家来处理的攻击类型。术业有专攻，专心干正事，其他的外包给专家。

误区 7：您无需多层防御措施

大多数企业并不真的相信这一点，一旦深信这一点，有时甚至还会自建防御策略。例如，考虑采用混合防御法。对希望增强本地部署安全解决方案的企业来说，可通过添加来自同一供应商的云解决方案进行升级。一站式购物可能很方便，但不一定能提供深度防御措施。这是因为，如果多层防御措施都构建于同一种底层技术上，则所有防御层将具有相同的漏洞和弱点，同样会致使您的企业面临风险。

提示：根据不同优势及劣势，对同类最佳技术进行分层，因而某一层存在的缺陷可被另一层防御所弥补。

误区 8：所有 SOC 提供的支持等级都相同

众多供应商的数据表上均宣称提供安全操作中心 (SOC) 支持服务。但拥有一个全天候的 SOC 并不是最重要的。最重要的是，当您的资产受到攻击时，您能够享受到所期望的专业服务。在评估 DDoS 防御提供商时，要考虑的一些关键因素包括：在遭到攻击之前、攻击期间和攻击之后，您能得到哪类支持和分析服务？SOC 如何配备人员以确保防御的连续性？在您联系 SOC 时，您联系的是能进行缓解操作的实际分析人员，还是仅提供问题升级的对接人？提供商是否有接受了防御培训的安全专业人员，还是只有将流量路由到现成缓解设备的流量操作人员？对方是否提供定制化的行动手册？安全提供商的 SOC 应作为企业事件响应团队的有效扩充，从而实现其真正的价值。

提示：对您将从服务提供商 SOC 获得的预期支持服务品质进行评估。除了提供攻击检测和缓解措施之外，确定对方是否还提供集成和测试、事件故障排除、事后分析（经验教训总结）和设计支持，从而帮助您缩小攻击层面。

误区 9：DDoS 防护包罗万象

低价虽然看起来很有吸引力，但可能会导致一些隐性成本。某些供应商的报价很低，但对其能够防御的攻击数量或规模会有所限制。一旦您遭遇过多或过大攻击，对方会要求您升级到更高（且更昂贵）的服务层才能为您终止攻击，而这时您往往一心只想恢复业务，只能任由对方安排。在对比供应商和报价时，请务必考虑好侧重点及其对您风险状况的影响。

提示：签约之前，务必弄清楚报价中包含哪些内容。

一旦您遭遇过多或过大攻击，某些供应商会要求您在攻击停止之前升级到更高（且更昂贵）的服务层，所有这些都会在您尝试使业务恢复在线时遇到。

DDoS 安全问题不仅复杂多变，而且费时费力。与客户、消费者、员工保持互联是保障业务的基础。没有犯错的余地，也没有必要独自承担试错造成的高昂成本。作为最大、最值得信赖的网络安全云交付平台，Akamai 可随时为您提供帮助。请访问 www.akamai.com/secureapps 以了解详情。

Akamai

Akamai 为全球的大型企业提供安全的数字化体验。Akamai 的智能边缘平台涵盖了从企业到云端的一切，从而确保客户及其公司获得快速、智能且安全的体验。全球优秀品牌依靠 Akamai 敏捷的解决方案扩展其多云架构的功能，从而获得竞争优势。Akamai 使决策、应用程序和体验更贴近用户，帮助用户远离攻击和威胁。Akamai 一系列的边缘安全、Web 和移动性能、企业访问和视频交付解决方案均由优质客户服务、分析和全天候监控提供支持。如需了解全球顶级品牌信赖 Akamai 的原因，请访问 www.akamai.com 或 blogs.akamai.com，或者扫描下方二维码，关注我们的微信公众号。您可访问 www.akamai.com/locations 查找全球联系信息。发布时间：2020 年 12 月。

扫码关注，获取最新CDN前沿资讯