Microsoft

云服务中的 DDoS 防御策略

Microsoft Azure 由世纪互联运营

Office 365 由世纪互联运营

发布时间：2015 年 2 月

序言

微软作为一个具有显著互联网影响力和众多杰出互联网资产的全球性组织，基于微软技术的服务是黑客们和其他怀有恶意的个人重要的攻击目标。事实上，在过去的几年里，基于微软技术的服务一直持续地受到各种形式的网络攻击。几乎在任何时间，用于这些服务的网络资产都在面临着某种形式的拒绝服务（DoS）攻击。如果没有可靠和持久的缓解系统可以抵御这些攻击，这些服务将处于脱机状态。

基于微软技术由世纪互联运营的 Microsoft Azure 和 Office 365 采用了防御纵深安全策略，来抵御内部和外部的风险。客户端与 Azure 和 Office 365 之间的通信层——网络，是恶意攻击的最大目标之一。

本文介绍了不同类型的 DDoS 攻击，使用微软技术如何保护由世纪互联运营的 Microsoft Azure 和 Office 365 及其网络免受攻击。

DDoS 攻击的定义和特征

攻击网络服务的一种方式是，向某个服务的主机创建发起大量请求，使网络和服务器过载，继而拒绝合法用户的请求。这被称为一个拒绝服务（DoS）攻击。当这种攻击由多个主体和载体发起时，就被称之为分布式拒绝服务（DDoS）攻击。

虽然攻击的方式、动机和攻击目标可能会有所不同，DDoS 攻击通常由一人或多人协作发起，为了暂时或永久中断某个网站或服务的正常运行。

美国计算机应急准备小组（US-CERT）定义的 DDoS 攻击的特征包括：

- 异常缓慢的网络性能（打开文件或访问互联网网站时）
- 特定网站的不可用
- 无法访问特定网站
- 收到的垃圾邮件数量剧增
- 无线或有线网络无法连接
- 长时间的无法访问网络或任何互联网服务

DDoS 攻击的概述

DDoS 攻击主要表现为五种方式：

- 字节/秒攻击（bps）
- 包/秒攻击（pps）
- 交易/秒攻击（tps）
- 连接/秒攻击（cps）
- 最大并发连接攻击（mcc）

字节/秒攻击

原理上讲，字节/秒攻击是指发送超过网络可处理的数据。这种攻击侧重于基于数据包大小的网络饱和度上，而非网络数据传输率。其目的在于占用大量网络带宽资源，从而使之丢包。基本上，攻击者会企图占满两台设备间已明确带宽的固定链路。恶意流量会消耗掉大量可用带宽，以至于合法的用户请求无法通过已饱和的链路上传送。实际传输的载荷通常是随机的且不相关的。举例来说，一种典型的攻击方式是对网络时间协议（NTP）反射的利用。网络时间协议反射攻击，攻击者会用伪造的 IP 地址（被攻击者的 IP）发送少量数据到 NTP 服务器。作为对该 IP 请求的回应，NTP 服务器会发送大量反馈数据，继而使被攻击者的网络瘫痪。

包/秒攻击

这种攻击利用了一个简单的事实：并非所有的数据包生而同等大小。这种攻击侧重于使用过量的数据包而非数据引起网络饱和。处理数据包需要消耗一定的资源，与数据包的大小无关。一个既定网络的带宽能够承受一定大小的数据包流量（例如，1500 字节大小的数据包），一旦达到包/秒上限，即使非常快的网络和网络设备也会被拖慢。较小数据包（例如，64 字节）也可能会导致带宽最大性能急剧下降。

尽管不是制造大量流量来导致网络或设备瘫痪，攻击者却选择了发送大量小数据包，从而延长处理数据包所需的时间，最终拖慢整个网络。用户数据报协议（UDP）洪水攻击是进行这种类型攻击的典型方法。

交易/秒方式的攻击

这种类型攻击通常是前面提到的字节/秒攻击和包/秒攻击无效之后设计出的针对目标机器的攻击方式。攻击者将对目标机器正在运行的服务进行分析，然后尝试执行针对该服务的组件的交易，以测试其响应速度。攻击者试图找出哪些交易具有更长的响应时间，因为这会表明该服务正在执行更多的工作，和消耗更多的资源来响应此类交易请求。如果攻击者对目标机器的架构有很好的理解，那么他们可以进一步调整攻击策略，只需很少的数据包就可以中断服务。

假设，攻击者知道执行以下任何活动时某个服务将消耗 10%的 CPU 时间：

三个并发搜索操作
七个并发登录成功
一个重新索引操作
四个并发登录失败

比如，攻击者仅仅需要发送每秒 40 个非法并发登录请求，就可消耗目标机器上的 100%CPU 时间。在字节/秒、包/秒阈值达到之前，该攻击已致使目标机器脱机。

通常在实施此类攻击之前会有很多嗅探行为，并且这些嗅探行为是由僵尸程序（在互联网上自动执行任务的一类软件程序）执行。基于微软多年在网络空间攻防经验的积累，微软已经能够发现大量僵尸程序，同时建立已知僵尸程序和被感染的 IP 地址的庞大数据库。我们使用 Azure 活动目录优质服务（Azure Active Directory Premium）与客户分享信息，以便他们进行鉴证关联和分析。

连接/秒方式的攻击

这种攻击方式使用高连接需求策略，旨在降低维护“状态与连接列表”的设备的整体容量。这种攻击的目的在于持续建立大量请求，直至“状态与连接列表”处于撑满状态，而不能处理合法的连接请求。一种典型的攻击方法是 SYN 洪水攻击，其中攻击者发送一系列的 SYN 请求撑满列表。SYN 认证是用来防范 SYN 洪水攻击的一个常见和经济的保护机制。

最大并发连接攻击

与连接/秒攻击相同，此种攻击的目标也是针对维护“状态与请求列表”的设备。但是，不同于连接/秒方式的攻击关注新连接率，最大并行连接攻击关注于连接的数量，攻击者常常缓慢地制造这些连接，以避免检测，然后尽可能使它们保持开启状态。 Slowloris 是进行此类攻击的一种典型的黑客工具。

DDoS 防御的核心原则

防御 DDoS 攻击时有三个核心原则：

1. 吸收
2. 检测
3. 缓解

吸收应在检测之前，而检测应在缓解之前。吸收是针对 DDoS 攻击的唯一可靠的防御手段。攻击如果无法被检测到，就不能被缓解。而如果最小量级的 DDoS 攻击也不能被吸收的话，那么，服务无法存活到 DDos 被检测到。

当然，过度扩容用于吸收 DDoS 攻击的能力，对于组织来说这在经济上往往是不可行的。因此，必须在吸收、检测和缓解之间寻找一种平衡。为了找到这种平衡，就必须了解攻击的增长速率，这样就可以估算您需要拓展多少吸收能力。

检测是一场猫鼠游戏。您必须查明不断涌现出的攻击您或试图击垮您的系统的黑客手法。检测->缓解->检测->缓解，循环往复，这是一个永久的、持续的状态，将无限期地继续。

防御 DDoS 攻击

DDoS 攻击与容量和时间相关，这里有可用于确定 DDoS 影响的公式：

最大容量/（最大容量 x 攻击增长率）=冲击时间

如果检测时间长于冲击时间，那么，DDoS 攻击很可能是成功的。如果检测时间短于冲击时间，那么，正在被攻击的服务应该保持在线和可用的，但前提是，采用缓解策略。

因此，实际上用来抵御 DDoS 攻击只有两件事可以做：

1. 增加容量，提高最大容量的上限（提供了更多的时间来检测攻击）；或者

2. 减少检测时间。

提高容量有着直接的财务影响。我们确实建议客户要增加他们的容量，至少具备某些吸收攻击的能力。客户增加容量的多少因其脆弱点、风险、能力等因素而有所不同。最终，从经济角度来考虑，最具成本效益的防御方式是投入研究如何减少检验时间。

基于微软技术的 DDoS 防御策略

世纪互联使用的是基于微软技术的 DDoS 防御策略，而微软的规模和全球足迹造就了微软的 DDoS 攻击防御策略的独特性。微软技术能够做的事情，许多其他供应商无法做到，而且大多数（如果不是全部）非云平台企业都无法做到。我们的 DDoS 战略的基石是借力于微软技术的全球影响力。微软与来自世界各地的互联网服务提供商、对等伙伴（上市和私营）、和私人公司一起合作，从而产生一个巨大的互联网影响力，使得微软技术能够在较大范围内抵御 DDoS 攻击。

鉴于这种独特性，微软技术采用的检测和缓解流程与许多大企业沿用的传统方法有所不同。世纪互联的策略是基于微软技术和策略，在多个边界将检测与缓解分离，将全局缓解与分布式缓解分离。许多企业采用的第三方解决方案：在边界进行检测和缓解策略。随着我们的边界容量的增长，对个人或特定边界的任何攻击显然意义不大。由于微软技术的独特配置所致，

我们已经分离了检测和缓解组件。我们已经部署了多层次的检测，使我们能够更接近饱和点检测到攻击，同时保持边界的全局缓解。这种策略保证了世纪互联能够同时处理多个攻击。

微软技术采用应对 DDoS 攻击的最有效和低成本的防御方法是减少攻击面。这样做可以使世纪互联在边界削减不受欢迎的流量，而不是串联式的分析、处理和清洗数据。

微软还自行开发了一个使用流量数据、性能指标及其它信息的内部 DDoS 关联和检测系统。这是在由世纪互联运营的 Microsoft Azure 中运行的一个云规模的服务，该服务对来源于微软网络和服务的不同点收集到的数据进行分析。另外，世纪互联还拥有完备而迅捷的 DDoS 快速响应机制和成熟的团队建设，多个团队紧密配合，保证了第一时间发现，第一时间处理，第一时间反馈。并且，由世纪互联运营的 Office 365 的工作负载配置了基于以独特方式保护相关工作负载的协议以及带宽使用量的优化阈值。

Azure 平台 DDos 防御

为了保护 Azure 平台服务，由世纪互联运营的 Microsoft Azure 提供了分布式拒绝服务（DDoS）防御系统，该系统已成为 Azure 持续监控流程的一部分，并会通过渗透实验进行持续的改进。

按照设计，由世纪互联运营的 Microsoft Azure 的 DDoS 防御系统不仅可以承受来自外部的攻击，而且可以防御来自其他 Azure 租户的攻击：

1. 网络层高容量攻击。这些攻击会用数据包堵塞整个网络，耗尽网络线路和数据包处理容量。Azure DDoS 防御技术具备 SYN cookie、速率限制，以及连接限制等检测和减缓技术，可确保此类攻击不会对客户环境造成影响。

2. 应用程序层攻击。这些攻击可针对客户的虚拟机发起。Azure 没有提供能够减缓或主动阻止影响特定客户部署的网络通讯的机制，因为基础架构无法判断对于客户的应用程序来说，哪些行为是合理的。在这种情况下，与 on-premises 环境类似，可考虑下列减缓措施：
   - 在负载平衡的公共 IP 地址之后运行多个虚拟机 instance。
   - 使用防火墙代理设备终止通讯，或将通讯转发至虚拟机的 endpoints。这种方式可防范一系列 DoS 和其他攻击，例如低速率、HTTP，以及其他应用程序层威胁。此外可使用一些虚拟化解决方案执行入侵检测和预防操作。
   - 保护防范某种类型 DoS 攻击的 Web 服务器加载项。
   - 网络 ACL，可防止来自某些 IP 地址的数据包到达虚拟机。

Office 365 应用层防御 DDoS 攻击

由世纪互联运营的 Office 365 服务在网络层享受和 Azure 同等的分布式拒绝服务（DDoS）防御系统的同时，通过实现一种向外扩展的系统框架，Office 365 被设计成支持高负荷工作

模式，从而支持保护和缓解应用层面的 DDoS 攻击。而在这系统框架下，服务通过在多个区域隔离的数据中心和某些工作负载中的节流功能进行分布实施的。

由世纪互联运营的 Office 365 服务位于两个分属于不同城市的数据中心里。通过主/备份方式，客户数据被复制到冗余的数据中心。主数据中心就是运行应用软件以及软件中运行的客户数据所在的位置。备份数据中心是用于故障切换。如果主数据中心出于任何原因而不再正常运行，应用软件和软件中运行的客户数据在备用数据中心依然可以获取的。在任意时间，客户数据不是在主数据中心就是在备用数据中心进行处理。一旦某个数据中心被攻击，数据多个中心分布机制会减少了被攻击面。此外，作为一种恢复机制，服务可快速从受影响的数据中心切换到备份数据中心。

Exchange Online 和 SharePoint Online 中的节流机制 ,也是抵御 DDoS 攻击的一种重要工具。用户的“Exchange 服务”节流机制是基于某用户所消耗的活动目录（Active Directory）、Exchange 服务储存以及其他资源的数量。每个客户端都分配一个预算，限制特定用户消耗的资源。针对用户活动和系统组件的“Exchange 服务”节流机制是基于工作负载管理的。“Exchange 服务”的工作负载可能是指某个“Exchange 服务”功能、协议、或是为了 Exchange 系统资源管理的目的而明确定义了的服务。每个“Exchange 服务”的工作负载消耗系统资源，如 CPU、邮箱数据库操作、或用以运行用户请求或后台工作的活动目录（Active Directory）请求。 “Exchange 服务”工作负载的例子包括 Outlook Web App、Exchange ActiveSync、邮箱迁移和邮箱助理等。租户管理员可以通过 Exchange Management Shell 管理用户的“Exchange 服务”工作负载节流设置。应用于“Exchange Online 服务”中的节流机制有多种形式，包括 PowerShell、Exchange Web Services、以及 POP 和 IMAP、Exchange ActiveSync、移动设备连接、收件人等等。虽然本地“Exchange 服务”部署中可以配置节流策略，但是，管理员无法配置“Exchange Online 服务”的节流策略。

“SharePoint Online 服务”中实施节流的最典型的原因是高频率执行太多动作的“客户端对象模型”（CSOM）编程规则。因为 CSOM 机制，许多动作都可以通过单个请求实施，可能导致超过使用限制，并按用户逐个节流。

- 不考虑可能导致节流的活动，当用户超过使用限制时，“SharePoint Online 服务”通常会短时间内节流该用户帐户发出的任何进一步的请求。当节流生效时，该用户的所有操作都遭到节流，直到这个节流失效为止：对于用户直接在浏览器执行的请求，“SharePoint Online 服务”重定向至一个提示节流信息的页面：请求失败。

- 对于所有其他请求，包括 CSOM 调用，“SharePoint Online 服务”返回 HTTP 状态代码 429（“太多请求”）：请求失败。

如果这些进程继续超过使用限制，那么，“SharePoint Online 服务”可能会完全阻断该进程并返回 HTTP 状态代码 503（“服务不可用”）。

总结

由世纪互联运营的 Microsoft Azure 和 Office 365 服务是特别设计构建成 :可支持非常高负荷工作模式，并通过实施节流、一个向外扩展的体系结构、区域隔离、和高性能组件来保护和缓解应用层 DDoS 攻击的。为了保护 Office 365 ,世纪互联给予 Office 365 内置了应用层 DDoS 防护机制。同时，在网络层和传输层的 DDoS 防护方面，实施了一种基于 Microsoft Azure 的 DDoS 解决方案。

世纪互联认为：我们总会受到攻击，并且我们将永远无法阻止所有的攻击，面对 DDoS 攻击是从事在线服务业务内容的一部分。世纪互联将继续利用微软技术在 DDoS 检测与缓解策略方面的研究成果。鉴于微软技术的独特性，我们能够使用有别于其他大型企业的传统检测和缓解政策，而采用了基于吸收在检测和缓解之前的策略。

微软技术的策略实施的基石是：利用全球影响力，实施分布式服务。微软技术拥有显著的互联网影响力，并且该影响力每 18 个月左右增长一倍。利用微软技术这样一个庞大的影响力，使得世纪互联能够在较大范围内抵御 DDoS 攻击。