AWS分布式拒绝服务弹性最佳实践

2018年6月

注意事项

本文档仅供参考。它表示截至本文档发布之日止，AWS当前提供的产品和实践，如有更改，恕不另行通知。客户有责任对本文档中的信息以及对AWS产品或服务的任何使用进行独立评估，每种产品或服务均按“原样”提供，无任何形式的明示或暗示保证。本文档不提供任何由AWS，其分支机构，供应商或许可方提供的担保，陈述，合同承诺，条件或保证。职责 以及AWS对客户的负债均受AWS协议控制，且本文档不属于AWS与其客户之间的任何协议，亦不对其进行修改。

内容

摘要

本文适用于希望提高运行在亚马逊网络服务（AWS）上的应用程序的抵御分布式拒绝服务（DDoS）攻击的客户。概述了分布式拒绝服务攻击，AWS提供的功能，缓解技术以及分布式拒绝服务弹性参考架构（可用作帮助保护应用程序可用性的指南）。

本文面向熟悉网络，安全和AWS基本概念的IT决策者和安全工程师。每个部分都有指向AWS文档的链接，其中提供了有关最佳实践或功能的更多详细信息。

引言

您将努力保护企业免受分布式拒绝服务（DDoS）攻击以及其他网络攻击的影响。您想通过保持应用程序的可用性和响应能力来保持客户对服务的信任。而且，当基础设施必须扩展以应对攻击时，您希望避免不必要的直接成本。

AWS致力于为您提供工具，最佳实践和服务，帮助确保高可用性，安全性和弹性，抵御互联网上的不良行为。

在本白皮书中，我们为您提供规范性的分布式拒绝服务指南。我们描述了不同的攻击类型，如基础设施层攻击和应用程序层攻击，并解释了哪种最佳实践对每种攻击类型的管理最有效。我们还将概述适合分布式拒绝服务缓解策略的服务和功能，以及如何使用每种服务和应用程序保护您的应用程序。

拒绝服务攻击

拒绝服务攻击是一种故意使用户无法使用您的网站或应用程序的尝试，例如，向网络流量泛洪。为实现这一点，攻击者使用各种技术消耗大量网络带宽或占用其他系统资源，破坏合法用户的访问。最简单的形式是，孤独攻击者使用单一来源对目标执行拒绝服务攻击，如下图所示（图1）。

图1：DOS攻击图

但是，在分布式拒绝服务（DDoS）攻击中，攻击者使用多个来源（可能是感染了恶意软件的计算机，路由器，IoT设备和其他端点的分布式组）编排针对目标的攻击。如下图分布式拒绝服务攻击图（图2）所示，受感染主机网络参与攻击，生成大量数据包或请求使目标不堪重负。

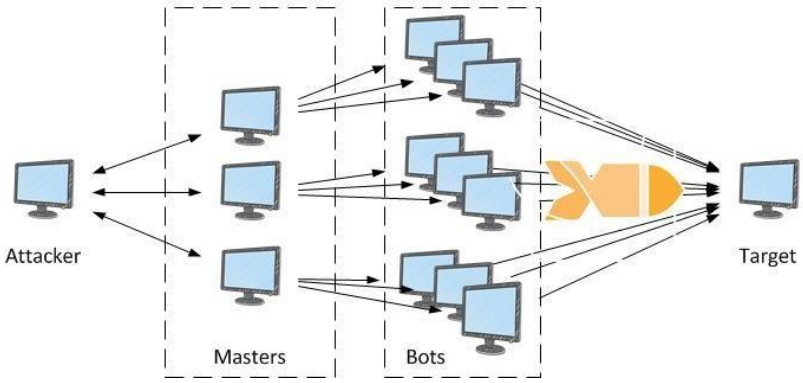

图2：分布式拒绝服务攻击示意图

分布式拒绝服务攻击最常见于开放系统互连（OSI）模型的第3、4、6和7层，如表1所示。第3层和第4层攻击分别对应于OSI模型的网络层和传输层。我们将这些统称为基础设施层攻击。第6层和第7层攻击对应于Presentation和

OSI模型的应用程序层。我们将它们作为应用程序层攻击一起解决。我们将在下一部分中介绍这些攻击类型的示例。

#	层数	单位	内容描述	向量示例
7	应用程序	数据	网络流程到应用程序	HTTP洪水，域名系统查询洪水
6	简报	数据	数据表示和加密	TLS滥用
5	会话	数据	主机间通信	不适用
4	交通运输	细分	端到端连接和可靠性	SYN洪水
3	网络	数据包	路径确定和逻辑寻址	UDP反射攻击
2	数据链接	框架	物理寻址	不适用
1	物理的	比特	媒体，信号和二进制传输	不适用

表1：开放系统互连（OSI）模型。

基础设施层攻击

最常见的分布式拒绝服务攻击（UDP反射攻击和SYN泛洪）是基础设施层攻击。攻击者可以使用这两种方法来生成大量流量，这些流量可能淹没网络容量或占用服务器，防火墙，IPS或负载平衡器等系统上的资源。尽管可以轻松识别这些攻击，但要有效缓解，则必须拥有比入站流量泛洪更快地扩展容量的网络或系统。这种额外的容量可以过滤或吸收攻击流量，使系统和应用程序能够对合法客户流量做出响应。

UDP反射攻击

UDP反射攻击利用了UDP是无状态协议这一事实。攻击者可以制作一个有效的UDP请求数据包，列出攻击目标的IP作为UDP源IP地址。攻击者现在已经篡改或“欺骗”了UDP请求数据包的源IP。然后，攻击者将包含欺骗源IP的UDP数据包发送到中间服务器。服务器被欺骗将UDP响应数据包发送到目标受害者IP，而不是返回到

攻击者的IP地址。使用中间服务器是因为中间服务器生成的响应是请求数据包的几倍，有效放大了发送到目标IP地址的攻击流量。

放大因子，即响应大小与请求大小的比率，根据攻击者使用的协议（DNS，NTP或SSDP）而变化。例如，域名系统（DNS）的放大倍数可以是原始字节数的28到54倍。因此，如果攻击者向域名系统（DNS）服务器发送64字节的请求有效载荷，他们会向攻击目标生成3400字节的有害流量。下图说明了反射策略和放大效果（图3）。

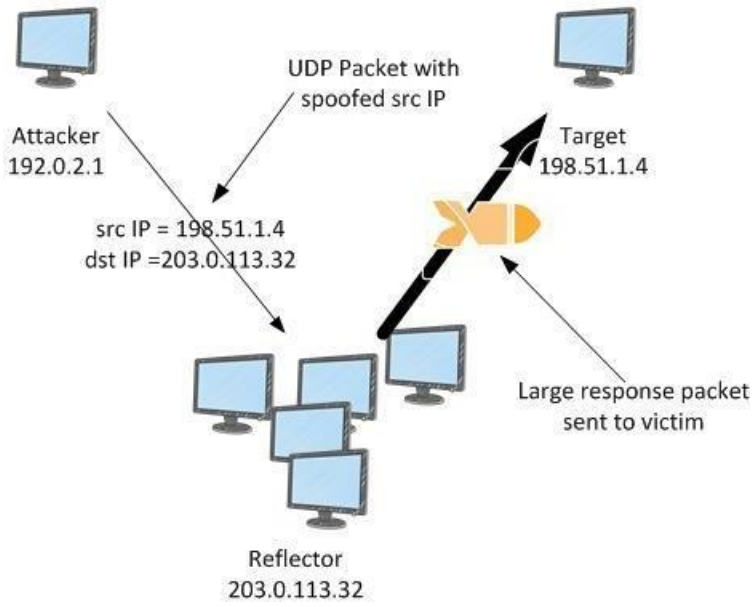

图3：UDP反射攻击

SYN泛洪攻击

当用户连接到TCP服务（如网络服务器）时，客户端发送SYN（同步）数据包。服务器返回一个确认的SYN-ACK数据包，最后，客户端以一个ACK数据包响应，完成了预期的三次握手。下图说明了这种典型的握手（图4）：

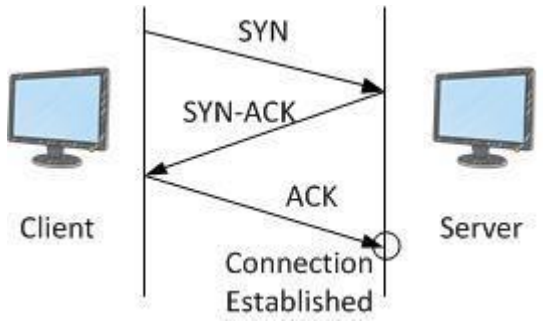

图4：SYN 3次握手

在SYN泛洪攻击中，恶意客户端发送大量SYN数据包，但从不发送最终ACK数据包完成握手。服务器处于等待状态，以等待对半开的TCP连接的响应，最终容量不足，无法接受新的TCP连接。这样可以防止新用户连接到服务器。 SYN泛洪可能高达100s Gbps，但攻击的目标不是SYN流量，而是捆绑可用的服务器连接，导致没有合法连接资源。

应用程序层攻击

攻击者可以使用第7层攻击或应用程序层攻击将应用程序自身作为目标。在这些攻击中，类似于SYN泛洪基础设施攻击，攻击者试图使应用程序的特定功能超载，以使应用程序无法使用或对合法用户极为不响应。有时，这可以通过非常低的请求量（仅产生少量网络流量）来实现。这会使攻击难以检测和缓解。应用程序层攻击的例子包括HTTP洪水，缓存清除攻击和WordPress XML-RPC洪水。

在HTTP泛洪攻击中，攻击者发送的HTTP请求似乎来自网络应用程序的真实用户。一些HTTP泛洪针对特定资源，而更复杂的HTTP泛洪试图模仿人类与应用程序的交互。这会增加使用常见缓解技术（如请求速率限制）的难度。

缓存清除攻击是一种HTTP洪水攻击，使用查询字符串中的变体规避内容分发网络（CDN）缓存。 CDN不能返回缓存的结果，而必须为每个页面请求与原始服务器联系，并且这些原始提取会对应用程序网络服务器造成额外压力。

借助WordPress XML-RPC泛洪攻击（也称为WordPress pingback泛洪），攻击者滥用WordPress内容管理软件上托管的网站的XML-RPC API函数，生成大量HTTP请求。借助pingback功能，托管在WordPress（站点A）上的网站可以通知其他WordPress站点（站点B）站点A已创建到站点B的链接。然后，站点B尝试获取站点A验证链接是否存在。在pingback泛洪攻击中，攻击者滥用此能力导致站点B攻击站点A。这种类型的攻击有一个清晰的签名：“ WordPress”通常出现在HTTP请求标头的“用户代理”中。

此外，还有其他形式的恶意流量会影响应用程序的可用性。
Scraper机器人自动执行访问网络应用程序的尝试，以窃取内容或记录竞争性信息，如定价。暴力破解和凭证填充攻击是经过编程的努力，旨在获得对应用程序安全区域的未授权访问。这些并不是严格的分布式拒绝服务攻击；但它们的自动化特性看起来类似于分布式拒绝服务攻击，可以通过实施一些相同的最佳实践（在本文稍后部分介绍）来缓解。

应用程序层攻击也可以针对域名系统（DNS）服务。在这些攻击中，最常见的是域名系统（DNS）查询泛洪，攻击者使用许多格式良好的域名系统（DNS）查询耗尽域名系统（DNS）服务器的资源。这些攻击还可能包括缓存清除组件，攻击者在其中随机分配子域字符串，以绕过任何给定解析器的本地域名系统（DNS）缓存。因此，解析器无法利用缓存的域查询，而必须反复联系权威域名系统（DNS）服务器，放大攻击。

如果网络应用程序通过TLS交付，则攻击者还可以选择攻击TLS协商过程。 TLS的计算量巨大，因此攻击者可以通过发送难以理解的数据来降低服务器的可用性。在这种攻击的一种不同形式中，攻击者完成TLS握手，但永久重新协商加密方法。否则，攻击者可能会通过打开和关闭许多TLS会话来试图耗尽服务器资源。

缓解技术

某些形式的分布式拒绝服务缓解自动包含在AWS服务中。您可以通过结合使用具有特定服务的AWS架构和实施其他最佳实践，进一步提高分布式拒绝服务容灾能力。

所有AWS客户均可免费获得AWS Shield Standard的自动保护。 AWS Shield Standard可以防御针对您的网站或应用程序的最常见，频繁发生的网络和传输层分布式拒绝服务攻击。所有AWS服务和每个AWS区域均提供此服务，无需支付额外费用。在AW S区域，分布式拒绝服务攻击由系统自动检测流量基线，识别异常并在必要时创建缓解措施。该缓解系统可抵御许多常见的基础设施层攻击。您可以将AWS Shield Standard用作弹性分布式拒绝服务架构的一部分，以保护网络和非网络应用程序。

此外，您可以利用从边缘位置运行的AWS服务（如Amazon CloudFront和Amazon Route 53）构建全面的可用性保护，抵御所有已知的基础设施层攻击。当您从全球边缘位置服务于网络应用程序流量时，使用这些服务（属于AWS全球边缘网络的一部分）可以提高应用程序的分布式拒绝服务弹性。

使用Amazon CloudFront和Amazon Route 53的若干具体好处包括：

- 与AWS边缘服务集成的AWS ShieldDDoS缓解系统，将缓解时间从几分钟缩短到亚秒级。
- 无状态SYN洪水缓解技术，在传入的连接传递到受保护的服务之前，代理和验证传入的连接。
- 自动流量工程系统，可以分散或隔离大容量分布式拒绝服务攻击的影响。
- 无需更改当前应用程序架构（例如，在AWS区域或本地数据中心）与AWS WAF结合使用的应用程序层防御。

AWS上的入站数据传输免费，您无需为AWS Shield缓解的分布式拒绝服务攻击流量付费。

有关包括AWS全球边缘网络服务的分布式拒绝服务弹性参考架构，请参见下图（图5）。

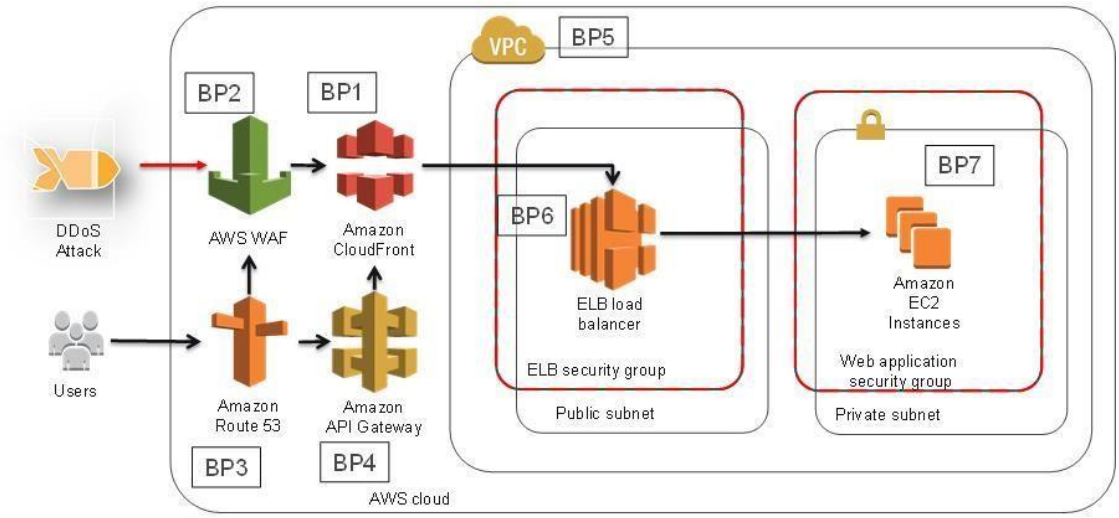

图5：分布式拒绝服务弹性参考架构。

该参考架构包括多项AWS服务，可帮助您提高网络应用程序抵御分布式拒绝服务攻击的弹性。有关这些服务及其可以提供的功能的摘要，请参见下表（表2）。我们为每个服务添加了“最佳实践指标”（BP1，BP2等）标记，以便您在阅读本文档的其余部分时可以轻松地在此再次引用它们。例如，下一节将讨论Amazon CloudFront提供的功能，并包括最佳实践指标BP1。

AWS边缘位置			AWS区域			
	亚马逊CloudFront（BP1）与AWS网络应用防火墙（BP2）	亚马逊53路（BP3）	弹性加载平衡（BP6）	亚马逊API网关（BP4）	亚马逊VPC（BP5）	亚马逊EC2自动缩放比例（BP7）
第3层（例如UDP反射）攻击缓解	✔	✔	✔	✔	✔	✔

AWS边缘位置			AWS区域		
第4层（例如SYN泛洪）攻击缓解	✔	✔	✔	✔	
第6层（例如TLS）攻击缓解	✔		✔	✔	
减少攻击面	✔	✔	✔	✔	✔
扩展以吸收应用程序层流量	✔	✔	✔	✔	✔
第7层（应用程序层）攻击缓解	✔	✔	✔（如果与AWS WAF一起使用）		
地理隔离和分散多余流量，以及更大的分布式拒绝服务攻击	✔	✔			

表2：最佳实践摘要。

订阅AWS Shield Advanced，可以提高准备响应和缓解分布式拒绝服务攻击的另一种方法。此可选的分布式拒绝服务缓解服务可帮助您保护托管在任何AWS区域或AWS外部的应用程序。该服务在全球范围内适用于Amazon CloudFront和Amazon Route53。在经典负载均衡器（CLB），应用程序负载均衡器（ALB）和弹性IP地址（EIP）的选定AWS区域中也可用。将AWS Shield Advanced与EIP结合使用，可以保护网络负载平衡器（NLB）或Amazon EC2实例。

借助AWS Shield Advanced，您还可以享受以下额外好处：

- 访问AWS DDoS响应团队（DRT）以协助缓解影响应用程序可用性的DDoS攻击。

- 分布式拒绝服务通过使用AWS管理控制台，API和Amazon CloudWatch指标和警报来攻击可见性。
- 访问全球威胁环境仪表板，该仪表板概述了AWS观察到和缓解的分布式拒绝服务攻击。
- 为减轻应用程序层分布式拒绝服务攻击（与Amazon CloudFront或ALB结合使用），免费访问AWS WAF。
- 与AWS WAF一起使用时，将自动为网络流量属性提供基准。
- 免费访问AWS Firewall Manager，用于自动策略实施。通过此服务，安全管理员可以集中控制和管理AWS WAF规则。
- 灵敏的检测阈值，与EIP结合使用时，可以将流量更早地路由到分布式拒绝服务缓解系统，并可以缩短针对Amazon EC2或NLB的缓解攻击时间。
- 成本保护，让您可以要求退款有限的分布式拒绝服务攻击造成的与扩展相关的成本。
- 增强服务水平协议，特定于AWS Shield Advanced客户。

有关AWS Shield Advanced功能的完整列表，以及更多有关AWS Shield的信息，请参阅。AWS Shield – Managed DDoS Protection

在以下各节中，我们将更深入地介绍建议的分布式拒绝服务防护最佳实践。有关为静态或动态Web应用程序构建分布式拒绝服务缓解层的快速简便实施指南，请参阅。How to Help Protect Dynamic WebApplications Against DDoS Attacks by Using Amazon CloudFront and Amazon Route 53

基础设施层防御（BP1，BP3，BP6，BP7）

在传统的数据中心环境中，可以使用超额配置容量，部署分布式拒绝服务缓解系统或借助分布式拒绝服务缓解服务清理流量等技术来缓解基础设施层分布式拒绝服务攻击。在AWS上，会自动提供分布式拒绝服务缓解功能-但您可以通过选择最能利用这些功能的架构选择来优化应用程序的分布式拒绝服务弹性，并允许您扩展以应对多余流量。

帮助缓解容量分布式拒绝服务攻击的关键考虑因素包括确保有足够的传输能力和多样性，以及保护您的AWS资源（如Amazon EC2实例）免受攻击流量。

实例大小（BP7）

Amazon EC2提供可调整大小的计算容量，因此您可以根据需求变化快速扩展或缩小规模。您可以通过向应用程序中添加实例来水平扩展，也可以使用更大的实例垂直扩展。某些Amazon EC2实例类型支持可以更轻松地处理大量流量的功能，例如25个千兆位网络接口和增强型网络。借助25个千兆位网络接口，每个实例可以支持更大量的流量。这有助于防止到达Amazon EC2实例的流量发生接口拥塞。

与传统实现相比，支持增强网络的实例可提供更高的IO性能和更低的CPU利用率。这样可以提高实例处理具有更大数据包量的流量的能力。

25千兆位功能可用于最大规模的实例，例如M4。要了解有关支持25个千兆位网络接口和增强网络的Amazon EC2实例的更多信息，请参阅。要了解如何启用增强网络，请参阅。Amazon EC2 Instance TypesEnabling Enhanced Networking on Linux Instances in a VPC

选择区域（BP7）

AWS服务可在全球多个地方使用。这些地理上分开的区域称为区域。设计应用程序架构时，可以根据需要选择一个或多个区域。常见的考虑因素包括性能，成本和数据主权。在每个区域，AWS均提供对一组独特的互联网连接和对等关系的访问权限，为这些区域的用户提供最佳延迟和吞吐量。

在为应用程序选择区域时，考虑分布式拒绝服务弹性也很重要。许多地区靠近互联网交换中心，因此与主要网络的连接更多。靠近国际运营商和大型同业有强大影响力的交易所，可以帮助您减轻大型攻击的互联网容量。

要了解有关选择区域的更多信息，请参见。您也可以询问客户团队有关您考虑的每个区域的特征，以帮助您做出明智的决定。Regions and Availability Zones

负载平衡（BP6）

大型分布式拒绝服务攻击可能会淹没单个Amazon EC2实例的容量，因此添加负载平衡可以帮助增强弹性。您可以从多个选项中进行选择，以通过平衡多余流量来缓解攻击。借助弹性负载平衡（ELB），您可以通过在多个后端实例之间分配流量来降低应用程序超载的风险。
ELB可以自动扩展，允许您在意外流量增加（例如，由于闪存人群或分布式拒绝服务攻击）而管理更大的流量。对于在Amazon VPC内构建的应用程序，根据应用程序类型考虑两种类型的ELB：应用程序负载平衡器（ALB）或网络负载平衡器（NLB）。

对于网络应用程序，可以使用ALB根据其内容路由流量，仅接受格式正确的网络请求。这意味着ALB将阻止许多常见的分布式拒绝服务攻击，如SYN泛洪或UDP反射攻击，保护您的应用程序免受攻击。当ALB检测到这些类型的攻击时，会自动扩展以吸收更多流量。要了解有关使用ALB保护网络应用程序的更多信息，请参阅 Getting Started withApplication Load Balancers.

对于基于TCP的应用程序，您可以使用NLB以超低延迟将流量路由到Amazon EC2实例。创建NLB时，将为启用的每个可用区（AZ）创建一个网络接口。您可以选择为为负载平衡器启用的每个子网分配一个弹性IP（EIP）地址。
NLB的一个关键考虑因素是，到达有效监听器上的负载平衡器的任何流量都将路由到您的Amazon EC2实例，而不是被吸收。要了解有关使用NLB保护TCP应用程序的更多信息，请参阅。 Getting Started withNetwork Load Balancers

使用AWS Edge位置（BP1，BP3）大规模交付

访问大规模，多样的互联网连接可以显着提高优化用户延迟和吞吐量，吸收分布式拒绝服务攻击和隔离故障的能力，同时最大程度降低对应用程序可用性的影响。
AWS边缘位置提供了一层额外的网络基础设施，可为使用Amazon CloudFront和Amazon Route 53的任何网络应用程序提供这些好处。使用这些服务时，将为您的内容提供服务，并从更接近您的位置解析域名系统（DNS）查询用户。

边缘网络应用交付（BP1）

Amazon CloudFront是一项可用于交付整个网站的服务，包括静态，动态，流媒体和交互式内容。持久性TCP连接和可变的生存时间（TTL）设置可用于卸载源流量，即使您不是

提供可缓存内容。这些功能意味着使用Amazon CloudFront可以减少返回到源的请求和TCP连接数量，帮助保护您的网络应用程序免受HTTP洪水攻击。 Amazon CloudFront仅接受格式正确的连接，有助于防止许多常见的分布式拒绝服务攻击（如SYN泛洪和UDP反射攻击）到达您的来源。分布式拒绝服务攻击在地理位置上也离源头很近，可以防止流量影响其他位置。这些功能可以大大提高大型分布式拒绝服务攻击期间向用户继续提供流量的能力。您可以使用Amazon CloudFront保护AWS或互联网其他地方的来源。

如果您使用Amazon S3在互联网上提供静态内容，则应使用Amazon CloudFront保护存储桶。您可以使用原始访问标识（OAI）来确保用户仅通过使用Cloud Front URL访问对象。要了解有关OAI的更多信息，请参见Usingan Origin Access Identity to Restrict Access to Your Amazon S3 Content.

要了解有关使用Amazon CloudFront保护和优化网络应用程序性能的更多信息，请参阅。Getting Started with CloudFront

边缘域名解析（BP3）

Amazon Route 53是一种高度可用的可扩展域名系统（DNS）服务，可用于将流量定向到您的网络应用程序。它包括高级功能，如流量，基于延迟的路由，地理域名系统以及运行状况检查和监视，可让您控制服务如何响应域名系统（DNS）请求，提高网络应用程序性能并避免站点中断。

Amazon Route 53使用混洗分片和任播条带化技术，即使域名系统拒绝服务攻击针对的是域名系统服务，也可以帮助用户访问您的应用程序。使用随机分片，委派集中的每个名称服务器都对应一组唯一的边缘位置和互联网路径。这样可以提供更大的容错能力，并最大程度地减少客户之间的重叠。如果委派集中的一个名称服务器不可用，用户可以重试并从不同边缘位置的另一台名称服务器接收响应。任播条带化使每个域名系统（DNS）请求都由最佳位置服务，从而分散网络负载并减少域名系统（DNS）延迟。反过来，这可以为用户提供更快的响应。此外，Amazon Route 53可以检测域名系统（DNS）查询的来源和数量异常，并区分来自可靠用户的请求。

要了解有关使用Amazon Route 53将用户路由到您的应用程序的更多信息，请参阅。GettingStarted with Amazon Route 53

应用程序层防御（BP1，BP2，BP6）

本文讨论的许多技术都可以有效缓解基础设施层分布式拒绝服务攻击对应用程序可用性的影响。为了同时防御应用程序层攻击，您需要实现一种架构，允许您专门检测，扩展以吸收和阻止恶意请求。这是一个重要的考虑因素，因为基于网络的分布式拒绝服务缓解系统通常无法有效缓解复杂的应用程序层攻击。

检测和过滤恶意Web请求（BP1，BP2）

当应用程序在AWS上运行时，可以同时利用Amazon CloudFront和AWS WAF防御应用程序层分布式拒绝服务攻击。

Amazon CloudFront允许您缓存静态内容并从AWS边缘位置提供静态内容，这有助于减少原始负载。它还可以防止非网络流量到达您的来源，从而帮助减轻服务器负载。此外，CloudF ront可以自动关闭来自慢速读取或慢速写入攻击者（如Slowloris）的连接。

通过使用AWS WAF，您可以在CloudFront分配或应用程序负载平衡器上配置网络访问控制列表（Web ACL），以基于请求签名过滤和阻止请求。每个网络访问控制列表均包含规则，您可以配置为字符串匹配或正则表达式匹配一个或多个请求属性，例如URI，查询字符串，HTT P方法或标头密钥。此外，通过使用AWS
WAF的基于速率的规则，当与规则匹配的请求超过您定义的阈值时，可以自动阻止不良行为者的IP地址。
来自有问题的客户端IP地址的请求将收到“ 403 Forbidden”错误响应，并保持阻塞状态，直到请求速率降至阈值以下。这对于缓解伪装成常规网络流量的HTTP洪水攻击很有用。

要阻止来自已知作用不良的IP地址的攻击，您可以使用IP匹配条件创建规则，也可以使用AWS Marketplace中卖家提供的AWS WAF托管规则，阻止包含在IP信誉列表中的特定恶意IP地址。借助AWS WAF和Amazon CloudFront，您都可以设置地理位置限制，以阻止或将来自所选国家/地区的请求列入白名单。这样可以帮助阻止源自您不希望为用户服务的地理位置的攻击。

为帮助识别恶意请求，您可以查看网络服务器日志或使用WAF的采样请求功能，该功能提供在过去3个小时内与AWS WAF规则之一相匹配的请求的详细信息。您可以使用此信息识别潜在的恶意流量签名，并创建新规则拒绝这些请求。如果看到许多带有随机查询字符串的请求，则可以决定禁用查询

Amazon CloudFront中的字符串转发。这有助于缓解针对原始服务器的缓存破坏攻击。

如果您订阅了AWS Shield Advanced，则可以与AWS DDoS响应团队（DRT）互动，帮助您创建规则来缓解损害应用程序可用性的攻击。 DRT仅在获得您的明确授权后才能获得对您帐户的有限访问权限。有关更多信息，请参见本文档后面的“支持”部分。

使用AWS防火墙管理器可以帮助简化组织中AWS WAF规则的管理。通过使用AWS防火墙管理器，您可以跨许多账户和资源启用AWS WAF，包括创建自动应用于组织中现有或新账户的规则。

要了解有关使用地理限制限制访问Amazon CloudFront分配的更多信息，请参阅。Restricting the Geographic Distribution of Your Content

要了解有关使用AWS WAF的更多信息，请参阅和Getting Started with AWS WAF Viewing aSample of the Web Requests that CloudFront has Forwarded to AWS WAF.

要了解有关配置基于速率的规则的更多信息，请参阅Protect Web Sites & Services UsingRate-Based Rules for AWS WAF.

要了解如何使用AWS Firewall Manager管理跨AWS资源的AWS WAF规则部署，请参阅。Getting Started with AWS Firewall Manager

扩大以吸收（BP6）

缓解应用程序层攻击的另一种方法是大规模运行。如果拥有网络应用程序，则可以使用ELB将流量分配到多个Amazon EC2实例，这些实例已超额配置或配置为自动扩展。这些实例可以处理由于各种原因突然发生的流量激增，包括闪存人群或应用程序层分布式拒绝服务攻击。您可以将Amazo n CloudWatch警报设置为启动自动扩展，以响应定义的事件自动扩展Amazon EC2机群的规模。当请求量意外增加时，这可以保护应用程序可用性。如果您对应用程序使用Amazon CloudFront或应用程序负载平衡器（ALB），则TLS协商由分发或负载平衡器处理。通过扩展到处理合法请求和TLS滥用攻击，可以帮助保护实例免受基于TLS攻击的影响。

要了解有关使用Amazon CloudWatch调用Auto Scaling的更多信息，请参阅。Monitoring YourAuto Scaling Instances and Groups Using Amazon CloudWatch

减少攻击面

架构AWS解决方案时，另一个重要的考虑因素是限制攻击者针对应用程序的机会。例如，如果不希望用户直接与某些资源交互，则可以确保无法从互联网访问这些资源。同样，如果不希望用户或外部应用程序在某些端口或协议上与应用程序通信，则可以确保不接受该流量。

这个概念称为攻击面减少。在本节中，我们提供最佳实践，以帮助您减少攻击面并限制应用程序的互联网暴露。未暴露于互联网的资源更难以攻击，这限制了攻击者针对应用程序可用性的选择。

混淆AWS资源（BP1，BP4，BP5）

通常，用户可以快速轻松地使用应用程序，而无需将AWS资源完全暴露给互联网。例如，当ELB后面有Amazon EC2实例时，可能无需公开访问这些实例本身。相反，您可以为用户提供某些TCP端口上的ELB访问权限，并且仅允许ELB与实例通信。您可以通过在Amazon虚拟私有云（VPC）中配置安全组和网络访问控制列表（NACL）来进行设置。Amazon VPC允许您配置AWS云中逻辑隔离的部分，您可以在其中定义的虚拟网络中启动AWS资源 。

安全组和NACL相似，它们可让您控制对VPC中AWS资源的访问。但是，安全组可让您在实例级别控制入站和出站流量，而NACL在VPC子网级别提供类似的功能。使用安全组或NACL不收取额外费用。

安全组和网络访问控制列表（BP5）

您可以在启动实例时指定安全组，也可以稍后将实例与安全组关联。除非您创建允许规则以允许流量，否则将隐式拒绝所有流向安全组的互联网流量。例如，如果您有一个使用ELB和多个Amazon EC2实例的网络应用程序，则可能会决定为ELB创建一个安全组（“ELB安全组”），为实例创建一个安全组（“网络应用程序服务器安全组”）。然后，您可以创建一个允许互联网流量的允许规则

到ELB安全组，以及另一条允许从ELB安全组到网络应用程序服务器安全组的流量的规则 。这样可以确保互联网流量无法直接与您的Amazon EC2实例通信，从而使攻击者更难了解和影响您的应用程序。

创建NACL时，可以同时指定允许和拒绝规则。如果要明确拒绝应用程序的某些类型的流量，这很有用。例如，可以定义拒绝访问整个子网的IP地址（如CIDR范围），协议和目标端口。如果您的应用程序仅用于TCP流量，则可以创建规则拒绝所有UDP流量，反之亦然。当响应分布式拒绝服务攻击时，此选项很有用，因为当您知道源IP或其他签名时，可使用此选项创建自己的规则来缓解攻击。

如果您订阅了AWS Shield Advanced，则可以将弹性IP（EIP）注册为受保护资源。更快地检测到针对已注册为受保护资源的EIP的分布式拒绝服务攻击，这可以缩短迁移时间。当检测到攻击时，分布式拒绝服务缓解系统读取与目标EIP相对应的NACL，并在AWS网络边界强制实施。这样可以大大降低您受到多种基础设施层分布式拒绝服务攻击的影响风险。
要了解有关配置安全组和NACL以优化分布式拒绝服务弹性的更多信息，请参阅How to Help Prepare for DDoS Attacks by Reducing Your Attack Surface.
要了解有关结合使用带有EIP的AWS Shield Advanced和受保护资源的更多信息，请参阅Enableand Configure AWS Shield Advanced.

保护您的起源（BP1，BP5）

如果您使用的Amazon CloudFront源于VPC内，则应使用AWS Lambda函数自动更新安全组规则，仅允许Amazon CloudFront流量。通过帮助确保恶意用户访问网络应用程序时不会绕过Amazon CloudFront和AWS WAF，从而提高来源安全性。

要了解有关如何通过自动更新安全组来保护来源的详细信息，请参阅How to Automatically Update Your Security Groups for Amazon CloudFront andAWS WAF by Using AWS Lambda.

您可能还需要确保只有Amazon CloudFront分配可以将请求转发到源。使用边缘到源请求标头，当Amazon CloudFront将请求转发到源时，您可以添加或覆盖现有请求标头的值。您可以使用X-Shared-Secret标头来帮助验证对源发起的请求是从Amazon CloudFront发送的。

要了解有关使用X-Shared-Secret标头保护原始资源的更多信息，请参见 ForwardingCustom Headers to Your Origin.

保护API端点（BP4）

通常，当您必须向公众公开API时，就有可能被分布式拒绝服务攻击以API前端为目标。为帮助降低风险，您可以将Amazon API Gateway用作运行在Amazon EC2，AWS Lambda或其他地方的应用程序的“前门”。通过使用Amazon API Gateway，您不需要自己的服务器即可使用API前端，并且可以混淆应用程序的其他组件 。通过更难检测到您的应用程序组件，可以帮助防止分布式拒绝服务攻击针对这些AWS资源。

使用Amazon API Gateway时，可以从两种类型的API终端节点中选择。第一个是默认选项：通过Amazon CloudFront分配访问的边缘优化API终端节点。但是，该分发由API网关创建和管理，因此您无权控制。第二种选择是使用区域API终端节点，该终端节点可从与部署REST API相同的AWS区域访问。我们建议您使用第二种终端节点，然后将其与自己的Amazon CloudFront分配关联。这样，您就可以控制Amazon CloudFront分配以及使用AWS WAF进行应用程序层保护的能力。

当将Amazon CloudFront和AWS WAF与Amazon API网关结合使用时，请配置以下选项：

- 为您的发布配置缓存行为，以将所有标头转发到API网关区域端点。这样，CloudFront会将内容视为动态内容，并跳过内容缓存。
- 通过在API网关中设置相应的值，将分发配置为包括原始自定义标头x-api-key，防止API网关直接访问。API key
- 通过为REST API中的每种方法配置标准或突发速率限制，保护后端免遭过多流量的侵害。要了解有关使用Amazon API Gateway创建API的更多信息，请参阅。

  Getting Started with Amazon API Gateway

操作技术

本文中的缓解技术可帮助您构建抵御分布式拒绝服务攻击的应用程序。在许多情况下，了解分布式拒绝服务攻击何时将您的应用程序作为目标也很有用，您可以采取缓解措施。如果遭受攻击，则可以在评估威胁和查看应用程序体系结构方面获得帮助，或者可能需要其他帮助。本节讨论最佳实践，以了解异常行为，警报和自动化，并邀请AWS获得更多支持。

能见度

当关键运营指标严重偏离期望值时，攻击者可能会试图针对应用程序的可用性。如果您熟悉应用程序的正常行为，可以在检测到异常时更快地采取措施。

通过使用Amazon CloudWatch，您可以监控在AWS上运行的应用程序。例如，您可以收集和跟踪指
标，收集和监控日志文件，设置警报并自动响应AWS资源的更改。

如果您采用的是分布式拒绝服务防护参考架构来构建应用程序，则在到达应用程序之前，将阻止常见的基础设施层攻击。如果您订阅了AWS Shield Advanced，则可以访问许多CloudWatch指标，这些指标表明您的应用程序已被定位。例如，可以将警报配置为在正在进行分布式拒绝服务攻击时通知您，以便检查您的 应用程序的运行状况，并决定是否启用DRT。您可以配置DDoSDetected指标来告诉您是否检测到攻击。如果希望根据攻击量收到警报，还可以使用DDosAttackBitsPerSecond，D DosattackPacketsPerSecond或DDosattackRequestsPerSecond指标。您可以通过将Amazon CloudWatch与自己的工具集成或使用第三方提供的工具（如Slack或PagerDuty）来监控这些指标。

应用程序层攻击可以提升许多Amazon CloudWatch指标。如果您使用的是AWS WAF，则可以使用CloudWatch监控并警告在其中设置的请求的增加

WAF允许，计数或阻止。如果流量级别超过应用程序可以处理的水平，这将使您收到通知。您还可以使用CloudWatch中跟踪的Amazon CloudFront，Amazon Route53，ALB，NLB，Amazon EC2和Auto Scaling指标来检测可能指示分布式拒绝服务攻击的更改。

有关通常用于检测分布式拒绝服务攻击并对其做出反应的Amazon CloudWatch指标的描述，请参阅下表（表3）。

主题	公制	内容描述
AWS Shield高级	分布式拒绝服务攻击	表示特定亚马逊资源名称（ARN）的分布式拒绝服务事件。
AWS Shield高级	每秒DDoS攻击位数	在特定的亚马逊资源名称（ARN）的分布式拒绝服务事件期间观察到的字节数。此指标仅适用于第3/4层分布式拒绝服务事件。
AWS Shield高级	每秒DDoS攻击数据包	在特定的亚马逊资源名称（ARN）的分布式拒绝服务事件期间观察到的数据包数量。此指标仅适用于第3/4层分布式拒绝服务事件。
AWS Shield高级	每秒DDoS攻击请求	在分布式拒绝服务事件期间观察到的特定亚马逊资源名称（ARN）的请求数。该指标仅适用于第7层分布式拒绝服务事件，仅报告最重要的第7层事件。
AWS网络应用防火墙	允许的请求	允许的网络请求数。
AWS网络应用防火墙	被阻止的请求	阻止的网络请求数。
AWS网络应用防火墙	计数请求	计算的网络请求数。
亚马逊CloudFront	要求	HTTP / S请求数
亚马逊CloudFront	总错误率	HTTP状态代码为4xx或5xx的所有请求的百分比。
亚马逊路线53	健康检查状态	健康检查端点的状态。
ALB	活动连接数	从客户端到负载平衡器，以及从负载平衡器到目标，活动的并发TCP连接总数。
ALB	消耗的LCU	负载平衡器使用的负载平衡器容量单位（LCU）数。

主题	公制	内容描述
ALB	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	负载平衡器生成的HTTP 4xx或5xx客户端错误代码数。
ALB	新连接计数	从客户端到负载平衡器以及从负载平衡器到目标建立的新TCP连接总数。
ALB	处理字节数	负载平衡器处理的字节总数。
ALB	拒绝连接计数	由于负载平衡器达到最大连接数而被拒绝的连接数。
ALB	请求计数	已处理的请求数。
ALB	目标连接错误计数	负载均衡器和目标之间未成功建立的连接数。
ALB	目标响应时间	从请求离开负载平衡器到收到目标响应的时间（秒）。
ALB	不健康的主机计数	被认为不健康的目标数量。
美国职业棒球大联盟	活动流量计数	从客户端到目标的并发TCP流（或连接）总数。
美国职业棒球大联盟	消耗的LCU	负载平衡器使用的负载平衡器容量单位（LCU）数。
美国职业棒球大联盟	新流量计数	在这段时间内从客户端到目标建立的新TCP流（或连接）总数。
美国职业棒球大联盟	处理字节数	负载平衡器处理的字节总数，包括TCP / IP标头。
自动缩放	组最大大小	Auto Scaling组的最大大小
亚马逊EC2	CPU利用率	当前正在使用的分配的EC2计算单元的百分比。
亚马逊EC2	网络输入	实例在所有网络接口上接收到的字节数。

表3：建议的Amazon CloudWatch指标。

要了解有关使用Amazon CloudWatch检测应用程序上的分布式拒绝服务攻击的更多信息，请参阅。[Getting Started with Amazon CloudWatch]

AWS包括其他几种指标和警报，可向您通知发生攻击并帮助您监控应用程序资源。 AWS Shield控制台或API提供了已检测到攻击的摘要和详细信息。此外，全球威胁环境仪表板还提供有关AWS检测到的所有分布式拒绝服务攻击的摘要信息。这对于更好地了解更大数量的应用程序中的分布式拒绝服务威胁，了解攻击趋势以及与您可能已经观察到的攻击进行比较很有帮助。

另一个可以帮助您了解以应用程序为目标的流量的工具是VPC流日志。在传统网络上，可能会使用网络流日志对连接和安全问题进行故障排除，并确保网络访问规则按预期工作。通过使用VPC流日志，可以捕获有关往返VPC中网络接口的IP流量的信息。

每个流日志记录包括以下内容：源和目的地IP地址，源和目的地端口，协议以及在捕获窗口期间传输的数据包和字节数。您可以使用此信息帮助识别网络流量异常并识别特定的攻击媒介。例如，大多数UDP反射攻击都有特定的源端口，例如域名系统反射的源端口53。这是清晰的签名，可以在流日志记录中识别。作为响应，如果您的应用程序可以选择在实例级别阻止特定的源端口，也可以创建NACL规则阻止整个协议不需要。

要了解有关使用VPC流日志识别网络异常和分布式拒绝服务攻击媒介的更多信息，请参阅和。VPC Flow Logs VPC Flow Logs – Log and View Network Traffic Flows

技术支持

在实际事件发生之前为分布式拒绝服务攻击创建响应计划非常重要。本文概述的最佳实践旨在作为在启动应用程序之前实施的主动措施，但仍然可能发生针对应用程序的分布式拒绝服务攻击。查看本节中的选项，确定最适合您的方案的支持资源。您的客户团队可以评估您的用例和应用程序，并为您解决特定的问题或挑战。

如果您在AWS上运行生产工作负载，请考虑订阅业务支持，该服务可为您提供24 x 7全天候24小时服务访问云支持工程师，以协助解决分布式拒绝服务攻击问题。如果您运行的是关键任务型工作负载，请考虑使用企业支持，它可以打开“关键”案例并获得客户的最快响应。

高级云支持工程师。

如果您订阅了AWS Shield Advanced，并且还订阅了业务支持或企业支持，则如果发生与分布式拒绝服务相关的事件（影响到应用程序的可用性），则可以升级到AWS分布式拒绝服务响应团队（DRT）。如果由于分布式拒绝服务攻击而导致应用程序响应速度下降，则可以与AWS支持实时联系。另一个选择是使用AWS Shield参与Lambda函数更快地启动与DRT的联系。例如，如果发生紧急情况，可以使用A WS IoT按钮触发AWS Lambda功能。当您按下按钮时，将通过AWS支持自动打开案例并立即通知DRT。您会收到针对您的案件的直接回复，包括一个Amazon Chime会议桥，您可以加入该会议桥与AWS支持和DRT互动。 AWS Shield参与Lambda可以与AWS Lambda支持的任何触发器一起使用。

要了解有关使用AWS Lambda函数进行快速DRT参与的更多信息，请参阅AWS ShieldEngagement Lambda.

DRT通常无权访问您的AWS账户或AWS WAF采样请求。您可以授权DRT从AWS Shield控制台或API访问账户上的AWS WAF，AWS Shield和相关API操作。例如，您可能需要允许DRT查看采样请求或放置规则，以帮助缓解应用程序层分布式拒绝服务攻击。您也可以授权DRT访问您指定的Amazon S3存储桶。例如，您可能有一个存储网络请求日志的存储桶，并且希望DRT在攻击期间可以访问它们进行分析。
DRT仅会在升级事件期间访问您的帐户或进行更改，任何更改都必须征得您的同意。要了解更多有关授予有限帐户访问DRT的信息，请参阅。Authorize the DDoS Response Team

在某些情况下，DRT可能会了解分布式拒绝服务攻击并主动与您互动。如果在DRT驱动的升级过程中有特定联系人需要联系，您可以在AWS Shield控制台中单击“摘要”，然后在“”其他联系人”部分。

结论

本文概述的最佳实践可以帮助您构建可抵抗分布式拒绝服务攻击的体系结构，通过防止许多常见的基础设施和应用程序层分布式拒绝服务攻击保护应用程序的可用性。架构应用程序时遵循这些最佳实践的程度将影响可以缓解的分布式拒绝服务攻击的类型，向量和数量。您可以构建弹性，而无需订阅分布式拒绝服务缓解服务。或者，您可以选择订购AWS Shield Advanced，以获得更多支持，可见性，缓解和成本保护功能，进一步保护本已具有弹性的应用程序架构。

要了解有关AWS上的分布式拒绝服务缓解和分布式拒绝服务弹性最佳实践的更多信息，请参阅附录A：其他资源。

贡献者

以下个人和组织对此文件做出了贡献：

- AWS解决方案架构师Andrew Kiggins
- Jeffrey Lyon，AWS外围保护
- AWS解决方案架构师Achraf Souk
- Tino Tran，AWS解决方案架构师
- AWS解决方案架构师Yoshihisa Nakatani

文件修订

日期	内容描述
2018年6月	已更新，包括AWS Shield，AWS WAF功能，AWS防火墙管理器和相关最佳实践。
2016年6月	添加了说明性架构指南，并进行了更新，包括AWS WAF。

日期	内容描述
2015年6月	首次出版。

附录A：其他资源

您可以使用以下资源详细了解AWS的分布式拒绝服务缓解和分布式拒绝服务弹性最佳实践：

- Best Practices for DDoS Mitigation on AWS
- SID216 – re:Invent 2017: Cloud-Native App Protection: Web Application Security at Pearson
- SID324 – re:Invent 2017: Automating DDoS Response in the Cloud
- CTD304 – re:Invent 2017: Dow Jones & Wall Street Journal's Journey to Manage Traffic Spikes While Mitigating DDoS & Application Layer Threats
- CTD310 – re:Invent 2017: Living on the Edge, It's Safer Than You Think! Building Strong with Amazon CloudFront, AWS Shield, and AWS WAF