AWS 白皮书

AWS DDoS弹性最佳实践

AWS DDoS弹性最佳实践: AWS 白皮书

Table of Contents

AWS DDoS弹性最佳实践

发布日期：2023 年 8 月 9 日 (文档修订)

保护您的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非常重要。通过保持应用程序的可用性和响应能力来保持客户对您的服务的信任是当务之急。当您的基础设施必须扩展以应对攻击时，您还希望避免不必要的直接成本。Amazon Web Services (AWS) 致力于为您提供工具、最佳实践和服务，以防范互联网上的不良行为者。使用来自的正确服务 AWS 有助于确保高可用性、安全性和弹性。

在本白皮书中，为您 AWS 提供了规范性DDoS指导，以提高运行应用程序的弹性。 AWS这包括一个DDoS弹性参考架构，可用作帮助保护应用程序可用性的指南。本白皮书还描述了不同的攻击类型，例如基础设施层攻击和应用层攻击。 AWS 解释了哪种最佳做法对管理每种攻击类型最有效。此外，还概述了适合DDoS缓解策略的服务和功能，以及如何使用每种服务和功能来帮助保护您的应用程序。

本 paper 面向熟悉网络、安全和基本概念的 IT 决策者和安全工程师 AWS。每个部分都有指向 AWS 文档的链接，这些文档提供了有关最佳实践或能力的更多详细信息。

AWS 每年检测超过一百万次DDoS攻击，每天缓解成千上万次针对客户的攻击。根据我们的 Shield Response 团队 (SRT) 的说法，大多数因DDoS攻击而受到业务影响的客户都没有实施本指南中的建议。

您的架构是否良好？

当您在云端构建系统时，AWS Well-Architected Framework 可帮助您了解所做决策的利弊。利用此框架的六个支柱，您可以了解到设计和运行可靠、安全、高效、经济有效且可持续的系统的架构最佳实践。使用 AWS Management Console（需要登录）中免费提供的，您可以通过回答每个支柱的一组问题，根据这些最佳实践来查看您的工作负载。AWS Well-Architected Tool

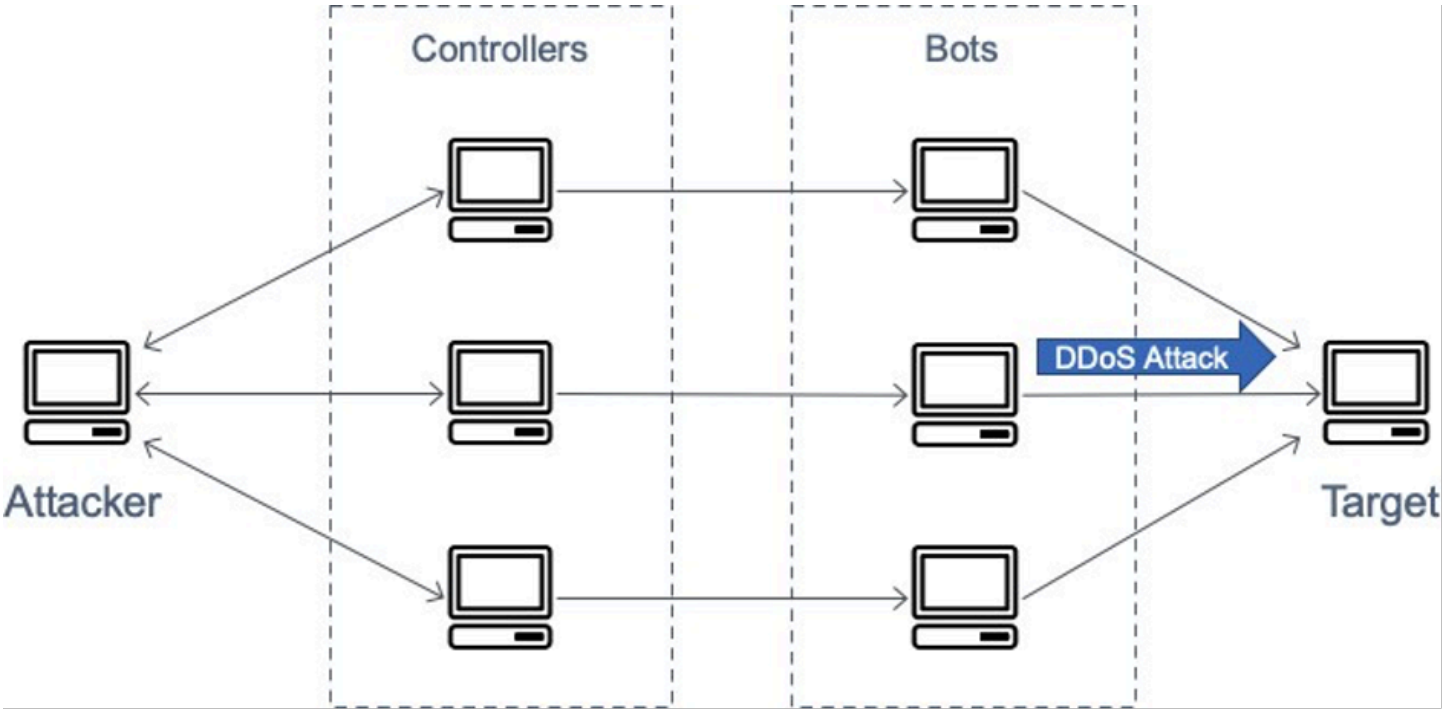
有关云架构的更多专家指导和最佳实践（参考架构部署、图表和白皮书），请参阅架构中心。AWS

拒绝服务攻击简介

拒绝服务 (DoS) 攻击或事件是故意使用户无法访问网站或应用程序的行为，例如向其充斥网络流量。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，从而中断合法用户的访问。在最简单的形式中，孤独的攻击者使用单一来源对目标进行 DoS 攻击，如下图所示。

描绘 DoS 攻击的示意图

在分布式拒绝服务 (DDoS) 攻击中，攻击者使用多个来源策划针对目标的攻击。这些来源可能包括分布式的受恶意软件感染的计算机、路由器、物联网设备和其他端点。下图显示了一个由参与攻击的受感染主机组成的网络，这些主机生成了大量数据包或请求，使目标不堪重负。



描绘攻击的示意图 DDoS

开放系统互连 (OSI) 模型中有七个层，下表对它们进行了描述。DDoS攻击最常见于第 3、4、6 和 7 层。

- 第 3 层和第 4 层攻击对应于OSI模型的网络层和传输层。在本白皮书中， AWS 将这些攻击统称为基础设施层攻击。
- 第 6 层和第 7 层攻击对应于OSI模型的演示层和应用层。本白皮书将这些问题作为应用层攻击一并解决。

此 paper 将在以下各节中讨论这些攻击类型。

表 1 — OSI 型号

#	层	单位	描述	向量示例
7	应用程序	数据	网络进程到应用程序	HTTP洪水，DNS查询洪水
6	呈现方式	数据	数据表示和加密	传输层安全 (TLS) 滥用
5	会话	数据	主机间沟通	不适用
4	传输	分段	E nd-to-end 连接和可靠性	同步 (SYN) 洪水
3	网络	数据包	路径确定和逻辑寻址	用户数据报协议 (UDP) 反射攻击
2	数据链接	帧	物理寻址	不适用
1	物理	Bits	媒体、信号和二进制传输	不适用

基础设施层攻击

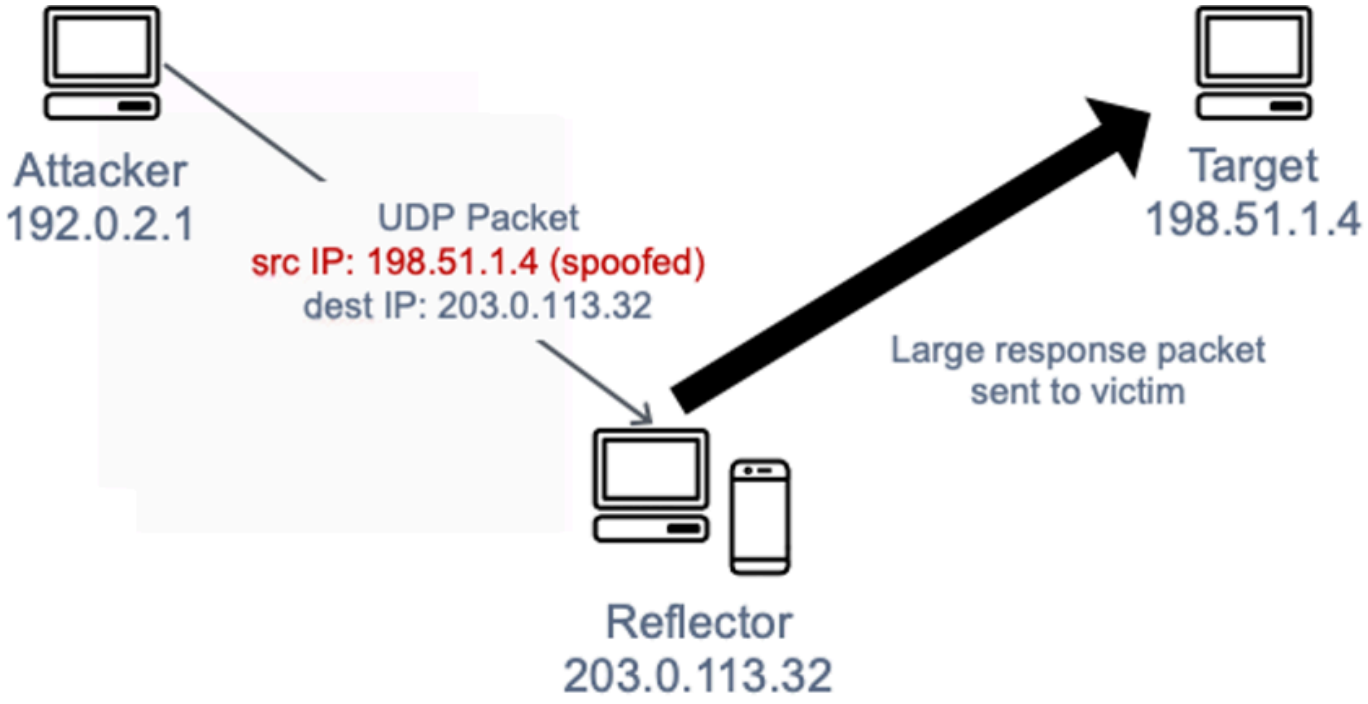
最常见的DDoS攻击，即用户数据报协议 (UDP) 反射攻击和SYN洪水，是基础设施层攻击。攻击者可以使用这两种方法中的任何一种生成大量流量，这些流量可能会淹没网络的容量或占用服务器、防火墙、入侵防御系统 (IPS) 或负载平衡器等系统的资源。虽然这些攻击很容易识别，但要有效缓解这些攻击，您的网络或系统必须比入站流量泛滥更快地扩展容量。这种额外的容量是过滤或吸收攻击流量所必需的，从而腾出系统和应用程序来响应合法的客户流量。

UDP反射攻击

UDP反射攻击利用了无状态协议这一UDP事实。攻击者可以制作一个有效的UDP请求数据包，将攻击目标的 IP 地址列为UDP源 IP 地址。攻击者现在伪造了请求数据包的源 IP（欺骗）UDP。该UDP数据包包含伪造的源 IP，由攻击者发送到中间服务器。服务器被诱骗将其UDP响应数据包发送到目标受害者 IP，而不是发送回攻击者的 IP 地址。之所以使用中间服务器，是因为它生成的响应比请求数据包大几倍，从而有效地放大了发送到目标 IP 地址的攻击流量。

放大系数是响应大小与请求大小的比率，它因攻击者使用的协议而异：DNS、网络时间协议 ()、简单服务目录协议 (NTP)、无连接轻量级目录访问协议 (SSDPCLDAP)、Memcached、字符生成器协议 (CharGen) 或每日报价 ()。QOTD

例如，的放大系数DNS可以是原始字节数的 28 到 54 倍。因此，如果攻击者向DNS服务器发送 64 字节的请求有效负载，他们可能会向攻击目标生成超过 3400 字节的不想要的流量。UDP与其他攻击相比，反射攻击导致的流量更大。下图说明了反射策略和放大效果。

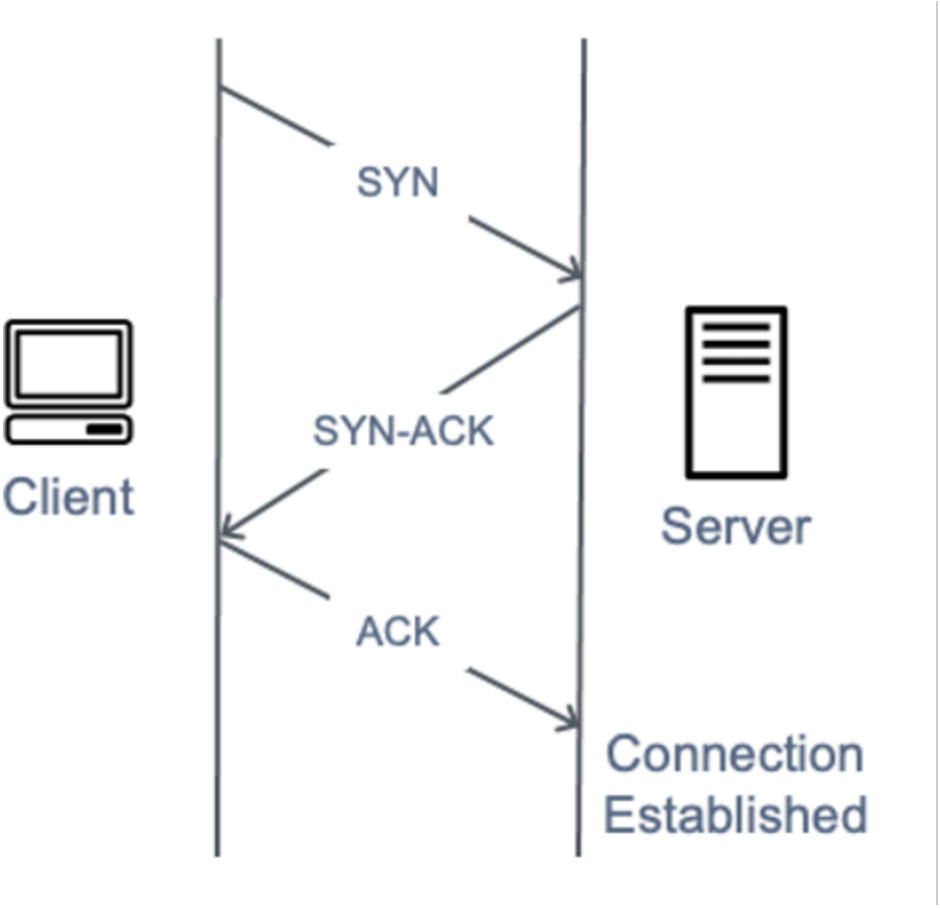


描绘UDP反射攻击的示意图

应该注意的是，反射攻击虽然为攻击者提供“免费”放大，但需要 IP 欺骗能力，而且随着越来越多的网络提供商采用无处不在的源地址验证 (SAVE)，或者 BCP38，这种功能已被删除，要求DDoS服务提供商停止反射攻击或迁移到不实施源地址验证的数据中心和网络提供商。

SYN洪水袭击

当用户连接到传输控制协议 (TCP) 服务（例如 Web 服务器）时，他们的客户端会发送一个SYN数据包。服务器返回同步确认 (SYN-ACK) 数据包，最后，客户端使用确认 () 数据包进行响应，该数据包完成了预期ACK的三次握手。下图说明了这种典型的握手。



描绘SYN三方握手的示意图

在SYN洪水攻击中，恶意客户端发送大量SYN数据包，但从不发送最后ACK的数据包来完成握手。服务器只能等待对半开TCP连接的响应，其想法是目标最终会耗尽容量，无法接受新TCP连接，这会阻止新用户连接到服务器，但是实际影响更加细微差别。默认情况下，现代操作系统都实现了 SYN Cookie，以此作为抵御SYN洪水攻击导致状态表耗尽的机制。SYN队列长度达到预先确定的阈值后，服务器将使用ACK包含精心编制的初始序列号的 SYN-进行响应，而不在其SYN队列中创建条目。如果服务器随后收到ACK包含正确递增的确认号，则可以将该条目添加到其状态表中并照常进行。SYN洪水对目标设备的实际影响往往是网络容量和CPU耗尽，但是防火墙（或EC2安全组连接跟踪）等中间状态设备可能会出现TCP状态表耗尽并丢弃新连接。

TCP中间框反射

这种相对较新的攻击媒介于2021年8月在一份学术白皮书中首次披露，该白皮书解释了民族国家和市售防火墙TCP的不合规行为如何导致这些防火墙被欺骗成为放大载体。TCP自 2022 年初以来，我们已在“野外” 看到这些攻击，并且至今仍在继续。由于供应商实现此 “功能” 的方式不同，放大系数会有所不同，但可能会超过 Memcached UDP 的放大倍数。

应用层攻击

攻击者可以通过使用第 7 层或应用程序层攻击来瞄准应用程序本身。在这些攻击中，与SYN洪水基础设施攻击类似，攻击者试图使应用程序的特定功能过载，以使该应用程序不可用或对合法用户没有响应。有时，这可以通过非常低的请求量来实现，只会产生少量的网络流量。这会使攻击难以检测和缓解。应用层攻击的示例包括HTTP洪水、缓存破坏攻击和-洪水。 WordPress XML RPC

- 在HTTP洪水攻击中，攻击者发送的HTTP请求看似来自 Web 应用程序的有效用户。有些HTTP洪水会针对特定的资源，而更复杂的HTTP洪水则试图模拟人类与应用程序的互动。这可能会增加使用常见缓解技术（例如请求速率限制）的难度。
- 缓存破坏攻击是一种HTTP洪水，它使用查询字符串中的变体来规避内容分发网络 () 缓存。CDN它们不能返回缓存的结果，而是CDN必须为每个页面请求联系源服务器，而这些源提取会给应用程序 Web 服务器带来额外的压力。
- 通过RPC洪水攻击（也称为 WordPress pingback flood），攻击者将目标对准 WordPress 内容管理软件上托管的网站。WordPress XML攻击者滥用 XML-RPC API 函数生成大量HTTP请求。pingback 功能允许托管在 WordPress （站点 A）上的 WordPress 网站通过站点 A 创建的指向站点 B 的链接通知其他站点（站点 B），然后网站 B 尝试获取站点 A 以验证该链接的存在。在 pingback 洪水中，攻击者滥用此功能使站点 B 攻击站点 A。这种类型的攻击具有明确的签名：“`WordPress:`” 通常出现在请求标头的 User-Agent 中。HTTP

还有其他形式的恶意流量可能会影响应用程序的可用性。抓取机器人会自动尝试访问网络应用程序以窃取内容或记录竞争信息（例如定价）。暴力攻击和凭据填充攻击是经过编程的行为，旨在未经授权地访问应用程序的安全区域。严格来说，这些DDoS攻击并不是攻击，但其自动化性质可能与DDoS攻击类似，可以通过实施本paper中介绍的一些相同的最佳实践来缓解攻击。

应用层攻击也可以针对域名系统 (DNS) 服务。这些攻击中最常见的是DNS查询洪水，在这种攻击中，攻击者使用许多格式良好的DNS查询来耗尽DNS服务器的资源。这些攻击还可能包括缓存破坏组件，攻击者通过随机化子域字符串来绕过任何给定解析器的本地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DNS服务器，这会放大攻击。

如果 Web 应用程序是通过传输层安全性 (TLS) 传送的，攻击者也可以选择攻击TLS协商过程。TLS计算成本很高，因此攻击者通过在服务器上产生额外的工作负载，将无法读取的数据（或难以理解（密文））作为合法握手进行处理，从而降低服务器的可用性。在这种攻击的变体中，攻击者完成了TLS握手，但会永久重新协商加密方法。攻击者也可以尝试通过打开和关闭多个TLS会话来耗尽服务器资源。

缓解技术

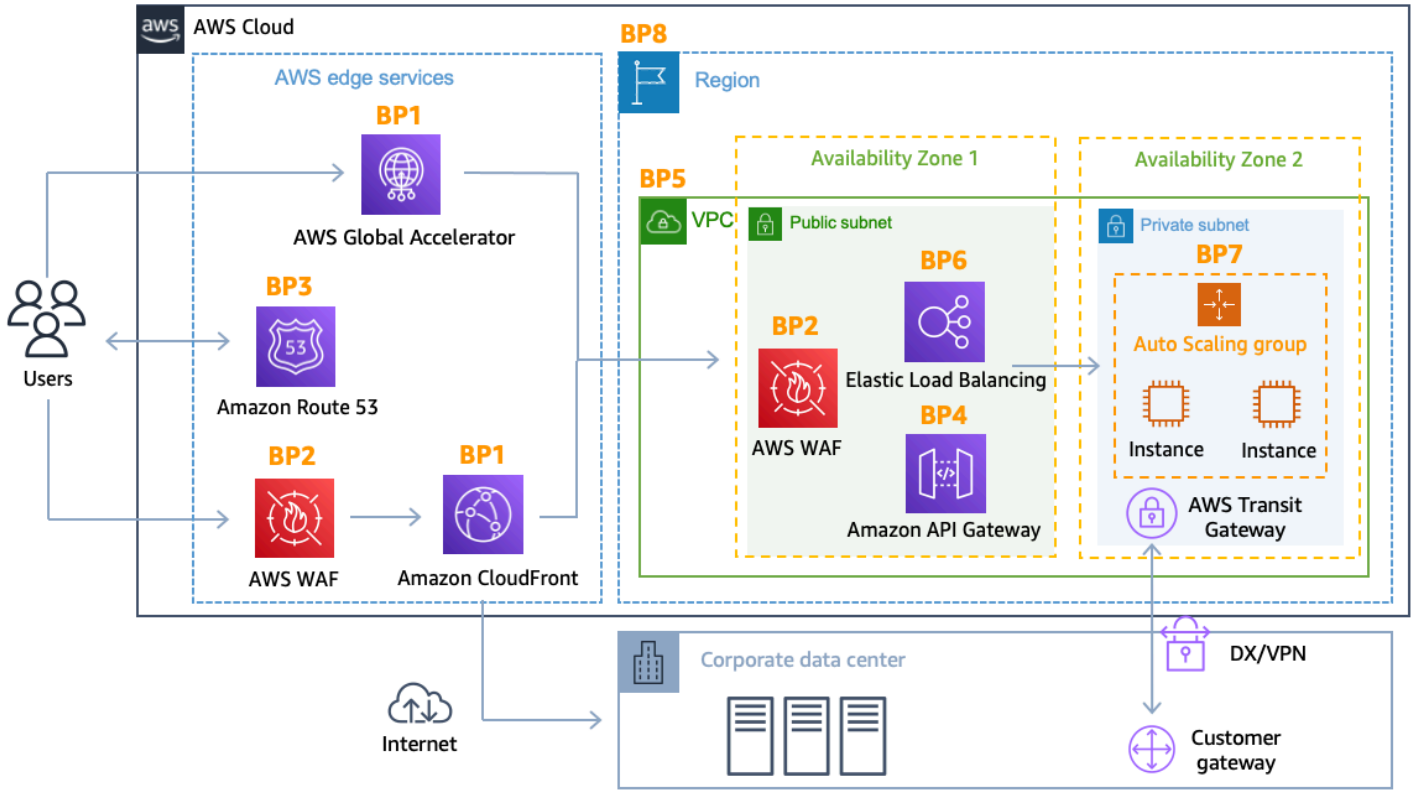
某些形式的DDoS缓解措施会自动包含在 AWS 服务中。DDoS通过使用具有特定服务的 AWS 架构（将在以下各节中介绍），以及通过为用户和应用程序之间的网络流的每个部分实施其他最佳实践，可以进一步提高弹性。

您可以使用在边缘位置运行的 AWS 服务，例如 Amazon CloudFront、G AWS lobal Accelerator 和 Amazon Route 53 来构建针对所有已知基础设施层攻击的全面可用性保护。这些服务是AWS 全球边缘网络的一部分，在为来自分布在世界各地的边缘位置的任何类型的应用程序流量提供服务时，它们可以提高应用程序的DDoS弹性。您可以在任何环境中运行您的应用程序 AWS 区域，并使用这些服务来保护您的应用程序可用性，并为合法的最终用户优化应用程序的性能。

使用亚马逊 CloudFront、全球加速器和亚马逊 Route 53 的好处包括：

- 通过 AWS 全球边缘网络访问互联网和DDoS缓解能力。这对于缓解更大的容量攻击很有用，这种攻击可能达到太比特规模。
- AWS Shield DDoS缓解系统与 AWS 边缘服务集成， time-to-mitigate 从几分钟缩短到不到一秒钟。
- 无状态SYN洪水缓解在将传入的连接传递给受保护的服务之前，使用 SYN Cookie 对其进行验证。这样可以确保只有有效的连接才能到达您的应用程序，同时保护您的合法最终用户免受误报丢失的影响。
- 自动交通工程系统，可分散或隔离大规模攻击的影响。DDoS所有这些服务都会在攻击到达您的源头之前将其隔离在源头，这意味着对受这些服务保护的系统的影响较小。
- 应用程序层防御与之结合使用 CloudFront AWS WAF时不需要更改当前的应用程序架构（例如，在 AWS 区域 或本地数据中心中）。

开启的入站数据传输不收费 AWS ，也无需为缓解的DDoS攻击流量付费。 AWS Shield以下架构图包括 AWS 全球边缘网络服务。



DDoS-弹性参考架构

该架构包括多项 AWS 服务，可帮助您提高 Web 应用程序抵御DDoS攻击的弹性。下表概述了这些服务及其可以提供的功能。 AWS 为便于在本文档中参考，已使用最佳实践指标 (BP1,BP2) 标记了每项服务。例如，下一节将讨论亚马逊 CloudFront 和全球加速器提供的功能，其中包括最佳实践指标 BP1。

表 2-最佳做法摘要

	AWS Edge			AWS 区域		
	将 Amazon CloudFront (BP1) 与 AWS WAF (BP2) 一起使用	使用全球加速器 (BP1)	使用亚马逊 Route 53 (BP3)	将 Elastic Load Balanc BP6 ing () 与 AWS WAF (BP2) 一起使用	ACLs在 Amazon 中使用安全组和网络 VPC (BP5)	使用亚马逊弹性计算云 (亚马逊 EC2) Auto Scaling (BP7)

	AWS Edge			AWS 区域		
第 3 层（例如UDP反射）攻击缓解	✓	✓	✓	✓	✓	✓
缓解第 4 层（例如SYN洪水）攻击	✓	✓	✓	✓		
第 6 层（例如TLS）攻击缓解	✓	✓	✓	✓		
减少攻击面	✓	✓	✓	✓	✓	
进行扩展以吸收应用层流量	✓	✓	✓	✓	✓	✓
第 7 层（应用层）攻击缓解	✓	✓(*)	✓	✓	✓(*)	✓(*)
过剩流量和较大规模DDoS攻击的地理隔离和分散	✓	✓	✓			

✓ (*)：如果与 Application Loa d Balancer AWS WAF 一起使用

提高应对和缓解DDoS攻击的准备程度的另一种方法是订阅。 AWS Shield Advanced使用的好处 AWS Shield Advanced 包括：

- 获得AWS Shield 响应小组 (AWS SRT) 提供的全天候专业支持，以帮助缓解影响应用程序可用性的DDoS攻击，包括可选的主动参与功能

- 敏感的检测阈值可以更早地将流量路由到DDoS缓解系统，当与弹性 IP 地址一起使用时，可以改善对亚马逊EC2（包括弹性负载均衡器）或网络负载均衡器的 time-to-mitigate 攻击
- 与一起使用时，基于应用程序的基线流量模式量身定制的第 7 层检测 AWS WAF
- 自动应用层DDoS缓解，Shield Advanced 通过创建、评估和部署自定义 AWS WAF 规则来响应检测到的DDoS攻击
- 无需额外费用即可访问以 AWS WAF 缓解应用程序层DDoS攻击（与 Amazon CloudFront 或 Application Load Balancer 一起使用时）
- 无需额外费用AWS Firewall Manager即可集中管理安全策略。
- 成本保护，使您能够申请有限退还因攻击而产生的与扩展相关的费用。DDoS
- 针对 AWS Shield Advanced 客户的增强服务级别协议。
- 保护组使您能够捆绑资源，通过将多个资源视为一个单元，提供了一种自助服务方式，可以自定义应用程序的检测和缓解范围。有关保护组的信息，请参阅 Shield 高级保护组。
- DDoS使用AWS Management ConsoleAPI、和 Amazon CloudWatch 指标和警报来监控攻击。

这项可选的DDoS缓解服务有助于保护托管在任何服务器上的应用程序 AWS 区域。该服务在全球范围内可用于 CloudFront Route 53 和全球加速器。在区域方面，您可以保护应用程序负载均衡器、Classic Load Balancer 和弹性 IP 地址，从而保护网络负载均衡器 (NLBs) 或亚马逊EC2实例。

有关 AWS Shield Advanced 功能的完整列表和更多信息 AWS Shield，请参阅AWS Shield 工作原理。

DDoS缓解措施的最佳实践

在以下各节中，将更深入地描述每种推荐的DDoS缓解最佳实践。有关为静态或动态 Web 应用程序构建DDoS缓解层的快速 easy-to-implement 指南，请参阅如何使用 Amazon CloudFront 和 Amazon Route 53 帮助保护动态 Web 应用程序免受DDoS攻击。

基础设施层防御 (BP1、BP3、BP6、BP7)

在传统的数据中心环境中，您可以使用容量过剩、部署缓解系统或借助DDoS缓解服务清理流量等技术来缓解基础设施层DDoS攻击。DDoS开启后 AWS，系统会自动提供DDoS缓解功能；但您可以通过选择架构来优化应用程序的DDoS弹性，这些架构可以最好地利用这些功能，同时还允许您针对多余的流量进行扩展。

帮助缓解容量DDoS攻击的关键考虑因素包括确保有足够的传输容量和多样性可用，以及保护 AWS 资源（如 Amazon EC2 实例）免受攻击流量的侵害。

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，例如高达 100 Gbps 的网络带宽接口和增强的联网。这有助于防止已到达 Amazon EC2 实例的流量出现接口拥塞。与传统实施相比，支持增强联网的实例可提供更高的输入/输出 (I/O) 性能、更高的带宽和更低的CPU利用率。这提高了实例处理大量流量的能力，并最终使它们对每秒数据包 (pps) 负载具有很强的弹性。

为了实现这种高水平的弹性， AWS 建议使用亚马逊EC2专用实例，或者网络吞吐量更高、带有 “N” 后缀并支持网络带宽高达 100 Gbps 的增强联网的 A EC2 mazon 实例，`c6gn.16xlarge`以及 `c5n.18xlarge` /或金属实例（例如）。`c5n.metal`

有关支持 100 千兆位网络接口和增强联网的 Amazon EC2 实例的更多信息，请参阅亚马逊EC2实例类型。

增强联网所需的模块和必需的`enaSupport`属性集包含在 Amazon Linux 2 和最新版本的亚马逊 Linux 中AMI。因此，如果您在支持的实例类型上使用硬件虚拟机 (HVM) 版本的 Amazon Linux 启动实例，则您的实例已启用增强联网功能。有关更多信息，请参阅在 Linux 上测试是否启用了增强联网和增强联网。

EC2带有 Auto Scaling 功能的亚马逊 (BP7)

缓解基础设施和应用层攻击的另一种方法是大规模运营。如果您有 Web 应用程序，则可以使用负载均衡器将流量分配到大量配置过剩或配置为EC2自动扩展的 Amazon 实例。这些实例可以处理因任何原因而发生的突然流量激增，包括闪电人群或应用程序层DDoS攻击。您可以将 Amazon CloudWatch 警报设置为启动 Auto Scaling，以根据您定义的事件（例如CPU网络 I/O 甚至自定义指标）自动扩展您的 Amazon EC2 队列规模。RAM

当请求量意外增加时，这种方法可以保护应用程序的可用性。在应用程序中使用 Amazon CloudFront、Application Load Balancer、Classic 负载均衡器或网络负载均衡器时，TLS协商由分配 (Amazon CloudFront) 或负载均衡器处理。这些功能通过扩展以处理合法请求和TLS滥用攻击，帮助保护您的实例免受TLS基于攻击的影响。

有关使用亚马逊 CloudWatch 调用 Auto Scaling 的更多信息，请参阅监控您的 Auto Scaling 组和实例的亚马逊 CloudWatch 指标。

Amazon EC2 提供可调整大小的计算容量，因此您可以根据需求的变化快速向上或向下扩展。您可以通过扩展 Amazon A EC2 uto Scaling 组的大小自动向应用程序添加实例来进行水平扩展，也可以使用更大的EC2实例类型进行垂直扩展。

通过使用 Amazon RDS Proxy，您可以允许应用程序共享和共享数据库连接，以提高其扩展和处理不可预测的数据库流量激增的能力。 您也可以为 Amazon RDS 数据库实例启用存储自动缩放。有关更多信息，请参阅使用 Amazon RDS 存储自动扩展功能自动管理容量。

Elastic Load Balancin BP6 g (

大型DDoS攻击可能会使单个 Amazon EC2 实例的容量不堪重负。借助 Elastic Load Balancing (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过载的风险。Elastic Load Balancing 可以自动扩展，允许您在出现意想不到的额外流量（例如由于闪电人群或DDoS攻击而导致的额外流量）时管理更大的容量。对于在 Amazon 内部构建的应用程序VPC，根据您的应用程序类型，ELBs 需要考虑三种类型：应用程序负载均衡器 (ALB)、网络负载均衡器 (NLB) 和 Classic Load Balancer (CLB)。

对于 Web 应用程序，您可以使用 Application Load Balancer 根据内容路由流量，并且仅接受格式正确的 Web 请求。Application Load Balancer 可以阻止许多常见DDoS攻击，例如SYN洪水攻击或UDP反射攻击，从而保护您的应用程序免受攻击。当检测到这些类型的攻击时，Application Load Balancer 会自动扩展以吸收额外的流量。由于基础设施层攻击而导致的扩展活动对 AWS 客户来说是透明的，不会影响您的账单。

有关使用 Application Load B alancer 保护 Web 应用程序的更多信息，请参阅应用程序负载均衡器入门。

对于非HTTP/HTTPS应用程序，您可以使用 Network Load Balancer 以超低的延迟将流量路由到目标（例如 Amazon EC2 实例）。Network Load Balancer 的一个关键考虑因素是，通过有效侦听器到达负载均衡器的任何TCPSYN或UDP流量都将路由到您的目标，而不是被吸收，但这不适用于终止连接的 TLS-listeners。TCP对于带有TCP侦听器的网络负载均衡器，我们建议部署全球加速器来防范SYN洪水。

您可以使用 Shield Advanced 为弹性 IP 地址配置DDoS保护。将每个可用区的弹性 IP 地址分配给网络负载均衡器时，Shield Advanced 将对网络负载均衡器流量应用相关DDoS保护。

有关使用 Network Load Balancer 保护TCP和UDP应用程序的更多信息，请参阅网络负载均衡器入门。

> **Note**
>
> 根据安全组的配置，它要求使用安全组的资源使用连接跟踪来跟踪有关流量的信息，这可能会影响负载均衡器处理新连接的能力，因为跟踪的连接数量有限。
> 如果安全组配置包含接受来自任何 IP 地址（例如`0.0.0.0/0`或`::/0`）的流量的入口规则，但没有允许响应流量的相应规则，则安全组使用连接跟踪信息来允许发送响应流量。如果发生DDoS攻击，所跟踪的最大连接数可能会耗尽。要提高面向公众的 Application Load Balancer 或 Classic Load Balancer 的DDoS弹性，请确保将与您的负载均衡器关联的安全组配置为不使用连接跟踪（未跟踪的连接），这样流量就不受连接跟踪限制的约束。

为此，请为您的安全组配置一条规则，允许入站规则接受来自任何 IP 地址（`0.0.0.0/0`或`::/0`）的TCP流量，并在出站方向添加相应的规则，允许此资源发送响应流量（允许任何 IP 地址的出站范围`0.0.0.0/0`或`::/0`）所有端口（0-65535），这样就可以根据安全组规则而不是跟踪信息来允许响应流量。 使用此配置，Classic 和 Application Load Balancer 不受可能影响与其负载均衡器节点建立新连接的耗尽连接跟踪限制，并且允许其在DDoS发生攻击时根据流量的增加进行扩展。 有关未跟踪连接的更多信息，请访问：安全组连接跟踪：未跟踪的连接。

只有当DDoS流量来自安全组允许的来源时，避免安全组连接跟踪才会有所帮助——来自安全组中不允许的来源的DDoS流量不会影响连接跟踪。在这种情况下，无需重新配置安全组以避免连接跟踪，例如，如果您的安全组允许列表由您高度信任的 IP 范围组成，例如公司公司防火墙或可信VPN出口IPs或。CDNs

使用 AWS 边缘位置进行缩放 (BP1,BP3)

访问高度扩展、多样化的互联网连接可以显著提高您优化用户延迟和吞吐量、吸收DDoS攻击和隔离故障的能力，同时最大限度地减少对应用程序可用性的影响。 AWS 边缘站点提供了额外的网络基础设施层，可为使用亚马逊 CloudFront、全球加速器和 Amazon Route 53 的任何 Web 应用程序提供这些好处。借助这些服务，您可以在边缘全面保护运行的应用程序 AWS 区域。

在边缘交付 Web 应用程序 (BP1)

Amazon CloudFront 是一项可用于交付您的整个网站的服务，包括静态、动态、流媒体和交互式内容。即使您没有提供可缓存的内容，也可以使用永久连接和变量 time-to-live (TTL) 设置从您的源站卸载流量。使用这些 CloudFront 功能可以减少返回源站的请求和TCP连接数量，从而帮助保护您的 Web 应用程序免受HTTP洪水的侵害。

CloudFront 只接受格式良好的连接，这有助于防止许多常见DDoS攻击（例如SYN洪水攻击和UDP反射攻击）到达您的源头。DDoS攻击在靠近源头的地理位置上也是隔离的，这样可以防止流量影响其他位置。这些功能可以极大地提高您在大规模DDoS攻击期间继续向用户提供流量的能力。您可以使用 CloudFront 来保护互联网上 AWS 或其他地方的来源。

如果您使用亚马逊简单存储服务 (Amazon S3) 在互联网上提供静态内容， AWS 建议您使用亚马逊 CloudFront 来保护您的存储桶，它具有以下好处：

- 限制对 Amazon S3 存储桶的访问权限，使其不可公开访问。
- 确保查看者（用户）只能通过指定的 CloudFront 分配访问存储桶中的内容，也就是说，防止他们直接从存储桶或通过非预期的分发访问内容。 CloudFront

为此，请配置 CloudFront 为向 Amazon S3 发送经过身份验证的请求，并将 Amazon S3 配置为仅允许访问来自的经过身份验证的请求 CloudFront。 CloudFront 提供了两种向 Amazon S3 源发送经过身份验证的请求的方法：源访问控制 (OAC) 和源访问身份 (OAI)。我们建议使用，OAC因为它支持：

- 所有 Amazon S3 存储桶 AWS 区域，包括 2022 年 12 月之后推出的可选区域
- 使用 AWS KMS (SSE-KMS) 的 Amazon S3 服务器端加密
- 对 Amazon S3 的动态请求（ PUT 和 DELETE ）

有关OAC和的更多信息OAI，请参阅限制访问 Amazon S3 源。

有关使用 Amazon 保护和优化 Web 应用程序性能的更多信息 CloudFront，请参阅亚马逊入门 CloudFront。

使用 AWS 全球加速器保护远离源站的网络流量 (BP1)

Global Accelerator 是一项网络服务，可将用户流量的可用性和性能提高多达 60%。这是通过在离用户最近的边缘位置传入流量，然后通过 AWS 全球网络基础设施将其路由到您的应用程序来实现的，无论它是以单个还是多个应用程序运行。 AWS 区域

Global Accelerator 根据距离用户最近的性能将UDP流量路由TCP AWS 区域 到最佳端点。如果应用程序出现故障，Global Accelerator 会在 30 秒内故障转移到下一个最佳端点。Global Accelerator利用 AWS 全球网络的巨大容量以及与Shield的集成，例如无状态SYN代理功能，该功能可以挑战新的连接尝试，并且仅为合法的最终用户提供服务，以保护应用程序。

即使您的应用程序使用不支持的协议， CloudFront 或者您正在运行需要全局静态 IP 地址的 Web 应用程序，您也可以实施一种DDoS弹性架构，该架构具有许多与 Web 应用程序交付边缘最佳实践相同的优势。

例如，您可能需要最终用户可以将其添加到防火墙的允许列表中且不被任何其他 AWS 客户使用的 IP 地址。在这些场景中，您可以使用全球加速器来保护在 Application Load Balancer 上运行的 Web 应用程序，还可以结合使用 AWS WAF 来检测和缓解 Web 应用程序层请求洪水。

有关使用全球加速器保护和优化网络流量性能的更多信息，请参阅全球加速器入门。

边缘域名解析 (BP3)

主题

- 使用 Route 53 了解DNS可用性

- 配置 Route 53 以保护其免受NXDOMAIN攻击的成本

使用 Route 53 了解DNS可用性

Amazon Route 53 是一项高度可用且可扩展的域名系统 (DNS) 服务，可用于将流量引导至您的 Web 应用程序。它包括诸如流量流、Health Checks and Monitoring、基于延迟的路由和地理位置等高级功能。DNS这些高级功能允许您控制服务如何响应DNS请求，从而提高 Web 应用程序的性能并避免网站中断。它是唯一一个数据平面可用性达到 100% 的 AWS 服务SLA。

Amazon Route 53 使用诸如随机分片和任意广播条带化之类的技术，即使DNS服务成为攻击目标，也能帮助用户访问您的应用程序。DDoS

使用 shuffle 分片时，您的委托集中的每个域名服务器都对应于一组独特的边缘位置和互联网路径。这提供了更大的容错能力，并最大限度地减少了客户之间的重叠。如果委托集中的一个域名服务器不可用，则用户可以重试并从另一个边缘位置接收来自另一台域名服务器的响应。

Anycast 条带化允许通过最优的位置为每个DNS请求提供服务，从而分散网络负载并减少延迟。DNS这为用户提供了更快的响应。此外，Amazon Route 53 可以检测查询来源和DNS查询量中的异常情况，并对来自已知可靠用户的请求进行优先排序。

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 Amazon Route 53 入门。

配置 Route 53 以保护其免受**NXDOMAIN**攻击的成本

NXDOMAIN攻击发生在攻击者通常通过已知的 “良好” 解析器向托管区域发送大量请求以获取不存在的子域名时。这些攻击的目的可能是影响递归解析器的缓存和/或权威解析器的可用性，也可能是试图发现托管区域记录的一种DNS侦察形式。将 Route 53 用作权威解决程序可以降低可用性/性能影响的风险，但结果可能会导致每月 Route 53 的成本大幅增加。为了防止成本上涨，请利用 Route 53 的定价，当满足以下两个条件时，DNS查询是免费的：

- 查询中的域名或子域名（`example.com`或`store.example.com`）和记录类型（`A`）与别名记录相匹配。
- 别名目标是一个 AWS 资源，而不是另一个 Route 53 记录。

例如，创建通配符记录，`*.example.com`其类型A（别名）指向EC2实例、Elastic Load Balancer 或 CloudFront 分配等 AWS 资源，这样在查询时，将返回该资源的 IP，并且无需为查询付费。`qwerty12345.example.com`

应用层防御 (BP1,BP2)

到目前为止，本 paper 中讨论的许多技术都可有效缓解基础设施层DDoS攻击对应用程序可用性的影响。为了同时抵御应用程序层攻击，你需要实现一种架构，允许你专门检测、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DDoS缓解系统通常无法有效缓解复杂的应用层攻击。

检测和过滤恶意 Web 请求 (BP1,BP2)

当您的应用程序运行时 AWS，您可以利用 Amazon CloudFront （及其HTTP缓存功能）和 Shield 高级自动应用程序层保护来帮助防止在应用程序层DDoS攻击期间不必要的请求到达您的源。 AWS WAF

Amazon CloudFront

Amazon CloudFront 可以通过阻止非网络流量到达您的源站来帮助减少服务器负载。要向 CloudFront 应用程序发送请求，必须通过完整的握手使用有效的 IP 地址建立连接，该TCP握手无法伪造。此外，CloudFront 还可以自动关闭来自读取速度慢或写入速度慢的攻击者（例如 S lowloris）的连接。

CDN 缓存

CloudFront 允许您从 AWS 边缘位置提供动态内容和静态内容。通过从CDN缓存中提供可代理缓存的内容，可以防止请求在缓存期间从给定的边缘缓存节点到达您的源。TTL再加上对过期但可缓存的内容的请求崩溃，即使很短也TTL意味着在该内容的请求泛滥期间，到达来源的请求数量可以忽略不计。此外，启用诸如 CloudFront Origin Shield 之类的功能还可以进一步帮助减少源站的负载——你可以采取的任何措施来提高缓存命中率，都可能意味着有影响力和无影响力的请求洪水攻击之间的区别。

AWS WAF

通过使用 AWS WAF，您可以在全球 CloudFront 分发或区域资源上配置 Web 访问控制列表 (WebACLs)，以根据请求签名筛选、监控和阻止请求。要确定是允许还是阻止请求，您可以考虑诸如 IP 地址或原产国、请求中的某些字符串或模式、请求中特定部分的大小以及是否存在恶意SQL代码或脚本等因素。您还可以根据请求运行CAPTCHA拼图和静默客户端会话挑战。

两者都 AWS WAF 允许您设置地理限制，以阻止或允许来自选定国家/地区的请求。 CloudFront 这可以帮助阻止或限制来自您不希望为用户提供服务的地理位置的攻击。借助中精细的地理匹配规则语句 AWS WAF，您可以将访问权限控制到区域级别。

您可以使用 scope-down 语句来缩小规则评估的请求范围以节省成本，并使用 “标签” Web 请求来允许匹配请求的规则将匹配结果传达给稍后在同一 Web 中评估的规则。ACL选择此选项可在多个规则中重复使用相同的逻辑。

您还可以定义完整的自定义响应，包括响应代码、标头和正文。

要帮助识别恶意请求，请查看您的 Web 服务器日志或 AWS WAF用户的日志记录并请求采样。通过启用 AWS WAF 日志记录，您可以获得有关 Web 分析的流量的详细信息。ACL AWS WAF 支持日志过滤，允许您指定记录哪些 Web 请求以及哪些请求在检查后从日志中丢弃。

日志中记录的信息包括从您的 AWS 资源 AWS WAF 收到请求的时间、有关该请求的详细信息以及所请求的每条规则的匹配操作。

抽样请求提供有关过去三小时内符合您的 AWS WAF 规则之一的请求的详细信息。您可以使用此信息来识别潜在的恶意流量签名，并创建拒绝这些请求的新规则。如果您看到许多带有随机查询字符串的请求，请确保仅允许与应用程序缓存相关的查询字符串参数。此技术有助于缓解针对您的来源的缓存破坏攻击。

AWS WAF — 基于费率的规则

AWS 强烈建议在 5 分钟滑动窗口内收到的HTTP请求数量超过您定义的阈值时，使用中基于速率的规则自动屏蔽不良行为者的 IP 地址， AWS WAF 从而防止请求泛滥。违规的客户端 IP 地址将收到 403 禁止的响应（或配置的区块错误响应），并一直处于屏蔽状态，直到请求速率降至阈值以下。

建议对基于速率的规则进行分层，以提供增强的保护，这样您就可以：

- 基于速率的一揽子规则，可保护您的应用程序免受大规模HTTP洪水的侵害。
- 一个或多个基于费率的规则，用于保护比基于费率URIs的一揽子规则更严格的特定费率。

例如，您可以选择在 5 分钟内限制为 500 个请求的基于速率的一揽子规则（没有范围缩小语句），然后使用 scope-down 语句创建以下一个或多个限制低于 500（5 分钟内低至 100 个请求）的基于速率的规则：

- 使用诸如 “`if NOT uri_path contains '.'`” 之类的范围缩小语句保护您的网页，以便进一步保护对不带文件扩展名的资源请求。这还可以保护您的主页 (/)，这是一条经常被定位的URI路径。
- 使用范围缩小语句（例如 “”）保护动态端点 `if method exactly matches 'post' (convert lowercase)`
- 使用像 “” 这样的范围缩小来保护访问您的数据库或调用一次性密码 (OTP) 的繁重请求 `if uri_path starts_with '/login' OR uri_path starts_with '/signup' OR uri_path starts_with '/forgotpassword'`

“阻止” 模式下的基于速率是防范请求泛滥 defense-in-depth WAF配置的基石，也是批准 AWS Shield Advanced 成本保护请求的必要条件。我们将在以下各节中研究其他 defense-in-depth WAF配置。

AWS WAF — 知识产权声誉

要防止基于 IP 地址信誉的攻击，您可以使用 IP 匹配或使用托管规则来创建规则 AWS WAF。

亚马逊的 IP 信誉列表规则组包括基于亚马逊内部威胁情报的规则。这些规则寻找作为机器人、对 AWS 资源进行侦察或积极参与DDoS活动的 IP 地址。据观察，该AWSManagedIPDDoSList规则阻止了90%以上的恶意请求洪水。

匿名 IP 列表规则组包含用于阻止来自允许混淆查看者身份的服务的请求的规则。其中包括来自代理 VPNs、Tor 节点和云平台（不包括 AWS）的请求。

此外，您还可以使用安全自动化的 IP 列表解析器组件来使用第三方 IP 信誉列表作为 AWS WAF解决方案。

AWS WAF -智能威胁缓解

僵尸网络是一种严重的安全威胁，通常用于进行非法或有害的活动，例如发送垃圾邮件、窃取敏感数据、发起勒索软件攻击、通过欺诈性点击进行广告欺诈或发起分布式 denial-of-service (DDoS) 攻击。要防止机器人攻击，请使用AWS WAF 机器人控制托管规则组。该规则组提供了一个基本的 “通用” 保护级别，该级别为自我识别的机器人添加标签，验证普遍需要的机器人，检测高度可信的机器人签名，以及一个 “定向” 保护级别，用于增加对无法自我识别的高级机器人的检测。

有针对性的保护使用浏览器查询、指纹识别和行为启发式等高级检测技术来识别恶意的机器人流量，然后应用缓解控制，例如速率限制CAPTCHA和挑战规则操作。Targeted 还提供了速率限制选项，以强制执行类似人类的访问模式，并通过使用请求令牌来应用动态速率限制。有关更多详细信息，请参阅AWS WAF 机器人控制规则组。要检测和管理应用程序登录页面上的恶意接管企图，你可以使用 F AWS WAF raud Control 账户接管预防 (ATP) 规则组。规则组通过检查客户端发送到应用程序登录端点的登录尝试来实现此目的，还会检查您的应用程序对登录尝试的响应，以跟踪成功率和失败率。

账户创建欺诈是一种在线非法活动，攻击者试图创建一个或多个虚假账户。攻击者使用虚假账户进行欺诈活动，例如滥用促销和注册奖金、冒充他人以及网络攻击（例如网络钓鱼）。虚假账户的存在会损害您在客户中的声誉并面临财务欺诈，从而对您的业务产生负面影响。

您可以通过实施 Fraud Control 账户创建欺 AWS WAF 诈预防 (ACFP) 功能来监控和控制账户创建欺诈企图。 AWS WAF 在 AWS 托管式规则 规则组中提供此功能AWS ManagedRulesACFPRuleSet以及配套应用程序集成SDKs。

在AWS WAF 智能威胁缓解中详细了解这些保护措施。

自动缓解应用层DDoS事件 (BP1、、BP2) BP6

如果您已订阅 AWS Shield Advanced，则可以启用 Shield Advanced 自动应用层DDoS缓解功能。此功能可自动创建、评估和部署 AWS WAF 规则，以代表您缓解第 7 层DDoS事件。

AWS Shield Advanced 为与 WAF Web 关联的每个受保护资源建立流量基准ACL。明显偏离既定基线的流量将被标记为潜在DDoS事件。检测到事件后，会 AWS Shield Advanced 尝试识别构成该事件的 Web 请求的签名，如果识别出签名，则会创建 AWS WAF 规则以减少使用该签名的流量。

根据历史基准评估规则并认为规则是安全的，它们就会被添加到 Shield 管理的规则组中，您可以选择在计数模式还是阻止模式下部署规则。Shield Advanced 在确定事件已完全消退后会自动移除 AWS WAF 规则。

参与SRT（仅限 Shield 高级版订阅者）

此外，订阅 Shield Advanced 后，你可以使用 AWS SRT来帮助你创建规则，以缓解影响应用程序可用性的攻击。您可以授予对您账户 AWS Shield Advanced 和的 AWS SRT有限访问权限 AWS WAF APIs。 AWS SRT只有在您明确授权的情况下，才会访问这些内容APIs以对您的账户进行缓解措施。有关更多信息，请参阅本文档的支持章节。

您可以使用 AWS Firewall Manager 在整个组织中集中配置和管理安全 AWS WAF 规则，例如 AWS Shield Advanced 保护和规则。您的 AWS Organizations 管理帐户可以指定管理员帐户，该帐户有权创建 Firewall Manager 策略。这些策略允许您定义标准，例如资源类型和标签，以确定规则的应用位置。当您有多个账户并想要标准化保护时，这很有用。

有关以下内容的更多信息：

- AWS 托管式规则 有关 AWS WAF信息，请参AWS 托管式规则 阅 AWS WAF。
- 使用地理限制来限制对您的 CloudFront 分发内容的访问权限，请参阅限制内容的地理分布。
- 使用 AWS WAF，请参阅：
  - 入门 AWS WAF
  - 记录网络ACL流量信息
  - 查看 Web 请求示例
- 配置基于速率的规则，请参阅使用基于速率的规则保护网站和服务。 AWS WAF
- 如何使用 Firewall Manager 管理 AWS 资源中的规则部署，请参阅：
  - F@@ irewall Manager AWS WAF 策略入门。
  - Fi@@ rewall Manager Shield 高级策略入门。

减少攻击面

在设计 AWS 解决方案时，另一个重要的考虑因素是限制攻击者瞄准您的应用程序的机会。这个概念被称为减少攻击面。未暴露在互联网上的资源更难受到攻击，这限制了攻击者瞄准应用程序可用性的选项。

例如，如果您不希望用户直接与某些资源进行交互，请确保无法从 Internet 访问这些资源。同样，不要通过非通信所需的端口或协议接受来自用户或外部应用程序的流量。

在下一节中， AWS 提供了最佳实践，以指导您减少攻击面并限制应用程序的互联网暴露。

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 资源完全暴露在互联网上。

安全组和网络 ACLs (BP5)

Amazon Virtual Private Cloud (AmazonVPC) 允许您配置逻辑上隔离的部分，您可以在 AWS 云 其中启动您定义的虚拟网络中的 AWS 资源。

安全组和网络的ACLs相似之处在于，它们允许您控制对内部 AWS 资源的访问权限VPC。但是安全组允许您在实例级别控制入站和出站流量，而网络在VPC子网级别ACLs提供类似的功能。使用安全组或网络不收取额外费用ACLs。

您可以选择是在启动实例时指定安全组，还是稍后将该实例与安全组关联。除非您创建允许规则来允许流量，否则所有流向安全组的 Internet 流量都将被隐式拒绝。

例如，如果您在 Elastic Load Balancer 后面有 Amazon EC2 实例，则这些实例本身不必是可公开访问的，而应IPs仅具有私有性。相反，您可以使用允许访问 0.0.0.0/0（以避免连接跟踪问题——见下文）的安全组规则，以及目标组子网上的网络访问控制列表 (NACL)，为所需的目标侦听器端口提供 Elastic Load Balancance 访问权限，仅允许 Elastic Load Balancing IP 范围与实例通信。这可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。

创建网络时ACLs，可以指定允许和拒绝规则。如果您想明确拒绝某些类型的流量流向您的应用程序，则此功能非常有用。例如，您可以定义拒绝访问整个子网的 IP 地址（作为CIDR范围）、协议和目标端口。如果您的应用程序仅用于TCP流量，则可以创建一条规则来拒绝所有UDP流量，反之亦然。此选项在响应DDoS攻击时非常有用，因为它允许您在知道来源IPs或其他特征码时创建自己的规则来缓解攻击。

如果您已订阅 AWS Shield Advanced，则可以将弹性 IP 地址注册为受保护资源。DDoS可以更快地检测到针对已注册为受保护资源的弹性 IP 地址的攻击，从而缩短缓解攻击的时间。检测到攻击时，DDoS缓解系统会读取与目标弹性 IP 地址相对应的网络ACL，并在 AWS 网络边界而不是子网级别强制执行攻击。这可以显著降低您受到多种基础设施层DDoS攻击影响的风险。

有关配置安全组和网络ACLs以优化DDoS弹性的更多信息，请参阅如何通过减少攻击面来帮助做好DDoS攻击准备。

有关使用带有弹性 IP 地址的 Shield Advanced 作为受保护资源的更多信息，请参阅订阅步骤 AWS Shield Advanced。

保护你的起源 (BP1,BP5)

如果您使用亚马逊 CloudFront 的来源位于您的内部VPC，则可能需要确保只有您的 CloudFront 配送才能将请求转发到您的来源。借助 Edge-to-Origin 请求标头，在将请求 CloudFront 转发到您的源时，您可以添加或覆盖现有请求标头的值。您可以使用 Origin Custom Headers（例如`X-Shared-Secret`标头）来帮助验证向您的源发出的请求是否来自发送 CloudFront。

有关使用 Origin 自定义标头保护您的源的更多信息，请参阅向源请求添加自定义标头和限制对应用程序负载均衡器的访问。

有关实施示例解决方案以自动轮换源访问限制的 Origin 自定义标头值的指南，请参阅如何使用 AWS WAF 和 Secrets Manager 增强亚马逊 CloudFront 源安全性。

或者，您可以使用AWS Lambda功能自动更新您的安全组规则，使其仅允许 CloudFront 流量。这有助于确保恶意用户无法绕过 CloudFront 和 AWS WAF 访问您的 Web 应用程序，从而提高源站的安全性。

有关如何通过自动更新您的安全组以及`X-Shared-Secret`标题来保护您的来源的更多信息，请参阅如何自动更新您的亚马逊安全组 CloudFront 和 AWS WAF 使用 AWS Lambda。

但是，该解决方案涉及额外的配置和运行 Lambda 函数的成本。为了简化这一点，我们现在引入了AWS托管前缀列表，用于 CloudFront限制仅从 CloudFront面向源的 IP HTTPS 地址发送到您的来源的入站 HTTP /流量。 AWS-managed 前缀列表由创建 AWS 和维护，无需支付额外费用即可使用。您可以在您的 (AmazonVPC) 安全组规则、子网路由表、常用安全组规则以及任何其他可以使用托管前缀列表的 AWS 资源中引用托管前缀列表。 CloudFront AWS Firewall Manager

有关使用亚马逊 AWS托管前缀列表的更多信息 CloudFront，请参阅使用亚马逊托 AWS管前缀列表限制对您的来源的访问权限。 CloudFront

> **Note**
>
> 如本文档其他部分所述，在请求泛滥期间，依靠安全组来保护您的来源可能会将安全组连接跟踪作为潜在的瓶颈。除非您能够 CloudFront 使用启用缓存的缓存策略来过滤恶意请求，否则最好依靠前面讨论的 O rigin Custom Headers 来帮助验证向您的源发出的请求是否来自安全组 CloudFront，而不是使用安全组。将自定义请求标头与 Application Load Balancer 侦听器规则一起使用可防止由于跟踪限制而导致的限制，这可能会影响与负载均衡器建立新连接，从而允许应用程序负载均衡器在发生攻击时根据流量的增加进行扩展。DDoS

保护API端点 (BP4)

当你必须API向公众公开时，API前端就有可能成为DDoS攻击的目标。为了帮助降低风险，您可以使用 Amazon API Gateway 作为在亚马逊EC2或其他地方运行的应用程序的入口。 AWS Lambda通过使用 Amazon API Gateway，您无需在API前端使用自己的服务器，并且可以混淆应用程序的其他组件。通过使检测应用程序组件变得更加困难，可以帮助防止这些 AWS 资源成为DDoS攻击的目标。

使用 Amazon API Gateway 时，您可以从两种类型的API终端节点中进行选择。第一个是默认选项：通过 Ama CloudFront zon 分配访问的边缘优化的API终端节点。但是，该发行版由 API Gateway 创建和管理，因此您无法对其进行控制。第二种选择是使用区域API终端节点，该终端节点可以从部署您的RESTAPI终端节点进行访问。 AWS 区域 AWS 建议您使用第二种终端节点并将其与您自己的 Amazon CloudFront 分销相关联。这使您可以控制 Amazon CloudFront 分发并能够 AWS WAF 用于应用程序层保护。此模式使您可以访问 AWS 全球边缘网络中扩展的DDoS缓解能力。

使用 Amazon CloudFront 和 AWS WAF Amazon API Gateway 时，请配置以下选项：

- 为您的分配配置缓存行为，以将所有标头转发到 Gate API way 区域终端节点。通过这样做，CloudFront 会将内容视为动态内容并跳过缓存内容。
- 通过在 API Gateway 中设置API密钥值，将分配配置为包含 Origin 自定义标头 x-api-key，保护您的API网关免受直接访问。
- 通过为每种方法配置标准或突发速率限制，保护后端免受过多流量的侵害RESTAPIs。

有关使用 Amazon API Gateway APIs 进行创建的更多信息，请参阅 Amazon API Gateway 入门。

操作技巧

本 paper 中的缓解技术可帮助您设计本质上具有抵御DDoS攻击能力的应用程序。在许多情况下，了解DDoS攻击何时针对您的应用程序也很有用，这样您就可以采取缓解措施。本节讨论了解异常行为、警报和自动化、大规模管理保护以及寻求额外支持的最佳实践。 AWS

负载测试

使用我们的《负载测试应用程序》白皮书中的指南，定期对您的应用程序进行负载测试，包括预期和高于预期的流量水平，这样您就可以了解架构的有效性、Auto Scaling 策略的运作方式以及错误处理的运作方式。测试预期的流量放大和缩小，还要测试 “flash-crowd” 类型的行为。定期或在任何主要版本发布之前重新测试。对于第 3 层或第 4 层DDoS仿真测试，例如SYN洪水，请遵循我们的DDoS模拟测试政策。

指标和警报

作为最佳实践，您应该使用基础设施和应用程序监控工具来检查应用程序的可用性，以确保您的应用程序不受DDoS事件的影响，作为一种选择，您可以为资源配置应用程序和基础架构 Route 53 运行状况检查，以帮助改善DDoS事件检测。有关运行状况检查的更多信息，请参阅AWS WAF《Fi rewall Manager 和 Shield 高级开发者指南》。

当关键操作指标明显偏离预期值时，攻击者可能会试图瞄准应用程序的可用性。熟悉应用程序的正常行为意味着在检测到异常时可以更快地采取行动。Amazon CloudWatch 可以通过监控您运行的应用程序来提供帮助 AWS。例如，您可以收集和跟踪指标、收集和监控日志文件、设置警报以及自动响应 AWS 资源的变化。

如果您在设计应用程序时遵循DDoS弹性参考架构，那么常见的基础架构层攻击将在到达您的应用程序之前被阻止。如果您已订阅 AWS Shield Advanced，则可以访问许多 CloudWatch指标，这些指标可以表明您的应用程序已成为目标。

例如，您可以将警报配置为在DDoS攻击进行时通知您，这样您就可以检查应用程序的运行状况并决定是否参与攻击 AWS SRT。您可以配置该DDoSDetected指标以告知您是否检测到攻击。如果您想根据攻击量收到警报，也可以使用DDoSAttackBitsPerSecondDDoSAttackPacketsPerSecond、或DDoSAttackRequestsPerSecond指标。您可以通过 CloudWatch 与自己的工具集成或使用第三方提供的工具（例如 Slack 或 PagerDuty）来监控这些指标。

应用层攻击可以提升许多 Amazon CloudWatch 指标。如果您正在使用 AWS WAF，则可以使用 CloudWatch 来监控和激活已设置为允许、计数或阻止的 AWS WAF 请求数量增加时的警报。这

样，当流量超出您的应用程序所能处理的流量时，您就可以收到通知。您还可以使用跟踪的亚马逊 CloudFront、亚马逊 Route 53、Application Load Balancer、Network Load Balancer EC2、Amazon 和 Auto Scaling 指标 CloudWatch 来检测可能表明DDoS攻击的变化。

下表列出了常用于检测和应对DDoS攻击的 CloudWatch 指标的描述。

表 3-推荐的亚马逊 CloudWatch 指标

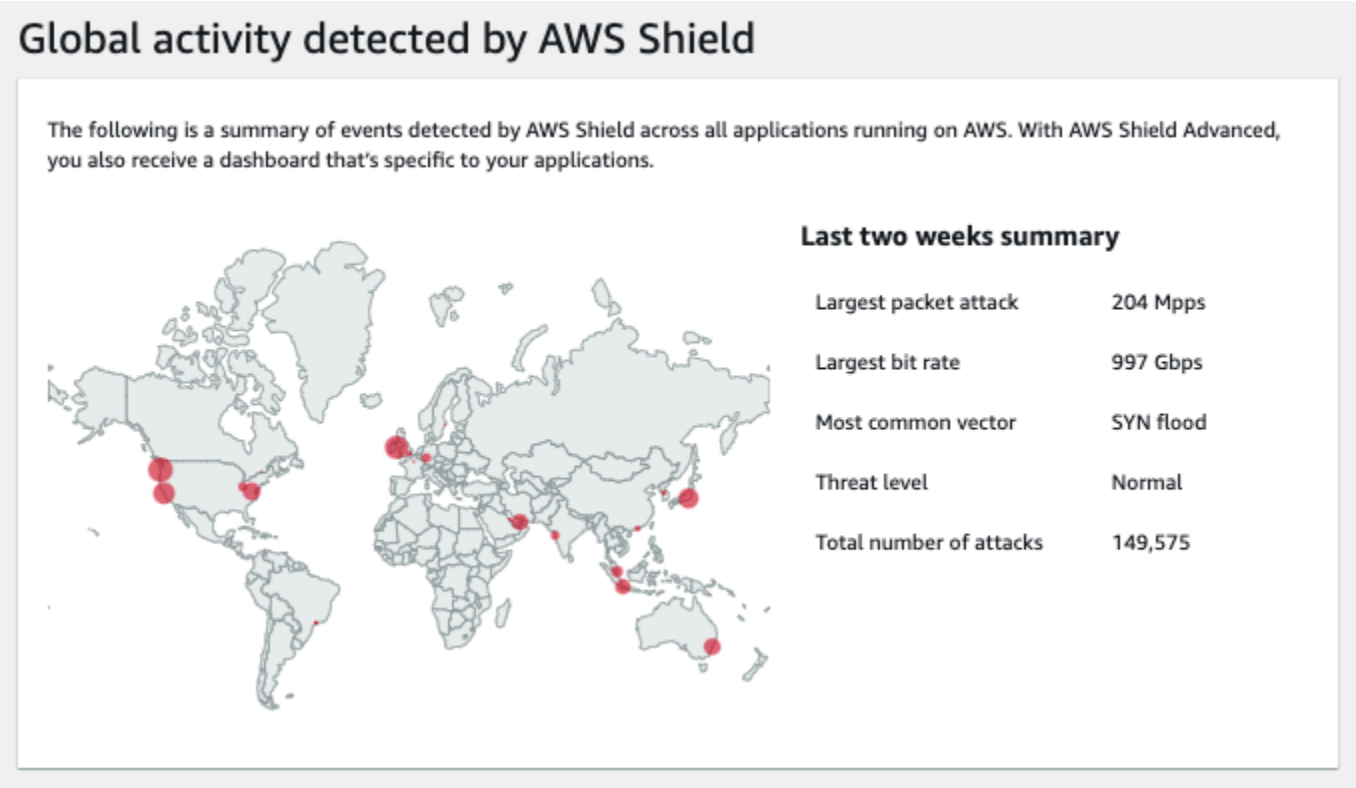
主题	指标	描述
AWS Shield Advanced	DDoSDetected	表示针对特定 Amazon 资源名称 (ARN) DDoS 的事件。
AWS Shield Advanced	DDoSAttackBitsPerSecond	在特定DDoS事件期间观察到的字节数ARN。此指标仅适用于第 3 层或第 4 层DDoS事件。
AWS Shield Advanced	DDoSAttackPacketsPerSecond	在特定DDoS事件期间观察到的数据包数量ARN。此指标仅适用于第 3 层或第 4 层DDoS事件。
AWS Shield Advanced	DDoSAttackRequestsPerSecond	在事件期间观察到的针对特定DDoS事件的请求数ARN。此指标仅适用于第 7 层DDoS事件，并且仅报告最重要的第 7 层事件。
AWS WAF	AllowedRequests	允许的 Web 请求数。
AWS WAF	BlockedRequests	阻止的 Web 请求数。
AWS WAF	CountedRequests	计数的 Web 请求数。
AWS WAF	PassedRequests	已通过的请求数。这仅用于通过规则组评估但不匹配任何规则组规则的请求。
Amazon CloudFront	Requests	HTTP/S 请求的数量。

主题	指标	描述
Amazon CloudFront	TotalErrorRate	HTTP状态码为4xx或的所有请求的百分比5xx。
Amazon Route 53	HealthCheckStatus	运行状况检查端点的状态。
应用程序负载均衡器	ActiveConnectionCount	从客户端到负载均衡器以及从负载均衡器到目标的活动并发TCP连接总数。
应用程序负载均衡器	ConsumedLCUs	您的负载均衡器使用的负载均衡器容量单位 (LCU) 的数量。
应用程序负载均衡器	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	负载均衡器生成的HTTP4xx或5xx客户端错误代码的数量。
应用程序负载均衡器	NewConnectionCount	从客户端到负载均衡器以及从负载均衡器到目标的新TCP连接总数。
应用程序负载均衡器	ProcessedBytes	负载均衡器处理的总字节数。
应用程序负载均衡器	RejectedConnectionCount	由于负载均衡器达到连接数上限被拒绝的链接的数量。
应用程序负载均衡器	RequestCount	已处理的请求数。
应用程序负载均衡器	TargetConnectionErrorCount	负载均衡器和目标之间连接建立不成功的次数。
应用程序负载均衡器	TargetResponseTime	从请求离开负载均衡器到收到来自目标的响应所经过的时间（以秒为单位）。
应用程序负载均衡器	UnHealthyHostCount	被视为未正常运行的目标数量。

主题	指标	描述
网络负载均衡器	ActiveFlowCount	从客户端到目标的并发TCP流（或连接）总数。
网络负载均衡器	ConsumedLCUs	您的负载均衡器使用的负载均衡器容量单位 (LCU) 的数量。
网络负载均衡器	NewFlowCount	一段时间内从客户端到目标的新TCP流（或连接）总数。
网络负载均衡器	ProcessedBytes	负载均衡器处理的总字节数，包括 TCP /IP 标头。
Global Accelerator	NewFlowCount	一段时间内从客户端到端点的新UDP流量TCP和已建立的流（或连接）总数。
Global Accelerator	ProcessedBytesIn	加速器处理的传入字节总数，包括 TCP /IP 标头。
Auto Scaling	GroupMaxSize	自动扩缩组的最大大小。
Amazon EC2	CPUUtilization	当前正在使用的已分配EC2计算单元的百分比。
Amazon EC2	NetworkIn	实例在所有网络接口上收到的字节数。

有关使用 Amazon CloudWatch 检测应用程序DDoS攻击的更多信息，请参阅 Amazon 入门 CloudWatch。

AWS 包括其他几个指标和警报，用于通知您攻击并帮助您监控应用程序的资源。 AWS Shield 控制台或API提供每个账户的事件摘要以及有关已检测到的攻击的详细信息。



检测到的全球活动 AWS Shield

此外，全球威胁环境控制面板还提供有关已检测到的所有DDoS攻击的摘要信息 AWS。这些信息可能有助于更好地了解更多应用程序群中的DDoS威胁以及攻击趋势，并与您可能观察到的攻击进行比较。

如果您已订阅 AWS Shield Advanced，服务控制面板会显示在受保护资源上检测到的事件的其他检测和缓解指标以及网络流量详细信息。 AWS Shield 从多个维度评估流向受保护资源的流量。检测到异常时， AWS Shield 会创建一个事件并报告观察到异常的流量维度。通过采取缓解措施，可以保护您的资源免于接收与已知DDoS事件签名匹配的过量流量和流量。

检测指标基于网络与受保护资源关联时采样的网络ACL流量或 AWS WAF 日志。缓解指标基于Shield的DDoS缓解系统观察到的流量。缓解指标可以更精确地衡量进入您的资源的流量。

网络贡献率最高的指标可以深入了解检测到的事件期间流量的来源。您可以查看容量最高的贡献者，并按协议、源端口和TCP标志等方面进行排序。贡献率最高的指标包括各个维度上在资源上观察到的所有流量的指标。它提供了其他指标维度，可用于了解事件期间发送到您的资源的网络流量。请记住，对于非反射第 3 层或第 4 层攻击，源 IP 地址可能已被欺骗，无法依赖。

服务仪表板还包含有关为缓解DDoS攻击而自动采取的操作的详细信息。这些信息使您可以更轻松地调查异常情况、探索流量维度，并更好地了解 Shield Advanced 为保护您的可用性而采取的措施。

日志记录

根据我们为应用程序所有者提供的日志和监控指南，在所有服务上启用有用的日志记录，以最大限度地提高可见性并协助进行故障排除。这包括但不限于：

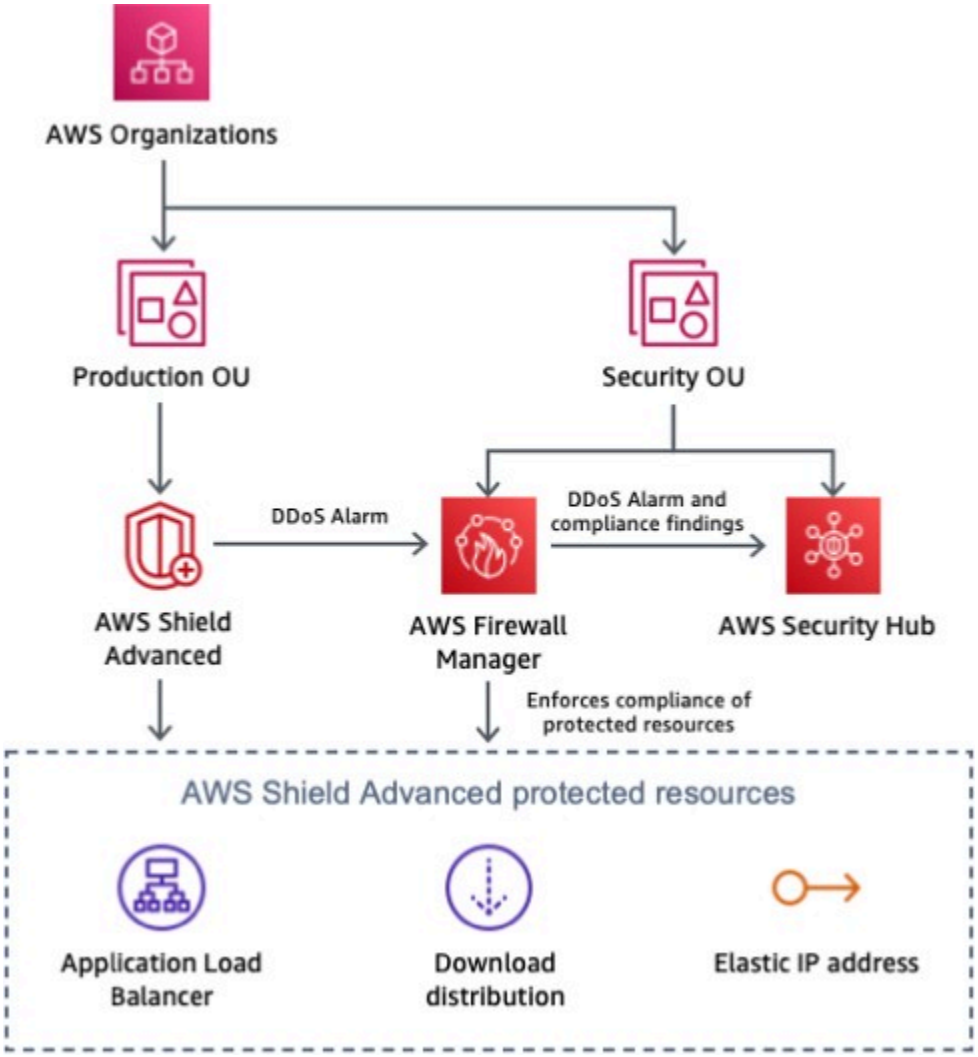
- AWS CloudTrail
- AWS WAF 日志
- CloudFront访问日志
- VPC流日志（请参阅记录和查看网络流量）-在包含的`tcp-flags`字段中包含字段以最大限度地提高可见性
- ELB访问日志 (ALB、CLB、NLB)
- Web 服务器HTTP访问日志
- 操作系统安全日志
- 应用程序日志

跨多个账户的可见性和保护管理

在您跨多个组件运行 AWS 账户 并且需要保护多个组件的情况下，使用使您能够大规模运营并减少运营开销的技术可以提高您的缓解能力。在管理多个账户中的 AWS Shield Advanced 受保护资源时，您可以使用 AWS Firewall Manager 和来设置集中监控 AWS Security Hub。借助 Firewall Manager，您可以创建一项安全策略，强制所有账户的DDoS保护合规性。您可以将这两项服务结合使用，跨多个账户管理受保护的资源，并集中监控这些资源。

Security Hub 自动与 Firewall Manager 集成，允许 Shield Advanced 客户在单个控制面板中查看安全发现以及其他高优先级安全警报和合规状态。

例如，当 Shield Advanced 检测到发往 AWS 账户 范围内任何受保护资源的异常流量时，此发现将在 Security Hub 控制台中可见。如果进行了配置，Firewall Manager 可以将资源创建为 Shield Advanced 保护的资源，然后在资源处于合规状态时更新 Security Hub，从而自动使其合规。



架构图显示了使用 Firewall Manager 和 AWS Shield Security Hub 监控受保护的资源

有关集中监控 Shield 保护资源的更多信息，请参阅为DDoS事件设置集中监控和自动修复不合规资源。

事件响应策略和操作手册

制定DDoS攻击事件响应策略并围绕该策略建立安全事件响应流程对所有组织都至关重要。推荐的方法是根据NIST建议的步骤（例如收集证据、缓解、恢复和进行事后分析）对您的应对手册进行建模。例如，提供了 Web 应用程序 DoS 或DDoS攻击的响应手册作为示例。其他资源可在《AWS 安全事件响应指南》中找到。

支持

如果您遇到攻击，也可以从评估威胁和审查应用程序架构方面的支持 AWS 中受益，或者您可能需要请求其他帮助。在实际事件DDoS发生之前，为攻击制定响应计划非常重要。本 paper 中概述的最佳实践旨在成为您在启动应用程序之前实施的主动措施，但仍可能发生针对您的应用程序的DDoS攻击。查看本节中的选项，以确定最适合您的场景的支持资源。您的客户团队可以评估您的用例和应用程序，并协助解决您遇到的具体问题或挑战。

如果你正在运行生产工作负载 AWS，可以考虑订阅 Business Support，它允许你全天候联系可以协助解决DDoS攻击问题的云支持工程师。如果您正在运行任务关键型工作负载，可以考虑使用 Enterprise Support，它可以打开关键案例并从高级云支持工程师那里获得最快的响应。

如果您已订阅 AWS Shield Advanced 并订阅了商业支持或企业支持，则可以配置 Shield 主动参与。它允许您配置运行状况检查、关联资源并提供全天候运营联系信息。当 Shield 检测到迹象DDoS并且您的应用程序运行状况检查显示出性能下降的迹象时， AWS SRT会主动与您联系。这是我们推荐的互动模式，因为它可以实现最快的 AWS SRT响应时间，甚至可以在 AWS SRT与您建立联系之前就开始故障排除。

有关更多信息，请参阅比较 支持 套餐。

主动参与功能要求您配置 Route 53 运行状况检查，该检查可以准确测量应用程序的运行状况，并与 Shield Advanced 保护的资源相关联。在 Shield 控制台中关联了 Route 53 运行状况检查后，Shield Advanced 检测系统就会使用运行状况检查状态作为应用程序运行状况的指标。Shield Advanced 中基于生命值的检测功能将确保在您的应用程序运行状况不佳时收到通知并更快地采取缓解措施。 AWS SRT将与您联系以排除运行状况不佳的应用程序是否成为DDoS攻击的目标，并根据需要采取其他缓解措施。

完成主动交战的配置包括在 Shield 控制台中添加联系方式。 AWS SRT将使用此信息与您联系。您最多可以配置十个联系人，如果您有任何特定的联系人要求或偏好，还可以提供其他备注。主动

项目联系人应全天候担任职务，例如安全运营中心或随时待命的个人。

您可以为所有资源或响应时间至关重要的特定关键生产资源启用主动互动。这是通过仅为这些资源分配运行状况检查来实现的。

您也可以使用支持 控制台（需要登录）或者 Support（API如果您有影响应用程序可用性的DDoS相关事件）创建 支持 案例，则可以升级到 Support。 AWS SRT

结论

本 paper 中概述的最佳实践可以帮助您构建DDoS弹性架构，通过防止许多常见的基础设施和应用层DDoS攻击来保护应用程序的可用性。您在设计应用程序时遵循这些最佳实践的程度将影响您可以缓解的DDoS攻击类型、向量和数量。您无需订阅DDoS缓解服务即可整合弹性。选择订阅后， AWS Shield Advanced 您将获得额外的支持、可见性、缓解和成本保护功能，从而进一步保护本已具有弹性的应用程序架构。

贡献者

本文档的贡献者包括：

- 罗德里戈·费罗尼，安全专家 AWS TAM
- 德米特里·诺维科夫，解决方案架构师 AWS
- Achraf Souk，解决方案架构师 AWS
- Joanna Knox，工程系 支持
- Anuj Butail，解决方案架构师 AWS
- Harith Gaddamanugu，边缘专家 SA AWS

延伸阅读

如需了解其他信息，请参阅：

- 实施指南 AWS WAF（AWS 白皮书）
- NIS301 — re: inForce 2023： AWS 威胁情报如何变成托管防火墙规则（视频）YouTube
- NET314-re: Invent 2022：使用（视频DDoS）构建具有弹性的应用程序 AWS Shield YouTube
- SEC321-re: Invent 2020：通过DDoS响应小组的升级抢占先机（视频）YouTube
- William Hill： AWS 2020 的高性能DDoS保护（YouTube视频）
- SEC407-re: Invent 2019：一种构建 Web 应用程序 defense-in-depth 的方法（视频）YouTube
- 2018 年@@ DDoS缓解措施的最佳实践（YouTube视频） AWS
- SID324— re: Invent 2017：云端自动DDoS响应（视频）YouTube
- CTD304 — re: Invent 2017：道琼斯和《华尔街日报》的管理流量激增之旅（视频）YouTube
- 缓解DDoS和应用层威胁（YouTube 视频）
- CTD310 — re: Invent 2017：生活在边缘，比你想象的要安全！借助 Amazon 强大建设（YouTube 视频）
- CloudFront AWS Shield、和 AWS WAF（YouTube 视频）

文档修订

要收到有关本白皮书更新的通知，请订阅该提RSS要。

变更	说明	日期
白皮书更新	添加OAC了 CloudFront 通DNS配符成本保护。扩展了对操作技术、缓存、基于速率的规则和托管规则组的讨论。将本地部署添加到架构图中，删除了重复内容，并澄清了文本以消除歧义。	2023 年 8 月 9 日
白皮书更新	为清晰起见进行了修改；已更新以包括最新建议和功能：安全组连接跟踪和 Shield Advanced 自动应用层DDoS缓解。	2022 年 4 月 13 日
白皮书更新	已更新以包含最新的建议和功能。 AWS Global Accelerator 是作为边缘全面保护的一部分添加的。 AWS Firewall Manager 用于集中监控DDoS事件并自动修复不合规的资源。	2021 年 9 月 21 日
白皮书更新	更新以澄清检测和过滤恶意 Web 请求 (BP1,BP2) 部分中的缓存破坏ELB以及 S cale to Asborce (BP6) 部分中的ALB用法。更新了标有 “区域选择” 的图表和表 2。如BP8。更新了包含更多细BP7节的部分。	2019 年 12 月 18 日

白皮书更新	已更新，将 AWS WAF 日志记录作为最佳实践。	2018 年 12 月 1 日
白皮书更新	已更新 AWS Shield，包括 AWS WAF 功能和相关的最佳实践。 AWS Firewall Manager	2018 年 6 月 1 日
白皮书更新	添加了规范性架构指南，并更新为包括 AWS WAF。	2016 年 6 月 1 日
初次发布	已发布白皮书。	2015 年 6 月 1 日

版权声明

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。