AWS 白皮书

实现 DDoS 弹性的 AWS 最佳实践

实现 DDoS 弹性的 AWS 最佳实践: AWS 白皮书

Table of Contents

摘要 1
- 摘要 1

简介：拒绝服务攻击 2
- 基础设施层攻击 3
  - UDP 反射攻击 4
  - SYN 泛洪攻击 4
- 应用层攻击 4

缓解技术 6
- DDoS 缓解的最佳实践 9
  - 基础设施层防御（BP1、BP3、BP6、BP7） 9
  - Amazon EC2 与 Auto Scaling（BP7） 10
  - Elastic Load Balancing（BP6） 11
- 利用 AWS 边缘站点进行扩展（BP1、BP3） 11
  - 边缘的 Web 应用程序交付（BP1） 11
  - 使用 AWS Global Accelerator 保护远离源的网络流量（BP1） 12
  - 边缘的域名解析（BP3） 12
- 应用层防御（BP1、BP2） 13
  - 检测和过滤恶意 Web 请求（BP1、BP2） 13

缩小攻击面 15
- 模糊 AWS 资源（BP1、BP4、BP5） 15
  - 安全组和网络访问控制列表（网络 ACL）（BP5） 15
  - 保护您的源（BP1、BP5） 16
  - 保护 API 终端节点（BP4） 16

操作技术 18
- 可见性 18
- 跨多个账户的可见性和保护管理 22
- 支持 23

总结 24

贡献者 25

资源 26

文档修订 27

声明 28

AWS实现 DDoS 弹性的最佳实践

发布日期：2021 年 9 月 21 日 (文档修订)

摘要

保护您的企业免受分布式拒绝服务（DDoS）攻击及其他网络攻击的影响非常重要。当务之急是，通过确保应用程序的可用性和响应能力来保持客户对您服务的信任。当您的基础设施必须进行扩展以应对攻击时，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 Internet 上的恶意分子。使用 AWS 提供的正确服务，这有助于确保高可用性、安全性和弹性。

在本白皮书中，AWS 为您提供了规范性 DDoS 指南，以提高在 AWS 上运行的应用程序弹性。其中包括 DDoS 弹性参考架构，它可用作帮助保护应用程序可用性的指南。本白皮书还介绍了不同的攻击类型，例如，基础设施层攻击和应用层攻击。AWS 解释了对管理每种攻击类型最有效的最佳实践。此外，还概述了适合 DDoS 缓解策略的服务和功能，并说明了如何使用每种服务和功能来帮助保护您的应用程序。

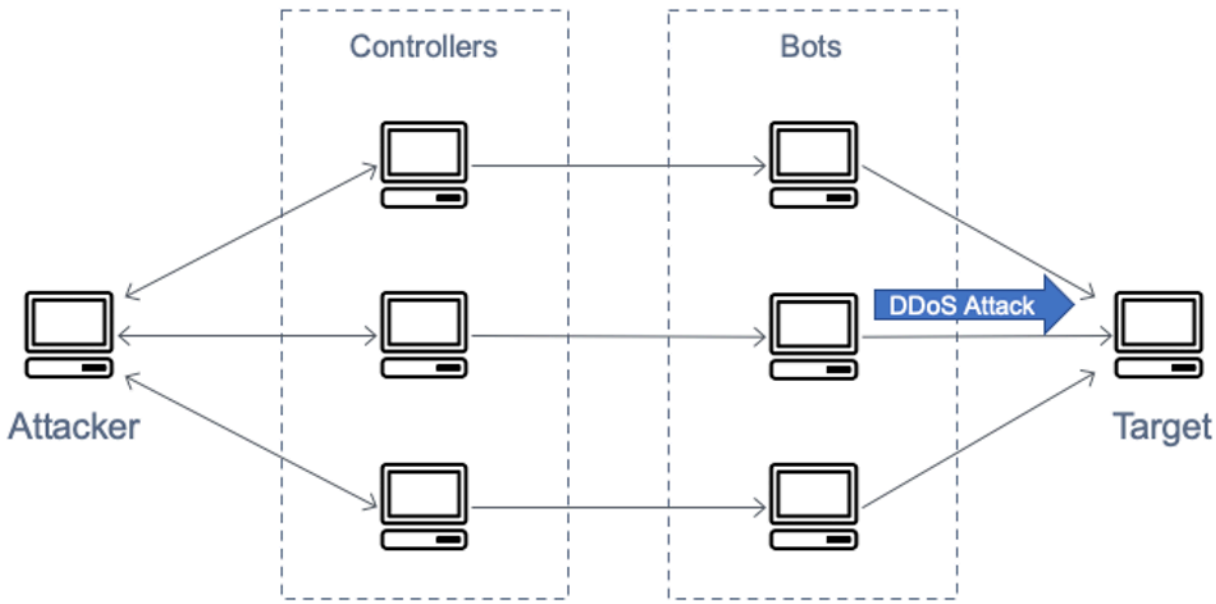
本白皮书面向熟悉联网、安全性和 AWS 基本概念的 IT 决策者和安全工程师。每一部分都有指向 AWS 文档的链接，该文档提供了有关最佳实践或功能的更多详细信息。

简介：拒绝服务攻击

拒绝服务（DoS）攻击是故意使用户无法访问网站或应用程序的攻击，例如，通过向其发送大量的网络流量。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。最简单的形式是，攻击者本人使用单一源对目标发起 DoS 攻击，如下图所示。

表 1：DoS 攻击示意图

在 DDoS 攻击中，攻击者使用多个源编排针对目标的攻击。这些源可能包括由受恶意软件感染的计算机、路由器、物联网设备和其他端点组成的分布式群组。下图显示了一个由受感染的主机组成的网络参与了攻击，它生成了大量数据包或请求，使目标不堪重负。



DDoS 攻击示意图

开放系统互连（OSI）模型中有七个层，开放系统互连（OSI）模型表中对它们进行了描述。DDoS 攻击最常见于第三、第四、第六和第七层。第三层和第四层攻击对应于 OSI 模型的网络层和传输层。在本白皮书中，AWS 将其统称为基础设施层攻击。第六层和第七层攻击对应于 OSI 模型的表示层和应用层。AWS 将这些统一作为应用层攻击来解决。以下各部分将讨论这些攻击类型的示例。

开放系统互连（OSI）模型

编号	层	单位	说明	媒介示例
7	应用	数据	应用程序的网络进程	HTTP 泛洪、DNS 查询泛洪
6	表示	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	传输	分段	端到端连接和可靠性	SYN 泛洪
3	网络	数据包	路径确定和逻辑寻址	UDP 反射攻击
2	数据链路	帧	物理寻址	不适用
1	物理	比特	媒体、信号和二进制传输	不适用

主题

- 基础设施层攻击
- 应用层攻击

基础设施层攻击

常见的 DDoS 攻击、用户数据报协议（UDP）反射攻击和同步（SYN）泛洪都属于基础设施层攻击。攻击者可以使用这些方法中的任何一种生成大量流量，从而使网络容量不堪重负或占用服务器、防火墙、入侵防御系统（IPS）或负载均衡器等系统上的资源。尽管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能够比入站流量泛滥更快地扩展容量。这种额外容量对于过滤或吸收攻击流量很有必要，从而释放系统和应用程序以响应合法的客户流量。

主题

- UDP 反射攻击
- SYN 泛洪攻击

UDP 反射攻击

用户数据报协议（UDP）反射攻击利用了 UDP 是无状态协议这一事实。攻击者可以伪造有效的 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 UDP 请求数据包的源 IP。UDP 数据包中包含伪造的源 IP，由攻击者将其发送到中间服务器。服务器遭到诱骗后，向目标受害者 IP 发送其 UDP 响应数据包，而不是将其发回给攻击者的 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。

放大因子是响应大小与请求大小的比值，它取决于攻击者使用的协议：
DNS、NTP、SSDP、CLDAP、Memcached、CharGen 或 QOTD。例如，DNS 的放大因子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，他们可以向攻击目标生成超过 3400 字节的有害流量。与其他攻击相比，UDP 反射攻击造成的流量更大。UDP 反射攻击图展示了反射策略和放大效果。

UDP 反射攻击

SYN 泛洪攻击

当用户连接到传输控制协议 (TCP) 服务（例如 Web 服务器）时，其客户端会发送 SYN 同步数据包。服务器在确认中返回 SYN-ACK 数据包，最后客户端以确认（ACK）数据包作为响应，完成了预期的三向握手。下图说明了这种典型的握手。

SYN 三向握手

在 SYN 泛洪攻击中，恶意客户端发送大量 SYN 数据包，但从未发送最终的 ACK 数据包来完成握手。服务器需要等待对半开放的 TCP 连接的响应，最终会耗尽容量来接受新的 TCP 连接。这会使新用户无法连接到服务器。该攻击试图占用可用的服务器连接，使资源无法用于合法连接。虽然 SYN 泛洪可能高达数百 Gbps，但攻击的目的不是增加 SYN 流量。

应用层攻击

攻击者可以通过使用第 7 层或应用层攻击来攻击应用程序本身。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，从而使应用程序不可用或无法响应合法用户。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。这可能使攻击难以检测和缓解。应用层攻击的示例包括 HTTP 泛洪、缓存破坏攻击和 WordPress XML-RPC 泛洪。

在 HTTP 泛洪攻击中，攻击者发送看似来自 Web 应用程序有效用户的 HTTP 请求。有些 HTTP 泛洪以特定资源为目标，而更复杂的 HTTP 泛洪则试图模拟人类与应用程序的交互。这可能会增加诸如请求速率限制等常见缓解技术的使用难度。

缓存破坏攻击是一种 HTTP 泛洪攻击，它在查询字符串中使用变体来规避内容分发网络（CDN）缓存。CDN 无法返回缓存的结果，而是必须为每个页面请求联系源服务器，而这些源获取会给应用程序 Web 服务器带来额外压力。

通过 WordPress XML-RPC 泛洪攻击（也称为 WordPress pingback 泛洪），攻击者将目标锁定在 WordPress 内容管理软件上托管的网站。攻击者滥用 XML-RPC API 函数生成大量 HTTP 请求。pingback 功能允许在 WordPress 上托管的网站（站点 A）通过站点 A 已经创建的指向站点 B 的链接通知另一个 WordPress 站点（站点 B）。然后，站点 B 尝试获取站点 A 以验证该链接是否存在。在 pingback 泛洪中，攻击者滥用此功能，导致站点 B 攻击站点 A。此类攻击具有明确的特征：HTTP 请求标头的 User-Agent 中通常存在 WordPress。

还有其他形式的恶意流量可能会影响应用程序的可用性。Scraper 机器人会自动尝试访问 Web 应用程序，以窃取内容或记录竞争信息（例如定价）。暴力攻击和凭证填充攻击经过编程，旨在获得对应用程序安全区域的未经授权的访问。严格来说，这些不是 DDoS 攻击；但其自动化性质看起来类似于 DDoS 攻击，可通过实施本文中介绍的一些相同最佳实践来缓解这些攻击。

应用层攻击还可以针对域名系统（DNS）服务。这些攻击中最常见的是 DNS 查询泛洪，其中攻击者使用许多格式正确的 DNS 查询来耗尽 DNS 服务器的资源。这些攻击还可以包括缓存破坏部分，其中攻击者将子域字符串随机化，以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，这会加剧攻击。

如果通过传输层安全性（TLS）传送 Web 应用程序，则攻击者也可以选择攻击 TLS 协商流程。TLS 的计算成本很高，因此，攻击者通过在服务器上生成额外工作负载，将无法读取的数据（或无法理解的（密文））作为合法握手来处理，从而降低服务器的可用性。在这种攻击的一种变体中，攻击者完成了 TLS 握手，但不断地重新协商加密方法。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。通过使用包含特定服务的 AWS 架构（在以下各部分中有介绍），以及针对用户和应用程序之间网络流的每个部分实施其他最佳实践，可以进一步提高 DDoS 弹性。

所有 AWS 客户都可从 AWS Shield Standard 的自动防护功能中获益，不需要额外支付费用。AWS Shield Standard 可以抵御以您的网站或应用程序为目标的最为常见、经常发生的网络和传输层 DDoS 攻击。此防护功能始终处于开启状态，经过预配置，静态，且不提供报告或分析。它适用于所有 AWS 服务和每个 AWS 区域。在 AWS 区域中，系统会检测到 DDoS 攻击，Shield Standard 系统会自动确定流量基准，识别异常情况，并在必要时创建缓解措施。您可以使用 AWS Shield Standard 作为 DDoS 弹性架构的一部分，来保护 Web 和非 Web 应用程序。

您还可以利用从边缘站点运行的 AWS 服务（例如 Amazon CloudFront、Global Accelerator 和 Route 53）来构建全面的可用性保护，抵御所有已知的基础设施层攻击。这些服务是 AWS Global Edge Network 的一部分，在为分布于世界各地边缘站点的任何类型的应用程序流量提供服务时，可以提高应用程序的 DDoS 弹性。您可以在任何 AWS 区域运行应用程序，使用这些服务来保护应用程序的可用性，并为合法终端用户优化应用程序的性能。

使用 Amazon CloudFront、Global Accelerator 和 Amazon Route 53 的好处包括：

- 通过 AWS Global Edge Network 访问 Internet 和 DDoS 缓解容量。这对于缓解更大范围的容量耗尽攻击非常有用，这种攻击可以达到 TB 规模。
- AWS ShieldDDoS 缓解系统与AWS边缘服务集成，将缓解时间从几分钟缩短到几秒钟。
- 无状态 SYN 泛洪缓解技术在将传入连接传递给受保护的服务之前，代理并验证此类连接。这样可确保只有有效连接才能到达您的应用程序，同时保护您的合法终端用户免受误报丢失的影响。
- 自动流量工程系统，可分散或隔离大范围的容量耗尽 DDoS 攻击的影响。所有这些服务都会在攻击到达源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。
- 应用层防御与 AWS WAF 结合使用时，不需要更改当前应用程序架构（例如，在 AWS 区域或本地部署数据中心中）。

AWS 的入站数据传输不收取任何费用，您无需为通过 AWS Shield 缓解的 DDoS 攻击流量付费。以下架构图包含 AWS Global Edge Network 服务。

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。最佳实践汇总表概述了这些服务及其可提供的功能。AWS 已使用最佳实践指标（BP1、BP2）标记了每项服务，方便在

本文档中参考。例如，下一部分将讨论 Amazon CloudFront 和 Global Accelerator 提供的功能，其中包括最佳实践指标 BP1。

表 2 – 最佳实践汇总

AWS 边缘	AWS 区域					
	将 Amazon CloudFront（BP1）与 AWS WAF（BP2）结合使用	使用 Global Accelerator（BP1）	使用 Amazon Route 53（BP3）	将 Elastic Load Balancing（BP6）与 AWS WAF（BP2）结合使用	在 Amazon VPC 中使用安全组和网络 ACL（BP5）	使用 Amazon EC2 Auto Scaling（BP7）
第 3 层（例如 UDP 反射）攻击缓解	✓	✓	✓	✓	✓	✓
第 4 层（例如 SYN 泛洪）攻击缓解	✓	✓	✓	✓		
第 6 层（例如 TLS）攻击缓解	✓	✓	✓	✓		
缩小攻击面	✓	✓	✓	✓	✓	
扩展以吸收应用层流量	✓	✓	✓	✓	✓	✓
第 7 层（应用层）攻击缓解	✓	✓(*)	✓	✓	✓(*)	✓(*)

AWS 边缘	AWS 区域					
地理隔离以及分散多余流量和更大的 DDoS 攻击	✓	✓	✓			
✓(*)：如果将 AWS WAF 与 Application Load Balancer 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。

客户将根据以下条件获得量身定制的检测：

- 应用程序的特定流量模式。
- 抵御第 7 层 DDoS 攻击，包括 AWS WAF，不收取额外费用。
- 获得 AWS SRT 提供的全天候专业支持。
- 通过 AWS Firewall Manager 集中化管理安全策略。
- 成本保护，防止因与 DDoS 相关的使用峰值而产生的扩缩费用。

这项可选 DDoS 缓解服务有助于保护托管在任何 AWS 区域的应用程序。该服务在全球范围内可用于 CloudFront、Route 53 和 Global Accelerator。使用带有弹性 IP 地址的 Shield Advanced，可保护 Network Load Balancer（NLB）或 Amazon EC2 实例。

使用 AWS Shield Advanced 的好处包括：

- 访问 AWS SRT，获取有关缓解影响应用程序可用性的 DDoS 攻击的帮助。
- 通过使用 AWS Management Console、API 和 Amazon CloudWatch 指标与警报，了解 DDoS 攻击。
- 访问过去 13 个月内所有 DDoS 事件的历史记录。

- 访问 AWS Web 应用程序防火墙（AWS WAF），无需额外费用即可缓解应用层 DDoS 攻击（与 Amazon CloudFront 或 Application Load Balancer 一起使用时）。
- 与 AWS WAF 一起使用时，Web 流量属性的自动基准化。
- 无需额外费用即可访问 AWS Firewall Manager，以自动实施策略。
- 敏感检测阈值可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，可以缩短针对 Amazon EC2 或 Network Load Balancer 的攻击缓解时间。
- 成本保护，使您能够申请有限的退款，以补偿因 DDoS 攻击而产生的与扩缩相关的费用。
- 特定于 AWS Shield Advanced 客户的增强服务等级协议。
- 当检测到 Shield 事件时，AWS SRT 会主动参与。
- 使您能够绑定资源的保护组，通过将多个资源作为单个单元处理，为您提供一种自助方式来自定义应用程序的检测和缓解范围。资源分组可以提高检测的准确性，最大限度地减少误报，简化对新创建的资源的自动保护，并缩短缓解针对构成单个应用程序的许多资源的攻击时间。有关保护组的信息，请参阅 Shield Advanced 保护组。

有关 AWS Shield Advanced 功能的完整列表以及有关 AWS Shield 的详细信息，请参阅 AWS Shield 的工作原理。

主题

- DDoS 缓解的最佳实践
- 利用 AWS 边缘站点进行扩展（BP1、BP3）
- 应用层防御（BP1、BP2）

DDoS 缓解的最佳实践

在以下各部分，将更深入地介绍每条建议的 DDoS 缓解最佳实践。有关为静态或动态 Web 应用程序构建 DDoS 缓解层的易于实施快速指南，请参阅如何帮助保护动态 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，您可以通过使用诸如过度配置容量、部署 DDoS 缓解系统或在 DDoS 缓解服务的帮助下清理流量等技术来缓解基础设施层 DDoS 攻击。在 AWS 中，系统会自动提供 DDoS 缓解功能；但您可以进行架构选择，以最好地利用这些功能，并允许您针对过多流量进行扩展，从而优化应用程序的 DDoS 弹性。

帮助缓解容量耗尽 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，及保护 AWS 资源（如 Amazon EC2 实例）免受攻击流量的影响。

某些 Amazon EC2 实例类型支持可更轻松地处理大量流量的功能，例如高达 100Gbps 网络带宽接口和增强型联网。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，支持增强型联网的实例可提供更高的 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，从而提高其对每秒数据包数（pps）负载的弹性。

要实现这种高水平的弹性，AWS 建议使用具有 N 后缀且网络吞吐量更高的 Amazon EC2 专用实例或 Amazon EC2 实例，此类实例支持网络带宽高达 100Gbps 的增强型联网，例如 c6gn.16xlarge 和 c5n.18xlarge 或裸机实例（如 c5n.metal）。

要详细了解支持 100Gb 网络接口和增强型联网的 Amazon EC2 实例，请参阅 Amazon EC2 实例类型。

增强型联网所需的模块和所需的 enaSupport 属性集包含在 Amazon Linux 2 和最新版本的 Amazon Linux AMI 中。因此，如果使用 HVM 版本的 Amazon Linux 在支持的实例类型上启动实例，则已为您的实例启用增强型联网。有关详细信息，请参阅测试是否启用了增强型联网。要详细了解如何启用增强型联网，请参阅 Linux 上的增强型联网。

Amazon EC2 与 Auto Scaling（BP7）

缓解基础设施和应用层攻击的另一种方法是大规模操作。如果您有 Web 应用程序，则可以使用负载均衡器，将流量分配到过度预置或配置为自动扩展的许多 Amazon EC2 实例。这些实例可以处理由于任何原因而导致的突发流量激增，包括闪族涌入或应用层 DDoS 攻击。您可以将 Amazon CloudWatch 警报设置为启动 Auto Scaling，以便根据您定义的事件（如 CPU、RAM、网络 I/O 甚至自定义指标）自动扩展 Amazon EC2 机群的大小。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。将 Amazon CloudFront、Application Load Balancer、Classic Load Balancer 或 Network Load Balancer 用于应用程序时，TLS 协商由分配（Amazon CloudFront）或负载均衡器处理。这些功能可扩展以处理合法请求和 TLS 滥用攻击，从而帮助保护您的实例免受基于 TLS 的攻击的影响。

有关使用 Amazon CloudWatch 调用 Auto Scaling 的更多信息，请参阅监控 Auto Scaling 组和实例的 Amazon CloudWatch 指标。

Amazon EC2 提供可调整大小的计算容量，以便您在需求变化时快速纵向扩展或缩减。您可以通过扩缩 Amazon EC2 Auto Scaling 组的大小自动向应用程序添加实例来进行横向扩展，也可以使用较大的 EC2 实例类型进行纵向扩展。

Elastic Load Balancing（BP6）

大型 DDoS 攻击可能会使单个 Amazon EC2 实例的容量不堪重负。使用 Elastic Load Balancing（ELB），您可以通过在许多后端实例之间分发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，由于闪族涌入或 DDoS 攻击）时管理更大容量。对于在 Amazon VPC 内构建的应用程序，根据您的应用程序类型，有三种类型的 ELB 供考虑：Application Load Balancer（ALB）、Classic Load Balancer（CLB）和 Network Load Balancer（NLB）。

对于 Web 应用程序，您可以使用 Application Load Balancer 根据内容路由流量，并仅接受格式正确的 Web 请求。Application Load Balancer 可阻止许多常见的 DDoS 攻击（例如 SYN 泛洪或 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流量。基础设施层攻击导致的扩缩活动对 AWS 客户透明，不会影响您的账单。

要详细了解如何使用 Application Load Balancer 保护 Web 应用程序，请参阅 Application Load Balancer 入门

对于基于 TCP 的应用程序，您可以使用 Network Load Balancer 以超低延迟将流量路由到目标（例如 Amazon EC2 实例）。使用 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流量都将路由到您的目标，而不是被吸收。您可以使用 Shield Advanced 为弹性 IP 地址配置 DDoS 防护。当每个可用区向 Network Load Balancer 分配弹性 IP 地址时，Shield Advanced 将对 Network Load Balancer 流量应用相关的 DDoS 防护。

要详细了解如何使用 Network Load Balancer 保护 TCP 应用程序，请参阅 Network Load Balancer 入门

利用 AWS 边缘站点进行扩展（BP1、BP3）

访问高度扩展、多样化的 Internet 连接可以显著提高您优化延迟和用户吞吐量、吸收 DDoS 攻击以及隔离故障的能力，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网络基础设施层，为使用 Amazon CloudFront、Global Accelerator 和 Amazon Route 53 的任何 Web 应用程序提供这些优势。借助这些服务，您可以在边缘全面保护从 AWS 区域运行的应用程序。

边缘的 Web 应用程序交付（BP1）

Amazon CloudFront 是一种服务，可用于交付您的整个网站，包括静态、动态、流媒体和交互内容。持久连接和可变存活时间（TTL）设置可用于从源分载流量，即使您没有提供可缓存的内容也是如此。使用这些 CloudFront 功能可减少返回源的请求和 TCP 连接的数量，有助于保护您的 Web 应用程序免

受 HTTP 泛洪的影响。CloudFront 仅接受格式正确的连接，以防止许多常见的 DDoS 攻击（如 SYN 泛洪和 UDP 反射攻击）到达您的源。此外，DDoS 攻击在地理上与源相隔离，这可防止流量影响其他位置。这些功能都可以极大地提高您在大型 DDoS 攻击期间继续为用户提供流量的能力。您可以使用 CloudFront 来保护 AWS 或 Internet 上其他位置的源。

如果您使用 Amazon S3 在 Internet 上提供静态内容，AWS 建议您使用 Amazon CloudFront 来保护您的存储桶。您可以使用源访问标识（OAI）来确保用户只能使用 CloudFront URL 访问您的对象。

有关 OAI 的更多信息，请参阅使用源访问标识限制对 Amazon S3 内容的访问。

要详细了解如何使用 Amazon CloudFront 保护和优化 Web 应用程序性能，请参阅 CloudFront 入门。

使用 AWS Global Accelerator 保护远离源的网络流量（BP1）

Global Accelerator 是一项联网服务，最多可将用户流量的可用性和性能提高 60%。为此，可通过在距离用户最近的边缘站点传入流量，然后通过 AWS 全球网络基础设施将流量路由到您的应用程序，无论该应用程序是在单个还是多个 AWS 区域中运行。

Global Accelerator 根据距离用户最近的 AWS 区域的性能，将 TCP 和 UDP 流量路由到最佳端点。如果应用程序出现故障，Global Accelerator 会在 30 秒内提供到下一个最佳端点的故障转移。Global Accelerator 利用 AWS 全球网络的巨大容量以及与 Shield 的集成（例如，挑战新连接尝试且仅为合法终端用户提供服务的无状态 SYN 代理功能）来保护应用程序。

即使您的应用程序使用 CloudFront 不支持的协议，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 DDoS 弹性架构，以提供与边缘 Web 应用程序交付最佳实践相同的许多好处。例如，您可能需要终端用户可添加到其防火墙中允许列表的 IP 地址，而其他任何 AWS 客户都不会使用这些地址。在这些情况下，您可以使用 Global Accelerator 保护在 Application Load Balancer 上运行的 Web 应用程序，并结合使用 AWS WAF 来检测和缓解 Web 应用层请求泛洪。

要详细了解如何使用 Global Accelerator 保护和优化网络流量性能，请参阅 Global Accelerator 入门。

边缘的域名解析（BP3）

Amazon Route 53 是一种高度可用且可扩展的域名系统（DNS）服务，可用于将流量定向到您的 Web 应用程序。它包括许多高级功能，例如流量、运行状况检查和监控、基于延迟的路由和地理 DNS。这些高级功能允许您控制服务响应 DNS 请求的方式，以提高 Web 应用程序的性能并避免站点中断。

Amazon Route 53 使用随机分区和任播条带化等技术，即使 DNS 服务成为 DDoS 攻击的目标，这些技术也可以帮助用户访问您的应用程序。

使用随机分区，您的委托集中的每个名称服务器都对应一组唯一的边缘站点和 Internet 路径。这可提供更强的容错能力并尽可能减少客户之间的重叠。如果委托集中的一个名称服务器不可用，则用户可以重试并接收其他边缘站点中的另一个名称服务器的响应。

任播条带化允许在最佳位置处理每个 DNS 请求，从而分散网络负载并减少 DNS 延迟。这为用户提供了更快的响应。此外，Amazon Route 53 还可以检测 DNS 查询的来源和数量异常，并优先处理来自已知可靠的用户的请求。

要详细了解如何使用 Amazon Route 53 将用户路由到您的应用程序，请参阅 Amazon Route 53 入门。

应用层防御（BP1、BP2）

本白皮书到目前为止讨论的许多技术都可以有效地减轻基础设施层 DDoS 攻击对应用程序可用性的影响。为了抵御应用层攻击，您需要实施一种架构，使您能够专门检测、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 缓解系统在缓解复杂的应用层攻击方面通常无效。

检测和过滤恶意 Web 请求（BP1、BP2）

当您的应用程序在 AWS 上运行时，您可以同时利用 Amazon CloudFront 和 AWS WAF 来防御应用层 DDoS 攻击。

Amazon CloudFront 允许您缓存静态内容，并从 AWS 边缘站点提供这些内容，从而帮助减少源的负载。它还可以通过防止非 Web 流量到达源，来帮助减少服务器负载。此外，CloudFront 还可以自动关闭来自慢速读取或慢速写入攻击者（例如 Slowloris）的连接。

通过使用 AWS WAF，您可以在 CloudFront 分配或 Application Load Balancer 上配置 Web 访问控制列表（Web ACL），以便根据请求签名筛选和阻止请求。每个 Web ACL 都包含一些规则，您可以将这些规则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，例如统一资源标识符（URI）、查询字符串、HTTP 方法或标头键。此外，通过使用 AWS WAF 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，您可以自动阻止恶意分子的 IP 地址。

来自违规客户端 IP 地址的请求将收到 403 禁止访问错误响应，并一直处于阻止状态，直到请求速率降至阈值以下。这有助于缓解伪装成常规 Web 流量的 HTTP 泛洪攻击。要阻止基于 IP 地址信誉的攻击，您可以使用 IP 匹配条件创建规则，或使用 AWS Marketplace 中卖方提供的 AWS WAF 托管规则。AWS WAF 直接将 AWS 托管规则作为托管式服务提供，您可以在其中选择 IP 信誉规则组。Amazon IP 声誉列表规则组包含基于 Amazon 内部威胁情报的规则。如果您想阻止通常与自动程序或其他威胁相关联的 IP 地址，此规则组非常有用。此匿名 IP 列表包含用于阻止来自以下服务的请求的规则：这些服务允许对查看者身份进行模糊处理。其中包括来自 VPN、代理、Tor 节点和云平台

（包括 AWS）的请求。AWS WAF 和 CloudFront 还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。这有助于阻止来自您不希望为用户提供服务的地理位置的攻击。

要帮助识别恶意请求，请查看 Web 服务器日志或使用 AWS WAF 日志记录和采样请求功能。通过启用 AWS WAF 日志记录，您可以获得有关 Web ACL 分析的流量的详细信息。AWS WAF 支持日志筛选，允许您指定在检查后记录哪些 Web 请求以及哪些请求将从日志中丢弃。

日志中记录的信息包括 AWS WAF 从您的 AWS 资源收到请求的时间、请求的相关详细信息以及所请求的每个规则的匹配操作。采样请求提供过去三个小时内与您的某一 AWS WAF 规则相匹配的请求的详细信息。您可以使用此信息来识别潜在恶意流量签名，并创建新规则来拒绝这些请求。如果您看到许多请求带有随机查询字符串，请确保只允许与应用程序缓存相关的查询字符串参数。此技术可帮助缓解针对源的缓存破坏攻击。

如果您已订阅 AWS Shield Advanced，可以与 AWS Shield 响应团队（SRT）联系，帮助您创建规则来缓解损害应用程序可用性的攻击。您可以授予 AWS SRT 对您账户 Shield Advanced 和 AWS WAF API 的有限访问权限。只有经过您的明确授权，AWS SRT 才会访问这些 API 以对您的账户实施缓解措施。有关详细信息，请参阅本文档的支持部分。

您可以使用 AWS Firewall Manager 在整个企业中集中配置和管理安全规则，例如 Shield Advanced 保护和 AWS WAF 规则。您的 AWS Organizations 管理账户可以指定管理员账户，该账户有权创建 Firewall Manager 策略。这些策略允许您定义标准（如资源类型和标签），以确定规则的应用位置。当您有多个账户并希望实现标准化保护时，这非常有用。

相关详细信息：

- 适用于 AWS WAF 的 AWS 托管规则，请参阅适用于 AWS WAF 的 AWS 托管规则。
- 有关如何使用地理位置限制来限制对 CloudFront 分配的访问，请参阅限制内容的地理位置分配。
- 有关如何使用 AWS WAF，请参阅
  - AWS WAF 入门
  - 记录 Web ACL 流量信息
  - 查看 Web 请求示例
- 有关如何配置基于速率的规则，请参阅使用 AWS WAF 基于速率的规则保护网站和服务
- 有关如何使用 Firewall Manager 管理 AWS 资源的 AWS WAF 规则部署，请参阅
  - Firewall Manager AWS WAF 策略入门。
  - Firewall Manager Shield Advanced 策略入门。

缩小攻击面

构架 AWS 解决方案时的另一个重要考虑因素是，限制攻击者将您的应用程序作为攻击目标的机会。这个概念被称为缩小攻击面。未暴露给 Internet 的资源更难以攻击，这限制了攻击者将您的应用程序可用性作为攻击目标的可能。

例如，如果您不希望用户直接与某些资源进行交互，则需确保这些资源不能通过 Internet 进行访问。同样，不要接受端口或协议上对于通信不必要的用户或外部应用程序的流量。

在以下部分中，AWS 提供了最佳实践来指导您缩小攻击面并限制应用程序的 Internet 暴露。

主题

- 模糊 AWS 资源（BP1、BP4、BP5）

模糊 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 Internet。例如，当 Elastic Load Balancing 后面有 Amazon EC2 实例时，这些实例本身可能不需要能够公开访问。相反，您可以为用户提供在某些 TCP 端口上访问 Elastic Load Balancing 的权限，只允许 Elastic Load Balancing 与实例进行通信。您可以对此进行设置，方法为：在 Amazon Virtual Private Cloud（VPC）中配置安全组和网络访问控制列表（NACL）。Amazon VPC 允许您预置 AWS 云的逻辑隔离部分，让您可以在自己定义的虚拟网络中启动 AWS 资源。

安全组和网络 ACL 的类似之处在于，它们都允许您控制对 VPC 内 AWS 资源的访问。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 ACL 在 VPC 子网级别提供类似功能。使用安全组或网络 ACL 无需额外付费。

安全组和网络访问控制列表（网络 ACL）（BP5）

您可以选择是在启动实例时指定安全组，还是稍后将实例与安全组关联。除非创建允许 规则以允许流量，否则从 Internet 到安全组的所有流量都会被隐式拒绝。例如，如果您有一个 Web 应用程序使用 Elastic Load Balancing 和多个 Amazon EC2 实例，则您可以决定为 Elastic Load Balancing 创建一个安全组（Elastic Load Balancing 安全组），为实例创建另一个安全组（Web 应用程序服务器安全组）。然后，您可以创建允许 规则，允许从 Internet 到 ELB 安全组的流量，并创建另一个规则，允许从 ELB 安全组到 Web 应用程序服务器安全组的流量。这样可确保 Internet 流量无法直接与 Amazon EC2 实例通信，从而使得攻击者更难了解和影响您的应用程序。

创建网络 ACL 时，您可以同时指定允许规则和拒绝规则。如果您希望显式拒绝某些类型的流量通往您的应用程序，这非常有用。例如，您可以定义拒绝对整个子网访问的 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，您可以创建规则来拒绝所有 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源 IP 或其他特征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。可以更快地检测针对已注册为受保护资源的弹性 IP 地址的 DDoS 攻击，从而缩短缓解攻击的时间。当检测到攻击时，DDoS 缓解系统会读取与目标弹性 IP 对应的网络 ACL，并在 AWS 网络边界强制执行。这大大降低了受众多基础设施层 DDoS 攻击影响的风险。

要详细了解如何配置安全组和网络 ACL 来优化 DDoS 弹性，请参阅如何通过缩小攻击面来帮助防范 DDoS 攻击。

要详细了解如何使用带有弹性 IP 地址的 Shield Advanced 作为受保护资源，请参阅订阅 AWS Shield Advanced 的步骤。

保护您的源（BP1、BP5）

如果您将 Amazon CloudFront 与位于您的 VPC 内的源一起使用，可能需要确保只有您的 CloudFront 分配才能将请求转发到您的源。使用 Edge-to-Origin 请求标头，您可以在 CloudFront 将请求转发到源时添加标头或覆盖现有请求标头的值。您可以使用源自定义标头（例如 X-Shared-Secret 标头）来帮助验证向您的源发出的请求是否从 CloudFront 发送。

有关使用源自定义标头保护源的更多信息，请参阅向源请求添加自定义标头和限制对 Application Load Balancer 的访问。

有关实施示例解决方案来自动轮换源自定义标头值以进行源访问限制的指南，请参阅如何使用 AWS WAF 和 Secrets Manager 增强 Amazon CloudFront 源安全性。

或者，您可以使用 AWS Lambda 函数自动更新安全组规则，使其仅允许 CloudFront 流量。这有助于确保恶意用户在访问您的 Web 应用程序时无法绕过 CloudFront 和 AWS WAF，从而提高源的安全性。

有关如何通过自动更新安全组来保护源的更多信息，请参阅 X-Shared-Secret 标头，以及如何通过使用 AWS Lambda 自动更新 Amazon CloudFront 和 AWS WAF 的安全组。

保护 API 终端节点（BP4）

通常，当您必须向公众公开 API 时，存在 API 前端可能会成为 DDoS 攻击目标的风险。为了帮助降低风险，您可以使用 Amazon API Gateway 作为在 Amazon EC2、AWS Lambda 或其他地方运行的应用

程序的入口通道。通过使用 Amazon API Gateway，您不需要为 API 前端运行自己的服务器，且可以故意模糊您应用程序的其他组件。通过让检测应用程序组件变得更难，您可以帮助防止这些 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 端点中进行选择。第一个是默认选项：通过 Amazon CloudFront 分配访问的边缘优化 API 端点。但是，分配由 API Gateway 创建和管理，因此您无法对其进行控制。第二个选项是，使用从部署 REST API 的同一 AWS 区域访问的区域性 API 端点。AWS 建议您使用第二种类型的端点，并将其与您自己的 Amazon CloudFront 分配关联。这样，您就可以控制 Amazon CloudFront 分配，并能够将 AWS WAF 用于应用层保护。借助此模式，您能够在 AWS 全球边缘网络中访问扩展的 DDoS 缓解容量。

将 Amazon CloudFront 和 AWS WAF 与 Amazon API Gateway 一起使用时，请配置以下选项：

- 配置分配的缓存行为，将所有标头转发到 API Gateway 区域性端点。这样，CloudFront 会将内容视为动态内容，并跳过缓存内容。
- 通过将分配配置为包含源自定义标头 `x-api-key`，并在 API Gateway 中设置 API 密钥值，从而保护您的 API Gateway 免受直接访问。
- 通过为 REST API 中的每个方法配置标准或突发速率限制来避免过多流量，从而保护后端。

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

操作技术

本白皮书中的缓解技术有助于您构建天生就能够抵御 DDoS 攻击的应用程序。在许多情况下，了解 DDoS 攻击何时针对您的应用程序以便采取缓解措施，这也很有用。本部分讨论了以下方面的最佳实践：了解异常行为、警报和自动化、大规模管理保护以及接洽 AWS 以获得更多支持。

主题

- 可见性
- 跨多个账户的可见性和保护管理
- 支持

可见性

当关键操作指标严重偏离预期值时，攻击者可能正试图将应用程序可用性作为目标。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措施。Amazon CloudWatch 可通过监控您在 AWS 上运行的应用程序来提供帮助。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，并自动应对您的 AWS 资源的变化。

如果您在构架应用程序时遵循 DDoS 弹性参考架构，则常见基础设施层攻击将在到达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正在成为目标。例如，您可以配置警报，以便在发生 DDoS 攻击时通知您，这样，您就可以检查应用程序运行状况并决定是否使用 AWS SRT。您可以配置 `DDoSDetected` 指标以告知您是否检测到攻击。如果您希望根据攻击量收到警报，也可以使用 `DDoSAttackBitsPerSecond`、`DDoSAttackPacketsPerSecond` 或 `DDoSAttackRequestsPerSecond` 指标。您可以通过将 CloudWatch 与您自己的工具集成，或使用第三方提供的工具（如 Slack 或 PagerDuty）来监控这些指标。

应用层攻击可以提升许多 Amazon CloudWatch 指标。如果您使用的是 AWS WAF，可以使用 CloudWatch 监控和激活有关已在 AWS WAF 中设置为允许、计数或阻止的请求数量增加的警报。这样，当流量超出应用程序的处理能力时，您就可以收到通知。您还可以使用 CloudWatch 中跟踪的 Amazon CloudFront、Amazon Route 53、Application Load Balancer、Network Load Balancer、Amazon EC2 和 Auto Scaling 指标，来检测可能指示 DDoS 攻击的更改。

推荐的 CloudWatch 指标表列出了通常用于检测和响应 DDoS 攻击的 CloudWatch 指标说明。

表 3 – 推荐的 Amazon CloudWatch 指标

主题	指标	说明
AWS Shield Advanced	DDoSDetected	指示特定 Amazon Resource Name（ARN）的 DDoS 事件。
AWS Shield Advanced	DDoSAttackBitsPerSecond	在针对特定 ARN 的 DDoS 事件期间观察到的字节数。该指标仅适用于 3/4 层 DDoS 事件。
AWS Shield Advanced	DDoSAttackPacketsPerSecond	在针对特定 ARN 的 DDoS 事件期间观察到的数据包数。该指标仅适用于 3/4 层 DDoS 事件。
AWS Shield Advanced	DDoSAttackRequestsPerSecond	在针对特定 ARN 的 DDoS 事件期间观察到的请求数。该指标仅适用于第 7 层 DDoS 事件，仅针对最重要的第 7 层事件报告。
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	传递的请求数。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	请求	HTTP/S 请求的数量。
Amazon CloudFront	TotalErrorRate	HTTP 状态代码为 4xx 或 5xx 的所有请求所占的百分比。
Amazon Route 53	HealthCheckStatus	端点的运行状况检查状态。

主题	指标	说明
Application Load Balancer	ActiveConnectionCount	从客户端到负载均衡器以及从负载均衡器到目标的并发活动 TCP 连接的总数。
Application Load Balancer	ConsumedLCUs	负载均衡器使用的负载均衡器容量单位（LCU）数量。
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	负载均衡器生成的 HTTP 4xx 或 5xx 客户端错误代码的数量。
Application Load Balancer	NewConnectionCount	从客户端到负载均衡器以及从负载均衡器到目标建立的新 TCP 连接的总数。
Application Load Balancer	ProcessedBytes	负载均衡器处理的总字节数。
Application Load Balancer	RejectedConnectionCount	由于负载均衡器达到连接数上限被拒绝的链接的数量。
Application Load Balancer	RequestCount	已处理的请求数。
Application Load Balancer	TargetConnectionErrorCount	负载均衡器和目标之间连接建立不成功的次数。
Application Load Balancer	TargetResponseTime	请求离开负载均衡器直至收到来自目标的响应所用的时间（以秒为单位）。
Application Load Balancer	UnHealthyHostCount	被视为未正常运行的目标数量。
网络负载均衡器	ActiveFlowCount	客户端至目标的并发 TCP 流（或连接）的总数。
网络负载均衡器	ConsumedLCUs	负载均衡器使用的负载均衡器容量单位（LCU）数量。

主题	指标	说明
网络负载均衡器	NewFlowCount	时段内建立的客户端至目标的新 TCP 流（或连接）的总数。
网络负载均衡器	ProcessedBytes	负载均衡器处理的字节总数，包括 TCP/IP 标头。
Global Accelerator	NewFlowCount	时段内建立的客户端至端点的新 TCP 和 UDP 流（或连接）的总数。
Global Accelerator	ProcessedBytesIn	加速器处理的传入字节总数，包括 TCP/IP 标头。
Auto Scaling	GroupMaxSize	Auto Scaling 组的最大大小。
Amazon EC2	CPU 使用率	当前正在使用的已分配 EC2 计算单位的百分比。
Amazon EC2	NetworkIn	实例在所有网络接口上收到的字节数。

要详细了解如何使用 Amazon CloudWatch 检测针对您的应用程序的 DDoS 攻击，请参阅 Amazon CloudWatch 入门。

要查看使用上表中某些指标构建的控制面板示例，请参阅自定义基准监控系统

AWS 包括几个额外的指标和警报，用于通知攻击并帮助您监控应用程序的资源。AWS Shield 控制台或 API 提供基于账户的事件摘要以及已检测到的攻击的详细信息。

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

如果您已订阅 AWS Shield Advanced，则服务控制面板将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。通过放置的缓解措施，这可以保护您的资源免受与已知 DDoS 事件签名匹配的过量流量和流量的影响。

当 Web ACL 与受保护的资源相关联时，检测指标基于采样的网络流量或 AWS WAF 日志。缓解指标基于 Shield 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资源的流量。

网络排名靠前的贡献者指标可让您深入了解检测到的事件期间流量的来源地。您可以查看数量最高的贡献者，并按协议、源端口和 TCP 标志等方面进行排序。排名靠前的贡献者指标包括针对资源各个维度观察到的所有流量的指标。它提供了额外指标维度，可用于了解事件期间发送到资源的网络流量。

服务控制面板还包括有关自动采取以缓解 DDoS 攻击的措施的详细信息。通过这些信息，可以更轻松地调查异常情况，查看流量维度，并更好地了解 Shield Advanced 为保护可用性而采取的措施。

可帮您了解针对应用程序的流量的另一款工具是 VPC 流日志。在传统网络上，您可以使用网络流日志来排查连接和安全问题，并确保网络访问规则正常运行。通过使用 VPC 流日志，您可以捕获有关在您的 VPC 中传入和传出网络接口的 IP 流量的信息。

每个流日志记录都包括以下信息：源和目标 IP 地址、源和目标端口、协议，以及在捕获窗口期间传输的数据包数和字节数。您可以使用此类信息，帮助识别网络流量中的异常并识别特定攻击媒介。例如，大多数 UDP 反射攻击具有特定源端口（例如，用于 DNS 反射的源端口 53）。这是一个明确的攻击特征，您可以在流日志记录中轻松识别出来。作为回应，您可以选择在实例级别阻止特定源端口，或者创建网络 ACL 规则以阻止整个协议（如果应用程序不需要该协议）。

要详细了解如何使用 VPC 流日志识别网络异常和 DDoS 攻击媒介，请参阅 VPC 流日志和 VPC 流日志 – 记录和查看网络流量流。

跨多个账户的可见性和保护管理

当您跨多个 AWS 账户进行操作并需要保护多个组件时，使用能够大规模运营并减少运营开销的技术，这样可提高您的缓解能力。在多个账户中管理 AWS Shield Advanced 受保护资源时，您可以使用 AWS Firewall Manager 和AWS Security Hub 设置集中式监控。借助 Firewall Manager，您可以创建安全策略，以对所有账户强制执行 DDoS 防护合规性。您可以同时使用这两种服务，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性状态。例如，当 Shield Advanced 检测到范围内任何 AWS 账户中发往受保护资源的异常流量时，此发现将显示在 Security Hub 控制台中。如果已配置，则 Firewall Manager 可以将资源创建为受 Shield Advanced 保护的资源来自动将其置于合规状态，然后在资源处于合规状态时更新 Security Hub。

要详细了解如何集中监控受 Shield 保护的资源，请参阅为 DDoS 事件设置集中式监控和自动修复不合规资源。

支持

如果您遇到攻击，还可以获得 AWS 的支持，以便评估威胁和审查应用程序架构，或者您可能希望请求其他帮助。必须在 DDoS 攻击实际发生之前制定响应计划，这一点非常重要。本白皮书中概述的最佳实践旨在作为您在启动应用程序之前实施的主动措施，但仍可能发生针对应用程序的 DDoS 攻击。查看本部分中的选项，以确定最适合您场景的支持资源。您的客户团队可以评估您的使用场景和应用程序，并协助解决您遇到的具体问题或挑战。

如果您在 AWS 上运行生产工作负载，请考虑订阅 Business Support，该服务可让您全天候联系云支持工程师，对方可协助解决 DDoS 攻击问题。如果您运行的是任务关键型工作负载，请考虑使用 Enterprise Support，通过该服务，您能够打开关键案例，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，且还订阅了 Business Support 或 Enterprise Support，则可以配置 Shield 主动联系。它允许您配置运行状况检查，与您的资源关联并提供全天候运营联系信息。当 Shield 检测到 DDoS 迹象，且您的应用程序运行状况检查显示性能下降时，AWS SRT 将主动与您联系。这是我们推荐的联系模式，因为它允许最快的 AWS SRT 响应时间，并使 AWS SRT 可在与您建立联系之前就开始进行故障排除。

主动联系功能要求您配置 Route 53 运行状况检查，以准确评估应用程序的运行状况，并与受 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 检测系统将使用运行状况检查状态作为应用程序运行状况的指示器。Shield Advanced 基于运行状况的检测功能将确保您在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。

完成主动联系的配置包括在 Shield 控制台中添加联系人详细信息。AWS SRT 将使用此信息与您联系。如果您有任何特定联系人要求或偏好，可以配置最多 10 个联系人并提供其他备注。主动联系联系人应担任全天候角色，例如，安全运营中心或立即就绪的个人。

您可以针对所有资源或对响应时间至关重要的选定关键生产资源启用主动联系。这可通过仅将运行状况检查分配给这些资源来实现。

如果您有影响应用程序可用性的 DDoS 相关事件，也可以使用 AWS Support 控制台或 Support API 创建 AWS Support 案例来上报到 AWS SRT。

总结

本白皮书中概述的最佳实践可帮您构建 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。您在架构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 攻击的类型、媒介和数量。您可以在不订阅 DDoS 缓解服务的情况下整合弹性。通过选择订阅 AWS Shield Advanced，您可以获得额外的支持、可见性、缓解和成本保护功能，从而进一步保护已经具有弹性的应用程序架构。

贡献者

本文档的贡献者包括：

- AWS Perimeter Protection Jeffrey Lyon
- AWS 安全专家 TAM Rodrigo Ferroni
- AWS 解决方案构架师 Dmitriy Novikov
- AWS 解决方案构架师 Achraf Souk
- AWS 解决方案构架师 Yoshihisa Nakatani

资源

延伸阅读：

- AWS 上 DDoS 缓解的最佳实践
- AWS WAF 实施指南
- 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
- SEC407 - re:Invent 2019: A defense-in-depth approach to building web applications
- SEC321 - re:Invent 2020: Get ahead of the curve with DDoS Response Team escalations
- William Hill：AWS 提供高性能 DDOS 防护

文档修订

要获得有关此白皮书更新的通知，请订阅 RSS 源。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
白皮书更新	经过更新，以包含最新建议和功能。已添加 AWS Global Accelerator 作为边缘全面保护的一部分。AWS Firewall Manager 用于集中监控 DDoS 事件和自动修复不合规资源。	2021 年 9 月 21 日
白皮书更新	经过更新，以阐明检测和筛选恶意 Web 请求（BP1、BP 2）部分中的缓存破坏，以及扩展以吸收（BP6）部分中的 ELB 和 ALB 使用情况。更新了图表和表 2，将“区域选择”标记为 BP8。更新了 BP7 部分，提供了更多详细信息。	2019 年 12 月 18 日
白皮书更新	经过更新，添加了 AWS WAF 日志记录并将其作为最佳实践。	2018 年 12 月 1 日
白皮书更新	经过更新，以包括 AWS Shield、AWS WAF 功能、AWS Firewall Manager 和相关最佳实践。	2018 年 6 月 1 日
白皮书更新	添加了规范性架构指南，并进行了更新以包含 AWS WAF。	2016 年 6 月 1 日
初次发布	发布了白皮书。	2015 年 6 月 1 日

声明

客户有责任对本文档中的信息，进行独立评估。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实践，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。