AWS 白皮书

AWS DDoS恢復能力的最佳做法

AWS DDoS恢復能力的最佳做法: AWS 白皮书

Table of Contents

AWS DDoS恢復能力的最佳做法

出版日期：二零二三年八月九日 () 文件修訂

保護您的企業免受分散式拒絕服務 (DDoS) 攻擊以及其他網路攻擊的影響非常重要。維持應用程式的可用性和回應能力，以保持客戶對您服務的信任是首要任務。當您的基礎架構必須因應攻擊而擴充時，您也希望避免不必要的直接成本。Amazon Web Services (AWS) 致力於為您提供工具、最佳實務和服務，以防禦網際網路上的不良行為者。使用適當的服務 AWS 有助於確保高可用性、安全性和恢復能力。

在本白皮書中，為您 AWS 提供規範性DDoS指導，以改善在其上執行的應用程式的彈性。 AWS這包括一個 DDoS-彈性參考架構可用作為幫助保護應用程式可用性的指南使用。本白皮書也說明不同的攻擊類型，例如基礎架構層攻擊和應用程式層攻擊。 AWS 說明管理每種攻擊類型最有效的最佳作法。此外，還概述了適合DDoS緩解策略的服務和功能，以及如何使用每種服務和功能來協助保護您的應用程式。

本 paper 適用於熟悉網路、安全性和基本概念的 IT 決策者和安全工程師 AWS。每個區段都有 AWS 文件連結，提供最佳實務或功能的詳細資訊。

AWS 每年偵測超過一百萬次DDoS攻擊，每天針對我們的客戶減輕數千次攻擊。根據我們的 Shield Response 團隊 (SRT) 所說，大多數受到DDoS攻擊業務影響的客戶並未實作本指南中的建議。

你是否 Well-Architected？

AWS Well-Architected 的架構可協助您瞭解在雲端中建置系統時所做決策的優缺點。Framework 的六大支柱可讓您學習如何設計和操作可靠、安全、高效、符合成本效益且可持續發展的系統的架構最佳實務。使用 AWS Well-Architected ToolAWS Management Console(需要登入) 中免費提供的，您可以針對每個支柱回答一組問題，根據這些最佳做法來檢閱工作負載。

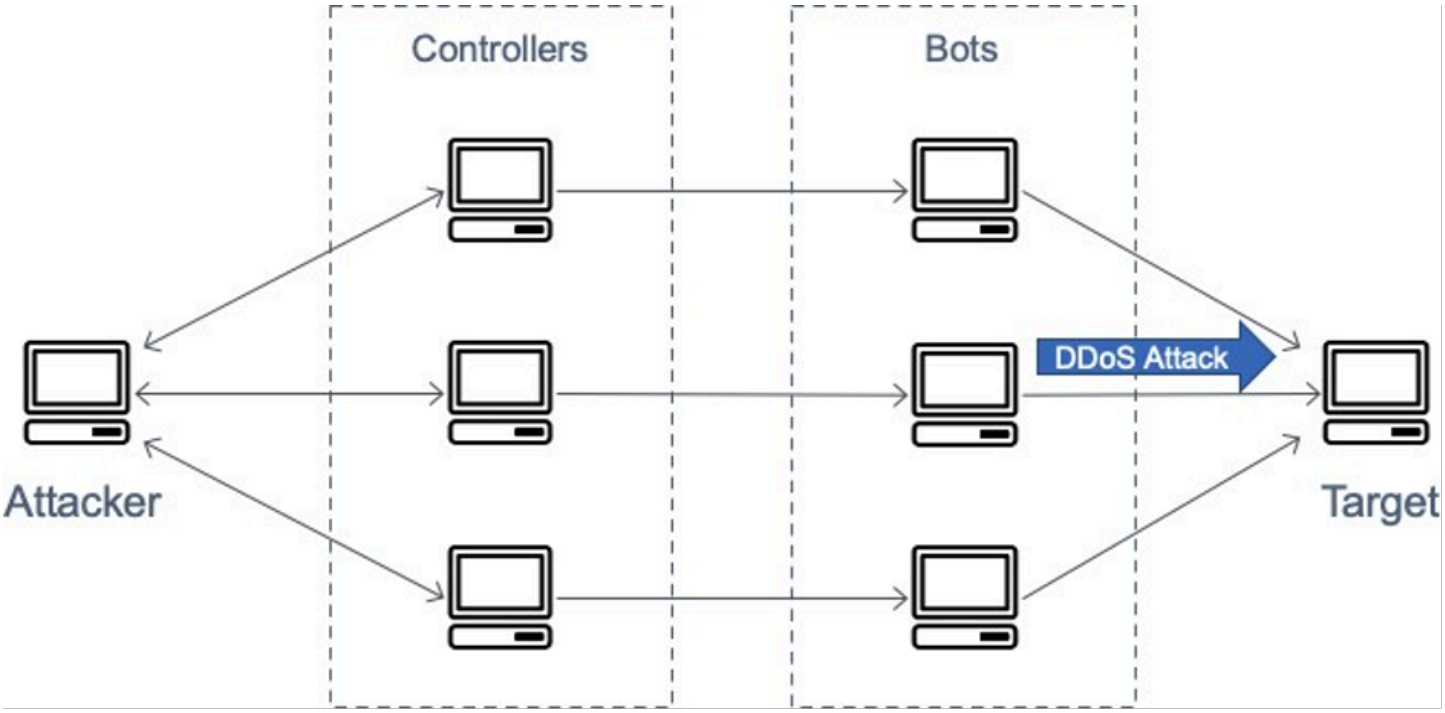
如需雲端架構的更多專家指導和最佳實務 (參考架構部署、圖表和白皮書)，請參閱架構中心。AWS

拒絕服務攻擊簡介

拒絕服務 (DoS) 攻擊或事件是蓄意嘗試讓使用者無法使用網站或應用程式，例如將網站或應用程式充斥網路流量。攻擊者使用各種消耗大量網絡帶寬或綁定其他系統資源的技術，從而中斷合法用戶的訪問。單獨攻擊者以最簡單的形式使用單一來源對目標進行 DoS 攻擊，如下圖所示。

描繪 DoS 攻擊的圖表

在分散式拒絕服務 (DDoS) 攻擊中，攻擊者會利用多個來源協調針對目標的攻擊。這些來源可能包括受惡意軟體感染的電腦、路由器、IoT 裝置和其他端點的分散式群組。下圖顯示了參與攻擊的遭到入侵的主機網路，產生大量封包或要求來壓倒目標。



描繪攻擊的DDoS圖表

「開放系統互連」(OSI) 模型中有七層，如下表所述。DDoS攻擊最常見於第 3、4、6 和 7 層。

- 第 3 層和第 4 層攻擊對應於OSI模型的網路和傳輸層。在本白皮書中， AWS 將這些統稱為基礎結構層攻擊。
- 第 6 層和第 7 層攻擊對應於OSI模型的簡報層和應用程式層。本白皮書將這些問題一起解決為應用程式層攻擊。

本 paper 在接下來的章節中討論這些攻擊類型。

表 1 — OSI 型號

#	Layer	單位	描述	向量範例
7	應用程式	資料	網路程序到應用程式	HTTP洪水，DNS查詢洪水
6	簡報	資料	數據表示和加密	傳輸層安全性 (TLS) 濫用
5	Session (工作階段)	資料	主機間通訊	N/A
4	傳輸	客群	E nd-to-end 連接和可靠性	同步（SYN）洪水
3	網路	封包	路徑確定和邏輯定址	使用者資料包通訊協定 (UDP) 反射攻擊
2	資料連結	影格	物理定址	N/A
1	實體	位元	媒體，信號和二進制傳輸	N/A

基礎架構層攻擊

最常見的DDoS攻擊，用戶數據報協議（UDP）反射攻擊和SYN洪水，是基礎設施層攻擊。攻擊者可利用其中一種方法產生大量流量，這些流量可能會淹沒網路容量，或結合伺服器、防火牆、入侵防護系統 (IPS) 或負載平衡器等系統上的資源。雖然這些攻擊很容易識別，但為了有效地緩解這些攻擊，您必須

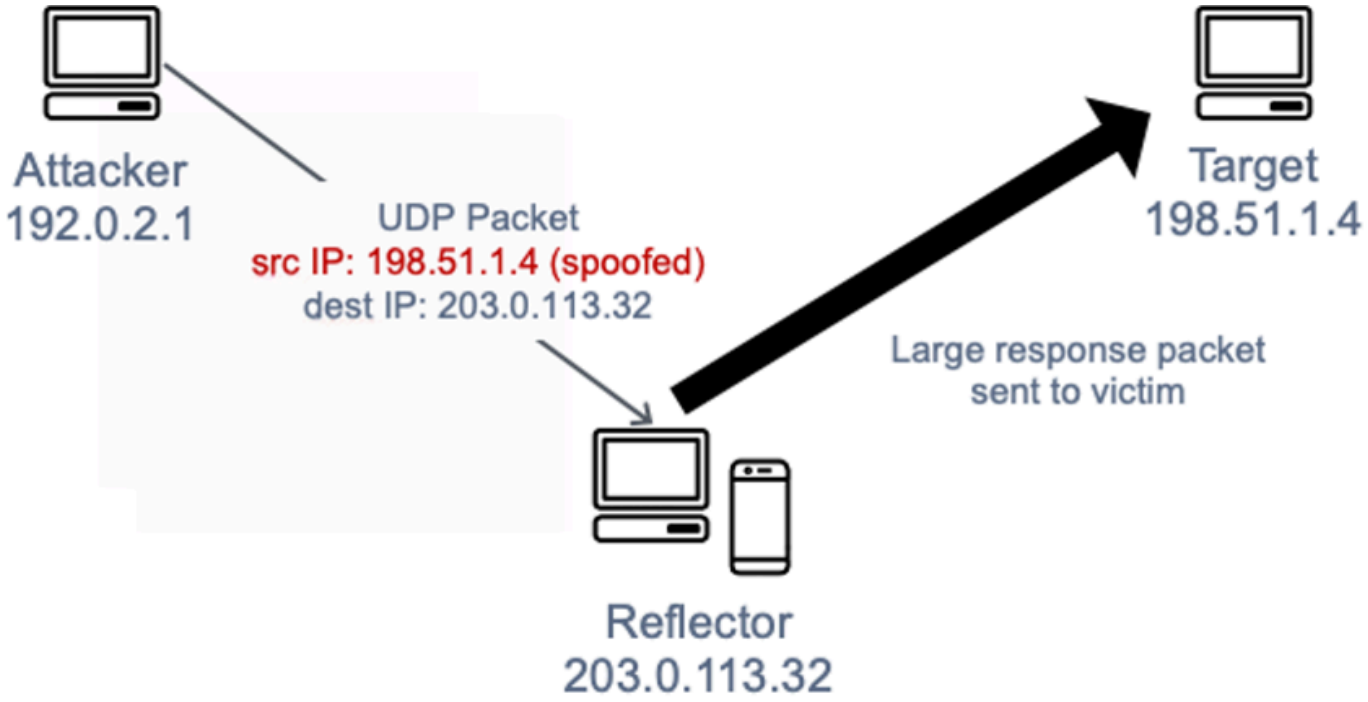
擁有一個或多個網絡系統，比入站流量洪水更快地擴展容量。這種額外的容量對於過濾掉或吸收釋放系統和應用程序以響應合法客戶流量的攻擊流量是必需的。

UDP反射攻擊

UDP反射攻擊利用無狀態協議的事實。UDP攻擊者可以製作一個有效的UDP請求數據包，列出攻擊目標的 IP 地址作為UDP源 IP 地址。攻擊者現在偽造了要求封包的來源 IP (多工緩衝UDP處理)。UDP封包包含偽造的來源 IP，並由攻擊者傳送至中繼伺服器。伺服器遭誘騙，將其回UDP應封包傳送至目標受害者 IP，而非傳回攻擊者的 IP 位址。使用中繼伺服器的原因是因為它會產生比要求封包大數倍的回應，有效地放大傳送至目標 IP 位址的攻擊流量。

放大因子是回應大小與要求大小的比率，而且視攻擊者使用的通訊協定而有所不同：DNS、網路時間通訊協定 (NTP)、簡易服務目錄通訊協定 (SSDP)、無連線輕量型目錄存取通訊協定 (CLDAP)、Memcached、字元產生器通訊協定 (CharGen) 或每日報價 ()。QOTD

例如，的放大係數DNS可以是原始位元組數的 28 到 54 倍。因此，如果攻擊者向DNS服務器發送 64 字節的請求有效負載，則可以向攻擊目標生成超過 3400 字節的不需要流量。UDP與其他攻擊相比，反射攻擊對更大的流量負責。下圖說明了反射策略和放大效果。

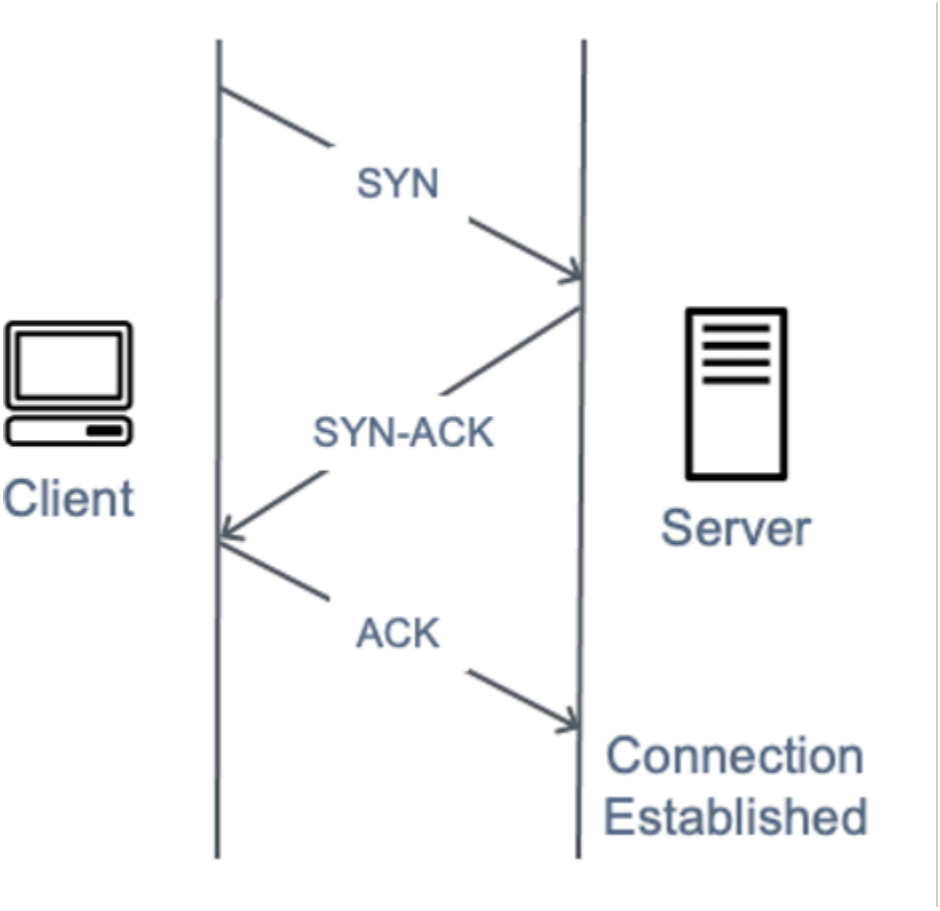


描繪UDP反射攻擊的圖表

應該注意的是，反射攻擊雖然它們為攻擊者提供「免費」放大，但它們需要 IP 欺騙能力，並且隨著越來越多的網絡提供商採用源代碼地址驗證到處（SAVE）BCP38，或者刪除了該功能，要求DDoS服務提供商停止反射攻擊或重新定位到數據中心和網絡提供商沒有實施源地址驗證。

SYN洪水襲擊

當使用者連線到傳輸控制通訊協定 (TCP) 服務 (例如 Web 伺服器) 時，其用戶端會傳送SYN封包。伺服器會傳回同步處理確認 (SYN-ACK) 封包，最後用戶端會回應一個通知 (ACK) 封包，完成預期的三向交換。下圖說明了這種典型的握手。



描繪SYN三向握手的圖表

在SYN洪水攻擊中，惡意客戶端發送大量數SYN據包，但永遠不會發送最終數ACK據包來完成握手。伺服器會等待對半開啟TCP連線的回應，而這個想法是目標最終會耗盡容量以接受新的TCP連線，從而阻止新使用者連線到伺服器，但實際影響會更加細微。現代操作系統默認情況下都實現了 SYN cookie作為一種機制來對抗SYN洪水攻擊的狀態表耗盡。一旦SYN佇列長度達到預先決定的臨界值，伺服器就會以ACK包含特製的初始序號的 SYN-回應，而不會在其SYN佇列中建立項目。如果服務器接著收到一個ACK包含正確遞增的確認號碼，則可以將該條目添加到其狀態表中並正常進行。SYN洪水對目標

設備的實際影響往往是網絡容量和CPU耗盡，但是防火牆（或EC2安全組連接跟踪）之類的中間可設置設備可能會遭受TCP狀態表耗盡並丢棄新的連接。

TCP中間盒反射

2021 年 8 月，這種相對較新的攻擊媒介首次在學術白皮書中披露，該白皮書解釋了國家防火牆和商業可用防火牆的TCP不合規性如何導致這些被欺騙成為放大載體。TCP自 2022 年初以來，我們已經「在野外」看到了這些攻擊，並今天繼續看到它們。由於供應商實施此「功能」的方式不同，放大係數會有所不同，但可能超過 Memcached UDP 放大。

應用程式層攻擊

攻擊者可以通過使用第 7 層或應用程序層攻擊來定位應用程序本身。在這些攻擊中，與SYN洪水基礎結構攻擊類似，攻擊者會嘗試超載應用程式的特定功能，使應用程式無法使用或對合法使用者沒有回應。有時候，這可以通過非常低的請求量來實現，這只會產生少量的網絡流量。這可能會使攻擊難以檢測和緩解。應用層攻擊的例子包括HTTP洪水，緩存破壞攻擊和-洪水。 WordPress XML RPC

- 在HTTP洪水攻擊中，攻擊者會傳HTTP送看似來自 Web 應用程式有效使用者的要求。一些HTTP洪水針對特定資源，而更複雜的HTTP洪水試圖模擬人與應用程序的互動。這可能會增加使用常見緩解技術（例如請求速率限制）的難度。
- 緩存破壞攻擊是一種HTTP洪水類型，它使用查詢字符串中的變化來規避內容交付網絡（ ）緩存。CDN而不是能夠返回緩存的結果，CDN必須聯繫原始服務器為每個頁面請求，這些來源提取會導致應用程序 Web 服務器的額外壓力。
- 通過RPC洪水攻擊（也稱為 WordPress pingback 洪水），攻擊者將 WordPress 內容管理軟件上託管的網站作為目標。WordPress XML攻擊者錯誤使用 XML-RPC API 函數來產生大量HTTP要求。pingback 功能可讓託管於 WordPress (網站 A) 的網站透過網 WordPress 站 A 建立至站台 B 的連結，通知不同的網站 (網站 B)，然後嘗試擷取站台 A 以驗證連結是否存在。在 pingback 洪水中，攻擊者會濫用此功能，造成網站 B 攻擊網站 A。此類型的攻擊具有明確的簽章："WordPress:" 通常存在於要求標頭的使用者代理程式中HTTP。

還有其他形式的惡意流量會影響應用程式的可用性。Scraper 漫遊器會自動嘗試訪問 Web 應用程序以竊取內容或記錄競爭性信息，例如定價。暴力破解和憑證填充攻擊是編程努力，以獲得對應用程序安全區域的未經授權訪問。這些不是嚴格的DDoS攻擊，但它們的自動化性質看起來與DDoS攻擊類似，並且可以通過實施本 paper 中涵蓋的一些相同的最佳實踐來緩解它們。

應用程式層攻擊也可以鎖定網域名稱系統 (DNS) 服務。這些攻擊中最常見的是DNS查詢洪水，其中攻擊者會使用許多格式良好的查DNS詢來耗盡DNS伺服器的資源。這些攻擊還可能包括緩存破壞組件，

其中攻擊者隨機化子域字符串以繞過任何給定解析器的本地緩存。DNS因此，解析器無法利用緩存的域查詢，而必須反复聯繫權威DNS服務器，該服務器可以放大攻擊。

如果 Web 應用程式是透過傳輸層安全性 (TLS) 傳送，攻擊者也可以選擇攻擊交TLS涉程序。TLS計算成本非常昂貴，因此攻擊者透過在伺服器上產生額外的工作負載來處理無法讀取的資料 (或無法理解 (密文) 作為合法握手，可降低伺服器的可用性。在此攻擊的變化中，攻擊者完成TLS交握，但永遠重新協商加密方法。攻擊者也可以透過開啟和關閉許多TLS工作階段來嘗試耗盡伺服器資源。

緩解技術

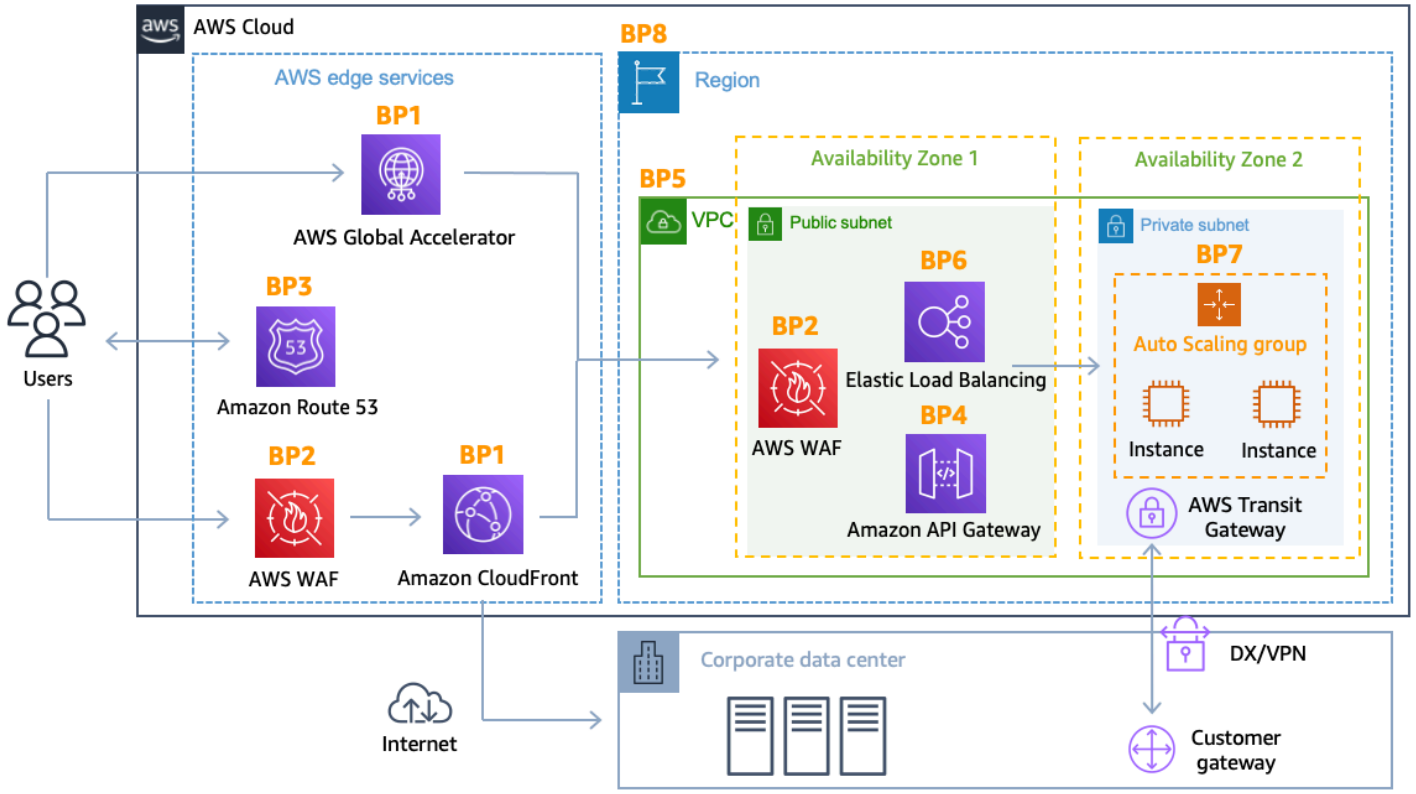
某些形式的DDoS緩解措施會自動包含在 AWS 服務中。DDoS您可以使用具有特定服務的 AWS 架構 (下列各節涵蓋)，以及針對使用者與應用程式之間網路流程的每個部分實作其他最佳作法，進一步提升復原能力。

您可以使用從 Amazon、 AWS 全球加速器和 Amazon CloudFront Route 53 等節點運作的 AWS 服務，建立全面的可用性保護，以抵禦所有已知的基礎設施層攻擊。這些服務屬於AWS 全球邊緣網路的一部分，在提供來自世界各地的邊緣位置的任何類型應用程式流量時，可提升應用程式的DDoS彈性。您可以在任何應用程式中執行應用程式 AWS 區域，並使用這些服務來保護應用程式的可用性，並針對合法使用者最佳化應用程式的效能。

使用 Amazon CloudFront，全球加速器和 Amazon 路線 53 的好處包括：

- 跨 AWS 全球邊緣網路存取網際網路和DDoS緩解容量。這對於緩解可達到太位規模的較大體積攻擊非常有用。
- AWS Shield DDoS緩解系統與 AWS 邊緣服務整合， time-to-mitigate 從幾分鐘縮短到秒。
- 無狀態SYN洪水緩解措施會先使用 SYN Cookie 驗證傳入連線，然後再將它們傳送至受保護的服務。這樣可確保只有有效的連線才能連線到您的應用程式，同時保護合法使用者免於誤判性下降。
- 分散或隔離大容量DDoS攻擊影響的自動交通工程系統。所有這些服務在攻擊到達您的來源之前，將其從源頭隔離出來，這意味著對受這些服務保護的系統的影響較小。
- 與應用程式層防禦結合 CloudFront 時 AWS WAF，不需要變更目前的應用程式架構 (例如，在 AWS 區域 或內部部署資料中心)。

傳入資料傳輸不會收取任何費用，而 AWS 且您也不需為減輕的DDoS攻擊流量付費。 AWS Shield下列架構圖包含 AWS 全球邊緣網路服務。



DDoS-彈性參考架構

此架構包含數種 AWS 服務，可協助您提升 Web 應用程式對DDoS攻擊的彈性。下表提供這些服務及其可提供之功能的摘要。 AWS 為每個服務加上最佳實務指標 (BP1,BP2) 標籤，以便在本文件中更容易參考。例如，即將到來的一節討論 Amazon CloudFront 和全球加速器提供的功能，其中包括最佳實務指標BP1。

表 2-最佳做法摘要

	AWS 邊緣			AWS 區域		
	使用 Amazon CloudFront （BP1）與 AWS WAF （BP2）	使用全域加速器 (BP1)	使用 Amazon 路線 53（BP3）	使用 Elastic Load Balancing (BP6) 搭配 AWS WAF (BP2)	ACLs在 Amazon 中使用安全組和網絡 VPC（BP5）	使用 Amazon 彈性計算雲（AmazonEC2）Auto Scaling（BP7）

	AWS 邊緣			AWS 區域		
第 3 層（例如UDP反射）攻擊緩解	✓	✓	✓	✓	✓	✓
第 4 層（例如SYN洪水）攻擊緩解	✓	✓	✓	✓		
第 6 層（例如TLS）攻擊緩解	✓	✓	✓	✓		
減少攻擊面	✓	✓	✓	✓	✓	
擴充以吸收應用程式層流量	✓	✓	✓	✓	✓	✓
第 7 層（應用程序層）攻擊緩解	✓	✓(*)	✓	✓	✓(*)	✓(*)
地理隔離和分散過多的流量和更大的DDoS攻擊	✓	✓	✓			

✓ (*)：如果與應用 Ap plication Load Balancer AWS WAF 搭配使用

另一種提高您對應攻擊和緩解DDoS攻擊的準備程度的方法是訂閱 AWS Shield Advanced. 使用的好處 AWS Shield Advanced 包括：

- 取得AWS Shield 回應團隊 (AWS SRT) 提供的全年無休專業支援，協助緩解影響應用程式可用性的DDoS攻擊，包括選購的主動參與功能

- 與彈性 IP 地址一起使用時，可以更早將流量路由到DDoS緩解系統，並可改善對 Amazon EC2 (包括彈性 Load Balancer) 或 Network Load Balancer 的 time-to-mitigate 攻擊的敏感偵測閾值
- 搭配使用時，根據應用程式的基線流量模式量身打造第 7 層偵測 AWS WAF
- Shield Advanced 透過建立、評估和部署自訂 AWS WAF 規則來回應偵測到的DDoS攻擊的自動應用程式層DDoS緩解
- 免費存取 AWS WAF 應用程式層DDoS攻擊的緩解 (與 Amazon CloudFront 或應用程式 Application Load Balancer 搭配使用時)
- 集中管理安全性原則 AWS Firewall Manager，無需額外費用。
- 成本保護，可讓您針對因攻擊而造成的擴充相關成本要求有限退款。DDoS
- 針對 AWS Shield Advanced 客戶的增強服務等級協議。
- 保護群組可讓您捆綁資源，提供自助方式，藉由將多個資源視為單一單元來自訂應用程式的偵測和緩解範圍。如需保護群組的相關資訊，請參閱 Shield 進階保護群組。
- DDoS使用AWS Management Console、API和 Amazon CloudWatch 指標和警示的攻擊可見性。

這項選用的DDoS緩解服務可協助保護裝載於任何 AWS 區域. 該服務在全球範圍內提供 53 CloudFront 號公路和全球加速器。就區域而言，您可以保護 Application Load Balancer 器、Classic Load Balancer 和彈性 IP 地址，以保護 Network Load Balancer (NLBs) 或 Amazon EC2 執行個體。

如需 AWS Shield Advanced 功能的完整清單以及相關詳細資訊 AWS Shield，請參閱如何 AWS Shield 運作。

DDoS緩解措施的最佳做法

在以下各節中，每個建議的DDoS緩和措施最佳做法會更深入地說明。如需為靜態或動態 Web 應用程式建置DDoS緩解層的快速 easy-to-implement 指南，請參閱如何使用 Amazon CloudFront 和 Amazon Route 53 協助保護動態 Web 應用程式免受DDoS攻擊。

基礎架構層防禦 (BP1BP3、BP6、、BP7)

在傳統的資料中心環境中，您可以使用諸如過度佈建容量、部署DDoS緩解系統或清理流量等技術，藉助緩解服務來DDoS緩解基礎結構層DDoS攻擊。在上 AWS，系統會自動提供DDoS緩解功能；但是您可以選擇最佳的架構選擇，以最佳化應用程式的DDoS彈性，同時也可讓您針對過多的流量進行擴充。

協助減輕容量DDoS攻擊的關鍵考量事項包括確保足夠的傳輸容量和多樣性可用，以及保護 Amazon EC2 執行個體等 AWS 資源免受攻擊流量的影響。

某些 Amazon EC2 執行個體類型支援更容易處理大量流量的功能，例如，高達 100 Gbps 的網路頻寬界面和增強型聯網。這有助於防止已到達 Amazon EC2 執行個體的流量發生介面擁塞。與傳統實作相比，支援增強型聯網的執行個體可提供更高的輸入/輸出 (I/O) 效能、更高的頻寬以及更低的CPU使用率。如此可改善執行個體處理大量流量的能力，並最終讓它們對每秒封包 (pps) 負載進行高度彈性。

若要允許這種高度的彈性， AWS 建議使用 Amazon EC2 專用執行個EC2體或具有較高聯網輸送量且尾碼為 "N" 且支援高達 100 Gbps 網路頻寬的增強型聯網的 Amazon 執行個體，例如`c6gn.16xlarge`和/`c5n.18xlarge`或金屬執行個體 (例如`c5n.metal`)。

如需支援 100 個 Gigabit 網路界面和增強型聯網之 Amazon EC2 執行個體的詳細資訊，請參閱 Amazon EC2 執行個體類型。

增強型聯網所需的模組和必要的`enaSupport`屬性集包含在 Amazon Linux 2 和最新版本的 Amazon Linux 中AMI。因此，如果您在受支援的執行個體類型上使用 Amazon Linux 的硬體虛擬機器 (HVM) 版本啟動執行個體，則您的執行個體已啟用增強型聯網功能。如需詳細資訊，請參閱在 Linux 上測試是否已啟用增強型網路和增強型網路。

Amazon EC2 與 Auto Scaling（BP7）

減輕基礎架構和應用程式層攻擊的另一種方法是大規模運作。如果您有 Web 應用程式，則可以使用負載平衡器將流量分配到多個過度佈建或設定為自動擴展的 Amazon EC2 執行個體。這些執行個體可以處理因任何原因而發生的突然流量激增，包括閃爍人群或應用程式層DDoS攻擊。您可以設定 Amazon CloudWatch 警示以啟動 Auto Scaling，以根據您定義的事件 (例如CPU、RAM網路 I/O 甚至是自訂指標) 自動擴展 Amazon EC2 叢集的大小。

當要求量意外增加時，此方法可保護應用程式的可用性。將 Amazon CloudFront、應用程式負載平衡器、傳統負載平衡器或 Network Load Balancer 與應用程式搭配使用時，TLS交涉是由分發 (Amazon CloudFront) 或負載平衡器處理。這些功能透過擴展來處理合法要求和TLS濫用攻擊，協助保護您的執行個體不受TLS基於攻擊的影響。

如需有關使用 Amazon CloudWatch 叫用 Auto Scaling 的詳細資訊，請參閱監控 Auto Scaling 群組和執行個體的 Amazon CloudWatch 指標。

Amazon EC2 提供可調整大小的運算容量，因此您可以在需求變更時快速擴展或縮減規模。您可以透過擴展 Amazon EC2 Auto Scaling 群組的大小，自動將執行個體新增至應用程式，以水平擴展，也可以使用較大的EC2執行個體類型垂直擴展。

透過使用 Amazon RDS Proxy，您可以允許應用程式集區和共用資料庫連線，以改善其擴展和處理資料庫流量中無法預測的突波的能力。 您也可以為 Amazon RDS 資料庫執行個體啟用儲存 auto-scaling 能。如需詳細資訊，請參閱使用 Amazon RDS 儲存自動調度資源自動管理容量

Elastic Load Balancing (BP6)

大型DDoS攻擊可能會壓倒單一 Amazon EC2 執行個體的容量。使用 Elastic Load Balancing (ELB)，您可以將流量分散到許多後端執行個體，以降低應用程式過載的風險。Elastic Load Balancing 可以自動擴展，允許您在出現意想不到的額外流量（例如由於人群或DDoS攻擊）時管理更大的磁碟區。對於在 Amazon 內建置的應用程式VPC，視您的應用程式類型而定，需ELBs要考慮三種類型：Application Load Balancer (ALB)、Network Load Balancer (NLB) 和 Classic Load Balancer (CLB)。

對於 Web 應用程式，您可以使用應用 Application Load Balancer 根據內容路由流量，並只接受格式良好的 Web 要求。Application Load Balancer 會封鎖許多常見的DDoS攻擊，例如SYN洪水或UDP反射攻擊，保護您的應用程式免受攻擊。當偵測到這些類型的攻擊時，Application Load Balancer 會自動擴展以吸收額外的流量。由於基礎架構層攻擊而導致的擴展活動對 AWS 客戶來說是透明的，不會影響您的帳單。

如需有關使用應用程式負載平衡器保護 Web 應用程式的詳細資訊，請參閱應用程式負載平衡器入門。

對於非HTTP/HTTPS應用程式，您可以使用 Network Load Balancer 以超低延遲將流量路由到目標 (例如 Amazon EC2 執行個體)。Network Load Balancer 的一個主要考慮因素是，TCPSYN任何到達有效接TLS聽程式上負載平衡器的UDP流量都會路由到達您的目標，而不會被吸收，但這不適用於終止TCP連線的-listener。對於具有TCP接聽程式的網路負載平衡器，我們建議部署全域加速器以防止SYN洪水。

您可以使用防 Shield 進階來設定彈性 IP 位址的DDoS保護。將每個可用區域的彈性 IP 位址指派給 Network Load Balancer 時，「Shield 牌進階」會針對 Network Load Balancer 流量套用相關DDoS保護。

如需有關使用 Network Load Balancer 保護TCP和UDP應用程式的詳細資訊，請參閱開始使用網路負載平衡器。

> **Note**
>
> 視安全性群組組態而定，它需要使用安全性的資源群組才能使用連線追蹤來追蹤流量的相關資訊，這可能會影響負載平衡器處理新連線的能力，因為追蹤的連線數目有限。
> 安全群組組態包含接受來自任何 IP 位址 (例如`0.0.0.0/0`或`::/0`) 之流量的輸入規則，但沒有允許回應流量的對應規則的輸入規則，會導致安全性群組使用連線追蹤資訊來允許傳送回應流量。發生DDoS攻擊時，可能會用盡最大追蹤連線數目。若要改善面向公開的 Application Load Balancer 或 Classic Load Balancer 的DDoS彈性，請確定與負載平衡器關聯的安全性群組設定為不使用連線追蹤 (未追蹤的連線)，因此流量流程不受連線追蹤限制的限制。

為此，請使用允許輸入規則接受來自任何 IP 位址 (0.0.0.0/0或::/0) 的TCP流程，並在輸出方向新增對應規則，允許此資源傳送回應流量 (允許任何 IP 位址的輸出範圍0.0.0.0/0或::/0) 所有連接埠 (0-65535)，因此會根據安全性群組規則傳送回應流量，而非追蹤資訊允許回應流量。 使用此組態時，傳統和 Application Load Balancer 不會受到耗盡連線追蹤限制的限制，這些限制可能會影響到其負載平衡器節點的建立新連線，並允許其根據發生DDoS攻擊時的流量增加進行調整。 有關未追蹤連線的詳細資訊，請參閱：安全性群組連線追蹤：未追蹤的連線。

只有在DDoS流量源自安全性群組允許的來源時，避免安全性群組連線追蹤才有幫助 — 來自安全性群組中不允許的來源的DDoS流量不會影響連線追蹤。在這些情況下，不需要重新設定安全性群組以避免連線追蹤，例如，如果您的安全性群組允許清單包含您具有高度信任的 IP 範圍，例如公司企業防火牆或受信任的VPN輸出IPs或。CDNs

使用 AWS 邊位置進行縮放 (BP1,BP3)

存取高規模、多樣化的網際網路連線，可大幅提升您最佳化使用者延遲和輸送量、吸收DDoS攻擊並隔離故障的能力，同時將對應用程式可用性的影響降到最低。 AWS 節點提供額外的網路基礎設施層，可為使用 Amazon CloudFront、全球加速器和 Amazon Route 53 的任何 Web 應用程式提供這些好處。有了這些服務，您就可以在執行應用程式的邊緣全面保護。 AWS 區域

邊緣的 Web 應用程式交付 (BP1)

Amazon CloudFront 是一種服務，可用於交付您的整個網站，包括靜態、動態、串流和互動式內容。即使您沒有提供可快取的內容，持續連線和變數 time-to-live (TTL) 設定也可以用來卸載來源的流量。使用這些 CloudFront 功能可減少回原始伺服器的要求和TCP連線數量，協助保護您的 Web 應用程式免受HTTP洪水的影響。

CloudFront 只接受格式良好的連接，這有助於防止許多常見的DDoS攻擊（例如SYN洪水和UDP反射攻擊）到達您的起源。DDoS攻擊也會在靠近來源的地理位置隔離，以防止流量影響其他位置。這些功能可以大幅提升您在大型DDoS攻擊期間繼續為使用者提供流量的能力。您可以用 CloudFront 來保護網際網路上 AWS 或其他地方的來源。

如果您使用 Amazon 簡單儲存服務 (Amazon S3) 在網際網路上提供靜態內容， AWS 建議您使用 Amazon CloudFront 保護儲存貯體，並提供以下好處：

- 限制對 Amazon S3 儲存貯體的存取，使其無法公開存取。
- 請確定檢視者 (使用者) 只能透過指定的 CloudFront 發行版本存取值區中的內容，亦即防止他們直接從值區存取內容，或透過非 CloudFront 預期的發佈存取內容。

若要達成此目標，請設定 CloudFront 為將經過驗證的請求傳送至 Amazon S3，並將 Amazon S3 設定為僅允許存取已驗證的請求來源 CloudFront。 CloudFront 提供兩種將驗證請求傳送至 Amazon S3 來源的方式：來源存取控制 (OAC) 和來源存取身分 (OAI)。我們建議使用，OAC因為它支持：

- 所有 Amazon S3 儲存貯體 AWS 區域，包括 2022 年 12 月後推出的選擇加入區域
- 使用 AWS KMS (SSE-KMS) 的 Amazon S3 伺服器端加密
- 對 Amazon S3 的動態請求 (PUT 和 DELETE)

如需OAC和的詳細資訊OAI，請參閱限制對 Amazon S3 來源的存取。

如需使用 Amazon 保護和最佳化 Web 應用程式效能的詳細資訊 CloudFront，請參閱 Amazon 入門 CloudFront。

使用 AWS 全域加速器進一步保護來自您來源的網路流量 (BP1)

全球加速器是一種網路服務，可將使用者流量的可用性和效能提升高達 60%。這是透過將流量輸入離您使用者最近的節點，並透過 AWS 全球網路基礎結構將流量路由到您的應用程式，無論是在單一或多個中執行。 AWS 區域

全域加速器會根據最接近使用者的效能，將UDP流量路由TCP傳 AWS 區域 送至最佳端點。如果應用程式發生故障，全域加速器會在 30 秒內提供容錯移轉至下一個最佳端點。Global Accelerator 使用 AWS 全球網路的龐大容量，並與 Shield 整合，例如無狀態 SYN Proxy 功能，挑戰新的連線嘗試，並且僅提供合法使用者服務，以保護應用程式。

即使您的應用程式使用不受支援的通訊協定， CloudFront 或者您操作的 Web 應用程式需要全域靜態 IP 位址的 Web 應用程式，您也可以實作DDoS復原架構，以提供與 Edge 最佳實務的 Web 應用程式相同的許多優點。

例如，您可能需要使用者可以將 IP 位址新增至防火牆中的允許清單，而且不會被任何其他 AWS 客戶使用。在這些情況下，您可以使用全域加速器來保護在應用程式負載平衡器上執行的 Web 應用程式，並與 AWS WAF 同時偵測和緩解 Web 應用程式層要求洪水。

如需有關使用全域加速器保護及最佳化網路流量效能的詳細資訊，請參閱全域加速器入門。

邊緣的網域名稱解析 (BP3)

主題

- 使用路線 53 以取得DNS可用性

- 設定 Route 53 以保護NXDOMAIN免受攻擊的成本

使用路線 53 以取得DNS可用性

Amazon Route 53 是高可用性和可擴展的網域名稱系統 (DNS) 服務，可用來將流量導向您的 Web 應用程式。它包括高級功能，例如流量流量，運行 Health 檢查和監控，基於延遲的路由和地理位置。DNS這些進階功能可讓您控制服務如何回應要DNS求，以改善 Web 應用程式的效能並避免網站中斷。這是唯一具有 100% 資料層可用性的 AWS 服務SLA。

Amazon Route 53 使用隨機分片和任意廣播等技術，即使DNS服務受到攻擊的目標，也能協助使用者存取您的應用程式。DDoS

使用隨機分片，委派集中的每個名稱伺服器都會對應於一組唯一的邊緣位置和網際網路路徑。這樣可以提供更大的容錯能力，並將客戶之間的重疊 如果委派集中的一個名稱伺服器無法使用，使用者可以在不同節點重試並接收來自另一個名稱伺服器的回應。

Anycast 分割可讓每個DNS要求由最佳的位置提供服務，藉此分散網路負載並減少延遲。DNS這為用戶提供了更快的響應。此外，Amazon Route 53 可以偵測DNS查詢來源和數量中的異常情況，並排定來自已知可靠使用者的請求的優先順序。

如需有關使用 Amazon Route 53 將使用者路由到您的應用程式的詳細資訊，請參閱 Amazon 路線 53 入門。

設定 Route 53 以保護**NXDOMAIN**免受攻擊的成本

NXDOMAIN當攻擊者通常透過已知的「良好」解析器向不存在子域的託管區域發送大量請求時，就會發生攻擊。這些攻擊的目的可能是影響遞歸解析器的緩存和/或權威解析器的可用性，或者可能是一種嘗試發現託管區域記錄的DNS偵察形式。將 Route 53 用於您的權威解析器可減輕可用性/效能影響的風險，但結果可能會大幅增加 Route 53 每月成本。為了防止成本增加，請利用 Route 53 定價，在以下兩個條件都成立時，DNS查詢是免費的：

- 查詢中的網域或子網域名稱 (`example.com`或`store.example.com`) 和記錄類型 (A) 與別名記錄相符。
- 別名目標是另一個 Route 53 記錄以外的 AWS 資源。

例如，建立萬用字元記錄，`*.example.com`其類型 A (別名) 指向EC2執行個體、Elastic Load Balancer 或 CloudFront 分佈等資 AWS 源，以便在進`qwerty12345.example.com`行查詢時，會傳回資源的 IP，且不會向您收取查詢費用。

應用程式層防禦 (BP1,BP2)

本 paper 皮書目前所討論的許多技術，都能有效減輕基礎架構層DDoS攻擊對應用程式可用性的影響。為了防禦應用程式層攻擊，您需要實作可讓您特別偵測、擴充以吸收及封鎖惡意要求的架構。這是一個重要的考慮因素，因為基於網絡的DDoS緩解系統通常無效地緩解複雜的應用程序層攻擊。

偵測並篩選惡意 Web 要求 (BP1、BP2)

在應用程式上執行時 AWS，您可以利用 Amazon CloudFront (及其HTTP快取功能) 和 Shield 進階自動應用程式層保護 AWS WAF，協助防止在應用程式層DDoS攻擊期間不必要的請求到達原點。

Amazon CloudFront

Amazon CloudFront 可防止非 Web 流量到達您的來源，協助減少伺服器負載。若要傳送要求至 CloudFront 應用程式，必須透過完成的TCP握手，使用有效的 IP 位址建立連線，而且無法偽造。此外，還 CloudFront 可以自動關閉來自緩慢讀取或寫入速度慢的攻擊者（例如 Slowloris）的連接。

CDN 快取

CloudFront 可讓您從 AWS 邊緣位置提供動態內容和靜態內容。透過從CDN快取提供 Proxy 可快取內容，您可以防止要求在快取期間從特定邊緣快取節點到達您的來源。TTL與對過期但可緩存內容的請求崩潰結合使用，甚至很短的TTL意味著在該內容的請求洪水期間，可以忽略不計的請求數量將到達您的來源。此外，啟用諸如 CloudFront Origin Shield 之類的功能可以進一步幫助減少來源的負載-您可以採取的任何措施來提高緩存命中率都可能意味著具有影響力和非影響力的請求洪水攻擊之間的差異。

AWS WAF

透過使用 AWS WAF，您可以在全域 CloudFront 發佈或區域資源上設定 Web 存取控制清單 (WebACLs)，以根據請求簽章篩選、監視和封鎖要求。若要判斷是否允許或封鎖要求，您可以考慮諸如 IP 位址或原始國家/地區、要求中的特定字串或模式、要求特定部分的大小，以及存在惡意SQL程式碼或指令碼等因素。您也可以針對要求執行CAPTCHA謎題和無訊息用戶端工作階段挑戰。

AWS WAF 並且 CloudFront 還使您能夠設置地理限制以阻止或允許來自選定國家/地區的請求。這有助於封鎖或限制來自您不希望為使用者提供服務的地理位置的攻擊。使用中的精細地理比對規則陳述式 AWS WAF，您可以控制區域層級的存取權。

您可以使用 ScopeDlow 陳述式來縮小規則評估的要求範圍以節省成本，並在 Web 要求上使用「標籤」來允許符合要求的規則，將比對結果傳達給稍後在相同網頁中評估的規則。ACL選擇此選項可在多個規則中重複使用相同的邏輯。

您還可以定義完整的自定義響應，包含響應代碼，標題和正文。

為了幫助識別惡意請求，請查看 Web 服務器日誌或使用 AWS WAF的日誌記錄和請求採樣。通過啟用日誌 AWS WAF 記錄，您可以獲得有關 Web 分析流量的詳細信息。ACL AWS WAF 支援防護記錄篩選，可讓您指定要記錄哪些 Web 要求，以及在檢查之後從記錄檔捨棄哪些要求。

記錄檔中記錄的資訊包括從您的 AWS 資源 AWS WAF 接收要求的時間、有關請求的詳細資訊，以及每個要求規則的比對動作。

抽樣的請求會提供過去三小時內符合您 AWS WAF 其中一個規則的要求詳細資料。您可以使用此資訊來識別潛在惡意流量特徵，並建立新規則來拒絕這些要求。如果您看到許多包含隨機查詢字串的要求，請確定只允許與應用程式快取相關的查詢字串參數。此技術有助於緩解針對您的來源的快取破壞攻擊。

AWS WAF — 基於速率的規則

AWS 強烈建議您在 5 分鐘的滑動視窗中 AWS WAF 收到的HTTP要求數目超過您定義的閾值時，使用中的速率型規則自動封鎖不良參與者的 IP 位址，以防止要求洪水發生。違規的用戶端 IP 位址將會收到 403 個禁止回應 (或設定的區塊錯誤回應)，並保持封鎖狀態，直到要求率降至閾值以下為止。

建議您將以速率為基礎的規則分層以提供增強的保護，以便您擁有：

- 以比率為基礎的總括規則，可保護您的應用程式免受大量HTTP洪水侵害
- 一或多個以比率為基礎的規則，用比以總括費率為基礎的規則更具限制性的比率來保護特定URIs費率。

例如，您可以在 5 分鐘期間內，選擇限制為 500 個請求的總括費率型規則 (不計算範圍對帳單)，然後使用向下計算陳述式，建立下列一或多個以比率為基準的規則，其下限低於 500 (5 分鐘期間內低至 100 個請求)：

- 使用像 "`if NOT uri_path contains '.'`" 這樣的範圍語句保護您的網頁，以便對沒有文件擴展名的資源請求得到進一步保護。這也可以保護您的主頁（`/`），這是一個經常針對性的URI路徑。
- 使用像 "」這樣的範圍陳述式保護動態端點 `if method exactly matches 'post' (convert lowercase)`
- 保護到達數據庫的繁重請求或調用一次性密碼（OTP），例如「」`if uri_path starts_with '/login' OR uri_path starts_with '/signup' OR uri_path starts_with '/forgotpassword'`

以速率為基礎的「封鎖」模式是您 defense-in-depth WAF設定的基礎，可防止要求洪水發生，也是核准 AWS Shield Advanced 成本保護要求的必要條件。我們將在以下各節中檢查其他 defense-in-depth WAF配置。

AWS WAF — IP 信譽

若要防止以 IP 位址信譽為基礎的攻擊，您可以使用 IP 比對來建立規則，或將受管規則用於 AWS WAF.

Amazon 的 IP 信譽清單規則群組包含以 Amazon 內部威脅情報為基礎的規則。這些規則會尋找作為機器人的 IP 位址、對 AWS 資源進行偵察或積極參與活動。DDoS該AWSManagedIPDDoSList規則, 已觀察到阻止超過 90% 的惡意請求洪水.

匿名 IP 清單規則群組包含封鎖允許檢視者身分模糊化之服務的要求的規則。其中包括來自代理 VPNs，Tor 節點和雲平台（不包括 AWS）的請求。

此外，您可以使用 AWS WAF解決方案之安全自動化的 IP 清單剖析器元件，使用協力廠商 IP 信譽清單。

AWS WAF -智慧型威脅緩解

殭屍網絡是一種嚴重的安全威脅，通常用於進行非法或有害活動，例如發送垃圾郵件，竊取敏感數據，發起勒索軟件攻擊，通過欺詐性點擊進行廣告欺詐或發動分佈式 denial-of-service （ ）DDoS攻擊。若要防止機器人攻擊，請使用AWS WAF 機器人控制受管規則群組。此規則群組提供基本的「一般」保護層級，可將標籤新增至自我識別機器人、驗證一般需要的機器人，並偵測高信賴度的機器人簽章，以及「目標式」保護等級，可新增對無法自我識別之進階機器人的偵測。

目標式保護使用進階偵測技術 (例如瀏覽器詢問、指紋識別和行為啟發式法) 來識別不良的機器人流量，然後套用緩解控制，例如速率限制和挑戰規則動作。CAPTCHATarGET 還提供速率限制選項，以強制執行類似人類的存取模式，並透過使用要求權杖套用動態速率限制。如需詳細資訊，請參閱AWS WAF 機器人控制規則群組。若要偵測並管理應用程式登入頁面上的惡意接管嘗試，您可以使用 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。規則群組會檢查用戶端傳送至應用程式登入端點的登入嘗試，並檢查應用程式對登入嘗試的回應，以追蹤成功率和失敗率，進而達到此目的。

帳戶創建欺詐是一種在線非法活動，攻擊者嘗試創建一個或多個虛假帳戶。攻擊者使用虛假帳戶進行欺詐活動，例如濫用促銷和註冊獎金，冒充某人以及網絡釣魚等網絡攻擊。虛假帳戶的存在可能會損害您與客戶的聲譽並暴露於金融欺詐行為，對您的業務產生負面影響。

您可以通過實施欺詐控制帳戶創建欺詐預防（ACFP）功能來監控和控制帳戶創建欺詐嘗試。 AWS WAF AWS WAF 在 AWS 受管規則 規則群組中提供此功能，並AWS ManagedRulesACFPRuleSet具有隨附應用程式整合SDKs。

進一步瞭解AWS WAF 智慧型威脅緩解中的這些保護。

自動緩解應用程式層DDoS事件 (BP1、BP2、BP6)

如果您已訂閱 AWS Shield Advanced，則可以啟用 Shield 進階自動應用程式層DDoS緩和措施。此功能會自動建立、評估和部署 AWS WAF 規則，以代表您緩解第 7 層DDoS事件。

AWS Shield Advanced 為與 WAF Web 關聯的每個受保護資源建立流量基準ACL。顯著偏離已建立基準線的流量會標記為潛在DDoS事件。偵測到事件後，會 AWS Shield Advanced 嘗試識別構成事件的 Web 要求簽章，如果識別簽章，則會建立 AWS WAF 規則以減輕具有該簽章的流量。

根據歷史基準評估規則並視為安全之後，規則就會新增至受防護管理的規則群組，而且您可以選擇要以計數或封鎖模式部署規則。護 Shield 進階在確定事件已完全結束後，自動移除 AWS WAF 規則。

參與SRT（僅限護 Shield 進階訂閱者）

此外，訂閱 Shield Advanced 時，您可以參與 AWS SRT以協助您建立規則，以減輕損害應用程式可用性的攻擊。您可以授予您帳戶 AWS Shield Advanced 和的 AWS SRT有限訪問權限 AWS WAF APIs。AWS SRT只有在您明確授權的情況下，才會存取這些資訊，APIs以便在您的帳戶上放 如需詳細資訊，請參閱本文件的一支援節。

您可以用 AWS Firewall Manager 來集中設定和管理整個組織中的安全性規 AWS WAF 則，例如 AWS Shield Advanced 保護和規則。您的 AWS Organizations 管理帳戶可以指定有權建立 Firewall Manager 員策略的管理員帳戶。這些策略可讓您定義準則，例如資源類型和標籤，以決定要套用規則的位置。當您擁有多個帳戶並希望將防護標準化時，此功能非常有用。

如需更多相關資訊：

- AWS 受管規則 關於 AWS WAF，請參閱「」中AWS 受管規則 的「 AWS WAF」。
- 使用地理限制來限制對 CloudFront 分佈的存取，請參閱限制內容的地理分佈。
- 使用中 AWS WAF，請參閱：
  - 開始使用 AWS WAF
  - 記錄網絡ACL流量信息
  - 檢視 Web 要求範例
- 設定以速率為基礎的規則，請參閱〈使用以速率為基礎的規則保護網站和服務〉。 AWS WAF
- 如何使用 Firewall Manager 員管理 AWS 資源中的規則部署，請參閱：
  - 開始使用 Firewall Manager 員 AWS WAF 策略。
  - 開始使用 Firewall Manager 員防 Shield 進階策略。

減少攻擊面

建構 AWS 解決方案時，另一個重要的考量因素是限制攻擊者針對您應用程式的機會。這個概念被稱為攻擊面減少。未暴露在網際網路的資源更難受到攻擊，這會限制攻擊者針對應用程式可用性的選項。

例如，如果您不希望使用者直接與特定資源互動，請確定這些資源無法從網際網路存取。同樣地，請勿接受來自使用者或外部應用程式上的通訊埠或通訊協定的流量。

在下一節中， AWS 提供最佳做法，以指導您減少攻擊面並限制應用程式的網際網路曝光率。

混淆 AWS 資源 (、、) BP1 BP4 BP5

通常，用戶可以快速輕鬆地使用應用程序，而不需要將 AWS 資源完全暴露在 Internet 上。

安全群組和網路 ACLs (BP5)

Amazon Virtual Private Cloud (AmazonVPC) 可讓您佈建邏輯隔離的區段，您可以在 AWS 雲端 其中啟動您定義的虛擬網路中的 AWS 資源。

安全性群組和網路ACLs類似，因為它們可讓您控制VPC. AWS 但是安全群組可讓您在執行個體層級控制輸入和輸出流量，而網路則在子網VPC路層級ACLs提供類似的功能。使用安全性群組或網路無須額外付費ACLs。

您可以選擇是否要在啟動執行個體時指定安全群組，或是在稍後將執行個體與安全群組建立關聯。除非您建立允許流量的允許規則，否則所有連至安全性群組的網際網路流量都會隱含拒絕。

例如，當您在 Elastic Load Balancer 後方有 Amazon EC2 執行個體時，執行個體本身不需要公開存取，而且應該IPs只有私有執行個體。相反地，您可以使用允許存取 0.0.0.0/0 (以避免連線追蹤問題 — 請參閱下方附註) 與目標群組子網路上的網路存取控制清單 () 搭配目標群組子網路上的網路存取控制清單 (NACL)，提供 Elastic Load Balancer 連接埠的 Elastic Load Balancing 器存取權限，以便僅允許彈性負載平衡 IP 範圍與執行個體通訊。如此可確保網際網路流量無法直接與 Amazon EC2 執行個體通訊，進而使攻擊者更難瞭解並影響您的應用程式。

建立網路時ACLs，您可以同時指定允許和拒絕規則。如果您想要明確拒絕特定類型的應用程式流量，這會很有用。例如，您可以定義拒絕存取整個子網路的 IP 位址 (做為CIDR範圍)、通訊協定和目的地連接埠。如果您的應用程式僅用於TCP流量，您可以建立規則來拒絕所有UDP流量，反之亦然。此選項在回應攻DDoS擊時非常有用，因為它可讓您建立自己的規則，以在知道來源IPs或其他簽章時緩解攻擊。

如果您已訂閱 AWS Shield Advanced，則可以將彈性 IP 位址註冊為受保護的資源。DDoS針對已註冊為受保護資源的彈性 IP 位址的攻擊會更快速地偵測到，進而縮短緩解的時間。偵測到攻擊時，DDoS緩和系統會讀取與目標 Elastic IP 位址對應的網路，並在網路邊界 (而非子 AWS 網路層級) 強制執行ACL該網路。如此可大幅降低您受到許多基礎架構層DDoS攻擊的影響風險。

如需有關設定安全群組和網路ACLs以最佳化DDoS恢復能力的詳細資訊，請參閱如何透過減少攻擊面協助準備攻擊。DDoS

如需使用 Shield 進階搭配彈性 IP 位址做為受保護資源的詳細資訊，請參閱訂閱步驟 AWS Shield Advanced。

保護您的來源 (BP1,BP5)

如果您使用的 Amazon 來源位於您的原產地VPC，您可能需要確保只 CloudFront 有您的 CloudFront 分發才能將請求轉發到您的來源。使用邊對來源請求標頭，您可以在將請求 CloudFront 轉發到來源時，新增或覆寫現有請求標頭的值。您可以使用 Origin 自訂標頭 (例如標`X-Shared-Secret`頭) 來協助驗證對您來源所發出的要求是從中傳送的 CloudFront。

如需有關使用 Origin 自訂標頭保護來源的詳細資訊，請參閱將自訂標頭新增至原始要求和限制應用程式負載平衡器的存取權。

如需實作範例解決方案以自動輪替原始存取限制的 Origin 自訂標頭值的指南，請參閱如何使用 AWS WAF 和 Secrets Manager 來增強 Amazon CloudFront 來源安全性。

或者，您可以使用AWS Lambda功能自動更新安全群組規則，以僅允許 CloudFront 流量。這可協助確保惡意使用者無法略過，以及存取您的 Web 應用程式 AWS WAF 時 CloudFront ，藉此改善來源的安全性。

如需如何透過自動更新安全群組和`X-Shared-Secret`標頭來保護原始伺服器的詳細資訊，請參閱如何自動更新 Amazon 的安全群組 CloudFront 和使 AWS WAF 用 AWS Lambda。

不過，該解決方案涉及額外的組態和執行 Lambda 函數的成本。為了簡化此操作，我們現在引入了一個 AWS-managed 前綴列表，用 CloudFront於僅限從 CloudFront面向起點的 IP 地址將入站HTTP/HTTPS流量限制到您的來源。 AWS-managed 前綴列表由創建和維護， AWS 並且可以使用，無需額外費用。您可以參考 (AmazonVPC) 安全群組規則、子網路路由表、一般安全群組規則，以及任何其他可使用受 AWS 管前置詞清單的受管前置詞清單。 CloudFront AWS Firewall Manager

如需有關在 Amazon 使用 AWS-managed 前置詞清單的詳細資訊 CloudFront，請參閱使用 Amazon 的 AWS-managed 前置詞清單限制對來源的存取。 CloudFront

> **Note**
>
> 如本文件其他章節所討論的，依賴安全群組來保護您的來源，可以在要求氾濫期間，將安全性群組連線追蹤新增為潛在的瓶頸。除非您能夠 CloudFront 使用啟用快取的快取政策來篩選惡意要求，否則最好依賴先前討論過的 Origin 自訂標頭，以協助驗證對您來源所發出的要求是從中傳送的 CloudFront，而不是使用安全性群組。將自訂要求標頭與 Application Load Balancer 接聽程式規則搭配使用，可防止因追蹤限制而影響到負載平衡器建立新連線而導致的限制進行調整，進而允許「Application Load Balancer」根據發生攻擊時的流量增加進行調整。DDoS

保護API端點 (BP4)

當您必須向公眾暴露時，存在API前端可能受API到DDoS攻擊目標的風險。為了協助降低風險，您可以使用 Amazon API Gateway 做為在 Amazon EC2 或其他地方執行之應用程式的入口通 AWS Lambda 道。透過使用 Amazon API Gateway，您不需要自己的API前端伺服器，而且可以混淆應用程式的其他元件。藉由使偵測應用程式元件變得更加困難，您可以協助防止這些 AWS 資源受到DDoS攻擊的目標。

使用 Amazon API 閘道時，您可以從兩種API端點類型中進行選擇。第一個是預設選項：透過 Amazon CloudFront 分發存取的邊緣最佳化API端點。但是，該分發由 API Gateway 創建和管理，因此您無法控制它。第二個選項是使用從部署的相同API端點存取 AWS 區域 的區域端點。REST API AWS 建議您使用第二種類型的端點，並將其與您自己的 Amazon CloudFront 分發產生關聯。這使您可以控制 Amazon CloudFront 分發以及用 AWS WAF 於應用程序層保護的能力。此模式可讓您存取整個 AWS 全球邊緣網路的擴充DDoS緩和容量。

使用 Amazon CloudFront 和 AWS WAF Amazon API 閘道時，請設定下列選項：

- 為您的分發配置緩存行為，以將所有標頭轉發到 API Gateway 地區端點。通過這樣做， CloudFront 會將內容視為動態內容並跳過緩存內容。
- 透過在 API Gateway 中設定API金鑰值，將散發設定為包含來源自訂標頭 x-api-key，以保護API閘道不受直接存取的影響。
- 透過為您的 RESTAPIs. 中的每個方法設定標準或突發速率限制，以保護後端免受過量流量的影響

如需有關APIs使用 Amazon API 閘道建立的詳細資訊，請參閱 Amazon API 閘道入門。

操作技巧

本 paper 中的緩解技術可協助您架構具備本質彈性抵禦攻擊DDoS的應用程式。在許多情況下，了解DDoS攻擊何時針對您的應用程序也很有用，以便採取緩解措施。本節討論瞭解異常行為、警示和自動化、大規模管理保護，以及獲得額外支援的最 AWS 佳實務。

負載測試

使用我們的負載測試應用程式白皮書中的準則，定期對應用程式進行負載測試，其中包含預期和高於預期流量水平，因此您可以了解架構的有效性、Auto Scaling 政策的運作方式以及錯誤處理的運作方式。測試預期的流量向上和向下擴展，但也測試「閃光人群」類型行為。定期或在任何主要版本之前重新測試。對於第 3 層或第 4 層DDoS模擬測試，例如SYN洪水，請遵循我們的DDoS模擬測試政策。

指標與警示

最佳作法是使用基礎結構和應用程式監視工具來檢查應用程式的可用性，以確保您的應用程式不受DDoS事件影響，您可以選擇為資源設定應用程式和基礎結構 Route 53 運作狀態檢查，以協助改善DDoS事件的偵測。如需狀態檢查的詳細資訊 AWS WAF，請參閱 Firewall Manager 員和 Shield 進階開發人員指南。

當金鑰作業指標大幅偏離預期值時，攻擊者可能會嘗試鎖定應用程式的可用性。熟悉應用程式的正常行為，意味著您可以在偵測到異常情況時更快地採取行動。Amazon CloudWatch 可以透過監控您執行的應用程式來提供協助 AWS。例如，您可以收集和追蹤指標、收集和監視記錄檔、設定警示，以及自動回應 AWS 資源中的變更。

如果您在架構應用程式時遵循 DDoS-彈性參考架構/彈性參考架構，常見的基礎架構層攻擊會在到達應用程式之前遭到封鎖。如果您已訂閱 AWS Shield Advanced，則可以存取許多指標，這些度CloudWatch量可以指出您的應用程式已成為目標。

例如，您可以將警示設定為在DDoS攻擊進行時通知您，以便檢查應用程式的健康狀態並決定是否要參與 AWS SRT。您可以設定`DDoSDetected`指標，告訴您是否已偵測到攻擊。如果您想要根據攻擊量收到警示，您也可以使用`DDoSAttackBitsPerSecond`DDoSAttackPacketsPerSecond、或`DDoSAttackRequestsPerSecond`指標。您可以透過與自己的工具整 CloudWatch 合或使用第三方提供的工具 (例如 Slack 或 PagerDuty) 來監控這些指標。

應用程式層攻擊可提升許多 Amazon CloudWatch 指標。如果您正在使用 AWS WAF，則可以用 CloudWatch 來監控和啟用您設定為允許、計數或封鎖的 AWS WAF 要求增加時的警示。如果流量級別超過應用程式可以處理的範圍，這可讓您收到通知。您也可以使用追蹤的 Amazon

CloudFront、Amazon Route 53、Application Load Balancer 用程式負載平衡器EC2、Network Load Balancer、Amazon 和 Auto Scaling 指標，以偵測可能指出DDoS攻擊的變更。 CloudWatch

下表列出常用於偵測和回應DDoS攻擊的 CloudWatch 度量說明。

表 3-推薦的 Amazon CloudWatch 指標

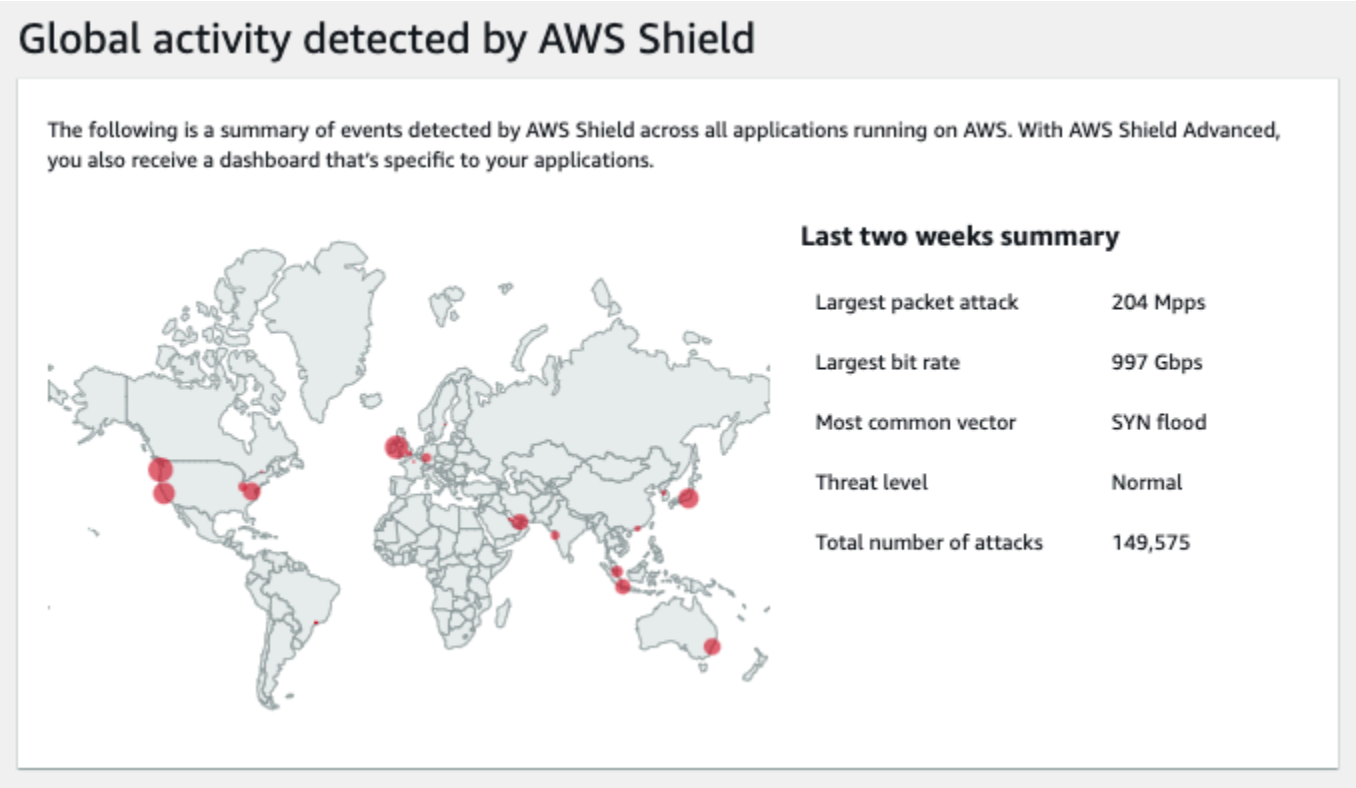
主題	指標	描述
AWS Shield Advanced	DDoSDetected	表示特DDoS定 Amazon 資源名稱 (ARN) 的事件。
AWS Shield Advanced	DDoSAttackBitsPerSecond	特定DDoS事件期間觀察到的位元組數ARN。此量度僅適用於第 3 層或第 4 層DDoS事件。
AWS Shield Advanced	DDoSAttackPacketsPerSecond	特定DDoS事件期間觀察到的封包數目ARN。此量度僅適用於第 3 層或第 4 層DDoS事件。
AWS Shield Advanced	DDoSAttackRequestsPerSecond	特定DDoS事件期間觀察到的要求數目ARN。此量度僅適用於第 7 層DDoS事件，且僅針對最重要的第 7 層事件報告。
AWS WAF	AllowedRequests	允許的 Web 要求數目。
AWS WAF	BlockedRequests	封鎖的 Web 要求數目。
AWS WAF	CountedRequests	計入的 Web 要求數目。
AWS WAF	PassedRequests	傳遞的要求數目。這僅適用於經過規則群組評估但不符合任何規則群組規則的要求。
Amazon CloudFront	Requests	HTTP/S 請求的數量。
Amazon CloudFront	TotalErrorRate	HTTP狀態碼為4xx或之所有要求的百分比5xx。

主題	指標	描述
Amazon Route 53	HealthCheckStatus	健全狀況檢查端點的狀態。
Application Load Balancer	ActiveConnectionCount	從用戶端到負載平衡器，以及從負載平衡器到目標的作用中並行TCP連線總數。
Application Load Balancer	ConsumedLCUs	負載平衡器使用的負載平衡器容量單位 (LCU) 數目。
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	負載平衡器產生的HTTP4xx或5xx用戶端錯誤碼數目。
Application Load Balancer	NewConnectionCount	從用戶端到負載平衡器，以及從負載平衡器到目標之間建立的新TCP連線總數。
Application Load Balancer	ProcessedBytes	負載平衡器處理的位元組總數。
Application Load Balancer	RejectedConnectionCount	因負載平衡器已達其連線數目上限而拒絕的連線數目。
Application Load Balancer	RequestCount	已處理的要求數目。
Application Load Balancer	TargetConnectionErrorCount	在負載平衡器與目標之間未成功建立的連線數目。
Application Load Balancer	TargetResponseTime	要求離開負載平衡器後，直到收到來自目標的回應所經過的時間 (以秒為單位)。
Application Load Balancer	UnHealthyHostCount	視為不健康的目標數目。
Network Load Balancer	ActiveFlowCount	從用戶端到目標的並行TCP流程 (或連線) 總數。

主題	指標	描述
Network Load Balancer	ConsumedLCUs	負載平衡器使用的負載平衡器容量單位 (LCU) 數目。
Network Load Balancer	NewFlowCount	期間內從用戶端到目標建立的新TCP流程 (或連線) 總數。
Network Load Balancer	ProcessedBytes	負載平衡器處理的位元組總數，包括 TCP /IP 標頭。
Global Accelerator	NewFlowCount	此時段內從用戶端到端點建立的新UDP流程TCP和流程（或連線）總數。
Global Accelerator	ProcessedBytesIn	加速器處理的傳入位元組總數，包括 TCP /IP 標頭。
Auto Scaling	GroupMaxSize	Auto Scaling 群組的最高大小。
Amazon EC2	CPUUtilization	目前使用中的已配置EC2運算單元百分比。
Amazon EC2	NetworkIn	執行個體在所有網路介面上收到的位元組數目。

如需有關使用 Amazon 偵測應 CloudWatch 用程式DDoS攻擊的詳細資訊，請參閱 Amazon 入門 CloudWatch。

AWS 包含數個額外的指標和警示，以通知您有關攻擊並協助您監控應用程式的資源。 AWS Shield 控制台或API提供每個帳戶的事件摘要和有關已檢測到的攻擊的詳細信息。



偵測到的全域活動 AWS Shield

此外，全域威脅環境儀表板還提供有關偵測到的所有DDoS攻擊的摘要資訊 AWS。除了攻擊趨勢之外，這項資訊可能有助於更好地瞭解更多應用程式中的DDoS威脅，並與您可能觀察到的攻擊進行比較。

如果您已訂閱 AWS Shield Advanced，服務儀表板會顯示在受保護資源上偵測到的事件的其他偵測和緩和措施指標，以及網路流量詳細資料。 AWS Shield 沿著多個維度評估受保護資源的流量。偵測到異常時， AWS Shield 會建立事件並報告觀察到異常的流量維度。使用放置緩解措施，可防止您的資源接收符合已知DDoS事件簽章的過多流量和流量。

偵測指標是以取樣的網路流程或 AWS WAF 記錄檔ACL為基礎，當網路與受保護的資源相關聯。緩解指標是以 Shield DDoS 緩解系統觀察到的流量為基礎。緩解指標是更精確地衡量資源流量。

網路主要貢獻者量度可讓您深入瞭解偵測到的事件期間流量來自何處。您可以檢視最高的磁碟區貢獻者，並依通訊協定、來源連接埠和TCP旗標等方面進行排序。頂級貢獻者量度包括在不同維度上在資源上觀察到的所有流量的指標。它提供了額外的指標維度，您可以用來瞭解事件期間傳送至資源的網路流量。請記住，對於非反射層 3 或第 4 層攻擊，源 IP 地址可能已被欺騙並且無法依賴。

服務儀表板也包含自動為緩解DDoS攻擊而採取的動作的詳細資料。此資訊可讓您更輕鬆地調查異常情況、探索流量的維度，並更好地瞭解 Shield Advanced 採取的行動來保護您的可用性。

日誌

根據應用程式擁有者的記錄和監控指南，在所有服務上啟用有用的記錄功能，以最大程度地提高可見性並協助進 這包括但不限於：

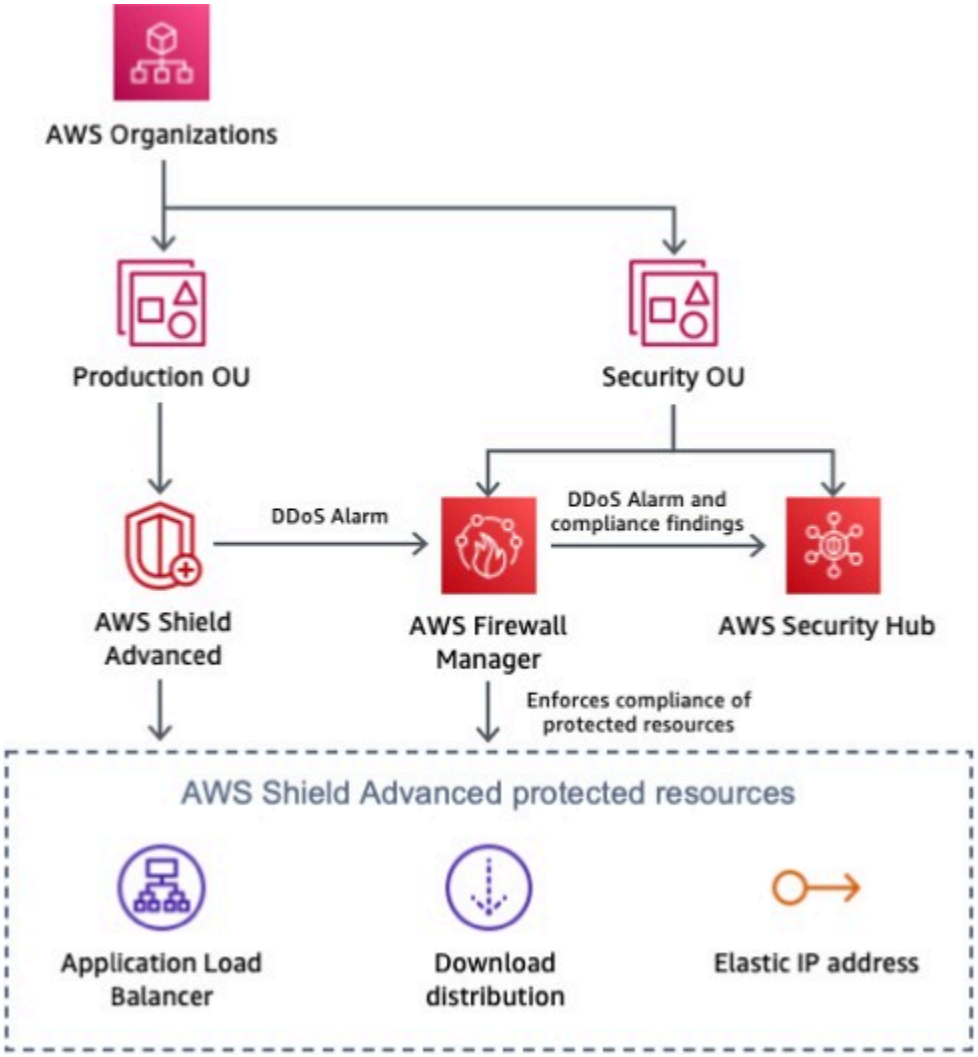
- AWS CloudTrail
- AWS WAF 日誌
- CloudFront存取記錄
- VPC流量日誌（請參閱記錄和查看網絡流量）— 在包含的字tcp-flags段中包含字段以最大程度地提高可見性
- ELB存取記錄 (ALB、CLB、NLB)
- Web 伺服器HTTP存取記錄
- 作業系統安全性記錄
- 應用程式記

跨多個帳戶的能見度和保護管理

在您跨多個作業 AWS 帳戶 且要保護多個元件的情況下，使用可讓您大規模操作並減少營運開銷的技術，可增加您的緩解功能。在多個帳戶中管理 AWS Shield Advanced 受保護的資源時，您可以使用 AWS Firewall Manager 和來設定集中監控 AWS Security Hub。使用 Firewall Manager 員，您可以建立安全性原則，在所有帳戶中強制執行DDoS保護法規遵循。您可以同時使用這兩項服務，跨多個帳戶管理受保護的資源，並集中監控這些資源。

Security Hub 會自動與 Firewall Manager 員整合，讓 Shield Advanced 客戶可以在單一儀表板中檢視安全發現項目，以及其他高優先順序的安全警示和合規狀態。

例如，當 Shield Advanced 偵測到目的地在範圍 AWS 帳戶 內任何受保護資源的異常流量時，此發現項目將會顯示在 Security Hub 主控台中。如果已設定，Firewall Manager 可以將資源建立為受防護進階保護的資源，藉此自動將資源設為符合規範，然後在資源處於相容狀態時更新 Security Hub。



架構圖顯示使用 Firewall Manager 器和 Security Hub 監控 AWS Shield受保護的資源

如需有關 Shield 受保護資源的集中監控的詳細資訊，請參閱設定DDoS事件集中監控和自動修復不符合標準的資源。

事件應變策略和手冊

對於所有組織而言，制定DDoS攻擊事件回應策略並圍繞其建立安全事件回應流程至關重要。建議的方法是根據建議的步驟 (例如收集證據、緩解、復原和執行事件後分析) 來建立回應手冊的模型。NIST例如，提供 Web 應用程式 DoS 或DDoS攻擊的回應教戰手冊做為範例。有關其他資源，請參閱保AWS安事故應變指南。

支援

如果您遭遇攻擊，您也可以從評估威脅和檢閱應用程式架構方面獲得支援，或者您可能想要求其他協助。 AWS 在實際事件發生之前，建立DDoS攻擊的回應計畫很重要。本 paper 概述的最佳作法旨在成為您在啟動應用程式之前實施的主動式措施，但仍可能會發生針對應用程式的DDoS攻擊。檢閱本節中的選項，以決定最適合您案例的支援資源。您的客戶團隊可以評估您的使用案例和應用程序，並協助解決您遇到的特定問題或挑戰。

如果您正在執行生產工作負載 AWS，請考慮訂閱商業 Support，這可讓您全年無休存取可協助解決DDoS攻擊問題的雲端 Support 工程師。如果您正在執行關鍵任務工作負載，請考慮 Enterprise Support，該支援可提供開啟關鍵案例的能力，並從資深雲端 Support 工程師獲得最快回應。

如果您已訂閱 AWS Shield Advanced 並訂閱商業支援或企業支 Support，您可以設定 Shield 主動參與。它可讓您設定運作狀態檢查、與您的資源建立關聯，以及提供全年無休的作業聯絡資訊。當 Shield 偵測到跡象DDoS並且您的應用程式健康狀態檢查顯示出降解跡象時， AWS SRT會主動與您聯絡。這是我們推薦的參與模式，因為它允許最快的 AWS SRT響應時間，並有權 AWS SRT在與您建立聯繫之前開始進行故障排除。

如需詳細資訊，請參閱比較 AWS Support 計劃。

主動參與功能需要您設定 Route 53 健康狀態檢查，以準確測量應用程式的健康狀態，並與受 Shield Advanced 保護的資源產生關聯。在 Shield 主控台中關聯 Route 53 健康狀態檢查後，Shield 進階偵測系統就會使用健康狀態檢查狀態作為應用程式健康狀態的指標。Shield Advanced 中的健康狀況型偵測功能可確保您收到通知，並在您的應用程式運作狀況不佳時更快地放置緩解措施。 AWS SRT將連絡您以疑難排解狀態不良的應用程式是否受到DDoS攻擊的目標，並視需要設置其他緩和措施。

完成主動互動的組態包括在 Shield 主控台中新增聯絡人詳細資料。 AWS SRT將使用此信息與您聯繫。您最多可以設定十個連絡人，如果您有任何特定的聯絡需求或偏好設定，請提供其他備註。主動

參與聯繫人應該擔任 24/7 的角色，例如安全運營中心或立即可用的個人。

您可以為所有資源啟用主動參與，或針對回應時間至關重要的特定主動生產資源啟用。這是透過僅將健康狀態檢查指派給這些資源來完成的。

您也可以使用AWS Support 主控台建立 AWS Support 案例 (需要登入)，或者API如果您有影響應用程式可用性的DDoS相關事件，則可以升級為「Sup port」。 AWS SRT

結論

本 paper 概述的最佳作法可協助您建置DDoS彈性架構，藉由防止許多常見的基礎架構和應用程式層DDoS攻擊來保護應用程式的可用性。您在架構應用程式時遵循這些最佳做法的程度，將會影響您可以緩解的DDoS攻擊類型、媒介和數量。您可以在不訂閱DDoS緩解服務的情況下合併復原。透過選擇訂閱， AWS Shield Advanced 您可獲得額外的支援、可見性、緩解和成本保護功能，進一步保護已有彈性的應用程式架構。

貢獻者

本文件的貢獻者包括：

- 羅德里戈·費羅尼, 安全專家 AWS TAM
- 德米特里·諾維科夫，解決方案架構師 AWS
- 阿赫拉夫市集，解決方案架構師 AWS
- 喬安娜·諾克斯, 工程 AWS Support
- 阿努吉·布塔爾, AWS 解決方案架構師
- 哈里斯·卡達曼努古邊緣專家 SA AWS

深入閱讀

如需其他資訊，請參閱：

- 實施指引 AWS WAF (AWS 白皮書)
- NIS301 — Re：InForce 2023： AWS 威脅情報如何成為受管理的防火牆規則（影片）YouTube
- NET314-RE：發明 2022 年：使用（視頻）構建DDoS具有彈性的應用程序 AWS Shield YouTube
- SEC321-Re：2020 年發明：通過DDoS響應團隊升級（視頻）來領先曲線 YouTube
- 威廉·希爾：具有 AWS-2020 的高性能DDoS保護（YouTube視頻）
- SEC407-重要：發明 2019 年：構建 Web 應用程序的 defense-in-depth 方法（視頻）YouTube
- 2018 年DDoS緩解措施的 AWS最佳做法（YouTube視頻）
- SID324— 回复:發明 2017: 在雲中自動化DDoS響應 (視頻) YouTube
- CTD304 — RE：發明 2017 年：道瓊斯和華爾街日報管理交通峰值的旅程（視頻）YouTube
- 緩解DDoS與應用程式層威脅 (YouTube 影片)
- CTD310 — 重要:發明 2017: 生活在邊緣, 它比你想像的更安全! 建立強大的 Amazon（YouTube 視頻）
- CloudFront、 AWS Shield、和 AWS WAF (YouTube 影片)

文件修訂

若要收到有關此白皮書更新的通知，請訂閱RSS摘要。

變更	描述	日期
白皮書更新	添加OAC了DNS通 CloudFront 配符成本保護。擴大操作技巧、快取、速率型規則和受管規則群組的討論。將內部部署新增到架構圖中、移除重複項目，以及澄清文字以消除歧義。	2023 年 8 月 9 日
白皮書更新	為了清楚起見而修訂；更新為包含最新建議和功能：安全群組連線追蹤和 Shield Advanced 自動應用程式層DDoS緩解功能。	2022 年 4 月 13 日
白皮書更新	已更新以包含最新的建議和功能。 AWS Global Accelerator 作為邊緣全面保護的一部分添加。 AWS Firewall Manager 用於集中監控DDoS事件並自動修復不符合標準的資源。	2021 年 9 月 21 日
白皮書更新	已更新以闡明「偵測並篩選惡意 Web 要求」(BP1,BP2) 區段中的快取破壞，以ELB及「縮放至吸收」(BP6) 區段中的和ALB使用情況。更新圖表和表 2，標記為「區域的選擇」。作為BP8。更新了更多的細BP7節部分。	2019 年 12 月 18 日

白皮書更新	已更新，將 AWS WAF 記錄納入為最佳作法。	2018 年 12 月 1 日
白皮書更新	已更新為包含 AWS Shield AWS Firewall Manager、AWS WAF 功能和相關的最佳做法。	2018 年 6 月 1 日
白皮書更新	已新增規範架構指引，並已更新為包含 AWS WAF。	2016 年 6 月 1 日
初次出版	白皮書已發佈。	2015 年 6 月 1 日

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品供應項目和做法，如有變更，恕不另行通知，且 (c) 不會向其關聯公司、供應商或授權人建立任何承諾或保證。 AWS AWS 產品或服務係依「原狀」提供，不含任何明示或暗示之擔保、陳述或條件。客戶的責任和責任由 AWS 協議控制，本文件不屬於與客戶之間 AWS 的任何協議的一部分，也不會修改。 AWS

AWS 詞彙表

有關最新 AWS 術語，請參閱AWS 詞彙表 參考文獻中的AWS 詞彙表。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。