DATA SHEET

A10 Defend Detector

精確、高度可擴展的全網路異常偵測

A10 Defend Detector (前身為 Thunder TPS) 為 A10 Defend 套件的一部分，提供流量型高效能網路異常偵測，可透過自動流量行為剖析提供精確、更快的 DDoS 偵測。有了 A10 Defend Orchestrator 和 Mitigator，便能實現適合全網路防護的智慧自動化 DDoS 防禦。

偵測現代 DDoS 攻擊

在現今的超連結世界中，服務供應商和大型企業面臨著持續不斷的威脅。在各種威脅之中，分散式阻斷服務 (DDoS) 攻擊因其強大的威力，以及有能力破壞關鍵服務和基礎架構而脫穎而出。DDoS 攻擊以大量惡意流量淹沒受害者的網路，刻意造成服務中斷、擾亂營運，最終損害企業聲譽。

對組織來說，現代 DDoS 攻擊是一項巨大的挑戰。攻擊者擁有大量工具可供運用，從 DDoS 工具組、線上服務 (DDoS 即服務) 和武器化物聯網裝置，再到 DDoS 殭屍網路。攻擊者經常利用開放式網際網路伺服器中的漏洞，發動反射放大攻擊，進而放大攻擊量並隱藏其真正來源。讓情況更為複雜的是，攻擊者可能採用地毯式轟炸攻擊，將攻擊傳播到多個目標 (一系列 IP 位址)，可能多次觸發警示，耗盡 DDoS 清理能力。眾多技巧的組合運用，使得 DDoS 防禦的挑戰變得異常艱鉅。

平台

實體設備

虛擬設備

相關的產品與服務

A10 Defend Mitigator

A10 Defend Orchestrator

A10 Defend Threat Control

DSIRT

DSIRT 支援

與 A10 交談

A10Networks.com/a10-defend

精準至關重要

簡單的流量攻擊雖然可透過監控流量來偵測，但這種方法可能無法有效應對現今的複雜威脅。傳統解決方案存在著高誤報率、延遲偵測及資源消耗緩解等問題。因此服務網路容易遭受攻擊，在關鍵時刻浪費寶貴的資源和時間。

隨著現代 DDoS 攻擊的數量和複雜性不斷增加，DDoS 防護也不斷進化，因此我們需要一套全方位 DDoS 防護套件。A10 Defend Detector 為全方位 A10 Defend 套件的一部分，是一款具有更高精度且智慧的高效能全網路 DDoS 偵測解決方案。

A10 Defend Detector 是一種基於網路流量的獨立流量異常偵測技術，可透過 NetFlow 或 IPFIX 從路由器收集網路流量資訊，追蹤流量行為和模式，並使用獨特的指示器建立基線分析。其支援持續的流量模式學習，能省去繁瑣且耗時的工作，同時還能確保動態閾值，實現精確的異常偵測並加快緩解速度。

其提供無與倫比的效能和容量，能讓組織減少基於流量的偵測器，並簡化部署。與 A10 Defend Orchestrator 和 Mitigator 結合，將能簡化整個 DDoS 保護週期，還可透過智慧自動化流暢執行，從偵測、流量分流到清理中心，以及事件過後的緩解和報告。

由 A10 Defend Detector、Mitigator、Orchestrator 和 Threat Control 組成的 A10 Defend 套件可協助組織實現更有效的 DDoS 防護和/或為其客戶建立可獲利的 DDoS 清理服務。A10 Networks 會在您最需要協助時伸出援手。A10 Networks 支援提供 24 小時全年無休服務，包括來自 A10 DDoS 安全事件應變團隊 (DSIRT) 的緊急援助，可立即協助您瞭解並回應 DDoS 事件。

A10 Defend 套件

A10 Defend Detector

高效能 NetFlow、sFlow、基於 IPFIX 的 DDoS 偵測器可輕鬆管理 SP 網路的規模和異質性質，產生統一的 DDoS 防護解決方案。

A10 Defend Mitigator

高精度、自動化、可擴展且智慧的 DDoS 緩解解決方案，以硬體或虛擬設備的形式提供，速度從 1 Gbps 到 1 Tbps 以上。

A10 Defend Orchestrator

使組織能取得其環境的全域視圖，以快速識別和修復 DDoS 攻擊，並確保從中心點一致執行政策。

A10 Defend Threat Control

獨立 SaaS 平台透過提供可採取行動的分析和封鎖清單，主動建立強大的第一層防禦。

優勢

最大化

服務可用性

停機會立即對任何企業造成生產力和營收損失。因此對組織來說，保護其網路基礎架構、關鍵任務應用程式及其訂戶和租戶免受現今不斷發展的 DDoS 攻擊至關重要。A10 Defend Detector 透過利用獨特的行為流量指示器和持續學習來提供精確的流量異常偵測，協助組織在 DDoS 攻擊影響其網路和客戶服務之前採取適當的行動和補救措施。

簡化

部署和作業

DDoS 防護部署和作業可以是一個非常複雜的過程，沒有組織能取得無限的訓練有素的人員或資源，因為許多其他的安全考量和問題大多交給 SecOps 團隊處理。A10 Defend 套件提供完整的解決方案，包括自動流量剖析和監控、精確的 DDoS 偵測、最小化誤報和漏報、無縫編排和流量轉移、智慧自動化的多模式緩解和自動產生事件報告。此外，A10 的 DSIRT 可在 DDoS 攻擊事件發生的任何階段與 SecOps 團隊即時合作。

對抗

現代攻擊

現代 DDoS 攻擊持續發展，早已遠遠超出簡單的大容量洪水攻擊。現在的攻擊更為複雜、多層次，且經常利用多種技術來逃避偵測。例如，反射放大攻擊就是一種常用的技術，通常利用網際網路伺服器中的漏洞來放大攻擊流量，因此更難識別真正的來源。地毯式轟炸攻擊是另一種將攻擊目標傳播到廣泛 IP 位址的技術，同樣也會使得目標識別變得更加困難，並可能產生數量難以控制的警示。攻擊者有時會結合這些技術。A10 Defend Detector 具有多種偵測機制，可精確偵測此類複雜的目標性容量攻擊。

降低

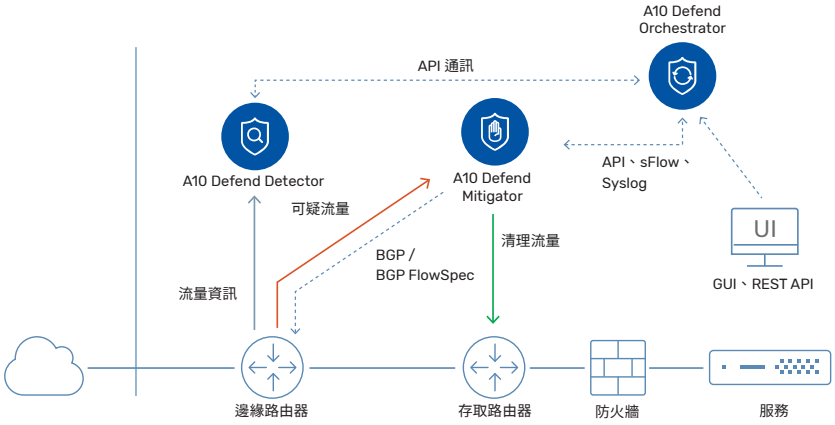
安全營運支出

在監控全網路和大流量時，基於網路流量的 DDoS 偵測就營運和成本效益來說是正確的選擇。

A10 Defend Detector 極其有效，儘管外型尺寸小巧，卻具備高效能，1 RU 的體積每秒能處理高達 600 萬個流量，可覆蓋廣泛範圍的網路 (或將數十個傳統的流量型偵測器整合為一)。這能降低營運成本，亦能大幅降低用電量、機架空間和冷卻需求。

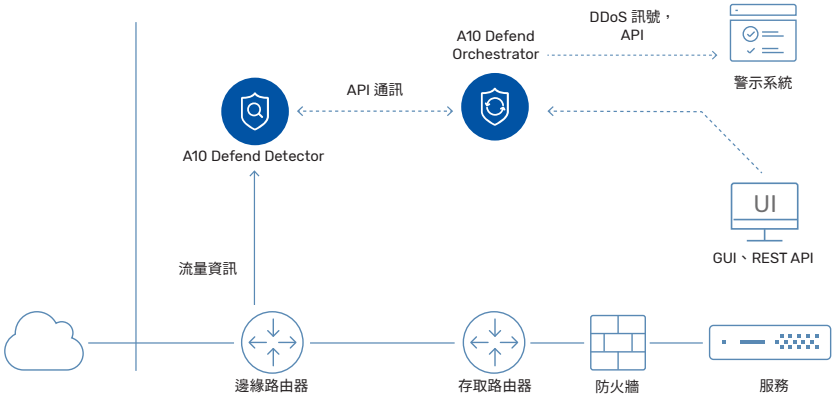
A10 Defend Detector 的規模和智慧自動化經由 A10 Defend Orchestrator 協調，簡化從偵測、緩解到報告的完整 DDoS 防護工作流程和生命週期，同時加強安全態勢。A10 Defend 解決方案不只能最大化 SecOps 團隊的效率，還能降低營運成本，進而改善投資報酬率。

參考架構



反應式部署

對於大型網路而言，手動觸發或由流量分析系統觸發的隨選緩解功能很有幫助。A10 Defend Detector 可作為獨立設備（硬體或虛擬）使用。流量型 DDoS 偵測器支援與 A10 Defend Orchestrator 和 Mitigator 緊密整合，以實現智慧自動化 DDoS 防禦解決方案。A10 Defend Mitigator 能傳送 BGP FlowSpec，改善與上游路由器的協作。



僅偵測的部署

為了建立 DDoS 防護策略和里程碑，建議必須充分瞭解網路流量和異常活動。A10 Defend 套件可使用 A10 Defend Detector 和 Orchestrator 以僅偵測模式部署，用於深入瞭解受監控實體的網路流量，讓組織能根據收集的網路流量資訊瞭解實際的 DDoS 活動。A10 Defend Detector 偵測到 DDoS 攻擊時，Orchestrator 將提供詳細資訊，或可將警示轉發到組織的警示系統。

特色

高效能

偵測

A10 Defend Detector 為網路流量收集和 DDoS 偵測提供無與倫比的效能，硬體設備每秒可處理高達 600 萬個流量 (fps)，虛擬設備則能處理高達 150 萬個 fps。A10 Defend Detector 可透過區域配置監控多達 3,000 個受保護物件，或透過獨特的自動網路探索技術涵蓋網路物件配置中的數百個 B 類或數千個 C 類網路子網路。可將 10 個以上的流量型傳統 DDoS 偵測系統整合到一個 A10 Defend Detector 之中，如此將減少需要管理的裝置，進而簡化部署與管理。

精確

行為異常偵測

服務停機是任何組織都無法承受的後果；因此，DDoS 偵測對於最小化即將發生的 DDoS 攻擊的衝擊發揮重要的作用。A10 Defend Detector 使用獨特的流量和行為指標來追蹤網路流量模式，不僅有封包速率 (pps) 或流量 (bps)，也包含基於通訊協定或行為的速率，例如 TCP empty ACK rate 和 SYN/FIN ratio，還能針對區域物件下定義的每個服務自動學習，並建立行為流量設定檔。由於有這項技術，因此得以減少誤報並實現更快的偵測作業，實現精確的偵測。

智慧型

受害者識別

A10 Defend Detector 的網路區域物件使用受害者識別技術，適合需要自動化 DDoS 防禦解決方案的服務供應商，以保護其企業用戶，以及網路和服務基礎架構免受流量型 DDoS 攻擊及地毯式轟炸攻擊。其使用智慧自動化，自適應地切割受監控的網路實體，並根據即時流量分佈對作用中的子網路或 IP 的每個實體進行階層式分析。縮小受害者範圍，有助於保護 DDoS 清理中心資源，實現高效運作。在偵測策略方面，其採用進階基準，使用特徵直方圖，同時搭配使用以流量為中心的流量指示器的自動基準，確保高精度 DDoS 偵測。

自動

基線和剖析

判定流量模式基線是達成有效 DDoS 偵測的基礎。傳統上，判定網路流量基線會造成人力上的負擔，影響到敏捷性和準確性。A10 Defend Detector 提供自動基線，可持續學習流量模式並使用各種獨特的流量指標進行調整。如此將省去繁瑣的工作，同時確保擁有動態的閾值。無論是面臨季節性高峰或新興威脅，即時調整都有助於確保精確的異常偵測並加快緩解速度。自動化一方面提供速度和效率，另一方面也強化彈性和精細控制。客製化的基線和閾值可運用在特定的用戶、服務甚至單一伺服器上，實現精確的偵測，進而實現簡單、快速的偵測。透過自動化基線來簡化防禦，組織便能專注在最重要的工作，保護其網路和業務。

智慧

自動化

A10 Defend 套件為服務供應商和大型企業提供完整且自動化 DDoS 防護解決方案，能保護服務和用戶免受 DDoS 攻擊。在反應式或依據需求部署中，A10 Defend Detector 能與 A10 Defend Mitigator 和 Orchestrator 協同合作。當 Detector 偵測到攻擊並回報時，Orchestrator 會指示 Mitigator 啟動緩解措施並傳送 BGP 通知，以重新導向可疑流量。接著，Mitigator 會套用自適應對策，包括五級的漸進式緩解政策，以及自動升級和機器學習支援的自動零時差攻擊模式識別，然後再將乾淨的流量傳輸到預期目的地。

A10 Defend Detector 實體設備規格

Defend Detector	Thunder 3350-E	Thunder 5845-40G	Thunder 5845	Thunder 7445
流量偵測效能				
每秒流量 (fps)	1 Million	3 Million*3	3 Million	6 Million
網路介面				
1 GE 銅纜	6	0	0	0
1 GE 光纖 (SFP)	2	0	0	0
1/10 GE 光纖 (SFP+)	8+4*1	48	48	48
1/10 GE 光纖 (固定)	0	0	0	0
40 GE 光纖 (QSFP+)	0	0	0	0
100 GE 光纖	0	4 (QSFP28)	4 (QSFP28)	4 (QSFP28)
管理連接埠	乙太網路管理連接埠、RJ-45 主控台連接埠			
硬體規格				
處理器	Intel Xeon 8 核心	Intel Xeon 18 核心*3	Intel Xeon 18 核心	2 個 Intel Xeon 18 核心
記憶體 (ECC RAM)	16 GB	64 GB *3	64 GB	128 GB
儲存裝置	SSD	SSD	SSD	SSD
硬體加速	軟體	2 個 FTA-4，SPE	2 個 FTA-4，SPE	3 個 FTA-4，SPE
尺寸 (吋)	1.75 (H) x 17.5 (W) x 18(D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)
機架單元 (可安裝)	1U	1U	1U	1U
單元重量	18 lbs	34.3 lbs	34.3 lbs	35.7 lbs
電源 (提供 DC 選項)	雙 750W RPS	雙 1500W RPS	雙 1500W RPS	雙 1500W RPS
	80 Plus Platinum 效率，100-240 VAC，50-60 Hz			
耗電量 (典型/最大)*2	151W / 205W	585W / 921W	585W / 921W	784W / 1,078W
每小時熱量 (典型/最大) (單位：BTU)*2	516 / 700	1,997 / 3,143	1,997 / 3,143	2,676 / 3,679
冷卻風扇 (從前到後的氣流)	可拆式風扇、熱插拔智慧風扇			
作業範圍	溫度 0° - 40° C | 濕度 5% - 95%			
法規認證	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS	FCC Class A, UL, CE, CB, VCCI, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, CB, VCCI, BSMI, RCM | RoHS
標準保固	90 天硬體與軟體保固			

硬體規格和效能數據如有變更，恕不另行通知，並且可能因配置和環境條件而異。對於網路介面，強烈建議使用 A10 Networks 的合格光學/收發器，以確保網路的可靠性和穩定性。

*1 僅限 10Gbps 速度 | *2 使用基本型號 | *3 每秒流量 (fps)、作用中 CPU 核心數和記憶體大小可能因模組授權而異 | ^ 認證中

A10 Defend Detector 虛擬設備規格

A10 Defend Detector 虛擬設備	
支援的 Hypervisor	VMware ESXi 6.7 或以上版本 (SR-IOV)
硬體要求	請參閱安裝指南
標準保固	90 天軟體保固

虛擬設備授權和大小調整建議*

區域物件配置			
每秒流量 (fps)	150K	500K	1.5M
vCPU	2	3	5
vRAM	16 GB	32 GB	64 GB
vDisk	40 GB	40 GB	40 GB

網路物件配置			
每秒流量 (fps)	150K	500K	1.5M
vCPU	6	8	24
vRAM	16 GB	32 GB	64 GB
vDisk	40 GB	40 GB	40 GB

* 使用 A10 Defend Detector (前身為 Thunder TPS) 獨立式 Detector 映像。

詳細功能清單

功能可能因設備而異。

偵測/分析

- 網路流量型異常偵測
- 適用於超過 25.6 萬部伺服器和服務的個別偵測政策
- 持續的行為學習和剖析
- 自動化自適應閾值
- 自訂閾值
- 行為流量指示器和 TOP 排名
- 入站和出站偵測
- 服務探索
- 受害者網路/主機識別

受保護物件

- 每個服務等級監控的保護區
- 每個 IP 等級監控的保護區
- 子網路和 IP 等級監控的網路物件

動作

- 異常通知訊號 (啟動/停止)
- 報告和可視化
- 使用 A10 Defend Orchestrator 和 Mitigator 進行全自動緩解
- 使用 A10 Defend Orchestrator 和 Mitigator 進行手動緩解

管理

- 專屬內建管理介面 (GUI、CLI、SSH、Telnet)
- 適用於全面管理的 A10 Defend Orchestrator
- SNMP、Syslog、電子郵件警示
- REST API (aXAPI)
- LDAP、TACACS+、RADIUS 支援
- 可配置的控制 CPU

遙測

- 豐富的流量和 DDoS 統計資料計數器
- sFlow**
- NetFlow v5**、v9、IPFIX
- 用於流量型匯出的自訂計數器區塊
- 高速記錄
- CEF 記錄
- REST API (aXAPI)

高效能可擴展平台

- 先進核心作業系統 (ACOS)
- 線性應用程式擴充
- 資料平台上的 ACOS
- 控制平台上的 Linux
- IPv6 功能同位
- 安全政策引擎 (SPE) 支援硬體加速以執行政策*
- 高效能硬體封鎖*

電信級硬體*

- 先進硬體架構
- 熱插拔備援電源供應器 (AC 和 DC)
- 智慧風扇 (熱插拔)
- 固態硬碟 (SSD)
- 竄改偵測
- 40 GbE 和 100 GbE 連接埠

安全和功能保證認證*

- Common Criteria EAL 2+
- FIPS 140-1 Level 1 合規 (全部)

* 功能和認證可能因設備而異。

** 適用於區域型偵測。適用於網路物件偵測，將於 2024 年上半年開始支援。

深入瞭解

關於 A10 Networks

聯絡我們

APAC@a10networks.com

Part Number: A10-DS-15138-TW-01 Mar 2024