DATA SHEET

A10 Defend Orchestrator

DDoS 防禦監控、編排與管理

A10 Defend Orchestrator (前身為 aGalaxy® 管理系統) 是 A10 Defend 套件的一部分，與 A10 Defend Detector 和 Mitigator (前身為 Thunder TPS®) 整合，可實現智慧自動化 DDoS 防護，為流暢的 DDoS 防禦管理和執行提供集中控制點。

即時全球 DDoS 防禦管理

隨著現代 DDoS 攻擊的複雜性和數量不斷增加，DDoS 防護也不斷進化，因此我們需要一套全方位 DDoS 防護套件。部分全方位 A10 Defend 套件為集中管理元件。這個集中管理控制台確實有其必要，有助於客戶瞭解及管理現代 DDoS 攻擊和現代 DDoS 防護設備帶來的新複雜性。

A10 Defend DDoS 防護套件使企業、資料中心和服務供應商能精確區分 DDoS 攻擊者和有效使用者，並遏止不需要的流量。

此解決方案擁有領先業界的可擴展性，確保組織的第一線安全人員利用最佳化的戰時工作流程提高效率。

A10 Defend Orchestrator 使組織能取得其環境的全域視圖，以快速識別和修復攻擊，並確保從中心點一致執行 DDoS 防護政策。管理員可以使用來自 Defend Detector 和 Defend Mitigator 的遙測資料來配置及全面監控網路活動，即時觀察 DDoS 攻擊，並深入查看 DDoS 攻擊事件的詳細資料。

Defend Orchestrator 可擴充以管理跨地理位置的多個 Detector 和 Mitigator 部署，進而簡化營運並降低 IT 營運成本。

平台

虛擬設備

相關的產品與服務

DSIRT 支援

與 A10 交談

A10Networks.com/a10-defend

優勢

自動化

可強化保護的 DDoS 防禦

作為 DDoS 防護架構的中心點，A10 Defend Orchestrator 可在發生 DDoS 攻擊時與 A10 Defend Detector 和 Mitigator 協同合作，實現智慧自動化 DDoS 防禦。使用的方法包括 DDoS 偵測、警示、可疑流量轉移、DDoS 流量清理、採用多模式方法緩解攻擊，以及持續分析直到攻擊平息。這將大幅減輕手動作業的負擔，因為手動操作既耗時又容易出錯。

DDoS 事件結束後，Defend Orchestrator 會自動產生可透過電子郵件傳送的 DDoS 事件報告。安全操作人員可以安心取得智慧自動化 DDoS 防禦，包括從佈建、戰時作業到事件報告等工作流程。

加速

戰時回應

在即時 DDoS 攻擊期間，沒有組織能取得無限的訓練有素的人員或資源。A10 Defend 套件中的 A10 Defend Detector 可對即時流量執行流量分析，以監控 DDoS 攻擊，並根據動態學習的偵測閾值偵測流向受保護服務和受害者 IP 主機的任何流量異常。

如果發生 DDoS 攻擊，安全操作人員可透過 Defend Orchestrator 上名為「緩解控制台」的即時儀表板即時監控事件狀態，並可根據需要控制及管理 DDoS 防禦政策。A10 Defend Mitigator 強制執行多模式保護方法，包括基於 DDoS 威脅情報清單和攻擊篩選清單的緩解、具有自動緩解升級和降級的五級自適應保護，以及由機器學習技術支援的自動化零時差攻擊模式識別。如此能大幅改善回應時間，並將攻擊期間耗時的手動變更和重新評估緩解策略的需求降至最低。

最大化

IT 敏捷性和安全性

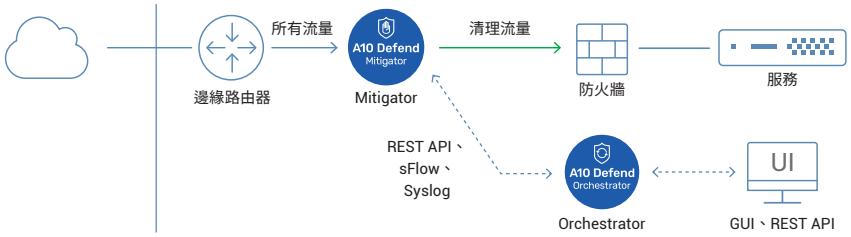
隨著網路業者轉為網路規模和 SecOps/DevOps 作法，他們需要快速佈建變更、識別問題並在必要時回溯配置。A10 Defend Orchestrator 可使用 A10 Defend Detector 輕鬆評估和瞭解網路流量模式，並使用圖形使用者介面或透過 REST API (aGAPI) 從中心點一次更新多個 A10 Defend Mitigator 上的緩解政策。A10 Defend Orchestrator 也支援與現有第三方 DDoS 偵測系統、外部 SIEM 和/或 Syslog 伺服器輕鬆整合，以實現整合的安全作業。

降低

安全營運支出

A10 Defend DDoS 防護極其有效。A10 Defend Detector 和 Mitigator 設備儘管外型尺寸小巧，卻具備高效能，可大幅降低用電量、機架空間和冷卻需求，進而降低營運成本。A10 Defend Orchestrator 支援智慧自動化 DDoS 防禦，有助於進一步降低營運複雜性和相關成本。

參考架構

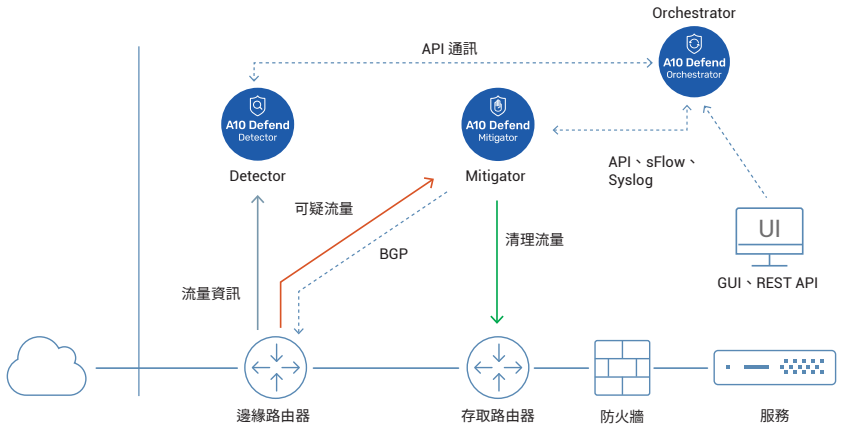


主動式部署

(非對稱或對稱)

在主動模式下部署 A10 Defend Mitigator 可提供持續、全面偵測和快速緩解。此模式對於使用者體驗至關重要的遊戲和 DNS 等即時服務以及針對應用層攻擊的防護非常有用。

A10 Defend Orchestrator 提供流量可見性及戰時 DDoS 緩解儀表板和控制台。



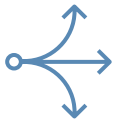
反應式部署

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 Orchestrator 與全域部署的 A10 Defend Detector 和 Mitigator 無縫整合，並能在偵測到流量異常時啟用自動化 DDoS 防護，以保護受害者免受 DDoS 攻擊。

A10 Defend 套件也可使用 A10 的開放 API 和/或 BGP FlowSpec 與第三方偵測解決方案搭配使用，以保護您的投資，同時強化 DDoS 防禦基礎架構。

特色

整個保護週期的智慧自動化



簡化

自動化操作

A10 Defend 提供業界最先進的智慧自動化功能，在整個防護生命週期內由機器學習提供支援。

操作人員定義要保護的網路後，A10 Defend Orchestrator 便會根據操作人員預定義的偵測和緩解策略完成其餘工作，包括個別學習的偵測閾值、自動流量重新導向編排、緩解和升級的啟動，以及套用自適應保護政策，然後擷取並套用攻擊模式篩選器。當攻擊消退時，網路和防禦將恢復到和平時期的態勢，並產生詳細的事件報告以供將來分析。

單一

管理平台

A10 Defend Orchestrator 具有直覺式介面，能讓組織管理跨地理位置的全域 DDoS 防禦部署，並取得其網路和 DDoS 事件的全域檢視。操作人員可以從一個中心點對所有託管的 A10 Defend 設備執行運行狀況檢查、備份、更新、修改配置、套用緩解範本及產生報告。

簡便

彈性的整合

A10 Defend Orchestrator 與現有第三方 DDoS 偵測系統無縫整合，可自動識別 DDoS 攻擊的跡象 (例如通訊協定異常、流量突然激增、來自已知機器人的大量請求)。一旦偵測到異常，便會使用 REST API (aGAPI) 動態建立 DDoS 攻擊事件。事件管理除了追蹤關鍵資訊 (例如攻擊持續時間和類型)，還能讓操作人員根據事件資料直接緩解攻擊。

戰時作業和報告

即時

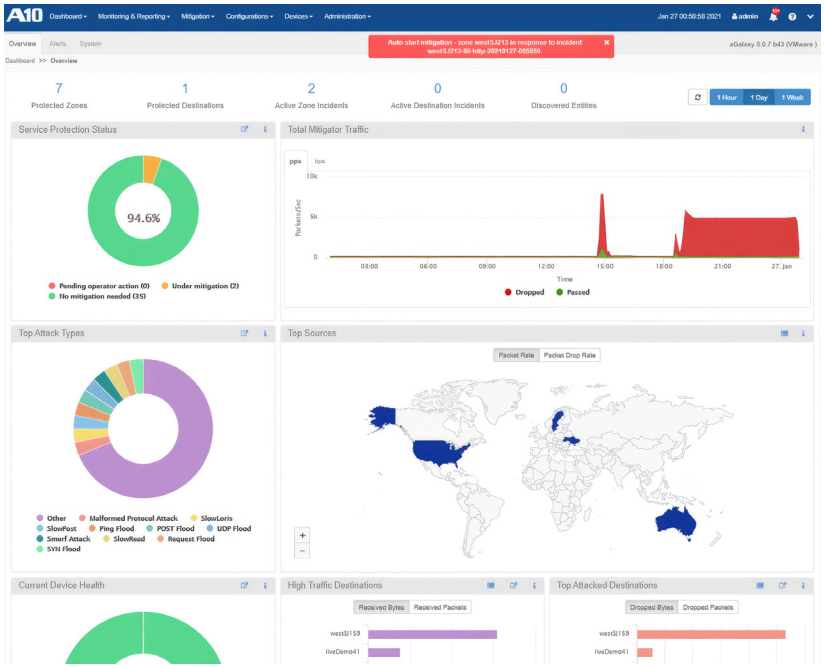
緩解控制台

在 A10 Defend Orchestrator 緩解控制台中，安全操作人員可以透過即時儀表板即時監控事件。以 DDoS 防禦為導向的儀表板提供即時可疑流量統計資料、套用的對策、事件詳細資訊 (包括緩解升級等級)、前 k 個資訊和活動日誌。為協助進一步進行事件調查，可以遠端啟用封包擷取和除錯器，並根據需要立即建立自訂對策。

健全

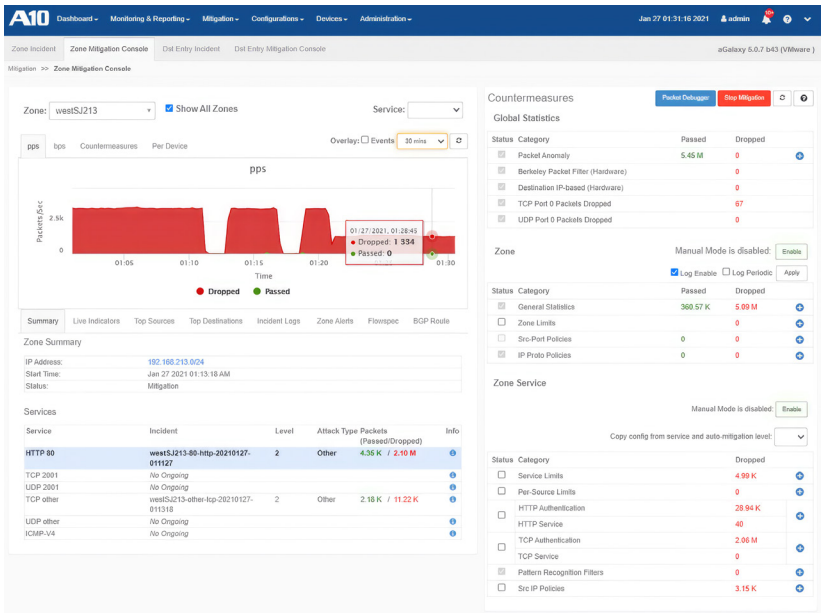
報告

A10 Defend Orchestrator 從託管的 A10 Defend Detector 和 Mitigator 裝置收集所有必要資料，以產生易於閱讀的事件報告，這些報告可以 PDF 或 CSV 格式匯出，還能立即透過電子郵件傳送、排程定期傳送或作為一次性通知。一旦 DDoS 攻擊事件結束，就會自動產生包含豐富遙測、計數器、圖表和事件日誌的詳細事件報告，而且可透過電子郵件分享給所有利害關係人。



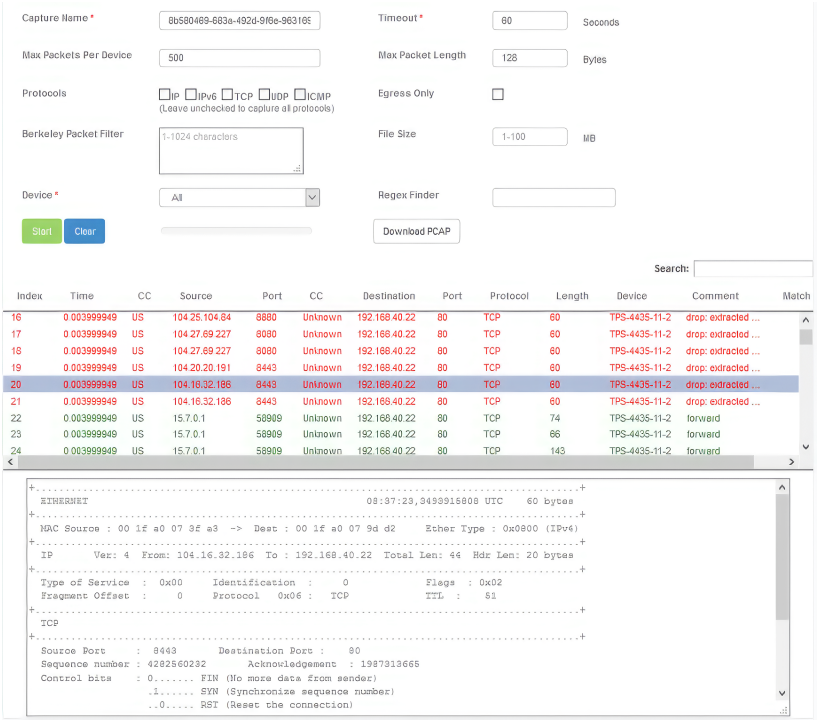
A10 Defend Orchestrator 儀表板

以 DDoS 防禦為導向的儀表板提供即時可疑流量統計資料和各種 DDoS 事件摘要，讓組織能追蹤安全事件、識別攻擊趨勢並解決法規遵循風險。



即時 DDoS 緩解控制台

從緩解控制台，安全操作人員可以檢視即時攻擊儀表板、檢查緩解狀態，並在需要時立即套用任何進階對策。緩解控制台提供即時統計資料和事件詳細資料，包含緩解升級等級、前 k 個資訊和活動日誌。



遠端封包擷取和除錯工具

為了協助在攻擊後或攻擊期間進行進一步事件調查，A10 Defend Orchestrator 可以遠端啟用封包擷取和除錯器，有助於根據需要建立自訂對策或篩選器。

A10 Defend Orchestrator 規格

A10 Defend Orchestrator 虛擬設備	
支援的 Hypervisor	VMware ESXi、KVM QEMU
硬體要求	請參閱安裝指南
標準保固	90 天軟體保固

虛擬設備大小調整建議

部署規模	100 個區域/1,000 項服務	1,000 個區域/8,000 項服務	3,000 個區域/15,000 項服務
vCPU	8	12	16
vRAM	24 GB	40 GB	96 GB
vDisk	500 GB	1 TB	1.5 TB

詳細功能清單

簡化的 DDoS 防禦管理

- 用於佈建、戰時作業和事件報告的中央 DDoS 防禦作業控制台
- A10 Defend Detector 和 Mitigator 設備的集中管理
- 即時 DDoS 防護儀表板和控制台
- 配置、備份、還原、升級映像庫的集中管理
- 用於重新開機、關閉和升級的集中裝置管理
- 託管裝置的健康監控
- 可自訂範本中預定義的緩解政策和組態設定檔
- 戰時期間的遠端封包擷取和除錯器
- 可搜尋的託管裝置和 A10 Defend Orchestrator 稽核日誌
- 內建管理 GUI
- REST API (aGAPI)

事件管理和報告

- 攻擊視覺化和地理位置追蹤
- 儀表板可持續監控最常受攻擊的服務
- 將多個設備的資料整合到即時儀表板中
- 戰時即時緩解控制台
- 全自動化攻擊偵測和緩解，只需最少的操作員介入
- 可自訂的事件警示/警報
- 從所有託管的 A10 Defend Mitigator 集中封包擷取
- 隨選和排程報告
- 透過電子郵件的自動 DDoS 事件報告

存取管理

- 角色型存取控制管理
- 支援 RADIUS 和 TACACS+ 的外部驗證

* 功能可能因授權選項而異。
選項包括基本裝置管理和 A10 Defend (前身為 Thunder TPS) 裝置管理套件。

深入瞭解

關於 A10 Networks

聯絡我們
APAC@a10networks.com

Part Number: A10-DS-15137-TW-01 Feb 2024