DATA SHEET

A10 Defend DDoS Mitigator

透過智慧自動化的 DDoS 緩解

A10 Defend DDoS Mitigator (前身為 Thunder TPS) 為 A10 Defend 套件的一部分，是由先進機器學習提供支援的可擴展和自動化 DDoS 防護解決方案，在精度、可擴展性和效能方面領先業界。

精確的多向量 DDoS 防護

為確保商業服務的可用性，組織需要重新思考如何建立可擴展的 DDoS 防禦，如此才能精確區分攻擊者與合法使用者。

新的威脅向量已改變攻擊者可用選項的廣度、強度和複雜性。現今的攻擊已不同以往，現在包含 DDoS 工具組、武器化物聯網裝置、線上 DDoS 服務等。現有解決方案若繼續依賴無效的特徵碼 IPS 或僅依賴流量速率限制，將不再適用。

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。在這套全方位的 A10 Defend 套件中，包含高精度、智慧化、可擴展且自動化的 DDoS 緩解功能。

A10 Defend DDoS Mitigator 可擴展以防禦「DDoS IoT」和傳統殭屍網路，並精確篩選包括反射和零時差攻擊在內的多向量 DDoS 攻擊，將對使用者的附帶損害降到最低。其採用獨特的多模式和基於來源的防護態勢，並考慮到智慧自動化，包括大規模自動更新的威脅智慧清單、五級自適應緩解原則，以及由機器學習技術支援的自動化零時差攻擊模式識別等等。

Mitigator 的規模和零接觸智慧自動化架構搭配 A10 Defend DDoS Orchestrator，能讓人數有限的員工達到最高效率，同時降低營運成本，進而改善投資報酬率。A10 Defend DDoS 防護套件由 Detector、Mitigator、Orchestrator 和 Threat Control 組成，可協助組織實現更有效的 DDoS 防護，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 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。

平台


實體與 SPE 設備

虛擬設備

雲端

相關的產品與服務


A10 Defend DDoS Detector


A10 Defend DDoS Orchestrator (A10 Control)


A10 Defend Threat Control

DSIRT 支援

深入瞭解

A10Networks.com/a10-defend

優勢

維持

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。Mitigator 可自動發現整個流量範圍內的異常，並緩解多向量 DDoS 攻擊，藉此確保服務可用性。

對抗

日益成長的攻擊

Mitigator 能保護最大型及要求最高的網路環境。Mitigator 可將常見攻擊向量卸載到專用硬體，使其強大的多核心 CPU 能區分合法使用者與攻擊殭屍網路，以及需要資源密集型深度封包檢測 (DPI) 的複雜應用層攻擊。

可擴展

防護

特定 Mitigator 硬體機型可從我們的安全及原則引擎 (SPE) 硬體加速中受惠，利用基於 FPGA 的 FTA 技術和其他硬體最佳化的安全檢查，實現高度可擴展的封包處理和硬體 DDoS 防護功能。無論外型尺寸如何，也無論是硬體或虛擬設備，Mitigator 設備都可透過叢集和同步技術，將緩解能力擴展至八倍。

部署

戰時支援

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。Mitigator 支援在每個保護區提供五級的程式化緩解升級和降級。第一線人員無需對升級緩解策略進行耗時的手動變更，同時也能縮短攻擊期間的回應時間。管理員可以選擇在攻擊的任何階段手動介入並與 A10 的 DSIRT 進行協調。

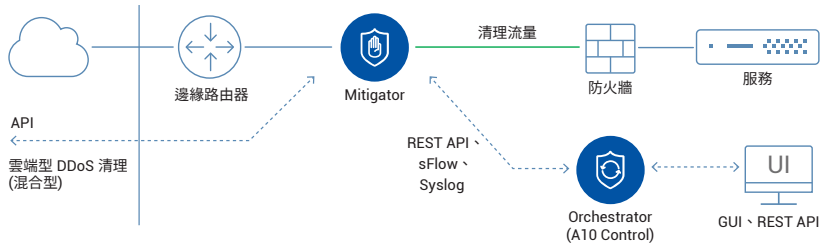
降低

安全營運支出

Mitigator 極其有效，儘管外型精巧，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。Mitigator 的規模和智慧自動化緩解架構搭配 Orchestrator，可簡化從偵測、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 DDoS 防護解決方案不只能協助 SecOps 團隊達到最高效率，還能降低營運成本，進而改善投資報酬率。

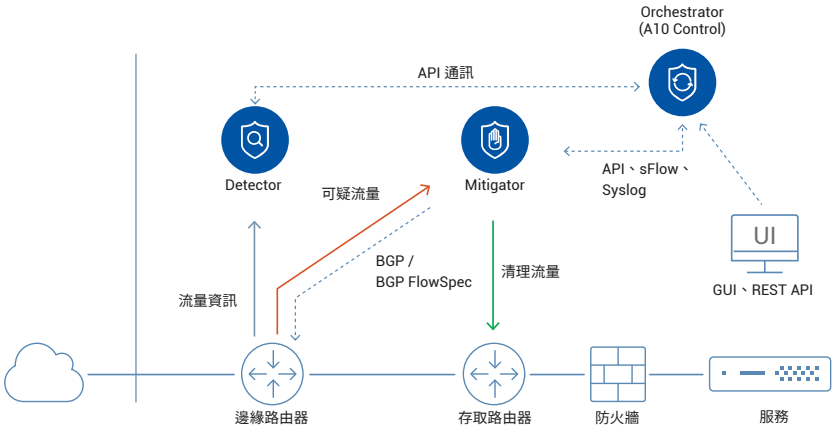
參考架構



主動式部署

(非對稱或對稱)

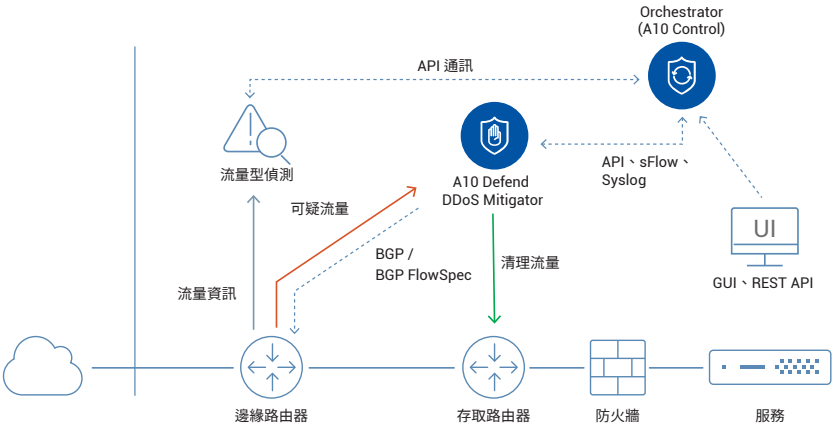
在服務網路內部或路徑內部署 A10 Defend DDoS Mitigator，可提供持續、全面偵測和快速緩解。此模式最適合用於高度重視使用者體驗的遊戲和 VoIP 等即時服務，以及企業 DDoS 防護使用案例。DDoS Mitigator 支援 L2 或 L3 路徑內部署。



反應式部署

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

參考架構



使用第三方流量偵測器的反應式部署

A10 Defend DDoS Mitigator 適用於任何具有整合 BGP 和其他路由通訊協定的網路配置，因此不必加裝任何轉移或回注的路由器。A10 Networks 與業界領先的網路監控和 DDoS 偵測公司合作，提供額外的彈性，為每個客戶的獨特業務需求建立一流的解決方案。第三方 DDoS 偵測可利用 API、Syslog 或 BGP Flowspec，建立緊密整合的 DDoS 防護解決方案。

特色

完整的 DDoS 防護提供服務可用性

完整解決方案

適用於彈性部署

Mitigator 提供完整解決方案，能夠以隨時啟用的主動模式或是隨選反應模式進行 DDoS 防禦，以符合客戶的業務目標。Mitigator 可以部署在 L2 或 L3 內部模式下，並提供全面的 IPv4 和 IPv6 支援，其中主動模式非常適合遊戲、語音和 DNS 等關鍵的即時服務。在反應模式下，Mitigator 能搭配 Detector 和 Orchestrator 協同運作，且只在需要時才啟動。當 Detector 偵測到攻擊時，Orchestrator 會指示 Mitigator 針對可疑流量發起 BGP 路由重新定向。然後，Mitigator 使用漸進式自動緩解級別升級技術，在清理流量遞送至預期目的地之前，應用適當的對策。

多向量

攻擊防護

緩解多種類型的 DDoS 攻擊，包括大流量、通訊協定或資源攻擊、應用層攻擊或物聯網型攻擊。硬體加速減輕 CPU 的負擔，讓 Mitigator 特別適合應對同時進行的多向量攻擊。

ZAP

零時差自動防護

零時差自動防護 (ZAP) 利用啟發式和機器學習自動探索緩解篩選條件，無需進階配置或手動介入。ZAP 加快針對日益複雜的多向量攻擊的反應時間，同時盡可能減少停機時間和錯誤，並降低營運成本。

不間斷 DNS

權威 DNS 快取

Mitigator 可配置為高效能權威 DNS 快取，使 Mitigator 的不間斷 DNS 操作模式能夠使用區域傳輸快取多達 240 Million 筆 DNS 記錄，並以每秒高達 35 Million 次查詢的速率回應查詢。不間斷 DNS 還能與使用 Mitigator 的一般 Thunder DNS DDoS 防護搭配運作，建立具有高度恢復能力的 DNS 服務。

A10 DDoS 威脅情報

聚集且支援來自 40 多個知名資料來源彙總和關聯的 DDoS 武器情報，使 Mitigator 能夠快速識別並封鎖已知惡意來源的流量。該服務包括數百萬個 DDoS 武器目前準確 IP 位址，這些 IP 位址經常用於反射放大攻擊和破壞性物聯網僵屍網路攻擊。

以高效能及高效率因應持續成長的攻擊規模

高效能
防護

特定的 Mitigator 機型具備高效能 FPGA 型彈性流量加速 (FTA) 技術，可在涉及資料 CPU 之前，以每秒高達 500 Million 封包 (Mpps) 的速度，立即緩解硬體中多達 60 種常見的攻擊向量，包括封包和通訊協定異常。Mitigator 可執行間隔最短 100 ms 的高度精細流量速率。

同步
受保護物件

為保護整個網路、應用程式和服務，Mitigator 可以同時緩解多達 3,000 個區域，其中包含每個區域的數千個主機、子網路和服務的單獨防護原則。同步緩解的規模可幫助組織對受保護的物件應用精細控制，並創造可盈利的 DDoS 清理服務。

可擴展性
領先的緩解能力

Mitigator 提供解決方案，以高能效且外型精巧的硬體保護組織免受各種規模 (從 5 到 550 Gbps) 的攻擊。還可以作為具有功能同位的虛擬設備，並提供 100 Gbps 的處理量。

Mitigator 可透過清單同步技術叢集化多達 8 個設備 (例如硬體為 4.4 Tbps，虛擬設備為 800 Gbps)，輕鬆擴展其緩解能力。

精確
大規模攻擊緩解

Mitigator 會追蹤超過 27 個流量和行為指示器，並運用不斷升級的通訊協定驗證技術，精確區分攻擊者與有效使用者，進而適當緩解多達 350 Million 個同時追蹤的連線。

複雜的應用程式攻擊 (例如 HTTP、DNS 等) 可透過跨大量 CPU 核心進階平行處理得到緩解，以保持高效能系統擴展，即使面對多向量攻擊也是如此。

A10 Defend DDoS Mitigator

8665S

重要數據

4.8 Tbps 硬體封鎖	550 Gbps 處理量	4.4 Tbps 叢集處理量	8x16M 威脅類別清單
400 GE 連接埠	820 Mpps 異常丟失 (硬體輔助)	60 硬體緩解	64K 受保護物件

大威脅

情報類別清單

可定義八個清單，每個清單最多包含 16 Million 個項目，以利用如 A10 Defend Threat Control 等 DDoS 威脅情報來源的資料。這些類別清單及其自己的自訂封鎖 / 允許清單可以配置為 IP 封鎖清單，也可根據需要用於來源 IP 型緩解原則。

零時差

攻擊模式識別

DDoS 攻擊者繼續使用新策略打造創新的多向量攻擊庫。Mitigator 零時差攻擊模式識別 (ZAPR) 引擎自動識別 DDoS 攻擊特性並動態套用緩解篩選條件，無需進階配置或手動介入。

全面掌控及智慧自動化，實現靈活防護

有效率

智慧自動化

任何組織都沒有無限的資源或時間進行人工介入。A10 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，A10 防禦依據操作人員預定義的原則完成其餘工作，包括每個受監控實體的單個已知偵測閾值、自動流量重新定向編排、開始緩解和升級，然後擷取和應用攻擊模式篩選條件。當攻擊消退時，網路和防禦將恢復到和平時期的態勢，並產生詳細報告以供將來分析。

簡便

網路整合

Mitigator 提供多種效能選項及彈性的部署模式，可整合至任何規模的網路架構之中 (包括 MPLS 和 BGP 偵測)。此外 Mitigator 也具備 aXAPI 這款 A10 的 100% 可程式化 RESTful API，能夠輕鬆整合至第三方偵測解決方案和敏捷的 SecOps 工作流程中。

利用 BGP Blackhole 和 Flowspec 功能等開放標準，Mitigator 可輕鬆與任何 DDoS 偵測和具備 DDoS 緩解功能的 BGP 路由器解決方案整合。開放式 API 和網路標準可與其他裝置緊密整合，包括 A10 威脅偵測合作夥伴、SDN 控制器及其他安全產品。

有效

管理

Mitigator 支援業界標準 CLI、內建 GUI 和 Orchestrator 集中管理系統。CLI 能讓技術純熟的操作人員輕鬆進行疑難排解和除錯。直覺式內建 GUI 簡單易用並提供基本的圖形報告。Orchestrator 提供全方位儀表板，包含適用於多個 Mitigator 和 Detector 裝置的進階報告、緩解控制台及原則實施。

A10 Defend DDoS Mitigator 實體設備規格

DDoS Mitigator	Thunder 1060S*4	Thunder 3350-E	Thunder 5845-40G	Thunder 5845
緩解效能				
處理量 (軟體清理)*1	5/10/20 Gbps	10 Gbps	40 Gbps	100 Gbps
硬體封鎖	N/A	N/A	250 Gbps	250 Gbps
封包速率 (pps)*1	2.5/5/8 Million	6 Million	12 Million	25 Million
軟體型 - SYN 驗證 (pps)	2.5/5/8 Million	6 Million	12 Million	25 Million
硬體型 - 異常流量封鎖 (pps)	N/A	N/A	125 Million	125 Million
最大同時連線數 (非對稱部署)	8/10/16 Million	8 Million	32 Million	48 Million
平均延遲	15 µs	20 µs	50 µs	50 µs
最小速率執行間隔	100 ms	100 ms	100 ms	100 ms
DNS 權威快取效能				
每秒 DNS 查詢數 (qps)	N/A	N/A	10 Million	18 Million
網路介面				
1 GE (BASE-T)	7	6	0	0
1 GE 光纖 (SFP)	0	2	0	0
10/1 GE 光纖 (SFP+/SFP)	4	8 + 4*3	48	48
25/10 GE 光纖 (SFP28/SFP+)	2	0	0	0
40 GE 光纖 (QSFP+)	0	0	0	0
100/40 GE 光纖 (QSFP28/QSFP+)	0	0	4	4
400 GE 光纖 (QSFP-DD)	0	0	0	0
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 通訊處理器 20 核心*5	Intel Xeon 8 核心	Intel Xeon 18 核心*5	Intel Xeon 18 核心
記憶體 (ECC RAM)	32 GB	16 GB	64 GB	64 GB
儲存裝置	SSD	SSD	SSD	SSD
硬體加速	軟體	軟體	2 個 FTA-4，SPE	2 個 FTA-4，SPE
尺寸 (吋)	1.75 (H) x 17.5 (W) x 17(D)	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)
機架單元 (可安裝)	1U	1U	1U	1U
單元重量	12 lbs	18 lbs	34.3 lbs	34.3 lbs
電源 (提供 DC 選項)	雙 300W RPS	雙 750W RPS	雙 1500W RPS	雙 1500W RPS
	80 Plus Gold 效率，100-240 VAC，50-60 Hz	80 Plus Platinum 效率，100-240 VAC，50-60 Hz		
耗電量 (典型/最大)*2	112W / 127W	151W / 205W	585W / 921W	585W / 921W
每小時熱量 (典型/最大) (單位：BTU)*2	383 / 434	516 / 700	1,997 / 3,143	1,997 / 3,143
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^, ICES, CE, UKCA, CB^, VCCI, BSMI^, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM, MTCTE^ | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM, MTCTE^ | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM, MTCTE^ | RoHS
標準保固	90 天硬體與軟體保固			

A10 Defend DDoS Mitigator 實體設備 (續)

DDoS Mitigator	Thunder 7465		
模組化授權	40 Gbps	100 Gbps	270 Gbps
緩解效能			
傳輸量 (軟體清理)*1	40 Gbps	100 Gbps	270 Gbps
硬體封鎖	800 Gbps	800 Gbps	1 Tbps
封包速率 (pps)*1	13 Million	28 Million	60 Million
軟體型 - SYN 驗證 (pps)	13 Million	28 Million	60 Million
硬體型 - 異常流量封鎖 (pps)	550 Million	550 Million	550 Million
最大同時連線數 (非對稱部署)	32 Million	64 Million	128 Million
平均延遲	40 µs	40 µs	40 µs
最小速率執行間隔	100 ms	100 ms	100 ms
DNS 權威快取效能			
每秒 DNS 查詢數 (qps)	N/A	N/A	N/A
網路介面			
1 GE (BASE-T)	0		
1 GE 光纖 (SFP)	0		
10/1 GE 光纖 (SFP+/SFP)	0		
25/10 GE 光纖 (SFP28/SFP+)	24		
40 GE 光纖 (QSFP+)	0		
100/40 GE 光纖 (QSFP28/QSFP+)	8		
400 GE 光纖 (QSFP-DD)	0		
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 36 核心*5		
記憶體 (ECC RAM)	256 GB		
儲存裝置	SSD		
硬體加速	1 個 FTA-6，SPE		
尺寸 (吋)	1.75 (H) x 17.5 (W) x 30 (D)		
機架單元 (可安裝)	1U		
單元重量	38.5 lbs		
電源 (提供 DC 選項)	雙 1500W RPS 80 Plus Platinum 效率，100-240 VAC，50-60 Hz		
耗電量 (典型/最大)*2	680W / 770W		
每小時熱量 (典型/最大) (單位：BTU)*2	2,321 / 2,628		
冷卻風扇 (從前到後的氣流)	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, KCC, BSMIˆ, RCM, MTCTEˆ, ANATELˆ | RoHS		
標準保固	90 天硬體與軟體保固		

A10 Defend DDoS Mitigator 實體設備 (續)

DDoS Mitigator	Thunder 7445	Thunder 7655S	Thunder 8665S
緩解效能			
處理量 (軟體清理)*1	220 Gbps	380 Gbps	550 Gbps
硬體封鎖	500 Gbps	1.2 Tbps	4.8 Tbps
封包速率 (pps)*1	50 Million	100 Million	120 Million
軟體型 - SYN 驗證 (pps)	50 Million	100 Million	110 Million
硬體型 - 異常流量封鎖 (pps)	250 Million	500 Million	820 Million
最大同時連線數 (非對稱部署)	64 Million	256 Million	350 Million
平均延遲	60 µs	40 µs	40 µs
最小速率執行間隔	100 ms	100 ms	100 ms
DNS 權威快取效能			
每秒 DNS 查詢數 (qps)	35 Million	N/A	N/A
網路介面			
1 GE (BASE-T)	0	0	0
1 GE 光纖 (SFP)	0	0	0
10/1 GE 光纖 (SFP+/SFP)	48	0	0
25/10 GE 光纖 (SFP28/SFP+)	0	0	0
40 GE 光纖 (QSFP+)	0	0	0
100/40 GE 光纖 (QSFP28/QSFP+)	4	16	0
400 GE 光纖 (QSFP-DD)	0	0	12
管理連接埠	乙太網路管理連接埠、RJ-45 主控台連接埠		2 個乙太網路管理連接埠、RJ-45 主控台連接埠
硬體規格			
處理器	2 個 Intel Xeon 18 核心	2 個 Intel Xeon 28 核心	2 個 Intel Xeon 36 核心
記憶體 (ECC RAM)	128 GB	384 GB	512 GB
儲存裝置	SSD	SSD	SSD
硬體加速	3 個 FTA-4，SPE	2 個 FTA-5，SPE	3 個 FTA-6，SPE
尺寸 (吋)	1.75 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
機架單元 (可安裝)	1U	1.5U	1.5U
單元重量	35.7 lbs	44.2 lbs	44.9 lbs
電源 (提供 DC 選項)	雙 1500W RPS	雙 1500W RPS	雙 2500W RPS
	80 Plus Platinum 效率，100-240 VAC，50-60 Hz		
耗電量 (典型/最大)*2	784W / 1,078W	1,121W / 1,300W	1,491W / 1,720W
每小時熱量 (典型/最大) (單位：BTU)*2	2,676 / 3,679	3,826 / 4,436	5,088 / 5,869
冷卻風扇 (從前到後的氣流)	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, MTCTE^ | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM, MTCTE^ | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, 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 處理量效能為流量轉送能力，在啟用 DDoS 防護下使用合法流量進行測量。
*2 使用基本型號 | *3 僅 10Gbps 速度 | *4 以模組化授權提供不同容量。規格及數據可能依模組化授權層級而異
*5 作用中 CPU 核心數可能依模組化授權而異 | ^ 認證中

A10 Defend DDoS Mitigator 軟體規格

A10 Defend DDoS Mitigator 虛擬設備	
支援的 Hypervisor	VMware ESXi 7.0 或以上版本 (SR-IOV、DirectPath I/O)、KVM QEMU (SR-IOV、PCI Passthrough)
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

處理量	Lab/1/2/5 Gbps	50 Gbps*1	100 Gbps*1
vCPU	8	16	32
vRAM	16 GB	32 GB	64 GB
vDisk	128 GB	256 GB	384 GB
授權類型	頻寬授權 (每個實例)	FlexPool	FlexPool
Hypervisors	ESXi, KVM	ESXi, KVM	ESXi, KVM

*1 支援 ACOS 6.0 及以上版本用於 ESXi，支援 ACOS 7.0.2 及以上版本用於 KVM，並依據 NVIDIA Mellanox ConnectX-6 NIC 進行測試。

雲端專用 A10 Defend DDoS Mitigator	Microsoft Azure
每執行個體的處理量	高達 5 Gbps
映像格式	Microsoft VHD
授權	30 天試用授權 | BYOL FlexPool 授權

詳細功能清單

功能可能因設備而異。

偵測/分析

- 線上封包式 DDoS 偵測
- 適用於超過 25.6 萬部伺服器和服務的個別偵測原則
- 手動和學習閾值
- 通訊協定異常偵測
- IPinIP 內的檢查 (例如網路、封裝)
- 封鎖/允許清單
- 流量指示器和最大流量者
- 緩解控制台
- 封包除錯工具
- 前 k 個見解 (來源、目的地)
- 出站偵測
- 受害者 IP 識別

DDoS 威脅情報清單

- 大容量類別清單可主動阻止有毒 IP 位址，作為第一層防護
- 多達 96 Million 個有效項目 - 最多 8 個清單，每個清單最多包含 16 Million 項
- 可以為每個清單定義動作或緩解原則
- 支援各種類型的 DDoS 威脅情報源，包括來自 A10 Defend Threat Control 的 ThreatSTOP 和 IP 封鎖清單

零時差自動防護

- ZAPR：機器學習驅動的攻擊模式識別和篩選
- TCP 進展追蹤
- 防止零時差攻擊
- 免預先配置或手動介入
- 快速自動化回應

資源攻擊防護

- 碎片攻擊
- Slowloris
- 慢速 GET/POST
- 長表單提交
- SSL 重新協調

應用程式攻擊防護

- 應用程式感知篩選條件
- 正規表示式篩選條件 (TCP/UDP/HTTP/SIP)
- HTTP 要求速率限制 (依 URI)
- DNS 要求速率限制 (依類型、FQDN、標籤數)
- SIP 要求限制 (依類型)
- 應用程式要求格式錯誤檢查 (DNS/HTTP/SIP)
- DNS 網域清單
- HTTP/S 通訊協定合規
- 應用程式 (DNS/HTTP/SIP) 洪水防護
- QUIC 版本控制和格式錯誤的標頭檢查
- 遊戲流量的封包浮水印 (UDP)
- 加密洪水攻擊防護

通訊協定攻擊防護

- 無效封包
- 異常 TCP 旗標組合 (無旗標、SYN-FIN、SYN 片段、LAND 攻擊)
- SYN-ACK 放大攻擊防護
- IP 選項
- 封包大小驗證 (ping of death)
- POODLE 攻擊
- TCP/UDP/SSL/ICMP 洪水防護
- 每個連接的流量控制

查問式驗證

- TCP SYN Cookie、SYN 驗證
- ACK 驗證
- 欺騙偵測
- DNS 驗證
- HTTP 挑戰

受保護物件

- 用於自動偵測和緩解的保護區
- 來源/目的地 IP 位址/子網路
- 來源和目的地 IP 對組
- 目的地連接埠
- 來源連接埠
- 通訊協定 (例如 HTTP、DNS、SIP、TCP、UDP、ICMP 等)
- 類別清單/地理位置
- 被動模式
- 出站緩解對稱部署

不間斷 DNS 解決方案

- 作為權威 DNS 快取
- 清理中心使用 A10 Defend Mitigator 提供流暢分層保護
- DNS 水刑 (隨機子網域) 攻擊防護
- 選擇性和可自訂的動作 (回應/轉發/丟棄)

動作

- 擷取封包
- 執行指令碼
- 丟棄
- TCP 重設
- 動態驗證
- 加入封鎖清單
- 加入允許清單
- 記錄
- 限制同時連線數
- 限制連線速率
- 限制流量速率 (pps/bps)
- 轉發至其他裝置
- 遠端觸發黑洞 (RTBH)
- BGP Flowspec

管理

- 專屬內建管理介面 (GUI、CLI、SSH、Telnet)
- A10 Defend DDoS Orchestrator (ADO) 應用程式於 A10 Control 執行，提供全方位的管理及作業功能
- SNMP、Syslog、電子郵件警示
- REST API (aXAPI) 或 SDK
- LDAP、TACACS+、RADIUS 支援
- 可配置的控制 CPU

網路與部署

- 主動、回應、非對稱、對稱、頻外 (TAP)
- 透明 (L2)、路由 (L3)
- 虛擬線
- 路由：靜態路由、BGP4+、OSPF、OSPFv3、IS-IS
- 雙向轉送偵測 (BFD)
- VLAN (802.1Q)
- 主幹連線 (802.1AX)、LACP
- 存取控制清單 (ACL)
- 網路位址轉換 (NAT)
- MPLS 流量防護
- BGP 路由注入
- BGP FlowSpec
- IPinIP (來源和終端)
- GRE 隧道介面
- VXLAN

詳細功能清單 (續)

遙測

- 豐富的流量和 DDoS 統計資料計數器
- sFlow v5
- 用於流量型匯出的自訂計數器區塊
- 高速記錄
- CEF 記錄

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
- 安全原則引擎 (SPE) 支援硬體加速以執行原則*
- 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
- 25GE、40GE、100GE 和 400GE 介面

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。

深入瞭解

關於 A10 Networks

聯絡我們

apac@a10networks.com

Part Number: A10-DS-15136-TW-06 January 2026