DATA SHEET

A10 Control

以統一的管理、控制及分析平台實現敏捷作業及自動化

這款集中管理及分析平台可協助您完整控制 A10 解決方案，不論部署於內部、雲端或混合環境都沒問題。

敏捷管理及智慧型分析

現代網路及安全基礎架構日漸複雜，再加上各界快速採用 AI 及雲端技術，讓組織在管理及支援關鍵任務服務和業務時面對重大挑戰。

部署地點一旦橫跨各個不同地區及多個雲端環境，瞭解網路基礎架構資源及追蹤服務狀態就會複雜又耗時。精準的容量規劃及立即回應擴充需求，對 AI 驅動應用程式及應用程式服務基礎架構而言至關重要，因為這類基礎架構不但需要更高的流量及交易量，也非常容易受到延遲影響。因此管理員應運用敏捷管理及智慧型分析功能，建立高效的作業及管理工作流程。

A10 Control 是新一代的管理及分析平台，適用於 A10 解決方案，可整合現有的 A10 Harmony 控制器及 aGalaxy 功能。A10 Control 可集中管理 A10 安全和基礎架構解決方案，包括部署在任何網路或雲端環境的應用程式交付、DNS、CGNAT、SSL Insight、Gi 防火牆及 DDoS 防護。集中平台可協助收集、分析和報告通過 A10 設備的應用程式及服務流量，並透過智慧型分析功提供可視化的資訊，幫助掌握服務和安全態勢。

平台

軟體/VM

相關的產品與服務

- ADC
- A10 Defend DDoS 防護
- CFW
- CGN
- SSLi

深入瞭解

A10Networks.com/a10-control

優勢

獲得

即時智慧分析及觀察能力

組織必須保證服務可持續運作。因此營運團隊的關鍵任務，就是瞭解服務狀況並具備觀察能力。A10 Control 可對採用 A10 先進核心作業系統 (ACOS) 的 A10 裝置，收集通過其中流量的相關指標資料和交易記錄，並提供深度可視性，協助掌握服務及網路基礎架構的情況。智慧型分析及可自訂警示有助於識別潛在問題，避免影響最終使用者，並可存取情境式流量資料和記錄，主動進行疑難排解。

簡化

管理服務及安全性

單一管理平台適用於任何 A10 解決方案；A10 獨一無二的技術優勢之一，就是所有 A10 解決方案均於共同 OS (ACOS) 執行，不受平台或外型尺寸影響。現在 A10 Control 成為管理員需要的唯一管理平台，整合了 A10 Harmony 控制器及 aGalaxy 的各項功能。

A10 Control 提供豐富的智慧型分析功能，以及嵌入式自動化工作流程工具，協助您簡化 IT 作業及改善服務連續運作時間。

提升

營運效率

組織可簡化工作流程及實現自動化流程，以提升營運團隊的敏捷度和效率。裝置生命週期管理包含備份、健全狀態檢查、軟體升級、庫存及授權管理，可說是困難又耗時的作業。A10 Control 的智慧型自動化功能和各項工具能夠促進高效作業，幫助管理部署在資料中心乃至於任何雲端等各種基礎架構的大量設備和服務。

全方位 API 能夠輕鬆整合熱門的 DevOps、基礎架構即程式碼和觀察能力工具鏈，以及主要的公有雲和私有雲基礎架構。

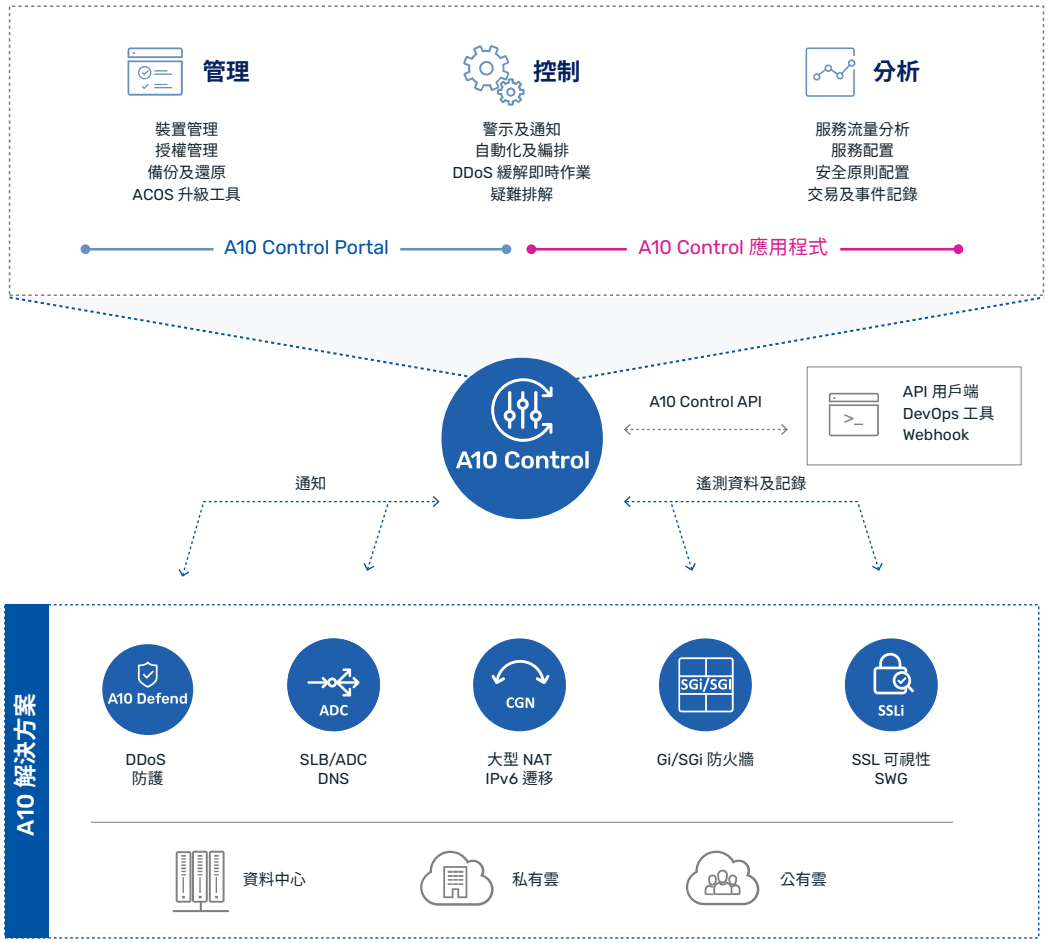


圖 1：A10 Control 是集中的管理及作業平台，適用於 A10 基礎架構服務和安全解決方案。

特色

集中管理

裝置生命週期管理

集中的裝置生命週期管理功能，適用於 A10 硬體及虛擬設備，包括公有雲、私有雲及裸機。直覺操作的庫存和授權管理功能，適用於多種 A10 Thunder 及 A10 Defend DDoS 設備。自動化例行作業，例如備份、庫存報告，以及排程自動化軟體升級。

裝置分析

A10 裝置可跨不同地理區域部署在各種網路及雲端環境中，提供詳細的裝置層級分析功能。裝置健全狀態監控及儀表板可提供系統資源使用率、裝置位置、流量及連線指標、交易記錄和事件資訊。

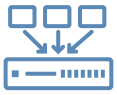
警示和報告

從 A10 裝置收集的指標和記錄會依據使用者定義規則建立關聯及評估，以便針對異常事件提出警示。這類警示可透過電子郵件通知及/或 Webhook 傳送，並使用 Slack 及 Microsoft Teams 等協作工具實現自動化行動。

服務作業

服務及原則管理

利用共用資源從中央主控台為部署在不同地區的 A10 裝置變更配置及執行安全原則更新，例如類別清單或 IP 清單。



多租戶

彈性的多租戶架構和角色型存取控制功能，可讓各個應用程式團隊及服務負責人擁有名為組織單位 (organization-unit) 的租戶工作空間，以便管理各自的服務與作業。租戶分配可彈性地在租戶中設置多個 A10 裝置叢集，或是精細地為 A10 裝置的各個 L3V/ADP 分區指派租戶。

API 驅動的自動化與整合

全方位的 A10 Control API 可利用 Ansible、Chef 及 Jenkins 等 DevOps 工具鏈輕鬆整合，透過 A10 Control 自動化 A10 裝置配置管理，並為受管理的 A10 解決方案簡化監控及作業工作流程。

憑證管理及自動更新

憑證管理公用程式可協助管理員有效管理憑證、檢查憑證狀態 (啟用、過期、已撤銷)，甚至還能配合特定憑證供應商進行自動化更新流程。

架構及系統

可靠的控制器平台

A10 Control 以穩固的 RHEL 基礎建構而成，搭配使用 Kubernetes 的微架構，除了可讓控制器達到最高可用度，也能確保完整的法規遵循，符合最新的業界標準。控制器能以安全方式收集和處理 A10 裝置的各種遙測資料，絕對不會處理通過 A10 裝置資料平台的服務流量。這項架構也能在控制器與 A10 裝置之間連線中斷時，確保絕對不會發生服務流量中斷的情況。

提升安全性及維護能力

包含 Harmony 控制器在內的 A10 產品系列，多年來持續使用微服務架構。A10 Control 設計使用最新及最出色的 RHEL 軟體，並採用新一代架構。這有助於提升系統的安全性及維護能力，特別是在安全性及 CVE 修補程式方面。

翻新架構提升穩定度及效能

A10 Control 用於建構產品的所有元件、框架和技術均為升級版，大幅提升穩定度及效能。A10 Control 使用的資料庫系統有別於 Harmony 控制器，提供簡化及低延遲的資料作業，此外還以全新的標準型技術提供使用者驗證管理。

高可用性

控制器可安裝為自助管理軟體解決方案，在其中一個站台以單節點或多節點高可用性 (HA) 部署。在 HA 部署中，微服務及控制器的資料儲存會分散在節點之間。

A10 Control 也支援災難復原，專為分佈於各地站台的高可用性架構 (主動-被動) 所設計，能夠預先佈建待機系統及執行主動健全狀況檢查，以確保業務連續性。

如需深入瞭解系統需求及安裝 A10 Control 的先決條件，請參閱最新產品文件或聯絡 A10 銷售代表。

彈性部署選項

A10 Control 提供彈性的部署選項，以因應各種規模組織的需求。

- **A10 Control Standard**：專為需要高可用性及擴充性的大型企業及服務供應商所設計，可支援高達 200 個受管理裝置。
- **A10 Control Lite**：適合用於小規模部署，提供基本的管理功能，對基礎架構及資源的需求較低。

A10 Control 應用程式

以解決方案為基礎的全方位分析、配置及服務作業工具，全部都內建為 A10 Control 的應用程式。

應用程式交付控制器 (ADC) 應用程式

提供集中配置工具及可視性，適用於單站台或多站台的 ADC 及 DNS 部署。豐富的分析功能及情境式記錄，有助於取得出色見解，掌握應用程式及流量，並在需要時簡化疑難排解工作流程。

電信級 NAT (CGN) 應用程式

提供 CGNAT 技術配置工具、管理功能及深入見解，協助掌握訂閱用戶流量及 NAT 集區使用率。豐富的服務分析包括使用者工作階段記錄，以提升作業效率並協助未來規劃。

Gi/SGi 防火牆 (Gi-FW) 應用程式

提供詳細見解，協助掌握通過 CFW-CGN 裝置的使用者流量，包括依據防火牆規則的分析、CGNAT 分析，以及依據應用程式類別的分類。

A10 Defend Orchestrator (ADO) 應用程式

之前稱為 aGalaxy，目前則是以 ADO 應用程式的名義提供使用。為 DDoS Detector 及 Mitigator 提供集中保護配置和即時監控功能。如果發生 DDoS 事件，編排行動可透過即時緩解主控台協助簡化工作流程。

SSL Insight (SSLi) 應用程式

提供精靈型配置、引導式疑難排解工具，以及全方位的觀察能力，協助掌握 SSL Insight 或安全網路閘道部署的 TLS/SSL 加密流量。

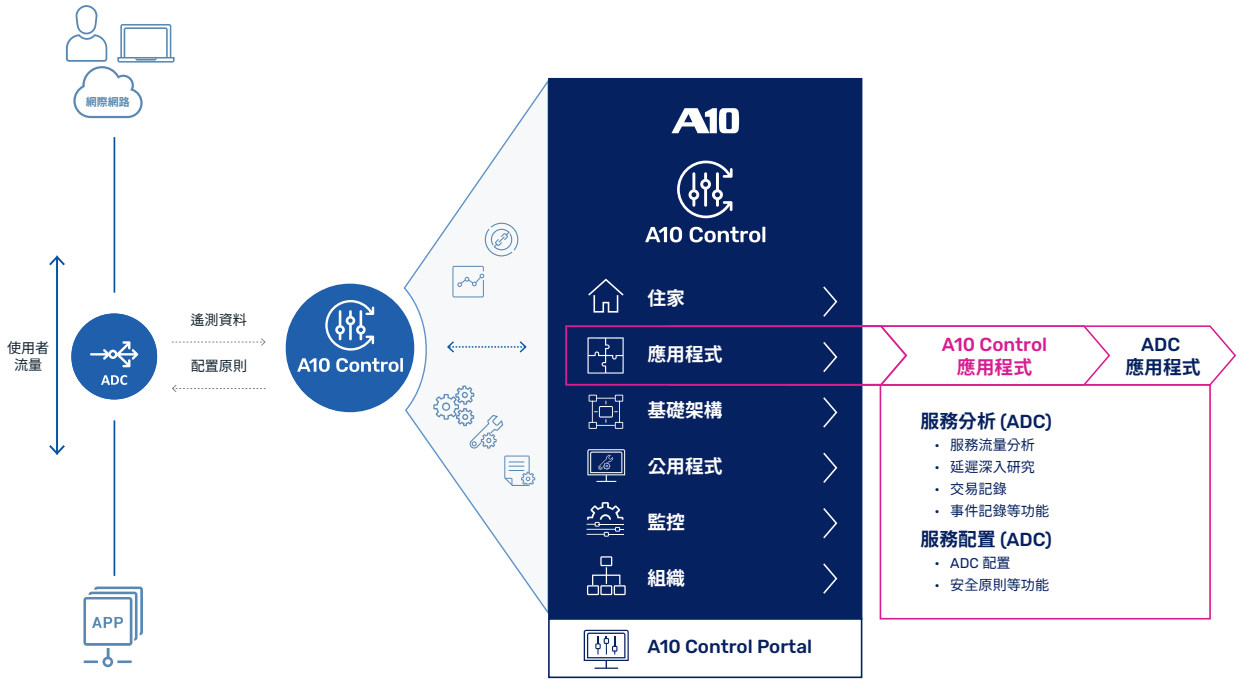


圖 2：A10 Control 透過控制平台收集 A10 裝置的遙測資料，並利用服務專屬的 A10 Control 應用程式提供分析及控制功能。

使用案例

支援的 A10 解決方案

應用程式交付

高效能的進階負載平衡解決方案，讓應用程式高度可用、加速且安全無虞。部署搭配 A10 Thunder ADC 或 Thunder CFW-ADC，可採用任何外型尺寸，包括硬體、Hypervisor 型軟體、裸機、容器，或是混合雲及多雲環境。

CGNAT 及 Gi/SGi 防火牆

A10 Thunder CGN 可部署用於高擴充性及高效的 NAT 解決方案，協助服務供應商及企業延長使用 IPv4 連線，同時順利轉移至 IPv6 基礎架構。A10 Thunder CFW-CGN 則可整合 CGNAT、Gi/SGI 防火牆及應用程式可視性等網路功能，支援高效的 Gi-LAN 及行動核心安全性。

DNS

可擴展且安全無虞的 DNS 負載平衡及快取解決方案，讓 DNS 基礎架構更具韌性且效率更高。部署搭配 A10 Thunder ADC 或 Thunder CFW-ADC，可採用任何外型尺寸及環境。

DDoS 防護

全方位的 DDoS 防禦解決方案，具備可擴展、經濟實惠、精準及智慧化等特色，協助組織確保延長服務連續運作時間。部署搭配 A10 Defend DDoS Detector 及 Mitigator。

SSL Insight

全方位的 TLS/SSL 解密解決方案，可讓安全裝置分析加密的企業流量，並利用整合式安全網路閘道功能進一步提高安全態勢。能以 A10 Thunder CFW-ADC 在任何外型尺寸中部署。

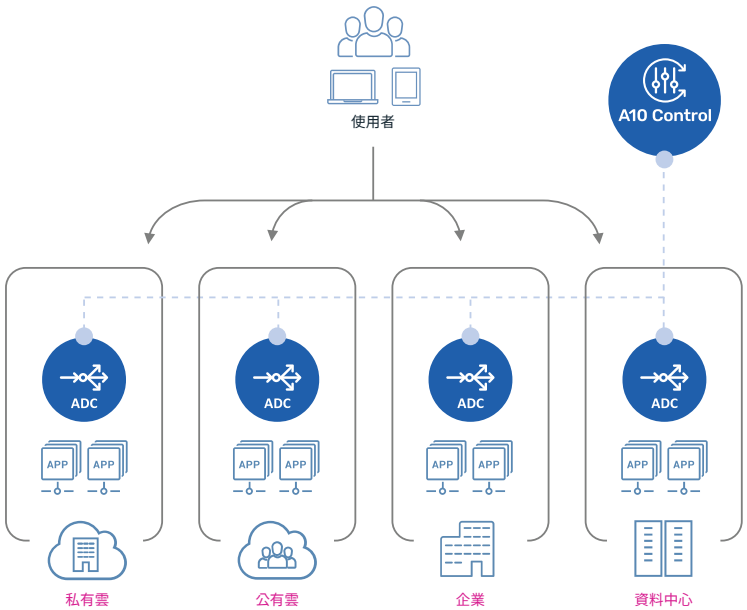


圖 3：多雲 ADC 使用案例。

多雲應用程式交付部署

A10 Control 可集中管理及控制部署在混合雲或多雲環境的應用程式交付服務，並提供以下功能：

- ADC 分析
- ADC 及安全原則執行
- ADC 裝置和配置管理等功能

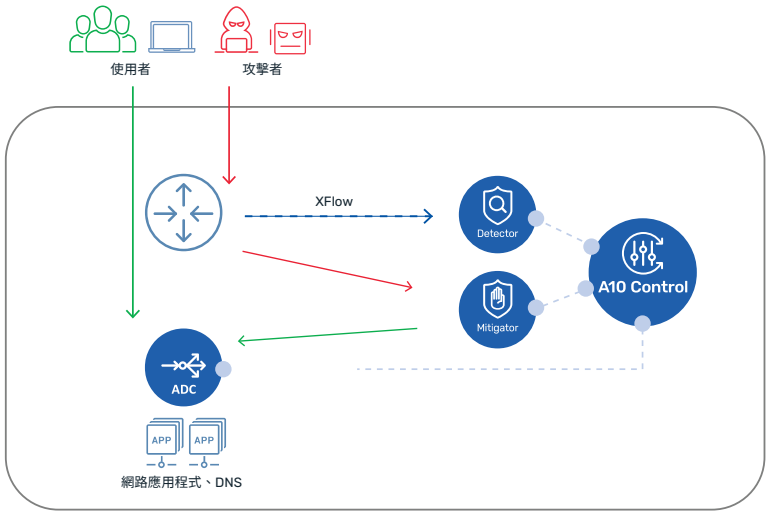


圖 4：DDoS 防護使用案例。

適用於網路應用程式及 DNS 的 DDoS 防護

A10 Defend DDoS Orchestrator (ADO) 於 A10 Control 執行運作，搭配使用 Mitigator 及 Detector，可實現智慧自動化防護功能，對抗鎖定應用程式服務及/或網路基礎架構的現代 DDoS 攻擊。

ADO 應用程式提供以下功能：

- DDoS 防禦編排及自動化
- DDoS 緩解控制台
- DDoS 防禦原則配置
- 事件報告等功能

如果 A10 ADC 用於應用程式服務，也可由相同的 A10 Control 進行管理和控制。

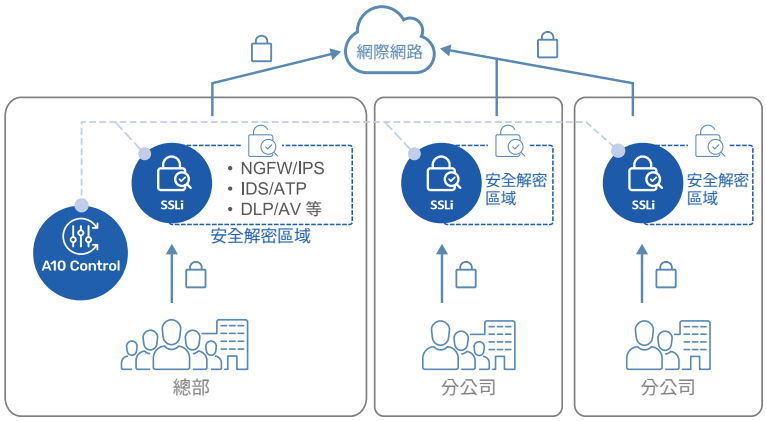


圖 5：SSL Insight 使用案例。

SSLi/安全網路閘道保護企業邊界

A10 Control 可集中管理 SSL Insight/SWG 部署，範圍橫跨不同地點及分公司，因應組織的邊界保護需求。

SSLi 應用程式提供以下功能：

- SSLi 分析
- 集中安全及原則執行
- 疑難排解工具
- 部署精靈

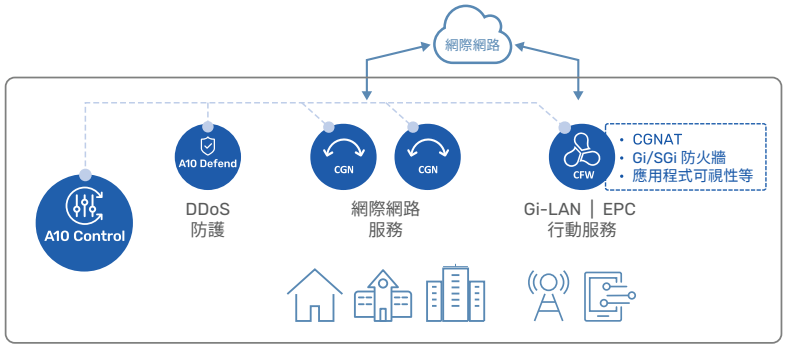


圖 6：行動及服務供應商解決方案使用案例。

適用於行動/SP 網路的網路及安全解決方案

CGNAT 及 GiFW 服務可由 A10 Control 集中管理並提供以下功能：

- 集中 CGNAT 配置及安全原則執行
- 整合式裝置管理
- 詳細的 CGNAT 及防火牆分析

此外 DDoS 防護解決方案也可由相同的 A10 Control 管理。

詳細功能清單

A10 Control Portal

裝置管理	
裝置管理儀表板	完整的裝置庫存可於個別裝置及叢集檢視 (單節點、VRRP-a 配對等) 提供一般系統及網路資訊，並詳細分析系統資源使用情況和流量統計資料。
備份及還原	A10 裝置配置可定期備份，儲存於 A10 Control 之中。備份可在需要時用於還原裝置。
ACOS 映像升級	映像升級公用程式具備升級前後檢查功能，提供直覺可靠的 ACOS 映像升級流程，包含手動及排程方法，適用於註冊的 A10 裝置。所有升級作業記錄均於歷史記錄檢視中提供。
監控及警示	
服務層級健全狀態監控及警示	自訂觸發規則可使用各種服務層級指標和閾值，用於監控服務流量及狀況。警示可透過電子郵件及 Webhook 傳送，更輕鬆與現有監控系統整合。
裝置層級健全狀態監控及警示	精細的裝置層級觸發規則可依據各種項目設定，包括基礎架構/裝置資源使用情況、基於裝置層級流量的閾值，以及系統記錄。警示可透過電子郵件及 Webhook 傳送，更輕鬆與現有監控系統整合。
報告	全方位庫存及每項服務的作業報告可隨需產生，或排程產生進行自動交付。報告可透過 PDF 下載或直接電子郵件發佈等方式取得。
事件和稽核記錄	事件檢視器可從所有註冊的 A10 裝置中，提供整合的系統及服務事件記錄。稽核檢視器可存取 A10 控制器的稽核記錄，以及所有註冊的 Thunder 和授權管理活動記錄。提供精細的記錄篩選條件，記錄可下載為 CVS 格式。
管理及公用程式	
多租戶管理	多租戶功能提供精細的角色型存取，適用於應用程式團隊及服務負責人。每個租戶 (組織單位) 可與 A10 裝置分區 (ADP/L3V) 層級對應。
CLI 命令公用程式	單一或批次 CLI 命令可同時於多個裝置分區遠端執行。
共用配置資源集區	類別清單、封鎖/允許清單、SLB 範本、安全範本及 TLS/SSL 憑證等共同配置資源/範本，可建立為共用資源，並在任何註冊的 A10 裝置之間使用，不受服務類型影響。
憑證管理	TLS/SSL 的 ADC 和 SSLi 服務憑證及金鑰可由 A10 Control 管理，協助組織管理員儲存、提供、更新及監控狀態 (啟用、過期、已撤銷)。能夠與 Venafi 等憑證供應商整合，實現完全自動化的憑證生命週期管理 (包括自動更新)。
授權管理	A10 Control 以企業授權管理工具的形式運作，可用於管理及控制註冊 A10 裝置的 FlexPool 容量授權。
使用者管理	角色型存取控制提供彈性的使用者管理功能。例如，存取區域可依據組織、租戶、裝置或特定服務/分區進行設定，而權限層級可以是管理員、作業人員，或特定作業的自訂規則。
驗證管理	除了本機驗證以外，也可選擇 Azure、Okta 或 LDAP 等身分供應商 (IdP) 進行外部驗證和單一登入 (SSO)。

A10 Control 應用程式

應用程式交付	
ADC 應用程式首頁	• 提供整合資訊，協助掌握租戶之下的虛擬伺服器 (VIP) 狀態及部署圖 (組織單位) • 主要虛擬伺服器 • 事件及警示儀表板
分析	• ADC 服務分析功能適用於組織單位之下的各項虛擬服務 • 即時 ADC 服務層級 KPI，包含流量資訊、錯誤率及延遲 • 基於使用者流量的分析，包括使用者見解 (位置、瀏覽器)、前 k 個資訊、請求見解、時間序列延遲等項目 • 常見通訊協定的 ADC 服務分析 (HTTP/S、SSL 及 HTTP2) • ADC 叢集分析，提供資源使用見解 • 應用程式服務分析，提供詳細的應用程式服務狀況及趨勢 • 應用程式伺服器分析，協助掌握伺服器健全狀況及狀態 • 延遲深入研究及分析，協助掌握端對端延遲狀況，涵蓋從請求到回應的完整週期
交易記錄檢視器	• 詳細的工作階段記錄 (HTTP/TCP)，包含用戶端、封包、通訊協定、請求標頭、延遲資訊及其他項目 • ADC 系統記錄的事件檢視 • 依據自訂監控和警示規則的警示檢視器
配置工具	• 適用於服務物件 (VIP、服務群組、伺服器) 及共用物件的集中 ADC 配置功能，包括範本、aFleX 及健全狀態監控 • 自動配置學習 (棕地部署) 及配置同步

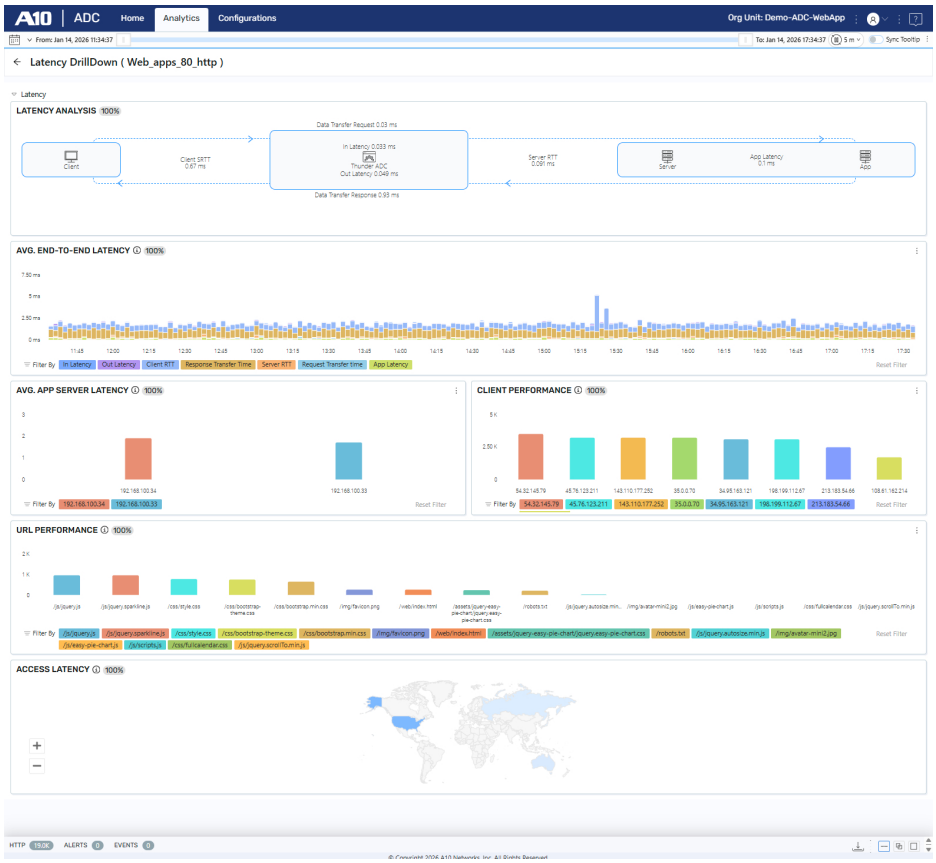


圖 7：以 ADC 分析深入研究延遲。

Defend Orchestrator	
防護工作流程編排	• 實現無縫的自動化 DDoS 防護，涵蓋偵測、緩解及報告等階段 • 攻擊結束後自動提出 DDoS 事件報告
Orchestrator 儀表板	• DDoS 事件及活動概觀 • DDoS 防護狀態及活動概觀 • 服務防護健全狀態儀表板、以彙總流量緩解攻擊 • 攻擊趨勢見解 (前 K 個) 提供攻擊類型、來源、受害者/目的地及其他項目
DDoS 事件控制台	• 用於 DDoS 防禦監控和即時作業的緩解控制台 (深入分析至服務連接埠層級) • 即時流量圖表可依據對策提供封包速率、流量、流量指標及封包下降數圖表 • 前 K 個 (來源及目的地)、事件及事件記錄、警示檢視器，以及全域及服務連接埠層級緩解統計資料 • 手動介入以自訂緩解原則
監控	• 受監控區域/物件的即時流量圖表和統計資料 • 受害者和來源 (前 K 個) 的詳細 IP 可視性及見解 • 遠端觸發封包擷取工具 (隨需或自動) • 為 DDoS 事件、受保護區域及裝置庫存等提供隨需及排程報告
配置工具	• 集中 DDoS 防護設定檔及作業原則配置 • 直覺操作的配置，提供可重複使用的預定義範本、防護設定檔及作業原則 • 支援基於 BGP 的流量重新導向 (在反應式部署中)、RTBH、Flowspec • DDoS 防護專用的裝置管理 (Mitigator 及 Detector 設定)

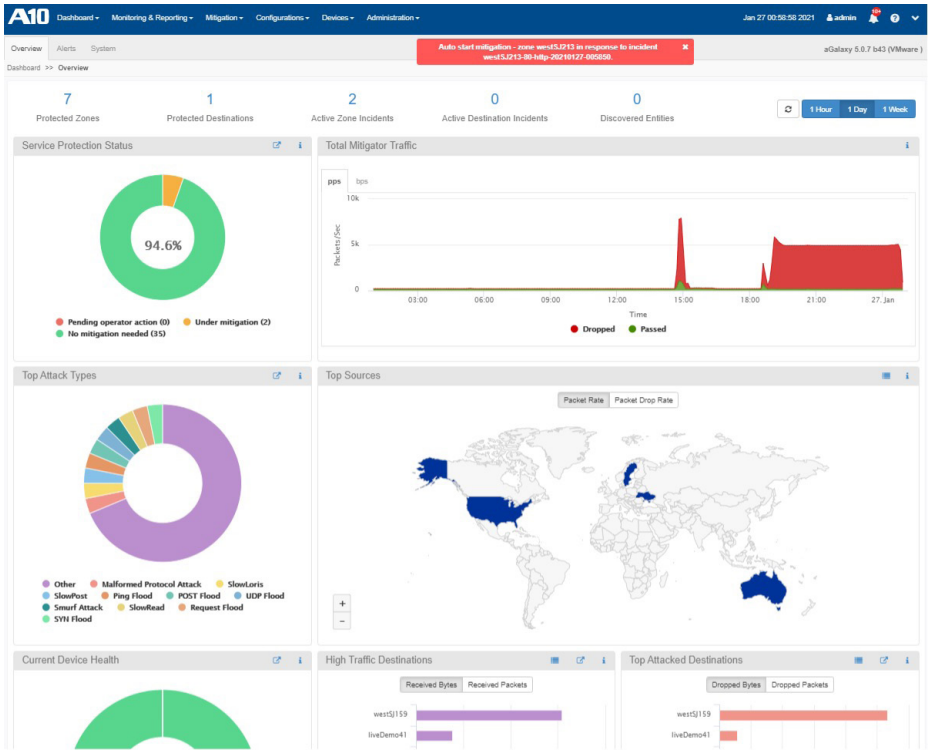


圖 8：A10 Defend Orchestrator 儀表板提供即時攻擊統計資料及 DDoS 事件摘要。

SSL Insight	
部署精靈	• 直覺操作的配置精靈，搭配引導式或非引導式工作流程選項，適用於 SSLi 及安全網路閘道 • 支援線地及棕地部署用於任何部署選項 (單或雙設備、高可用度、透明/明確代理、服務鏈、L2/L3/虛擬線等)，並提供建議的安全原則 • 快速存取全域 (站台群組)、站台或裝置層級配置，針對特定站台或裝置進行新站台部署、原則或配置變更 • 支援使用配置差異對比及回復功能以檢閱配置變更情況
集中配置管理	• 儲存及管理各種 SSLi 配置作為共用物件，包括 ACL、原則範本、SSL 設定檔、憑證管理、URL 篩選、ICAP、AAM、SAML、G-suites 及 Office 365 等 • 標記管理工具可定義及管理實體和邏輯介面及連線屬性
SSLi 分析	• 站台群組範圍的 SSL Insight 分析提供即時 KPI，包括連線及速率、解密速率、錯誤及原則違規率 • TLS 流量觀察及見解提供前 K 個解密流量 (來源/目的地)、TLS 及憑證特定資訊、快取憑證及其他項目 • 安全相關見解 (依據 URL 類別、應用程式類別及威脅情報)，以連線及流量觀點提供流量趨勢及模式，並將各個區域的高風險及可疑存取可視化 • 觀察清單可讓管理員建立自訂的 URL 及應用程式類別清單，以進行即時流量監控及分析
疑難排解工具	• 透過 SSL Insight 進行引導式的逐步測試，用於驗證系統、資源及端對端通訊 • 指標關聯可用於比較相同裝置的不同 KPI，以及比較不同裝置的相同 KPI
交易記錄檢視器	• 提供 SSLi 交易、錯誤及防火牆事件記錄的延伸檢視及搜尋功能，用於疑難排解及分析 • 以豐富的搜尋篩選條件 (IP、TLS、URL/應用程式類別、大小、狀態及許多其他項目) 和嵌入式 Threat Investigator 查詢功能 (由 Webroot 提供支援) 進行詳細的工作階段深入分析

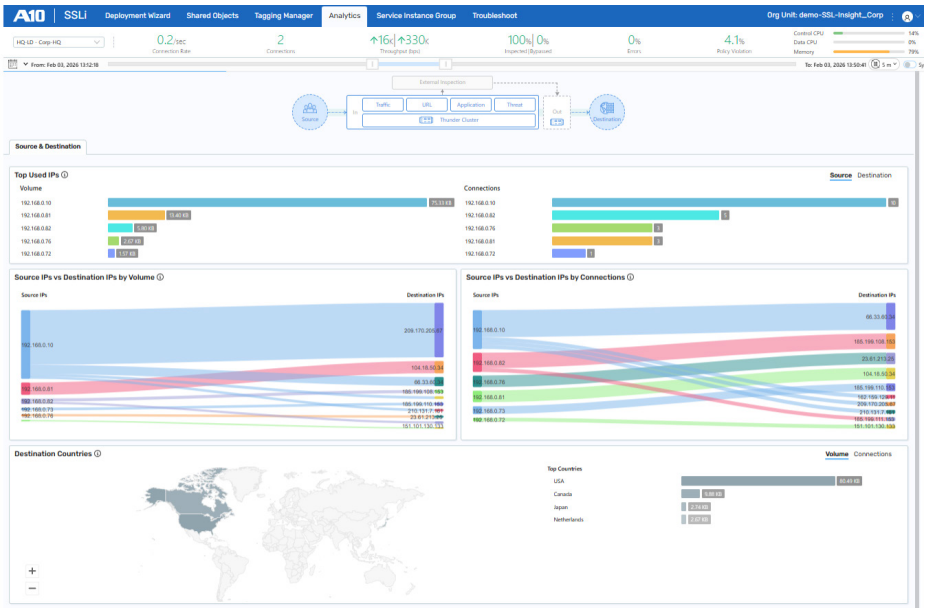


圖 9：SSLi 應用程式提供來源及目的地 IP 關聯分析資料。

電信級 NAT	
CGN 應用程式首頁	• 提供整合資訊協助掌握租戶之下的 CGNAT 部署資訊 (組織單位) • CGNAT 服務狀態分析適用於 LSN/固定 NAT/1:1 NAT/DS-Lite/NAT64/NAT46 無狀態技術 • 事件及警示儀表板
分析	• CGNAT 服務分析適用於組織單位之下的各項 CGN 技術 (LSN/固定 NAT/1:1 NAT/DS-Lite/NAT64/NAT46 無狀態) • 即時 CGNAT 服務層級 KPI，包含流量及工作階段資訊、NAT 集區使用情形等項目 • 有關流量、工作階段、連接埠對應、下降流量及錯誤、連結探測及 CGN 系統的 CGNAT 服務見解 • 詳細的 CGNAT 技術分析 - 流量見解包括工作階段、前 K 個、使用者配額；CGN 服務見解包括連接埠對應、集區使用情況及不當行為，以及應用程式類別見解 • 安全分析用於整合式 DDoS 防護、封鎖清單 IP 及其他項目
交易記錄檢視器	• 提供各種資訊，協助掌握 CGN 工作階段及交易，包括 IP：連接埠對應、訂閱用戶資訊 (例如 MSISDN、IMSI)、工作階段狀態、自訂欄位及其他項目 • 詳細的工作階段深入分析，包含豐富的搜尋篩選條件及追蹤訂閱用戶 • 事件檢視器用於 CGN 錯誤記錄及系統事件和警示
配置工具	• 集中 CGNAT 配置 (LSN/NAT64/DNS64) 以及共用物件 (NAT 集區、類別清單、EIM/EIF、ALG)、整合式 DDoS 防護，以及記錄範本和其他項目

圖 10：CGN 應用程式提供 LSN 服務流量分析。

Gi/SGi 防火牆	
Gi 防火牆應用程式首頁	• 提供整合資訊協助掌握租戶之下的 Gi/SGi 防火牆部署資訊 (組織單位) • 事件及警示儀表板
分析	• Gi 防火牆服務分析功能適用於組織單位之下的各項防火牆原則規則集 • 即時 GiFW 服務層級 KPI，包含流量及工作階段資訊、規則命中計數器等項目 • 詳細的 GiFW 服務分析 – 依據防火牆規則的見解，包括規則效能、舊型規則清單、前 K 個訂閱用戶，而流量見解則包括 CGNAT 對應及使用率、應用程式類別及其他項目
交易記錄檢視器	• 提供廣泛資訊協助掌握防火牆工作階段，包括防火牆區域及介面、相關規則及訂閱用戶資訊，以及 NAT 流量的 IP：連接埠對應及追蹤交易等其他項目 • 詳細的工作階段深入分析，包含豐富的搜尋篩選條件 • GiFW/CFW 系統記錄的事件檢視器 • 依據自訂監控和警示規則的警示檢視器

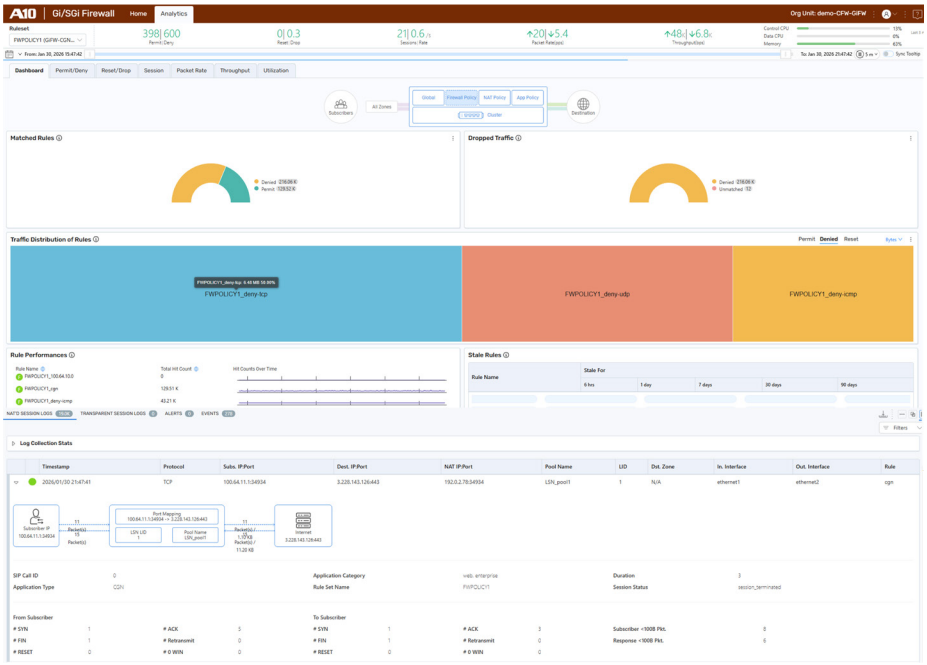


圖 11：Gi/SGi 防火牆應用程式以詳細的工作階段檢視器提供防火牆原則分析。

關於 A10

A10Networks.com

聯絡我們

A10Networks.com/contact

Part Number: A10-DS-15139-TW-03 Feb 2026

A10 中文資源網

請按讚並追蹤 A10 facebook粉絲專頁