A10

Always Secure. Always Available.

完整型錄

實現安全可用的數位世界

A10 優勢：簡化而不妥協

關鍵任務應用程式的最快回應和最低延遲

包括新一代 WAF、DNS 應用程式防火牆以及整合 DDoS 保護的選項

擁有全包式授權和跨多雲或混合雲的彈性橫向擴充

隨時待命且忠誠的團隊在您需要時提供支援

支援關鍵業務應用程式交付並為各種平台帶來最新的安全性

打造安全可用的數位世界

A10 Networks 於 2004 年成立，總部位於加州聖荷西 (San Jose)，為全球客戶提供服務。

A10 Networks 透過下列方式致力於協助客戶獲得更好的業務成果：提供網路安全見解來協助客戶應對不斷擴大的網路安全威脅情勢；為客戶提供複雜的混合基礎設施所需的解決方案；以及協助服務供應商確保其網路安全並擴大向服務不足社群提供更廣泛服務的能力。

為了在網路與應用程式中建立安全性與彈性，客戶需要考慮零信任、使用者體驗、自動化及新技術的採用 - 商機與需求。A10 Networks 透過以下方式協助客戶：

- 保護關鍵服務供應商與企業網路免受現代網路攻擊
- 支援具有應用程式安全性與可用性的高效雲端營運模式
- 運用互聯智慧、自動化、機器學習、AIOps 及 DevOps/SecOps 工具簡化 IT 營運

ISP/電信業者

網路服務公司

法人企業

資料中心

A10 Networks 解決方案組合

整合監控和可視化解決方案

Harmony

Harmony 控制器

DDoS 威脅情報服務

A10 Defend

A10 Defend Threat Control

負載平衡器/DNS

ADC

Thunder ADC

新一代 WAF

Next-Gen WAF

新一代 WAF

IPv6 遷移 電信級 NAT

CGN

Thunder CGN

雲端存取代理/FW/DPI
(ADC+CGN+FW+SSL 可視化)

CFW

Thunder CFW

雲端代理服務

Cloud Access

雲端存取控制器※1

DDoS 攻擊對策/不間斷 DNS

A10 Defend

A10 Defend Detector、Mitigator、Orchestrator

先進核心作業系統 (ACOS)

※1 於特定區域提供

解決方案

DDoS 攻擊預防

- DDoS 緩解
- DDoS 偵測
- 威脅情報

取得更多詳細資料 ▶ P8

伺服器負載平衡/應用程式交付

- 伺服器負載平衡
- 全域伺服器負載平衡
- 快取 DNS

取得更多詳細資料 ▶ P10

頻寬控制/公平性控制

- DPI
- 公平性控制

取得更多詳細資料 ▶ P12

A10

代理

- 安全網路閘道
- SSL/TLS 可視化

取得更多詳細資料 ▶ P13

IPv6 遷移和 IPv4 耗盡措施

- 電信級 NAT (CGNAT)
- IPv6 遷移技術

取得更多詳細資料 ▶ P14

本地卸載/雲端存取代理

- 流量分佈
- 租戶控制

取得更多詳細資料 ▶ P16

各種授權模式

請參閱產品系列平台相容性列表

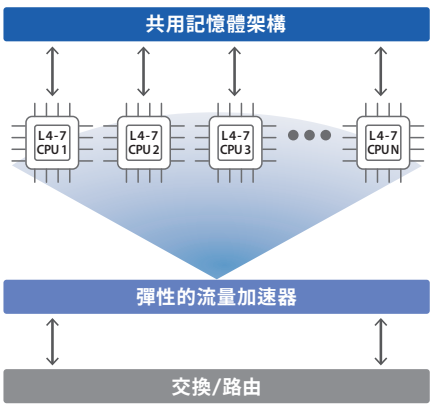
硬體電器	虛擬實例	裸機	容器	雲端實例	FlexPool
高效能 高連接埠密度	高機動性	硬體通用性	雲端原生	每小時/每月價格 訂閱、BYOL	頻寬池授權

安全選項 (附加授權)

- URL 篩選/URL 信譽
- IP 位址信譽
- 應用程式感知 L7 防火牆

我們專有的作業系統 ACOS (先進核心作業系統) 支援 Thunder 系列的效能。

ACOS 平台



Thunder 系列透過 A10 Networks 專有的作業系統和專用 64 位元硬體提供領先業界的效能。

ACOS 具有多核心、多 CPU 配置，每個 CPU 執行完全獨立的平行處理。透過去除多核心 CPU 特有的資料複製和鎖定問題，ACOS 能將 CPU 效能最大化。

ACOS 平台特點

- 加速應用程式
- 先進的安全功能
- 提高應用程式服務的可用性

特色解決方案

雲端服務，可讓您監控公司服務中使用的 IP 位址是否被用於 DDoS 攻擊。

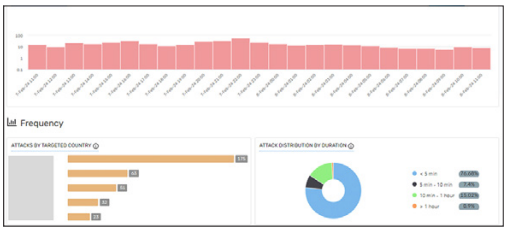
A10 Defend Threat Control

詳細資料
請參閱
我們的網站

監控公司服務的 IP 位址

- **您可能是攻擊的同謀嗎？**
- **您正在發動攻擊嗎？**
- **您正受到攻擊嗎？**

瞭解這些可以降低遭受攻擊的風險



查看全球 DDoS 攻擊狀態

提供給世界各地的服務供應商 基於 Anti-DDoS 技術的威脅情報

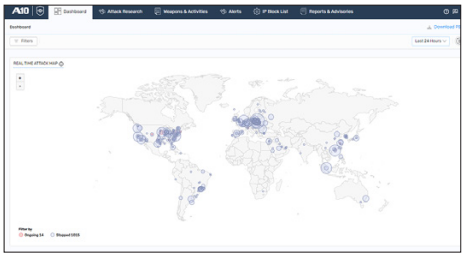
獨特的掃描器

- 掃描受攻擊工具的裝置
- 攻擊基礎架構分析

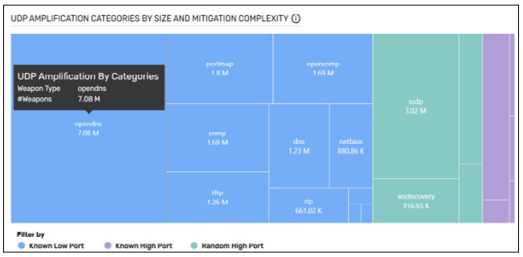
專有感測器網路

- 監控惡意活動
- 瞭解攻擊趨勢

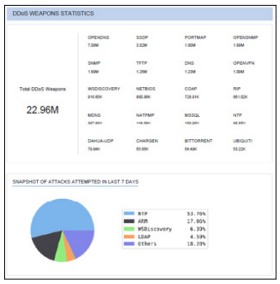
A10 Defend Threat Control 的範例畫面



入口網站螢幕擷取畫面 (儀表板)



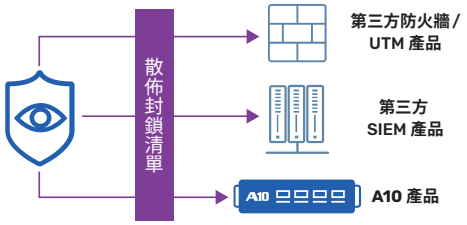
每個通訊協定的 UDP 放大器攻擊工具數量



每個通訊協定的反射器數量

高精度封鎖清單，專為 DDoS 攻擊所設計，可與現有安全設備配合使用

- 提供各種阻止清單 (殭屍網路、反射器、C2 伺服器等)
- 可匯入第三方防火牆和 SIEM 產品
- 可自訂的封鎖清單大小
- 所有 A10 產品無論大小均可匯入



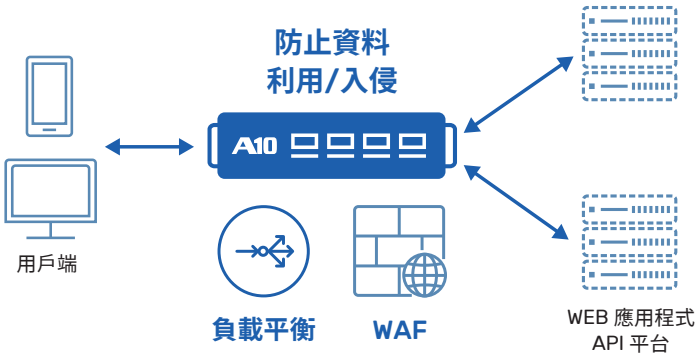
確認全球 DDoS 攻擊趨勢諮詢和報告以協助制定防禦計劃

- 透過專用入口網站隨時瞭解威脅狀況
- 可以搜尋被用作攻擊工具的設備和受害者 IP
- 查看全球 DDoS 攻擊趨勢
- 支援主動防禦的諮詢和報告
- 雲端服務代表無需安裝新設備或進行整合

應用程式交付 + 新一代 WAF
可用於封鎖模式，誤報率較低

由 Fastly 提供支援的 A10 新一代 WAF

詳細資料
請參閱
A10 網站



將誤報減至最少

在封鎖模式下可用

將誤報減至最少的實用解決方案

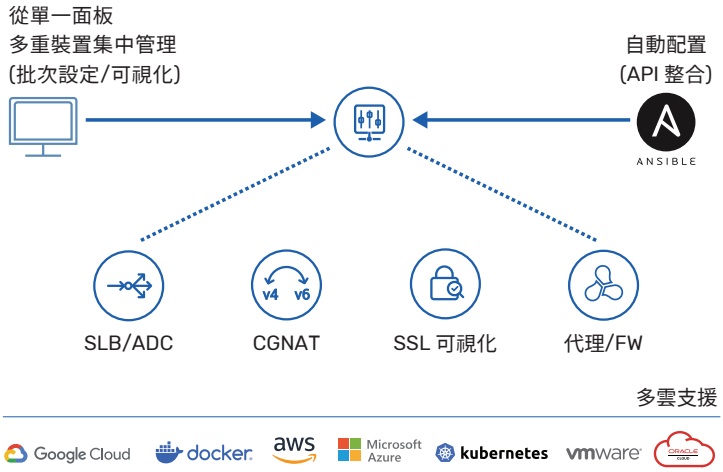
- 可在真實環境中使用全封鎖模式，大幅減少運轉負載
- 除了在雲端收集和分析資訊之外，還利用先進技術將誤報減至最少
- 也提供 TLS 卸載和 DDoS 防護等功能，改善使用者體驗並提供安全的操作環境。

「A10 新一代 WAF，由 Fastly 提供支援」是將 A10 的應用程式交付和負載平衡與 Fastly 新一代 WAF 整合在一起的解決方案。有多種外型尺寸可供選擇，包括虛擬機器和硬體。實用的解決方案，可將誤報減至最少並保護您的 Web 服務。

集中管理多個 A10 產品的平台

A10 Harmony 控制器

詳細資料
請參閱
A10 網站



LB/ADC 服務狀態可視化

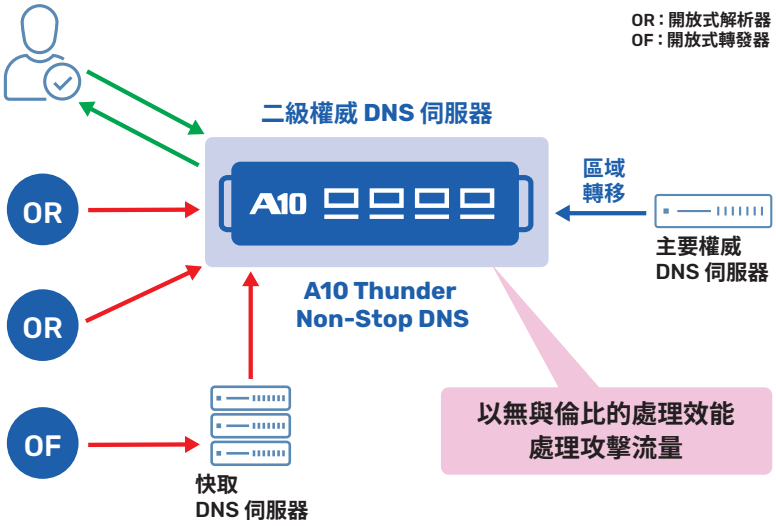
從單一面板集中管理多個裝置 (批次設定和可視化)

為部署在任何基礎架構 (包括資料中心、私有雲、公有雲和混合雲) 的 A10 產品提供集中管理、自動化和分析能力。為 Thunder ADC、CGN、SSLi、CFW、A10 Defend 等多種 A10 產品提供應用設定和策略管理的集中管理和分析能力。

保護權威 DNS 伺服器免受隨機子網域攻擊
(水刑式攻擊)

Non-Stop DNS

詳細資料
請參閱
A10 網站



■ 在現有權威 DNS 伺服器前面部署 Non-STOP DNS

無與倫比的 DNS 處理效能，正常的 DNS 服務即使受到攻擊也能繼續正常運作

■ Non-STOP DNS 回應來自用戶端的所有 DNS 查詢

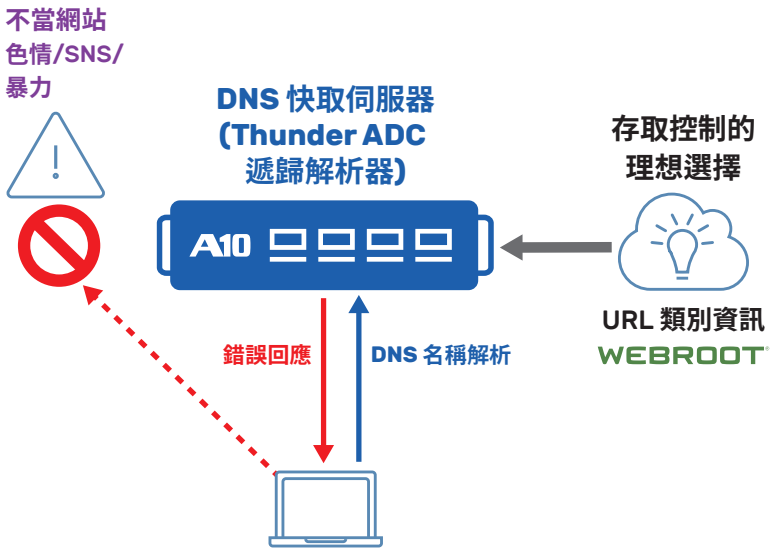
現有權威 DNS 伺服器作為主要權威 DNS 伺服器運作，用於區域資訊管理 (隱藏主要 DNS 配置)

Non-stop DNS 是 A10 Defend Mitigator (原 A10 Thunder TPS 系列) 提供的功能，可作為大容量的二級權威 DNS 伺服器。即使受到水刑式攻擊，其也會繼續回應，如果主要權威 DNS 伺服器出現故障，其將繼續提供服務，直到恢復。

基於 DNS 的安全措施

DNS 篩選

詳細資料
請參閱
A10 網站



■ DNS 存取控制

名稱解析時透過類別資訊進行存取控制，類似 URL 篩選器

✓ 相當於 URL 篩選器，更簡單的存取控制

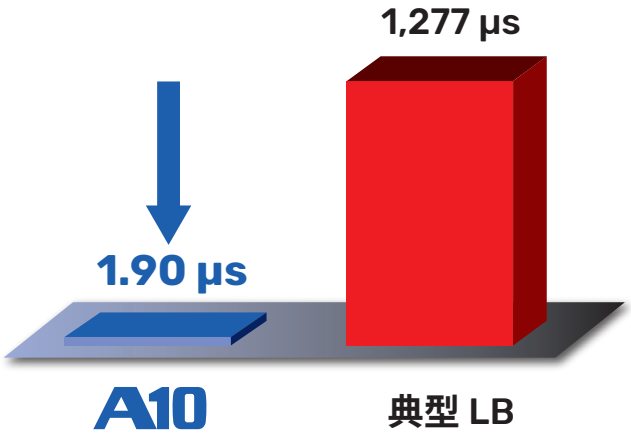
A10 的 DNS 篩選是一項執行基於 DNS 的存取控制的功能。
A10 可作為 DNS 伺服器並限制對特定類別網站的存取。

超低延遲的 TCP 流量負載平衡

超低延遲負載平衡

詳細資料
請參閱
A10 網站

與典型 LB 的延遲比較



獨特架構

實現超低延遲

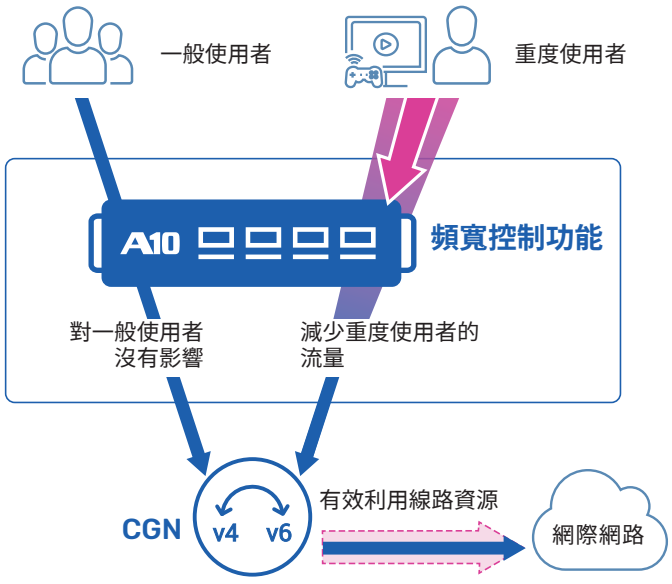
A10 Thunder 超低延遲型號

The A10 Thunder 超低延遲型號採用獨特架構，以超低延遲和低抖動對常見的 TCP 通訊進行負載平衡。能在超高速交易等需要低延遲的應用中提供更高速穩定的服務。

服務訂戶之間公平的頻寬使用

頻寬控制/公平性控制

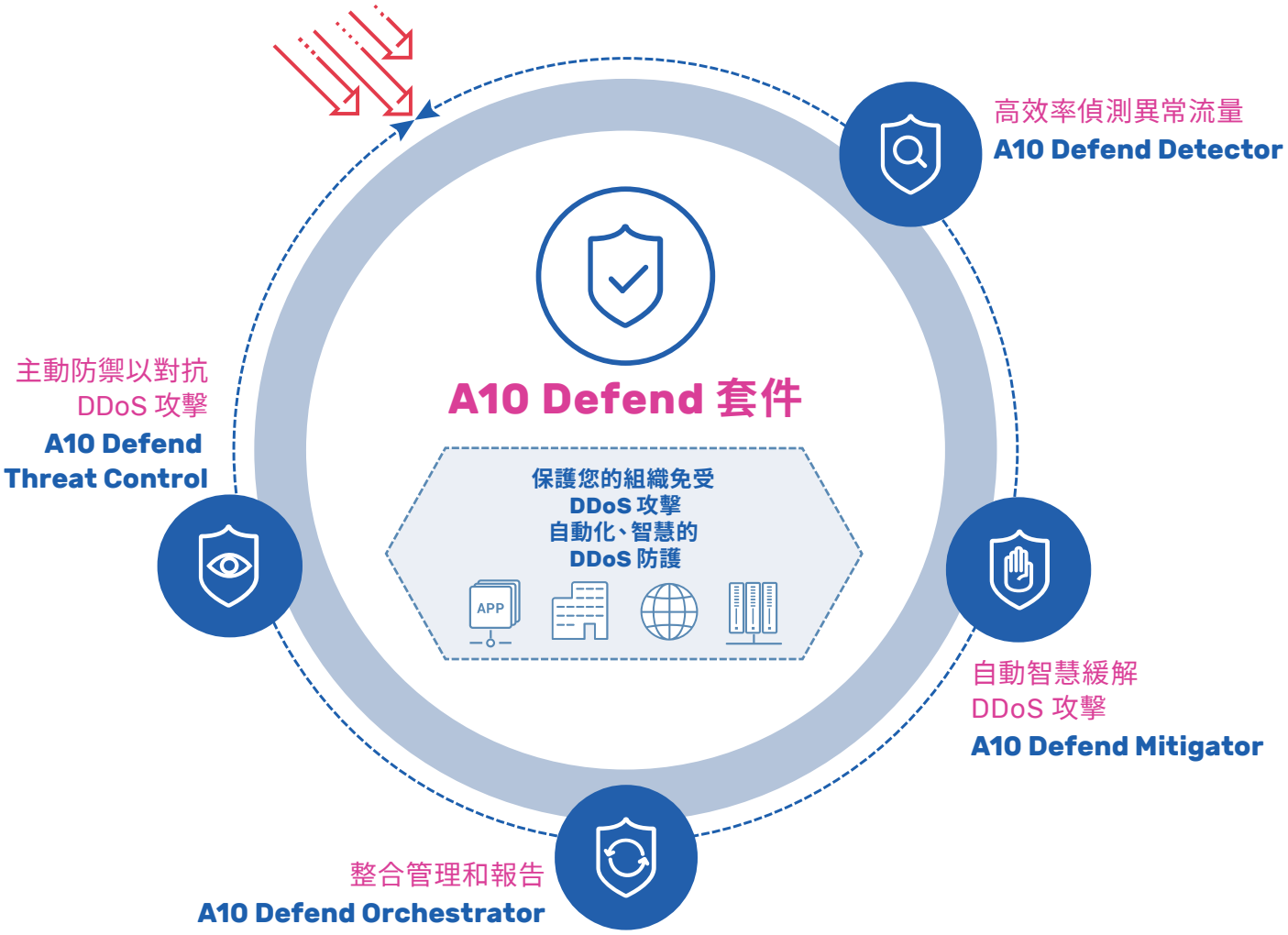
詳細資料
請參閱
A10 網站

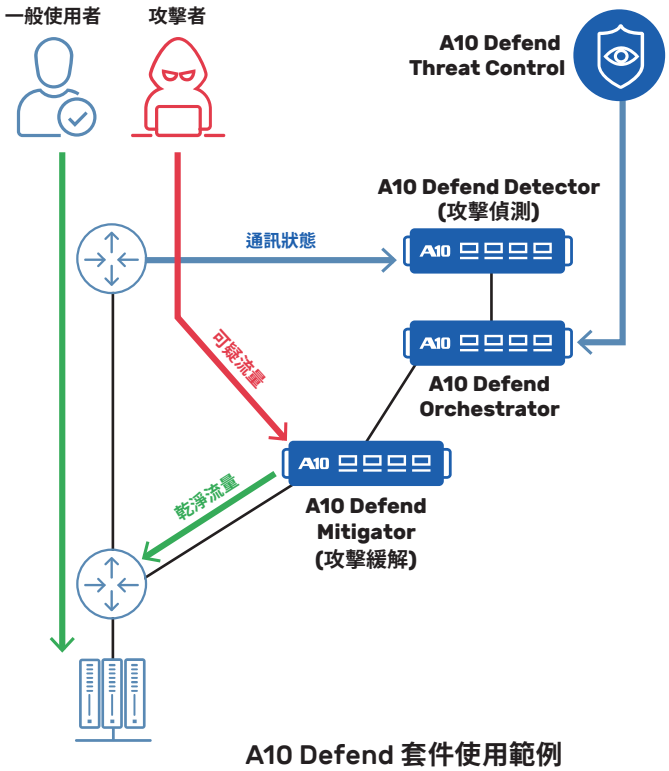


- 可根據來源 IP 位址和應用程式類型設定頻寬、每秒封包、每秒連線數和同時連線數的限制
- 作為防火牆的一部分提供，可與 CGNAT/ADC 功能結合使用
- 提供多種 A10 Thunder 外型尺寸，包括硬體、虛擬、裸機和容器

對重度使用者進行頻寬限制，確保服務訂戶頻寬的公平使用。
也可以對分組的訂戶套用分級控制。

A10 Defend 套件：DDoS 攻擊對策整合解決方案





A10 Defend 套件使用範例

A10 Defend 套件是一款 DDoS 攻擊防禦解決方案，在主要服務供應商和線上遊戲公司中擁有良好的記錄。利用 AI/機器學習來偵測和緩解 DDoS 攻擊，從而保護您的網路免受大規模 DDoS 攻擊。

A10 Defend Mitigator：
緩解 DDoS 攻擊並防止服務中斷。

A10 Defend Detector：
基於流量 (Flow) 的 DDoS 攻擊偵測。
基於 NetFlow、sFlow、IPFIX 等流量資訊偵測攻擊。

A10 Defend Orchestrator：
使用 Detector 和 Mitigator 集中管理 DDoS 攻擊偵測和緩解。
提供 Mitigator 和 Detector 之間的協調和管理、攻擊狀態監控和報告等功能。

A10 Defend Threat Control：
DDoS 攻擊預防關鍵功能。
由 A10 安全研究團隊進行收集、研究和分析。
用於瞭解攻擊面 (攻擊目標區域) 的現況並規劃對策。
主動防禦作為強大的第一層防禦。
分析和提供威脅情報。

A10 優勢

減少攻擊造成的損害以及回應攻擊所需的成本

盡量保護正常通訊

攻擊狀態即時可視化

主要特點

AI/機器學習自動防禦

如果發生流量攻擊，AI 會瞭解攻擊形式，並自動產生保護篩選器，將對正常通訊流量的影響降到最低。

主動防禦

透過使用未來 DDoS 攻擊中可能使用的裝置的 IP 資訊作為威脅情報，可以在攻擊發生之前設定防禦。

支援所有類型的 DDoS 攻擊

不僅保護網路免受流量攻擊，還保護網路免受應用層和網路層的複雜攻擊，以及加密流量攻擊。

彈性設定

可根據網路設定以內聯或外路徑設定自由部署，並具有與其他公司的攻擊偵測產品 (流量 (Flow) 收集器等) 整合的良好記錄。

高效能

透過專用硬體偵測並緩解 60 種常見攻擊模式，結合針對多核心最佳化的專有作業系統，實現高達 5 億 pps 的防禦效能。

各種外型尺寸

根據容量和位置選擇適當的機型，從專用實體設備到虛擬設備，或在 Azure 等公有雲上使用。

支援的產品

截至 2024 年 10 月

DDoS Mitigator (可透過改變模式改為偵測裝置)

~20 Gbps	10G ~ 100 Gbps	100 Gbps~
 **Thunder 1060S** **5G、10G、20 Gbps** 7x1GC、4x1/10GF、2x10/25GF	SPE 型號  **Thunder 5845** **100 Gbps** 48x1/10GF、4x100GF	SPE 型號  **Thunder 8665S** **550 Gbps** 12x400GF
 **Thunder 3350-E** **10 Gbps** 6x1GC、2x1/10GF、8x1/10GF、4x10GF	SPE 型號  **Thunder 5845-40G** **40 Gbps** 48x1/10GF、4x100GF	SPE 型號  **Thunder 7655S** **380 Gbps** 16x100GF
 **Mitigator VA** **1 - 5 Gbps** 虛擬設備	 **Mitigator VA** **10 - 100 Gbps** VMware ESXi (SR-IOV) FlexPool 授權	SPE 型號  **Thunder 7445** **220 Gbps** 48x1/10GF、4x100GF
 **適用於雲端的 Mitigator VA** **5 Gbps** Microsoft Azure		

管理

Orchestrator VA

訂閱者入口網站 VA

DDoS Detector

Detector VA
獨立式 Detector
15 萬 – 150 萬 fps

*SPE 型號：配備 SPE (安全和策略引擎) 的型號，這是一種加速安全策略應用的硬體功能

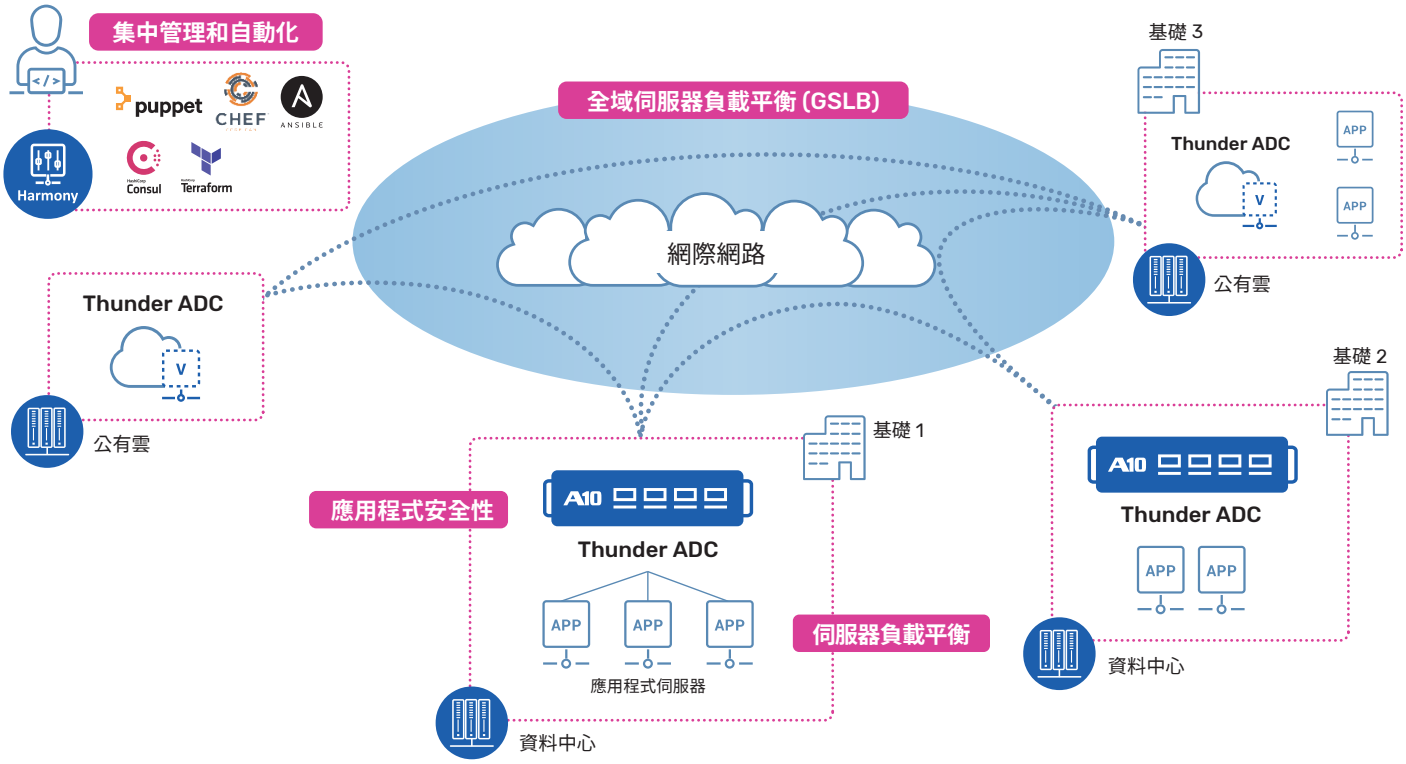
如需最新資訊或詳細資料，請參閱右側的網頁。

詳細資訊

Data Sheet

伺服器負載平衡/應用程式交付 (負載平衡器/ADC)

安全地交付關鍵業務應用程式



伺服器負載平衡

- 改善服務可用性
- 負載平衡快速回應

全球伺服器負載平衡 (GSLB)

- 跨站點的全球高可用性
- 內容在地化和監管合規性

應用程式安全性

- Web 應用程式防火牆 (WAF)
- DNS 應用程式防火牆
- 應用程式存取管理
- 整合 DDoS 防護

備援 / 叢集

- VRRP-a
- aVCS
- 橫向擴充

集中管理和自動化

- 集中政策執行
- 即時應用程式分析和可視化
- 編排和自動化

快取 DNS

- DNS 全方位服務解析器
- DNS 負載平衡

A10 優勢

提高應用程式可用性

- 在多個資料中心和多雲環境中高速、可靠的應用程式交付
- 將網路延遲和停機時間減到最短，改善使用者體驗

全面的應用程式安全

- 進階 SSL/TLS 卸載
- 單一登入 (SSO)
- 防禦 DDoS 攻擊
- Web 應用程式防火牆 (WAF)

應用程式可視性

- 透過與 A10 的 Harmony 控制器連結，以每個應用程式為基礎可視化配置狀態
- 可以在多雲環境中管理和控制服務，包括內部部署和公有雲

主要特點

進階伺服器負載平衡

- 透過彈性的流量控制、可自訂的服務運作狀況檢查，以及利用 aFleX 指令碼的全代理 L4-L7 負載平衡，確保應用程式可用性
- 實現機架空間的有效利用

多租戶軟體

- 可自訂的政策和角色型存取控制 (RBAC) 支援緊密隔離、最高密度的多租戶解決方案

部署到任何雲端

- 以硬體、虛擬、雲端、裸機和容器外形尺寸部署
- 使用 FlexPool 實現跨多雲的授權可移植性

加速應用程式效能

- 透過快取和 TCP 最佳化加速內容傳輸
- TLS/SSL 卸載，支援最新的 ECC 密碼

Web 和 DNS 保護

- 整合安全性，包括單一登入、CAPTCHA、Web 和 DNS 防火牆、DDoS 防護

特定應用程式分析

- 與 A10 Harmony 控制器整合，實現使用者體驗、流量概況、運作狀況檢查和效能監控的可視化

Rest 型可編程性

- 100% API 覆蓋率
- 與許多 DevOps 和自動化管理工具的原生整合

全球伺服器負載平衡 (GSLB)

- 擴展全域負載平衡。實現快速的伺服器回應時間
- 確保多雲環境中的業務連續性

DevOps 工具

- 使用 Terraform、Ansible 等自動化工具整合到 CI/CD 管道中

自動服務偵測

- 使用 A10 Thunder Kubernetes Connector (TKC) 或含 Consul 的 HashiCorp NIA 等第三方工具，在 Kubernetes 環境中自動探索服務

分析和事件監控

- 使用 Prometheus/Grafana 和內建 Prometheus 匯出器進行集中式網路可視性、事件監控和警報

支援的產品

截至 2024 年 10 月

虛擬設備	~25 Gbps	~100 Gbps	~200 Gbps	200 Gbps~	超低延遲機型
雲端 vThunder ADC Microsoft Azure、AWS：最高 10 Gbps Oracle Cloud：最高 24 Gbps	**Thunder 1060S** 25 Gbps 7x1GC、4x1/10GF、2x10/25GF	**Thunder 4440** 78 Gbps 24x1/10GF、4x40GF	**Thunder 6440** 150 Gbps 48x1/10GF、4x40GF	**Thunder 7655S** 370 Gbps 16x100GF SPE 型號	**Thunder 3745** 4 x 10GE
vThunder ADC 虛擬設備 最高 100 Gbps	**Thunder 1060S** 10 Gbps 7x1GC、4x1/10GF、2x10/25GF	**Thunder 3350S** 50 Gbps 6x1GC、2x1GF、8x1/10GF、4x10GF	**Thunder 5840** 115 Gbps 24x1/10GF、4x40GF **Thunder 5840-11** 115 Gbps 24x1/10GF、4x100GF	**Thunder 7440** 220 Gbps 48x1/10GF、4x40GF **Thunder 7440-11** 220 Gbps 48x1/10GF、4x100GF	
Thunder ADC 適用於容器 (Docker) 最高 100 Gbps		**Thunder 3350** 40 Gbps 6x1GC、2x1GF、4x25GF、4x40GF、4x10GF	**Thunder 5440** 100 Gbps 24x1/10GF、4x40GF		
裸機		**Thunder 3350 -E** 30 Gbps 6x1GC、2x1/10GF、8x1/10GF、4x10GF	**Thunder 6655S** 185 Gbps 16x100GF SPE 型號		
Thunder ADC 適用於裸機機型					

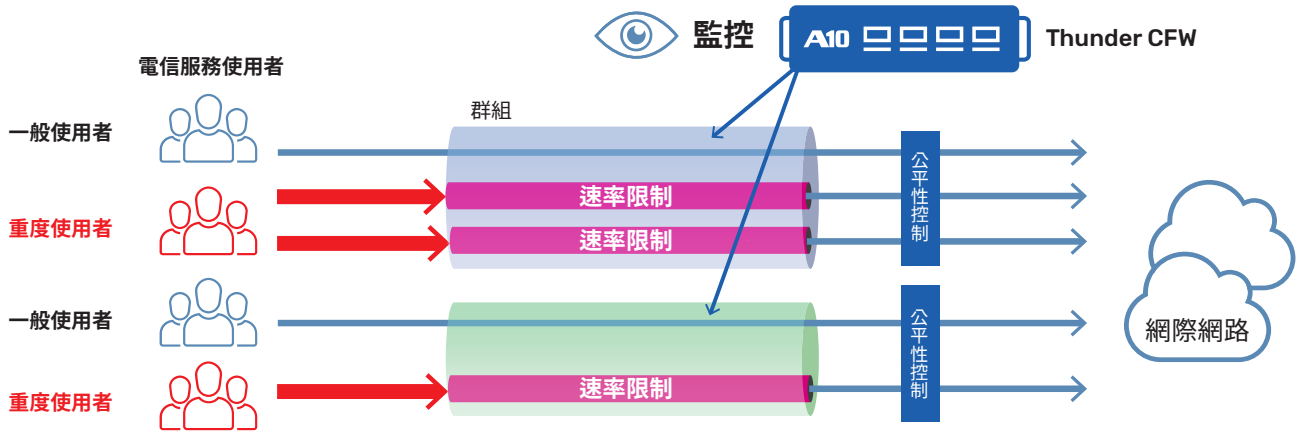
*SPE 型號：配備 SPE (安全和策略引擎) 的型號，這是一種加速安全策略應用的硬體功能

如需最新資訊或詳細資料，請參閱右側的網頁。

解決方案資訊

Data Sheet

頻寬控制/公平性控制



A10 的頻寬控制解決方案可以幫助抑制重度使用者過度使用頻寬，確保通訊頻寬的公平有效使用。可指定來源 IP 位址、目的 IP 位址以及 DPI 識別的應用類型，限制上下行通訊頻寬和連線數。

頻寬控制功能作為防火牆功能的一部分包含在內，除了公平性控制之外，還可以與 CGNAT 和 ADC 功能結合使用。

除了大容量專用硬體產品外，此功能也適用於裸機軟體、虛擬軟體和容器。

A10 優勢

分級公平性控制

透過在業務高峰時段限制重度使用者的頻寬，可以實現頻寬的公平使用，讓電信業者能提高其通訊服務訂戶的滿意度。也可以對分成組的服務訂戶套用分級控制。

有效利用網路資源

透過上下游聚合控制通訊頻寬、工作階段數量、每秒封包數等，實現網路資源的有效利用。

應用程式識別和控制

深度封包可偵測可識別通訊應用程式、可視化正在使用的應用程式、檢查正在使用的應用程式的狀態，並啟用每個應用程式的頻寬和通訊控制。

搭配 CGNAT 功能使用

電信級 NAT、防火牆、負載平衡、鏈路負載平衡、正向代理功能和其他 A10 Thunder 功能可以與流量控制整合在一起使用。

支援的產品

截至 2024 年 10 月

虛擬設備

雲端 vThunder CFW

vThunder
虛擬設備

Thunder
適用於容器 (Docker)

裸機

Thunder
適用於裸機機型

~100 Gbps*	~200 Gbps*	200 Gbps*~
Thunder 4440S 24x1/10GF、4x40GF	**Thunder 7440** 48x1/10GF、4x40GF **Thunder 7440-11** 48x1/10GF、4x100GF	**Thunder 8665S** 12x400GF
Thunder 5840 24x1/10GF、4x40GF **Thunder 5840-11** 24x1/10GF、4x100GF	**Thunder 6440S** 48x1/10GF、4x40GF	**Thunder 7655S** 16x100GF
Thunder 3350S 6x1GC、2x1GF、8x1/10GF、4x10GF		**Thunder 7650** 16x100GF
Thunder 5440 24x1/10GF、4x40GF		

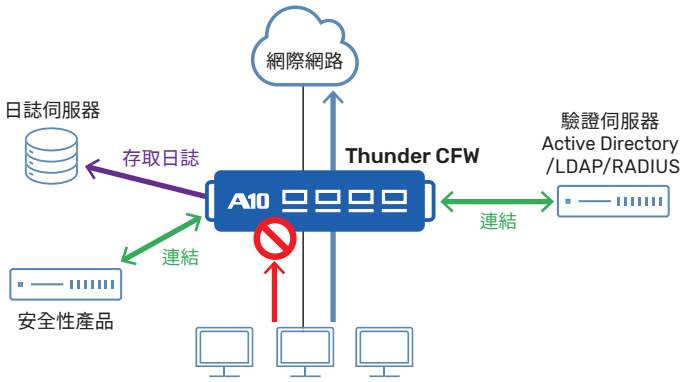
* 公平控制所需的近似處理量

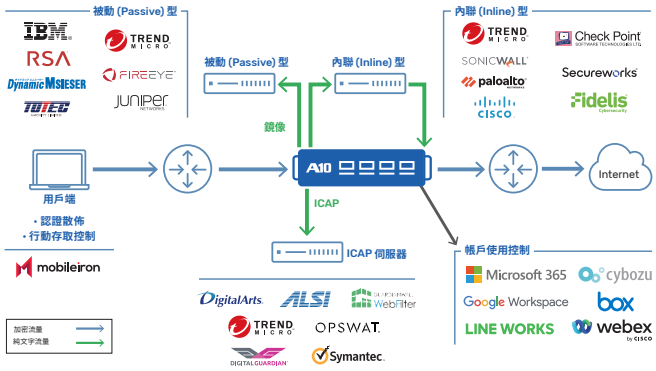
如需最新資訊或詳細資料，請參閱右側的網頁。

解決方案資訊

Data Sheet

代理





A10 的 Thunder 系列可作為 Web 的正向代理，具有較高的工作階段處理效能，足以應對因使用雲端服務而產生的網際網路大規模通訊工作階段處理，並可進行多種流量控制，例如代理鏈到上游代理、繞過雲端服務的流量，以及鏈路負載平衡。

透過與各種驗證伺服器/驗證服務連結，指定使用者和群組進行基於驗證和授權的存取控制，有助於實現公司和組織的零信任安全。

可視化 SSL/TLS 通訊，記錄詳細的使用者行為，並與各種安全產品搭配，解決隱藏在加密通訊中的威脅。威脅情報，包括 URL 篩選、URL 信譽和 IP 位址信譽，可針對不斷變化的威脅提供防護。還可以使用 L4 防火牆和應用程式防火牆功能進行流量控制。

多重掃描使用多個反惡意軟體引擎來改善偵測率、以內容威脅解除和重組 (CDR) 因應零時差攻擊，並可使用防止機密資訊外洩的資料遺失防護及代理功能。

A10 優勢

安全舒適的雲端服務環境

透過大規模流量分配和線路分配避免通訊瓶頸，並透過租戶控制實現基於 ID 的安全性

實現零信任安全性

結合身分驗證和授權基礎架構，彈性控制對資源和網際網路的存取

行為追蹤

加密通訊的可視化可以防範隱藏的威脅，並結合安全產品提供詳細的存取日誌，可靠地追蹤攻擊痕跡和員工行為

防止未經授權的存取

透過與威脅情報合作，防止未經授權的網站存取和攻擊者存取，從而強化安全性

支援的產品

截至 2024 年 10 月

虛擬設備	~5,000 個用戶端	~20,000 個用戶端	~50,000 個用戶端	50,000 個用戶端 ~
雲端 vThunder CFW vThunder 虛擬設備 Thunder 適用於容器 (Docker)	**Thunder 1060S 25G** 2 Gbps* 7x1GC、4x1/10GF、2x10/25GF	**Thunder 3350** 3 Gbps* 6x1GC、2x1GF、4x25GF、4x40GF、4x10GF	**Thunder 5440S** 15 Gbps* 24x1/10GF、4x40GF	**Thunder 7655S** 72 Gbps* 16x100GF
	Thunder 1060S 10G 1 Gbps* 7x1GC、4x1/10GF、2x10/25GF	**Thunder 3350-E** 3 Gbps* 6x1GC、2x1/10GF、8x1/10GF、4x10GF	**Thunder 4440S** 8 Gbps* 24x1/10GF、4x40GF	**Thunder 7440S** 25 Gbps* 48x1/10GF、4x40GF **Thunder 7440S-11** 25 Gbps* 48x1/10GF、4x100GF
裸機 Thunder 適用於裸機機型			**Thunder 3350S** 5.5 Gbps* 6x1GC、2x1/10GF、8x1/10GF、4x10GF	

Thunder 6440S 22 Gbps* 48x1/10GF、4x40GF	
Thunder 5840S 25 Gbps* 24x1/10GF、4x40GF **Thunder 5840S-11** 25 Gbps* 24x1/10GF、4x100GF	

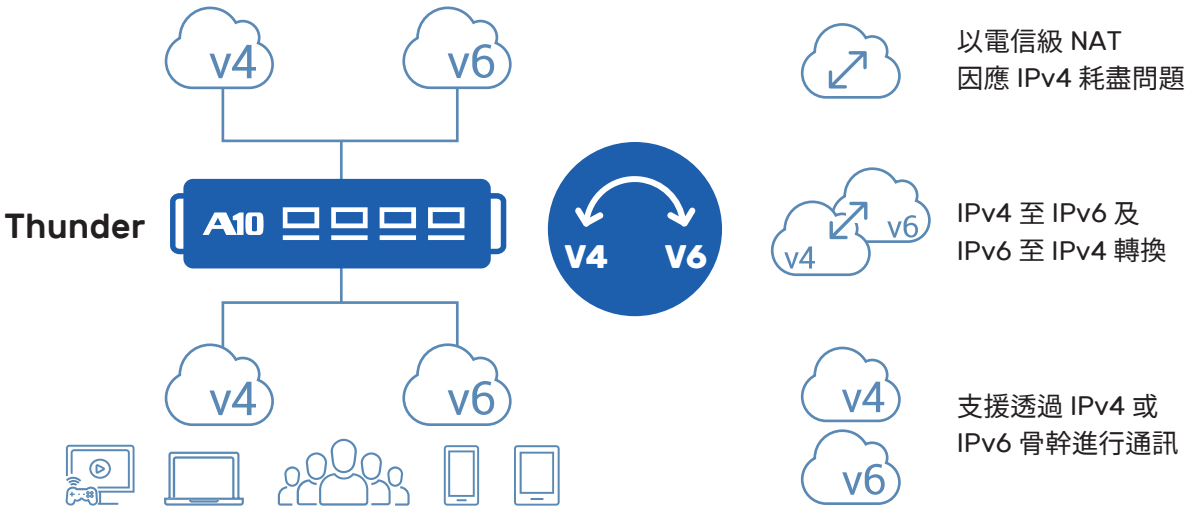
* 使用 SSL/TLS 可視化所有通訊時的最大處理量

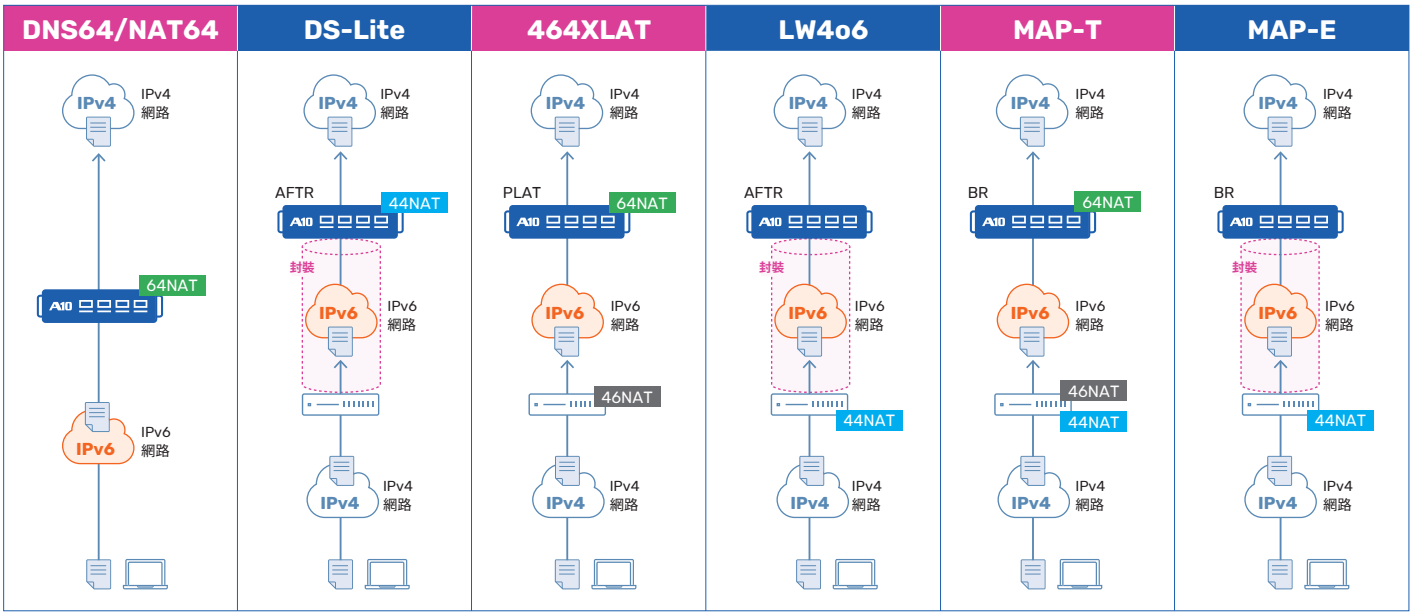
如需最新資訊或詳細資料，請參閱右側的網頁。

解決方案資訊

Data Sheet

IPv6 遷移、IPv4 耗盡措施





A10 的 IPv4 耗盡措施和 IPv6 過渡解決方案提供了 CGNAT 功能，可透過提高難以取得的 IPv4 位址的使用者容納效率來延長服務壽命，以及利用隧道和通訊協定轉換功能，同時在任何網路基礎架構上以低成本提供 IPv4 和 IPv6 服務。

A10 的 CGNAT 和 IPv6 遷移技術是高度可靠的解決方案，在過去十多年受到國內外許多電信業者的採用。

除了 CGNAT 和 IPv6 遷移，Thunder CFW 機型也允許使用 DPI 進行頻寬控制。

除了大容量專用硬體產品外，也提供裸機軟體、虛擬軟體和容器。

A10 優勢

降低購買 IP 位址的成本

透過標準化 IPv4 和 IPv6 基礎架構降低營運成本

提供使用者通訊控制和安全功能

主要特點

廣泛的商業卓著口碑

- 高可靠的解決方案，在國內外主要電信業者的 CGNAT 和 IPv6 遷移方面擁有豐富的商業經驗

支援所有 IPv6 過渡技術

- 支援商業市場中使用的幾乎所有的 IPv6 過渡技術，允許彈性配置以匹配現有的設施和投資計劃

大容量

- 支援高達 5.12 億同時連接的高容量，即使是擁有眾多使用者的大型電信業者也能以高容量效率配置服務

所有功能均為標準配置

- 提供服務所需的所有功能均作為標準配置包含在內，因此無需為每個功能購買額外的授權。邏輯分割區也允許同時使用 CGNAT 和多種遷移技術

彈性設定

- 即使現有設施是基於 IPv4 或 IPv6，也可以使用隧道和轉換功能來提供這兩個版本的服務

各種外型尺寸

- 根據容量和位置選擇適當的機型，從專用實體設備到虛擬設備、裸機軟體等

支援的產品

截至 2024 年 6 月

虛擬設備

vThunder
虛擬設備

Thunder CGN
適用於容器 (Docker)
最高 180 Gbps

裸機

Thunder CGN
適用於裸機機型

~100 Gbps

Thunder 4440
78 Gbps
24x1/10GF、4x40GF

Thunder 3350S
50 Gbps
6x1GC、2x1GF、8x1/10GF、4x10GF

Thunder 3350
40 Gbps
6x1GC、2x1GF、4x25GF、4x40GF、4x10GF

Thunder 3350 -E
30 Gbps
6x1GC、2x1/10GF、8x1/10GF、4x10GF

~200 Gbps

Thunder 6440
48x1/10GF、4x40GF

Thunder 5845 SPE 型號
115 Gbps
48x1/10GF、4x100GF

Thunder 5840
115 Gbps
24x1/10GF、4x40GF

Thunder 5840-11
115 Gbps
24x1/10GF、4x100GF

Thunder 5440
100 Gbps
24x1/10GF、4x40GF

200 Gbps~

Thunder 8665S SPE 型號
550 Gbps
12 x 400GF

Thunder 7655S SPE 型號
370 Gbps
16x100GF

Thunder 7650
370 Gbps
16x100GF

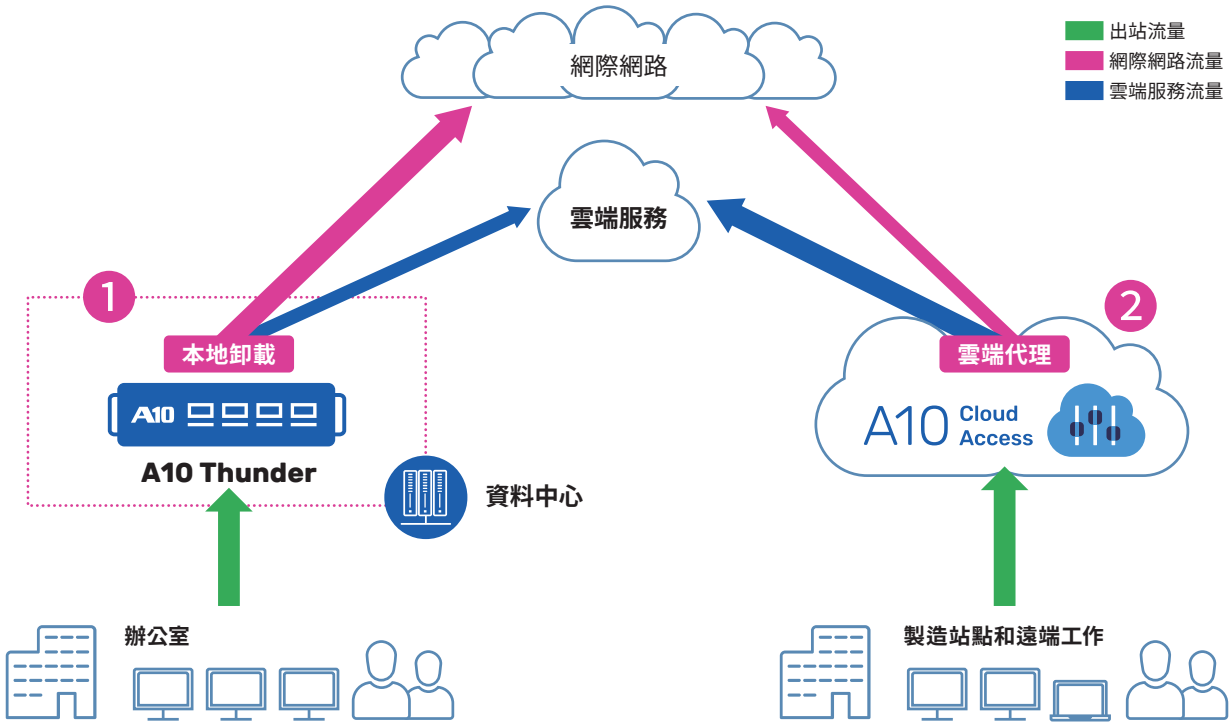
Thunder 7445 SPE 型號
220 Gbps
48x1/10GF、4x100GF

Thunder 7440
220 Gbps
48x1/10GF、4x40GF

Thunder 7440-11
220 Gbps
48x1/10GF、4x100GF

*SPE 型號：配備 SPE (安全和策略引擎) 的型號，這是一種加速安全策略應用的硬體功能

本地卸載/雲端存取代理



1 雲端存取代理

- 本地卸載
- 租戶控制
- 減少代理等網路裝置的負載
- 影子 IT 監控
- 每個應用程式的連線監控
- 防火牆和其他安全措施

2 雲端代理 (A10 雲端存取控制器)

- A10 提供的雲端服務
- 流量控制 + 存取控制 + 雲端安全
- 簡易授權結構
- 與各種安全性功能整合
- 與第三方 SaaS 和 SASE 解決方案整合以減少總成本
- 零信任網路存取 (ZTNA)
- 安全網路閘道

A10 優勢

流量隔離

- 本地卸載和資料中心卸載期間目的地網域的隔離
- SSL/TLS 通訊的可視化

存取控制

- ID 型存取控制
- 租戶控制
- 封鎖特定站點的外部存取
- URL 篩選器
- 存取記錄

安全性

- 保護卸載後的流量
- 提供多重掃描、內容威脅解除和重組 (CDR) 以及防資料外洩等多種安全功能

如需最新資訊或詳細資料，請參閱右側的網頁。

A10 雲端存取代理卸載解決方案詳細資料

A10 雲端存取控制器解決方案詳細資料

Data Sheet

主要特點

各種安全功能

- URL 篩選
- IP 信譽
- 與驗證基礎架構整合
- 應用程式防火牆
- 第 3 層、第 4 層防火牆
- 速限功能
- 多重掃描引擎
- 檔案清理 (CDR)
- 資料遺失防護 (DLP)
- SSL/TLS 解密
- 存取記錄

租戶限制

- 僅允許指定的企業帳戶登入雲端服務，限制個人和免費帳戶的使用，進而降低機密資訊外洩的風險

流量分佈

- A10 Thunder CFW 作為代理可減少 SaaS 部署後現有代理的負載
- 也可以自動續約不定期變更的 Microsoft 365 網域

線路卸載

- 對 SaaS 的存取直接路由到 SaaS 租用線路，無需經過代理，而非 SaaS 通訊則路由到現有的代理伺服器
- 確保安全，同時避免線路擁堵

安全網路閘道

- 作為顯性/透明 (explicit/transparent) 代理運作
- 透過 URL 篩選、應用程式可視性和控制、威脅情報和其他功能降低風險。微調使用者層級控制
- 透過與 SIEM 產品、高速日誌記錄等整合，確保遵守隱私標準
- SSL/TLS 可視性功能

支援的產品

截至 2024 年 10 月

虛擬設備	~5,000 個用戶端	~20,000 個用戶端	~50,000 個用戶端	50,000 個用戶端 ~
雲端 vThunder CFW	Thunder 1060S 25G 2 Gbps* 7x1GC、4x1/10GF、2x10/25GF	Thunder 3350 3 Gbps* 6x1GC、2x1GF、4x25GF、4x40GF、4x10GF	Thunder 5440S 15 Gbps* 24x1/10GF、4x40GF	Thunder 7655S 72 Gbps* 16x100GF
vThunder 虛擬設備	Thunder 1060S 10G 1 Gbps* 7x1GC、4x1/10GF、2x10/25GF	Thunder 3350-E 3 Gbps* 6x1GC、2x1/10GF、8x1/10GF、4x10GF	Thunder 4440S 8 Gbps* 24x1/10GF、4x40GF	Thunder 7440S 25 Gbps* 48x1/10GF、4x40GF
Thunder 適用於容器 (Docker)			Thunder 3350S 5.5 Gbps* 6x1GC、2x1/10GF、8x1/10GF、4x10GF	Thunder 7440S-11 25 Gbps* 48x1/10GF、4x100GF
裸機				
Thunder 適用於裸機機型				

虛擬設備	6,440S 22 Gbps* 48x1/10GF、4x40GF	5840S 25 Gbps* 24x1/10GF、4x40GF
雲端 vThunder CFW		
vThunder 虛擬設備		
Thunder 適用於容器 (Docker)		
裸機		
Thunder 適用於裸機機型		Thunder 5840S-11 25 Gbps* 24x1/10GF、4x100GF

* 使用 SSL/TLS 可視化所有通訊時的最大處理量

雲端存取控制器授權結構 A10 Cloud Access

截至 2024 年 6 月

- **僅限基本、標準和進階套裝授權**
  - 還有其他選項
- **依用戶端數量收費**
  - 收費單位：50 個用戶端
    (最低用量：50 個用戶端起跳)
- **期間：以年為單位 (最低合約：1 年)**
  - 免費試用：有 (1 個月)
- **存取日誌最長儲存 3 個月**
  - (日誌可透過 Web API 取得)

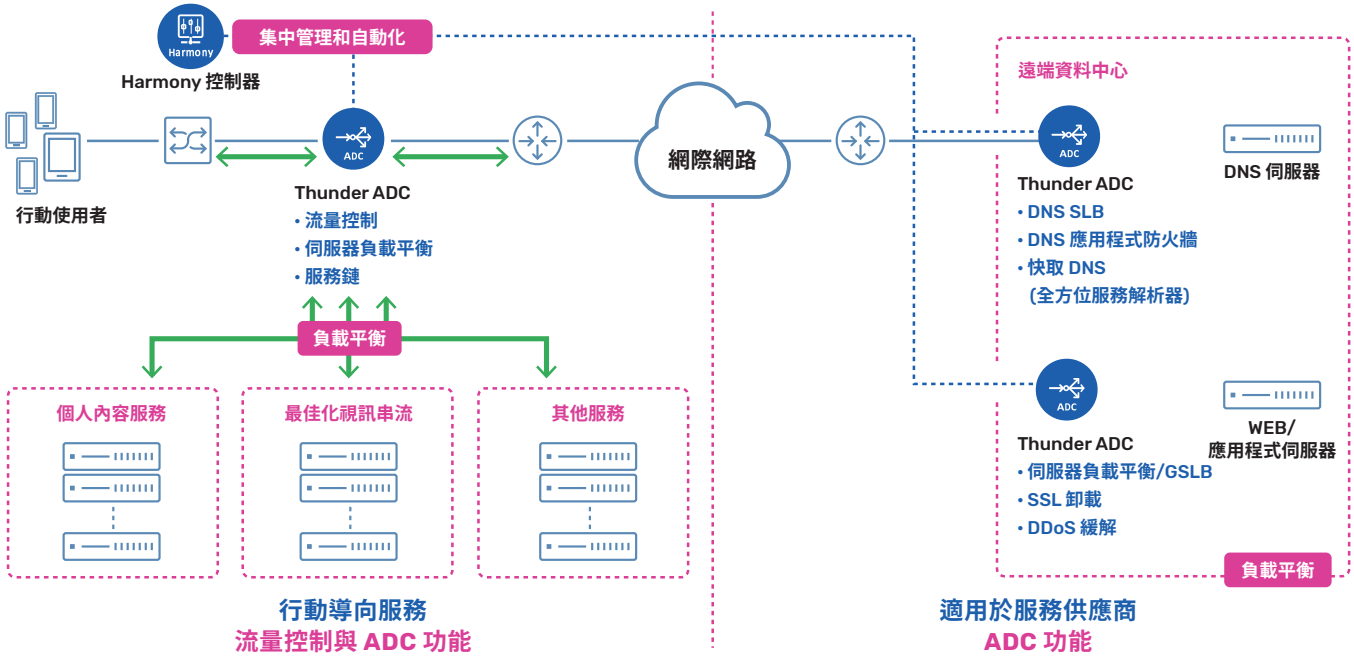
※目前僅於日本國內供應使用

功能	授權類型			
	基本	標準	進階	其他選項
正向代理	○	○	○	
反向代理	○	○	○	
流量控制功能	○	○	○	
驗證基礎架構鏈結	○	○	○	
存取日誌儲存	○	○	○	
URL 篩選	○	○	○	
SSL/TLS 解密		○	○	○
SaaS 服務的租戶控制		○	○	○
IP 位址信譽			○	○
應用程式可視性和控制			○	○
反惡意軟體				○
內容清理				○
資料遺失防護				○
透過站台對站台 IPsec VPN 連接				○
透過用戶端對站台 IPsec VPN 連接				○

案例研究

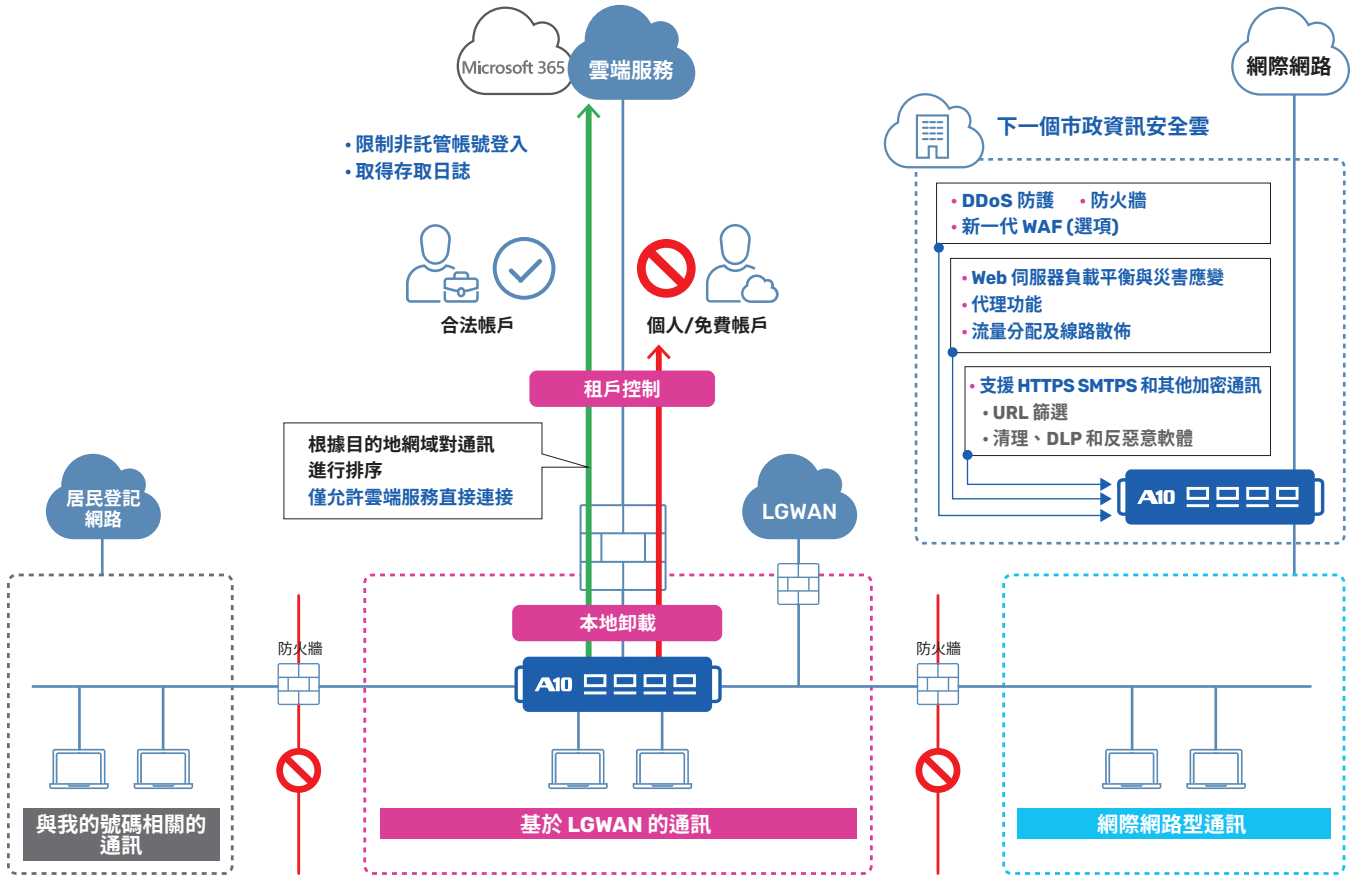
Web 商務

透過多雲環境中最佳化的應用程式交付、強化的安全性和簡化的操作，實現高品質、高可靠性的 Web 服務



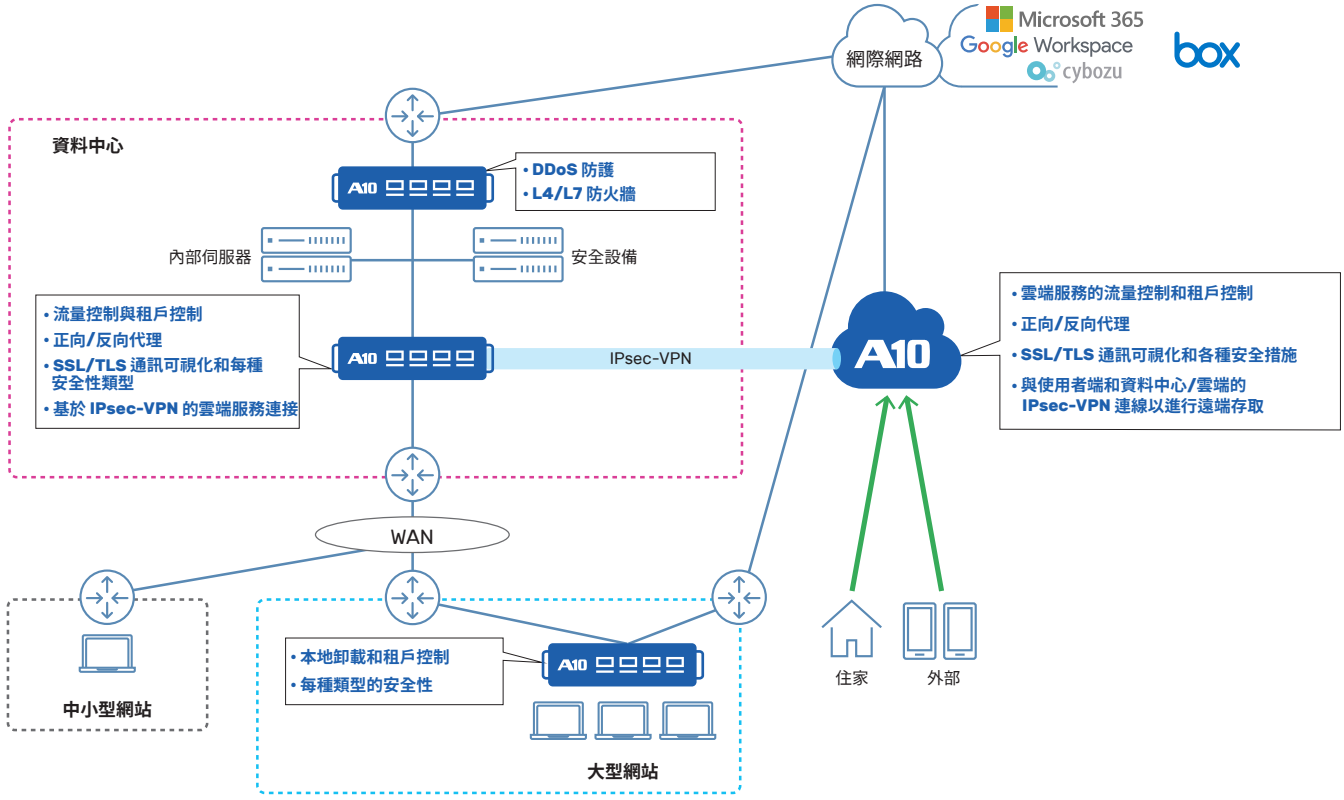
市政

與 α´ 機型相容。使 LGWAN 終端能連接到特定通訊，例如 Microsoft 365
提供本地卸載和租戶控制



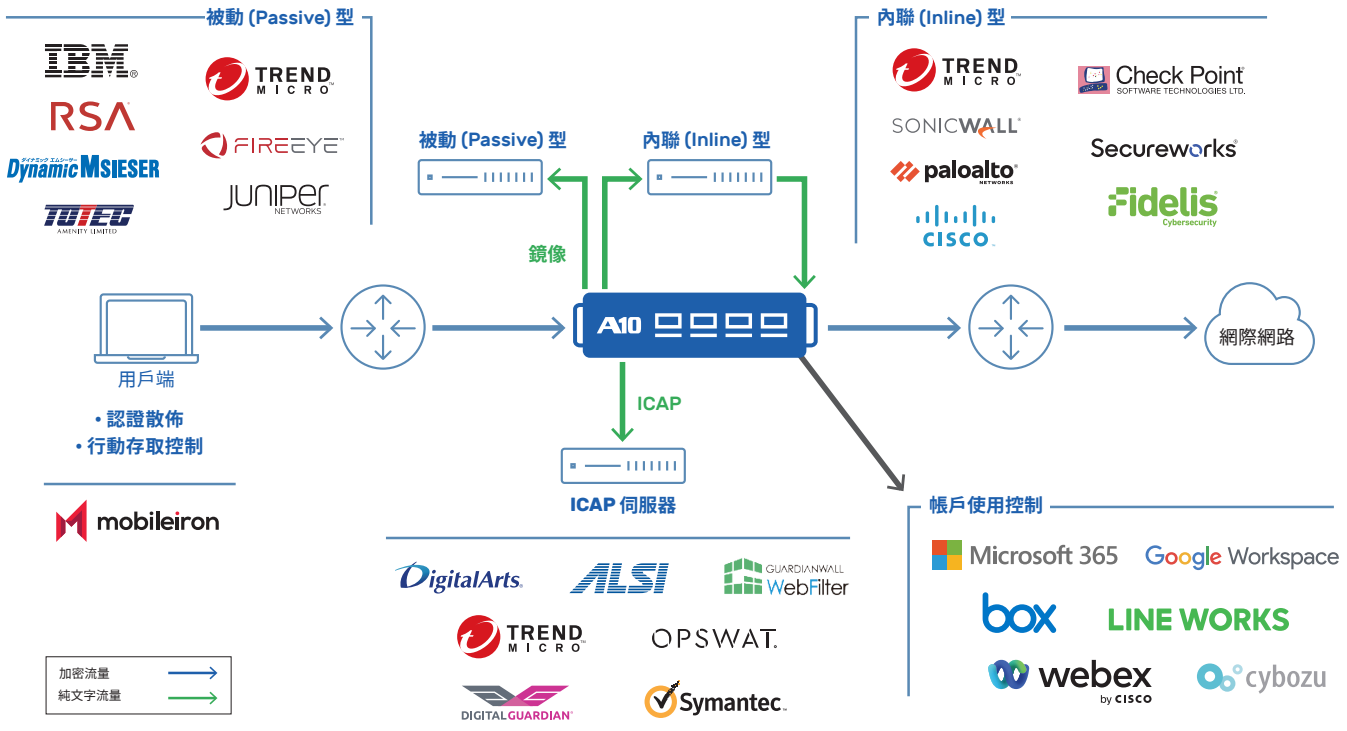
企業網路解決方案圖

最佳化通訊流量並強化每個資料中心/位置/雲點的安全性



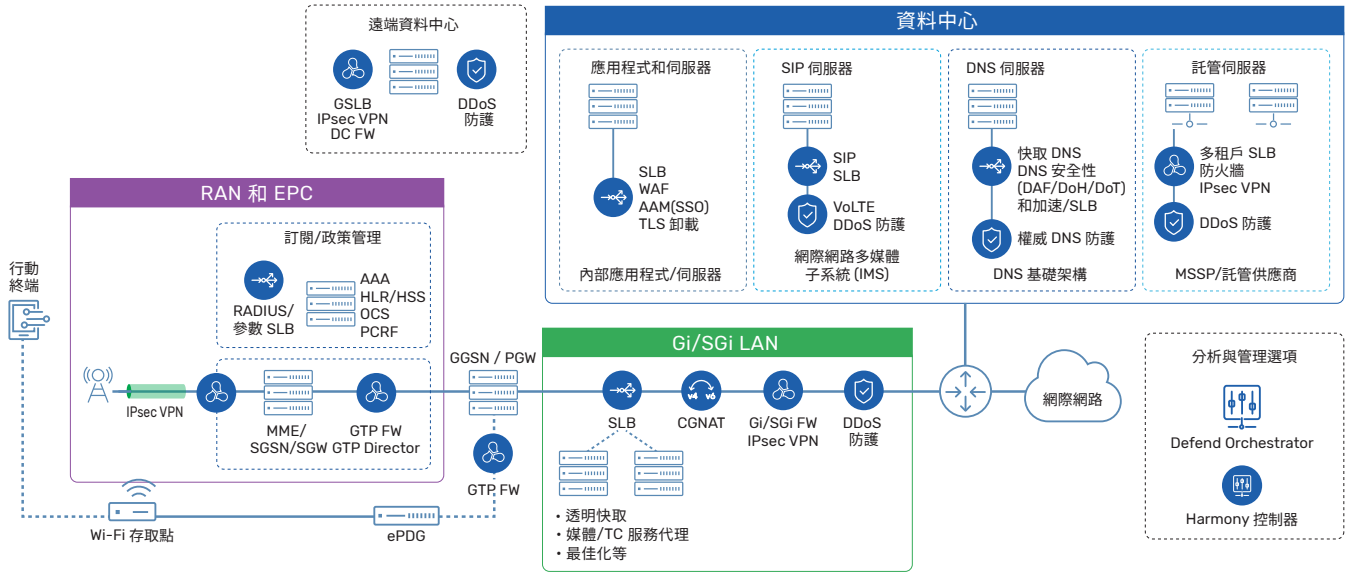
SSL/TLS 通訊可視性與整合式解決方案

對 SSL/TLS 通訊進行高速解密，並與多種安全產品整合，偵測和防範加密通訊中隱藏的威脅

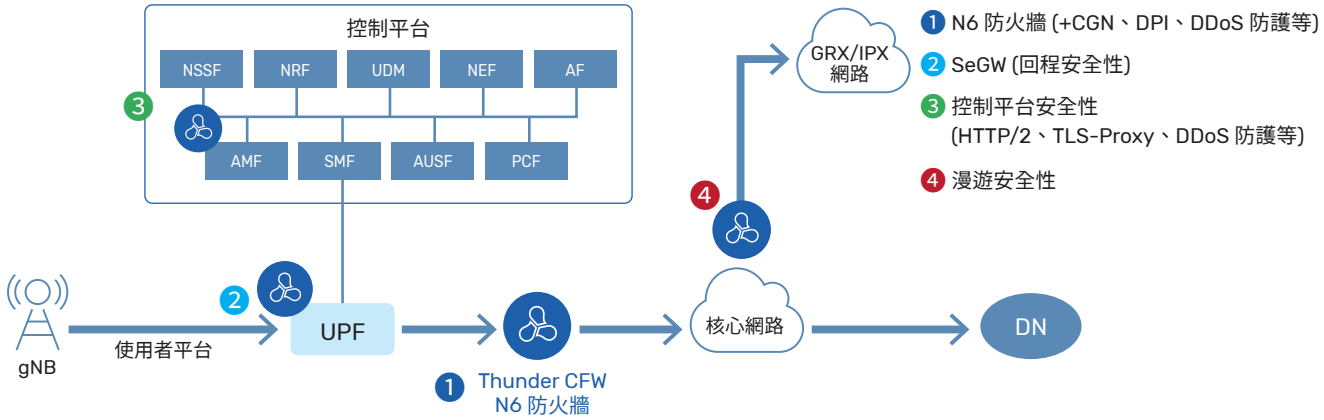


案例研究

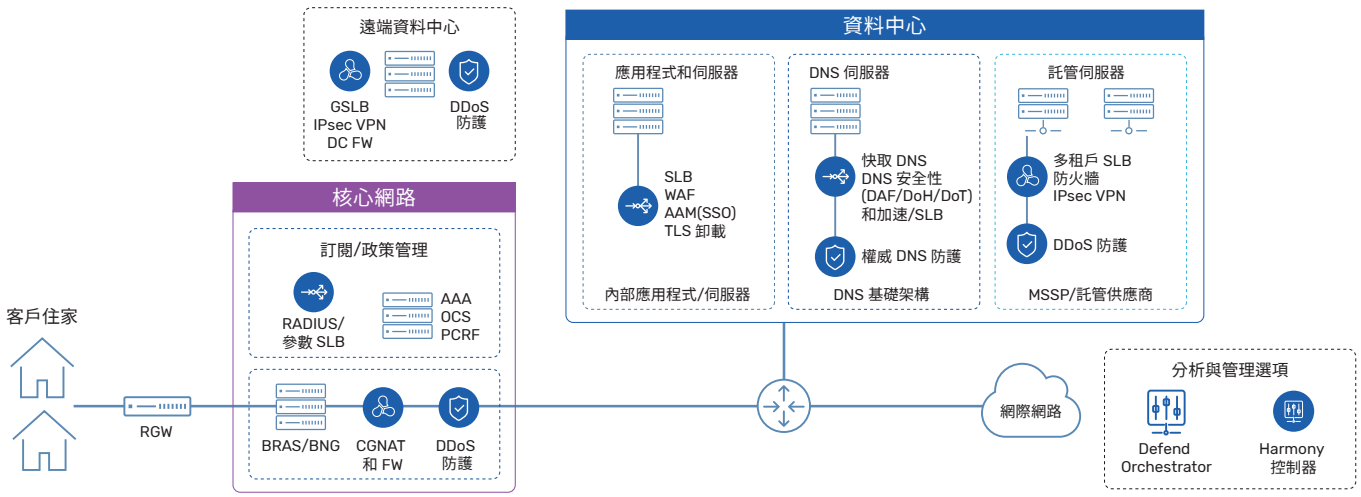
行動電信業者解決方案圖 (針對 LTE/5G-NSA)



行動電信業者解決方案圖 (針對 5G-SA)



ISP/CATV 電信業者解決方案圖



A10

A10 Defend DDoS 防護：

全方位的企業 DDoS 解決方案

DDoS 仍是排名第一的威脅事件，必須採用多向量分層式防禦方案加以因應。A10 的 DDoS 防護是套裝解決方案，結合偵測、緩解、編排及 DDoS 特定情報，提供準確、可擴充、智慧及主動防禦功能，協助對抗現今複雜的攻擊行動。A10 Defend 專為無縫整合所設計，除了能夠確保最出色的防護效果，也能維持營運效率及維護基礎架構安全，對抗持續增加的 DDoS 威脅。

威脅防護

使用案例 1：威脅防護

A10 的雲端原生威脅防護功能，是以 SaaS 解決方案的形式提供，可在盡量不中斷營運的情況下維護企業安全。其中不需要使用專屬的 DDoS 設備，而是以零萎縮的深入資料和分析協助您強化 DDoS 防禦。A10 的 DDoS 特定情報平台也能產生智慧型封鎖清單，在威脅影響營運之前就主動出擊加以阻止。這類清單可輕鬆與現有的安全基礎架構整合，提供統一及高效的防禦功能，對抗日趨複雜且為數眾多的威脅。

威脅偵測

使用案例 2：威脅偵測

A10 的 DDoS 特定偵測解決方案以流量型方法提供高速及高精度的偵測功能，只要三秒鐘就能識別潛在威脅。如此快速的偵測功能，可協助客戶盡量減少停機時間並維持服務可用性，即使正在遭受攻擊也沒問題。解決方案的彈性成為 DDoS 偵測的穩固基礎，不會中斷現有營運。

威脅緩解

使用案例 3：威脅緩解

A10 的 DDoS 緩解解決方案提供強大即時的防護，對抗流量型及應用層的 DDoS 攻擊，協助確保企業在最有攻擊性的威脅期間持續上線運作。A10 具備自動升級功能，可運用智慧功能遏止損害，無需手動介入。解決方案可內聯部署，或透過 BGP 路由或 DNS 路由進行整合。如果企業遭受預期之外的流量高峰，A10 目前以混合解決方案的方式提供雲端清理功能，可在必要時重新導向流量，確保持續安全性並維持正常運作時間。

A10 Defend DDoS 防護優勢

- **事先掌握威脅：**運用深入、準確及零萎縮的情報，在攻擊中斷業務之前就加以偵測及封鎖。
- **穩定的正常運作時間：**自動、智慧及可擴充的緩解功能，可確保正常運作時間，即使在大規模攻擊期間也沒問題。
- **簡化防禦：**專屬的編排功能可降低複雜度、加快回應時間及提升準確度，以便加速復原。

> *阻斷服務攻擊仍無所不在，成為最主要的事件模式。*
>
> — Verizon 2024 年資料外洩調查報告

資料來源：verizon.com/business/resources/Tfd3/reports/2024-dbir-data-breach-investigations-report.pdf

客戶信賴 A10 Networks

關鍵應用程式以及雲端移轉過渡期的管理

提供
始終在內部部署或雲端中提供應用程式交付和安全性

防護
企業及服務供應商的投資不受侵擾

支援
使用混合解決方案順暢遷移到雲端和雲端原生

安全
轉換到 5G 和雲端原生架構實現多世代網路

防護
網路免受攻擊而威脅到可用性

簡化
可提供 IT 營運互聯智慧、人工智慧 (AI)/機器學習 (ML) 和 DevOps/SecOps 工具

前 10 名中有 9 家	前 10 名中有 8 家	前 50 名中有 21 家	前 25 名中有 15 家	前 10 名中有 5 家
電信業者	雲端供應商	《財星》全球 500 大企業	電玩遊戲公司	媒體公司

已在全球 7,800 多家公司安裝

A10 Networks 的產品受到全球各行各業 7,800 多家頂尖公司的採用。
我們擁有各種需要高可靠性、容錯性和可用性的系統，特別適合網路內容供應商和服務供應商。受到 118 個國家 7,800 多家客戶的信賴：

支援最大品牌

關於 A10 Networks

A10 Networks 為內部部署、混合雲端及邊緣雲端環境提供安全性與基礎設施解決方案的廠商，協助客戶提供安全、高效能、高可用性的關鍵業務應用和網路。我們擁有超過 7,000 多家遍佈全球的客戶，包含大型企業、通訊、雲端和網路服務供應商。

A10 Networks 於 2004 年成立，總部位於加州聖荷西 (San Jose)，為全球客戶提供服務。如需詳細資訊，請造訪 A10networks.com 並在 A10Networks 關注我們。

深入瞭解

關於 A10 Networks

聯絡我們
apac@a10networks.com

A10 Networks

www.a10networks.com

©2024 A10 Networks, Inc. 保留所有權利。A10 Networks、A10 Networks 標誌、ACOS、Thunder、Harmony 和 SSL Insight 是 A10 Networks, Inc. 在美國和其他國家/地區的商標或註冊商標。所有其他商標均為其各自所有者的財產。A10 Networks 對本文件中的任何不精確處不承擔任何責任。A10 Networks 保留變更、修改、轉讓或以其他方式修訂本出版品的權利，恕不另行通知。有關商標的完整清單，請造訪：A10networks.com/a10trademarks。

A10-BR-20114-TW-04 NOV 2024

請按讚並追蹤 A10 facebook粉絲專頁