A10

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

橫跨多雲或混合雲的
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

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 的安全應用程式服務解決方案組合，旨在加速及保護全球最重要的企業及服務供應商網路。

A10 Networks 透過以下方式致力於協助客戶取得更好的業務成果：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；協助服務供應商確保其網路安全並擴展能力，向服務不足的社群提供更廣泛的服務。

為了鞏固網路與應用程式的安全性與恢復能力，客戶需要考慮零信任、使用者體驗、自動化，以及採用新技術所伴隨的商機和需求。

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 平台 — 業界最精良的可擴充平台

AI 驅動的分析、見解和自動化

A10 基礎架構		A10 Defend	
應用程式情報及監控服務		威脅情報及監控服務	
AI 推論及 LLM 效能	全域伺服器負載平衡	針對 AI 相關威脅的防護	
保留和保護 IPv4 及 IPv6 位址	狀態感知防火牆	機器人防護	API 防護
SSL 卸載、快取及壓縮	安全且可擴充的 DNS	DDoS 防護	網路應用程式防火牆

AI 就緒作業系統

我們提供安全、高度可用的關鍵任務網路，協助企業邁向成功。

A10 Networks 致力於協助客戶，確保其服務持續提供最安全且永遠連線的數位體驗。

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。眾多透過網路推動事業的客戶都肯定 A10 Networks 的表現，而我們始終致力提供物超所值的尖端技術。

A10 重點業務領域

滿足未來需求的基礎架構

- 內部部署
- 私有雲
- 公有雲

網路安全

- 以主動式網路安全保護關鍵服務

AI

- 防禦生成式 AI 帶來的威脅
- 防禦 AI 驅動的威脅
- AI 偵測即將發生的故障跡象，並建議因應對策

A10 提供的解決方案

A10 Control 詳細資訊請見 ▶ 第 6 頁

DDoS 防護

- DDoS 緩解
- DDoS 偵測
- 威脅情報

詳細資訊請見 ▶ 第 9 頁

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

詳細資訊請見 ▶ 第 11 頁

頻寬控制/公平性控制

- DPI
- 公平性控制

詳細資訊請見 ▶ 第 13 頁

代理

- 安全網路閘道
- SSL/TLS 可視化

詳細資訊請見 ▶ 第 14 頁

IPv6 過渡和 IPv4 耗盡措施

- 電信級 NAT (CGNAT)
- IPv6 遷移技術

詳細資訊請見 ▶ 第 15 頁

本地分流/雲端存取代理

- 流量分配
- 租戶控制

詳細資訊請見 ▶ 第 17 頁

ACOS (先進核心作業系統) 詳細資訊請見 ▶ 第 4 頁

卓越導入實績

A10 Networks 產品廣獲全球各行各業 7,700 多家頂尖公司採用，我們擁有豐富實作經驗，尤其熟悉各種需要高可靠性、恢復能力和可用性的系統，特別適合網路內容供應商、服務供應商等組織。(以日本為例 ，採用A10產品的客戶舉例如下，未以特定順序排列)

電信業者

KDDI Corporation
SoftBank Group Corp.
石川電腦中心 (Ishikawa Computer Center)
KCT Co., Ltd.
Wire and Wireless Co. Ltd
Himawari Network
Nihon Network Service Co., Ltd.
CableNet Suzuka Co., Ltd
NTT Plala
CableTv Co., Ltd.

資料中心

IDC Frontier
Bit-isle Equinix Inc.
NTT DATA Corporation
SAKURA Internet Inc.
Fujitsu Asia Pte Ltd
Link, Inc.
ODK Solutions Company, Ltd.
NEC Corporation
CLARA, Inc.
SCSK Corporation
Synergy Co., Ltd.

教育

福岡大學 (Fukuoka University)
琉球大學 (University of the Ryukyus)
群馬大學 (Gunma University)
京都產業大學 (Kyoto Sangyo University)
東京造形大學 (Tokyo Zokei University)
京都工藝纖維大學 (Kyoto Institute of Technology)

入口網站

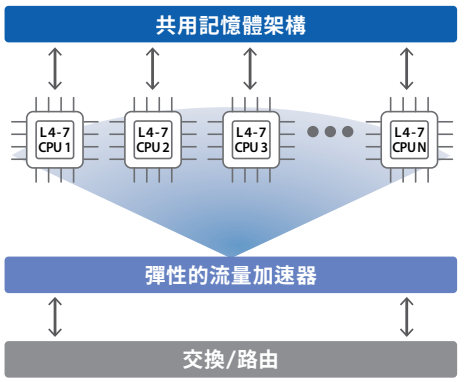
Yahoo Japan Corporation
Excite Japan Co., Ltd.

IT 服務

ITOCHU Techno-Solutions Corporation
Mitsui Knowledge Industry Co., Ltd.

我們專有的作業系統 ACOS (先進核心作業系統) 支援 Thunder 系列展現優異效能。

ACOS 平台



Thunder 系列透過 A10 Networks 專有的 ACOS 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**

多元部署型態

ACOS 能以多種部署形態提供相同功能，進而降低使用者的部署成本、學習成本與營運成本。

請參閱產品系列平台相容性列表

CLI/GUI/rest API 等介面共通的操作與管理體驗

虛擬	裸機	容器	雲端	設備
獨立執行個體	**最佳效能**	**雲端原生**	**雲端執行個體**	**高效能**
• KVM • VMware ESXi		• Docker	• AWS • Google Cloud • Microsoft Azure • Oracle Cloud	

授權結構

A10 產品授權提供各種授權方案，可因應使用者未來業務發展需求。其中包含各種不同的授權類型，包括可降低執行成本的「單次購買」授權、可降低初始成本的「訂閱型授權」、可於相同硬體切換模型並支援頻寬的「模組化授權」，以及可依據需求從頻寬池取用頻寬的「頻寬池授權」(Bandwidth pool license)。

單次購買型	訂閱型	頻寬池型	模組化型
vThunder	vThunder	FlexPool 10Gbps vThunder 裸機 Thunder Cloud Thunder Containers	硬體 軟體 ADC CGN CFW TPS 頻寬 10 Gbps、25 Gbps 等

以日本為例 ，採用A10產品的客戶舉例如下：

金融

Simplex Inc.
Hoken Minaoshi Hompo, Inc.

服務供應商/媒體

CyberAgent Inc.
ValueCommerce Co., Ltd.
DMM.com Lab Co., Ltd.
TV TOKYO Communications Corporation
GMO Internet Group, Inc.
Shochiku Co., Ltd.
IT Core Co., Ltd.

遊戲/內容經銷

SEGA Corporation
GameOn Co., Ltd.
Square Enix Co., Ltd.
DWANGO Co., Ltd.

製造

Casio Computer Co., Ltd.
DIGI Group
Shimizu Corporation

日本政府及市政當局

名古屋市
大分縣
長崎縣
山口縣
鹿兒島市
岐阜市
由利本莊市
足利市
八代市
日野市
舞鶴市
三原市
北本市
輪島市
甲州市
石門區
竹原市
有田市
高濱町
竹富町
十津川村
鳥取市
南阿爾卑斯市

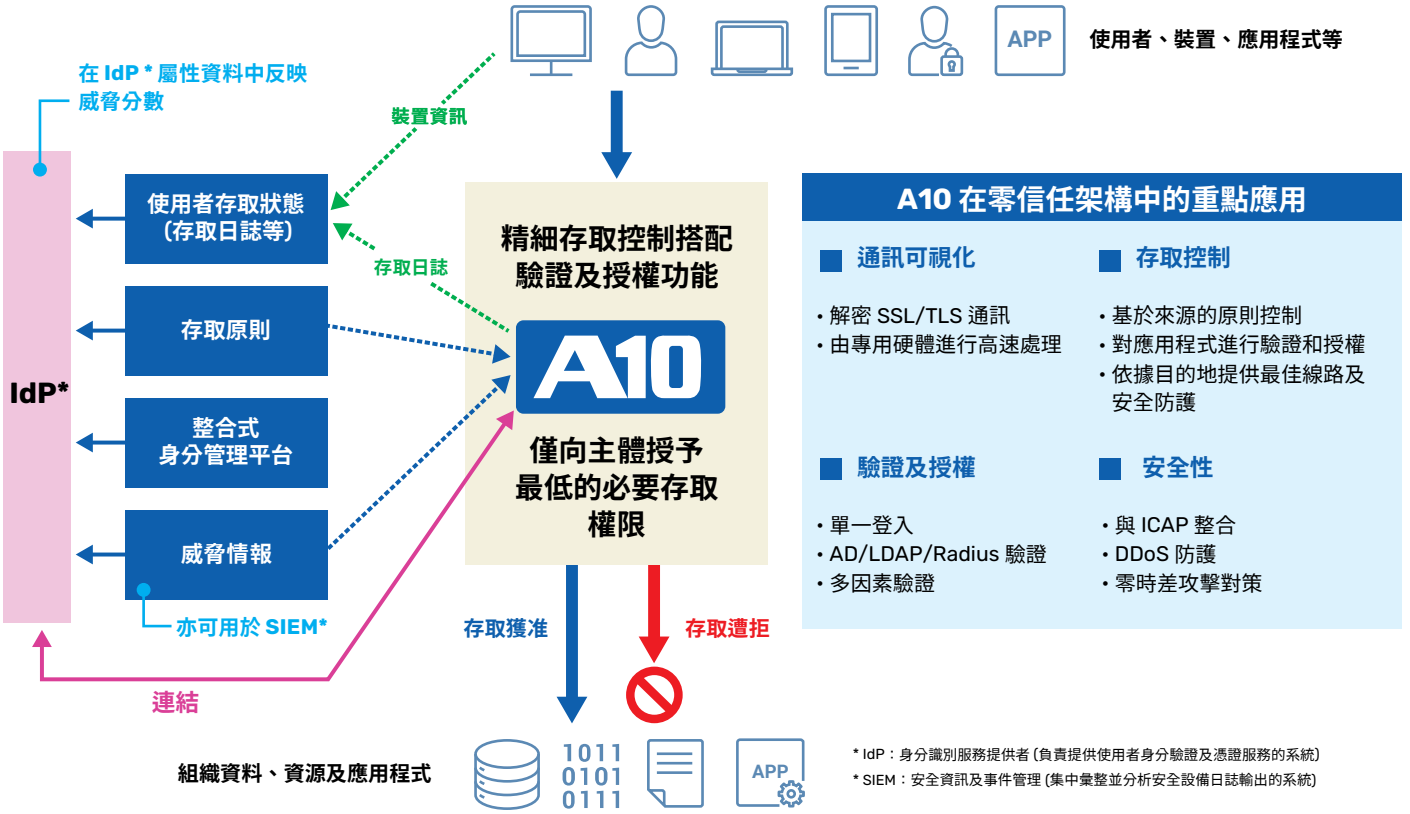
截至 2025 年 6 月

A10 零信任解決方案

混合型環境的零信任解決方案

請至官網
確認詳情

數位科技飛快進展，單憑傳統的邊界安全模型，已不足以抵禦現今的網路威脅，此時「零信任安全性」的概念便應運而生。
許多企業嘗試採用 SASE 與 SSE 達成此目標，但這類方法僅將「邊界防禦」推入雲端，未能充分發揮「零信任」的真正作用。零信任是一整套安全策略，無法仰賴單一解決方案而奏效，企業必須宏觀審視整體安全，並妥善整合既有基礎架構與新的方法對策。
A10 Networks 提供全方位網路解決方案，能夠實現完整的零信任架構。



A10 在零信任架構中的重點應用

通訊可視化
- 解密 SSL/TLS 通訊
- 由專用硬體進行高速處理

存取控制
- 基於來源的原則控制
- 對應用程式進行驗證和授權
- 依據目的地提供最佳線路及安全防護

驗證及授權
- 單一登入
- AD/LDAP/Radius 驗證
- 多因素驗證

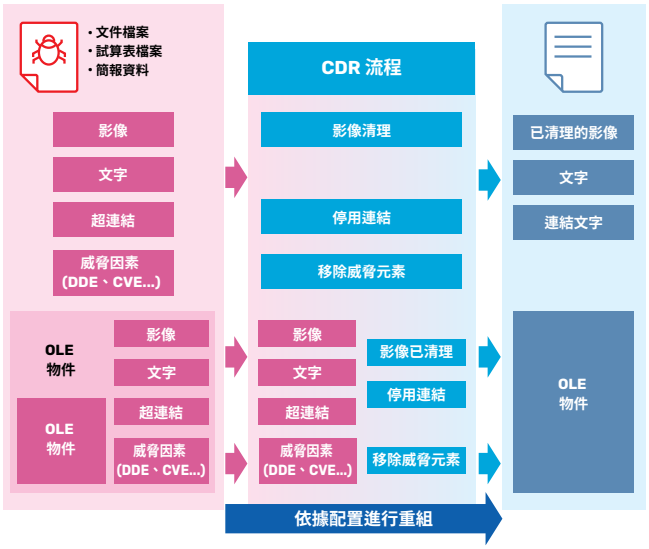
安全性
- 與 ICAP 整合
- DDoS 防護
- 零時差攻擊對策

* IdP：身分識別服務提供者 (負責提供使用者身分驗證及憑證服務的系統)
* SIEM：安全資訊及事件管理 (集中彙整並分析安全設備日誌輸出的系統)

可視化加密流量以消除威脅

內容威脅解除和重組 (CDR) 解決方案

請至官網
確認詳情



A10 的 SSL 可視性技術搭配 OPSWAT 的檔案清理技術 (MetaDefender)，可移除檔案中潛在的威脅 (如惡意軟體) 並進行重構，確保以原始檔案格式安全地使用。
使用 A10 高速 SSL/TLS 可視化技術，即使是加密檔案仍可安全檢視內容。

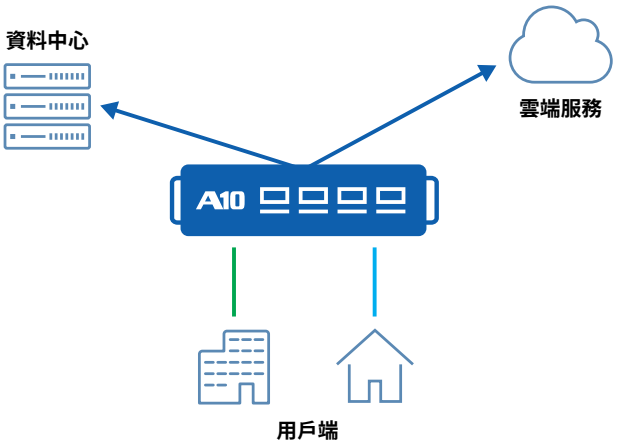
SSL 可視化：由專用硬體對加密通訊進行高速解密和重新加密。
深度 CDR：清理內容但不改變檔案格式

- 支援超過 180 種常用檔案格式 (MS-Excel、Word 等)
- 移除各種規避偵測的惡意軟體、已知與未知威脅
- 應對電子檔案中潛伏的各種威脅，例如敏感資訊及檔案漏洞

高效智慧的網路解決方案，讓您舒適、安全使用雲端服務

本地分流 (雲端存取代理)

請至官網
確認詳情

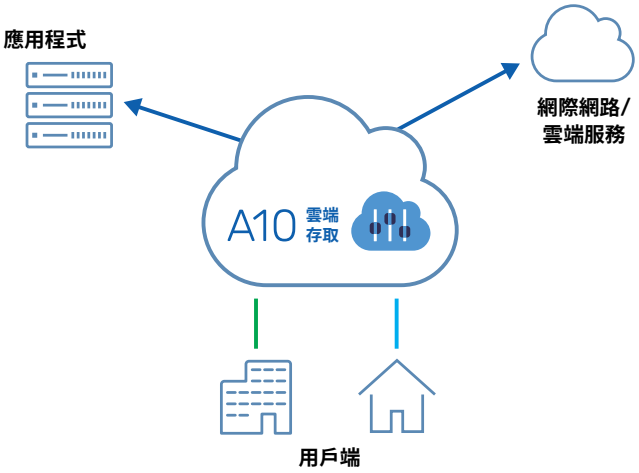


這款解決方案能自動判別通訊是否連向特定雲端服務，以允許各據點或遠端辦公室直接存取網際網路，而無需經由總部或資料中心。
進而減輕網路代理伺服器負載，有效因應雲端服務用量遽增趨勢；同時支援精準存取控制，例如僅允許地方政府、醫療機構與金融機構等封閉網路的通訊連往特定目的地。

- 可依目的地網域名稱準確卸載
- 可搭配 Microsoft 365、Google Workspace 等主流雲端服務
- 可封鎖個人帳戶的使用
- 可支援超過 10 萬個用戶端的高效能
- 在日本已有數百家企業成功導入

A10 雲端服務可妥善控管應用程式和網際網路的存取權限

雲端存取控制器*



雲端存取控制器 (Cloud Access Controller) 是一項雲端服務，能讓您根據組織的安全原則，控制並管理個別使用者對應用程式與網際網路的通訊。
此服務亦可整合內部部署 的 A10 Thunder 系列，在混合式架構的配置下，提供一致性的安全原則。

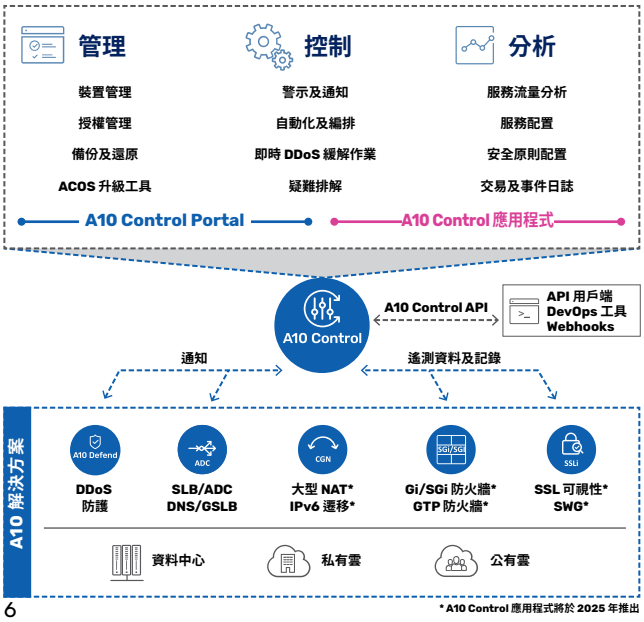
- 透過驗證/授權功能，控制各使用者的存取權限
- 依據連線來源及目的地進行適當的流量分類
- 同時控制應用程式特定通訊與外部通訊
- 提供 URL 篩選等各種安全功能
- 可透過安全 IPSec 協定使用 VPN 功能
- 易於部署的 SaaS 型服務
- 提供日誌記錄，以利監控存取活動

* A10 雲端存取控制器目前僅於日本國內供應使用。

A10 產品的集中化管理與流量可視化

A10 Control

請至官網
確認詳情



A10 Control 是 A10 解決方案新一代的統一化管理及分析平台，可集中管理分散在各環境的 A10 產品，包括內部部署、雲端及混合環境，且能可視化並分析應用程式及服務流量，有助於迅速規劃容量和調整規模，進而提升作業效率和安全性。

- 集中管理分散在多個位置及雲端環境的 A10 裝置，大幅減輕作業負荷
- 蒐集、分析並可視化應用程式和服務流量，簡化異常偵測及疑難排解流程

在 AI 時代保護您的網路及服務免於網路攻擊

網路攻擊日益精密複雜，新型態威脅也層出不窮，特別是利用 AI 技術的入侵手法。
面對如此情勢，如何保護自家網站，已成為企業刻不容緩的迫切課題。A10 Defend 安全解決方案提供全方位防護，不僅能抵禦針對系統與伺服器的 DDoS 攻擊，亦可防範鎖定應用程式和 API 的精密攻擊。此方案同時適用於內部部署或雲端環境，並提供全面託管的 SOC 服務。

請至官網確認詳情

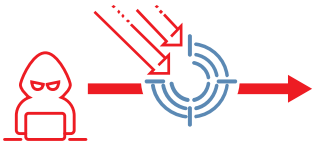
A10 Defend

Web 應用程式攻擊

AI 攻擊手法的演進

DDoS 攻擊

攻擊系統、伺服器
網路層攻擊



AI 攻擊手法的演進

A10 Defend 新一代 WAF

新一代 WAF

詳細資料請見 ▶ 第 8 頁

ThreatX by A10 Networks

WAAP/API 防護

詳細資料請見 ▶ 第 7 頁

A10 Defend Threat Control

DDoS 威脅情報

詳細資料請見 ▶ 第 9 頁

A10 Defend DDoS Mitigator

DDoS 緩解裝置

詳細資料請見 ▶ 第 9 頁

A10 Defend DDoS Detector

DDoS Detector

詳細資料請見 ▶ 第 9 頁

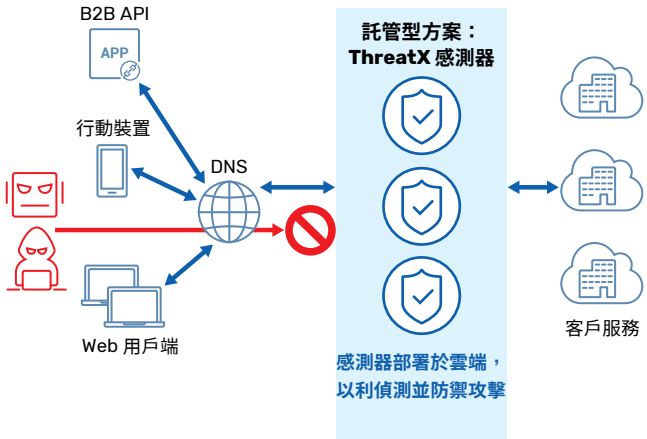
防禦目標

- WEB 應用程式
- API
- AI
- 系統/伺服器
  - DNS 伺服器
  - Web 伺服器
  - API 伺服器
  - AI 伺服器
  - 等類似目標
- 網路

雲端 WAAP 搭配全套完整的 API 防護、WAF、L7 DDoS 防護以及機器人防護功能

ThreatX by A10 Networks

請至官網確認詳情



ThreatX 是一款雲端原生的 Web 應用程式和 API 防護 (WAAP) 解決方案，能夠全面保護 Web 應用程式及 API，整合了 WAF、API 安全性、L7 DDoS 防護和機器人防護功能，並透過獨特的行為分析與風險評分機制，有效偵測並防禦精密攻擊，保護服務不受侵擾。
採用行為分析和威脅情報，可精準預防攻擊，效果優於傳統的特徵碼方法。
可依據風險評分自動封鎖，減少誤報並降低作業負載。
雲端原生架構可迅速部署於任何環境，包括雲端、內部部署及混合環境。

基於風險的自動封鎖　防護即服務

現場安裝僅需 15 分鐘

- 行為分析與風險評分的防禦機制
- 一體化安全防護
- SOC 團隊提供專業支援
- 雲端原生支援，部署迅速便捷

精準的第一層防禦，保護 Web 應用程式免於 DDoS 攻擊

A10 Defend Threat Control

請至官網確認詳情

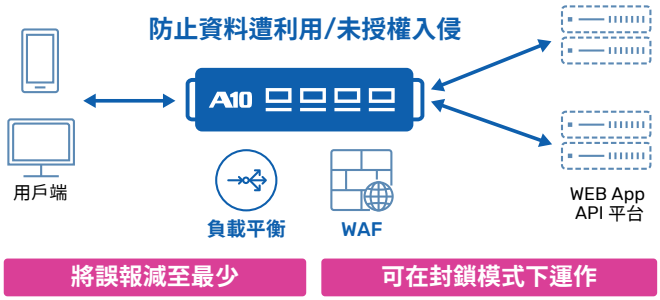
A10 Defend Threat Control 是專為 DDoS 攻擊設計的威脅情報解決方案，有助於主動防禦 DDoS 威脅。此服務由 A10 專責團隊蒐集、調查並分析資料，並以 SaaS (軟體即服務) 形式交付，能在偵測到攻擊前進行主動防禦。

- 若發現組織 IP 位址 可能捲入 DDoS 攻擊，系統會及早警示以確保安全
- 提供高度可靠的 IP 封鎖清單，可搭配既有安全裝置協同防禦
- 採用 SaaS 模型，無需使用專屬設備，有助於降低部署成本及作業負擔

新一代 WAF 具備應用程式交付功能，並可徹底減少誤報

由 Fastly 提供支援的 A10 Defend 新一代 WAF

請至官網確認詳情



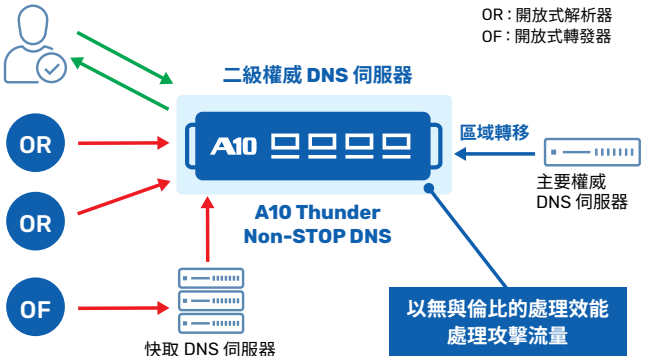
「A10 Defend 新一代 WAF，由 Fastly 提供支援」解決方案整合了 A10 的應用程式交付、負載平衡功能以及 Fastly 新一代 WAF 技術，提供虛擬機器、硬體設備等多種部署型態。此方案實用可靠，可將誤報減至最少，同時保護您的 Web 服務。

- 可在真實環境中使用全封鎖模式，大幅減少運轉負載
- 除了在雲端蒐集和分析資訊之外，亦利用先進技術徹底減少誤報
- 同時也供應 TLS 卸載及 DDoS 防護等功能

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

請至官網確認詳情



Non-Stop DNS 是 A10 Defend DDoS Mitigator 提供的功能，可用作大容量的二級權威 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。

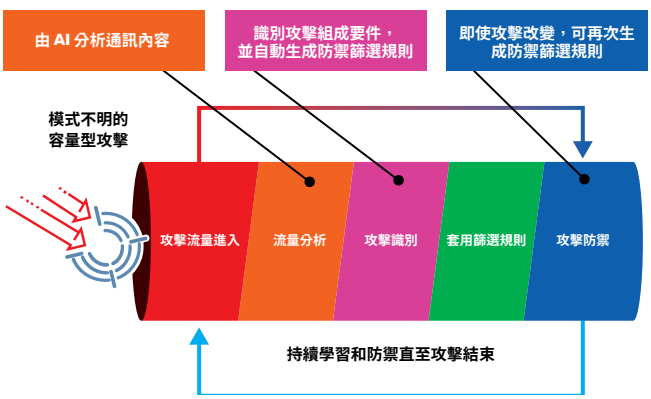
在現有權威 DNS 伺服器前面導入 Non-STOP DNS
無與倫比的 DNS 處理效能，正常的 DNS 服務即使受到攻擊也能繼續正常運作

Non-STOP DNS 回應來自用戶端的所有 DNS 查詢
現有權威 DNS 伺服器將作為主要權威 DNS 伺服器運作，用於管理區域資訊 (隱藏主要 DNS 配置)

可自動生成篩選規則，抵禦 AI 強化的巨流量攻擊 (volumetric attack)

ZAPR (零時差攻擊模式識別)

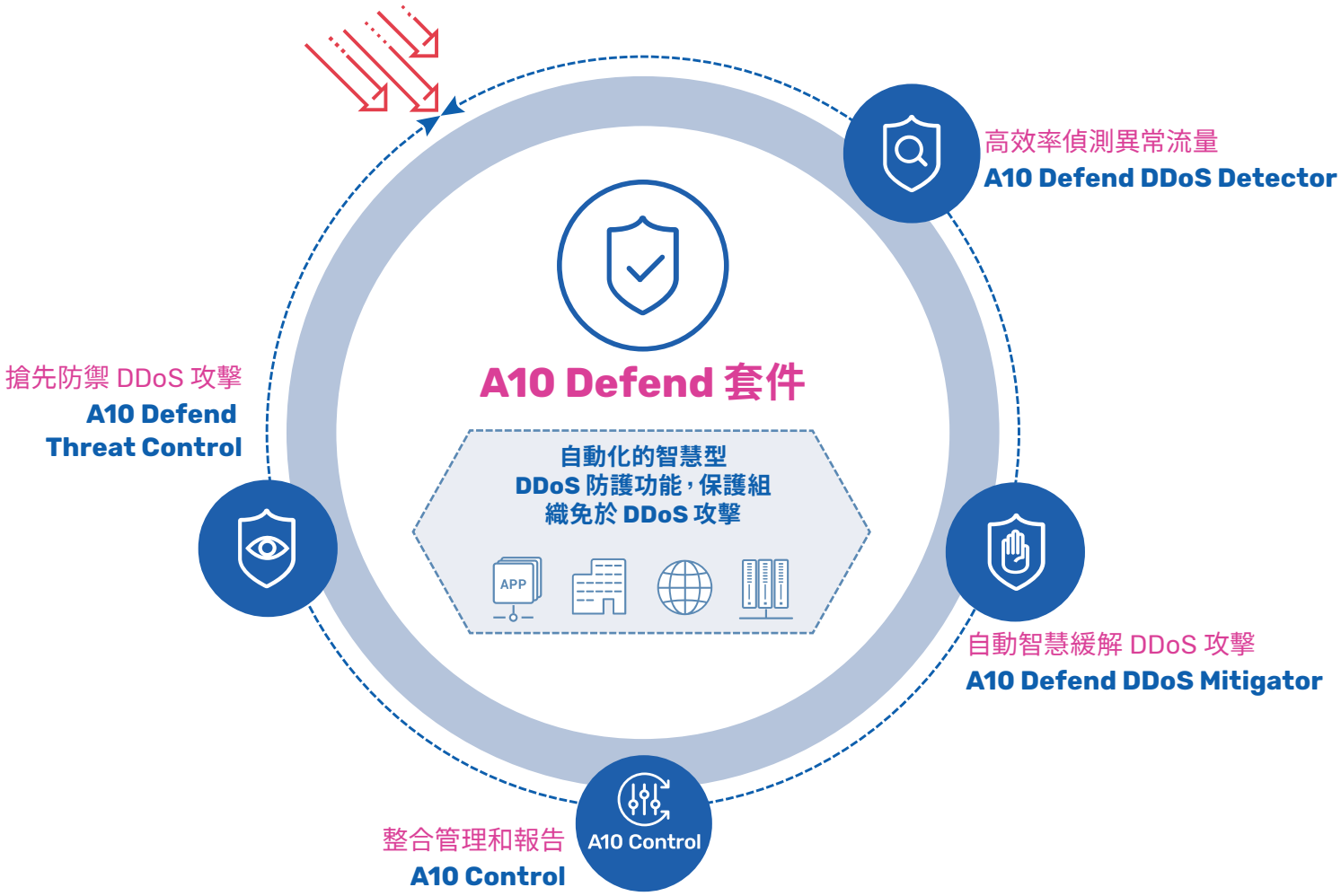
請至官網確認詳情

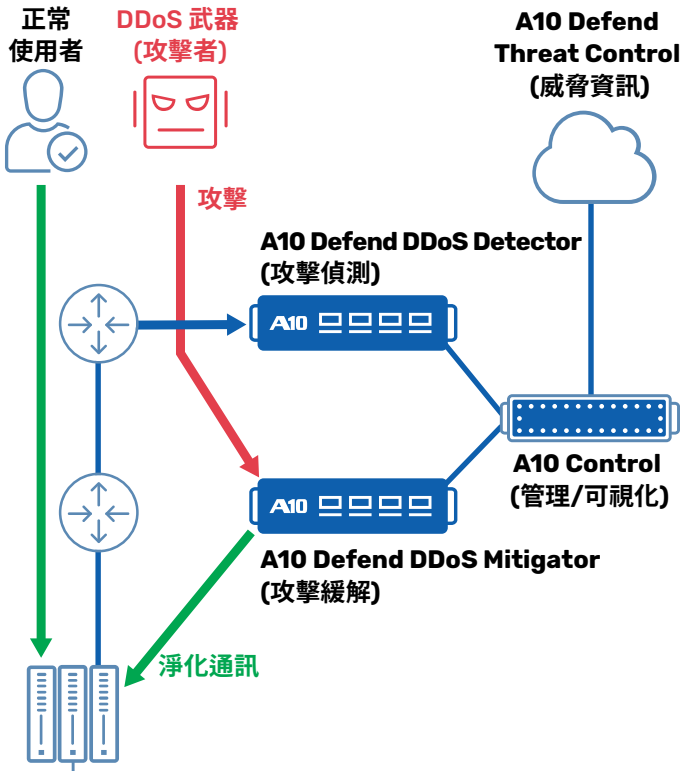


零時差攻擊模式識別 (ZAPR) 引擎利用機器學習技術，自動識別 DDoS 攻擊特性，並動態套用緩解篩選規則。

- 迅速、自動因應零時差攻擊和新型攻擊模式
- 無需進階的預先配置或手動介入
- 更精準緩解攻擊威脅

A10 Defend DDoS 套件：整合式 DDoS 攻擊防護解決方案





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。
此方案利用 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 DDoS Mitigator:
緩解 DDoS 攻擊並防止服務中斷

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

A10 Control:
使用 Detector 和 Mitigator 集中管理 DDoS 攻擊偵測和緩解
Mitigator 可搭配 Detector 提供詳細的攻擊報告和分析

A10 Defend Threat Control:
監控並分析 DDoS 攻擊對策
A10 專責團隊 24 小時待命支援，抵禦攻擊全年無休
提供日誌的儲存、分析及報告功能，並可共享威脅資訊

A10 解決方案的效益

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

如果發生容量型攻擊，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。

從容應對任何 DDoS 攻擊

不僅保護網路免受容量型攻擊，同時也抵禦來自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 (Inline) 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 種常見的攻擊模式，結合專有作業系統，針對多核心處理架構進行最佳化，可實現高達 5 億 pps 的防禦效能。

多種交付格式

可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 2025 年 6 月

緩解裝置：A10 Defend DDoS Mitigator

~ 10 Gbps	10 G ~ 100 Gbps	100 Gbps ~
模組化授權 **Thunder 1060S** **5 G、10 G、20 Gbps** 7x1GC、4x1/10GF、2x10/25GF	SPE 型號 **Thunder 5845** **100 Gbps** 48x1/10GF、4x100GF	SPE 型號 **Thunder 8665S** **550 Gbps** 12 x 400GF
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 Gbp** 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		

管理軟體

A10 Control 內建的
A10 Defend DDoS Orchestrator

Detector

A10 Defend DDoS Detector
Thunder 3350-E、5845、7445
獨立式 Detector
100 萬 – 600 萬 fps

A10 Defend DDoS Detector VA
獨立式 Detector
15 萬 – 150 萬 fps

*SPE 型號：配備 SPE (安全和原則引擎) 的型號，這是一種加速應用安全原則的硬體元件。*VA：虛擬設備
*模組化授權：此模式對軟體與硬體分別授權，即使硬體相同，授權涵蓋範圍仍依頻寬及其他規格而有所區分。

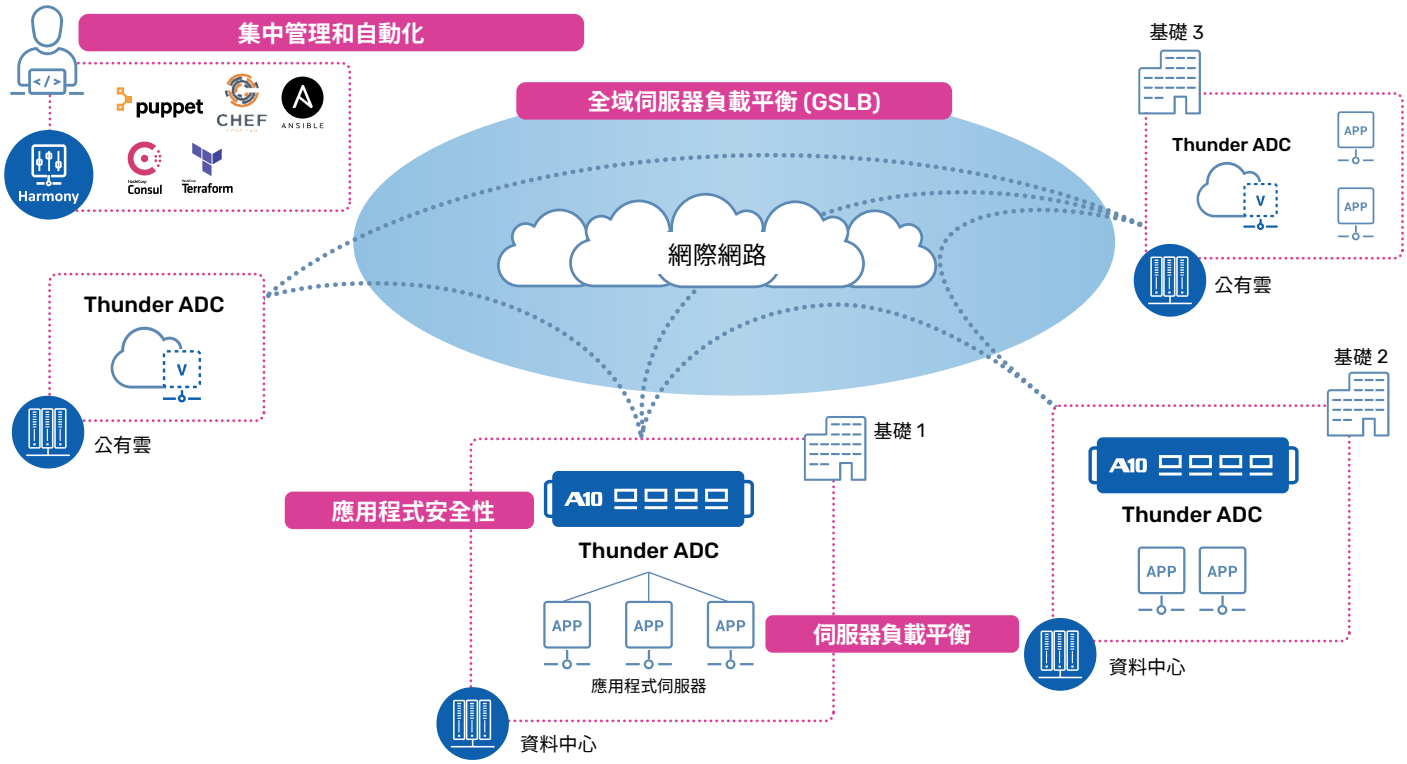
如需最新資訊或更多詳情，
請造訪右側的網頁。

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)
- 橫跨全球站點的高可用性
- 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 防禦

備援/叢集
- VRRP-a
- aVCS
- 橫向擴充

集中管理和自動化
- 集中原則執行
- 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 解決方案的效益

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)
- 防禦對抗 DDoS 攻擊
- Web 應用程式防火牆 (WAF)

應用程式可視性
- 整合 A10 Control，各項應用程式交付狀態一目瞭然
- 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

- 可自訂原則和角色型存取控制 (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、裸機和容器等型態進行部署
- 使用 FlexPool 實現跨多雲的授權可移植性

加速應用程式效能

- 透過快取與 TCP 最佳化技術，加快內容傳輸速度
- 具備 TLS/SSL 卸載功能，支援最新 ECC 加密

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

- 整合 A10 Control，全面可視化各項使用者體驗、流量概況、運作狀況檢查以及效能監控資訊

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 及 Ansible 等自動化工具整合到 CI/CD 管道中

自動服務偵測

- 使用第三方工具 (例如 Thunder Kubernetes Connector (TKC) 或含 Consul 的 HashiCorp NIA) 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 2025 年 6 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	模組化授權 **Thunder 1060S** **25 Gbps** 7x1GC、4x1/10GF、2x10/25GF	**Thunder 4440** **78 Gbps** 24x1/10GF、4x40GF	**Thunder 6440** **150 Gbps** 48x1/10GF、4x40GF	SPE 型號 **Thunder 7655S** **370 Gbps** 16x100GF	**Thunder 3745** 4 x 10GE
vThunder ADC **虛擬設備** 最高 100 Gbps	模組化授權 **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 **容器版 (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	SPE 型號 **Thunder 6655S** **185 Gbps** 16x100GF		
裸機 Thunder ADC					

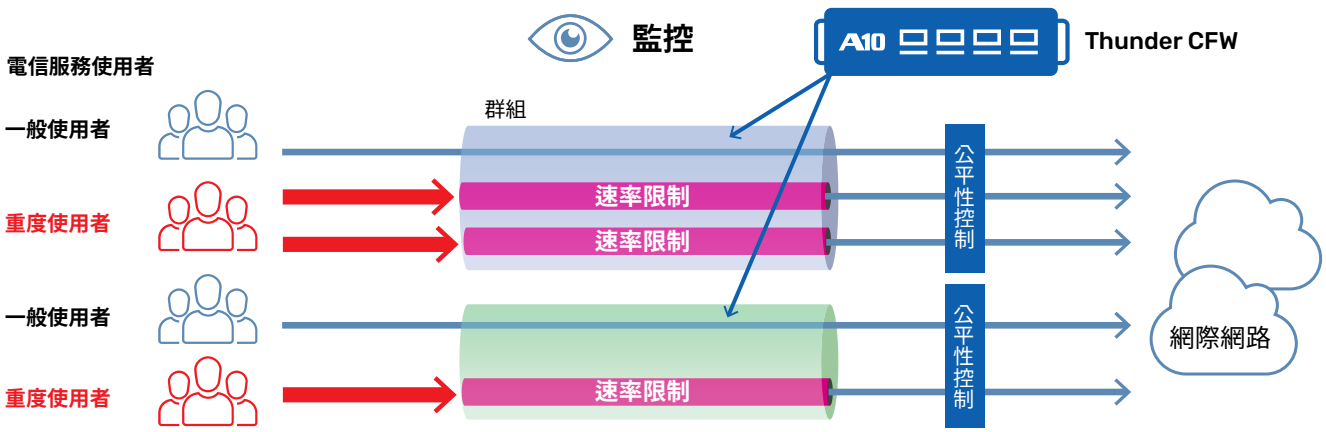
* SPE 型號：配備 SPE (安全和原則引擎) 的型號，這是一種加速應用安全原則的硬體功能
* 模組化授權：此模式對軟體與硬體分別授權，即使硬體相同，授權涵蓋範圍仍依頻寬及其他規格而有所區分。

如需最新資訊或更多詳情，
請造訪右側的網頁。

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，確保通訊頻寬公平、有效的使用。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 解決方案的效益

分級公平性控制

在流量高峰期間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電信服務訂戶的滿意度。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、線路平衡、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 2025 年 6 月

虛擬設備

雲端 vThunder CFW

vThunder 虛擬設備

Thunder 容器版 (Docker)

裸機

Thunder 裸機版

~ 100 Gbps*	~ 200 Gbps*	200 Gbps* ~
Thunder 4440S 24x1/10GF、4x40GF	**Thunder 7440** 48x1/10GF、4x40GF **Thunder 7440-11** 48x1/10GF、4x100GF	**Thunder 8665S** 12 x 400GF
Thunder 5840 24x1/10GF、4x40GF **Thunder 5840-11** 24x1/10GF、4x100GF		**Thunder 7655S** 16x100GF
Thunder 3350S 6x1GC、2x1GF、8x1/10GF、4x10GF	**Thunder 6440S** 48x1/10GF、4x40GF	**Thunder 7650** 16x100GF
Thunder 5440 24x1/10GF、4x40GF		

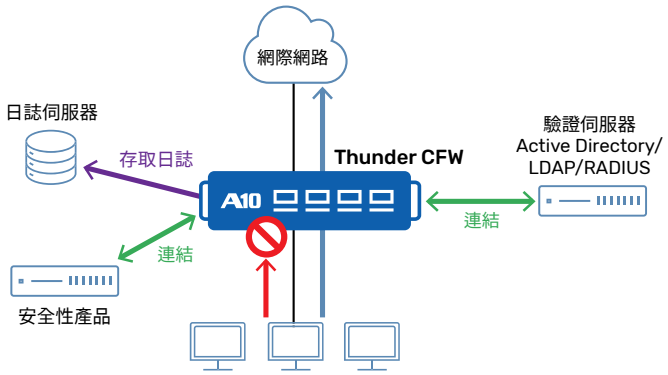
* 公平控制所需的近似處理量

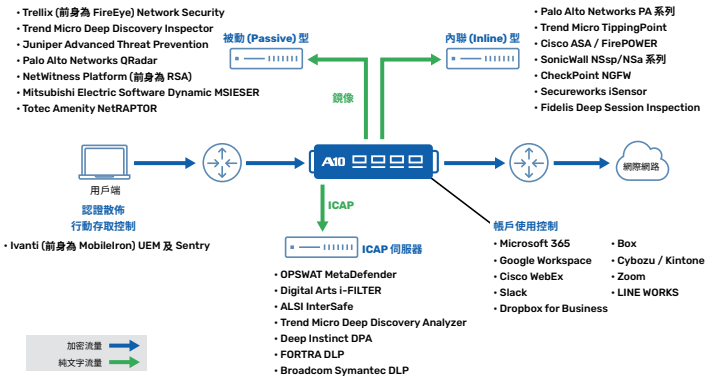
如需最新資訊或更多詳情，請造訪右側的網頁。

解決方案資訊

Data Sheet

代理





A10 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通訊控制。

除了代理功能以外，亦提供其他進階防護，包括「多重掃描」，透過多款反惡意軟體引擎改善偵測率；「內容解毒」用於抵禦零時差攻擊；而「資料遺失防護」則可避免機密資訊外洩。

A10 解決方案的效益

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 2025 年 6 月

~ 5,000 個用戶端	~ 20,000 個用戶端	~ 50,000 個用戶端	超過 50,000 個用戶端
模組化授權 **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 6440S 22 Gbps* 48x1/10GF、4x40GF
模組化授權 **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
		Thunder 3350S 5.5 Gbps* 6x1GC、2x1/10GF、8x1/10GF、4x10GF	**Thunder 5840S** 25 Gbps* 24x1/10GF、4x40GF **Thunder 5840S-11** 25 Gbps* 24x1/10GF、4x100GF

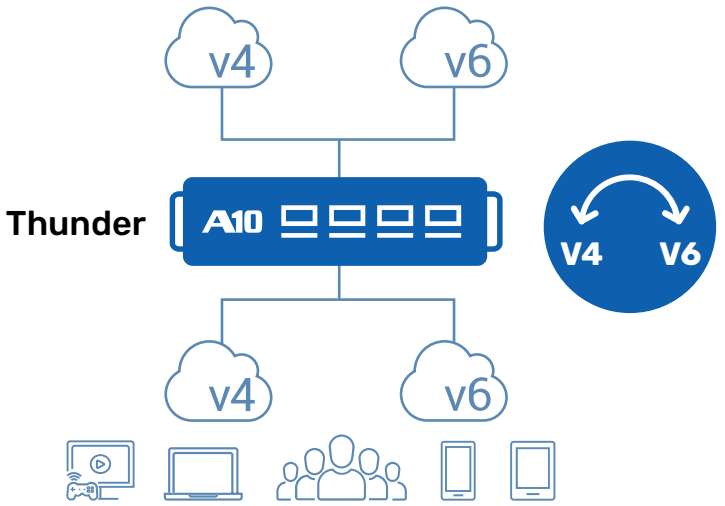
* 所有通訊均以 SSL/TLS 可視化處理時的最大處理量 * 模組化：模組化授權。此模式對軟體與硬體分別授權，即使硬體相同，授權涵蓋範圍仍依頻寬及其他規格而有所區分。

如需最新資訊或更多詳情，請造訪右側的網頁。

解決方案資訊

Data Sheet

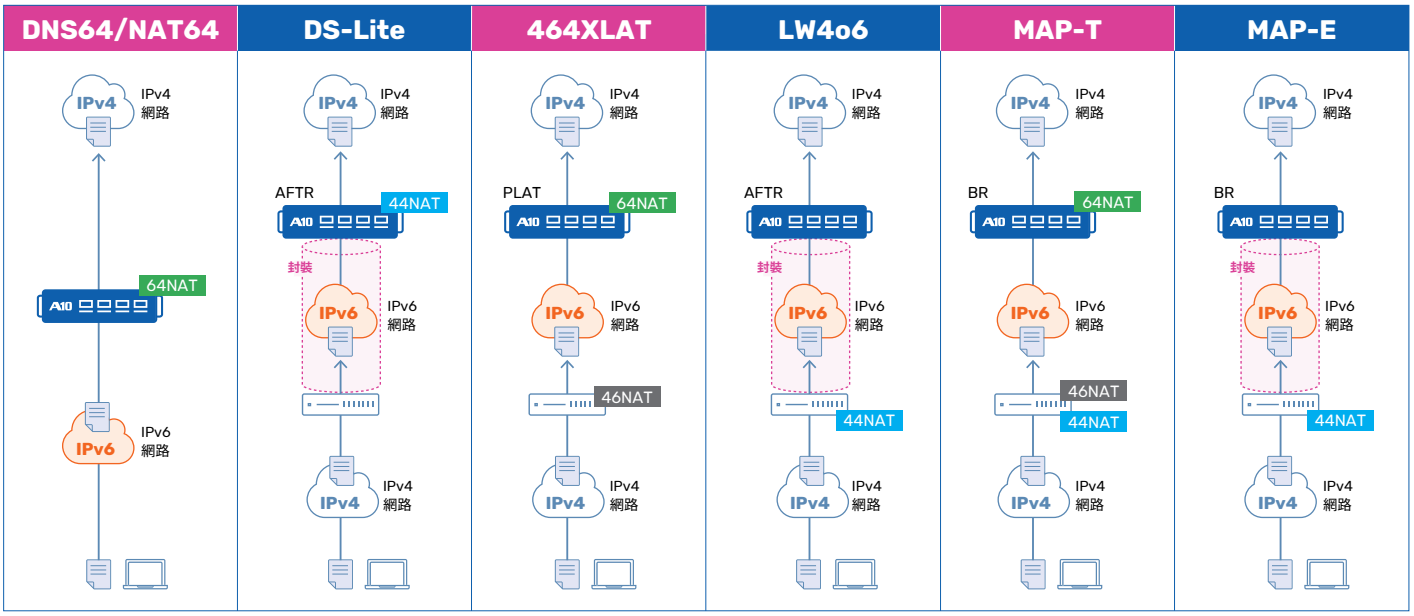
IPv6 過渡和 IPv4 耗盡措施



電信級 NAT IPv4 耗盡措施

IPv4 – IPv6 轉換

IPv4 和 IPv6 平台上均可進行通訊



A10 的 IPv4 耗盡對策和 IPv6 過渡解決方案提供 CGNAT 功能，可讓難以取得的 IPv4 位址提升使用者容納效率來延長服務壽命，並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 過渡技術是高度可靠的解決方案，十多年來商用實績卓越，廣受國內外眾多電信業者肯定。

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

除了大容量的專用硬體產品以外，亦可搭配使用裸機軟體、虛擬軟體和容器，實現彈性配置模式，靈活共用硬體及各種基礎架構設施。

A10 解決方案的效益

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

- 不論現有基礎架構是基於 IPv4 或 IPv6 協定，皆可使用隧道和轉換功能提供兩種版本的服務

多種交付格式

- 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 2025 年 6 月

虛擬設備

vThunder 虛擬設備

Thunder CGN 容器版 (Docker)
最高 180 Gbps

裸機

裸機 Thunder CGN

~ 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

SPE 型號

Thunder 5845
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 ~

SPE 型號

Thunder 8665S
550 Gbps
12 x 400GF

SPE 型號

Thunder 7655S
370 Gbps
16x100GF

Thunder 7650
370 Gbps
16x100GF

SPE 型號

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

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

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

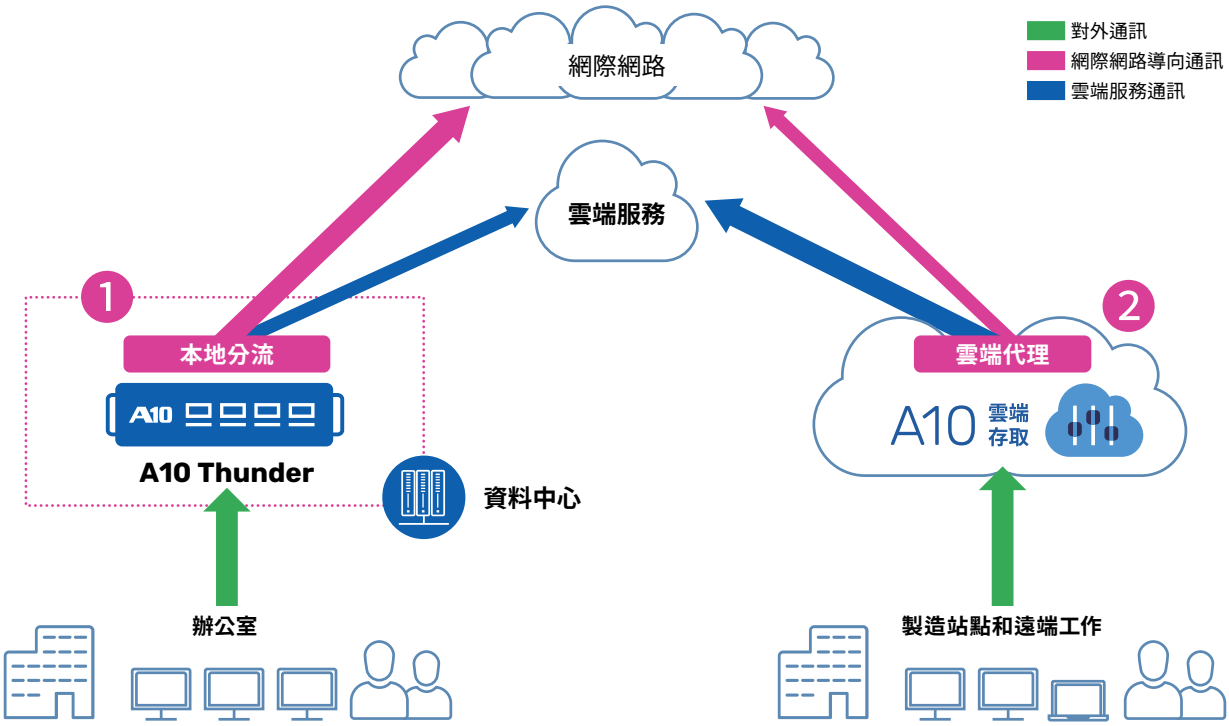
*SPE 型號：配備 SPE（安全和原則引擎）的型號，這是一種加速應用安全原則的硬體功能

如需最新資訊或更多詳情，
請造訪右側的網頁。

解決方案資訊

Data Sheet

本地分流/雲端存取代理



1 雲端存取代理

- 本地分流
- 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
- 與更高層級的 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 雲端存取控制器目前僅於日本國內供應使用。

A10 解決方案的效益

流量隔離

- 本地分流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
- 支援市政網路三層隔離

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
- 取得存取日誌

安全性

- 保護卸載後的流量
- 提供多重掃描、清理、防資料外洩等多種安全功能

如需最新資訊或更多詳情，請造訪右側的網頁。

A10 雲端存取代理卸載解決方案詳細資料

Data Sheet

主要特點

各種安全功能

- URL 篩選
- IP 信譽
- 與驗證基礎架構鏈結
- 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
- 存取日誌取得

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

- 部署 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 網域名稱

線路卸載

- 例如存取 SaaS 時會直接分配至專用 SaaS 線路，無需經過代理，而所有其他非 SaaS 通訊則分配至現有的代理伺服器
- 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 可視化功能

支援的產品

截至 2025 年 6 月

~ 5,000 個用戶端	~ 20,000 個用戶端	~ 50,000 個用戶端	超過 50,000 個用戶端
模組化授權  **Thunder 1060S 25G** **2Gbps*** 7x1GC、4x1/10GF、2x10/25GF	 **Thunder 3350** **3Gbps*** 6x1GC、2x1GF、4x25GF、4x40GF、4x10GF	 **Thunder 5440S** **15Gbps*** 24x1/10GF、4x40GF	 **Thunder 7655S** **72Gbps*** 16x100GF	 **Thunder 6440S** **22Gbps*** 48x1/10GF、4x40GF
模組化授權  **Thunder 1060S 10G** **1Gbps*** 7x1GC、4x1/10GF、2x10/25GF	 **Thunder 3350 -E** **3Gbps*** 6x1GC、2x1/10GF、8x1/10GF、4x10GF	 **Thunder 4440S** **8Gbps*** 24x1/10GF、4x40GF  **Thunder 3350S** **5.5Gbps*** 6x1GC、2x1/10GF、8x1/10GF、4x10GF	 **Thunder 7440S** **25Gbps*** 48x1/10GF、4x40GF **Thunder 7440S-11** **25Gbps*** 48x1/10GF、4x100GF	 **Thunder 5840S** **25Gbps*** 24x1/10GF、4x40GF **Thunder 5840S-11** **25Gbps*** 24x1/10GF、4x100GF

* 所有通訊均以 SSL/TLS 可視化處理時的最大處理量 * 模組化：模組化授權。此模式對軟體與硬體分別授權，即使硬體相同，授權涵蓋範圍仍依頻寬及其他規格而有所區分。

雲端存取控制器授權結構 A10 雲端存取 *

截至 2025 年 6 月

- **全面授權僅適用於基本、標準和進階授權**
  - 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：50 個用戶端)
- **期間：以年為單位 (最低合約：1 年)**
  - 免費試用：有 (1 個月)
- **存取日誌最長保留 3 個月**
  - (日誌可透過 Web API 取得)

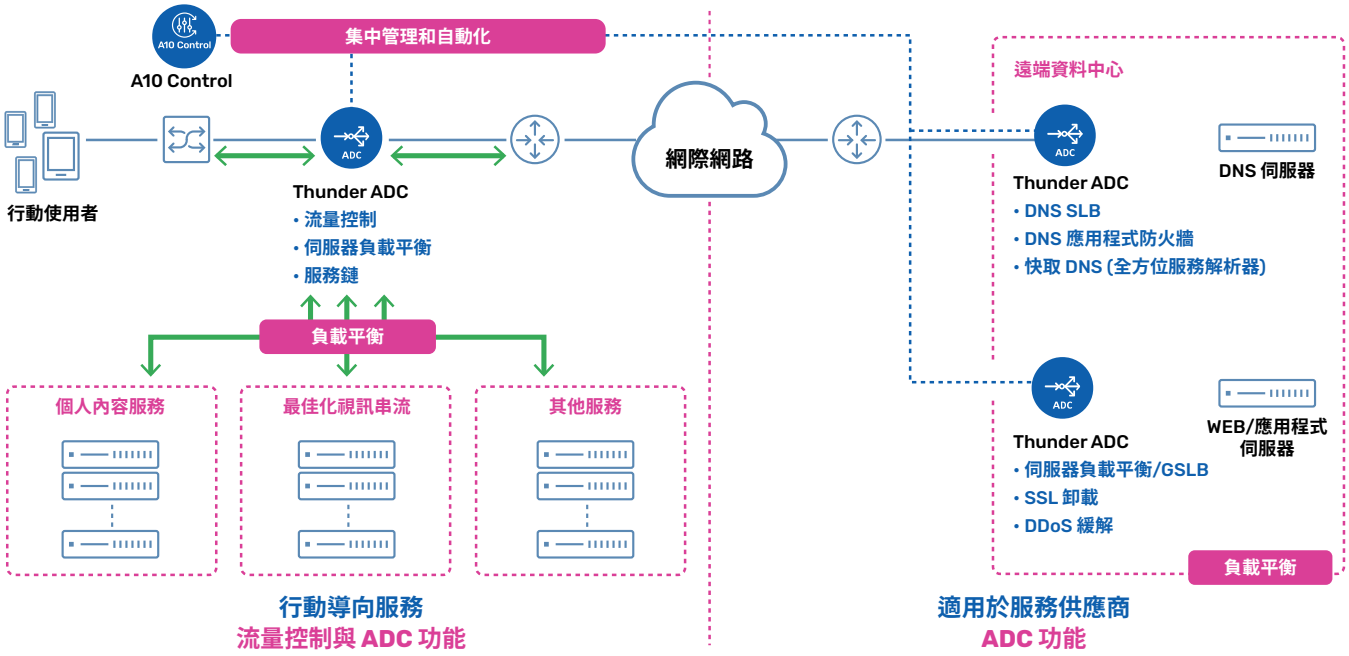
功能	授權類型			
	基本	標準	進階	其他選項
正向代理	○	○	○	
反向代理	○	○	○	
流量控制功能	○	○	○	
驗證基礎架構鏈結	○	○	○	
存取日誌儲存	○	○	○	
URL 篩選	○	○	○	
SSL/TLS 解密		○	○	○
SaaS 服務的租戶控制		○	○	○
IP 位址信譽			○	○
應用程式可視性和控制			○	○
反惡意軟體				○
內容清理				○
資料遺失防護				○
透過站台對站台 IPsec VPN 連線				○
透過用戶端對站台 IPsec VPN 連線				○

* A10 雲端存取控制器目前僅於日本國內供應使用。

案例研究

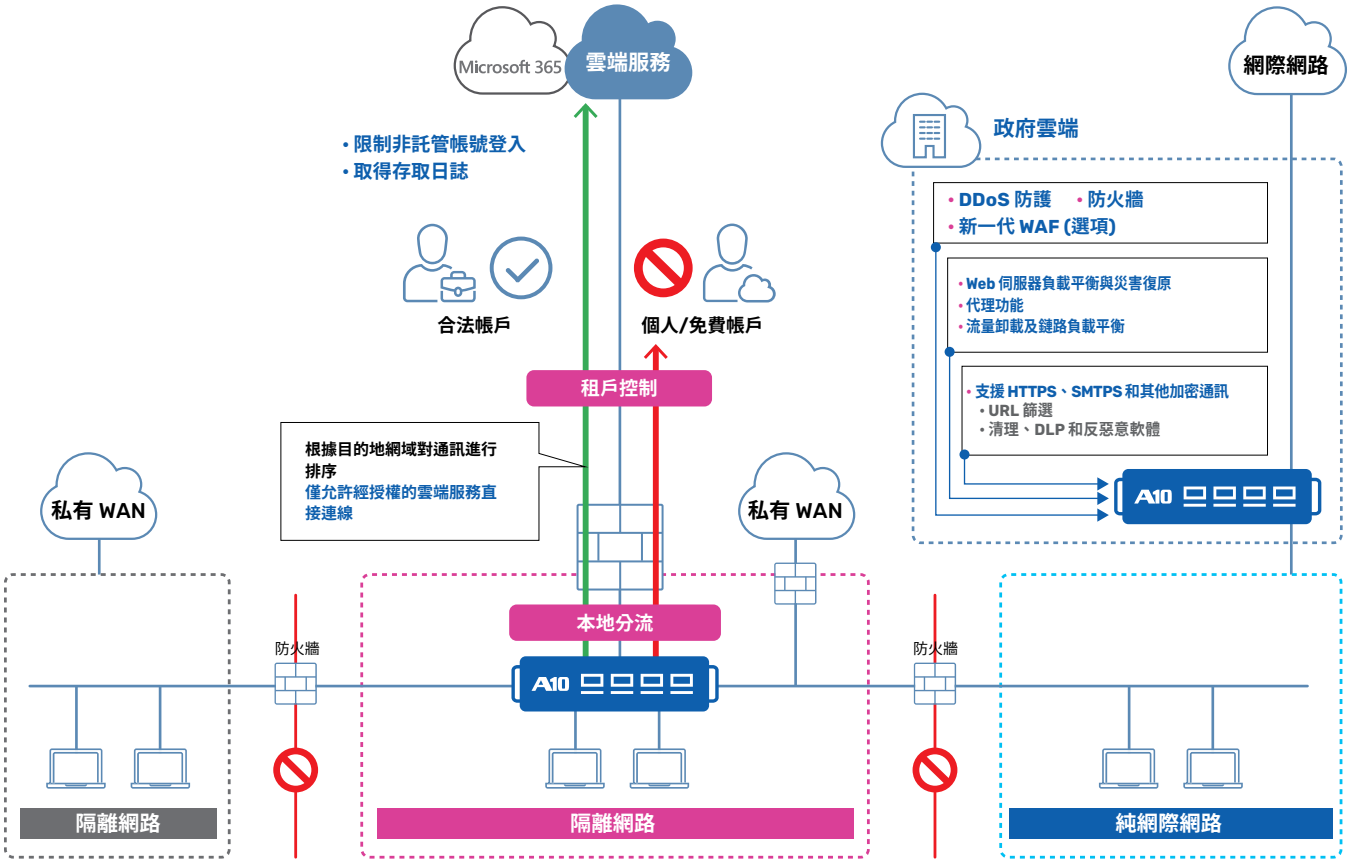
Web 供應商

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



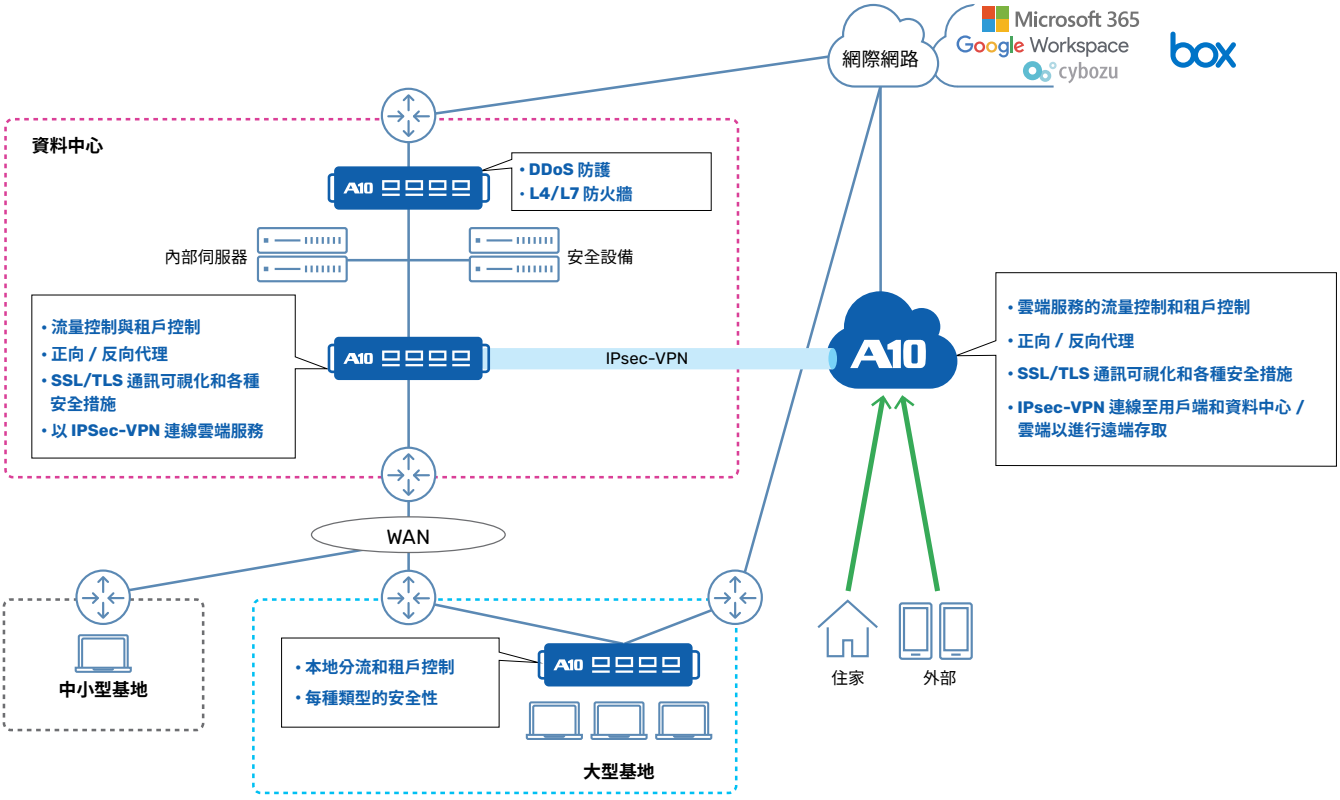
政府及醫療機構

本解決方案適用於隔離網路中的用戶端，能夠安全存取 Microsoft 365 等特定雲端服務，其透過本地分流機制自動篩選，僅將經核准的流量導向網際網路；同時內建租戶控制功能，嚴格限制個人帳號的存取行為



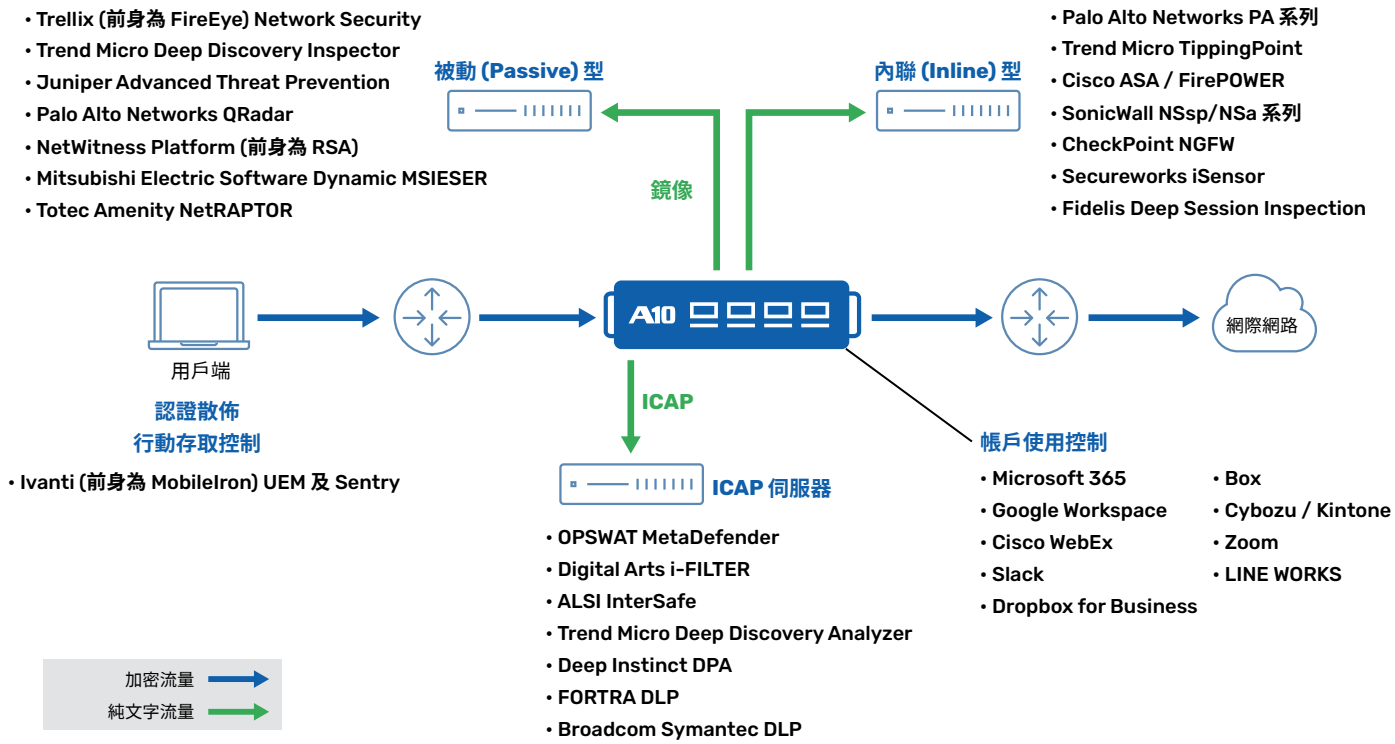
企業網路解決方案圖

最佳化通訊流量並強化每個資料中心/位置/雲點的安全性



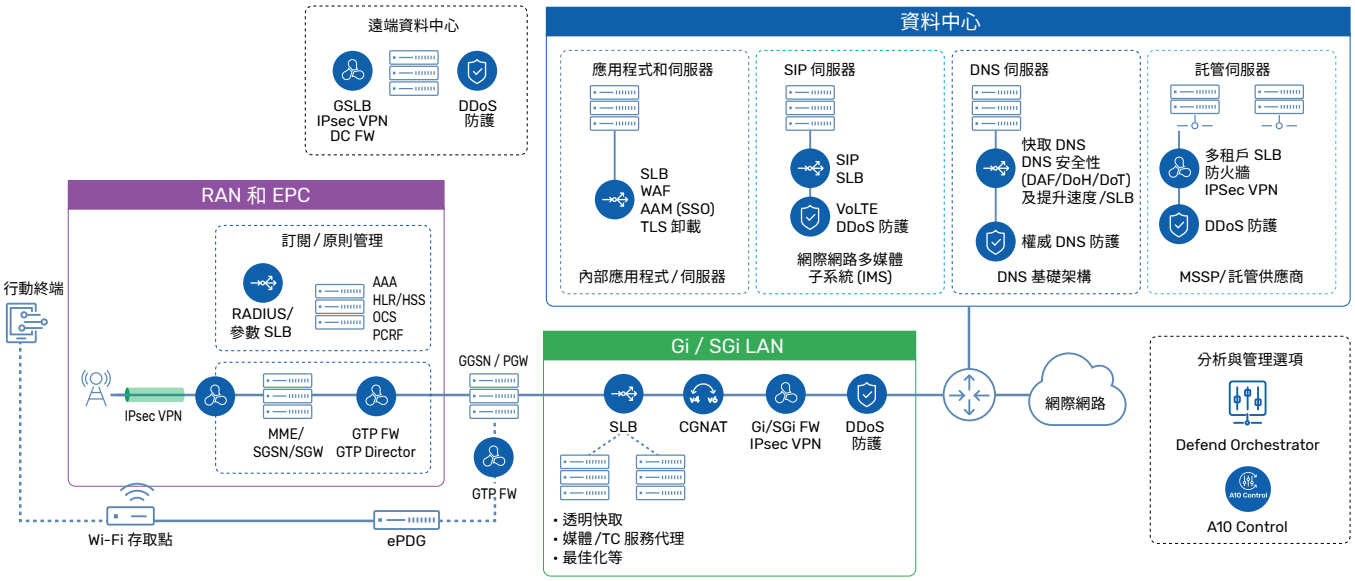
SSL/TLS 通訊可視化與整合式解決方案

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

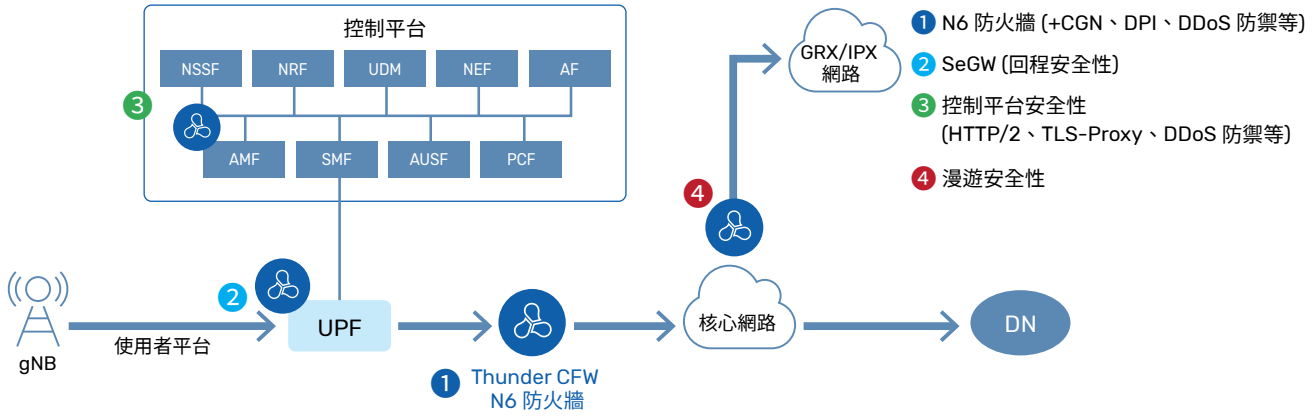


案例研究

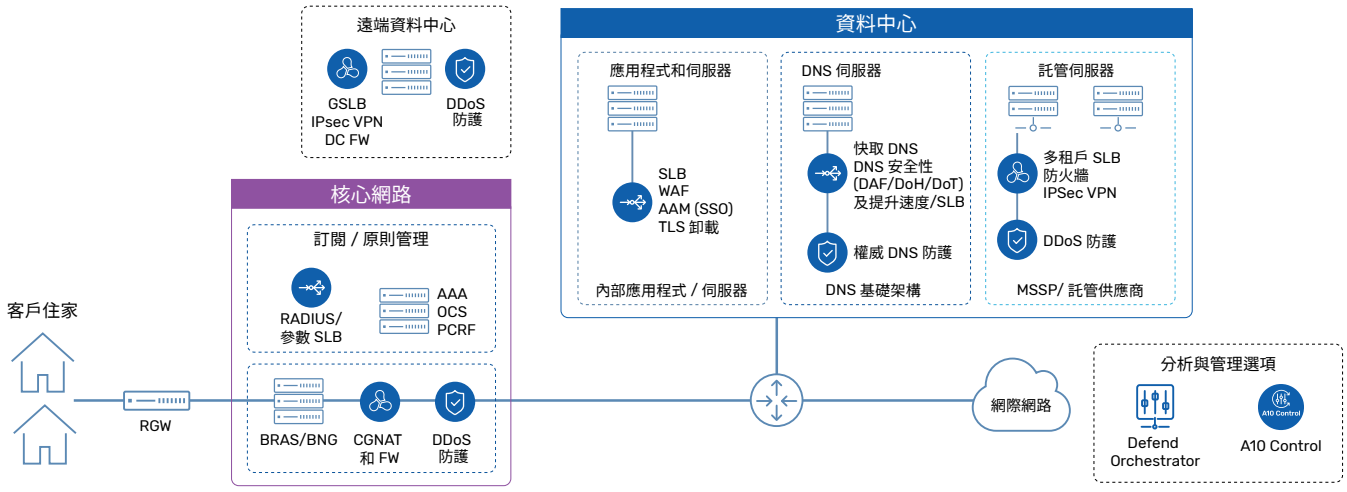
行動電信業者解決方案圖 (針對 LTE/5G-NSA)



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



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
永遠連線的應用程式交付和安全防護，涵蓋內部部署和雲端環境

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

防禦
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 7,000 多家公司安裝

A10 Networks 產品廣獲全球各行各業 7,000 多家頂尖公司採用。
我們的產品廣泛部署於各種需要高可靠性、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 7,000 多家客戶的信賴：

支援最大品牌

verizon
DELTA DENTAL
LY
Magnite
Digicel
IBM
SAMSUNG
Microsoft
KDDI
XBOX
COMCAST
LUCASFILM Ltd
LG U+
HCA Healthcare
SUBARU
CAESARS ENTERTAINMENT
Morgan Stanley
T-Mobile
NTT DATA
syniverse
UNIVERSITY OF CALIFORNIA
Charter COMMUNICATIONS
kt
SK telecom
stc
Türk Telekom
SoftBank
ROGERS
T2 TAKE-TWO INTERACTIVE
TURKCELL
Canada
CISCO
7-ELEVEN

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。我們的 7,000 多家客戶遍布全球大型企業、通訊、雲端和 Web 服務供應商，他們必須確保關鍵業務應用程式與網路是安全、可用且高效。

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

A10 中文資源網：
https://www.a10networks.co.jp/TW/resources/

Part Number: A10-BR-20114-TW-05 SEPT 2025

請按讚並追蹤 A10 facebook粉絲專頁