智慧型自我防禦功能 提供企業完善的網路資安保護 Cisco ASA 5500 系列

市場概況

思科市佔率

雖然全球網路安全市場由許多小型業者所盤據，但思科以 40% 的市佔率（2008 年第二季）仍穩佔市場龍頭寶座。自 2004 年以來，思科每季的市佔率均維持在 33% 至 39% 之間。

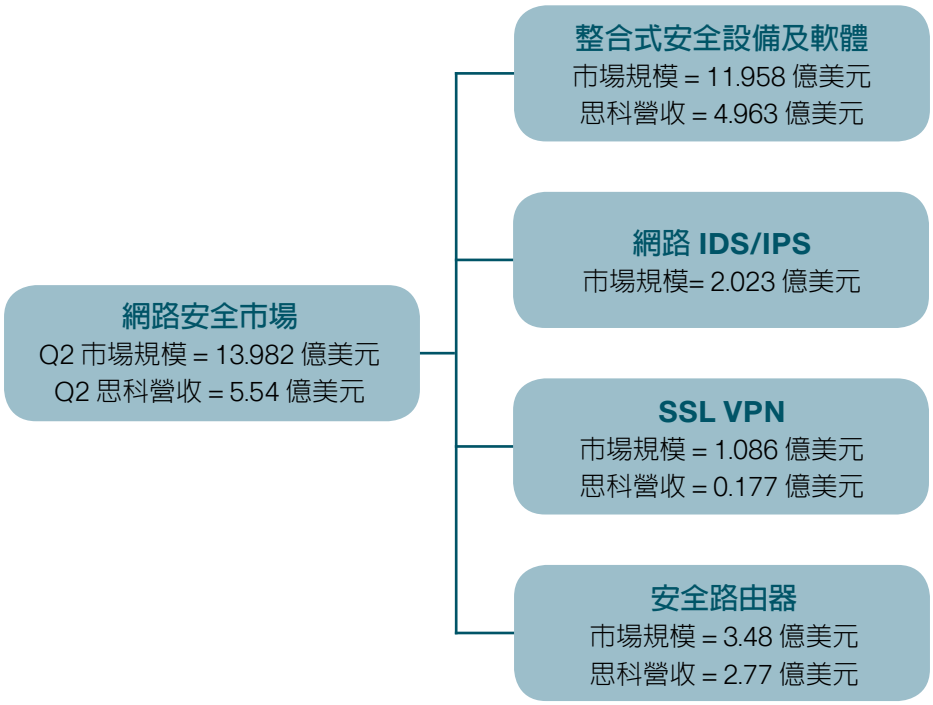

圖1：2008 年第二季全球市場規模與思科營收

產業評價

「Cisco ASA 5520 於整體威脅偵測成功率方面獲得 100% 的高分，而其競爭業者普遍僅獲得 30-40% 的評分。」

資料來源：Miercom Report：Cisco ASA 5500 Performance and Security Superior

「與智慧型架構進行全面整合，是一項重要因素—結合滲透式周邊、多層式認知及多元服務元件，產生整合式的威脅防禦措施。此套系統架構可於路由器上產生一個具備效率及有效性的安全環境。」

資料來源：MetaGroup WP: Unified Threat Defenses - The Route to Successful Security

思科歷年得獎獎項

- **SSA 2007 年年度傑出企業**
  http://newsroom.cisco.com/dlls/2008/prod_051908.html
- **Information Security 雜誌讀者票選獎**
  金牌獎 - UTM-Cisco ASA5500 系列
  金牌獎 - NAC-Cisco NAC設備
  金牌獎 - 電子郵件安全 - IronPort 電子郵件安全裝置
  銀牌獎 - 侵入偵測 / 防禦 - ASA5500 系列
  銀牌獎 - 無線網路 - 思科無線網路安全套裝軟體
- **2008 年亞太區 Frost & Sullivan 防火牆 / IPSec VPN 市場領導獎**
  此獎項旨在表彰思科於防火牆 / IPSec VPN 市場中卓越的領導地位。思科充分發揮在企業網路基礎架構的優勢，提供多項防火牆 / IPSec VPN 解決方案，以滿足眾多的客戶需求。
- **2006 年 Information Security & SearchSecurity.com 年度資訊安全產品獎（HTML）**
  思科以整合無線網路解決方案與 Cisco VPN 3000 系列連結器，贏得金牌獎，並以 ASA 5500 系列自適安全設備 (Adaptive Security Appliance) 與 Cisco PIX 500 系列安全平台贏得銀牌獎。
- **電腦零售商新聞 2005 年通路冠軍**
  最佳技術滿意度、網路安全、交換器與路由器、Wireless LAN、VoIP
- **網路雜誌 2005 年創新獎**
  網路硬體產品突破獎：整合式服務路由器系列；以及最具資安影響力獎：網路存取控制（Network Admission Control）
- **網路運算雜誌編輯票選獎：思科資安專家**
- **2006 年第 11 屆 Computerworld 雜誌讀者票選獎**
- **最佳企業防火牆與 VPN**
  - 最佳企業防火牆與 VPN
    防火牆 - Cisco ASA 5500 系列自適安全設備
    VPN - Cisco ASA 5500 系列自適安全設備
  - 最佳侵入偵測 / 防禦系統
    Cisco ASA 5500 系列 IPS 版本
  - 最佳 SAN 交換器
    Cisco MDS 9000 系列

Cisco ASA 5500 系列產品介紹

思科自我防禦網路解決方案

思科安全解決方案應定位為自我防禦網路，強調網路是最佳的安全平台，以系統為基礎、並優於 bolted-on 端點產品解決方案的安全措施。這是思科安全解決方案與市場上其他的產品差異所在。

思科自我防禦網路 (Cisco Self Defending Network) 為一套架構式解決方案，可運用網路來確認、回應及適應各種威脅。解決方案提供一項通用基礎架構，可整合網路每個層面的安全防護功能，並在此架構上面堆疊不同安全性、網路元件以及創新技術之間的協同作業，來適應新的安全威脅。思科與其他端點解決方案 (point solution) 安全設備廠商或網路供應商的相異處，在於其自我防禦網

路大幅簡化了安全、網路及商業環境，更加緊密整合安全與網路，帶給您更安全的環境。此舉不僅提高您的網路安全可見度，也能讓您更輕鬆地進行操作管理及控制政策遵循的情況。此外，將網路視為一個安全的平台亦能驅動安全服務的演進，您不僅無須進行全面更新或升級，還能提升您在安全投資方面的價值。與自我防禦網路相關的三項原則如下：

表1：Cisco 自我防衛網路相關的三項原則

整　合	協　同	適　應
將網路中的每個元件作為防禦點，這表示交換器、路由器、安全裝置及端點均包含安全功能，這些功能包括但不限於：防火牆、VPN 及信任與確認功能等。 此外，「整合」原則加入了保護分公司、資料中心、校園、WAN 及 LAN 環境的有線／無線網路，以及語音與數據網路。 「整合」代表加入了網路裝置安全操作所具備的技術，例如控制板政策及 CPU／記憶體門檻等。	不同的網路元件可共同運作，以提供新的保護措施。因此，「安全」將成為由端點、網路元件及政策執行之間相互合作的一套系統。 網路存取控制就是協同作業的一個範例—根據路由器及交換器等網路裝置遵守安全政策的情況，來判斷是否允許讓端點存取網路。	部署創新行為方法，以自動辨識新的網路威脅。在安全服務與網路智慧之間存有相互認知性，因此可增加安全的有效度，讓系統採取更主動的回應措施因應新的網路威脅。 藉由擴展威脅辨識能力，加上在網路多重層級中，解決安全威脅，能有效移轉安全風險，這包括了行為辨識、應用偵測及網路控制。

思科自我防禦網路 (Cisco Self Defending Network) 為企業客戶提供一個「安全基礎」，以保護其網路免受威脅，提升服務其客戶的效率，並可隨著企業成長與需求，安全地擴充網路平台。

Cisco Smart Business Roadmap 透過規劃一個符合營運目標的彈性化平台計畫，協助企業最佳化其運作，讓企業領導者能更有信心地制定支持企業長期目標的近期網路投資，同時亦能降低風險及總成本。

Cisco Smart Business Communications Architecture 為企業客戶提供一套備受肯定的架構、解決方案、合作廠商及支援服務，以滿足其商業需求。

深層防禦所面臨困難之處

資訊安全的規範已從保護網際網路範圍擴大至深入防禦模型，於基礎架構上堆疊多項反擊措施，以因應各種安全弱點及惡意攻擊。由於持續攀升的惡意攻擊、日趨複雜的攻擊手法及速度，模糊了網路與周邊的界線，導致企業必須採取多項反擊措施。

每天都有數千次的試探性威脅，嘗試想進入網路存取點及系統，企圖找出攻擊弱點。目前的混合式攻擊法使用多種詐騙方法，來攫取未經授權的系統存取，

並從企業內外進行控制。與日俱增的惡意破壞程式、零時差攻擊、病毒、木馬程式、間諜程式與攻擊工具，不斷挑戰著最堅固的基礎架構，導致更少的反應時間、停機時間及昂貴的維修成本。

在伺服器與網路裝置的數量之外，每個安全元件均針對異常偵測、威脅反應以及鑑識作業，提供了獨立的異常事件紀錄與警告功能。但可惜的是，操作人員必須花費大量時間與資源，分辨雜訊、提醒、日誌檔及誤判等情況，並分析這些資訊。此外，法規要求嚴格的資料隱私權、改善操作安全性及維護稽核作業。

思科 ASA5500 系列自適安全設備 Adaptive Security Appliance

Cisco ASA 5500 系列是一套易於部署的解決方案，將世界級的防火牆、整合通訊安全服務 (語音 / 視訊)、SSL 與 IPsec VPN、入侵偵測防護系統 (IPS) 及內容安全服務，整合至一項高彈性模組化的系列產品中。Cisco ASA 5500 系列是思科自我防禦網路的一個關鍵元件，提供智慧型威脅防禦及安全通訊服務，可在攻擊影響企業運作前加以遏止。Cisco ASA 5500 系列專門為保護各種規模網路所設計，讓企業能降低整體部署與運作成本，同時提供完整的多層級安全性。

表2：Cisco ASA 5500 能提供與 Cisco PIX 500 相關的完備功能性

	Cisco PIX	Cisco ASA	Cisco ASA 5500 優勢
以 IP 與使用者為基礎的彈性化存取控制	✔	✔	Cisco ASA 5500 擁有大量記憶體，可支援更多的 ACL
支援 30 種以上通用網路協定的進階應用程式層防火牆服務	✔	✔	Cisco ASA 5500 在進行深層封包檢查時，可提供更佳的效能
對加密語音 / 視訊通訊內容提供安全服務	✘	✔	只有 Cisco ASA 5500 可提供安全端對端加密語音 / 視訊通訊服務
Cisco Easy VPN 及 site-to-site IPSec VPN	✔	✔	Cisco ASA 5500 可提供卓越的 VPN 效能
Clientless SSL VPN 及 Cisco AnyConnect SSL VPN	✘	✔	Cisco ASA 5500 可提供世界級、高彈性的 SSL VPN 存取功能
VPN 叢集與負載平衡支援	✘	✔	Cisco ASA 5500 可提供企業級的VPN擴充性
全功能硬體加速 IPS 服務	✘	✔	Cisco ASA 5500 可提供卓越的攻擊防禦措施
趨勢科技所提供的防毒、反垃圾郵件、反網路釣魚及網址過濾服務	✘	✔	Cisco ASA 5500 可保護免於惡意軟體的攻擊，同時增加員工生產力
持續管理及監控	✔	✔	可運用 Cisco PIX Knowledge 與 Cisco ASA 5500 的工具

防火牆

可確保防範未經授權存取網路與資訊，同時徹底發揮網路回復及維持企業永續經營的能力。Cisco ASA 5500 提供先進的應用偵測防火牆服務，以及身分存取控制、阻絕服務 (DoS) 攻擊保護等功能。這些功能全都以備受市場肯定的 Cisco PIX 防火牆解決方案技術為基礎。

SSL/IPsec VPN

思科最高等級的 VPN 解決方案 Cisco ASA 5500 系列，以安全、彈性化、且無縫式遠端存取，來擴充網路，可提供無與倫比的無客戶端入口網站功能，以及跨平台全通道式客戶端，在一項裝置上最多可支援 10,000 個同步 SSL 或真正的 IPsec 連線。這些功能均具備世界級防火牆服務等功能的保護。

入侵防禦

透過先進全功能式的入侵偵測防禦系統 (IPS)，防禦關鍵網路資產免於遭受安全攻擊。Cisco ASA 5500 系列整合了威力強大、高效能的零時差保護措施，範圍涵蓋應用程式及作業系統安全漏洞、直接攻擊、惡意破壞程式及其他型態的惡意軟體。

AIP-SSM

Cisco ASA 5500 系列所包含的思科進階檢測及防衛安全服務模組 (Cisco® Advanced Inspection 與 Prevention Security Service Module, AIP-SSM)，可提供主動式的全功能侵入防禦服務，可於惡意破壞程式及網路病毒等惡意攻擊影響網路前加以遏止。

內容安全

可提升員工生產力並消除網路中不受歡迎的內容威脅。Cisco ASA 5500 系列可提供威力無窮的內容安全服務，包含網址過濾、反網路釣魚、反垃圾郵件、防毒程式、反間諜程式及內容過濾等，有助於降低營運成本、減少負債，同時提升員工生產力。

CSC-SSM

Cisco ASA 5500 Series Content Security 與 Control Security Services Module (CSC-SSM) 結合完整的惡意軟體保護措施，及 Cisco ASA 系列多功能安全裝置的先進網路流量與訊息合法性。此項解決方案可提供強大的保護及商業網路通訊控制，並可有效遏止病毒、惡意破壞程式、間諜程式、垃圾郵件與網路釣魚等網路威脅，控制不必要的訪客及網頁內容，同時能降低營運成本以及部署和管理多點解決方案的複雜性。

整合通訊安全性

ASA 系列自適安全設備提供領先市場的整合式通訊語音及視訊安全服務，包括強固的防火牆、全功能的IP Security (IPsec) 及 SSL VPN、侵入防禦與內容安全功能。在部署整合通訊方面，這些平台最多能保護 30,000 台電話，提供最廣泛的整合通訊協定應用程式檢查，包括：Skinny Client Control Protocol (SCCP)、Session Initiation Protocol (SIP)、H.323、Media Gateway Control Protocol (MGCP)、Computer Telephony Interface Quick Buffer Encoding (CTIQBE)、Real-Time Transport Protocol (RTP) 與Real-Time Transport Control Protocol (RTCP)。

如欲獲得更多資訊
請瀏覽 http://www.cisco.com/en/US/products/ps6120/products_data_sheet0900aecd8073cbbf.html 網站。

更多關於 Cisco ASA 5500 系列的資訊
請瀏覽 http://www.cisco.com/web/TW/solutions/segments/commercial/products/security/asa_5500_series_adaptive_security_appliances.html 網站。

欲知更多安全解決方案相關資訊
請瀏覽 http://www.cisco.com/web/TW/solutions/security/index.html

圖2：針對 Cisco PIX Security Appliance Customers 的建議移轉路徑

Cisco VPN 3000 與 Cisco ASA 5500 的比較

- ASA 5500 為 VPN 3000 的替代平台，且在許多方面均優於 VPN 3000
- ASA 可提供較佳的 SSL VPN 功能性
- ASA 可提供10 倍以上的 SSL VPN 擴充性
- ASA 可提供 4-50 倍的傳輸率
- ASA 較 IPSec 減少 45% 的成本
- ASA 可提供完整 IPS、Anti-X 與防火牆功能
- ASA 可提供狀態故障復原、整合 VPN 3000 負載平衡叢集
- ASA 不僅提供與 VPN 3000 相同的 IPSec 功能，並包含 QoS

將原有 VPN 3000 的客戶移轉至 ASA 5500 絕對是一大商機。客戶能享有：

1. 完備的 SSL VPN 功能性
2. 可運用 SSL VPN 降低遠端存取營運成本
3. 整合式安全措施，可完整保障 VPN
4. 更卓越的 VPN 擴充性與傳輸率

下表為 Cisco VPN 3000 系列連結器和 Cisco ASA 5500 系列 SSL/IPSec VPN Edition 的移轉路徑：

表3：Cisco VPN 3000 系列連結器和 Cisco ASA 5500 系列 SSL/IPSec VPN Edition 的移轉路徑

VPN 3000 系列連結器	ASA 5500 系列 S SL/IP Sec VPN Edition
VPN 3002 硬體客戶 VPN: 2.2 Mbps	ASA 5505 VPN: 100 Mbps
	ASA 5510 VPN: 170 Mbps
VPN 3020 與 3015 集中器 VPN: 50 Mbps	ASA 5510 VPN: 170 Mbps
	ASA 5520 VPN: 225 Mbps
VPN 3030 集中器 VPN: 50 Mbps	ASA 5520 VPN: 225 Mbps
	ASA 5540 VPN: 325 Mbps
VPN 3060 集中器 VPN: 100 Mbps	ASA 5540 VPN: 325 Mbps
	ASA 5550 VPN: 425 Mbps
VPN 3080 集中器 VPN: 100 Mbps	ASA 5550 VPN: 425 Mbps

為 Cisco ASA 加入安全支援功能：AIP 模組

Cisco ASA 進階檢測與防禦 (AIP) 模組

Cisco ASA 5500 系列自適安全設備解決方案所具備的思科進階檢測及防禦安全服務模組(AIP-SSM)，提供了主動式、全功能的入侵防禦服務，可於惡意破壞程式及網路病毒等惡意攻擊影響您的網路前，就可加以遏止。

透過 Cisco IPS Sensor Software Version 5.x，Cisco AIP-SSM 可結合在線防禦服務與創新技術，以提升正確率。入侵偵測防禦系統 (IPS) 解決方案可為您提供全面性的保護，而無須擔心遺漏任何合法的網路流量。將 AIP-SSM 部署於 Cisco ASA 5500 系列設備中時，藉由與其他網路安全資源協同作業，可主動對您的網路提供全面性的保護。如欲獲得更多關於 ASA AIP-SSM 的資訊，請瀏覽 http://www.cisco.com/en/US/products/ps6825/index.html 網站。

AIP 安全服務模組 + Cisco Security MARS

藉由整合自我防衛網路中以系統為基礎的安全措施，其集合效益遠大於單一服務。此項解決方案背後的設計關鍵因素，就是結合Cisco ASA (含 AIP 安全服務模組) 與 Cisco Security MARS，使客戶能大幅採用這項組合，以強化威脅能見度及控制性，並簡化安全資源管理作業，這是解決方案單一元件無法達到的。客戶可選擇階段性部署作業，例如先部署 MARS，之後再加入 Cisco IPS 或 ASA 的功能。

思科安全解決方案滿足企業需求

表4：思科安全解決方案滿足企業需求

BDM/TDM 的難處	客戶需求	建議使用的產品
網路攻擊（病毒、惡意破壞程式或駭客）造成企業營運中斷	零時差安全威脅移轉整合式網路安全平台	Cisco MARS 與 IPS Cisco ASA Anti-X with IPS
對於使用 MP3、即時訊息等的管理政策進行進一步的控制與執行	簡化營運管理支援	Cisco MARS 與 IPS
行動工作者帶來惡意破壞程式、病毒、木馬程式等	網路層能見度零時差安全威脅移轉	Cisco MARS 與 IPS
從分公司至總部均涵蓋在防禦範圍內的防火牆功能	整合式網路安全平台	Cisco ASA
誤判現有 IPS 中造成挫敗的來源	零時差安全威脅移轉	Cisco MARS 與 IPS
允許合法流量進入網站，同時將不合法流量進行轉向，以確保企業永續性	整合式網路安全平台	Cisco ASA

台北總公司
台北市信義路四段 460 號 12 樓
www.cisco.com.tw
Tel : 02 - 8758 - 7100
Fax : 02 - 8758 - 7199

台中辦事處
台中市公益路二段 51 號 20 樓 A2
www.cisco.com.tw
Tel : 04 - 2327 - 1372

高雄辦事處
高雄市苓雅區三多四路 110 號 19 樓之 2
www.cisco.com.tw
Tel : 07 - 338 - 1092
Fax : 07 - 338 -1094

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**