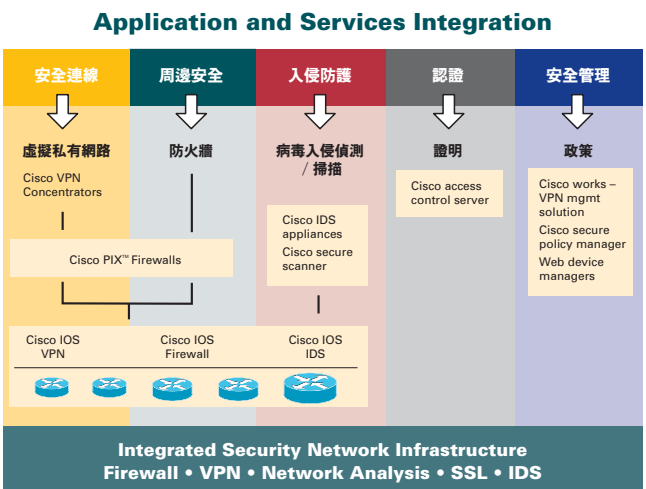
整合性網路是
有效的安全防衛方式



Cisco 產品型錄中每項產品都可連結應用至特定安全解決方案。

有效的網路安全解決方案，需整合網路中各個不同型式保護機制，使其共同運作。愈多層安全防護，就愈有機會阻檔下列可能的攻擊。

本章我們將針對三個最重要的實體安全層及進行說明：

- 安全連線
- 周邊安全
- 入侵防護

安全防護

虛擬私有網路（VPN）是在網際網路或其他公眾網路上具隱私的連線。它們允許用戶不受實際網路限制，可在網路中進行相同的安全層級作業。若我們拿建築物作為比喻，VPNs 就像具防護功能的車輛穿梭在公路上，並將機密資訊從外部帶入建築物內。

所有 VPN 軟體與硬體都利用加密技術，及數學演算法將訊息及所附加內容全數打亂，如此可確保訊息不會被其他人刻意攔截讀取。

周邊安全

若我們將網路看成一棟建築物，周邊安全就像網站周圍的柵欄與閘門。

周邊安全控制著關鍵應用服務與資料存取，因此，只有合法的使用者與資訊，才可經由受到信任的網域，從一個網路送至另一個網路。

存取控制

在用戶輸入密碼以取得存取權限前，網路必須確認使用者密碼是合法的。存取控制伺服器可確認用戶識別碼，並依照用戶資料，決定可使用何處的網路及何種資訊，而這項功能就像入口處的守衛檢視識別卡一樣。

防火牆

防火牆是一套硬體或軟體解決方案，可限制網路資源存取，就像鎖住的門，只允許擁有鑰匙的人（或特殊身份、知道密碼的人）進入。

防火牆技術在網路與外界環境間形成一道保護層，可過濾未經允許的認證，或是具潛在危害的資訊進入系統，同時也會記錄嘗試入侵的訊息，並警告網路管理者。

駭客入侵防護

若將您的網路看成是一棟建築物，駭客入侵防護就像是監控安全的攝影機，以及動作感應器（Motion Sensors），隨時觀測周圍狀況。

以網路為基礎的入侵偵測系統（Intrusion Detection System；IDS）可持續進行網路監控，分析網路中封包資料流，並搜尋如駭客攻擊的未經認證行為，並在系統受到攻擊前，就由用戶回報安全上的漏洞。

當系統偵測到未經授權的行為時，IDS 即送出一連串的警告給管理中控台，包括入侵細節，並傳送指令給其他系統（如路由器），以切斷未經認證的連線。

薄弱的網路安全將對您的業務帶來什麼風險呢？根據2002年美國聯邦調查局報告指出，平均每年因網路安全所造成的損失將近2百萬美元。

我們建立網路，
也能保障網路安全。

Cisco 提供三種安全層級硬體解決方案，其產品是以 SAFE（Security Architecture For Enterprise）為標準，同時也是設計與管理安全網路時最佳指導方針。

由於 Cisco 已發展出多數網路相關解決方案與產品，除了可增強網路效能，更可提供符合商務需求的安全防護解決方案。

Cisco 在網路上的專業性，充分顯示有能力提供智慧型安全防護解決方案，並整合不同企業的網路架構。

此外，當網路受到攻擊時，Cisco 安全防護解決方案具足夠偵測能力，可事先做出回應。一旦網路內部建立這類安全解決方案，企業便能擁有一套智慧型自我防衛網路。

在今日變動環境中，網路在公司基礎建設上已成為不可或缺的一部分，也同時影響所有系統與服務，而客戶比以前更瞭解網路整合安全是所有 IT 策略的中心。全球網路設備領導廠商思科系統（Cisco Systems），則可提供客戶更多元化的解決方案。