Page 1

整合網路與安全 發展捍衛電子商務的最新策略

您知道不健全的網路安全設施，將為您的企業帶來什麼樣的危機？根據美國聯邦調查局（FBI）2002 年最新調查顯示，網路安全所造成的損失金額已高達一年平均兩百萬美元。網路安全的威脅不僅已成為您經營企業永不間斷且嚴苛的挑戰，且將持續增加。當您的網路環境變得更為開放、延伸到更多地點、加入更多應用，以及支援更多新技術（如：行動通訊、IP 電話）時，新的威脅也將層出不窮。

網路安全需求的變化可從電腦安全漏洞急速增加的情況看出端倪。在 CSI/FBI 的 2002 年「電腦犯罪與安全性調查」(Computer Crime and Security Survey)報告中顯示，有高達 90%的受訪人士(主要為大型企業與政府單位人士)在十二個月內就曾發現電腦的安全漏洞問題，其中更有 80%的人承認因為這些漏洞而造成財物損失。

防火牆（Firewall）與其他獨立式（standalone）網路安全產品雖然依舊是整套安全方案的重要成員，但這些設備已不足以用來保衛您的網路，使其免於受到來自內部與外部的攻擊。而網路與安全專家也都發現，今日的網路需要一套嶄新、完整的解決方案來提供安全功能，換句話說，即是一種具彈性且多層次的架構，讓數種安全設備之間能夠互相涵蓋與整合。

Cisco 領先業界推出第一套完整網路安全解決方案，其包含五種全新模組，可將必要的安全功能整合於 Cisco Catalyst 6500 系列多層交換器中。這些模組可為防火牆、病毒入侵偵測、安全 Socket 層（SSL）處理、網路分析管理及虛擬私有網路（VPN）等功能，提供 Gigabit 等級的處理速度。搭配上現有的內容交換模組（Content Switching Module，CSM），其網路安全解決方案更可為 Catalyst 交換器增加商業上正確回覆與高可用性之服務。藉由支援完整的安全功能，Cisco Catalyst 6500 系列模組將協助您的網路、應用系統與商業運作模組化，並可彈性增加必要的安全措施。

為何需要內建式、整合式安全設計呢？

我們有充分的理由支持網路安全架構應該採用整合式設計，其中包括了：

- 網路威脅的多樣化及數量持續增加，唯有採用「深層防衛」策略，將多種安全設備緊密地結合在一起，才能解決此一問題。
- 舊有的安全產品是為特定企業網路量身打造，和其他網路僅有少許的連接線路。但是，今日的網際網路擁有數百條，甚至數千條的連接線路，因此企業需要的安全產品是能夠支援包含多種不同網路設計的安全架構。
- 隨著網路持續成長、演變，安全設計必須能保持步調、維持透通性（transparency），讓您的網路可以持續維持架構彈性與效能。
- 整合式安全設計能讓您的整個電子商務網路維持運作順暢，並確保安全功能不會變成銷售或其他線上活動的絆腳石。

關於 Cisco Catalyst 6500 系列交換器

Cisco Catalyst 6500 系列交換器為企業與服務供應商的網路提供了高可用性、安全性與整合的網路服務。這些交換器為骨幹網路、內容傳遞、配線拓樸和資料中心等環境，提供具備 Giagbit 等級的擴充能力、高可用性、多樣化服務以及多層交換功能。Catalyst 6500 系列同時還支援多種傳輸介面，並可整合功能強大的服務模組，為用戶提供更多的擴充性與價值。

在 Catalyst 6500 系列中，卓越的控制面設計和封包傳送技術結合多樣化的智慧型服務，為企業奠定整合式語音/影像/數據網路和電子商務的基石。

- 搭配整合式安全設計，網路運作與管理不僅變得更簡單，亦帶來營運成本降低的附加效益。
- 一套完整、內建式以及整合的安全設計更適合採用新型、互聯式網路技術（如：VPN、無線、IP 電話）的網路規劃。

「整合」真正的涵義不僅僅是單純地安全設備間相互運作，網路安全需要的是一套完整的規劃設計。Cisco 所提出的安全藍圖（SAFE Blueprint）為所有企業組織提供了一套完整的實務規劃，以建造一個安全、深度防衛的網路世界。Cisco Catalyst 6500 系列交換器的整合式安全模組就是採用 SAFE Blueprint 的架構，可精確地符合您整體網路與安全策略需求。

整合式網路安全功能的最佳建置地點是哪裡呢？答案就是網路基礎架構。區域交換器（campus switch）在網路基礎架構中扮演關鍵的角色，其優點包含了：

- 可提供更高安全效能，卻不會降低交換器本身之效能。
- 增加網路彈性、可擴充性與可用性。
- 可保護網路核心，因為 Cisco Catalyst 6500 系列交換器具備自我保護功能。
- 透過對現有網路資源的善加利用，可降低整體網路持有成本。
- 不論何種網路服務，皆能將其網路與安全功能天衣無縫的整合在一起。
- 可加深網路與安全運作之間的合作密切度，這也是對抗現今日益複雜之網路攻擊的重要需求。

將安全功能與 Cisco Catalyst 6500 系列交換器整合

Catalyst 6500 系列安全模組可支援兩種安裝架構：

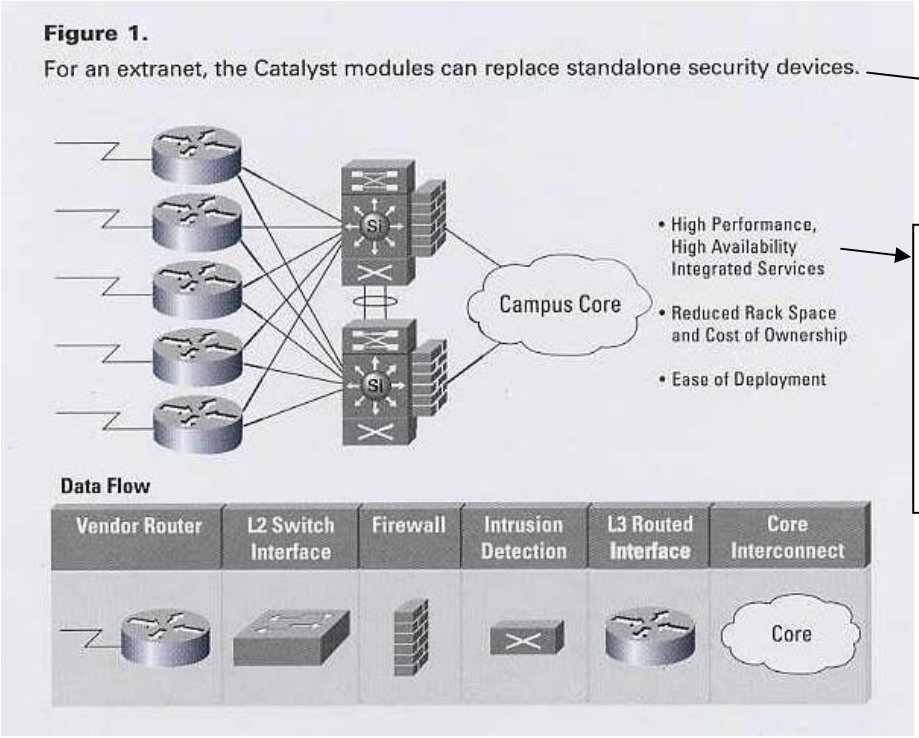
- 透過安裝適當的模組，將多種安全功能建置於單一交換器中。
- 透過安裝同一安全功能類型的多重模組於單一交換器中，特定強化其處理能力，例如入侵偵測。

Cisco Catalyst 6500 系列之服務模組	功能描述
防火牆服務模組（Firewall Services Module；FSM）	防火牆保護可處理 OC-48 或 5Gbps 的資料流量，並可同時處理高達一百萬條的連線。這套模組是由 Cisco 獲獎的 PIX Firewall 技術

	建構。
SSL 服務模組（SSL Services Module；SSLM）	安全網站交易，可同時處理六萬條連線，且每秒鐘可接受四千條的新連線。
IPSec VPN 服務模組（IPSec VPN Services Module；VPNM）	提供安全、Gigabit 傳輸速率的 VPN 連線與資料加密，可連接到遠端辦公室和行動用戶。
網路分析模組（Network Analysis Module；NAM）	在 Gigabit 高速環境中監視網路活動，並採用 web 介面的流量分析器，快速地在網路應用層確認潛在的安全威脅。
內容交換模組（Content Switching Module；CSM）	擁有 Layer 4 到 Layer 7 完整功能的 CSM，可將先進的內容交換技術融入 Catalyst 6500 系列中，如此可為防火牆、網站伺服器、快取伺服器，以及其他網路設備提供了高效能、高可用性的負載均衡功能。
病毒偵測保護系統模組（Intrusion Detection System Module，IDSM）	直接在交換器背板中處理網路流量，藉以偵測並減緩網路入侵的傷害。

Page 3

（圖一）



以內部網路而言，Catalyst 模組可替代獨立式網路安全裝置

- 高效能與高可用性的整合式服務
- 減少所需空間與持有成本
- 建置的簡易性

獨立式安全設備是否仍存在於您的網路中？

雖然這些討論都傾向於整合式網路安全設計，但獨立式設備依然適用於許多網路中。如防火牆的獨立式網路安全設備，對於一些特定場所或特殊應用而言或許才是最佳選擇。SAFE 藍圖在如何選擇整合式或獨立式設備上提供了一些建議，可滿足客戶特定的安全需求。

所有的模組都採用 Cisco 功能強大的節點交換處理器（Node Switch Processor，NSP）技術，和其他採用 ASIC 技術的競爭產品相比，NSP 提供了更佳效能、彈性與功能。

Catalyst 6500 系列的安全模組可採用 Cisco 網路管理產品加以管理，或是 Cisco 合作廠商的應用產品。Catalyst 6500 系列的整合式安全設計與 Cisco 獨立式安全產品相容，包括 Cisco PIX 防火牆和 Cisco 駭客入侵防護產品。

目前已有兩種企業網路架構可作為整合式安全設計的應用範例。第一個範例是企業間網路（參見圖一），其個別防火牆和駭客入侵偵測裝置都已被搭配適當模組的 Catalyst 6500 交換器所取代。在這範例中，企業可以省去個別設備的成本與管理負擔，同時達到更好的運作效率以及 Catalyst 6500 系列交換器的投資回收。

安全處理工作會影響交換器的效能嗎？

在網路流量和交換器服務需求激增的狀況下，網路管理者當然會害怕再增加新的功能於區域交換器（campus switch）上。網路安全功能需耗費大量的運算處理，因此引發了是否會影響交換器效能的疑慮。Cisco 為了解決此一問題而研發出安全模組，讓客戶不再需要為了提升安全性而犧牲網路效能。最新推出的 Cisco Catalyst 6500 安全模組提供了當今最高速的安全處理能力，保證不會對交換器的效能有重大影響。

從網路管理者的角度來看，網路安全整合還擁有更多的優勢，如：

- 藉由整合高效能 Catalyst 6500 系列交換器和領先市場的安全技術，將可產生功能更強大的網路產品解決方案。
- 可保障客戶在 Catalyst 和 NSP 技術上的投資，又不會降低安全功能和網路效能。
- 易於和現有的 Cisco Catalyst 6500 系列交換器進行整合。
- 具可擴充性和彈性的設計，並在需要時增添安全功能。
- 更緊密結合安全功能與網路服務，如：流量監視管理和控制。

Page 4

為何必需在區域交換器中加裝安全功能？

對網路安全管理者來說，若將所有的安全功能整合於單一個節點，亦即區域交換器，就是代表一種危險。但是，整合所帶來的好處卻強烈支持客戶由獨立式

設備走往此一方向。對於網路安全管理者，整合的優勢包括：

- 和獨立式設備相比，模組化設計帶來了高擴充性，並大幅降低成本、運作複雜度和管理負擔。
- 透過整合各種不同的安全模組，網路安全服務可應用於更廣泛的網路架構之中。
- 網路安全模組所提供的效能遠遠超過獨立式設備所能提供。
- 經由在單一設備上，如：防火牆，加裝多個模組，個別安全功能的效能可獲得提升。
- 網路的成長與變更可輕易透過增添新模組來因應，這是增添新獨立式設備之外的另一種選擇。

挑選一項整合式網路安全解決方案

Cisco 在網路安全中提出的整合式解決方案不僅反映 Cisco 在網路業界的領導地位，也將讓您的事業可更有效率的符合今日和未來安全需求。Cisco 是目前唯一能針對網路安全所有重要部分都提供整合式設計和區域交換器模組的廠商。Cisco Catalyst 6500 系列交換器與整合式安全模組相互搭配，已成為一套兼顧辦公區域網路和內建、整合式網路安全需求的傑出產品解決方案。

Cisco 和 WebEx 聯手運用 Catalyst 6500 系列產品擴展整合式網路安全功能

WebEx Communication Inc. 目前正在測試 Catalyst 6500 系列的新款防火牆、VPN 和 SSL 模組。WebEx 的網路工程經理 Hesham Eassa 表示：「到目前為止，經由對防火牆模組的測試，我們發現了更高的處理能力，並遠超過擁有類似功能的其他產品。」和獨立式設備相比，更傑出的防火牆效能使 WebEx 可安裝更多防火牆模組，而這對於大型的全球通訊網路業者更是一項重要考量。

WebEx 總部設立於加州 San Jose 市，其主要業務為利用電話線和網站來提供互動式會議服務。這些服務採用了 Cisco AVVID（Cisco 語音、影像和數據整合架構）網路，為企業活動，如：會議、研討會、員工訓練和組織合作等，整合了語音、影像和數據的傳輸。

若您欲和 Cisco 交換器與網路安全方面的專家做線上實況交談，或者需要更了解整合式網路安全如何保護您的網路；請至 www.cisco.com/go/SecurityTechTalk 登錄會員

更多相關資訊：

Cisco Catalyst 6500 系列：www.cisco.com/go/Catalyst6500

SAFE Blueprint：www.cisco.com/go/safe