Cisco ASA 軟體 7.0 版

「Cisco® ASA 5500 系列自適型安全裝置」提供中小企業、大型企業與網路服務供應商諸多領導市場的高效能安全管理與 VPN 服務，帶來了前所未有的服務彈性與擴充性，協助企業降低佈署與運作成本。

產品簡介

Cisco ASA 5500 系列自適型安全裝置創新採用「自適型威脅辨識與解除」（AIM: Adaptive Identification and Mitigation）架構，是一套結合業界最佳的安全管理與 VPN 服務而特別設計的解決方案。Cisco ASA 5500 系列產品是「Cisco 自我防禦網路」的核心元件之一，具備主動式的威脅防禦功能，在威脅散播到網路之前即可終止其威脅攻擊，並且可控制網路上的活動及應用層的資料傳輸，同時還能提供高彈性的 VPN 連線能力。這一系列功能強大的多功能網路安全設備，不僅可提供網路安全的深度與廣度，防衛中小企業與大型企業的網路運作，而且還能夠減少網路的佈署與營運成本，並降低網路安全的建構複雜度。

Cisco ASA 5500 系列產品在單一平台上，提結合許多業界認可的網路安全技術在單一平台上，因此能兼具維運及經濟效益上的需求，更完善地將網路安全服務佈署到更多的網路節點。它的多功能安全設定檔，讓管理者不需在強固的安全保障或多重裝置的維運成本間取捨，因而減少決策上的困難度及風險性。

Cisco ASA 5500 系列產品可協助企業更有效地保護網路，並妥善保障既有投資，其重要特色包括：

- **廣為市場接受的安全性與 VPN 功能**：全功能、高效能的防火牆、入侵防禦系統（IPS）、網路防毒、IPSec/SSL VPN 技術，皆可提供強固的應用程式安全性，提供使用者及應用程式的存取控制、網路蠕蟲與病毒之防禦、惡意軟體之防範，以及遠端使用者/據點的連線能力。
- **可擴充之「自適型威脅辨識與解除」（AIM）服務架構**：AIM 採用模組化服務處理及資安策略框架，可根據資料流啓動特定的安全服務或網路服務，提供精細的資安策略控制能力、Anti-X 防禦功能和流暢的資料流處理能力。Cisco ASA 5500 系列產品的 AIM 架構不但效率高，而且透過使用者可自行安裝的安全服務模組（SSM: Security Services Module），還可擴充軟體與硬體功能，讓現有服務逐步升級，使得在佈署新服務之際，不需更換平台或犧牲效能。以 AIM 作為 Cisco ASA 5500 系列產品的架構基礎，提供自訂性極高的安全政策以及前所未有的服務擴充性，以抵禦快速演進的外來攻擊。
- **降低佈署與營運成本**：這套多功能的應用設備，可讓平台、組態、管理作業標準化，協助降低佈署成本及例行的運作成本。

廣獲市場接受的安全性與 VPN 功能

Cisco 在開發安全系統與 VPN 解決方案方面，領先業界、頻獲大獎，Cisco ASA 5500 系列產品承繼這樣的專業，融合 Cisco PIX 500 系列防火牆、Cisco IPS 4200 系列入侵防禦系統與 Cisco VPN 3000 系列集中器（Concentrator）的最新技術，結合成一套無與倫比的業界最佳方案，以抵禦各種外來威脅，為企業提供高彈性而安全的連線選擇。Cisco ASA 5500 系列自適型安全設備所提供的安全性與網路服務，兼顧廣度與深度，可以保護網路上的各個區域，其中包括最常受威脅的層面，例如行動用戶、遠端據點，以及未受管理的桌上型電腦及伺服器。此外 Cisco ASA 5500 系列產品也是「Cisco 自適型威脅防禦」與以及「統合安全存取」兩大策略的重要元素，可整合各式各樣的網路安全與 VPN 技術，以提供完善的應用程式安全性、Anti-X 防禦能力、網路抵禦與控制、以及安全的連線能力。

應用程式安全性

「Cisco ASA 5500 系列產品」透過 30 個智慧型應用感知程式的偵查引擎，檢查 Layer 2 至 Layer 7 的網路資料流，提供強化的應用層安全性。為了防禦網路不受到應用層攻擊，並讓企業控制本身環境中的應用程式與通訊協定的使用方式，這些偵查引擎對應用程式與通訊協定有完善的瞭解，並採用多種安全性執行技術，包括應用程式過濾、通訊協定指令過濾、通訊協定異常偵測、應用程式與通訊協定狀態追蹤等等。為了進一步提高對應用程式的偵查與控制，這些偵查引擎也內含攻擊偵測與防禦技術，例如緩衝區滿溢（buffer overflow）防禦、內容過濾與驗證、URL 網址解析服務等等。這些偵查引擎可以應用於廣泛使用的應用程式與通訊協定，例如網頁、檔案傳輸、電子郵件、語音與多媒體、資料庫、作業系統、第三代（3G）行動無線網路服務。此外，這些偵查引擎也可讓企業控制來自多種來源的外來威脅，例如即時傳訊（instant messaging）、點對點（peer-to-peer）檔案共享以及其他通道化應用程式。而且企業還可以執行網路使用政策，保障合法企業的網路頻寬使用權。

Anti-X 防禦功能

Cisco ASA 5500 系列產品提供進階的高效能保護功能，可抵禦網路與應用層的攻擊、DoS（Denial-Of-Service）攻擊與惡意軟體的入侵，例如網路蠕蟲、病毒、特洛伊木馬、間諜軟體、廣告軟體等等。為了發揮最高效果，Anti-X 防禦功能有完善的攻擊偵測功能，搭配先進的分析技術，可在不影響合法網路資料流的前提下，精確分析外來威脅，採取適當的抵禦措施。

先進的偵測技術

為了確保能徹底偵查到外來威脅，Cisco ASA 5500 系列產品提供許許多多不同的方法，以辨識網路動態是否違反既定資安規範、是否有異常活動、以及網路弱點是否遭到利用。此外，這些產品也包含狀態模式辨識，用來防禦隱藏於資料流中的外來攻擊。系列產品的通訊協定分析功能，可以驗證網路資料流；而資料流異常偵測功能，可以辨識跨越數個傳輸階段與連線的攻擊；通訊協定異常偵測功能，可以在通訊協定/服務的正常 RFC 行為中，辨識出異常的外來攻擊；而 Layer 2 分析功能，可以偵測出人為中介（man-in-the-middle）的攻擊。這些產品具備特殊的保全措施，可以過濾網路資料流，以免外來攻擊躲避系統偵測，這些保全措施包括：IP 分段重組與正規化、TCP 資料流重組與正規化、TCP 躲避控制、IP 防詐欺功能（deobfuscation）等等。

除了豐富的偵測技巧之外，這些產品還具備 Cisco 公司創新開發的分析與關聯兩項技術，可以正確解除所偵測到的威脅。此兩項技術分別是「風險指數鑑定」(Risk Rating) 與「統合事件產生器」(Meta Event Generator)。

風險指數評估

Cisco ASA 5500 系列產品使用 Cisco 創新的風險鑑定技術，以確保在不影響合法資料流的情況下，能即時阻止惡意攻擊。Cisco 風險鑑定技術超越傳統以單方位判定威脅風險的方法。為精確判斷特定事件的風險，Cisco 風險指數鑑定技術綜合考量了下列四項衡量指標：

- **事件嚴重性**：顯示出每一事件所可能受到的傷害程度。
- **特徵比對可信度**：顯示入侵特徵檔的可信賴度。
- **資產價值**：使用者可自行設定的數值來代表被攻擊目標系統的重要性與價值，（例如：列印伺服器價值低，而電子商務伺服器則價值高）。
- **攻擊相關性**：基於目標系統對某攻擊的脆弱程度訂定攻擊有效指數。

這四項因子結合起來，可以精確鑑定外來威脅，以採取最妥當的解決措施。

Cisco 統合事件產生器

為了快速而精確地辨識網路蠕蟲的入侵，與防止蠕蟲迅速散佈造成大規模損失，Cisco ASA 5500 系列產品包含了 Cisco 統合事件產生器技術，內建獨特的事件關聯功能。這項功能可隨時針對蠕蟲的行為模式進行比對，考慮多種事件類型的相關度，以及個別事件之間的間隔時間。蠕蟲要在網路上散佈時，通常會透過多個封包的傳輸來進行，但這些封包通常外表看起來都像是合法的資料流。統合事件產生器可使用即時關聯服務，辨識蠕蟲散佈的初始封包，並阻止後續的受感染封包，因此蠕蟲無法完整抵達預定目標，繼而無法產生效力。

安全連線服務

Cisco ASA 5500 系列產品提供強大的點對點 (site-to-site) VPN 以及遠端存取 VPN 服務，可以透過公共網路，讓企業與行動用戶、遠端據點及企業夥伴之間建立安全連線。這套產品提供整合式安全功能，讓企業無須妥協企業安全政策的完整性，就能享用網際網路的連線能力與成本效益。

VPN 服務結合 Cisco ASA 5500 系列產品的各項安全服務之後，企業可以享有更強固、更安全的 VPN 連線能力。這套產品內建的 Cisco 自適型威脅防禦功能，可確保 VPN 免於成為網路蠕蟲、病毒、惡意軟體、駭客入侵的攻擊管道。而且 VPN 資料流也可使用詳細的應用程式與存取控制政策，讓個別用戶與群組用戶只能存取自己使用權限內的服務與資源。此外，企業還可為特定的用戶、群組、通道或資料流，自訂服務品質（QoS）政策，以確保特定的網路資料流享有適當的優先權與受到頻寬限制。

遠端存取 VPN

Cisco ASA 5500 系列產品的技術應用性彈性極高，可提供符合企業連線需求的客製方案，讓員工在使用公司管理的桌上型電腦時，能透過 IPSec VPN 享有功能強大、可自訂的遠端存取功能。如果網路端點不受公司管理，例如 Extranet、網際網路資訊站（Internet Kiosk）或員工私人電腦，則 Cisco ASA 5500 系列產品可透過 WebVPN 提供 SSL 遠端存取功能。利用 Cisco 專業的遠端存取技術，企業只需佈署單一的整合式平台，就可廣泛支援各種企業核心應用程式。

- **高彈性平台**：在單一平台上提供 IPSec 與 SSL 技術的 VPN 服務，不需要採用兩套個別的解決方案。由於不需要針對 SSL 和 IPSec VPN 佈署個別的獨立平台，因此 Cisco ASA 5500 系列產品可提昇效率、節省額外成本。
- **高韌性叢集**：所有 VPN 連線請求，不需要使用者介入操作，即可平均分配到 Cisco ASA 5500 系列產品和 Cisco VPN 3000 系列平台，因此可讓遠端存取功能的佈署，達到高成本效益的延展性。這項高韌性功能可避免任何單一設備之故障，並讓企業的 VPN 系統可隨實際需要而擴充，提供絕佳的投資保障。
- **Cisco Easy VPN**：提供一套獨特而具高延展性、高成本效益、容易管理的遠端存取 VPN 架構。Cisco ASA 5500 系列設備，可將最新的 VPN 安全政策推送到遠端的 VPN 裝置與客戶端，以確保遠程端點在建立連線之前，已先具備最新的安全政策，藉以達到最高的彈性、延展性與使用簡易性。除此之外，Cisco ASA 5500 系列產品為 VPN 客戶端軟體提供「自動更新」功能，讓遠端電腦的 Cisco VPN 客戶端軟體能夠自動進行版本升級。

點對點 Site-to-Site VPN

使用 Cisco ASA 5500 系列產品的標準化點對點 VPN 功能，企業可以透過低成本的網際網路連線，將網路安全地擴展到全球各地商務夥伴的營運點、遠端辦公室和小型分支機構。

- **最適合現今應用系統的 VPN 基礎架構**：Cisco ASA 5500 系列產品所提供的 VPN 基礎架構，能透過單一的安全 IPSec 網路，傳送整合式語音、視訊與數據，其強固的點對點VPN 支援能力，結合了強大的偵查功能、QoS、動態路由、狀態化故障網路備援（stateful failover）功能，讓企業能充分發揮整合式網路的各種效益。
- **強固的安全性與效能**：基於分公司與遠端辦公室可以將企業營運範圍延伸到重要的市場與地點。Cisco ASA 5500 系列產品的 VPN 方案，可在多個營運點之間建立安全的高速連線，提供企業通訊所需的效能、穩定性與可用性。

智慧型網路整合

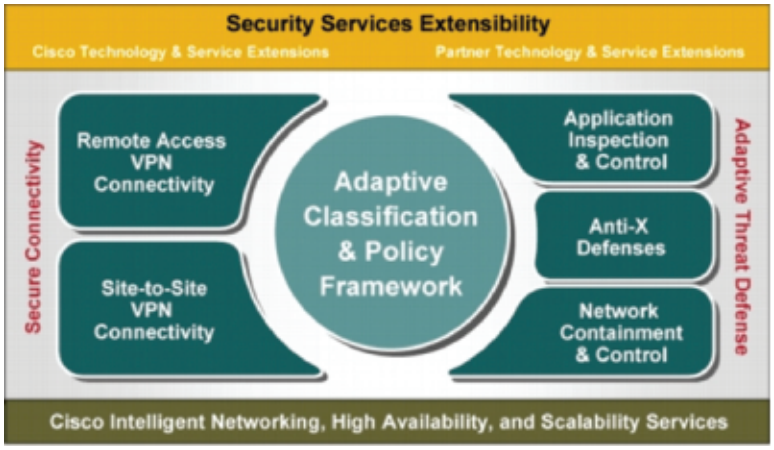
Cisco ASA 5500 系列產品發揮 Cisco 二十多年的網路技術領導優勢與創新技術，提供各式各樣的智慧型網路服務，完美地與現今多樣化的網路環境結合。其主要的網路整合服務包括：

- **Layer 2 通透式防火牆 (Transparent Firewall)**：可將 Cisco ASA 5500 系列設備快速地佈署到現有網路中，不需要變更任何網路位址，並且提供多項高效能隱藏式 Layer 2 – 7 的安全服務和防禦網路層攻擊行為的保護措施，並且與路由複雜、可用性高和多點播送的（multicast）環境加以整合。

- **服務虛擬化 (Services Virtualization)**：在邏輯上，可將一個 Cisco ASA 5500 系列設備切割成多個虛擬防火牆，每個虛擬防火牆都有自己的資安政策且分別進行管理。這種功能最適合企業將多個防火牆整合到單一 Cisco ASA 5500 系列設備當中，也很適合服務供應商應用於可管理防火牆 (managed firewall) 或主機代管服務。
- **支援標準 802.1q 技術的 VLAN**：可輕易整合至交換式網路環境中。
- **OSPF（Open Shortest Path First）動態路由服務**：可在數秒鐘之內偵測到網路故障點，並在進行路由傳送時特別避開，從而提高網路的永續性。
- **支援 PIM（Protocol Independent Multicast） Sparse Mode v2 以及雙向 PIM 路由功能**：可以安全傳送關鍵性、即時性的企業應用程式、協力運算應用程式、串流多媒體服務等等。
- **支援 IPv6**：可安全地佈署新一代 IPv6 網路，也可以部署需要 IPv4 與 IPv6 同步支援的雙重協定架構（dual-stack）混合環境。
- **服務品質（QoS）**：為了確保端對端的網路 QoS 策略，低延遲佇列（LLQ）與流量控管功能皆可支援對 QoS 需求較嚴格的應用程式，例如語音、視訊等等。使其相較於一般檔案傳輸和可容許延遲的資料流，可享有較高的優先權。
- **IP 電話自動配置（zero-touch provisioning）服務**：可協助電話登錄到正確的 Cisco CallManager 系統中，以簡化IP電話的佈署工作，並可下載任何額外的組態資訊與軟體映像檔。
- **高韌性架構**：可為企業提供 VPN 裝置叢集與狀態化 Active/Active 和 Active/Standby 的高可用性能，以達到最大的資料流量與網路正常運作時間。此外，Cisco ASA 5500 系列產品也支援「零停機軟體升級」，可在不干擾網路連線及運作的情況下，將更新版本的軟體安裝在一對互相備援的裝置上。其內建的動態負載平衡功能，可針對遠端存取 VPN 網路的佈署，提供高度的連線延展性及韌性。

獨特的「自適型威脅辨識與解除服務」架構

Cisco ASA 5500 系列產品透過其獨特的「自適型威脅辨識與解除」（AIM）服務架構，提供更高階的網路安全與策略控制（見圖一）。透過這套可自行設定的資料流導向安全政策，企業在 AIM 架構下可自行修改、延伸 Cisco ASA 5500 系列產品的安全服務設定檔。此外，這些可自行修改的資料流導向安全政策，不僅提供應用程式所需的安全性，更可透過使用者自行安裝的 SSM 模組，可擴充系統效能與安全服務。這套自適架構可讓企業根據本身的需求，隨時隨地佈署安全服務。例如，針對特定的應用程式或使用者需求，來修改檢測技術、或增添額外的入侵防禦及 Anti-X 服務，像是「自適型檢測與防禦安全服務模組」（AIP SSM) 模組所提供的服務。此外，AIM 架構可以整合未來新型的威脅辨識與解除服務，進一步延伸 Cisco ASA 5500 系列產品絕佳的投資保障，讓企業的網路防禦功能隨需提升，以抵禦新型威脅。



圖一：Cisco 自適型威脅辨識與解除架構

使用 Cisco ASA 5500 系列產品所提供的多功能策略框架，系統管理者可以調整策略的細節，指定哪些服務應用於哪些資料流。這些服務中內含三十多種不同的應用程式與通訊協定檢視引擎、QoS 策略、Anti-X 服務，以及其他的檢測服務與網路服務。這些策略可以根據多種不同的條件來制訂，例如網路位址、資料流類型、VPN 通道、應用程式或傳送目標等等。由於能根據不同的資料流選擇特定的安全服務或網路服務，因此安全服務的建構能更為精細，以支援特定的安全政策。

更低的佈署成本及營運成本

除了提高網路安全性之外，Cisco ASA 5500 系列產品也可以降低佈署與營運成本。具備廣泛的 VPN 和安全服務設定檔，讓單一裝置具備許多用途，因此平台與管理作業都能標準化。而且這套產品同時具備存取控制、應用程式的偵查功能和網路蠕蟲、病毒等惡意軟體的解除技術，故可作為整合式威脅防禦裝置。由於這套產品具有高延展性的點對點 IPSec 與 SSL 遠端存取 VPN 功能，因此也可以專門作為 VPN 終端裝置。此外，這套產品也很適合用於內部網路，提供部門與部門之間的存取控制，並防禦內部使用者無意間引入網路蠕蟲、病毒等惡意程式碼。在小型企業與分公司環境中，Cisco ASA 5500 系列產品可配合企業的預算與營運模式，提供完善的威脅防禦與 VPN 服務，作為一機多功能的全方位方案。這種「單平台、多用途」的自適設計，可減少企業佈署管理的平台數目，而在共通的作業環境之下，還可以簡化系統組態、監測、錯誤排除、以及資安人員的訓練工作。除此之外，Cisco ASA 5500 系列產品具備高度的網路感知能力，可在不干擾合法資料流及應用程式的狀況下，輕鬆地安裝在網路中，有助於進一步降低營運成本。

彈性化管理方案降低營運成本

Cisco ASA 5500 系列自適型安全裝置提供豐富的組態、監測、錯誤排除方法，企業可以根據本身的需求而彈性運用。為了支援一些遠端監測協定，例如 SNMP 與 syslog，其管理方案從政策式的中央管理工具含跨至整合式的網頁化管理功能。此外，這些設備還提供高達十六層可自訂的管理角色，企業可以針對每項設備，授予管理者與操作人員適當的存取權限，例如：只能進行監測、唯讀存取組態、只能存取網路組態、只能存取防火牆組態等等各種權限類別。

新一代集中管理方案

Cisco ASA 5500 系列設備採用 Cisco ASA 軟體 7.0 版，本系列設備可以透過 CiscoWorks VPN/Security Management Solution (VMS) 2.3 即將推出的更新版本來集中管理。這套富高延展性的新一代三層式管理方案，將包含下列特色：

- 完善的組態與軟體映像檔管理。
- 裝置管理具備階層性，可透過智慧型規則（Smart Rules）設定組態的繼承。
- 管理者角色與存取權限可自行修訂。
- 完善的企業變更管理與稽核功能。
- 具備智慧型安全政策與物件群組探索及其最佳化功能。
- 遠端 Cisco ASA 5500 系列設備享有全自動（Touchless）軟體映像檔管理。
- 支援動態定址的設備。

防禦攻擊與監測事件之解決方案

使用「Cisco 安全監測/分析/回應系統」(CS-MARS: Cisco Security Monitoring, Analysis, and Response System)，可以在商務及企業環境中，輕易而正確地辨識、管理並解除網路攻擊。CS-MARS 裝置能夠分析來自各種桌上型電腦、伺服器與網路安全方案中的安全事件、系統記錄（syslog）、NetFlow 資料等等，並研究其關聯性，以判定實際的攻擊路徑，提供防禦之道，進而簡化網安事件的管理。因此，即使沒有專責的網路安全分析師，網路環境也可安全無虞。

除此之外，Cisco 還提供 CiscoWorks 安全資訊管理方案（CiscoWorks SIMS）。這套管理方案非常適合大型企業與安全委外代管服務供應商，讓這些機構的專責安全分析師，能夠針對複雜的多品牌網路環境，進行深入的資料蒐集、調查分析、稽核與法規符合度、報告產生等等。

世界級裝置管理方案

整合式的 Cisco 自適型安全裝置管理員（ASDM: Adaptive Security Device Manager）提供世界級的網頁化管理介面，大幅簡化 Cisco ASA 5500 系列裝置的佈署、例行組態設定及監測工作。因此，系統管理者的電腦不需要加裝任何軟體，只要有標準的網頁瀏覽器及 Java Plug-In 即可。其智慧型設定精靈與 VPN 精靈，可以輕易整合到任何網路環境。其資訊監測功能包含一個儀表板與即時 syslog 檢視器，所以不論是重要裝置、網路的健康狀況，或是事件的監測，皆可一目了然。

除此之外，系統管理者也可以使用命令列介面（CLI），為在遠端的 Cisco ASA 5500 系列裝置進行組態設定、監測與除錯。其可透過多種方法達成存取命令列介面的安全性，包括 SSHv2 協定、Telnet over IPSec、或透過控制台連接埠（console port）進行存取。

Cisco ASA 軟體 7.0 版之功能與效益

Cisco ASA 5500 系列自適型安全裝置的 Cisco ASA 軟體 7.0 版，提供各式各樣的功能，表一簡單列出其主要功能，詳細的功能一覽表請參閱新產品發表註釋 (Release Notes)。

表一：Cisco ASA 軟體 7.0 版之功能與效益

功能	效益
應用程式安全服務	
進階應用程式的檢測與控制服務	• 30 種專業的偵查引擎，可為多種通訊協定提供豐富的應用程式控制與安全性服務，例如 Hypertext Transfer Protocol (HTTP)、File Transfer Protocol (FTP)、Extended Simple Mail Transfer Protocol (ESMTP)、Domain Name System (DNS)、Simple Network Management Protocol (SNMP)、Internet Control Message Protocol (ICMP)、SQL*Net、Network File System (NFS)、H.323 Versions 1–4、Session Initiation Protocol (SIP)、Cisco Skinny Client Control Protocol (SCCP)、Media Gateway Control Protocol (MGCP)、Real-Time Streaming Protocol (RTSP)、Telephony Application Programming Interface (TAPI) 以及Java Telephony Application Programming Interface (JTAPI) over Computer Telephony Interface Quick Buffer Encoding (CTIQBE) protocol、GPRS Tunneling Protocol (GTP)、Lightweight Directory Access Protocol (LDAP)、Internet Locator Service (ILS)、Sun Remote Procedure Call (RPC) 等多種協定。
進階網頁安全服務	• 針對網頁資料傳輸提供深入檢測服務，以精確控制 HTTP 傳輸階段、提高保護能力、防禦各式各樣的網頁式攻擊。 • 企業可精確控制何種資料流適用於何種 HTTP 指令與方法（例如：來自網際網路的資料流，與從測試網頁伺服器傳送到正式網頁伺服器的資料流，兩者適用不同的安全政策），這樣可以保護企業不受各種網頁式攻擊的侵害，例如網頁內容的非法刪除或修改。 • 提供各種額外的高功能 HTTP 安全服務，包括 RFC 規範、通訊協定異常偵測、通訊協定狀態追蹤、反應驗證、MIME 類別驗證與內容控制、URI 長度規範等等。
通道化應用程式控制	• 進階的偵查服務，可偵測即時傳訊（instant messaging）程式、點對點（peer-to-peer）檔案共享程式以及其他透過網頁程式通訊埠通道所傳輸的應用程式，並可選擇性地將其封鎖。 • 可封鎖一些流行的即時傳訊程式，例如 AOL Instant Messenger、Microsoft Messenger 以及 Yahoo Messenger。 • 可封鎖 KaZaA、Gnutella 等點對點檔案共享程式。 • 可封鎖 GoToMyPC 之類的通道化應用程式。
FTP 安全服務	• 提供進階的 FTP 偵查服務，包括支援通訊協定異常偵測、通訊協定狀態追蹤、網路位址轉譯（NAT）、通訊埠位址轉譯（PAT），以及動態通訊埠開關功能。 • 系統管理者更能充分控制各種 FTP 指令的使用，並透過安全設施來規範使用者及群組在 FTP 連線階段中執行作業的權限（例如 FTP 下載與上傳）。 • 伺服器混淆技術與額外的攻擊模式比對檔，可進一步保護FTP伺服器。
ESMTP 電子郵件安全服務	• 支援 ESMTP 安全偵查服務，包括通訊協定異常偵測、通訊協定狀態追蹤和以下支援 ESTMP 協定的新指令：AUTH、DATA、EHLO、ETRN、HELO、HELP、MAIL、NOOP、QUIT、RCPT、RSET、SAML、SEND、SOML、VRFY。 • 自動指令過濾功能，可保護企業不受惡意的 SMTP 及 ESTMP 指令攻擊。

功能	效益
SNMP 安全服務	• 提供 SNMP 過濾服務，系統管理者可以維持網路中流通的 SNMP 協定版本之一致性。 • 提供版本過濾功能。過濾所有流經 Cisco ASA 5500 系列裝置的 SNMP 資料流，並支援 SNMP v1、2、2c、3 的過濾。
ICMP 安全服務	• 提供 ICMP 連線的狀態追蹤服務，確保 ICMP 能在解決網路疑難功能中安全使用，並提升網路效能；另外也為 ICMP 錯誤訊息提供額外的控制項。
Sun RPC 與 NIS+ 安全服務	• 針對使用 Portmapper v2 或 RPCBind v3、v4 的 Sun RPC 與NIS+連線階段交易，提供狀態化偵查及NAT服務，以支援跳埠型（port-hopping）UNIX 應用程式。
3G行動無線網路安全服務	• 豐富的安全服務，應用於 GPRS 通道協定標準（GTP）提供封包交換式數據服務的 3G 行動無線網路環境。 • 進階的 GTP 偵查服務，可讓行動無線網路供應商與漫遊合作夥伴之間的互動更為安全。功能強大的過濾功能，可根據 GTP 專用參數來執行，例如國際行動訂戶身份（IMSI）字首、存取點名稱（APN）數值等等。 註：此項功能採獨立授權。
H.323安全服務	• 進階的 H.323 偵查服務，可支援 1~4 版的協定，並支援直接通話傳訊（DCS）與守門路由器控制傳訊（GKRCS），可以在各種 H.323 的 VoIP 環境中，提供彈性化的安全整合。 • 支援 H.323 服務的 NAT 與 PAT 功能，其中包括一些進階功能，例如 T.38 協定的 Fax over IP（FoIP）傳真功能。T.38 協定是一套用來定義即時傳送 FoIP 的 ITU 標準。
SIP 安全服務	• 強化的 SIP 偵查引擎，可以保衛 UDP 和 TCP 的 SIP 環境。 • 支援 SIP 形式的 IP 電話與應用程式的 NAT 與 PAT 位址轉譯功能，例如 Microsoft Windows Messenger 等等，同時也提供電話轉送、電話轉接等等進階服務。
SCCP 安全服務	• 安全地互相整合 Cisco 的 SCCP IP 電話服務和 Cisco CallManager v4.1，並跨越NAT與PAT界線，在多重協定的 VoIP 環境中接通電話。
MGCP 安全服務	• 提供豐富的 MGCP 安全服務與 NAT、PAT 位址轉譯服務，以進行媒體閘道器、通話代理器、媒體閘道控制器之間的 MGCP 連線。
RTSP 安全服務	• 為 RTSP 媒體資料流提供 NAT 位址轉譯服務，以提升即時網路環境的支援能力。
TAPI/JTAPI over CTIQBE 安全服務	• 可以偵查各種使用 CTIQBE 的 Cisco TAPI、JTAPI 應用程式，包括 Cisco IP SoftPhone 與 Cisco 客戶回應方案。
分段或分節的多媒體資料流檢視	• 可偵查已分段或分節的 H.323、SIP、SCCP 語音與多媒體資料流。
進階 TCP 安全引擎	• 支援多種基本功能，協助偵測協定層和應用層的攻擊。 • TCP 資料流的重組與分析服務，可協助偵測分散於一系列封包的攻擊。 • TCP 資料流正規化服務，可提供額外的攻擊偵測技巧，包括進階旗標與選項檢查、TCP 封包加總驗證、偵測重傳的封包中資料是否被竄改等等。

功能	效益
Anti-X 安全服務	
進階入侵防禦及 Anti-X 服務	• 提供進階的保護功能，防禦已知和未知的網路與應用層攻擊、DoS 攻擊、惡意軟體攻擊，其中包括網路蠕蟲、病毒、特洛伊木馬、間諜軟體、廣告軟體等等。 • 使用各式各樣的技術，精確分析網路資料流，偵測外來威脅。為偵測人為中介（man-in-the-middle）攻擊，這些技術包括：狀態化模式辨認、通訊協定分析、資料流異常偵測、通訊協定異常偵測，以及 Layer2 分析功能。 • 提供特殊的保全措施，可以「淨化」網路資料流，以免外來攻擊迴避系統偵測。這些保全措施包括：IP 分段重組與正規化、TCP 資料流重組與正規化、TCP 迴避控制、IP 防詐欺服務和 IP 解析（deobfuscation）服務等等。 • Here 採用 Cisco 創新的風險指數鑑定技術，在不影響合法的資料流情況下，適時阻止惡意攻擊。這套風險指數鑑定技術結合了四項衡量指標（事件嚴重性、特徵比對可信度、資產價值、攻擊相關性），精確決定特定事件的風險指數，以妥善執行系統管理者所指定的抵禦行動。 • 透過 Cisco 統合事件產生器，提供內建的事件關聯功能，達到快速辨識並封鎖新型威脅的成效，並且尚可選擇性地降低中央監測系統所需接收分析事件的數目。 • 在路由模式以及 Layer2 通透橋接模式中，可以只偵測外來攻擊，亦可線上即時防禦。 • 讓系統管理者能夠精確控制通訊協定，並提供自訂的常規表示（regular expression）比對工具，讓企業能自訂特定環境的比對資訊。 • 使用自動更新功能，從 Cisco.com 下載最新的系統威脅資訊（詳情請參閱「Cisco IPS 服務」）。 **註**：Cisco ASA 5500 系列設備需加裝 AIP SSM，才能提供上述功能。
多方位威脅防禦功能	• 包含各種技術，以防衛企業不受各種常見的攻擊，包括 DoS 攻擊、分段式攻擊、回覆攻擊、變形封包攻擊等等。 • 提供進階的攻擊防禦功能，以辨識多種類型的攻擊並加以封鎖，例如：DNSGuard、FloodGuard、FragGuard、MailGuard、IPVerify 與 TCP intercept 防禦功能。。 • 提供進階的 TCP 資料流重組與正規化服務，以協助偵測隱形的應用層與協定層攻擊。
URL 位址過濾功能	• 採用 Websense 與 Secure Computing/N2H2 技術，以整合 URL 過濾方案，提供強固的員工網頁使用管理及控制。 • 整合進階 Websense 功能，支援 HTTPS 和 FTP 網頁的過濾要求。
ActiveX 及 Java 過濾功能	• 可以選擇性過濾 ActiveX 和 Java applet，防止惡意軟體被下載而損害網路。
網路防禦及控制服務	
狀態化偵查防火牆服務	• 提供各式各樣的邊緣網路安全服務，避免網路被非法存取。 • 提供強固的狀態化偵查防火牆服務，追蹤所有網路的通訊狀態。 • 針對一百多種預先定義的應用程式、服務及通訊協定，提供彈性化存取控制功能，而且還可以自訂新的應用程式與服務。 • 支援網路介面、時間式存取控制清單、使用者規範、群組資安政策的內傳與外傳存取控制清單（ACL），以提高對網路及應用程式使用方式的控制。 • 簡化安全政策的管理，讓系統管理者能建立可重複使用、可參照多個安全政策的網路及服務物件群組，以簡化初期的資安政策制訂工作與後續維護政策的進行。

功能	效益
存取控制服務	• 可讓制訂存取控制政策的工作更富彈性，不僅能支援內傳的存取控制清單（ACL），也支援外傳的存取控制清單，讓網路資料流入或離開某個網路介面時，都受到存取控制的規範。 • 系統管理者能制訂時間式 ACL，指定哪些 ACL 項目應當作用，並針對某些 ACL 自訂時間範圍，以便更完整地控制資源的運用。 • 提供簡便的除錯工具，讓系統管理者無需刪除或更換 ACL 項目，即可測試、微調 ACL。 • 可以根據介面名稱而非 IP 位址來制訂安全政策；由於寬頻環境中的外部介面通常是採用動態 IP 位址，故這項功能在寬頻環境特別實用。 • 提供強大的報告及除錯功能，協助 ACL 數據的蒐集，以瞭解哪些 ACL 項目因為網路資料流試圖穿越某個安全設備而被啓動。 • 精確控制產生 ACL 項目相關的 syslog 事件。 • 使用者經過防火牆驗證身份之後，可以根據不同的使用者，動態下載並執行 ACL。
物件分組	• 系統管理者可將網路物件（例如裝置、網路及服務）分類成不同的邏輯群組，而大幅簡化存取控制規則的定義與維護。
NAT 及 PAT 服務	• 提供豐富的動態、靜態、策略式 NAT 及 PAT 服務。 • 簡化 Cisco ASA 5500 系列設備的佈署過程：在網路資料開始流動之前，不需要先設定位址轉譯規則；唯有真正需要位址轉譯的主機與網路，才需預設位址轉譯規則。
安全連線服務	
Cisco Easy VPN 伺服器與 IPSec 遠端存取集中器服務	• 領導市場的 IPSec 遠端存取 VPN 集中器服務，可同時支援高達 5000 個軟體式或硬體式的遠端 VPN 客戶端（採用 VPN Premium 使用許可的 Cisco ASA 5540 裝置）。 • 在連線時，可將VPN規則動態推廣到支援Cisco Easy VPN Remote 的方案（例如 Cisco VPN Client），因此無需個別管理每個客戶端，並確保客戶端能執行企業最新的 VPN 安全政策。 • 在收到 VPN 連線要求時，先檢查 VPN 客戶端的安全狀態，包括強制使用合法的主機式安全產品（例如 Cisco Security Agent）。 • 讓系統管理者能根據客戶端的種類與 VPN 客戶端軟體的版本，精確控制何種 VPN 客戶端可以連線（例如軟體客戶端、路由器、Cisco VPN 3002、Cisco PIX Security Appliance）。 • 可為 Cisco VPN 客戶端和 Cisco VPN 3002 硬體客戶端自動進行軟體更新。VPN 連線建立時可以誘發軟體更新，或針對已經連線的 VPN 客戶端之需要而進行更新。 • 延伸 VPN 功能到使用 NAT、PAT 的環境，支援 IETF UDP機制，並可安全穿越 NAT、PAT 介面，支援 Cisco TCP、UDP NAT 穿越方式。 • 系統管理者可以要求某個遠端 VPN 客戶端的所有資料流，都傳送到 Cisco ASA 5500 系列設備，讓來自遠端 VNP 客戶端存取用戶 VPN 通道的外傳網際網路資料流，都能經過原來進入的介面而離開（防火牆規則、URL 過濾規範以及其他政策檢查措施必須先選擇性地應用於此）。 • 支援 LZS（Lempel-Ziv Standard）壓縮法，以最佳化低頻寬連線的效能。

功能	效益
Cisco VPN 客戶端	• 免費內含一個無限使用的 Cisco VPN Client 授權許可，讓使用者能享用這套廣獲肯定、領導業界的產品。 • 適用於各種平台，包括 Microsoft Windows 98/ME/NT/2000/XP、Sun Solaris、Intel 架構的 Linux 版本與 Apple Macintosh OS X。 • 提供多種創新功能：支援 Cisco Easy VPN Server 的產品動態下載安全政策、故障時自動轉移到備援的 Easy VPN Server、系統管理者可自訂分配方式等等。 • 與榮獲大獎的 Cisco Security Agent 互相整合，提供完善的端點安全性。
WebVPN（SSL VPN）遠端存取集中器服務	• 只需使用網頁瀏覽器和瀏覽器內建的 SSL 加密功能，即可從任何上網地點，透過 SSL VPN 進行遠端存取連線。 • 讓遠端使用者無需依賴預先安裝好的 VPN 客戶端軟體，即能從不受企業管理的電腦存取網路資源，例如家用電腦、上網資訊站、無線網路上網點(hotspots)。 • 可同時支援高達 2500 個 SSL VPN 連線（採用 VPN Premium 使用許可的 Cisco ASA 5540 設備）。 • 系統管理者可以自訂遠端存取用戶的網頁介面。 • 透過簡單易用的網頁介面，提供 CIFS（Microsoft Windows）檔案共享存取功能。 • 透過執行精細的群組式存取控制，以限制使用者存取網路資源的權限。 • 透過 SSL VPN Port Forwarding Java applet 程式（系統需要執行 Sun Java Runtime Environment [JRE] 1.4 以上的版本），可以存取 TCP 應用程式，例如Telnet和Windows Terminal Services。 註：這個軟體版本的 WebVPN 功能目前採免費試用型態，未來的主要軟體更新版將需要購買並安裝 WebVPN 功能使用許可，才能使用這些 WebVPN 功能以及未來的 WebVPN 新功能。
遠端存取 VPN 叢集與負載平衡功能	• 透過內建 VPN 叢集與負載平衡服務，提高 IPSec 和 Cisco WebVPN 遠端存取的延展性與可靠性，而且還可加入 Cisco VPN 3000 Series Concentrator 叢集、或建立 Cisco ASA 5500 系列設備的叢集。
可和使用者身份驗證服務進行原生性整合	• 提供方便的 VPN 用戶身份驗證方式，與時下流行的身份驗證服務緊密整合，包括 Microsoft Active Directory、Microsoft Windows Domains、Kerberos、LDAP 和 RSA SecurID（不需要使用獨立的 RADIUS 或 TACACS+ 伺服器作為中介）。
點對點 VPN 服務	• 可將網路透過網際網路安全地加以延伸，與遠端網路之間有強固的資料私密性、資料完整性，以及身份驗證功能，並可同時支援 5000 個遠端連接點（採用 VPN Premium 使用許可的 Cisco ASA 5540 設備）。 • 支援網際網路金鑰交換（IKE）和 IPSec VPN 標準，採用輻射狀（hub-and-spoke）或網狀（meshed）VPN 組態。 • 點對點之間的 VPN 通道，支援 OSPF 動態路由與反向路徑插入（reverse-route injection），以提昇網路的可靠性與效能。
X.509 憑證與憑證取消清單（CRL）支援功能	• 搭配 Baltimore、Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA、VeriSign 的一流 X.509 解決方案，可支援簡易憑證登錄協定（SCEP）的登錄方式或採用手動登錄方式。 • 可支援 n 層憑證階層，且與大型 PKI 系統交互操作。 • 支援公鑰密碼標準（PKCS）#10 格式化憑證要求，能夠手動登錄 X.509 憑證單位。 • 可以透過 PKCS #7 手動匯入憑證，並可透過 PKCS #12 匯入具有私鑰的憑證。 • 支援各種長度的 RSA 金鑰，最高可達 4096 位元。 • 可支援 DSA 演算法的 X.509 憑證，金鑰長度可達 1024 位元。

功能	效益
高可用性服務	
Active/Standby 狀態化故障備援	• 可發揮 Cisco PIX Security Appliances 榮獲大獎的狀態化故障備援能力，確保企業網路環境的防護韌性。 • 兩個設定為互相備援的 Cisco ASA 5500 系列設備，會持續將本身的連線狀態與裝置組態資料同步化。如果系統或網路發生故障，網路連線階段會在防火牆之間自動轉移，使用者完全不會察覺。
Active/Active 狀態化故障備援	• 可和 Active/Standby 故障備援功能相輔相成。Active/Active 故障備援機制的兩套系統都會同時主動傳送網路資料，可讓突發性網路資料傳輸的流量加倍。 • Active/Active 故障備援機制的兩套系統會進行雙向狀態共享，故可支援不對稱路由結構的進階網路環境，在需要時，可讓資料流從一個 Cisco ASA 5500 系列設備進入，而從另一個設備傳出。
VPN 狀態化故障備援	• VPN 連線的新型 Active/Standby 狀態化故障備援功能，可發揮最高的 VPN 連線運作。 • 在互相備援的兩個裝置之間，同步化所有安全關聯狀態資訊和連線階段金鑰資料加以同步化，以提供高韌性的 VPN 方案。
以 LAN 為基礎之故障備援	• 兩個互相備援的 Cisco ASA 5500 系列設備可以位於不同地區。透過專用 LAN 連線，可以共享故障備援的資訊。
零停機軟體升級	• 企業為一對互相備援的 Cisco ASA 5500 系列設備進行軟體維護升級的同時，不會影響網路運作或連線。
智慧型網路服務	
安全環境設定組（Security Context）	• 單一 Cisco ASA 5500 系列設備可以設立多個安全環境設定組（虛擬防火牆），每個安全環境設定組都有自己一套安全政策、邏輯介面和系統管理領域。 • 支援四種授權等級的安全環境設定組：5、10、20、50（最高的安全環境數目乃根據 Cisco ASA 5500 系列產品型號）。 • 在每個虛擬環境都可以獨立管理的情況下，讓企業能簡便地將多個防火牆整合為單一的實體設備或故障備援配對。 • 服務供應商可透過一對互相備援的設備，提供高韌性的多租戶防火牆服務。 **註**：這項功能採獨立授權方式。
Layer 2 透通式防火牆	• 安全的 Layer 2 橋接模式佈署 Cisco ASA 5500 系列設備，為網路提供豐富的 Layer 2 到 Layer 7 防火牆安全服務，防火牆兩側的裝置也不會察覺。 • 無需重新定址受保護的網路，簡化了 Cisco ASA 5500 系列設備在現有網路環境中的佈署工作。 • 可針對 Layer 2 網路資料流，執行系統管理者定義的 Ethertype 存取控制策略，建立 Layer 2 的安全邊界。
VLAN 虛擬介面	• 可根據 IEEE 802.1q VLAN 標籤建立邏輯介面，並根據這些虛擬介面建立安全政策，讓安全政策的制訂更具彈性，簡化交換式網路環境的整體整合工作。 • 每個 Cisco ASA 5500 系列設備可提供多個 VLAN 幹道，並透過 VLAN 幹道功能，在單一實體介面上支援多個虛擬介面。 • Cisco ASA 5510 設備可支援 10 個 VLAN（採用 Security Plus 授權許可）；Cisco ASA 5520 設備可支援 25 個 VLAN；Cisco ASA 5540 設備可支援 100 個 VLAN。

功能	效益
OSPF 動態路由功能	• 在Cisco ASA 5500 系列設備上提供完整的動態路由服務，採用舉世聞名的 Cisco IOS 軟體。 • 透過快速路徑整合與安全有效率的路徑分配，提高網路的穩定性。 • 在使用 NAT 的環境中，提供安全的路由方案，與 Cisco ASA 5500 系列 NAT 服務緊密整合。 • 除了純文字 OSPF 身份驗證之外，也支援 MD5 的 OSPF 身份驗證，以防止路徑偽裝與各種路由式 DoS 攻擊。 • 在不同的 OSPF 程序之間重新分配路徑，包括 OSPF 路徑、靜態路徑和連線路徑。 • 在相同成本的多個路徑之間進行負載平衡。
RIP 動態路由功能	• 透過學習更新 RIP 協定 v1 和 v2 的路徑，安全整合於RIP的企業網路。 • 支援 RIPv2 的純文字身份驗證與金鑰式 MD5 身份驗證方式，以防止任何 RIP 的偵察行為。
多點播送（multicast）路由功能	• 透過支援 PIM Sparse Mode v2 與雙向 PIM 路由功能（根據 Cisco IOS 軟體的多點播送技術），讓多媒體資料流的傳輸更流暢，並有助於視訊會議、協力運算和關鍵性即時企業應用軟體的執行。 • 支援 IGMPv2 以及 Stub Multicast Routing 功能，包括 NAT、PAT 與建立多點播送資料流 ACL 的能力，有助於各種多點播送應用程式的執行。
QoS 服務	• 可針對個別資料流提供策略化 QoS 服務，支援 LLQ 與資料流控管功能，使不容許延遲的網路資料流可獲得較高優先權，並且讓系統管理者可以限制某些應用程式的頻寬使用量。 • 讓企業的延伸網路能擁有端對端的 QoS 策略。
IPv6 網路架構	• 支援雙重協定構架，為原生性 IPv6 網路與混合式 IPv4/IPv6 網路環境提供存取控制和深層封包檢視防火牆服務。 • 為採用 HTTP、FTP、SMTP、ICMP、TCP、UDP 協定的應用程式，提供 IPv6 的檢視服務。 • 可透過 IPv6 支援 SSHv2、Telnet、HTTP 與 HTTPS 和 ICMP 型式的管理。
每個網路介面的個別安全層級	• 發揮 Cisco PIX 安全設備的介面安全層級概念，簡化 DMZ 環境的佈署作業。 • 簡化 Cisco ASA 5500 系列設備在 intranet 環境的佈署作業，允許多個介面共享同等安全層級。系統管理者可以在不預設允許任何資料自動流通的情況下，針對相同安全層級的各個介面，自訂資料互相傳輸的安全政策。
DHCP 伺服器	• 在一個或多個介面提供 DHCP 伺服器服務，讓網路裝置能動態取得 IP 位址。 • 包含延伸模組，故可自動供應服務給 Cisco IP 電話和 Cisco SoftPhone IP 電話方案。
DHCP 請求代轉	• 可轉送內部裝置的 DHCP 請求到系統管理者指定的 DHCP 伺服器，有助於 IP 位址的集中分配、追蹤與維護。
NTPv3 客戶端	• 可以簡便化 Cisco ASA 5500 系列設備的時鐘與網路上其他裝置同步。
彈性化管理方案	
Cisco ASDM	• 可透過世界級的整合式網頁化使用者介面，簡易而安全從遠端管理 Cisco ASA 5500 系列設備. • 提供各種資訊化報表、即時報表與回顧性報表，充分瞭解使用趨勢、效能底線與安全事件。

功能	效益
命令列介面（CLI）	• 客戶不需要額外的訓練，只需運用現有的 Cisco PIX 安全設備及 Cisco IOS 軟體命令列介面命令列介面的知識，即可簡易地安裝並管理系統。 • 提昇使用指令完成、上下文感知式輔助說明、指令別名等服務的便利性。 • 可透過多種方式存取命令列介面，包括主控台連接埠、Telnet 以及 SSHv2。
Cisco 模組化策略架構	• 具有多功能、高彈性的架構，可針對資料流或等級制訂策略。系統管理者可根據多種不同的條件辨識網路資料流或等級，繼而針對每個資料流或等級，應用自訂的服務。 • 網路資料流或等級，有自己的防火牆、檢視策略、QoS 策略、連線限制與計時器等等，可提高對應用程式的控制。
身份驗證、授權與計費（AAA）服務	• 不論直接應用 TACACS+ 與 RADIUS，亦或間接應用 Cisco 安全存取控制伺服器（ACS），只需透過 Cisco ASA 5500 系列設備與本機使用者資料庫，或透過企業資料庫整合，便可紮實驗證使用者身份。 • 支援高達十六層可自訂的管理角色。企業可以針對每項設備，授予管理者與操作人員適當的存取權限，例如：只能進行監測、只能讀取組態、只能存取網路組態、只能存取防火牆組態等等各種權限類別。 • 能夠產生 TACACS+ AAA 記錄，以追蹤 Cisco ASA 5500 系列設備的系統管理存取狀況，與管理過程所做的所有組態變更。 • 可將計費資訊同時傳送到多個 RADIUS 伺服器。 • 外部 TACACS+ 伺服器或 RADIUS 伺服器故障時，系統管理者能退而求其次，動態使用本機使用者資料庫，以提高網路的韌性。
穿透代理服務	• 提供三種不同方式，選擇性地驗證使用者身份（可採用 HTTP、HTTPS 或 Telnet），因此可以先要求驗證使用者身份，而後才允許該使用者的資料通過 Cisco ASA 5500 系列設備。可使用 AAA 架構辨識使用者身份驗證來源，例如透過設備中的本機使用者資料庫進行驗證，或採用各種其他身份驗證服務（整合 TACACS+ 或 RADIUS）。
SNMP 監測功能	• 支援 SNMPv2 及 SNMPv2c，可深入檢視 Cisco ASA 5500 系列設備的狀態。 • 提供 64 位元計數器（以監測 Gigabit 乙太網路介面）等服務，並支援大量 MIB 資料傳輸。 • 支援許多 SNMP MIB，包括 SNMPv2 MIB (RFC 1907)、Interfaces Group MIB (RFCs 1573 與 2233)、IP MIB (RFC 2011) 以及 Entity MIB (RFC 2737)。 • 支援 Cisco IPSec Flow Monitoring MIB，可完整透視 VPN 連線狀態與每個通道的詳細數據，包括通道運作時間、已傳輸的位元組、封包數等等。
彈性化 syslog 與 SDEE 監測功能	• 透過管理主控台或外部 syslog 伺服器，可即時監測 Cisco ASA 5500 系列設備狀態。 • 可提供精確的 syslog 訊息時間戳記與計數，支援多個 syslog 伺服器，並可用 TCP 或 UDP 作為傳輸協定。 • 提供七個層級的 syslog 過濾功能，以配合各種企業規模的監測需求。 • 在設備上提供本機的訊息緩衝區，以確保重要訊息在網路繁忙時不致遺失。 • 可透過多種方式精確控制 syslog 訊息，包括變更 syslog 訊息的優先順序、可取消特定的 syslog 訊息、可根據特定 ACL 項目（ACE）來啓動或抑制記錄功能等等。

功能	效益
軟體與組態檔匯入/匯出	• 使用 TFTP、HTTP、HTTPS 或 SCP 協定，匯入組態檔與軟體檔，以快速進行服務供應及佈署。 • 可透過 TFTP 及 SCP 匯出組態資料，將組態儲存於裝置之外。
SSH 與 SCP	• 可使用 SSHv1 和 SSHv2 遠端管理 Cisco ASA 5500 系列設備，以提高與其他廠牌 SSH 工具的相容性。 • 支援 SCP 另一種可傳入/傳出 Cisco ASA 5500 系列設備中安全的檔案傳送方式，例如組態檔與軟體映像檔等等。
多重組態與軟體映像檔儲存於快閃記憶體中	• 系統管理者能進行組態還原，並可以在小巧的快閃記憶體中，儲存與使用多重組態與軟體映像檔。
安全地資產恢復功能	• 防止非法存取 Cisco ASA 5500 系列設備上敏感的組態資料、憑證與金鑰資料。如果執行資產復原或密碼重置程序，則快閃記憶體中的內容將自動刪除（但須預先完成以上的設定）。
系統重載預先排程	• 系統管理者可以預先排程 Cisco ASA 5500 系列設備何時重新載入（reload），可以指定特定時刻，也可指定多久之後才重載。這樣可以讓網路更容易排定停機時間，以通知遠端存取的 VPN用戶系統即將重開機。
專用頻外管理介面	• 企業可以比照 Cisco SAFE Blueprint 的說明建立最佳慣例。企業以頻外（out of-band）方式管理 Cisco ASA 5500 系列設備，將內建的高速乙太網路 10/100 管理介面只作為頻外管理介面之用。
封包捕捉功能	• Cisco ASA 5500 系列設備的每個介面都具備強大的封包捕捉功能，讓系統管理者能簡易進行除錯。 • 所捕捉的封包能透過多種方式加以存取，包括透過主控台、安全網頁存取、匯出到 TFTP 伺服器的檔案等等。
延伸 ICMP Ping 服務	• 支援 IPv6 位址和 ICMP 延伸選項以利除錯，選項包括：資料型態、DF 位元、重複計數、資料段（datagram）大小、逾時間隔、冗長輸出與各種不同的大小。
SMTP 電子郵件警示	• 提供一套便利的方式，當重大事件發生時，電子郵件警訊會傳送到系統管理者指定的電子郵件帳號，以通知系統管理者。

產品授權許可

Cisco ASA 5500 系列設備提供多種授權許可，其涵蓋的功能包括安全環境設定組、GTP 檢視功能、加密演算、增加 VPN 用戶端容量與平台功能。

功能授權許可

安全環境設定組授權許可

Cisco ASA 5520 及 5540 分別支援高達 10 個與 50 個安全環境設定組/虛擬防火牆 (Security Context/ Virtual Firewall)，而每個安全環境設定組都有其個別的安全政策與管理領域。這些設備包含兩個預設安全環境設定組，適用於 Active/Active 高可用性服務或虛擬防火牆服務。另外尚可選購各種層級的安全環境授權許可，分別為 5 個、10 個、20 個、50 個安全環境設定組。但 Cisco ASA 5510 並不支援這種授權型態及相關功能組。

GTP 檢視授權許可

Cisco ASA 5520 及 5540 可選購安裝 GTP 檢視授權許可，為 GTP 3G 行動無線網路環境提供進階安全服務。但 Cisco ASA 5510 並不支援這種授權型態及相關功能組。

加密授權許可

3DES/AES 加密授權許可

Cisco ASA 5500 系列產品支援兩種不同等級的加密演算。在預設情況下，所有的 Cisco ASA 5500 系列設備都支援 56 位元 DES、56 位元 RC4、512 位元 RSA 與 512 位元 DSA 加密演算法。此外，客戶還可選購強化的加密授權許可，以支援 168 位元 3DES、高達 128 位元的 RC4、高達 4096 位元的 RSA、高達 1024 位元的 DSA 加密演算法。客戶如果原先購買設備時，沒有訂購強化的加密授權許可，日後亦可從 Cisco.com 網站訂購。

平台授權許可

Cisco ASA 5510 自適型安全設備 Security Plus 授權許可

企業可選購 Security Plus 授權許可，安裝之後，Cisco ASA 5510 自適型安全設備的功能將大幅延展自適。這項授權許可會啓動第四個高速乙太網路通訊埠，並解除頻外管理埠的限制，讓這個管理埠可依照需要改為一般資料傳輸的通訊埠，以增加平台的通訊埠密度。這項授權許可也支援高達 10 個 VLAN，因此更容易與交換式網路環境整合。此外，升級使用許可之後，可大幅提昇企業永續性，不但提供 Active/Standby 高可用性服務，還將 VPN 容量增為三倍，同時再支援高達 150 個 VPN 連線，以供行動用戶、遠端據點、企業夥伴使用。

Cisco ASA 5520 自適型安全設備 VPN Plus 授權許可

企業可選購 VPN Plus 授權許可，將 Cisco ASA 5520 的 IPSec 與 SSL VPN 的容量擴展至超過兩倍以上，同時可支援高達750個VPN連線，以供行動用戶、遠端據點、企業夥伴使用。

Cisco ASA 5540 自適型安全設備 VPN Plus 與 VPN Premium 授權許可

欲延伸 Cisco ASA 5540 的 IPSec 與 SSL VPN 的容量，企業有多種選擇。若選購 VPN Plus 授權許可，可將平台的基本 VPN 容量增為四倍，同時支援高達 2000 個 IPSec VPN 連線與 1250 個 WebVPN 連線，以供行動用戶、遠端據點、企業夥伴使用。而 VPN Premium 授權許可，能發揮最高的平台 VPN 容量，其容量是基本平台的十倍，同時可支援高達 5000 個 IPSec VPN 連線與 2500 個 WebVPN 連線。

產品規格

表二到表四中列出 Cisco ASA 5500 系列設備與 VPN 客戶端、VPN 產品與某些加密標準之間的相容性。

Cisco VPN客戶端相容性

Cisco ASA 5500 系列設備支援多種軟體式/硬體式 Cisco VPN 客戶端，主要者列於表二。

表二：Cisco ASA 5500 系列設備與 VPN 客戶端之相容性

VPN 客戶端	所支援的版本
軟體式 IPSec VPN 客戶端	（略）
硬體式 IPSec VPN 客戶端（Cisco Easy VPN Remote）	

表三：Cisco ASA 5500 系列設備與 VPN 產品之點對點 VPN 相容性

VPN 閘道器	所支援的版本
Cisco ASA 5500 系列設備	（略）
Cisco IOS 軟體路由器	
Cisco PIX 安全設備	
Cisco VPN 3000 系列集中器	

所支援的加密標準

Cisco ASA 5500 系列設備支援多種加密標準與其他廠牌的相關產品服務（表四）。

表四：Cisco ASA 5500 系列設備所支援的加密標準與產品

加密標準	所支援的金鑰長度與雜湊大小
非對稱式（公開金鑰）加密演算法	• RSA 公開金鑰/私有金鑰組，512 至 4096 位元 • DSA 公開金鑰/私有金鑰組，512 至 1024 位元
對稱式加密演算法	• Advanced Encryption Standard (AES): 128、192、256 位元 • DES: 56 位元 • 3DES: 168 位元 • RC4: 40、56、64 以及 128 位元
Perfect Forward Secrecy (Diffie-Hellman 金鑰協商)	• Group 1: 768 位元 • Group 2: 1024 位元 • Group 5: 1536 位元 • Group 7: 163 位元(Elliptic Curve Diffie-Hellman)
雜湊演算法	• Message Digest Algorithm (MD5): 128 位元 • Secure Hash Algorithm 1 (SHA-1): 160 位元
X.509 憑證管理中心	• Baltimore UniCERT • Cisco IOS Software • Entrust Authority • iPlanet/Netscape CMS • Microsoft Certificate Services • RSA KEON • VeriSign OnSite
X.509 憑證登錄方法	• Simple Certificate Enrollment Protocol (SCEP) • 手動登錄 (PKCS #7 and #10)

系統需求

表五列出 Cisco ASA 5500 系列設備執行 Cisco ASA 軟體 7.0 版的系統需求。

表五：系統需求

系統需求	說明
所支援的平台	（略）
最小 **RAM** 數量	
最小系統快閃記憶體數量	
所支援的擴充卡	

訂購資訊

表六：如欲訂購，請參閱「Cisco 訂購網頁」或參見表六。

產品名稱	零件號碼
（略）	

下載軟體

請造訪「Cisco 軟體中心」下載 Cisco ASA 軟體（表七）。

訂購資訊

表七：Cisco ASA 5500 系列設備之軟體映像檔

產品名稱
（略）

服務與支援

Cisco 提供各式各樣的服務方案，以加速實現客戶的成功獲利。這些創新的服務方案結合了人力、流程、工具與合作夥伴，其獨特的組合，可讓客戶獲得最高的滿意度。Cisco 所提供的服務，協助您保障網路投資，使網路運作最佳化，讓您的網路能搭配新型網路應用，以延伸網路智慧，拓展您的商務優勢。關於這些 Cisco 服務詳情，請參閱「Cisco 技術支援服務」或「Cisco 進階服務」。關於 Cisco AIP SSM 所提供的 IPS 功能之相關服務，請參閱「Cisco IPS 服務」。

進一步詳情

如欲取得進一步詳情，請參閱下列網站：

- Cisco ASA 5500 系列自適型安全設備：http://www.cisco.com/go/asa。
- Cisco ASDM：http://www.cisco.com/go/asdm。
- CiscoWorks VMS：http://www.cisco.com/go/vms。
- Cisco Secure ACS：http://www.cisco.com/go/acs。
- Cisco 之 SAFE Blueprint：http://www.cisco.com/go/safe。

台灣思科系統股份有限公司
台北市敦化南路二段333號6樓B座
電話：(886)2-8176-7100
傳真：(886)2-8176-7199

思科系統高雄辦事處
高雄市三多四路110號19樓-2座
電話：(886)7-338-1092
傳真：(886)7-338-1094

若您欲進一步了解相關之資訊，請連結至台灣思科網頁查詢
www.cisco.com.tw