網路世界　需要整合式安全機制

Page 1

網路周邊安全（Perimeter Security）

網路周邊安全機制協助系統對重要應用服務與資料之存取控制，因此只有具權限的使用者與資訊才能在可信賴網域（trust domain）之間做連結動作。傳統上，防火牆即是被視為網際網路（不可信賴網路）與 DMZ（可信賴公眾網路），或是公司內部網路（可信賴私人網路）之間的周邊安全設備。而今，更廣域的網路周邊安全還包括存取控制表單（Access Control Lists；ACLs）與其他補充工具，例如：病毒掃瞄、內容過濾器等。我們將針對防火牆部分做進一步的介紹。

下圖為傳統三大介面防火牆的示意圖，包含三個最通用的可信賴網域。

防火牆並不僅限於網際網路的交會點與公司網路之間，實際上它的觸角可延伸至整個網路中。他可用來保護關鍵伺服器，例如 IP 電話伺服器或 DMZ 可信賴網域的外部伺服器，亦可將不同信賴等級的網域進行切割與分區，例如將鄰外（out-of-band）的網管網域從生產網路中區隔出來。當遠端使用者利用 VPN 連線的時候，防火牆亦能防止未被授權的連線發生。

PIX 防火牆管理

管理 Cisco 防火牆產品的方式有很多種，企業可依據自己的需求選擇最適合的管理方案。

PIX 防火牆能透過標準的瀏覽器介面，進行個別的組態設定與監控。PIX 設備管理軟體（PIX Device Manager；PDM）是一套以 JavaScript 開發的伺服器應用程式，可讓管理員控制個別的防火牆，並觀看其不同安全特性的使用報告。

如果公司有數量龐大的 PIX 防火牆，使用防火牆管理中心（Firewall Management Center）搭配自動更新伺服器（Auto Update Server），可從一個中心控制點來設定與維護數百個防火牆，即便這些防火牆不具固定 IP 位址。

最後，對於想透過策略伺服器（policy server）管理安全架構的公司，Cisco 安全策略伺服器（Cisco Secure Policy Manager；CSPM）是極佳的選擇。CSPM 集中控制支援 Cisco 安全產品組態設定的政策，包括 Cisco 安全 PIX 防火牆，與具 IOS 防火牆的 Cisco 路由器。透過使用策略管理員（Policy Manager），網路安全人員可為相關網路設備，將適當的策略定義至合宜的組態設定檔中，並可安全地將組態設定散佈至各安全裝置中。

為何需要 Cisco 網路周邊安全？
極高可用性 Cisco PIX 防火牆系列 UR515E、525 與 535 等型號，提供具成本效益與極高可用性。大致而言，以購買一個 UR 元件 1/4 的價錢，即可買下第二個 FO（FailOver）元件。FO 讓網路規劃者可盡量避免單一網路元件失效的情況，並可依據企業需求，

提供健全的網路安全設計。當使用區域網路時，FO 能得到和 UR 一樣的動態狀況表（dynamic state table），也就是說當其中一個元件失效時，並不會產生安全漏洞的疑慮。

戒備森嚴的網路週邊

每個 PIX 系列成員都具相同安全加值的特性。內建駭客入侵偵測系統（IDS）可防止來自非信賴網域的一般攻擊，而內建 VPN 功能則能確保企業之資料在非信賴網域傳送時的私密性。

擴充性與延展性

從 PIX501 到 PIX535，Cisco PIX 系列防火牆在價格與效能表現上雖略有不同，但都提供相同的企業安全特性。此外，PIX515E 能擴充到 6 個 FE 介面，PIX525 可擴充至 8 個，而 PIX535 更可擴充到 10 個介面，其中 2 個還可更換為 GE 介面。

Page 2

CiscoPIX 防火牆系列

Cisco PIX 防火牆不論在市場佔有率或是效能表現上，都已是排名第一的產品，也是 Cisco 自 1996 年來的安全旗艦產品。PIX 能決定所有通過網路的訊務是否合法，若是該訊務被判斷為合法，則該連線將幾乎不受到任何影響，反之，所有不合法的訊務將全部被摒除在外。

特性與好處

- **安全性**－Cisco PIX 防火牆採用堅實的安全設備與網路作業系統。許多競爭廠牌的防火牆僅建立多功能的一般作業系統，反而容易遭受網路侵害。

- **效能**－與其他防火牆產品相較，PIX 防火牆可應付多數倍的處理容量，並提供堅不可催的安全性，讓網路效能遭遇最小的衝擊。

- **穩定度**－因為 PIX 防火牆僅針對安全性設計，因此具有極穩定的特性。這對於在網路上扮演重要角色的設備是一項基本需求。而 PIX 防火牆發生錯誤的平均時間超過 6 年。

- **可擴充性**－PIX 平台適用於各種大小的網路裝設位置，小至辦公室、辦事處，大至全球企業總部。所有 PIX 平台皆執行相同的軟體，與使用相同的管理解決方案，以提供最大擴充整合性。

- **易於安裝與維護**－Cisco PIX 防火牆具有十分容易安裝與維護的特性，不需安裝額外的軟體與伺服器設定。

- **內建標準 VPN**－PIX 防火牆亦提供 IPSec 標準的 VPN 功能。除了這項市場領先的防火牆效能，PIX 防火牆同時提供端對端（site-to-site）與遠端存取的 VPN 功能。

優勢

- 控制整體成本的最佳選擇
- 整合式駭客入侵偵測系統（IDS）的最佳代表
- 可對特定的裝置卻又極廣的企業環境進行管理
- 防火牆設備最佳尺寸外型
- 良好支援服務
- 免費 VPN Client 軟體
- 極佳的錯誤移轉效能
- 全面整合的安全解決方案
- 防火牆快速流通率

	PIX 501	PIX 506E	PIX 515E-UR	PIX 525-UR GIG Enabled	PIX 535-UR GIG Enabled
市場	小辦公室 家庭辦公室	遠端辦公室	小型/中型 分公司	企業 商行	較大型企業 服務供應商
合法使用者數量	10 或 50 位	不限	不限	不限	不限
Max VPN 使用人數	5	25	2,000	2,000	2,000
尺寸（RU）	＜1	1	1	2	3
處理器（MHz）	133	300	433	600	1GHz
RAM（MB）	16	32	64	256	1GB
Max 介面	1 10BT + 4FE	2 10Base T	6	8	10
明文（Cleartext）（Mbps）	10	20	188	360	1.7 Gbps
3DES（Mbps）	3	16	63	70	95
介面數量	2 10baseT 4-port 交換器	2 10baseT	2 10/100 + 4 10/100	2 10/100 + 6FE/GE	2 10/100 + 8FE/GE
防火牆效能	10 Mbps	40 Mbps	180 Mbps	450 Mbps	1.7 Gbps
VPN（3DES）效能	3 Mbps	10 Mbps	63 Mbps	70 Mbps	90 Mbps
Failover	No	No	Yes, UR only	Yes, UR only	Yes, UR only
尺寸	Desktop	Desktop	1 RU	2 RU	3 RU

Cisco IOS 防火牆套件

Cisco IOS 防火牆提供先進防火牆功能並整合其他安全性技術，例如 VPN 網路 IPSec DES 加密、入侵偵測與授權認證。這套軟體是具附加性的模組，除可附加至 Cisco IOS 軟體中，還可附加於許多 Cisco 路由器與交換器上。因此，它大大提高了現存的安全功能，並充分利用內建於 IOS 軟體中之動態安全功能。

特性與優勢

- **內建式網路安全**－Cisco 將這項技術整合於網路作業系統中，而讓網路基礎變得更安全，也藉著增加網路基礎的安全性，Cisco IOS 防火牆改變網路安全市場，並提供非平行式整合。
- **彈性**－由於 Cisco IOS 防火牆能廣泛建置於 Cisco 路由器與交換器上，且先進的網路安全功能被設置在整個網路中。
- **利用現有網路建設的優勢**－Cisco IOS 防火牆能運作在 Cisco 網路裝置上，讓您將所有路由器與交換器轉換成安全平台。
- **整合 IDS 系統**－Cisco IOS 防火牆整合式駭客入侵偵測系統（IDS）技術，提供網路基礎建設額外的安全性。