



McAfee Firewall Enterprise

列出所有新威脅及弱點的特徵，一個不漏

McAfee Firewall Enterprise 功能 McAfee AppPrism™ 應用程式的可見性 與控制力包括：

- 封包、可設定狀態與完整應用程式篩選
- 完整的應用程式可見性與控制力
- 多種傳送選項，包括多重防火牆（一個裝置可管理高達 32 個虛擬防火牆）、McAfee Firewall Enterprise for Crossbeam 及虛擬防火牆裝置
- 網路位址轉譯 (NAT)

McAfee AppPrism 類別

- 匿名代理/Proxy
- 認證服務
- 商務 Web 應用程式
- 內容管理
- 商業監視
- 資料庫
- 目錄服務
- 電子郵件
- 加密通道
- 企業資源規劃 (ERP)/客戶關係管理 (CRM)
- 檔案共用
- 遊戲
- 即時傳訊
- 基礎架構服務
- IT 公用程式
- 行動軟體
- 點對點 (P2P)
- 相片/影片共用
- 遠端管理
- 遠端桌面/終端機服務
- 社交網路
- 軟體/系統更新
- 儲存裝置
- 串流媒體
- 工具列與個人電腦公用程式
- IP 網路語音電話 (VoIP)
- VPN
- Webmail
- Web 瀏覽
- 網路會議

與日俱增的企業應用程式與 Web 2.0 廣闊、日新月異的攻擊面，突顯出對新型防火牆安全性維護方法的需求。第一代防火牆的能力僅限於連接埠、通訊協定及 IP 位址。現在藉由 McAfee® 可靠的防火牆，您將可安心地控管新型與現有的應用程式，實作有效且高效率的規則。為了偵測這些應用程式內複雜的威脅，我們將主動式的威脅情報和多種檢查技術結合在一款經濟實惠且便於管理的裝置中。

傳統的防火牆強度取決於您定義的原則強度。然而對於當今複雜的 Web 2.0 流量來說，有效的安全性原則必須能鉅細靡遺地剖析流量，使威脅難以滲透。您需要在極短的時間內，除了連接埠與通訊協定之外，廣泛透析各項資訊，才能妥善保護各式的 Web 應用程式和使用者，並箝制鎖定這些目標的精密威脅。

在過去，您能等待特徵碼發佈以獲取所需的保護；然而在今天，若要應付一日千里的威脅演變速度，您需要主動、預測式的風險診斷。我們應該要評估諸如來源信用評價、內容及行為等多種屬性，才能趕在確認新威脅之前揭露惡意的企圖。

儘管如此，具備威脅預測的能力並不足夠。而精確、及時的封鎖能力需綜合多種傳統產品的功能才能實現。這些需求 (另外再加上必須驗證法規遵循的狀況) 都會增加網路團隊的營運負擔。不過預算依然吃緊，因此我們必須要改變。

近 15 年來最關鍵的防火牆革新

McAfee 推出的第 8 版 McAfee Firewall Enterprise，提供革命性的防火牆。三項創新功能可提供前所未有的保護，價格卻經濟實惠。我們結合了完整應用程式可見性與控制、信用評價感知威脅情報及多方位攻擊防護，除了能提升網路安全性之外，也能縮減花費的心力與費用。

此防火牆解決方案包含 McAfee Firewall Enterprise 裝置與 McAfee Firewall Enterprise Control Center 集中管理功能。

當今網路安全中最弱的一環是應用程式層。我們採用本公司經過證實且高度可靠的防火牆 (受到全球極安全環境的信任)，並加入了豐富的應用程式探索與控制功能。您現在可以保護全新與既有的 Web 2.0 應用程式，預防資料外洩、網路濫用及惡意攻擊等風險。在 McAfee 技術的協助之下，您可以確定使用網路的應用程式是在為公司賺取利潤。

應用程式可見性

McAfee AppPrism 技術可讓您識別所有流量及判斷確實在使用中的應用程式，並能提供如來源、頻寬及目的地等有用的內容。您可以檢查加密的應用程式層流量，以消除可能遭受網路竊賊與攻擊者利用的漏洞。

應用程式控制功能

您可依據業務需求，精確地控制以全面性強制執行原則。您現在可以為使用者名稱設置角色與一組應用程式，而不僅只是比對 IP 位址、連接埠或通訊協定的原則。

McAfee Firewall Enterprise 功能 (續) 驗證

- 本機
- Microsoft Active Directory
- 適用於 Active Directory 的透明身分識別 (McAfee Logon Collector)
- LDAP (Sun、OpenLDAP、Custom LDAP)
- RADIUS
- Microsoft Windows 網域驗證
- Microsoft Windows NTLM 驗證
- Passport (單一登入)
- 增強式驗證 (SecurID)
- 支援 CAC 驗證

高可用性

- 主動/主動
- 主動/被動
- 可設定狀態的工作階段容錯移轉
- 遠端 IP 監視

Global Threat Intelligence

- McAfee Global Threat Intelligence™ 網路連線信用評價
- 地理位置篩選
- McAfee Labs™

加密應用程式篩選

- SSH
- SFTP
- SCP
- 雙向 HTTPS 解密與重新加密

入侵防禦系統 (IPS)

- 超過 10,000 個特徵碼
- 自動更新特徵碼
- 自訂攻擊特徵
- 預先設定的特徵碼群組

防毒與防間諜軟體功能

- 抵禦間諜軟體、特洛伊木馬程式及蠕蟲
- 啟發式
- 自動更新特徵碼

Web 篩選

- 整合式的 McAfee URL 篩選與管理
- 封鎖 Java、ActiveX、JavaScript、SOAP

防垃圾郵件

- McAfee Global Threat Intelligence 網路連線信用評價

VPN

- IKEv1 與 IKEv2
- DES、3DES、AES-128 及 AES-256 加密
- SHA-1 與 MD5 驗證
- Diffie-Hellmann 群組 1、2 及 5
- 受原則限制的通道
- NAT-T
- Xauth

制訂結合以下屬性的應用程式使用規則：

- 業務或休閒性質
- 使用者身分識別
- 內嵌應用程式控制
- 白名單
- 地理位置

使用者身分識別

若無法深入瞭解及掌握使用者與使用內容，防火牆便無法抵禦連接埠機動力、迴避性及鎖定能力漸強的應用程式。McAfee Firewall Enterprise 能套用具有使用者感知能力的規則，並能控制應用程式。

當使用者連線時，系統會立即從現有的使用者目錄驗證權限，因此防火牆能迅速套用和使用者身分識別相對應的規則，以授與明確的應用程式使用權限。

因為追蹤使用者，規則的精細度便足以應付當代的營運作業。此外，以身分識別為基礎的規則也比較能符合營運的需求。因此，有越來越多的企業仰賴一致的使用者目錄與身分識別管理來支援存取控制。由於當使用者變更發生後隨即會傳播出去，所以安全性原則也會不時隨著使用者社群變更而更新。

內嵌應用程式控制

內嵌應用程式控制可讓您擁有調整應用程式權限的能力。例如，您可以允許 Yahoo!，但封鎖 Yahoo! 即時傳訊；或只允許特定使用者群組使用即時傳訊，例如客戶支援或銷售部門，或特定地點的人員 (如總部辦公室)。

您也可以藉由指定應用程式的使用時段來支援企業的適當使用與禁用原則。例如，規定允許客戶服務團隊於午餐時間使用 MySpace，並禁止任何人員週末時透過 VPN 使用財務應用程式。

有許多攻擊會將酬載隱藏於新潮的 Applet 之中，以侵入安全性鬆散的社交網站。有了 McAfee 之後，您可以允許存取如 Facebook 等網站的便利元素，同時降低威脅侵入應用程式的風險。

白名單

在進階控制能力方面，應用程式白名單可讓您明確地只針對核准為必要或適當的應用程式，允許該應用程式的流量。相較於冗長的黑名單，白名單的編列只需要撰寫及維護較少的規則數量。

地理位置

由於殭屍網路能透過熱門的社交網路應用程式迅速蔓延，因此能鎖定嘗試和特定位置通訊之惡意應用程式日漸成為不可或缺的能力。本產品可讓您設定地理位置，阻斷這類型的惡意傳播，預防資料外流及避免系統遭到濫用。

在簡化規則開發的同時，我們也提供這類型的精細控制。事實上，每個視圖中都只有一項原則。簡單扼要的主控台會呈現有效管理所有規則及提升防禦能力所需的選項。由於我們同時也強調規則互動性和重疊性，從長期及跨團隊流通的角度來看，這項整合式的操作模式更顯得格外具有優勢。我們利用彩色的欄位來標明潛在的衝突，使您得以預防錯誤並提升效能。

保護

McAfee AppPrism 除了能讓您降低應用程式層威脅的風險，同時還能最佳化企業頻寬的使用情形。McAfee AppPrism 技術來自強大的 McAfee Labs™。我們的威脅研究人員可持續辨識及評估 31 種類型應用程式的風險，利用威脅研究與情報資料來評斷從 Anonymizer 到影片與相片共用等應用程式的風險。

我們會動態地指派信用評價給網站、寄件者及位置，平均能在您發現前預先封鎖 70% 不需要的流量。這項功能甚至能協助本產品找出殭屍網路 (Botnet) 中難以察覺的命令與控制 (C&C) 通道。

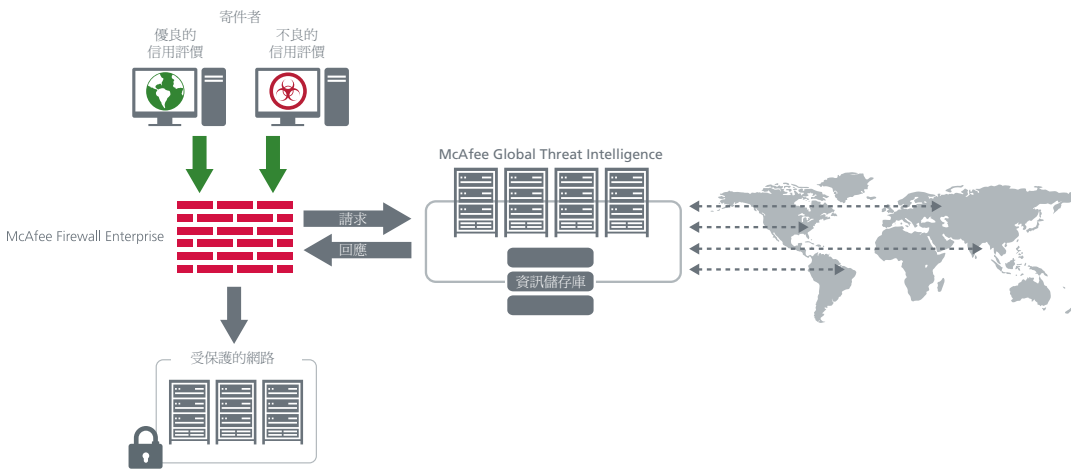


圖 1：採用 McAfee TrustedSource™ 的 Global Threat Intelligence 能依據信用評價來允許或封鎖流量。

唯一能提供信用評價分析與全球威脅情報的防火牆

唯有 McAfee 能將信用評價技術加入防火牆內，而這僅僅只是 McAfee Global Threat Intelligence™ 的其中一環。在 McAfee，我們有 400 名以上的安全研究員協力研究 Web、垃圾郵件、弱點、主機與網路入侵、惡意軟體及法規遵循等主題。如此廣泛的研究讓研究人員得以刻畫出每項新威脅與弱點的特徵。

他們的資訊來自全球超過 1 億台偵測器，而他們的努力則成就了協助您抵禦不斷演變之多面向威脅的即時預測風險分析。

不像傳統仰賴特徵碼的防火牆，來自 McAfee Labs 的自動威脅情報使防火牆無須離線即可取得最新的資訊。隨著如 Operation Aurora 等先進持續威脅的數量不斷增加，McAfee Global Threat Intelligence 是市面上最精密的防護，它能協助您降低弱點風險、避免違反法規，以及減輕修補的成本負擔。

將多方位的安全性融入一個整合式的裝置

眾多客戶選擇 McAfee 的其中一個原因在於我們具備廣博的安全性與法規遵循產品系列。現在，我們提供您這些強大的功能。McAfee Firewall Enterprise 現在將多個關鍵的威脅防護加入各個防火牆裝置中，以對付 Web 2.0 應用程式中的複雜威脅（混合型入侵攻擊、網路釣魚及目標性攻擊）。

在此之前，防火牆的作用不外乎是存取控制與分段。若要取得適當的保護，您就必須要為實作及維護數個單獨的產品而付出昂貴的代價。現在，只要一項裝置就能讓您獲得：

- McAfee AppPrism 完整的應用程式探索與控制功能
- 入侵防禦
- 全球信用評價分析
- 領先業界的 McAfee URL 篩選
- 加密應用程式篩選
- 防毒、防間諜軟體與防垃圾郵件功能

根據先前建構多方位解決方案的經驗，我們能在不需犧牲效能或生產力的情況下提供以上所有保護，也不需要收取額外的費用。

McAfee SecureOS® 作業系統

功能

- McAfee Type Enforcement® 技術
- 預先設定的作業系統 (OS) 安全性原則
- 作業系統區隔
- 網路堆疊分離

McAfee Firewall Enterprise Control Center

- Windows 圖形使用者介面
- 本機主控台
- 完整命令列
- USB 災難復原組態備份與還原

記錄與監視

- 本機系統記錄
- 排程的記錄封存與匯出
- McAfee Firewall Enterprise 記錄軟體擷取格式 (SEF)
- 匯出格式 (XML、SEF、W3C、WebTrends)
- Syslog
- SNMP v1、v2c 及 v3

網路與路由

- 符合 IPv6 規範
- 動態路由 (RIP v1 與 v2、OSPF、BGP 及 PIM-SM)
- 靜態路由
- 802.1Q VLAN 標記
- DHCP 用戶端
- 預設路由容錯移轉
- 服務品質

Secure 伺服器

- 安全 DNS (單一或分散)
- 安全 sendmail (單一或分散)

裝置與硬體

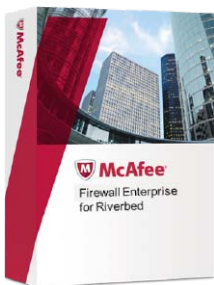
- 大部分的機型可供升級為 4 小時回應保固等級
- 提供虛擬化解決方案
- 單核心、雙核心及四核心處理器
- ASIC 加速
- RAID 硬碟組態
- 備援電源供應

技術支援

- 全天候電話技術支援
- 全天候 Web 型票證與知識庫技術支援

McAfee Firewall Enterprise 產品系列

Firewall Enterprise 產品系列含有適合各種規模之企業使用的裝置，以及 McAfee Firewall Enterprise Control Center 等附屬產品。本公司的 Control Center 與 Firewall Enterprise 裝置能搭配運作，以簡化管理活動的複雜度及縮減營運成本。彈性的混合式傳送選項包含實體裝置、多重防火牆裝置、虛擬裝置。運行於 Crossbeam X 系列硬體上的 McAfee Firewall Enterprise for Crossbeam 解決方案可提供速度達 40 Gbps 的電信業級安全性效能。請洽詢銷售代表以取得更多資訊。



保護虛擬基礎架構安全的虛擬防火牆

可管理的精細控制

可靠的安全性也必須具備易於設定的特性。此直覺式的 McAfee Firewall Enterprise 管理主控台可讓您的管理員從單一畫面建立規則，以及選擇性地套用如應用程式篩選、IPS 特徵碼及 URL 篩選等防禦功能。新軟體功能更新會透過網際網路自動傳送，可減少維護的人力。只要按一下滑鼠按鈕決定排程即可。

McAfee Firewall Enterprise 產品系列包含其他簡化管理作業的工具。McAfee Firewall Enterprise Control Center 是另行販售的產品，能為多個 McAfee Firewall Enterprise 裝置提供集中式的防火牆原則管理能力。它能協助您大幅提升營運效率、簡化原則控制、最佳化規則、精簡軟體更新作業及展示法規遵循。您甚至可以比較所有受 McAfee Firewall Enterprise Control Center 管理之裝置的原則組態，確保在整個網路中達到一致性。健全的組態管理功能可讓您集中追蹤、追溯及驗證所有原則變更。

除此之外，若將 McAfee Firewall Enterprise Control Center 和 McAfee ePolicy Orchestrator® (McAfee ePO™) 整合，便可深入掌握防火牆健康狀態資料與報告。

最安全的防火牆硬體平台

McAfee Firewall Enterprise 的核心運行著高速、高度可靠的 McAfee SecureOS 作業系統。取得專利的 McAfee Type Enforcement 技術保護著作業系統本身，提供無可比擬的平台安全性。這也是為什麼 McAfee SecureOS 能成就卓越的 CERT 建議記錄：從不需要任何緊急安全性修補程式。

預先設定的作業系統安全性原則可預防入侵，且整個作業系統已和外界區隔，因此攻擊者無法干擾作業系統的運作。

這些額外的措施使我們的防火牆成為第一個榮獲 Common Criteria EAL 4+ 認證及符合美國國防部保護設定檔規範的防火牆。

由於我們的創新與先進的安全性，McAfee Firewall Enterprise 目前已在全球保護 15,000 個網路，包括數千個政府機構、Fortune 500 (財星 500 大) 組織，以及前 10 大財務機構中的七個機構。立即使用 McAfee 來保護您的系統吧！



Crossbeam X 系列防火牆效能最高達 40 Gbps



硬體規格 ¹	S1104	S2008	S3008	S4016	S5032	S6032	S7032-XX
外形係數	小型 1U	1U	1U	企業級 1U	企業級 2U	企業級 2U	企業級 2U
無限使用者授權	是	是	是	是	是	是	是
建議的使用者人數	200	300	600	中等 - 大量 ³	中等 - 大量 ³	大型 ³	大型 ³
RAID	不適用	不適用	不適用	是	是	是	是
網路模組上限	不適用	不適用	不適用	1	3	3	2 ⁴
1 Gb 銅介面 (基本/最大)	4	8	8	8/16	8/32	8/32	8/16 ⁴
1 Gb 光纖介面選項 (最大)	不適用	不適用	不適用	8	24	24	8 ⁴
10 Gb 光纖介面選項 (最大)	不適用	不適用	不適用	6	18	18	4 ⁴
加密式篩選加速	不適用	不適用	整合式	整合式	整合式	整合式	不適用
頻外管理 (狀態、溫度、電壓、開啓/關閉等)	僅限序列主控台	僅限序列主控台	是	是	是	是	是
法規遵循	BSMI (台灣)、MIC/KCC (韓國)、C-Tick (澳洲/紐西蘭)、VCCI (日本)、FCC (美國)、UL (美國)、CSA (加拿大)、ICES (加拿大)、CE (歐盟)、GOST (俄羅斯)、CCC (中國)、SABS (南非)、IRAM (阿根廷)、NOM (墨西哥)						
效能¹							
防火牆效能 (最大) ²	750 Mbps	2 Gbps	4 Gbps	9 Gbps	12 Gbps	15 Gbps	12 Gbps
威脅防護 ²	250 Mbps	1 Gbps	2 Gbps	3 Gbps	5 Gbps	6 Gbps	5 Gbps
McAfee AppPrism ²	250 Mbps	1 Gbps	2 Gbps	7.5 Gbps	10 Gbps	12 Gbps	10 Gbps
並行工作階段 ²	200,000	500,000	750,000	1,500,000	3,000,000	4,000,000	3,000,000
每秒的新工作階段數 ²	5,000	15,000	20,000	35,000	50,000	70,000	50,000
IPSec VPN 輸送量 (AES) ²	60 Mbps	250 Mbps	350 Mbps	400 Mbps	450 Mbps	500 Mbps	450 Mbps
IPSec VPN 最大通道數目 ²	250	1,000	2,000	4,000	8,000	10,000	8,000
尺寸、重量、環境							
寬度	16.9 吋 42.93 公分	16.9 吋 42.93 公分	16.9 吋 42.93 公分	17.2 吋 43.8 公分	18.9 吋 48.04 公分	18.9 吋 48.04 公分	18.9 吋 48.04 公分
長度	8.5 吋 21.59 公分	28.0 吋 71.12 公分	28.0 吋 71.12 公分	24.4 吋 61.87 公分	30.0 吋 76.21 公分	30.0 吋 76.21 公分	30.0 吋 76.21 公分
高度	1.7 吋 4.32 公分	1.7 吋 4.32 公分	1.7 吋 4.32 公分	1.7 吋 4.32 公分	3.4 吋 8.71 公分	3.4 吋 8.71 公分	3.4 吋 8.71 公分
重量	10.93 磅 4.96 公斤	25 磅 11.34 公斤	25 磅 11.34 公斤	22 磅 9.98 公斤	40 磅 18.14 公斤	40 磅 18.14 公斤	40 磅 18.14 公斤
電源供應器詳細資料	100 W 110/220 V	350 W 110/220 V	350 W 110/220 V	雙 400 W 110/220 V	雙 750 W 110/220 V	雙 750 W 110/220 V	雙 750 W 110/220 V
運作溫度	10° C - 35° C	10° C - 35° C	10° C - 35° C	10° C - 35° C	10° C - 35° C	10° C - 35° C	10° C - 35° C

- 1 所有規格和效能結果都是以 S 系列裝置為準。
- 2 第 8 版的效能資料表示在最佳測試情況下測得的系統能力上限。部署與原則上的因素均會影響效能結果。
- 3 請連絡 McAfee 代表以判斷最符合需求的大小。
- 4 最多支援兩個網路模組 (任何類型)；最多支援一個 10 Gb 的網路模組 (最多填入四個收發器)。

