

FIREWALL-1

Secure Virtual Network Architecture

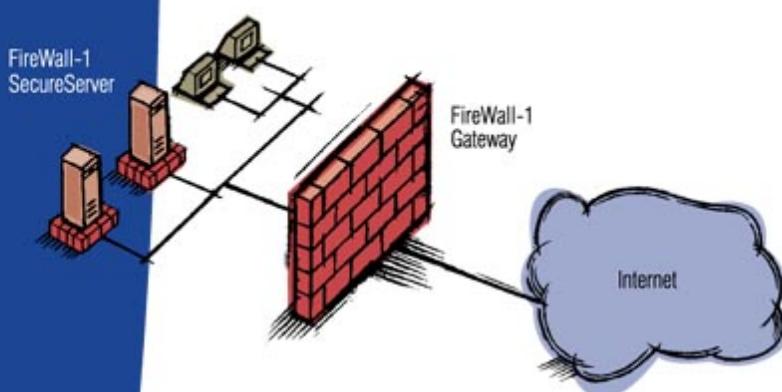
DATA
SHEET

挑戰

網路技術的發展，重新定義了企業、顧客與經銷商之間的溝通與關係建立的方式，而且形成一股真正的商業變革。正當企業手擁網路建立新的商業模式時，網路安全也頓時成為最重要的一項課題。為了維繫與合作夥伴及客戶的信任，企業不僅必須提供重要應用程式、資料、及其它資源的存取功能，同時必須保障企業內包括網路、作業系統、應用程式、網際網路、區域網路、以及區外網路所有使用者的安全。

解決方案

Check Point Software Technologies開發了先進的網路安全解決方案：FireWall-1。FireWall-1提供企業完備的網路安全功能，它整合了存取控制、認證機制、網路位址轉譯(NAT)、內容保全、稽核等多項功能，同時還可以讓企業建置單一、完整的保全策略，以保護企業內所有的網路應用資源。FireWall-1採用三層式架構，與Stateful Inspection專利技術，結合開放式網路安全平台Open Platform for Security(簡稱為OPSEC)，是一項極具擴充性的解決方案，且可整合集中管理網路安全的各項重要功能。FireWall-1超強的自訂組態能力，提供強大的保全功能，同時擁有自選作業平台的能力，以符合您企業的所有特殊需求。



FireWall-1可輕易地應用於整個網路架構內，以保障企業整體的安全。

產品特點

- 提供強大的存取控制、認證機制、文件保全及其它多項安全功能
- 整合各項保全管理功能，包括VPNs、NAT、QoS、及個人化防火牆等
- 集中管理並自動部署安全策略
- 支援開放式作業平台，並可整合硬體式防火牆
- 結合Check Point的SecureXL效能技術

產品優點

- 確保電子商務最高的安全性
- 簡化安全管理
- 建立精良的安全策略以應用至整個企業環境
- 擁有最大的彈性，以符合所選用的硬體作業平台
- 擁有multi-gigabit防火牆效能

保全執行重點

存取控制

FireWall-1採用Check Point開發的Stateful Inspection狀態式封包過濾技術，在不使用代理伺服器時，即可提供應用層（Application-layer）的安全控制。它可支援超過150種以上預設的應用程式、服務、與通訊協定，如HTTP、SMTP、FTP、及telnet等最常用的應用程式。除此之外，FireWall-1除可支援如Oracle SQL重要的商用程式，以及如Real Video與Windows Media等多媒體程式外，亦可支援類似透過IP與NetMeeting傳輸語音的H.323服務。

認證(Authentication)

在允許他人存取敏感的網路服務時，企業必須先確認使用者的身份後，才能允許存取的動作。Check Point的開放式架構，可以將多種認證方式整合在企業的網路安全政策上，如FireWall-1的密碼、Smart Card智慧讀取卡、SecureID、LDAP-stored密碼、RAIDUS或TACACS+認證伺服器、與X.509數位簽章等token型式的認證產品。

網路位址轉譯

(Network Address Translation，簡稱NAT)

透過簡便的網路位址轉譯機制，FireWall-1可以隱藏內部網路的位址，以防止外界透過網路侵入內部資訊。Check Point的NAT機制結合Stateful Inspection技術，可提供企業最安全的位址轉譯功能，並可支援多項網路服務。FireWall-1可依據網路管理者或經理人員於設置主機、網路、與閘道（Gateway）時的組態資訊，自動產生固定與動態兩種轉譯規則。NAT機制可以讓企業用以維護非固定的IP位址，並可以讓任一個企業IP位址上的使用者，來存取網際網路。

內容保全

Check Point FireWall-1透過內容保全的整合功能，可以保護使用者避免電腦病毒、惡意的Java及Active applet程式攻擊，並防止不必要的文件傳播。您可透過FireWall-1 Security Server來建立任一HTTP、SMTP、或FTP連線，並且有效掌控任一資源存取的細節。舉例來說，您可以控制使用存取特定的網頁、限制FTP檔案的操作（例如PUT或GET指令）、SMTP特定的表頭欄位（header fields）等。

支援Third-Party應用程式

透過OPSEC架構的支援功能，Check Point FireWall-1可以運用數個開放式API界面，用以結合其它廠商的內容保全程式。如此可以讓管理者擴充FireWall-1的安全性，並可提供更多的功能，例如防毒監控、URL過濾功能（filtering）、與Java程式保全等。

惡意攻擊活動偵測

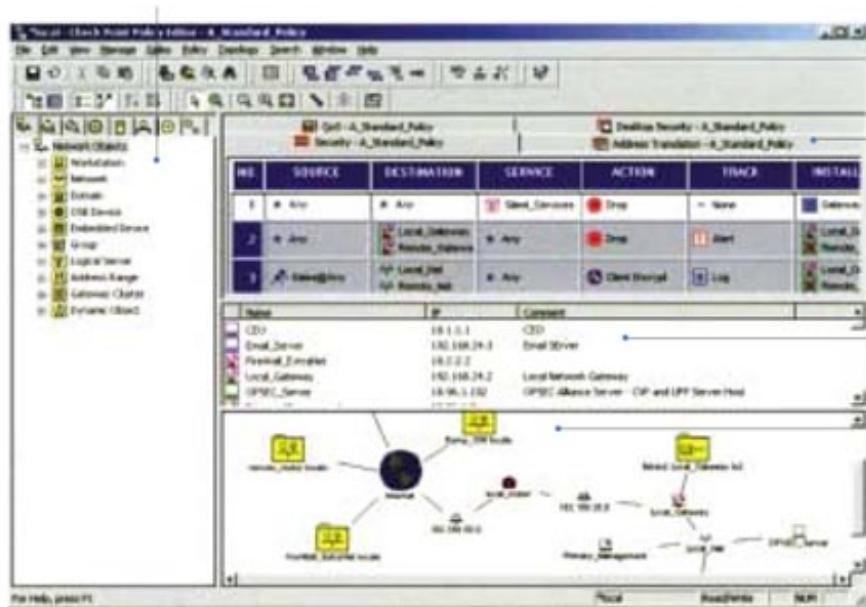
FireWall-1可以監測網際網路閘道上的惡意攻擊活動，並警告安全管理員，可能影響網路安全策略的變動。惡意攻擊活動偵測的功能是分析FireWall-1的記錄檔，以偵測一般網路攻擊或指出可疑的攻擊活動。

企業管理

管理控制台(Management Console)

Check Point的直覺式管理控制台提供圖形化使用者界面，用以定義與管理Secure Virtual Network的多重元件：包括防火牆安全、VPNs、網路位址轉譯、服務品質（QoS）、與VPN客戶保全。為有效建立保全策略與保全管理，所有應用程式均可分享全部的物件定義（包括使用者、主機、網路、服務等）。

管理者可以利用FireWall-1 提供的SecureUpdate功能來集中管理分散各地的防火牆，用以降低IT人員的負荷。您可選用SecureUpdate模組來追蹤軟體的版本資訊，並針對執行重點與其它廠商的OPSEC產品，自動進行主要元件的更新與服務套件的安裝，如此可讓管理者更輕易掌控整體安全環境。



所有物件均可透過Object Tree來管理，如網路、使用者等

透過政策清單可管理安全、VPN、NAT、QoS、與桌面保全（Desktop Security）

您可以在物件清單中輕易地應用最常用的物件

視覺化政策編輯器（Visual Policy Editor）可提供詳細的架構圖

FireWall-1管理控制台

FireWall-1集中管理的方式，可輕易地讀取任何資訊，來簡化保全的設定作業。

視覺化政策編輯器

視覺化政策編輯器是FireWall-1管理控制台的選用功能，它可以提供管理者詳細的物件配置架構圖（例如防火牆、VPNs、伺服器、網路等）。管理者可以選定物件的位置、編輯物件、並描述安全策略規則。管理者可應用視覺化政策編輯器，來進行安全規則的確認，並在取得或提升安全性的同時，簡化管理負荷。

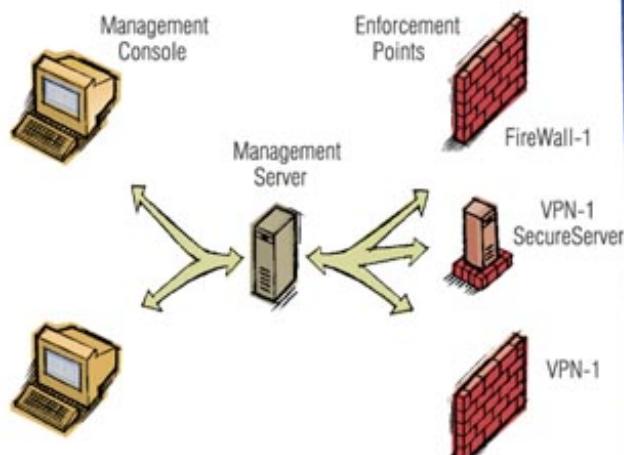
記錄與報表

FireWall-1的圖形化記錄檢視器（Log Viewer）可即時提供FireWall-1各個執行重點上連線的追蹤、監測與統計資訊。除此之外，記錄檢視器也會記錄管理人員的動作，例如更改物件定義或規則，如此可大幅降低排除組態設定錯誤的時間。管理人員可以搜尋或過濾登錄紀錄，以便快速地找尋或追蹤特定的事件。在發生攻擊或可疑的網路活動時，管理人員可以利用記錄檢視器，暫時或永久中斷特定IP位址的連線。

管理者可選用報表模組（Reporting Module）來詳細報告FireWall-1的記錄內容，它可將記錄轉換為決策管理報表，並以簡單、直覺化的表格與圖形，來顯現所須要的資訊。您可以應用預設或自訂的報表範本，來建立各種報表。

三層式架構(Three-tier Architecture)

FireWall-1適用任何規模的網路安全管理，小至一般辦公室，大到全球分布的企業網路。FireWall-1使用獨特的三層式架構，單一的企業保全策略，不但可集中管理，並可自動應用於無限多個FireWall-1上。FireWall-1自動化的政策派送機制，可在管理數個防火牆時，有效減少組態設定錯誤的可能性。



三層式的管理架構—使用者界面、管理伺服器與防火牆建置點—相互整合，可提供優越的組織規模擴張性與管理能力。

優越的效能與應用能力

現今的防火牆必須擁有gigabit的效能，以防折損安全功能。Check Point結合SecureXL結合數種創新的加速技術的安全效能架構，可產生優越的效能。SecureXL API包含於精良的架構中，可將大量的安全作業卸載至開放式的界面上，以進行硬體加速或軟體最佳化的動作，來提升效能。Check Point與它的協力廠商提供了許多SecureXL驅動的加速產品，可同時提供開放式伺服器、與整合gigabit等級以上的效能。

精密的負載平衡(Load Sharing)與Fail Over

ClusterXL是一項可供選用的SecureXL模組，它可用來解決所有閘道流量負載。由於各種網路流量都分布在防火牆閘道的叢集(cluster)上，當加入更多的閘道叢集時，則會獲得線性的效能增益。另外，所有狀態表(state-table)之間的內容資訊是持續同步化的，當某一個閘道無法工作時，所有新增或正在進行中的連線將被重導至現有的閘道叢集上，在fail-over的期間並不會有任何漏失的連線。

安全VPN(Virtual Private Network)的基礎

Check Point在先進的VPN解決方案應用FireWall-1的安全平台，整合網路安全與VPN功能，可以避免因為開放防火牆上連接埠、或「漏洞」而造成盲目地允許VPN連線通過的情形發生。此外，所有FireWall-1上的安全規則設定均可套用到VPN的連線上，以確保網路安全的完整性。

您可以輕易地將FireWall-1升級為VPN-1，或是選擇同時購買VPN-1與FireWall-1的整體解決方案。

系統需求

您可以在不同的平台上執行FireWall-1以符合您的需求—如硬體式防火牆，開放式的Linux、Unix與Windows伺服器平台。

規格

管理伺服器與防火牆執行模組

作業系統	Windows 2000(SP0與SP1) Windows NT 4.0(SP4~SP6a) Windows XP Server Sun Solaris 7(32-bit mode only) Sun Solaris 8(32-或64-bit mode) Red Hat Linux 6.2、7.0
硬碟空間	40 MB
記憶體	128 MB
網路介面	ATM Ethernet Fast Ethernet FDDI Gigabit Ethernet Token Ring

管理控制台

作業系統	Windows 2000、98、ME、NT、XP Sun Solaris SPARC
硬碟空間	40 MB

記憶體 128 MB

FireWall-1可支援Windows、Linux、Solaris與其它作業系統；或與硬體廠商設計的硬體式防火牆整合在一起。企業主可以將FireWall-1應用於外部或內部的網路閘道上，或應用FireWall-1 SecureServer來保護單一且重要的應用程式伺服器。

SVN(Secure Virtual Network)架構

所有Check Point產品採用SVN架構，以提供國際網路、區域網路、外部網路的保全，以及使用者、網路、作業系統、應用程式之間的完全連結。您可向世界各地的Check Point經銷商與服務廠商取得Check Point SVN解決方案的相關資訊。若要更詳細的資訊，請至www.checkpoint.com網站上查詢。

精誠公司為Check Point 全球ATC認證課程

台灣地區原廠獨家授權代理

 精誠資訊股份有限公司

SYSWARE CORPORATION

台北總公司：台北市羅斯福路二段100號17樓

電話：02-23686171 傳真：02-23686172

高雄分公司：高雄市新光路38號12樓之6

電話：07-5379288 傳真：07-5379299

網址：<http://www.sysware.com.tw>

企業網路安全專業網站：

<http://www.secum.com.tw>