Symantec™ Network Security 7100 Series

主動式的入侵防禦裝置可抵禦已知與未知的攻擊，保護重要網路的安全性

「縱深防禦」的需求

安全人員的任務在於確保企業內重要資料的可用性。企業內可能已經任用了非常專業的人員，但這些員工往往會為了日復一日的資安事端分析、資安事端回應、套用或測試修正程式，以及試圖預防可能發生的入侵事件而疲於奔命。同時，他們也必須面對日益增加的威脅，以及建立有效安全措施與控管機制的壓力。企業不僅需要維護及善用現有的安全防護機制，更需要具備持續主動監控、資安情報蒐集與分析能力。Symantec Network Security 7100 系列是一可簡化部署、集中管理與全面支援「縱深防禦」的網路安全解決方案。

主動式的入侵防禦

Symantec Network Security 7100 系列硬體裝置提供即時、主動式的網路入侵防禦，以保護企業網路，並可有效降低已知與未知 (或初始) 攻擊和病蟲造成的商業損失。

- **「單鍵防禦」(One-Click to Prevention)**：只需按一下滑鼠即可由偵測模式轉換為入侵防禦模式。這樣的轉換適用於任何網路拓蹼，並可針對所防護的網段進行調整。
- **在線部署選項 (Inline deployment option)**：可根據企業安全政策與業務營運需求，精準的警示或攔截威脅。在線模式的系統失效自動繞道備援選項可確保網路連線不被中斷。
- **高可用度/自動備援 (被動監聽模式)**：透過高可用度部署可達成不受中斷的網路監控，若主要裝置故障，備用的 Symantec Network Security 裝置可自動接手進行防護。
- **支援非對稱式路由環境**：介面群組 (Interface Grouping) 可以對非對稱式路由網路環境，進行攻擊偵測。
- **易於維護**：可根據企業需求與部署架構，選擇不同的設定。透過 Compact Flash 的讀卡機可彈性而簡單的進行設定，並可還原與備份系統組態。

* 僅適用於 Symantec Network Security 7160 與 7161 型號

重要功能

- 強化現有閘道與伺服器的安全防護，防止威脅經由網路進行擴散與滲透
- IMUNE 基礎架構結合多種偵測技術，包括通訊協定異常偵測與弱點攻擊攔截等重要技術，可精確地辨識與攔截已知及未知的攻擊和病蟲
- 協助企業建立、評估與掌握資安最佳實務準則施行與遵循程度
- 整合「賽門鐵克安全機制應變中心」的專業知識與服務，針對威脅提供早期預警，使企業組織擁有主動式的安全防禦機制
- 易於部署，不需重新設定網路即可進行安裝
- 最多可支援八個介面，讓企業得以監控更多的網段
- 有三種硬體型號可供選擇，支援 50 Mbps 至 2Gbps 的網路傳輸效能，可符合分公司、銷售點與網路骨幹的連線需求
- 「自動防護」(AutoProtect) 功能，使用 Live Update 技術自動更新防護政策，以協助組織有效防禦各類威脅
- 「單鍵防禦」只需按一下滑鼠即可由偵測模式轉換為入侵防禦模式

網路威脅防禦架構

Symantec Network Security 7100 系列硬體裝置運用創新的「整合式入侵防禦引擎」(Intrusion Mitigation Unified Network Engine, IMUNE)。

- **IMUNE 系統**：可偵測病蟲、掃描、探測、DoS 攻擊、後門程式、緩衝區溢位攻擊與分散封包攻擊等已知及未知威脅的防禦技術。
  - 通訊協定異常協定偵測：不須根據已知或公開的漏洞即可偵測攻擊。
  - 弱點攻擊攔截：防護已知與未知 (或初始) 的病蟲與駭客攻擊程式，可精確的辨識已公開的漏洞。
  - 流量偵測 (流量規則)：網路行為與使用政策違規偵測功能，可用來偵測違反企業網路使用政策的行為。
  - 即時通訊與點對點通訊偵測：偵測即時通訊及 P2P 通訊。
  - IPV6 通道 (Tunneled) 流量辨識：偵測經由網路傳輸的 IPv6 通道流量，以偵測可能的政策違規或入侵行為。
  - 強化攻擊特徵描述語言：更精確而有效率的偵測攻擊與威脅。

彈性化的企業部署架構

7100 系列提供三種型號，可彈性化的進行入侵防禦部署，以符合企業的部署需求，兼顧分公司、銷售點或網路骨幹的需求。

- **高度擴充性**：最多可監控八個網段，支援 50Mbps 至 2Gbps 的網路流量。
- **網路介面選擇**：企業可為網路骨幹選擇使用纜線或光纖介面。
- **部署選項**：支援多個在線模式配對介面 (inline pairs)，可於同一裝置同時監控被動式 (passive) 與在線模式 (Inline) 網段。
- **延伸式入侵防禦**：可動態更新 Symantec Enterprise Firewall 與 Symantec Gateway Security 5400 的防護規則，以建置最佳的網路邊界防禦。

智慧型安全內容與更新

整合「賽門鐵克安全機制應變中心」與 Symantec DeepSight™ 早期預警服務的技術，以及簡單易懂的安全準則，針對安全資安事端做出更快速的回應。

- **LiveUpdate™ 的防護資料更新**：LiveUpdate 會自動更新防護政策，協助組織防範持續演進的威脅。
- **「賽門鐵克安全機制應變中心」的安全更新**：隨著威脅的變化，企業隨時都可受到全年無休的「賽門鐵克安全機制應變中心」提供的安全防護。

完善的管理介面

完善的管理可協助組織建立、評估與掌握最佳的企業安全實務準則。

- **強大而彈性的政策管理**：允許安全人員根據其安全政策與業務運作需求，量身訂制安全防護機制，並為每一個裝置設定共用或個別的偵測與防禦政策。
- **記錄、攔截與自動回應機制**：可在被動監控模式中設定忽略、警示及自動回應網路安全事件，或於在線防禦模式 (inline prevention mode) 中攔截網路安全事件。
- **內定安全防護政策**：可根據威脅類別、嚴重性、意圖、可靠度及受防護的對象調整或直接套用內定的安全防護政策，以符合企業安全防護的需求。
- **爆發新威脅時，可自動更新安全政策**：不需手動執行，即可自動攔截新興與即將出現的威脅。
- **Symantec Network Security Management Console**：透過硬體裝置與管理主控台之間的安全通訊，以提供集中式的管理，並可擴充以支援分散式的大型企業部署。
- **彈性化的角色權限控管**：擴充式的管理，可定義管理使用者，並賦與不同的存取權限。
- **企業報表功能**：提供摘要到詳細的事件細部報告等多層式的報表，讓安全人員有效評估與掌握網路安全基礎架構的整體防護成效。

即時威脅分析

Symantec Network Security 7100 系列產品會蒐集整個企業中，由多個感應器所獲得的威脅資訊，並能夠迅速且自動的掌握攻擊趨勢及辨識相關事件。

- **可自訂的事件關聯性分析**：可大幅減少安全人員辨識威脅所投入的精力，讓他們得以將更多時間運用在更複雜的入侵研究與系統修復，以協助管理員更有效率的進行安全管理工作。
- **封包及連線內容的擷取與重播功能**：可深入分析相關事件。

可對多種產品提供入侵管理

Symantec Network Security Smart Agent 可對賽門鐵克及協力廠商的主機與網路安全防護產品進行事件蒐集、彙整並有效回應安全事件，以提供企業全面性的多重入侵管理。若能迅速辨識整個企業的多重威脅，可讓企業有效降低對重要資訊資產可能造成的潛在損害。

symantec™

裝置型號比較

規格	7120	7160	7161
效能			
IDS 整體效能	最高 200 Mbps	最高 2 Gbps	最高 2 Gbps
在線模式整體效能	最高 150 Mbps	最高 1.25 Gbps	最高 1.25 Gbps
最大同時連線數	100,000	1,000,000	1,000,000
每秒連線數	1,500	12,500	12,500
擴充性			
網路介面	4 10/100 銅線通訊埠	8 10/100/1000 銅線通訊埠	4 10/100/1000 銅線通訊埠 4 1000 Base-SX 光纖通訊埠
在線模式可支援網段數	2	4	4
管理介面	1 10/100 纜線連接埠	1 10/100/1000 纜線連接埠	1 10/100/1000 纜線連接埠
TCP 重設介面 (僅供被動式監控)	1 10/100 纜線連接埠	3 10/100/1000 纜線連接埠	3 10/100/1000 纜線連接埠
介面群組 (僅供被動式監控)	是 (最多 4 個介面)	是 (最多 4 個介面)	是 (最多 4 個介面)
高可用度			
電源供應	單一	雙重備援	雙重備援
裝置故障偵測	是	是	是
網路連結訊號偵測	是	是	是
磁碟機	固定式	抽取式	抽取式
被動模式容錯移轉	是	是	是
在線模式系統失效自動繞道 (Fail-open)	是[1]	是[1]	–[2]
管理			
讀卡裝置	是	是	是
集中化管理 (主控台)	是	是	是
Live Update 功能	是	是	是
單鍵防禦	是	是	是
實體與操作			
型式	1u rack-mountable (符合 19 吋機架)	2u rack-mountable (符合 19 吋機架)	2u rack-mountable (符合 19 吋機架)
高度	5.08 公分 (2 吋)	8.89 公分 (3.5 吋)	8.89 公分 (3.5 吋)
寬度	43.18 公分 (17 吋)	43.18 公分 (17 吋)	43.18 公分 (17 吋)
深度	43.18 公分 (17 吋)	61 公分 (24.0 吋)	61 公分 (24.0 吋)
重量	8.62 公斤 (19 磅)	16.33 公斤 (36 磅)	16.33 公斤 (36 磅)
電源	100-240 伏特, 50/60Hz 最大 430 W, 190 W Draw	100-240 伏特, 50/60Hz 最大 800 W, 240 W Draw	100-240 伏特, 50/60Hz 最大 800 W, 240 W Draw
操作環境	5º C 至 35º C (41º F 至 95º F) 5% 至 95% 相對溼度，不凝結	5º C 至 40º C (41º F 至 104º F) 5% 至 95% 相對溼度，不凝結	5º C 至 40º C (41º F 至 104º F) 5% 至 95% 相對溼度，不凝結
非操作環境	-10ºC 至 70ºC (14ºF 至 158ºF) 5% 至 95% 相對溼度，不凝結	-20ºC 至 60ºC (-4ºF 至 140ºF) 5% 至 95% 相對溼度，不凝結	-20ºC 至 60ºC (-4ºF 至 140ºF) 5% 至 95% 相對溼度，不凝結
操作海拔	最高 3000 公尺 (10,000 呎)	最高 3000 公尺 (10,000 呎)	最高 3000 公尺 (10,000 呎)
安規	UL and CSA - UL 60950 VCCI, CE / FCC part 15B, Class A EN60950 (2000) EN609825-1 (1994+A11)	UL and CSA - UL 60950 VCCI, CE / FCC part 15B, Class A EN60950 (2000) EN609825-1 (1994+A11)	UL and CSA - UL 60950 VCCI, CE / FCC part 15B, Class A EN60950 (2000) EN609825-1 (1994+A11)
電磁輻射	EMC Directive 89/336/EEC Low Voltage Directive – 73/23/EEC , both as amended by 93/68/EEC	EMC Directive 89/336/EEC Low Voltage Directive – 73/23/EEC , both as amended by 93/68/EEC	EMC Directive 89/336/EEC Low Voltage Directive – 73/23/EEC , both as amended by 93/68/EEC

[1] 提供外接式系統失效自動繞道裝置
[2] 於 Q4 2004/Q1 2005 提供外接式光纖介面系統失效自動繞道裝置

系統需求

SYMANTEC NETWORK SECURITY 7100 系列

Symantec Network Security 7100 系列硬體裝置是整合式的在線式安全裝置，因此不需要額外的軟體與硬體。

SYMANTEC NETWORK SECURITY MANAGEMENT CONSOLE 4.0

- Intel® Pentium® 或相容的處理器
  - 1.6GHz 或更高
- 作業系統
  - Microsoft Windows 2000 或 XP、Red Hat Enterprise Linux 3.0 ES
- 記憶體
  - 最低 256 MB (建議使用 512 MB)
- 磁碟空間
  - 50 MB 安裝空間，安裝後 100 MB
- 螢幕解析度
  - 1024 x 768 或更高
- Java
  - Sun Java™ 2 Runtime Environment (J2RE) 1.4.2 版