IBM 安全性網路非法入侵預防系統

對當今不斷進化發展的威脅提供全方位的保護

產品特性

- ***無與倫比的效能，保持安全性防護的深度和廣度***
- ***保護企業的網路、伺服器、桌上型電腦及應用程式等重要資產不受惡意威脅***
- ***保護網站應用程式不受資料隱碼攻擊 (SQL injection) 和跨網站指令碼的攻擊***
- ***使用整合式資料遺失防止 (DLP) 監控您網路的資料安全性風險***
- ***避免網路濫用與資料遺失傳送即時訊息和進行點對點 (P2P) 檔案分享***
- ***由世界知名 IBM X-Force® 研究團隊所提供的成長性防護，始終在威脅發生前「先發制人」***
- ***透過整併單點解決方案及整合其他安全性工具來降低成本與複雜性***

IBM 安全性網路非法入侵預防系統 (IPS) 的設計，是要在您的企業受到影響之前阻止網際網路威脅。IBM 提供的先行保護功能，可以透過其專屬的線路速度效能組合、安全性智慧及提供安全性整合的模組化保護引擎，在威脅發生之前即賦予保護。藉由整併對資料安全性及網站應用程式保護的網路安全性需求，IBM 安全性網路 IPS 可以做為一安全性平台，用於減少部署及管理單點解決方案成本與複雜性。

企業在評估入侵預防的技術時，通常很難在以下的六個關鍵領域當中找到平衡點和最佳選擇：效能、安全性、可靠度、部署、管理和信心。

IBM 安全性網路 IPS 針對這六個領域提出各項解決方案，包括業界領先的效能、由 X-Force 研究團隊提供先行威脅防護的技術、高度的可用性、簡化的部署與管理，以及世界級 IBM 客戶支援所帶來的信心。如果企業組織有意將網路防護這個重擔交給可信任的安全性夥伴，可以託付 IBM 來幫忙管理其安全性基礎建設。IBM 的客戶也在評估、設計、部署、管理及教育上從各種配套諮詢服務中獲益。

提供卓越的效能，絕不妥協

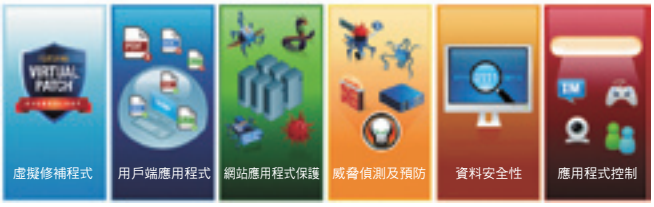
網路的效能應該隨著安全性的加入提升，而不該隨之降低。為此應運而生的 IBM 安全性網路 IPS 解決方案，提供有效維護網路操作所需的高傳輸量、低延遲時間及最高的可用性。這個解決方案包含使用全方位安全性防護的能力，並可讓使用者不用再為了維持關鍵商務應用程式的服務水準，而在最高等級的安全性和需要的效能間加以取捨。提供超越 20Gbps 的穩定傳輸量、效能領先業界的 IBM 安全性網路 IPS 解決方案，不僅提供您需要的效能，同時也提供高度的安全性。

整併網路安全性與先行保護功能

IBM 安全性網路 IPS 解決方案擁有模組化的產品架構，可以針對與日俱增的威脅加入全新的保護模組，藉此推動安全性整合 (security convergence)。這種模組化的產品架構，可以解決各種來自蠕蟲和僵屍病毒對網站應用程式與資料安全性問題所造成的安全性風險，並且讓 IBM 安全性網路 IPS 解決方案可以針對業務持續運作、資料安全性及法規遵循的需求提供保護。

IBM X-Force 研究和開發團隊設計出 IBM 通訊協定分析模組 (PAM)，並且提供維護先行威脅保護的內容更新。特定的保護模組包含：

- *IBM Virtual Patch® 技術－獨立於軟體修補程式之外，防護弱點暴露。*
- *用戶端應用程式保護－保護終端使用者對抗鎖定每日所使用應用程式的攻擊，例如 Microsoft Office® 檔案、Adobe® PDF 檔案、多媒體檔案和網頁瀏覽器。*
- *先進網路保護－先進的非法入侵預防功能，包括 DNS 保護。*



IBM 通訊協定分析模組 (PAM) 技術推動安全性整合 (security convergence)，可提供超越傳統 IPS 的網路保護，其中包含用戶端應用程式保護、資料安全性、網站應用程式保護及應用程式控制。

- *資料安全性－未加密個人可識別的資訊 (PII) 和其他機密資料的監視和確認。*
- *網站應用程式的安全性－保護網站應用程式、Web 2.0 和資料庫（與網站應用程式的防火牆保護相同）。*
- *應用程式控制－重新要求頻寬並阻絕 Skype、P2P (peer-to-peer) 網路與穿遂 (tunneling)。*

這些模組具備的功能，讓IBM安全性網路IPS解決方案得以保護企業組織不受各種威脅的影響，包括：

- *內含蠕蟲和間諜軟體的惡意軟體*
- *殭屍病毒 (botnet) 發動的攻擊*
- *與網路資源濫用和資料遺失等即時訊息和點對點檔案分享相關的風險*
- *阻斷服務 (DoS) 及分散式阻斷服務 (DDoS) 攻擊*
- *鎖定跨網站指令碼和資料隱碼攻擊等網站應用程式的目標式攻擊*
- *與私有或敏感資料相關的資料遺失*
- *緩衝區溢位攻擊*
- *以網頁瀏覽器為目標等用戶端攻擊*

X-Force 研究和開發團隊會從全球威脅行動中心 (Global Threat Operations Center) 追蹤全球網際網路威脅的等級，以強化及更新 IBM 安全性網路 IPS 解決方案的保護能力。

提供高度的可用性

置於網路流量中的裝置必須極為可靠。IBM 安全性網路 IPS 解決方案提供最高等級的可靠性與可用性。這種等級的可靠性與可用性，是透過高可用性組態（主動/主動或主動/被動），以及熱抽換式備援電源供應與熱抽換式備援硬碟來達成。此外，位置高可用性選項可以使用管理連接埠來分享隔離封鎖的決策，以在需要時確保對遠端待命裝置的安全容錯。

讓您輕鬆部署

每個 IBM 安全性網路 IPS 裝置在出廠前，都已預先設定備受驗證的 X-Force 預設安全性原則。這個安全性原則提供創新的立即安全性防護，並經由 X-Force 研究人員的詳加驗證，可以確保最高水準的精確度。IBM 安全性網路 IPS 也擁有不需要對網路進行重新設定的 Layer-2 網路結構。網路及安全性系統管理員可以輕易從三個作業模式中進行適當的選擇，包括：

- *主動保護（非法入侵預防模式）*
- *被動偵測（入侵偵測模式）*
- *線上模擬（模擬線上防護）*

集中式安全性控管

IBM 安全性網路 IPS 裝置是由 IBM Security SiteProtector 系統集中管理。SiteProtector 提供 IBM 代理程式簡單且功能強大的組態設定與控制，以及健全的報表、事件關聯與全面的警示。除了前述的功能外，SiteProtector 也具備 IBM 安全性網路 IPS 裝置的 IPv6 管理支援，其中包括顯示 IPv6 事件及 IPv6 來源/目的地 IP 位址的能力。

以安全性的專業與支援贏得您的信賴

IBM 是侵入偵測及預防的領導者，擁有信譽卓著的優秀客戶支援。IBM是安全性產業中第一批獲得全球 SCP 認證 (Support Center Practices Certification) 的其中一家廠商，而且是服務與支援專業人士協會 (SSPA) 諮詢委員會的其中一名成員。

IBM 爲何是首選？

IBM 瞭解對您網路造成影響的各種威脅，以及該如何在效能和保護間找到恰到好處的平衡點。因此 IBM 推出世界級安全性技術，讓貴企業在受到影響之前，就先阻止網際網路的威脅。有了 IBM 安全性網路 IPS，您可以獲得經濟實惠的高效率解決方案，這種解決方案提供：

- *由 IBM X-Force 研究和開發團隊提供先行保護功能的支援服務*
- *領先的安全性技術，包括用於封包深入檢測的 IBM 通訊協定分析模組 (PAM)*
- *有助於維護網路可用性的高效能*
- *方便進行安裝、設定與管理*

適合您網路的先行保護功能

擁有全系列高效能模組的 IBM 安全性網路非法入侵預防系統 (IPS)，在設計上是為了提供每一層網路絕不妥協的保護，避免您的企業受到內部與外部的威脅。

技術性規格

型號	GX4004-V2-200	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116	GX7800
效能特性*							
穩定傳輸量	Up to 200 Mbps	Up to 800 Mbps	Up to 1.5 Gbps	Up to 2.5 Gbps	Up to 4 Gbps	Up to 8 Gbps	23 Gbps
平均延遲時間	< 200 µs	< 200 µs	< 200 µs	< 200 µs	< 200 µs	< 150 µs	< 150 µs
每秒連線數	35,000	35,000	37,000	40,000	50,000	296,000	390,000
同時連線(最大速率)	1,300,000	1,300,000	1,500,000	1,700,000	2,200,000	5,000,000	12,500,000
實體特性							
外觀	1U	1U	2U	2U	2U	2U	3U
尺寸 高度 (in/mm)	1.75/44	1.75/44	3.5/88	3.5/88	3.5/88	3.5/88	5.25/133
寬度 (in/mm)	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429	前：18.85/479 後：17.28/439
深度 (in/mm)	15.5/394	15.5/394	21.5/546	21.5/546	21.5/546	21.5/546	26/662
重量 (lb/kg)	24.5/11.1	24.5/11.1	40.0/18	40.0/18	40.0/18	37.5/17	55/25
管理介面	10/100/1000 (支援 IPv6)	10/100/1000 (支援 IPv6)	10/100/1000 (支援 IPv6)	10/100/1000 (支援 IPv6)	10/100/1000 (支援 IPv6)	10/100/1000 (支援 IPv6)	10/100/1000/10000 (支援 IPv6)
監控介面	4x10/100/1,000 (僅限乙太網路介面)	4x10/100/1,000 (僅限乙太網路介面)	8x10/100/1,000 乙太網路介面或 8x SFP/mini-GBIC 連接埠 (1,000 TX/SX/LX)	8x10/100/1,000 乙太網路介面或 8x SFP/mini-GBIC 連接埠 (1,000 TX/SX/LX)	8x10/100/1,000 乙太網路介面或 8x SFP/mini-GBIC 連接埠 (1,000 TX/SX/LX)	16x SFP/mini-GBIC 連接埠 (1,000 TX/SX/LX)	8x10Gbe SFP+ (SR/LR) / 8x10Gbe Direct-Attach Copper/8x1Gbe SFP (TX/SX/LX)
線上受保護的區段	2	2	4	4	4	8	4
備援電源供應	否	否	是	是	是	是	是
備援儲存體	否	否	是	是	是	是	是
高可用性	Active-active: no; Active-passive: no Hardware-level bypass: integrated bypass	Active-active: no; Active-passive: no Hardware-level bypass: integrated bypass	Active-active: yes; Active-passive: yes; Geo-dispersed HA: yes Hardware-level bypass: external bypass (optional)	Active-active: yes; Active-passive: yes; Geo-dispersed HA: yes Hardware-level bypass: external bypass (optional)	Active-active: yes; Active-passive: yes; Geo-dispersed HA: yes Hardware-level bypass: external bypass (optional)	Active-active: yes; Active-passive: yes; Geo-dispersed HA: yes Hardware-level bypass: external bypass (optional)	Active-active: yes; Active-passive: yes; Geo-dispersed HA: yes Hardware-level bypass: external bypass (optional)

技術性規格

型號	GX4004-V2-200	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116	GX7800
電氣及環境參數							
電壓：	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac
輸入範圍：	100 - 240 V 全域電壓，輸入頻率 50/60 Hz	100 - 240 V 全域電壓，輸入頻率 50/60 Hz	100 - 240 V 全域電壓，輸入頻率 50/60 Hz	100 - 240 V 全域電壓，輸入頻率 50/60 Hz	100 - 240 V 全域電壓，輸入頻率 50/60 Hz	100 - 240 V 全域電壓，輸入頻率 50/60 Hz	100 - 240 V 全域電壓，輸入頻率 50/60 Hz
運轉時的溫度：	0° 到 40℃ (32° 到 104℉)	0° 到 40℃ (32° 到104℉)	0° 到 40℃ (32° 到104℉)	0° 到 40℃ (32° 到104℉)	0° 到 40℃ (32° 到104℉)	0° 到 40℃ (50° 到104℉)	5° 到35℃ (41° 到95℉)
相對濕度：	5%到85%為 40℃ (104℉)	5%到85%為 40℃ (104℉)	5%到85%為 40℃ (104℉)	5%到85%為 40℃ (104℉)	5%到85%為 40℃ (104℉)	20%到90%為 40℃ (104℉)	8%到80%為 28℃ (82℉)
安規認證/宣告	UL 60950-1, CAN/CSA C22.2, No. 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, No. 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, No. 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, No. 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, No. 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, No. 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CSA 60950-1, EN 60950-1 (CE Mark), IEC 60950-1, GB4943, GOST, UL-AR
電磁相容性 (EMC) 認證/宣告	FCC Part 15、Class A Verification Canada ICES-003、Class A EN 55022、Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000- 3-3 (CE Mark) VCCI Class A	FCC Part 15、Class A Verification Canada ICES-003、Class A EN 55022、Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000- 3-3 (CE Mark) VCCI Class A	FCC Part 15、Class A Verification Canada ICES-003、Class A EN 55022、Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000- 3-3 (CE Mark) VCCI Class A	FCC Part 15、Class A Verification Canada ICES-003、Class A EN 55022、Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000- 3-3 (CE Mark) VCCI Class A	FCC Part 15、Class A Verification Canada ICES-003、Class A EN 55022、Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000- 3-3 (CE Mark) VCCI Class A	FCC Part 15、Class A Verification Canada ICES-003、Class A EN 55022、Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000- 3-3 (CE Mark) VCCI Class A	FCC Class A、Industry Canada Class A、AS/NZS CISPR 22 Class A、EN 55022 Class A (CE Mark)、EN 61000-3-2 (CE Mark)、EN 61000-3-3 (CE Mark)、EN 55024 (CE Mark)、VCCI Class A、KCC Class A、GOST Class A、GB9254 Class A、GB17625.1
環保法規符合聲明	ROHS	ROHS	ROHS	ROHS	ROHS	ROHS	ROHS、WEEE 及 REACH

* IBM 安全性網路非法入侵防護系統的效能資料，是依據可以反映出一般即時流量的 TCP/UDP 混合流量測試所得到的結果。混合通訊協定與平均封包大小等環境因素會因個別網路而有所不同，而測量的效能結果也會因而有所不同。網路非法入侵預防系統 (NIPS) 的傳輸量，是根據推過裝置的混合通訊協定流量，以及計算傳送到目的地的零封包遺失傳輸量計算而得。以基準測試為例，GX7800 的部署方式為使用「Trust X-force」原則的預設線上防護模式；Spirent Avalanche 3100 測試設備 (韌體3.50 (或更新版本))；混合流量：HTTP=41%、HTTPS=17%、SMTP=10%、POP3=5%、FTP=9%、DNS=15%、SNMP=3%；使用 HTTP/S 1.1 GET要求、包含 44kb 物件大小的HTTP/HTTPS 流量；DNS 標準 A 記錄查詢；15000位元組的FTP GET要求 (2ms突衝)、兩名「使用者」信箱間包含 100KB 物件的 POP3 流量、不含物件傳輸的 SMTP 單純連線、SNMP 狀態查詢及回應。

關於進一步的資訊

如需進一步瞭解 IBM 安全性網路非法入侵預防解決方案，請聯絡 IBM 業務代表或 IBM 事業夥伴，或造訪下列網站：**ibm.com**/software/tivoli/products/security-networkintrusion-prevention/

台灣國際商業機器股份有限公司
台北市松仁路7號3樓
軟體事業處
技術諮詢熱線：0800-000-700

台灣印製
2011 年 6 月

Tivoli software