IBM 安全性網路非法入侵預防系統虛擬裝置

產品特性

- ***解決整併措施和昂貴的裝置叢生的問題，採用虛擬平台作爲安全性整合 (security convergence)***
- ***針對虛擬網路，延伸一般由傳統網路提供的強健非法入侵功能***
- ***藉由協助偵測和阻絕網路攻擊與未授權的網路存取，簡化資訊安全性和法規遵循的作業***
- ***讓雲端計算服務供應商在多租用戶的虛擬環境中，提供分段的安全性服務***
- ***以傳統網路保護方式整合虛擬安全性，降低整體安全性營運的複雜度***

同時針對傳統與虛擬的環境結合安全性與效率

雖然資訊安全性總已成為貴企業的最優先事項，但是日益複雜且與日俱增的安全性事件和法規遵循，依然大幅增強精密網路保護的需要。然而經濟的現實顯示出一種同樣迫切的需求：即找出方法透過整併和虛擬化來減少所有的硬體需求。這樣的挑戰是在既不危害貴企業的資訊安全性，也不危害您整併力氣的情況下，協調這些優先事項。

IBM 安全性網路非法入侵預防系統虛擬裝置，在一個虛擬安全性裝置中提供先進的先行保護功能，以協助您以最少的資源達到最大的業務連貫性。拜 IBM X-Force® 研究和開發團隊之賜，IBM 安全性網路非法入侵預防系統虛擬裝置在虛擬平台運轉，以同樣高水準的安全性措施，協助保護您實體與虛擬的網路。作為一個虛擬裝置，IBM 安全性網路非法入侵預防系統虛擬裝置，提供理想的解決方案給管理的雲端服務供應商，在多租用戶的虛擬環境中更有彈性的部署。單一的管理主控台和廣泛的顧問服務以協助簡化部署和管理安全性營運的複雜性，同時其模組化的系統架構更提供延伸的保護，協助確保您準備好接受下一個更大的威脅—不論會在何時何地發生。

透過虛擬安全性裝置來推動整併措施

傳統和虛擬平台的網路安全性經常需要可以提升資料中心需求的裝置，因此增加大小和花費。IBM 安全性網路非法入侵預防系統虛擬裝置，在一個虛擬安全性裝置同時提供兩個強項：先進網路非法入侵預防功能的強大能力與保護。精密的偵測技術和虛擬表單可以盡量減少裝置叢生並記錄整併計畫，不會危害網路營運的安全性。高傳輸量和低延遲協助可維護流量順暢，確保有效的網路運轉。

延伸和簡化安全性營運

IBM 安全性網路非法入侵預防系統虛擬裝置將同樣高水準的先行保護措施延伸至您的虛擬營運中，協助您阻隔威脅於環境之外。同時，IBM 解決方案讓您從單一管理介面管理虛擬安全性、傳統企業安全性和弱點管理，協助減輕複雜度。除了大幅減少多點解決方案和資源的需求，其在虛擬和實體網路安全性營運之間分享網路原則和最佳實務的能力，可以協助確保一致性。

日益增加的威脅和法規遵循措施

IBM安全性網路非法入侵預防系統虛擬裝置依靠由 IBM X-Force 團隊設計的 IBM 通訊協定分析模組 (PAM)，提供一個穩固、可延伸的保護引擎，在威脅來臨時增加新的保護區域。完全發揮 PAM 技術的強大能力，IBM 安全性網路非法入侵預防系統虛擬裝置是一個完備的網路保護解決方案，包括：

- 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。
- 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)。

藉由整併安全性需求，例如威脅偵測和預防、資料安全性、網站應用程式保護以及應用程式控制，IBM 安全性網路非法入侵預防系統虛擬裝置可協助降低部署和維護單點解決方案的成本。模組化技術可以協助守護您的網路，避免各類攻擊和威脅，包括：

- 蠕蟲和間諜程式
- 阻斷服務 (DoS) 病毒和分散式阻斷服務 (DDoS) 病毒
- 殭屍病毒 (botnet)
- 鎖定攻擊網站應用程式
- 脫離網路的私有或敏感資料

可在雲端運算環境中提供安全性服務

IBM安全性網路非法入侵預防系統虛擬裝置，以客製化的安全性原則選項或「trust X-Force」預設組態，提供的虛擬裝置讓管理的雲端服務供應商可保護特定虛擬網路區段。以 X-Force 安全性技術提供全新獲利服務，雲端服務供應商可以得到顯著的競爭優勢，同時可以展現客戶要求的可靠度。

提供簡化的實作和維護

專為簡易安裝、組態設定與管理所設計，IBM 安全性網路非法入侵預防系統虛擬裝置可以協助您應變人員需求和網路安全性優先順序的衝突。作為虛擬裝置和自足的解決方案，這解決方案可以展現安全性，不需要修改伺服器映像檔、虛擬伺服器、應用程式或虛擬基礎建設。您可以選擇不同的作業模式，包括：

- 主動－阻隔方式預防非法入侵
- 線上模擬－顯示何者被阻隔
- 被動－侵入偵測警示而不阻隔

如果您想要轉換保護您網路的負擔等值得信賴的安全性夥伴，IBM 提供建立顧問和管理的服務，完整技術的服務解決方案團隊從評估、設計、部署到管理。

系統要求和技術規格：Newtork IPS virtual appliance

	GV1000	GV200		
處理器	兩顆四核心Intel® Xeon® E5440 @ 2.83 GHz			
作業系統	VMware ESX Infrastructure 3 Version 3.5	VMware ESX Infrastructure 3 Version 3.5、VMware ESXi 3.5. VMware Server 2.0		
VM 客體作業系統 (guest operating system) 支援	N/A	N/A		
記憶體	1 GB RAM	1 GB RAM		
網路連接	任何支援 Vmware 的網路介面卡 (NIC)	任何支援 Vmware 的網路介面卡 (NIC)		
磁碟空間	10 GB 硬碟	10 GB 硬碟		
效能特性*		**ESX 3.5**	**ESXi 3.5**	**VMware Server 2.0**
產能 每秒連線數 同時連線 (最大速率)	最多700 Mbps 19,000 500,000	最多200 Mbps 19,000 500,000	最多150 Mbps 19,000 500,000	最多50 Mbps 12,000 400,000
作業模式	GV 1000	GV 200		
主動防護 被動偵測 線上模擬	是 是 是	是 是 是	 有	
受保護的網路區段	1	1		
*採用下列組態設定可達的效率	IBM BladeCenter® HT Chassis、Blade IBM eServer™ HS21 - 8853AC1、網路介面卡 (NIC)：NetXtreme Broadcom5704S、處理器：兩顆四核心 Intel Xeon E5440 @ 2.83 GHz、作業系統版本：ESX 3.5.0 Build 123630 Update 3	IBM BladeCenter HT Chassis、Blade IBM eServer HS21 - 8853AC1、網路介面卡 (NIC)：NetXtreme Broadcom5704S、處理器：兩顆四核心 Intel Xeon E5440 @ 2.83 GHz		

系統要求和技術規格：
Virtual Security Protection for VMware

	VSS
處理器	1 虛擬 CPU
作業系統	VMware ESX 4.0
VM 客體作業系統 (guest operating system) 支援	N/A
記憶體	1 GB RAM
網路連接	任何支援 Vmware 的網路介面卡 (NIC)
磁碟空間	10 GB 硬碟
效能特性*	VMware vSphere 4. ESX4.0, ESX/i4.1
產能 每秒連線數 同時連線 (最大速率)	N/A
作業模式	VSS
主動防護 被動偵測 線上模擬	是 是 是
受保護的網路區段	ESX Hypervisor controlled area
*採用下列組態設定可達	

IBM為何是首選？

IBM 安全性網路非法入侵預防系統虛擬裝置，以虛擬形式提供世界級的弱點型 (vulnerability-based) 安全性技術虛擬，可用於保護虛擬和實體網路環境，並支援您的整併目標。除了為您網路的每一層提供先行保護，以及簡單的部署和整合管理，此一完整的安全性平台由業界領先的 IBM X-Force 研究和開發團隊提供支援服務。

關於進一步的資訊

瞭解更多關於 IBM 安全性網路非法入侵預防系統虛擬裝置，請聯繫您的 IBM 業務代表或事業夥伴，或造訪 **ibm.com**/tivoli/solution/threat-mitigation

Tivoli software

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