

Country: HK

Date: September 2008

Publication: Capital CEO

Unified Multi-Threat Security Solutions Unifying Your Threat

Management Practice: A Pragmatic Approach to IT Security

Ever more sophisticated threats, increasing compliance requirements, and evolving applications continually expose new gaps in enterprise network security. Due to management issues, adding more point solutions is not always the best answer. Jens Andreassen, Vice President of Sales, APAC, Fortinet, looks at how enterprises can perform a pragmatic security gap analysis with an eye to selecting the right vendor to help improve network security without multiplying management complexity.

One way to construct a useful map for a smaller scale network consolidation and reap the benefits from unified threat management is to divide up the IT infrastructure into functional network segments, which may be either physical or logical.

- Perimeter
- Data Centre
- Core
- ROBO/SOHO
- Secure Email Messaging
- Endpoint

Unified security solutions offer IT executives concerned with network security a way to integrate multiple new security technologies into their network infrastructure. The solution must offer unified management and reporting consoles to pull it all together, as without these, the solution cannot deliver the promised reduction in operating expenses.

The network should be comprehensively and uniformly protected with an end-to-end UTM solution that gives IT administrators the flexibility to protect various parts of the network with the corresponding security features that make sense in that environment.



Jens Andreassen
Fortinet 亞太區
銷售副總裁

實用型 IT 保安法 整合式威脅管理解決方案

愈來愈複雜的威脅、不斷提高的法規要求，以及持續演變的應用程式，為企業網絡保安帶來不少挑戰。從管理角度而言，添置更多單點式解決方案並非最佳解決辦法，應考慮企業如何開展實用的保安差距分析，以及選擇合適的供應商來協助改善網絡保安，並降低管理複雜度。

IT 管理人員每天面對愈來愈複雜的威脅和法規，新的應用程式和技術同時也帶來了更多漏洞。現今黑客關注的是獲取經濟利益，而不是揚名立萬，攻勢日趨凌厲。因此，企業需要對網絡層面的保安多加警惕，防火牆和入侵防禦系統固然可以加強保安，然而內容（數據）層面的保安亦不容忽視。電子郵件保安、防病毒、防垃圾郵件、網頁過濾、防間諜軟件等企業所需的保安技術不斷演進，基於成本方面的考慮，中小企很難隨技術演進而不斷添置個別解決方案。此外，法規與最佳實務指引也為 IT 管理人員帶來沉重的負擔，他們不但要採用最新的技術來應付潛在的威脅，還要竭盡所能保護敏感資料和企業網絡。通過新增應用程式或升級現有應用程式，企業部署的新技術有助提升業務表現，然而亦增加了受新型漏洞攻擊的風險。

為了全力提升營運效率，取得競爭優勢及成功拓展業務，IT 管理人員致力為企業提供更高流動性、最佳的相互連結性和第三方網絡接入服務。

實用型網絡保安

IT 保安一般只佔整體 IT 預算的一小部分，而 IT 預算又只是整體業務預算的一小部分。企業不僅需要按照各種威脅對業務的潛在影響對它們進行分級，還需要在保安產品與 IT 預算中的其他項目之間取得平衡，一切以降低營運經費為大前提。這正是企業對整合式威脅管理愈來愈感興趣的原因。整合式威脅管理能夠減低執行和管理保安基礎架構所涉及的複雜性和成本。

整合式威脅管理提供了非常實用的企業保安法，以下為三大要點：

1. 網絡保安和應用程式的可用性十分關鍵。企業可以業務成效為目標來決定選用何種保安技術和產品，並按照整體 IT 目標和預期收益來作出有關保安的決定。

2. 有企業認為若要整合不同供應商出品的產品，只有全部整合或零整合兩個選擇；亦有企業選購不同供應商的「最佳」單一功能產品。其實整合兩至三項功能已能帶來莫大的好處，如降低管理複雜度、減少裝置的數量從而減低對環境的影響、以及提供更高的投資回報。相對於採用完全不同供應商的裝置，整合式解決方案有助保護網絡免受日增的保安威脅影響。
3. 企業採用的解決方案須配合現有的保安投資，企業難以完全避免管理的複雜性，但卻可以透過選擇合適的供應商將複雜性降低。

化解網絡保安危機

要從整合式威脅管理受益的話，其中一個方法是將 IT 基礎架構劃分為功能性網絡分區，這些分區可以是實體分區（例如：數據中心或核心網），或邏輯分區（例如：訪客登入或電子郵件通信）。企業可以透過網絡整合計劃辨識保安危機所在，而 IT 管理人員亦可以透過整合確定理想的解決方案。

IT 管理人員可以從以下角度分析各功能網絡分區是否採用了合適的產品和技術。

- 網絡邊界
- 數據中心
- 核心網
- 遙距/分支機構辦公（ROBO）及小型/家居辦公（SOHO）
- 安全的電子郵件通信
- 端點

網絡邊界

網絡邊界是企業保安的第一道防線，也是各種外來威脅的攻擊目標。潛在保安漏洞有機會出現在虛擬專用網絡（IPSEC 或 SSL）、防火牆、入侵防禦系統以及防毒

解決方案的吞吐量、可用性以及威脅程式更新。

數據中心

數據中心設有各種伺服器 and 應用程式，協助企業用戶進行數據儲存管理。數據中心面臨的最大挑戰是吞吐量和實時操作，特別是為重要應用程式進行防毒和內容掃描。如果解決方案不能有效保護數據的話，企業將不斷受到威脅所影響。

核心網

核心網的挑戰包括高頻寬和大量多層協定，以及如網絡電話通訊 (VoIP) 的小數據包即時應用程式。

許多解決方案號稱針對 512 位元組的高吞吐量，但處理較小數據包時，其成效通常會顯著下降。核心網主要涉及防火牆、虛擬專用網絡及入侵防禦技術，企業在選擇解決方案時要考慮其可擴展的容量、效能、高可用性和冗餘性。ATCA 硬件和專用 ASIC 處理器有助強化企業網絡和內容保護功能。

遙距/分支機構辦公 (ROBO) 及小型/家居辦公 (SOHO)

遙距/分支機構辦公 (ROBO) 和小型/家居辦公 (SOHO) 與大型企業同樣面對許多保安問題，但他們還要處理漫遊用戶數目增加、無線網絡和 DSL 數據機等接入裝置所帶來的保安漏洞，以及話音和即時應用程式。ROBO 及 SOHO 用戶要注意檢查解決方案的小數據包吞吐量。

安全的電子郵件通信

電子郵件受最多病毒感染，亦可能引致數據保安危機和法律爭議。在法規遵循方面，先進的歸檔功能尤其

關鍵，而外發內容過濾功能則可以保護重要資訊。

端點

企業須留意桌面電腦、筆記簿型電腦以及 PDA 電子手帳等網絡端點的保安。若端點保安不夠完善，可能會損害網絡和應用程式的完整性；而要符合企業保安標準，防間諜軟件和防毒方面的能力便顯得十分關鍵。另一方面，採用個人防火牆和可靠的虛擬專用網絡可以進一步加強防禦。

企業保安一體化

考慮是否在整個網絡保安系統或只在局部系統部署整合式威脅管理 (UTM) 解決方案時，最好選用能夠提供多元化保安技術，以及統一管理、報告及保安威脅研究的供應商。否則，不同供應商出品的單點式解決方案會加重管理負擔及增加營運開支。

保安基礎架構的管理關乎制定、發佈和實施保安策略，以及管理各種網絡保安設備配置。UTM 解決方案由單一管理主控台提供統一保安功能、保安政策及配置修訂控制，從而實現有效的管理控制。

政策管理需要強大的報告能力，以整合各種裝置和技術，同時提供網絡容量，並利用數據來進行優質網絡管理。企業可以視乎需要個人化預定及按需提供的報告、以及標準報告，而事件關聯、取證分析、漏洞掃描與管理主控台整合等能力，均非常重要。

UTM 解決方案及時更新用戶資料、攻擊特徵、網址和其他威脅資訊，以防範層出不窮的威脅。除了自動更

新以外，企業可以考慮以小時而不是日子為單位的最新服務層級協定，以便更有效保護網絡。

無論在整個網絡或局部網絡，部署整合式保安解決方案，都能夠讓 IT 管理人員在網絡基礎架構中整合多種新型保安技術。解決方案須提供統一管理和報告主控台，將所有保安功能融為一體，否則無法達成降低營運成本的目標。點對點 UTM 解決方案可為網絡提供全面和統一化的保護，使 IT 管理人員能夠靈活地利用適用於特定環境的保安功能來保護企業網絡。◊

