

UTM 的發展演進與未來趨勢

UTM 設備對於外部的網路威脅防護上有一定效果，但卻很難抵擋來自內部安全問題的侵襲，而愈來愈多的行動工作者，勢必讓安全廠商開始思考如何保護每一個網路節點，這應是網路安全發展演進的下一步

文◎ Richard Stiennon

過去近十年來，封包過濾的防火牆已足夠防護來自網際網路的所有威脅。然而，現今網路威脅的種類與複雜度已倍數成長，防火牆和電腦防毒軟體的防護能力已不再足夠。安全系統與軟體的一路演進，直至今日整合式威脅管理 (Unified Threat Management, UTM) 設備型式的解決方案，就像是一部駭客、黑客和病毒作者，與安全廠商之間的「軍備競賽史」。每當有一個新的系統弱點被偵測出，新的安全機制與措施也就跟著發展，但緊接著突破防護或攻擊安全措施的新方法也會出現。最近幾年，結合不同種類攻擊特徵的混合式威脅 (blended threats) 持續發展，例如一些內嵌垃圾郵件引擎的木馬程式，或是具備間諜軟體彈藥 (payload) 的病毒，而 UTM 技術與產品的發展演進，實應歸究於混合式威脅的浮現。

內在的威脅

目前，UTM 安全設備已能在網路邊界有效阻擋許多種外部的威脅，但來自內部的威脅卻難以抵禦。研究調查顯示網路事件有極大部分是由內部員工惡意造成，也因此安控人員試著藉由網路分區，或是隔離重要的企業資訊系統如資料庫或郵件伺服器，來降低這樣的可能性。這樣的策略也許對於特定的內部攻擊有效，但更重要的是：有愈來愈多的公司提供員工筆記型電腦，風險便在於這些筆記型電腦在外可能已經遭到感染或入侵，例

如差旅時連接不安全的無線熱點 (hotspot)。受感染的筆記型電腦回到企業網路內部連線時，就避開了閘道器的防禦，甚至可能感染整個網路區段的其他電腦。

網路內部的安全 vs. 網路安全

網路安全一連串的發展，造就了一個全方位的解決方案，能讓網路本身具備抗力，大多數的攻擊都難以滲透。此解決方案的關鍵元素便是來自整合式威脅管理廠商。但有兩個主要原因，迫使外部網路安全來到一個轉折點，必須朝內部網路安全來發展：

1. 網路犯罪。不論是竊取個人資料或詐欺，網路壞蛋顯得愈來愈成功，布下的陷阱也愈來愈廣。他們現在鎖定的是有滲透機會的特定公司和網站，因為他們通常執行非常重要的交易，或是擁有大量的個人資料，例如信用卡或銀行帳號。

2. 內部的壞蛋。一般人就能用來掃描、入侵和攻擊網路資源的工具和技術已大幅增加，內部網路事件導致資訊或企業資源損失的次數，終究也會高升。區域網路的每個存取點，都必須被看成是一個安全檢查範圍，才能保護企業組織應付來自該處的攻擊。

在 UTM 領域有許多種方案，從一部 Linux 伺服器執行個別的安全軟體，到硬體機架式機箱裝載多種伺服器。然而，所有因應特定目的而造的安全平臺，都具備深度的封包檢測功能，不斷地掃描所有網路流量，提供內容層

級 (content layer) 的安全防護。

完整的 UTM 功能一般而言包含以下元素：

- 防火牆機制：具備執行連接政策 (connection-based policy) 的能力，以及 SSL 和 IPSec VPN 功能。

- 入侵防護 (IPS)：由於 IPS 能防止蠕蟲的擴散，封阻某些特定的攻擊而被大幅採用。然而企業 IT 管理人員普遍關切 IPS 的地方，在於它在網路裏規畫了「乾淨」與「不乾淨」的兩邊。換句話說，當有電腦遭感染時，同一個網路區段裏的其他電腦便處於危險之中。IPS 要完全有效，就必須設置在每一個端點設備之前。

- In-line 防毒：安全設備市場的驅動力。主因在於 E-mail、IM 和 P2P 遭感染或濫發的檔案數量，已嚴重影響這些伺服器的服務處理能力。

- URL 內容過濾：起初與安全無關，但因愈來愈多的網站開始隱含惡意的內容，因此成為保護終端使用者的重要元件。

當一個整合的設備能同時封阻內含各種惡意軟體的攻擊，以及透過新通訊協定的網路攻擊時，整合各種功能的 UTM 便能帶來更多的優勢。

整合式安全設備的下一個發展演進，便是加入網路能力，例如路由通訊協定 OSPF、RIP 和 BGP，提供許多企業需要的網路建置彈性，勿需在設計、組態和維護路由器與負載平衡設備時，負擔額外的費用支出。在許多情況下，部署 UTM 將不再需要路

由器，因此它的價值將會提升。

內部網路分區 (internal segmentation) 常常是個問題。特別是當一部電腦隱含威脅，或是必須隔離部分的網路時，它就變成一個昂貴的異種系統，而非優雅的解決方案。同時所需的政策層級設定太過精細，所需技術的廣度與深度，則只有大型企業才能具備的。若量化建置的需求，結果不是太過於昂貴，就是已超越中小企業所能擔負的。

如同UTM已展現的，安全功能的整合可以是有效又經濟的解決方案，不論就費用還是工時而言，也適用於各種規模的企業網路。因此，開發整合網路交換 (network switch) 功能、IPS、防毒、防火牆及路由 (router) 功能的解決方案，對安全廠商而言將會是個契機，換句話說，就是將交換器和路由器，整合至傳統的UTM安全設備。

重回網路層解決威脅

這樣的解決方案倚賴的是交換網路

架構，所涉及的通常包括核心交換器 (core switch) 及存取交換器 (access switch)。虛擬區網 (VLAN) 可用來做為所需設備的細部控制，交換器則基於 Layer 2 和 Layer 3 的資訊執行政策。正常與獲准通行的資料則進一步透過 IPS 的功能過濾。IPS 過濾最理想的方式是直接交換器裏執行；網際網路 (或與第三方) 連線，則和防火牆功能同時內建在交換器中。下一代的 UTM 安全設備也將提供額外的網路分區，例如針對交易區 (Transaction Zone) 和分區隘口 (departmental barrier)。

這些超級 UTM 設備將會有三種典型的應用。

首先是電信廠商和服務供應商將能部署這些設備，完全過濾網路骨幹中惡意的網路流量，提供客戶乾淨的網路通道 (clean pipes)。這個概念在多年前就已出現，但受制於成本、技術與其他政策性考量而無法實現，現在是電信廠商應該要試試的時候，儘可

能地移除網路裏的病毒、木馬、蠕蟲和惡意軟體。

第二種應用則是在企業核心。這些先進的 UTM 設備將能夠畫分和保護每一個部門，最終則是每一個設備，史無前例地、真實地強化內部網路。

至於小型或遠距辦公室，也同樣能獲得極大的好處。因為一個設備就能取代許多安全裝置才能擁有的保護功能，同時也能取代路由器和交換器。

這樣的觀念將使 UTM 遠遠超越最初發展的原意：一個簡單的安全平臺，同時當安全設備開始納入網路功能時，整個產業將會產生重大轉變。傳統路由器與交換器廠商，將會發現基於速度與功能單純的產品，無法因應深度封包檢測與精密防護功能的需求；安全廠商特別是防火牆或 IPS，則會漸漸被同時整合安全與網路功能，且更具備有彈性的產品所取代。

專家建議

Fortinet 預測的 2007 年十大安全威脅

隨著網路犯罪模式逐漸增加，目前仍缺乏有效的方式來抵禦這些網路威脅。尤其網路攻擊者不再著重病毒技術的創新，反而專注於尋求獲利的商業模式開發。攻擊者似乎對於這邊賺 100 元，那邊賺 1000 元感到滿足，到處獵殺。在 2007 年，這樣的狀況似乎不會停歇。

Richard Stiennon 指出，2007 年企業資料可能成為網路攻擊者的首要目標，以便犯罪獲利倍增，營收則介於 40 億到 80 億美元。無論如何，網路勒索詐騙的對象將不再侷限於金融機構或企業，甚至包括政府、學校及製造商，都將正視如何防禦這些以商業目的為主的網路攻擊。

以下為 Richard Stiennon 對於 2007 年網路安全趨勢的十大預測：

- 網路犯罪營收將成長 100%
- 攻擊目標進一步鎖定企業儲存資料
- 阻絕攻擊 DDoS 將支援網釣攻擊
- 持續增加的 DNS 攻擊
- 個人識別資料的竊賊繼續增加
- 更多無線網路的攻擊
- MySpace 成長並變得安全
- YouTube 垃圾郵件氾濫
- 網路架構出現負載過高的徵兆
- Windows Vista 的普及，在網路威脅領域，未帶來任何影響

作者簡歷

Richard Stiennon



為 Fortinet 全球行銷長 (Chief Marketing Officer)，在安全產業擁有超過 25 年的經驗。曾任職

Gartner Group 安全與隱私部門研究副總裁，固定為全球 2000 大企業的資訊長提供策略性的建議，並榮獲 2003 年 Gartner 創新思維領導獎 (Thought Leadership Award)。

加入 Fortinet 前，為獨立 IT 研究公司 IT-Harvest 創辦人兼首席研究分析師。在此之前，則為 Webroot 軟體公司威脅研究部門副總裁。他曾獲 Network World 雜誌選為「網路業 50 大最具影響力人物 (50 Most Powerful People in Networking)」。畢業於密西根大學，擁有航空工程學位。