新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/7/2 - 2007/7/8 第32期

多功能 UTM / MS 系列報導

技術淺談與應用 - 多功能 UTM 防毒機制介紹 (Mail、Policy、IDP)

網路方便的運用在商業往來的各種環境中，無不促使產業蓬勃發展。在這看似正面且能帶來大量效益的訊息傳遞環境中，卻有人為了利益或其他意圖刻意散佈危及整體網路使用人權益的病毒程式，小則造成個人用戶使用的不便，大則造成網路的癱瘓、重要機密被竊、存檔資料遺失…。

為了因應堪稱網路蝗災的病毒程式，早期用戶只能在 PC 安裝防毒軟體以求自保。但常因為個人的疏忽而久未更新病毒碼，造成無法達到實際保護作用。而一般防火牆僅能針對各項網路服務攔阻，無法防禦來自病毒的危害。

有鑑於此，新軟多功能 UTM 針對各式各樣的網路服務建置了數種病毒掃描機制。以新軟 NUS-MS3500 來說，針對網路資料傳輸做的病毒偵測動作，可分為下列數種：

- 郵件病毒過濾－

一般來說，最大的病毒擴散管道就是透過電子郵件傳輸。當郵件傳遞時，NUS-MS3500 會先行將其存放於一暫存區，並針對信件的內容、所夾帶的檔案掃毒（壓縮檔解壓掃毒）。若郵件判斷為異常（病毒郵件、釣魚郵件...），NUS-MS3500 會將該郵件依照管理人員所設定的處置方式處理（隔離儲存、刪除...）剩下的郵件再交由垃圾郵件過濾機制處理。

- HTTP / Web Mail、FTP 病毒過濾－

以網頁方式散撥病毒、木馬、間諜程式...是目前駭客最喜歡的作法。常常可聽到某網站被駭客入侵，並在其網頁中植入惡意程式的消息。由於這些網站包含有電視台、醫院、企業廠商、學校、政府機構...這些知名單位、廠商，所以一般使用者根本不會考慮這些網站是否有問題而疏於防範。

NUS-MS3500 擁有 HTTP、FTP 病毒過濾功能。管理人員可在制定網路管理政策（Policy）時，啟用內建的病毒偵測功能。使用者在上網時 NUS-MS3500 會將透過 HTTP（包含 Web Mail）、FTP 服務傳輸的檔案，先行下載於一暫存區並進行掃毒動作。將判別有異的檔案直接阻絕並刪除，正常的檔案則由暫存區中提取出來，傳送到目的端。

• IDP 病毒過濾－

至於其他網路服務的病毒要如何防範呢？利用即時通訊傳遞檔案、P2P 下載軟體...這也是一般使用者會使用的網路行為。管理人員可以使用 NUS-MS3500 內建的 IDP 病毒過濾機制，針對往來的封包，逐一比對其所包含的資料是否有病毒特徵，來達到病毒防護的效果。將判別有異的封包直接阻絕，並終止該連線後續封包的傳送，無異常封包的連線則可持續完成傳送到目的端的動作。

	病毒郵件掃描	管制條例（Policy）HTTP、Web Mail、FTP 掃毒機制	IDP 病毒偵測
採用的掃毒引擎	Clam、Sophos	Clam、Sophos	Clam
掃描檔案的方式	先行儲存於一暫存區，對郵件夾帶的未加密檔案直接掃毒、壓縮檔解壓掃毒	先行儲存於一暫存區，對傳輸的未加密檔案直接掃毒、壓縮檔解壓掃毒	針對傳輸檔案的封包，檢查是否有病毒特徵

文 陳昱昇 josh@nusoft.com.tw

市場行銷報導 - 防毒引擎 ClamAV 與 Sophos 之差別

在這電腦病毒氾濫的時代，網頁、電子郵件、即時通訊軟體...都已成為病毒感染的途徑。電腦極易因為使用者的疏忽而中毒，造成無法彌補之損失。為此企業通常會架設防毒系統來保護其網路、資料之安全。

一般企業的防毒系統建置，除了在每台電腦上都安裝防毒軟體之外，另一種作法就是建構一個擁有防毒機制的閘道器（防毒牆），來過濾企業往來之封包。以防毒閘道器的方式來防護企業網路，可將病毒阻絕於企業網路之外，不讓它有任何機會進入企業網路，且其建置經費也較低於企業全面安裝防毒軟體。因此，建置防毒閘道器也漸漸企業防毒機制的主流選項。

為了順應此潮流，新軟系統所推出的多功能 UTM 內建了兩種掃毒引擎：ClamAV 與 Sophos 供企業選擇。企業可單獨選用其中一款掃毒引擎來防禦企業網路。甚至也可讓 Sophos 與 ClamAV 同時運作，提供企業網路雙重保障。

ClamAV－（NUS-MS3500、NUS-MS2000A、NUS-MS1500、NUS-MS700）

ClamAV 目前可以偵測超過四萬種病毒、蠕蟲以及木馬程式。並有一群分布在世界各地的電腦病毒專家，24 小時的隨時在線上更新及維護病毒資料庫。如有新型病毒出現，可立刻反應，並發布新病毒碼。屆時，透過新軟多功能 UTM 內建的自動線上更新系統（每十分鐘線上搜尋一次），即可取得最新病毒碼。

與其他商業防毒軟體需每年付費授權與使用人數有所限制不同的是，新軟多功能 UTM 所內建的 ClamAV 可永久免費更新病毒碼，而且並無使用人數限制。這可讓新軟多功能 UTM 的病毒防護功能，能以最少的成本，永遠保持在最新的狀態。

或許有人會懷疑，新軟多功能 UTM 所內建之掃毒引擎採取免費更新病毒碼的方式是否可靠，是否能永續服務下去。事實上，ClamAV 採取與 Linux 相同的運作模式：公開程式碼以及免費授權。因此，其安全性已接受過全球無數電腦工程師的檢驗，可確定安全無虞。再加上全世界已有無數個網站提供 ClamAV 線上病毒碼更新。如此彙聚眾人的力量，成就免費而且永續的網路服務。

Sophos－（NUS-MS3500、NUS-MS2000A、NUS-MS1500）

如果使用者無法相信免費的掃毒引擎，新軟多功能 UTM 亦提供了一套歐洲的著名的商業掃毒引擎－Sophos。Sophos 為出自英國的防毒引擎品牌，擁有多項病毒分析之專利，可以有效偵測各種病毒、蠕蟲、木馬程式...有害程式。品質受到各界的肯定（獲得 Information Security 雜誌 2004 年度資安風雲產品金獎）。

Sophos 在英國、美國、澳洲均設有病毒研究中心，全年二十四小時隨時更新病毒資料庫。新軟多功能 UTM 只需透過內建的自動線上更新系統（每十分鐘線上搜尋一次），即可自動更新病毒碼，完全不需管理人員手動更新。

06:42	Clam AV	06:51	Kaspersky	08:21	Bitdefender
08:45	Virusbuster	09:08	F-Secure	09:16	F-Prot
09:16	RAV	09:24	AntiVir	10:31	Quickheal
10:52	InoculateIT-CA	11:30	Ikarus	12:00	AVG
12:17	Avast	12:22	Sophos	12:31	Dr. Web
13:06	Trend Micro	13:10	Norman	13:59	Command
14:04	Panda	17:16	Esafe	24:12	A2
26:11	McAfee	27:10	Symantec	29:45	InoculateIT-VET
單位－ 小時：分鐘				Virus：MyDoor.s	

表一 各家防毒業者對新病毒的反應速度

文 程智偉 rayearth@nusoft.com.tw