NBL 歐洲參訪心得

陳一瑋、林盈達

摘要

台灣網路通訊廠商漸漸走向品牌之路，同時也希望具備開發高階產品的能力以健全三大通路銷售: 零售、標案以及企業，在這次的歐洲行程中，NBL 主任 林盈達與我一行二人前往英國拜訪了台灣兩大網通廠商 ZyXEL 與 D-Link，了解其品牌在歐洲市場中的嶄獲與困難，接著前往比利時參觀魯汶大學及 iMec (Interuniversitair Micro-Electronica Centrum)，觀察其產業界與學術界互動合作的狀況，最後到法國拜訪 Alcatel 及 NSS，從 Alcatel 身上比較國內、外的 Switch 廠商發展差異，也見習 NSS Lab 的運作方式以及在高階產品上的測試技術、更促成了進一步合作的可行性與必要性之討論(accredited lab or within the NSS Group)。對於 ZyXEL 及 D-Link 而言歐洲市場占總營收很大的比例、認證對於高階產品更為重要、零售市場是主要的通路但與另兩種通路之差異日漸減小、北歐的需求變化遠比南歐要快，而小國的需求變化比大國也來得較快、將來歐盟要實施綠色環保(無鉛)後，舊產品的淘汰率會大幅升高，IMECH 裡建置了 200mm 及 300mm 的晶圓廠，可讓研究人員有更多實踐想法的機會，Alcatel 已投入大量的資源在應用軟體開發上，目的是要將語音資料作更好的整合在不同的硬體平台上(Alcatel Unified Communication)，NSS 的測試範圍主要為 Security coverage 及 Performance，在攻擊程式的開發上主要是與一家 Assurent 合作取得相關函式庫，效能測試上是以 Spirent Avalanche/Reflector 進行。

1. 訪問對象、目的與結論

本次歐洲行的拜訪對象包括了網通廠商: ZyXEL、D-Link 及 Alcatel，研究組織: 魯汶大學及 iMec，測試實驗室: NSS，從 ZyXEL、D-Link、Alcatel 這三家國內、外著名之網通廠商身上，我們希望可以了解到網通產品的通路/市場分佈狀況以及認證對於網通產品的重要性，在拜訪魯汶大學及 iMec 的過程中我們可以了解目前比利時學術研究與產業開發兩者結合的狀況，至於 NSS Lab，由於 NSS award 在台灣的網安產品中是一項具說服力的認證，我們希望從這次的會議討論可以了解他們成功的原因，進一步來加強本身的營運模式與測試技術，同時也嘗試合作的機會，希望在台灣也能由 NBL 進行測試來發行 NSS Certificate、並邀請 NSS 人員來台灣舉辦說明會，讓台灣的網安技術相關人員更了解 NSS 的測試內涵。

英國: ZyXEL 及 D-Link

抵達歐洲後的第一站，是前往位於英國南部(Bracknell, Berkshire)郊區的 ZyXEL，與我們碰頭的是一位 Managing Director，在此會議中以網安產品為例，認為如果產品缺乏具代表性的認證，在產品對外的銷售上及對內的信心上都會有相當程度的影響、對於銷售通路目前還是以零售及標案為主，零售市場首重品牌而標案市場就看產品規格是否符合與產品價格的彈性度，至於企業市場還是占較小的部分，因其需要深入長期的布局且周邊合作伙伴也要夠強壯，因此目前

Enterprise 市場主要還是 Cisco 的天下、歐洲市場占整個公司的總營收六成以上，在 Security 主要的競爭對手為 SonicWall、WatchGuard、歐洲雖然成立了歐盟團體，不過地區性的差別還是不小，造成在產品規劃、銷售上的挑戰，以產品需求的變化而言最快速的是北歐國家(ex.瑞典)，再來是西歐國家(ex. 法國、德國)，相對較緩慢的是英國與南歐國家(ex. 義大利、西班牙)。

接下來前往倫敦與 D-Link 歐洲區 President 及 Product Manager 討論相關議題，歐洲區市場占 D-Link 總營收的三分之一左右、其市場分佈狀況相當平均，用戶端約 40%、企業端約 30%、電信市場約 30%，用戶端市場以北美為主，在中南美及蘇聯等地只有企業及電信市場，電信局端由於其 Technology Life Cycle 較短，因此所遇到的問題最多，其次是用戶端市場(ex. 客戶使用上的問題及 ISP 的設定改變)，最少有問題的是企業市場、為了解決用戶端市場的問題以及不同 ODM 產品間的互通，D-Link 正積極推展 D-Link 2.0 的協定、對於網安產品也是十分需要認證的取得，以 VPN 產品為例就必須通過 ICSA 及 VPNC 的測試。

圖 1: 分別在 ZyXEL 及 D-Link 的 Logo 前留影

比利時: 魯汶大學及 iMec

結束英國的行程後，我們搭程 EuroStar 穿越英吉利海峽抵達比利時首都布魯塞爾，然後再前往魯汶大學及 iMec 參觀，iMec 有點類似工研院的性質，裡的研發主題包含了 Nanotechnology, Organic electronics, Bioelectronics, Packaging, Wireless communication, Solar cells, RF devices and technology, GaN power devices, Non-volatile memories, Microsystems, Micro- and nanoelectronics 等等，在 iMec 裡我們看到了兩座不同規格的晶圓廠，不僅讓業界廠商可以合作開發 IC、也可讓學生們看到自己設計的成果，在 2005 年 10 月台灣的 TSMC 成為 iMec 中第八家核心合作伙伴，合作內容主要是 sub-45nm CMOS 的研發。


圖 2: 左圖是與魯汶大學教授 Luc 合影、右圖是在 iMec 裡參觀晶圓廠

法國: Alcatel 及 NSS

Alcatel 法國 HQ 在巴黎附近，與同開會人員主要是 Solution Marketing Managers，我們聽取了其對於市場趨勢的說明及產品規劃的 roadmap，觀看了 My Messaging, My Phone, My Teamwork 及 My Assistant 等語音整合應用軟體的 demo，技術主軸以 Alcatel Unified Communication 為主，讓使用者可以透過各種不同平台達到語音交談的目的，當然對於 VoIP 的安全性也是十分注重，Alcatel 跟一家叫作 THALES 的公司合作 VoIP 相關加密保護技術，因此 Alcatel 已經變成一家應用軟體比重很高的公司。

從巴黎前往 NSS 是很長的一個旅程，TGV 加上計程車的時間將近要四個小時，NSS 位於南法的一個城市 "Sumene"，而且是位於山中的一間別墅內，令我們意外的是其測試人員只有 4 位 Full-time，不過卻有著相當不錯的測試設備(Avalahcne 2500 + Reflector 2500 至少有 8 台)，除了在法國這四位的測試人員外，尚有兩位人員在英國負責 administration 的工作，NSS 主要測試範圍是 Security coverage 及 Performance。對於 NBL 與 NSS 的合作案提議，NSS 方面相當有興趣，由於 NSS 的整個驗證測試過程的花費相當可觀(i.e. 將近一百萬台幣)，再加上公司人員到法國的出差費用，的確是讓許多遠在台灣的網路安全公司望之怯步，若能在台灣在設立一個 Lab 進行 NSS Certificate 驗證將會吸引更多的台灣甚至是亞洲的廠商，基於雙方互惠的情形下，回國之後 NBL 一直持續與 NSS 聯絡討論更進一步的合作事宜，希望在不久的未來有機會實現此一合作案。


圖 3: 左圖為 Alcatel 人員介紹其產品、右圖與 NSS 人員在測試區前的合影

2. 網安產品認證機構介紹

網通市場的銷售通路主要有三種: 零售、標案以及企業，其中對於硬體式的網路/內容安全(NCSec)設備而言更是依賴後兩者的模式來進行，在標案及企業的市場中由於產品總價值不匪，因此通常會有專門的 MIS 人員進行採購評估避免造成組織/企業的損失，對 MIS 人員而言最容易辨別產品優劣的方法之一，便是了解產品有沒有獲得一些具代表性的「認證(Certificate)」，例如 ICSA、NSS、Common Criteria、MIPS 140-2 等等，然而對於這些認證的涵意，MIS 人員有真正的了解

了嗎? 認證本身是否也成為一種「品牌」了呢? 認證發行的過程中所實際進行的測試項目、所用到的測試技術才是採購人員真正該注意的地方，接下來介紹有關 ICSA、Common Criteria 及 FIPS 140-2 的相關資訊，並且另用一段完整介紹 NSS。

ICSA

ICSA 的全名叫作「International Computer Security Association」，是位於美國賓州的一家網路安全產品測試實驗室，發行認證的項目十分多樣化，其中包括了 anti-virus, firewall, IPSec VPN, cryptography, SSL VPN, network IPS, anti-spyware and PC firewall products 等等，除了測試產品、發行認證的主要業務外，也發表一些 surveys, security industry studies 及 buyers' guides，同時對於各個項目也有獨立的 community 可以定期討論相關技術，在 2005 年 4 月時 ICSA Labs 取得 ISO 9001:2000 成為一國際標準認可之測試中心，ICSA 目前也被 NIST-NVLAP 認可為可以進行 FIPS 140-2 密碼模組測試，而 IPSec 是 ICSA 較早就有的 Certificate Program，目前正在推行 IKE v2 的 Testing Program。

2004 年時 NBL 就有親自去拜訪 ICSA，那時 ICSA 有 35 位 Full-Time 員工，相較於其它拜訪的實驗室(UNH/IOL)來說，顯得較為封閉，只公開測試項目（criteria）而沒有測試步驟（procedure），也有許多世界各地實驗室希望與 ICSA 合作成為一個 branch 的要求，但都被回絕，原因是 Intellectual Property、credibility、quick update on criteria 三個考量，如果 NBL 進行 ICSA pre-test，ICSA 也不會提供額外協助但樂觀其成。對於為何 ICSA 難以通過，回答是因為許多廠商對自己程式及標準文件的掌握度不夠，往往無法解決 ICSA criteria 所列之問題。

MIPS 140-2 與 Common Criteria(CC)

MIPS 140-2

密碼模組主要用於保護通信網路所傳遞資訊之隱私性(Privacy)、完整(Integrity)、鑑別性(Authentication)、及不可否認性(Non-repudiation)。美國政府長期將密碼技術加以管制，美國國家標準技術局(NIST)於 1988 年 10 月採用聯邦標準第 1027 號(FS 1027)為藍本，改良成為聯邦資訊處理標準第 140 號(Federal Information Processing Standard, FIPS 140)，經多次討論於 1994 年 1 月正式公布成為 FIPS 140-1 標準，並於同年 6 月 30 日正式生效，同時與加拿大通訊安全主管機關(CSE)共同合作，目前使用中最新標準版本為 FIPS 140-2，FIPS 140-2 密碼模組安全需求標準，是將密碼模組區分為十一個安全需求類別，每一個安全需求類別皆分成安全等級一至安全等級四，以適用於不同敏感度的資料，及應用於各種不同安全威脅之環境，表 1 列出這些安全需求類別與安全等級。

<table>
<tr><td>FIPS 140-2 包括以下 11 個安全需求類別</td><td>FIPS 140-2 包括以下四個安全等級</td></tr>
<tr><td>1. Cryptographic Module Specification</td><td rowspan="3">Level 1:
密碼模組安全之最低需求，允許在單人使用模式中以軟體實現密碼模組功能，並可在個人電腦上執行。</td></tr>
<tr><td>2. Cryptographic Module Ports and Interfaces</td></tr>
<tr><td>3. Roles, Services, and Authentication</td></tr>
</table>

4. Finite State Model 5. Physical Security 6. Operational Environment 7. Cryptographic Key Management 8. EMI/EMC 9. Self-Tests 10. Design Assurance 11. Mitigation of Other Attacks	Level 2: 在多人使用環境下，允許在取得主管機關相關美國可信賴電腦系統安全評估準則 (Truste Computer System Evaluation Criteria, TCSEC) 認證 C2 等級以上認可之作業系統中以軟體實現密碼模組功能。 Level 3: 在多人使用環境下，允許在取得主管機關相關美國 TCSEC 認證 B1 等級以上認可之作業系統中以軟體實現密碼模組功能。 Level 4: 最高之安全等級。在多人使用環境下，允許在取得主管機關相關美國 TCSEC 認證 B2 等級以上認可之作業系統中以軟體實現密碼模組功能。

表 1: FIPS 140-2 密碼模組安全需求標準

CMVP (Cryptographic Module Validation Program)測試實驗室是來驗證 FIPS 140-2 標準，目前全世界共有 13 個這樣的實驗室(美國有 8 家、加拿大有 2 家、英國有 2 家、德國有 1 家)。

Common Criteria(CC)

CC 集合歐美資訊技術安全標準成為全球國際標準，其中包含美國 Orange Book(TCSEC)、歐洲 UK、German 及 French 的標準，在 1999 年 2.1 release 時成為 ISO/IEC 15408，現行通用版本為 V 2.2 (2004.1)，而 V3.0 版已公布，CC 的內容共分成三個部分:

Part 1 Introduction and general model	明確地定義資安評估的基本觀念與原則，並且呈現一個評價的基本模型，同時，對於資訊安全目標、資訊安全需求的選擇與定義，第一部也敘述 CC 對於各種 CC 使用者所代表的意義與用處。
Part 2 Security Functional Requirements	定義安全功能組件(Security Functional Components)，其中，安全功能組件是針對在 PP (Protect Profile)或 ST (Security Target)中，所敘述的 TOE (Target Of Evaluation) IT 安全功能需求的基礎，可以運用這些組件建立一套標準的方式來描述安全功能需求。這些需求描述了 TOE 中預期的安全行為，同時也傾向於滿足在 PP 或 ST 中的安全目標。
Part 3 Security Assurance Requirements	定義 CC 的保證需求，並且包括評估保證等級(Evaluation Assurance Levels, EALs)、各種的保證組件 (Assurance Components)，以及評價 PPs 與 STs 的準則。

表 2: CC 的三大部分

在第三部分所提到的評估保證等級(EALs)中共有 7 個安全等級，各等級所需時間約為 EAL1: 2~3 個月、EAL2: 4~6 個月、EAL3: 8~10 個月、EAL4: 12~16 個月，與網路安全相關的是 EAL4 (ex. Firewall)，到目前為止 CC 評估實驗室共有 44 家。表 3 列出 CC 與 US TCSEC、European ITSEC 在安全等級定義上的對應關係:

Common Criteria	US TCSEC	European ITSEC

-	D: Minimal Protection	E0
EAL1	-	-
EAL2	C1: Discretionary Security Protection	E1
EAL3	C2: Controlled Access Protection	E2
EAL4	B1: Labeled Security Protection	E3
EAL5	B2: Structured Protection	E4
EAL6	B3: Security Domains	E5
EAL7	A1: Verified Design	E6

表 3: CC 與 US TCSEC、European ITSEC 在安全等級定義上的對應關係

ISO/IEC 18045 Common Methodology for Information Technology Security Evaluation (資訊技術安全評估共同方法論，CEM)，此 CEM 作為資訊技術安全評估共同準則 (CC)之指引文件，為廣大國際合作之結果，於評估案中應用而養成實務經驗，所收回之釋疑說明等均將用於未來發展 CEM 之用。

3. NSS 介紹

NSS 在 1991 年時成立於 UK，剛開始的業務是與雜誌社合作進行產品測試，演變至今已經成為世界上相當有權威的網安產品測試中心，目前整個 NSS 組織有三個部分，第一個部分是在英國的 HQ (full-time: 2 人)，主要是處理測試工作以外的事務 (ex. administration)，第二個部分是位於法國南部 Sumene 的 Testing Lab (full-time: 4 人)，主要是測試網路安全產品 (ex. IPS, Multi-Gigabit IPS, Attack Mitigator, SCA)，目前為世人所推崇的 NSS Awards 即是在此測試，第三個部分是在南法城市 Carcassonne 的 Testing Lab (full-time: 4 人)，以測試網路基礎建置產品為主 (ex. Switch)，該 Lab 於兩年前已從 NSS 裡 spin-off 出來成為一獨立測試中心。Sumene 的 Testing Lab 位於山中一間別墅中，除了有美好的山中景色相伴外，還有個人游泳池可以使用，如此的工作環境讓人十分稱羨 (請參考下圖一)，不過這樣的地理位置會讓廠商有兩極化的反應，一種反應是認為這樣不錯，當送測產品來此時可以順便到附近渡假，另一類廠商會覺得將 Lab 設置於此造成整個送測過程的 Cost 增高許多 (i.e. 交通費與運費)。

圖 4: 位於山中之 NSS 測試中心，環境十分優雅

目前 Security Testing Lab 所提供的認證相關測試模式主要有三大類: Standard Test, Pre-Test 以及 Continuous Test， 表 4 列出三者的差異性，除此之外 NSS 也有其

它服務如 Consult、Group Testing、Confidential Testing 等等。

模式	Standard Test	Pre-Test	Continuous Test
收費方式 ($USD)	30K	20K	30K ~ 60K
測試時辰	定期，8 ~ 10 天	定期，一周	不定期，一年可有 15 天進行測試
特性	標準 Certificate 測試	產品 ship 前測試，當作 QA 的一環	時間較有彈性

附註:

1. Standard Test 可以延長天數，延長天數的前兩天收費為 6K/day，之後延長天數的收費為 3K/day。
2. Standard Test 一開始前兩天的 cut-down version 測試最為重要，大部分通過前兩天測試的產品皆可完成整個測試流程。
3. 這三類的測試是可以在執行過程中進行轉換，例如當廠商原本是要進行 Standard Test，但由於前兩天的測試發現產品的問題，此時便可以由 Standard Test 轉為 Pre-Test 以減少 Cost。

表 4: 三種測試模式

一般的 case 以 Standard Test 為主，通常為期 8 天，這 8 天中第 1 天~第 2 天為廠商工程師 on-site 與 NSS 測試人員 co-work 的時間，主要的工作為 install, configuration, cut-down version testing，若這兩天的測試沒有問題的話，拿到認證的機會就非常大，根據以往的經驗只有五次這樣的案件最後沒有通過測試，第 3 天~第 6 天會進行 overnight testing 檢查是否有類似 memory leakage 的問題，第 7 天~第 8 便著手撰寫測試報告。

NSS 的測試技術可以分為兩大類: Security Coverage 與 Performance。在 Security Coverage 的部分，NSS 與加拿大的一家公司 assurant 合作以取得 attack/exploit library，並且從一些 client sites 取得真實流量以 Traffic IQ 進行 replay，這些流量可協助 False-Positive 的測試，本身也開發了一些 evasion technology，例如在 evasion 開始前會要設定 seed 值，讓整個 evasion 過程是具有變化性的，而不會讓廠商以填入固定字串來阻擋該 evasion，至於 Performance 部分主要是使用 Spirent 的 Avalanche 2500 為主。

NSS Awards

NSS Awards 共分為三類: NSS Tested、NSS Approved、NSS Gold Award，這三類 awards 的等級剛好與所寫的順序相反，以 NSS Gold Award 為最高等級，在 NSS 的官方網站上有將所有拿到這三類 awards 的產品條列出來，可以參考 http://www.nss.co.uk/certification/tested.htm，以下為我們整理後所作的統計資料，X 軸為 award 的種類、Y 軸為產品測試類別，欄位中代表產品個數。

Award / Category	Tested	Approved	Gold
WAF	0	1	0
IPS	0	20	1
SCA	0	1	0
UTM	0	2	0
Gig IDS	0	10	0
IDS	2	24	0
Security Event Management	0	0	1
E-mail Security Gateway	0	1	0
Attack Mitigator	0	3	0
WebApp Firewall	0	1	0

PKI	0	22	0
VA	0	10	0
FW	0	5	1
Total	**2**	**100**	**3**

表 5: 參與 NSS Certificate Program 的產品統計資訊

大多數產品拿到的 award 為 NSS Approved (i.e. 100)，極少數的產品拿到的 award 種類為 NSS Tested (比 NSS Approved 還差)或 NSS Gold (比 NSS Approved 還好)，曾經有拿到 NSS Gold Award 的產品包括 Security Event Mgmt 類別的 Sourcefire RNA、IPS 類別的 TippingPoint UnityOne-1200 以及 FW 類別的 Stonesoft StoneGate 2.0.2，以 NSS Gold Award 的定義來說，這三項產品不僅是符合了 NSS Approved 的測試規範，同時也提供了更進階、更獨特的功能，可以讓使用者願意花更多的錢來購買該產品。

Certificate Programs

NSS 依產品功能不同而提供了各式各樣的 Certificate Programs，其中包含 UTM、Attack Mitigator、IPS、MGIPS (Multi-Gigabit IPS)、SCA (Secure Content Appliance)、WAF (Web Application Firewall)，以下分別作介紹。

Universal Threat Management (UTM)

UTM 的部分包括了七項功能的測試: Firewall、VPN、IDS/IPS、Anti Spam、Anti Virus、Content Filtering 以及 Web/URL Filtering，表 X 列出 UTM 各項功能的測試群組，在進行 Performance Comparison 的測試時有些共同的準則要遵守，例如「Breaking Points」代表了最後何時的測試結果可以採用，Breaking Points 有三項: Concurrent TCP connections exceeds 200、Current response time for HTTP transactions/SMTP sessions exceeds 100 ms、Unsuccessful HTTP transactions/SMTP sessions。在 Firewall 的測試中可決定 UTM 效能的「baseline」、Test 1.1 是用 Avalanche/Reflector，Test 1.2 與 1.3 是用 SmartBits/SmartFlow 進行。在 VPN 測試裡不會涉及到效能的部分、著重在功能支援度與管理的便易度。測試 IDS/IPS 時將以出廠建議的設定/規則來進行，如果沒有建議的話將開啟所有的 attack/exploit signatures，並且動作的設定為「阻擋」、IPS Capabilities 會使用 NSS exploit 及部分的 NSS evasion tests 測試，對於 NSS exploit 要偵測到 75%以上，而 NSS evasion tests 要偵測到 100%。Content Filtering 主要是測三個部分: URL filtering、HTTP/SMTP Content Filtering 以及 File Blocking，在測試 HTTP URL Filter 時 NSS 先行分析世界五大 URL filtering 資料庫，歸納出以下最受歡迎的五類 URL: 1. News (31%)、2. On-line shopping/Auctions (24%)、3. Adult oriented (19%)、4. Travel (16%)、5. Sports (10%)，當以 Avalanche/Reflector 模擬 HTTP client/server 時測試效能時，所存取的網頁就是根據上述比例產生的 100 URLs，HTTP/SMTP Content Filtering 的測試時，會在 web page/mail body 中產生以下「不好的」字串: SEX、Viagra、V1@gr@、V I A G R A、Xanax、X@n@x，HTTP/SMTP File Blocking 測試時，會產生以下「不好的」副檔名之檔案(request): BAS、BAT、CMD、COM、DLL、EXE、INF、PIF、SCR、VB、VBE、VBS。Anti-Virus 的 Performance Comparison 會用 HTTP 及 SMTP 流量來測試，NSS 目前的病毒檔案超過 10,000 個，其中 80%為 in the wild (www.wildlist.org)、20%為 zoo virus，而

這些病毒檔也透過目前三大 desktop AV 軟體掃瞄確定為 infected files，在測 AV Capabilities 時，NSS 選出 100 個病毒檔案(80 為 viruses in the wild、20 為 zoo viruses)，對於 in the wild 的 viruses 待測試必須 100%偵測到，zoo viruses 的部分主要不是看偵測率，而是要來了解 DUT 是否有持續維護 older viruses。Anti-Spam 的測試相關技術中，NSS 從 SpamArchive (www.spamarchive.org)裡搜集了大部分的 Spam，加上自身搜集而來的共超過 100,000 垃圾郵件，這些垃圾郵件中可能有許多掩飾的技巧，例如圖形表示法、URL 連結 encode 等等，因此 NSS 在 Anti-Spam Capabilities 測試時只要求 DUT 的偵測率要超過 50%，表 6 摘要了 UTM 每項功能的測試群組。

Section	Test Group
Firewall	Test 1.1 - Performance Comparison – Firewall Test 1.2 - Firewall Throughput Test 1.3 - Firewall Latency Test 1.4 - Firewall Capabilities
VPN	Test 2.1 - VPN Capabilities
IDS/IPS	Test 3.1 - Performance Comparison – IPS Test 3.2 - IPS Capabilities
Content Filtering	Test 4.1 - Performance Comparison - Content Filtering Test 4.2 - HTTP URL Filter Test 4.3 - HTTP Content Filter Test 4.4 - SMTP Content Filter Test 4.5 - HTTP File Blocking Test 4.6 - SMTP File Blocking Test 4.7 - Content Filtering Capabilities
Anti Virus	Test 5.1 - Performance Comparison - Anti Virus Test 5.2 - HTTP AV Filter Test 5.3 - SMTP AV Filter Test 5.4 - AV Capabilities
Anti Spam	Test 6.1 - Performance Comparison - Anti Spam Test 6.2 - SMTP Anti Spam Filter Test 6.3 - Anti Spam Capabilities
All Modules	Test 7.1 - Performance Comparison - All Modules
Management and Configuration	Test 8.1 - Management & Configuration Features

表 6: UTM Certification Program 之測試群組

Attack Mitigator

Attack Mitigator 是要測試 in-line rate-based 偵測技巧的 IPS 產品，在這類測試中所用到的攻擊主要是 DOS/DDOS 類型的流量，在 Detection Engine 測試中 NSS 使用的攻擊有 24 種，如 SYN Flood、ICMP Flood、UDP Flood、SQL Slammer、Spoofed IP attack、FIN Port Scan、Xmas Port Scan 等等，NSS 預期 DUT 必須要有完整、清楚地警示，除此之外還有「高流量」測試，攻擊流量的速度會逐步遞增 (i.e. 佔 10%, 20%, 40%, 80%的 DUT 頻寬)，看 DUT 是否依舊可以偵測到。Evasion 測試中會先有一 Baseline 的測試 (with no evasion)藉以了解 DUT 可以偵測到的攻擊，Evasion 的技術中包含「Fragmentation and Timing」及「URL Obfuscation」。Attack Mitigation Performance Under Load 測試是要讓 DUT 在不同速度的 background traffic 情形下，對於攻擊的偵測能力為何。至於 Latency & User Response Times 是測試當 background traffic 為正常或攻擊流量時，DUT 的 Latency

及 User Response Times 表現為何，Latency 是用 SmartBits/SmartFlow 來衡量而 User Response Times 是用 Avalanche/Reflector 來評估，表 7 摘要了 Attack Mitigator 每個 Section 的測試群組。

Section	Test Group
Detection Engine	Test 1.1 - Attack Detection/mitigation Test 1.2 - High Volume Attack Detection/Mitigation Test 1.3 - Resistance To False Positives
Evasion	Test 2.1 – Baselines Test 2.2 - Fragmentation and Timing Test 2.3 - URL Obfuscation
Attack Mitigation Performance Under Load	Test 3.1 - UDP Traffic To Random Valid Ports Test 3.2 - HTTP “Maximum Stress” Traffic With No Transaction Delays Test 3.3 - HTTP “Maximum Stress” Traffic With Transaction Delays Test 3.4 - Protocol Mix Traffic Test 3.5 - “Real World” Traffic Test 3.6 - Maximum Open Connections
Latency & User Response Times	Test 4.1 – Latency Test 4.2 - User Response Times
Stability & Reliability	Test 5.1.1 - Blocking Under Extended Attack Test 5.1.2 - Passing Legitimate Traffic Under Extended Attack Test 5.1.3 - Resistance to ISIC/ESIC/TCPSIC/UDPSIC/ICMPSIC traffic Test 5.1.4 - Mitigation of ISIC/ESIC/TCPSIC/UDPSIC/ICMPSIC mitigation traffic
Management and Configuration	Test 6.1 - Management Port Test 6.2 - Management & Configuration Features

表 7: Attack Mitigator Certification Program 之測試群組

Intrusion Prevention System (IPS)及 Multi-Gigabit IPS(MGIPS)

在 IPS 這個類別中，NSS Approved 分成四個等級: IPS(Baisc)、IPS + Branch Office、IPS + Enterprise、IPS + ISP/MSP，而 MGIPS 中是分成三個等級: MGIPS (Basic)、MGIPS + Enterprise、MGIPS + ISP/MSP。IPS 效能測試最高可測 1Gbps 而 MGIPS 最高可測 4Gbps，在功能面的測試方法上兩者都一樣，Attack Recognition 的攻擊類別包括 High Severity attacks、Medium Severity attacks、Low Severity attacks、Audit only、Reconnaissance、DOS/DDOS、P2P (optional)、Spyware (optional)、Server-to-Client Exploits (optional)等等，Resistance To False Positives 可利用錄到的一般流量搭配測試，在 Evasion 的技術中包含了 Packet Fragmentation、Stream Segmentation、RPC Fragmentation、URL Obfuscation、HTML Obfuscation、FTP Evasion 等等，表 8 摘要了 IPS/MGIPS 每個 Section 的測試群組。

Section	Test Group
Detection Engine	Test 1.1 - Attack Recognition Test 1.2 - Resistance To False Positives Test 1.3 - Resistance To False Negatives
Evasion	Test 2.1 – Baselines Test 2.2 - Packet Fragmentation Test 2.3 - Stream Segmentation Test 2.4 - RPC Fragmentation Test 2.5 - URL Obfuscation

	Test 2.6 - HTML Obfuscation Test 2.7 - FTP Evasion Test 2.8 - Miscellaneous Evasion Techniques
Stateful Operation	Test 3.1 - Maximum Simultaneous Open Connections Test 3.2 - Behavior Of The State Engine Under Load Test 3.3 - Stateless Attack Replay (Mid-Flows)
Detection/Blocking Performance Under Load	Test 4.1 - Raw Packet Processing Performance (UDP Traffic) Test 4.2 - HTTP Maximum Capacity Test 4.3 - HTTP Capacity With No Transaction Delays Test 4.4 - HTTP Capacity With Transaction Delays Test 4.5 - "Real World" Protocol Mix Traffic
Latency & User Response Times	Test 5.1 – Latency Test 5.2 - User Response Times
Stability & Reliability	6.1.1 Blocking Under Extended Attack 6.1.2 Passing Legitimate Traffic Under Extended Attack 6.1.3 ISIC/ESIC/TCPSIC/UDPSIC/ICMPSIC 6.1.4 Policy Push 6.1.5 Power Fail 6.1.6 Redundancy 6.1.7 Fail Open (Power Fail) 6.1.8 Fail Open (Resource Issues) 6.1.9 Fail Closed (Power Fail) 6.1.10 Fail Closed (Resource Issues) 6.1.11 High Availability (HA) Option (Stateful) 6.1.12 High Availability (HA) Option (Non-stateful) 6.1.13 Persistence Of Data 6.1.14 IPV6
Management and Configuration	Test 7.1 - Management Port Test 7.2 - Management & Configuration – General Test 7.3 - Management & Configuration – Policy Test 7.4 - Management & Configuration - Alert Handling Test 7.5 - Management & Configuration - Reporting

表 8: IPS 及 MGIPS Certification Programs 之測試群組

Secure Content Appliance (SCA)

NSS 定義了一個 SCA 的產品可能包含了以下幾種功能: Anti Malware、Anti Spam、Content Filtering 以及 Web Filtering，在 Baseline 的效能測試中會將所有功能先關掉才測試，Baseline Throughput 是以 Smartflow 進行，測試 DUT 的 maximum UDP throughput，可容忍的 packet loss rate 是 0 而測試的封包大小包括 64, 128, 256, 512 及 1024。在 Anti Malware、Anti Spam 及 Content/Web Filtering 的測試中所用到「不好的」內容與 UTM Anti-Virus、Anti Spam 及 Content Filtering 中的內容是大同小異，表 9 摘要了 SCA 每個 Section 的測試群組。

Section	Test Group
Baseline	Test 1.1 - Performance Comparison – Baseline Test 1.2 - Baseline Throughput Test 1.3 - Baseline Latency
Anti Malware	Test 2.1 - Performance Comparison - Anti Malware Test 2.2 - Anti Malware Performance With Varying File Sizes Test 2.3 - HTTP Anti Malware Filter Test 2.4 - SMTP Anti Malware Filter Test 2.5 - Anti Malware Capabilities

Anti Spam	Test 3.1 - Performance Comparison - Anti Spam Test 3.2 - SMTP Anti Spam Filter Test 3.3 - Anti Spam Capabilities
Content/Web Filtering	Test 4.1 - Performance Comparison - Content/Web Filtering Test 4.2 - HTTP URL Filter Test 4.3 - HTTP Content Filter Test 4.4 - SMTP Content Filter Test 4.5 - HTTP File Blocking Test 4.6 - SMTP File Blocking Test 4.7 - Content Filtering Capabilities
All Modules	Test 5.1 - Performance Comparison - All Modules
Management and Configuration	Test 6.1 - Management & Configuration Features

表 9: SCA Certification Program 之測試群組

Web Application Firewall (WAF)

本項類別是要測試與 Web 相關的安全防護技術，所用到的 Web 攻擊主是要根據「Open Web Application Security Project (OWASP)」(www.owasp.org)中，排行前 10 名最嚴重的漏洞所產生的相對應攻擊，例如 Buffer Overflows、Hidden Field Tampering、Cross Site Scripting (GET)、Cross Site Scripting (POST)、Parameter tampering、Input Validation、Injection Flaws、Broken Authentication、Cookie Poisoning、SQL Injection、Invalid Request、Forceful Browsing、Information Disclosure、Common Exploits 等等，表 10 摘要了 WAF 每個 Section 的測試群組。

Section	Test Group
Detection Engine	Test 1.1 - Attack Recognition
Evasion	Test 2.1 - URL Obfuscation
Performance Under Load (No Security Policies Applied)	Test 3.1 - UDP Traffic To Random Valid Ports Test 3.2 - Maximum Capacity HTTP Traffic
Performance Under Load (Security Policies Applied)	Test 4.1 - Standard Spirent Avalanche Traffic Test 4.2 - NSS Home Page Only - No Images Test 4.3 - NSS Home Page + Ten Associated Images Test 4.4 - Maximum Open Connections
Latency & User Response Times	Test 5.1 – Latency
Stability & Reliability	6.1.1 Blocking Under Extended Attack 6.1.2 Passing Legitimate Traffic Under Extended Attack 6.1.3 ISIC/ESIC/TCPSIC/UDPSIC/ICMPSIC
Management and Configuration	Test 7.1 - Management Port

表 10: WAF Certification Program 之測試群組

Test Equipment

NSS 測試中所使用的工具各式各樣，包含商業軟體/儀器以及一些 Open Source 的工具，表 11 列出其所使用的工具及用途。

測試工具名稱	廠商	目的
SmartBits SMB-6000/SMB-600	Spirent Communications	高 port 數之網路產品效能分析儀器，可藉由安裝在 windows 上的軟體，透過網路來控制測試、分析結果。
Avalanche/Reflector 2500	Spirent Communications	更具真實性的測試流量。用來模擬

		clients/servers，支援的 application 的種類包括 HTTP(S)、FTP、Streaming、MMS、POP3、SMTP、Telnet 以及 DNS。
Adtech AX/4000	Spirent Communications	高效能測試儀器，以 FPGA 的硬體架構設計而成，支援 Ethernet、ATM 及 Frame Relay，最高速可到達 10Gbps。
VRS	Assurent	Assurent 所提供的 Vulnerability Research Service (VRS)，會產生相關弱點資訊，足以讓 VA probe、IPS filter 產品寫出對應的 script，除了給予"proof of concept" exploit 外，還有對一些較嚴重的弱點寫出完整的"shell code"。
Traffic IQ Pro	Karalon	與 open source 工具 tcpreplay 及 Tomaahwk 類似，為一種流量 replay 工具，可以支援 transparent、router 及 NAT 模式，並且根據 IP address 的改變來修用 application layer 的資料。
CORE IMPACT	Core Security Technologies	IMPACT 是一套自動化的"penetration testing tool"。
Catalyst 6500 Series Switches	Cisco	建置測試環境的主要 switch。
Tomahawk	Open Source Tools	Tomahawk 可用來測試 IPS 產品的效能及阻擋能力，會將錄到的流量(pcap file)分成 client 及 server 兩端，傳輸過程是會依據目前封包是否有傳送成功再繼續下一個封包。
tcpreplay	Open Source Tools	播放時就根據 timestamp 的順序播放，因此適合 switches、routers、firewalls 以及 IPS 等「inline」類型的產品，可指定速度進行播放。
Metasploit Framework	Open Source Tools	這項工具提供一個開發、測試以及使用 exploit 程式碼的平台，有點類似 CORE IMPACT。

表 11: NSS 所使用的測試工具