TWAREN SSL-VPN 之紀錄分析與監控系統實作

林孟璋 張聖翊 廖威捷
財團法人國家實驗研究院國家高速網路與計算中心
{kent, changsy, wjl}@nchc.org.tw

摘要

台灣高品質學術研究網路提供良好的 SSL-VPN 服務，紀錄使用者相關資訊與設備監控成為熱門的重要議題，我們透過紀錄分析方法，淬取紀錄檔中的重要資訊，設計紀錄分析系統供管理者查詢，此外，為了提供良好服務，監控系統亦成為我們設計重點。本文最主要目的為詳述建置 SSL-VPN 服務中的紀錄分析與監控系統實作部分，在使用 SSL-VPN 服務日漸頻繁的現今社會，該系統有效管理使用者與提升更好的服務品質。

關鍵字: 台灣高品質學術網路(TWAREN)、SSL-VPN(Secure Socket Layer Virtual Private Network) 、紀錄分析器(Log Analyzer)、網路監控。

1. 前言

TWAREN(TaiWan Advanced Research and Education Network)SSL-VPN 服務，最主要提供學術單位良好的安全虛擬網路，讓申請 SSL-VPN 服務的使用者在公眾網路上連接回所屬服務單位，存取原單位的相關資源，並且省去斥資設置專線的成本，即可擁有如專線般的安全傳輸。舉例來說，當學生在校外使用公眾網路，但卻想要存取自己學校圖書館期刊文章時，即可使用 SSL-VPN 服務，取得自己學校的 IP，使用圖書館的期刊下載等各項服務。TWAREN SSL-VPN 透過 VPLS(Virtual Private LAN Service)技術，讓申請的連線單位擁有如專線般的服務，提供終端使用者穩定的連線需求。然而管理與查詢使用單位的相關紀錄與連線資訊，成為 TWAREN SSL-VPN 服務上的一個重要議題，我們設計 SSL-VPN 紀錄分析與監控系統，讓管理人員查詢使用 SSL-VPN 服務的相關歷史紀錄與數據報表，並且監控設備狀態，以利 SSL-VPN 的服務更盡善盡美。

2. 議題

2.1. TWAREN SSL-VPN 架構

目前 TWAREN SSL-VPN 服務由 Cisco ASA5550 與 Juniper SA6500 所構成。TWAREN SSL-VPN 服務建置初期， SSL-VPN 接取系統由 8 部 Cisco ASA 5550 設備所組成，其中 TWAREN 南科機房有 6 部，TWAREN 竹科機房有 2 部，設定為叢集架構以提高系統之處理能力與確保高可用度，對外連接 TWAREN 骨幹網路以通往 Internet，對內則連接 VPLS 網路以通往 12 個 GigaPOP 點，之後為了提高效率及服務更多使用者，採購 Juniper SA6500 一台，此設備同時提供 5000 個連線服務，並賦予連線單位管理者更有彈性的管理介面與連線紀錄，下圖 1 為 TWAREN SSL-VPN 服務架構圖

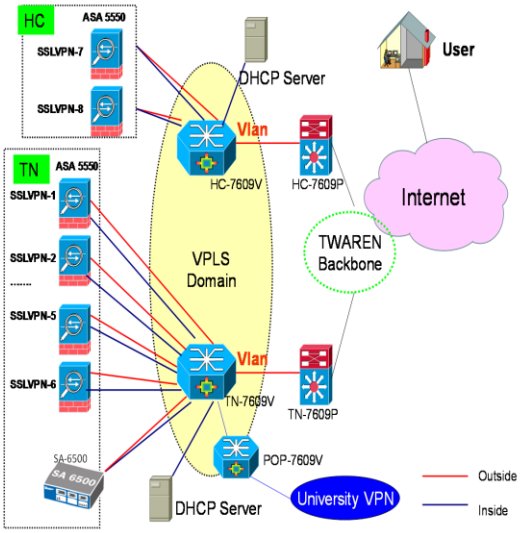

圖 1 TWAREN SSL-VPN 架構圖

2.2. SSL-VPN 紀錄分析與監控系統

然而我們提供 SSL-VPN 服務的同時，對於使用者的使用情形更是密切關注的議題，為了有效約束使用者透過 SSL-VPN 在 Internet 上的濫用情形，以及提供原學校單位查詢紀錄所用，我們精心設計了紀錄分析系統，該系統有效紀錄使用者透過那個 IP 連上 SSL-VPN，以及透過原學校單位的那個 IP 存取 Internet 資源，並且詳盡紀錄使用者使用 SSL-VPN 的時間及流量相關資訊。紀錄分析系統的目的將這些原始資料，經過分析，淬取出有效關鍵的紀錄，供管理者查詢。除此之外，為了維運 SSL-VPN 服務更加順利，我們設計 SSL-VPN 監控系統，能有效掌握目前該設備的狀態，提供目前設備的使用狀況，以提高 SSL-VPN 服務的可用率。目前 Cisco ASA5550 紀錄分析系統已上線，提供連線單位管理者使用，但由於紀錄資料頗為龐大，查詢時的回應時間略顯緩慢，因此我們重新構思其淬取紀錄的方法，能使回應時間縮短，並且隨著 Juniper SA6500 加入提供服務，將 Juniper SA6500

的紀錄查詢及監控系統一併納入，並開放上線，對於日後使用 SSL-VPN 服務更臻緻完美。

3. 系統架構分析

3.1. SSL-VPN 數據來源

當一個 SSL-VPN 的使用者登入我們 TWAREN SSL-VPN 服務系統時，如同使用 Internet 般，都會留下相關訊息，然而因為在登入過程中，需透過學校的認證伺服器，例如 Radius Server，做帳號的確認，但我們不可能取得連線學校的相關登入資訊，但在 TWAREN SSL-VPN 設備的紀錄(Log)檔中，確有使用者相關帳號的行為紀錄，以這些紀錄檔當成資料來源，進行分析比對，擷取出重要的紀錄，成為該使用者的登入資訊。此外我們透過 SNMP 的方式，取得設備的各項資訊，例如介面的流量、設備的 CPU 值、記憶體的使用率等等，以利之後監控所用。

3.1.1. Log 資料分析

由於紀錄檔所紀錄的資訊太過繁雜與龐大，如果直接將 SSL-VPN 所產生的紀錄檔提供管理者查詢，不僅查詢緩慢，對於管理人員查詢上更是一大難題，況且日後儲存這些紀錄檔更是麻煩，因此我們以紀錄檔中的紀錄識別碼(Log identifier)做為分析依據，以 Cisco ASA5550 設備而言，使用者結束 SSL-VPN 服務時，設備會紀錄識別碼為 113019 的一筆記錄，裡面紀錄使用者登入時間、上線 IP、帳號、使用時間長度、輸出流量、輸入流量等資訊，如圖 2 所示。除此之外，為了取得使用者的 DHCP IP，透過過濾識別碼為 722051 的這一筆紀錄，取得相關資訊。

以 Juniper SA6500 來說，同樣有著相同的紀錄模式可依循，當使用者結束 SSL-VPN 服務，關閉期程(Session)時，系統會產生紀錄識別碼為 NWC23464 與 JAV20023 這兩筆紀錄，這兩筆資料可以得到如同 ASA 5550 的資訊，比較特別的，當使用者透過網頁使用 WebVPN，或者透過 NC(Network Connect)這組應用程式使用 SSL-VPN，都可以透過這兩組紀錄識別碼過濾出使用者的相關資訊。最後透過程式撰寫將這些紀錄從龐雜的紀錄群中取出，寫進資料庫做日後查詢使用。

ServerDateTime	WhichASA	DateTime	MessageID	Message
2009-11-18 10:50:55	hc-asa2	2009-11-18 11:02:20	113019	Group = ncnu.edu.tw, Usernam
2009-11-18 10:50:55	hc-asa2	2009-11-18 11:02:20	722037	Group <NCNU> User <... 004
2009-11-18 10:50:55	hc-asa2	2009-11-18 11:02:20	716002	Group <NCNU> User <... 004
2009-11-18 10:47:38	tn-asa5	2009-11-18 10:59:03	734001	DAP: User w... 9@wlan.nthu.e
2009-11-18 10:47:38	tn-asa5	2009-11-18 10:59:03	722051	Group <NTHU> User <w... 9@wl
2009-11-18 10:47:38	tn-asa5	2009-11-18 10:59:03	722022	Group <NTHU> User <w... 9@wl
2009-11-18 10:47:30	tn-asa5	2009-11-18 10:58:55	716001	Group <NTHU> User <w... 9@wl
2009-11-18 10:47:38	tn-asa5	2009-11-18 10:59:03	722033	Group <NTHU> User <w... 9@wl
2009-11-18 10:47:30	tn-asa5	2009-11-18 10:58:55	734001	DAP: User w... 9@wlan.nthu.e
2009-11-18 10:42:13	hc-asa2	2009-11-18 10:53:37	734001	DAP: User s... 004, Addr 16
2009-11-18 10:42:13	hc-asa2	2009-11-18 10:53:37	722022	Group <NCNU> User <s... 004
2009-11-18 10:42:13	hc-asa2	2009-11-18 10:53:37	722051	Group <NCNU> User <s... 004
2009-11-18 10:42:13	hc-asa2	2009-11-18 10:53:37	722033	Group <NCNU> User <s... 004
2009-11-18 10:41:55	hc-asa2	2009-11-18 10:53:20	716001	Group <NCNU> User <s... 004
2009-11-18 10:41:55	hc-asa2	2009-11-18 10:53:20	734001	DAP: User s... 004, Addr 16

圖 2 ASA5550 紀錄檔圖

3.1.2. 監控資料蒐集

SNMP(Simple Network Management Protocol)是網管監控最常使用的技術之一，透過 SNMP MIB 的方式，輸入想要監控標的的 OID(Object identifier)，就可得到設備狀況數據，同樣的 Cisco ASA5550 以及 Juniper SA6500 都擁有我們想要監控標的 MIB 值，透過程式可取得監控標的值。例如，以 Juniper SA6500 來說，需要取得當時登入 WebVPN 的上線人數。我們參照 Juniper SA6500 及 Cisco ASA5550 的 MIB 描述檔，簡略描述如表 1 及表 2，透過程式處理其回應字串，取得我們所想要的監控標的，

表 1 Juniper SA6500 監控標的 OID

監控項目(說明)	MIB OID
signedInWebUsers(透過網頁登入的使用人數)	1.3.6.1.4.1.12532. 2
iveCpuUtil(CPU 使用率)	1.3.6.1.4.1.12532.10
iveConcurrentUsers(目前上線人數)	1.3.6.1.4.1.12532.12
blockedIPList(封鎖 IP 列表)	1.3.6.1.4.1.12532.26

表 2 Cisco ASA5550 監控標的 OID

監控項目 (說明)	MIB OID
crasNumSessionsMIB(每台 ASA 目前上線 Session 數)	1.3.6.1.4.1.9.9.392.1.3.1.0
crasNumUsersMIB(使用人數)	1.3.6.1.4.1.9.9.392.1.3.3.0
cpmCPUTot-al5minMIB(每五分鐘 CPU 值)	1.3.6.1.4.1.9.9.109.1.1.1.5.1
ifOperStatusMIB(介面狀態)	1.3.6.1.2.1.2.2.1.8
ipAdEntAddrMIB(子介面位址)	1.3.6.1.2.1.4.20.1.1
ipAdEntNetMaskMIB(子介面網路遮罩)	1.3.6.1.2.1.4.20.1.3
ipAdEntIfIndexMIB(子介面 ifIndex)	1.3.6.1.2.1.4.20.1.2

此外，對於無法透過 SNMP 方式取得資料，亦或者無法透過 Trap 主動發出設備告警的情況下，我們透過其他方式取得相關資料，例如某連線單位的使用 SSL-VPN 的流量，我們進而透過監控連線單位的 VPLS VLAN 介面取得。

3.2. SSL-VPN 數據彙整與儲存

SSL-VPN 記錄分析與監控的最終目的，為數據查詢與呈現，有良好的資料庫設計，更能加速查詢回應時間。依照系統開發流程，首先訪查管理人員需要查詢使用者哪些紀錄，或者維運人員需監控標的項目，才開始進入資料庫設計階段。以紀錄查詢功能來說，因為一個使用者登入並使用服務所產生的紀錄頗多，我們想要的資料分散於多筆紀錄中，不可能一次取得所有想要的關鍵資料，也因此在設計資料庫時，我們用了不少關連(Relation)方法，讓使用者的使用行為紀錄，分散在不同的資料表(Table)，但彼此做參照(Reference)，讓資料更有系統的儲存在資料庫中，以利於後續的網頁開發。

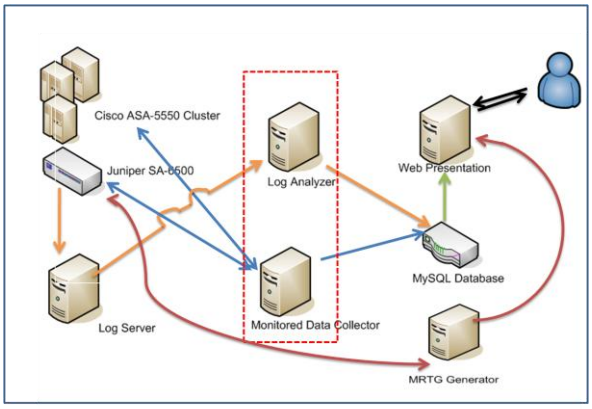

圖 3 記錄分析與監控資料蒐集模組

4. 系統設計與實作

4.1. 系統功能模組化

系統開發上，最主要由兩大模組構成，第一為紀錄分析器，分別收集 Cisco ASA5550 與 Juniper SA6500 的紀錄檔，我們並非直接對 SSL-VPN 設備存取紀錄檔，而是透過紀錄伺服器(Log Server)去接收這些紀錄，最主要的原因為，SSL-VPN 的設備紀錄量頗為龐大，與其讓紀錄檔佔滿了磁碟，不如交由紀錄伺服器儲存這些紀錄，所有的原始紀錄檔，就儲存在紀錄伺服器中，之後再透過程式方式解析紀錄檔，此模組不僅擔任解析紀錄檔的角色之外，更把使用者的登入資訊擷取重要訊息寫入資料庫中，其角色在系統模組中，如圖 3 的 Log Analyzer 所示。

在系統實作上另一大模組為監控資料收集模組，負責針對監控資料作收集動作，有鑑於網管監控軟體 Web 圖形化，我們也朝圖形化的風格呈現監控狀態，以最常見的軟體 MRTG 為例，MRTG 雖為以時間序列的方式儲存並呈現資料，但時間過一陣子之後，原始資料會被忽略與壓縮，對於日後需要查詢歷史紀錄，與產生報表將是一大難題，因此我們構思長期儲存監控資料的方案，擁有這些資料，不僅對於歷史紀錄的報表呈現有很大幫助，對於日後分析使用者行為更是一大利器。這些長期儲存歷史資料，在已開發的網管監控與告警系統上[1][2][3]已被使用且運行多年，擁有歷史的監控數據，對於日後網路趨勢告警及異常行為偵測上，有著莫大的幫助。此模組透過 SNMP MIB 分別取出監控資料，並寫入資料庫，其扮演的角色如圖 3 的 Monitored Data Collector。

4.2. 設計資料表

4.2.1. 紀錄分析資料庫階層化

當在設計與開發系統時，透過解析紀錄檔所得到的資料還是非常的大，每一個使用者使用 SSL-VPN 所產生的紀錄量非常的多，然而如果網頁程式直接存取這個資料庫，回應時間會非常的長，造成查詢者的怨聲載道，因此有了階層式資料庫的構想，針對資料庫我們設計分成原始紀錄資料庫(Raw Log databases)與後製資料庫(Prepared Log databases)，透過紀錄解析器(Log Parser)與紀錄分析器(Log Analyzer)分別將資料寫入這兩個相關資料庫。原始紀錄表等於是原始紀錄檔的快照(Snap)，透過紀錄解析器，原始紀錄檔所紀錄的任何資訊，一一寫入原始紀錄資料庫，而且欄位設計上，也是列舉出所有與記錄檔有關的相對應欄位，但原始紀錄資料庫不會是網頁直接擷取資料的來源，而是之後的後製記錄資料庫。

紀錄分析器最主要工作，是透過程式執行 SQL 語言(Structured Query Language)，以 LogID 欄位中特殊的號碼，以及 Message 這個欄位中的特殊的字元為搜尋條件，將原始紀錄資料庫蒐集至後製記錄資料庫，這些資料庫的資料雖已被精簡，但不失真，並且可以供程式做有效率的查詢。整個原始紀錄檔處理的流程如圖 4，及紀錄分析處理程式虛擬碼(pseudo code)如圖 5 所示。

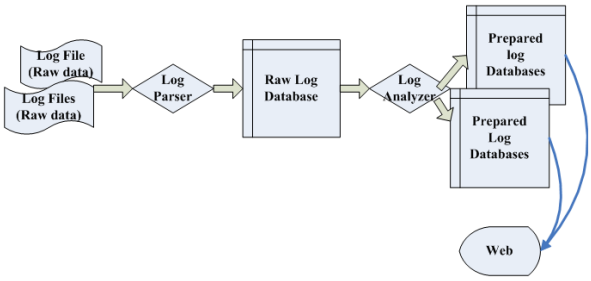

圖 4 紀錄分析階層化流程圖

```
//Log Analyzer for ASA5550
• InsertRawLogToPreparedLog(){
• array=query("select * from RawLogDatabases")
• If array[LogId]=113019
•   InsertPreparedDatabase()
• elseif array[Message] include 'SVC' and array[LogID]=722051
•   InsertPreparedDatabase()
• endif
• }
```

圖 5 紀錄分析虛擬碼

4.2.2. 監控標的資料表

本章節為 SSL-VPN 系統即時監控之資料庫 Table 設計，以下分別詳細描述：

◆ Device Table:

記載 SSL-VPN 設備 ID 與名稱對應資訊。

欄位	Type	說明
DeviceID	int	設備 ID 編號
DeviceName	varchar	設備名稱
DeviceIP	varchar	設備 IP，供 SNMP 查詢使用

◆ Device CPU Table:

記載 SSL-VPN 設備即時 CPU 資訊。

欄位	Type	說明
DeviceID	int	設備 ID 編號
CheckTime	datetime	SNMP 檢查時間點
CurrentCPU	int	設備 CPU 使用率

◆ Device User Table:

記載 SSL-VPN 設備上線使用人數資訊。

欄位	Type	說明
DeviceID	int	設備 ID 編號
CheckTime	datetime	SNMP 檢查時間點
CurrentUsers	int	設備上線使用人數

◆ Interface Table:

記載 SSL-VPN 設備上介面描述資訊。

欄位	Type	說明
DeviceID	int	設備 ID 編號
IfIndex	int	介面索引值
IfDescription	varchar	介面描述(ex.NCHC)

◆ Interface Status Table:

記載 SSL-VPN 設備上介面的所有資訊。

欄位	Type	說明
DeviceID	int	設備 ID 編號
IfIndex	int	介面索引值
CheckTime	datetime	SNMP 檢查時間點
IpAddress	varchar	介面設定 IP 位址
NetMask	varchar	IP 位址子網路遮罩
Status	varchar	介面即時狀態值

4.3. 網頁資料呈現與系統展示

4.3.1. 系統紀錄查詢介面

現今個人資料隱私備受關切，在設計網頁時，我們考量到這點，因此連線單位管理者申請連線紀錄查詢系統時，會有權限控管，也就是說，連線單位只能看到自己連線單位下所屬使用者的各項紀錄，確保各連線單位間的隱私安全。例如一個申請 Cisco ASA5550 的記錄查詢管理者，登入之後，只能限制查詢這個群組(Group)下，所擁有的連線訊息，沒辦法查到其他群組的相關資訊;同理，申請 Juniper SA6500 的管理者，也僅能查詢到屬於自己 IVE(Instant Virtual Extranet)的相關連線訊息。

在登入系統後，最高權限管理者可以透過選擇查詢哪一個群組或是 IVE 的相關訊息，並提供時間區間供查詢，選擇妥當查詢條件之後，按下查詢按鈕，即可在網頁上顯示登入時間、登出時間、使用者帳號、登入 IP、DHCP 配置的 IP、使用時間等相關資訊，如圖 6 所示。除了使用者紀錄查詢，紀錄相關報表也是我們開發的項目之一，同樣是透過輸

入要查詢的群組或是IVE及時間單位區間(年、月)，就可以查出這個時間區間的使用人數，以圖形化方式呈現，如圖 7。

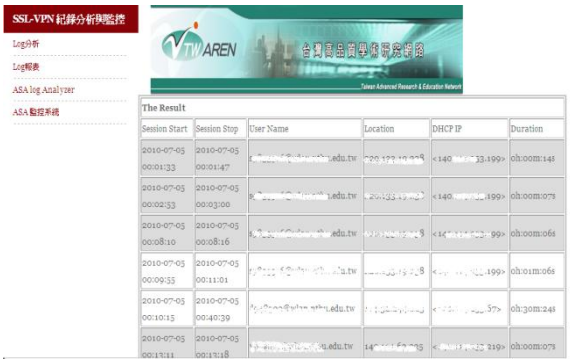

圖 6 使用者記錄查詢系統

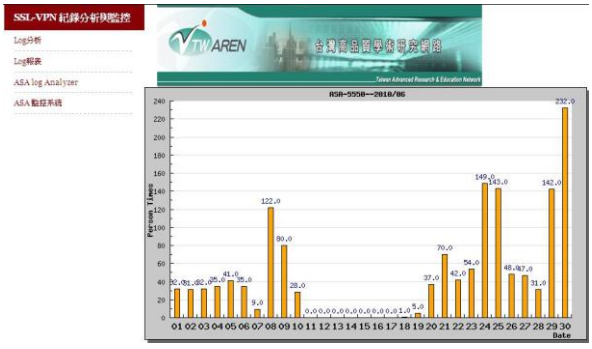

圖 7 當月使用人數報表

4.3.2. 系統即時監控畫面

在系統即時狀況監控部份，系統可以查看每台 SSL-VPN 設備提供給每一間連線單位之設備介面狀態：包含設備名稱、介面名稱、介面 IP、檢查時間、介面狀態，如圖 8，TN-ASA6 設備介面在 2010 年 7 月 26 日上午 11:40，設備上之國網中心的介面狀態從 UP 變成 DOWN，系統管理人員可以從網頁上監控資訊，達到迅速發現問題解決問題之功效，以提供給使用者一個高穩定性之 SSL-VPN 系統。

圖 8 SSL-VPN 系統即時監控狀態

圖 9 為每一台 SSL-VPN 設備即時上線使用人數監控圖表，可供系統管理人員了解目前每一台設備之使用狀況。

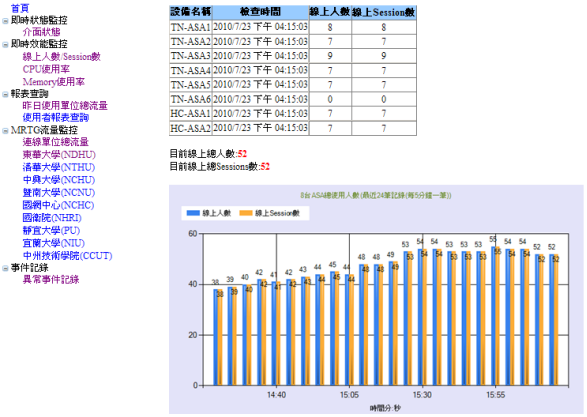

圖 9 SSL-VPN 系統即時上線人數監控圖表

為了監控每一間連線單位流量，本系統整合 MRTG 網路流量監控工具，系統管理員可以從網頁上查看每一間連線單位之使用狀況，我們亦將流量資料存入資料庫，以利後續統計報表開發。

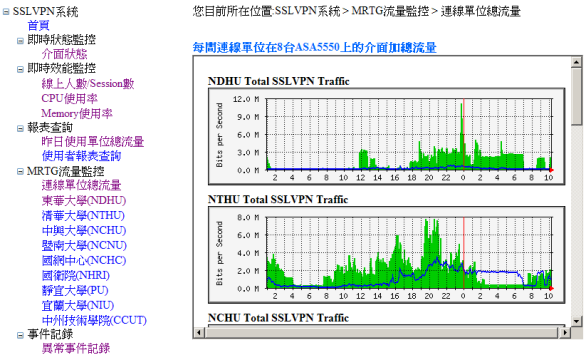

圖 10 SSL-VPN 系統即時流量監控

5. 結論與未來工作

SSL-VPN 日漸普及的今日，使用者相關紀錄是需要被有系統化留存的，因此有了紀錄查詢系統的需求，透過紀錄分析器，取出管理者想要的資訊，幫助管理者追蹤相關連線上的資訊，對於 SSL-VPN 管理上有著相當的幫助，並且，隨著服務滿意度日漸高昇的需求，監控 SSL-VPN 已成了維運團隊重要的一環，日後，SSL-VPN 的監控標的會日漸增加，透過各種方式取得所想要的監控標的，這是我們努力的方向，以利 SSL-VPN 服務達到更完美的境界。

參考文獻

[1] 梁明章、曾金山、張聖翊、廖威捷、謝新叡，

TWAREN 混和式網路監控系統之設計與實作，TANet2008 論文集，高雄，2008 年 10 月。

[2] 曾金山、劉德隆，台灣高品質學術研究網路整合式監控平台設計與實作，TANet2007 論文集，台北，2007 年 10 月。

[3] 張聖翊、謝欣叡，TWAREN 光網路之光通道服務異常警報系統平台開發，TANet2008 論文集，高雄，2008 年 10 月。

[4] 謝孟芳，在 IXDPG425 嵌入式系統上建置強安全性之虛擬私有網路，國立中興大學電機工程學系研究所碩士論文，台中，2007 年 6 月。