硬體式防火牆運用於國軍網路之研究

作者／丘國富 少校

提要

近年來，網路安全問題仍舊是一個很熱門的討論話題，儘管國軍網路(Minet)是建構在與網際網路(Internet)實體隔離政策的基礎下，惟網際網路的互聯性及無線網路技術的發展日新月異，加上駭客技術不斷翻新及內部使用者對網路的不當存取，造成各種有形及無形的攻擊事件或單位內部資料外洩的情事一再發生。因此，建置適當之防火牆以防護內部網路之安全實有其必要性。本文提出硬體式網路防火牆，運用於國軍網路之架構，來說明如何提昇國軍網路之安全，進而達到內部網路及資訊系統防護之功能。

前言

近期國軍對於資訊安全的重視不斷地持續上昇並搭配相關的因應措施，主要是由於電腦及周邊資訊儲存媒體與電子設備的越來越便利及普及，網路構連技術也不斷地提昇，進而衝擊國軍資訊網路安全，儘管國軍一再要求網路實體隔離政策，仍然有洩密及內部網路遭受入侵攻擊等事件發生，探究其原因，係由於網際網路的互聯性及無線網路技術的發展快速，加上近期國際（中共）駭客技術不斷翻新及內部使用者資訊防護意識淡薄，才會造成各種有形及無形的攻擊防不勝防，雖然電腦及網路帶給人們日常生活上各項的便利性，但就如同古語所說“水能載舟，亦能覆舟”，它也同時成為犯罪者的最新工具。

「安全與便利」的平衡一直是資訊安全最難解決的問題，國軍近年來不斷地投資大量的人力及預算在資訊安全工作上，並改善相關的軟硬體設施，尤其是各單位的防火牆設備，全面採用具有自適型安全裝置的新型硬體防火牆設備，目的就是要強化國軍內部網路及資訊系統之安全。然而大量的投資軟硬體設備，若是資訊作業人員未能靈活運用或不善於操作，是否會獲得相對應的成效，是一個值得討論的問題，故本研究以硬體防火牆為基礎，來說明如何運用於現行國軍網路架構中，提昇單位之網路安全。

本文首先概述防火牆概論，說明防火牆之定義、防火牆之相關技術與種類，再者介紹硬體式網路防火牆，最後提出如何將硬體防火牆運用於現行國軍網路之架構分析，希望透過本文提出之架構說明，使其成為兼具理論與實用之防火牆系統，以供網路作業人員及一般使用者之基本認知，提昇單位內部之網路作

業安全。

本文

根據統計，資安事件威脅的來源，約 15%是屬於環境的威脅，約 85%來自人的威脅，而人的威脅部份，其中以內部人員所佔的比例最多。國軍近幾年來持續推動網路實體隔離政策，部份單位還是有網路受到攻擊或資料外洩的情事發生，探究其原因都屬於內部的使用者不當使用網路所造成，因此建置適當的防火牆有其必要性。

防火牆概論

綜觀有關於防火牆系統的研究非常之多，討論的議題也非常廣泛，本文僅整理和探討與主題較有關之代表性論點。分述內容如下：

一、防火牆的定義

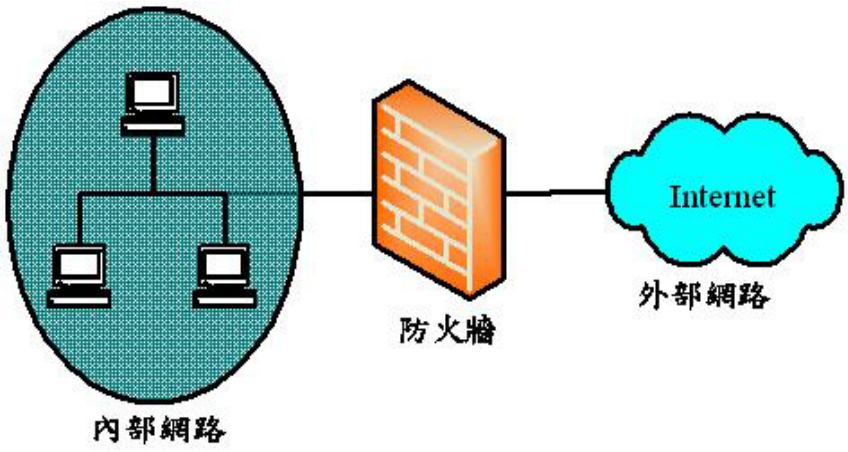
防火牆是建立在兩個網路之間的安全政策，用來過濾掉某些不可靠的資料封包，藉以阻止網路駭客(Hacker)的入侵，並提供稽核及控制存取網路資源等服務[1]。圖一為防火牆的基本架構圖，由圖中顯示架設防火牆系統之後將網路一分為二：

(一)外部網路(External Network)

外部網路為不可信任的網路，如開放式的網際網路。

(二)內部網路(Internal Network)

內部網路為可信任的網路，如受保護單位的內部網路。



圖一 防火牆基本架構圖

（資料來源：作者繪製）

[1] 伍恩祺，唐遜，ISA Server 2000，初版（台北市：碁峰資訊，民國 90 年 6 月），頁 4。

架設好防火牆系統之後，在正常情況下所有的封包，無論封包是從外部網路要進到內部網路，或是從內部網路要到外部網路，都應先經過防火牆的檢查，而防火牆只放行允許的資料封包通過，因此它在內部網路與外部網路之間建立了一個屏障。只要安裝一個簡單的防火牆，就可以屏蔽掉大多數外部網路的探測與攻擊，增加了內部網路的安全性。

二、防火牆的技術型態

一般來說，防火牆的技術型態可分為封包過濾器及代理伺服器兩種，然而大多數的防火牆，混合採用這兩種基本技術型態來加以建構。以下就分別敘述封包過濾器及代理伺服器兩種防火牆的工作原理。

(一)封包過濾器(Packet Filter)

封包過濾器是屬於網路層的防火牆(Network-Level Firewall)，而網路層是開放系統互連(Open System Interconnection, OSI)參考模型的第三層，它要解決如何透過具有多個中間節點的通資網路進行資料封包傳送。因此，網路層要決定資料封包在通資網路中傳送的路徑，控制資料封包的流量並防止擁塞等，提供建立、維護和終止網路連接的方法[2]。封包過濾器會對所有經過的封包進行檢查，按照所建立的規則表，來決定封包的處理方式，換句話說封包過濾器會針對封包的標頭加以檢查，藉以過濾掉非允許的封包；通常封包過濾器會檢查每個封包標頭內的四項欄位：

1.來源端的 IP 位址(Source IP Address)。

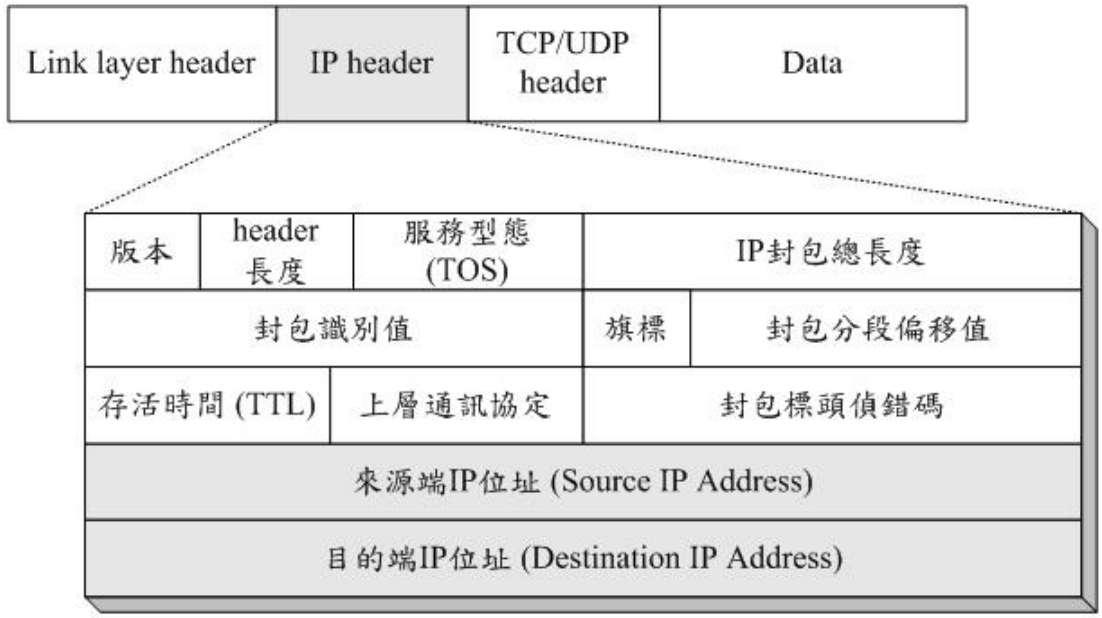
2.目的端的 IP 位址(Destination IP Address)。

3.來源端的 TCP/UDP 埠(Source TCP/UDP Port)。

4.目的端的 TCP/UDP 埠(Destination TCP/UDP Port)。

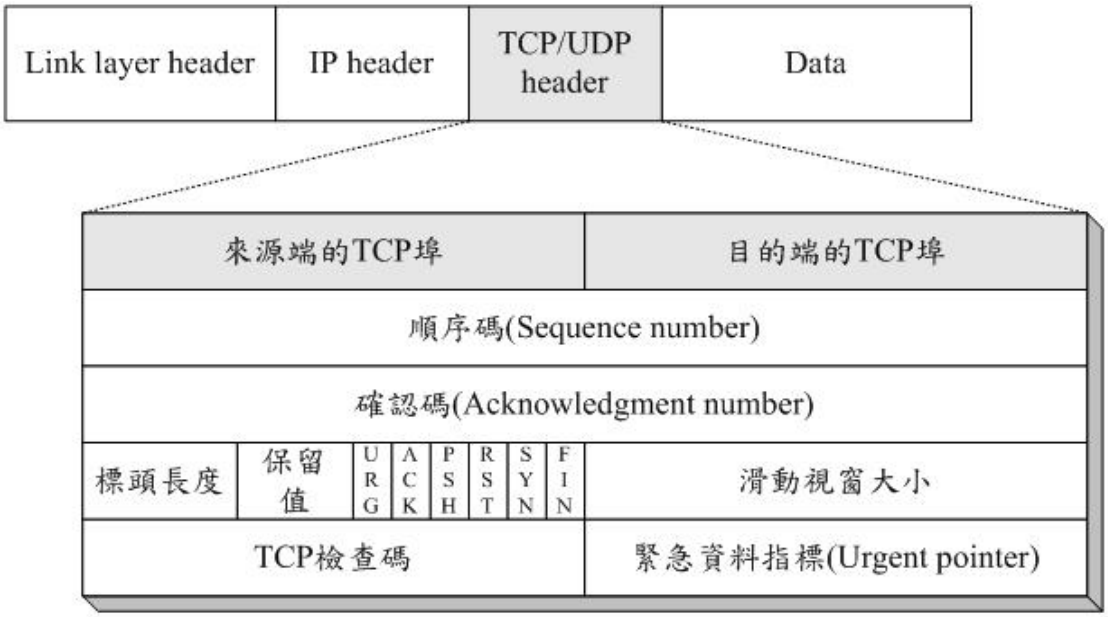
圖二顯示封包在乙太網路傳輸時的結構，來源端及目的端的 IP 位址是放在 IP 表頭(IP Header)的兩個欄位裡，至於來源端及目的端埠值則放在相對應的 TCP 表頭(TCP Header)或 UDP 表頭(UDP Header)的兩個欄位裡。圖三及圖四分別顯示封包在 TCP 層及 UDP 層的結構。

[2] 王信博，資料通訊概論，初版（台北市：金和資訊，民國 93 年 6 月），頁 2-24。



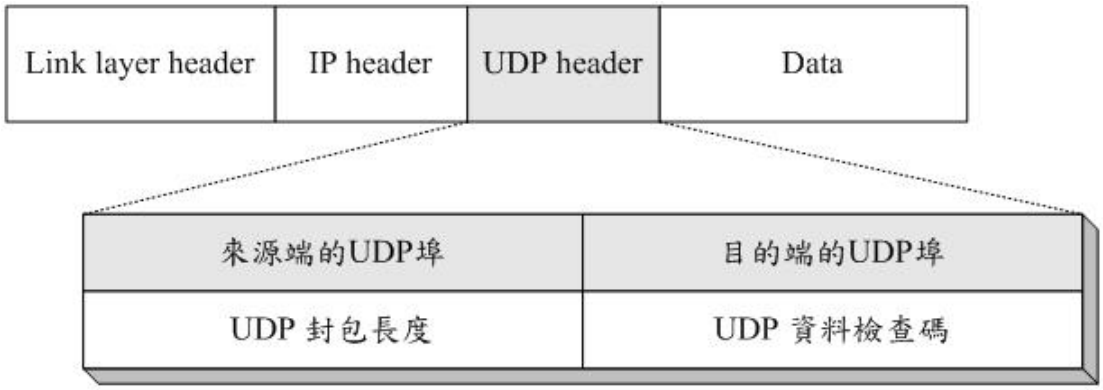
圖二 封包 IP 表頭的結構圖

（資料來源：作者繪製）



圖三 封包 TCP 表頭的結構圖

（資料來源：作者繪製）

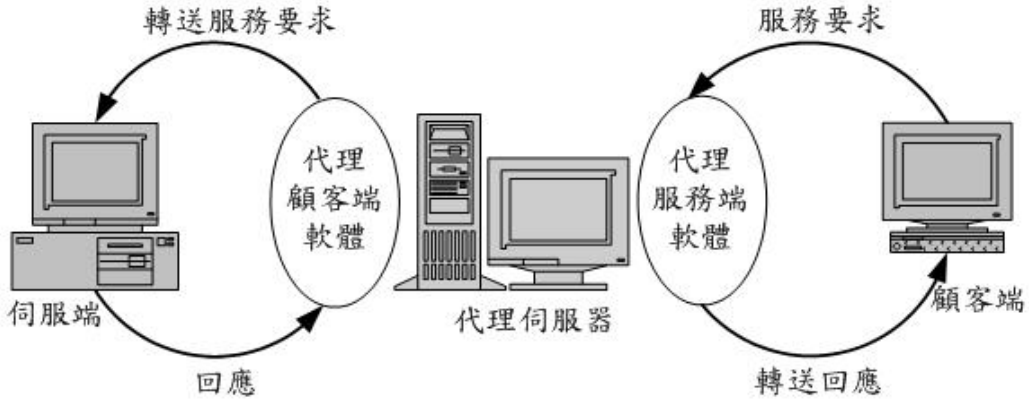


圖四 封包 UDP 表頭的結構圖

（資料來源：作者繪製）

(二)代理伺服器(Proxy Server)

代理伺服器是屬於應用層的防火牆(Application-Level Firewall)，而應用層是開放系統互連參考模型的最高層，應用層和用戶直接打交道，它涉及的協定是很多的，其內容取決於用戶的需要，每個用戶可以自行決定執行什麼程式和使用什麼協定[3]。在網路上有各式各樣的應用服務，提供服務的主機稱為服務端(Server)，而要求服務的主機稱為顧客端(Client)，當系統安裝了代理伺服器，它將負責處理及轉送網路上所提供的應用服務。



圖五 代理伺服器功能示意圖

（資料來源：作者繪製）

上圖五說明代理伺服器如何處理屬於應用服務的封包，在代理伺服器必須要安裝代理服務端及代理顧客端兩個代理軟體，其中代理服務端軟體是用來模

[3] 王信博，資料通訊概論，初版（台北市：金和資訊，民國 93 年 6 月），頁 2-56。

擬遠端真正服務端的行為，代理顧客端軟體則是用來模擬真正顧客端的行為。當顧客端送出請求服務的要求，代理服務端軟體將檢查該要求是否允許，若是允許的要求將轉由代理顧客端軟體送出該服務要求；同樣地當服務端送回服務的結果，代理顧客端軟體將檢查該結果是否允許，若是則轉由代理服務端軟體送回該服務結果給顧客端。

三、防火牆的種類

防火牆的種類就按照它的實際模式，可以將防火牆分為軟體防火牆和硬體防火牆[4]。以下簡單介紹這兩種防火牆。

(一)軟體防火牆

軟體防火牆安裝在隔離內部網路與外部網路的主機上，透過進行安全規則配置、存取控制、日誌管理、網路監控等實現對訊息的篩選過濾功能。個人電腦上所安裝的防火牆都屬於軟體防火牆，如Black Ice個人防火牆、天網個人防火牆、金山網鏢、瑞星個人防火牆等。另外，一些企業級防火牆也都是軟體防火牆，如Checkpoint Firewall、NAI Gauntlet等[5]。

(二)硬體防火牆

硬體防火牆主要採用純硬體設計和固化電腦兩種模式。純硬體設計是指採用ASIC晶片設計實現之複雜指令專用系統，它的作業系統及過濾軟體等都採用定製模式。固化電腦模式係透過裁剪Linux等作業系統核心使其與特殊設計的電腦硬體結合在一起，形成固化的防火牆。目前、固化電腦模式的防火牆是硬體防火牆產品中的主流產品。比較主流的企業級硬體防火牆有Cisco PIX、Net Screen等[6]。

下表一為軟體防火牆與硬體防火牆之比較表。由表可知，雖然硬體防火牆其安全性較軟體防火牆要高，相對的價格要比軟體防火牆要昂貴的多。另外，硬體防火牆安裝上要比軟體防火牆要容易的多，但不懂得運用的話，效果將會大打折扣；相反的，軟體防火牆價格雖然比較低廉，但是假若運用得宜，其效能並不輸給硬體防火牆。

[4] 劉吉，柳靖，駭客攻防實戰詳解，初版（台北市：文魁資訊，民國 96 年 9 月），頁 10-2。
[5] 同註 4，頁 10-3。
[6] 同註 5。

表一 軟體防火牆與硬體防牆之比較

種類 / 特性	軟體防火牆	硬體防火牆
安全性	安全性中	安全性高
價格	低	高
安裝	需對防火牆軟體安裝有相當了解之技術人員	安裝容易
管理	複雜，需對防火牆軟體有相當之了解	需會懂得操作
效能	視安裝之主機而定	高
彈性	高	低
軟體功能	多	低

（資料來源：作者繪製）

硬體式網路防火牆

市面上硬體防火牆產品種類繁多，各家出產的產品都有其特色，功能上也都大同小異，本文僅以國軍近期所建置之硬體防火牆，Cisco ASA 5505 硬體防火牆來說明。Cisco ASA 5505 硬體防火牆是屬於思科公司提供的 Cisco ASA 5500 系列的產品之一，不僅結合了以往硬體防火牆 Cisco Pix 系列產品技術，也大大提昇了網路偵測及防護的功能，以下簡介設備及其特色。

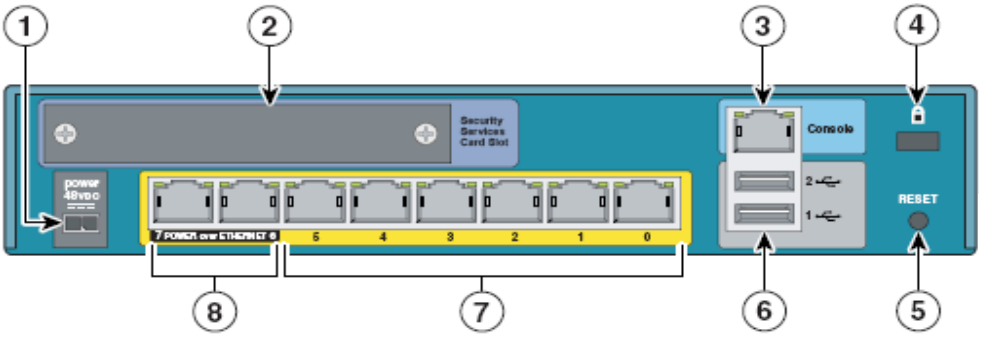
一、Cisco ASA 5505 硬體防火牆簡介

Cisco ASA 5505 硬體防火牆是採用「自適型威脅辨識與解除(Adaptive Identification and Mitigation, AIM)」架構，也是「Cisco 自我防禦網路」的核心元件之一，具備主動式的威脅防禦功能，在威脅散播到網路之前即可終止其威脅攻擊，並且可控制網路上的活動及應用層的資料傳輸，同時還能提供高彈性的虛擬私有網路(Virtual Private Network, VPN)連線能力。如此具有多功能網路安全防火牆，不僅可提供網路安全的深度與廣度，防護單位內部網路的運作，而且還能夠減少網路的佈署與建置成本，同時也降低網路安全的建構複雜度，大幅提高網路安全上的彈性運用。

Cisco ASA 5505 硬體防火牆不僅體積小，且具有高可靠度的延伸能力。圖六為設備的背面圖，它提供 6 個乙太網路(Ethernet)連接埠，可以連接乙太網路設備，另外它也具備兩個可連接網路供電(Power of Ethernet, PoE)裝置的連接埠，可提供網管作業人員就需要來彈性運用。

圖六的功能說明，詳如表二 Cisco ASA 5505 設備背面板說明，其中有很多

連接埠尚未定義，將適度的保留給未來開發上的彈性運用。



圖六 Cisco ASA 5505 設備背面圖

（資料來源：San Jose,Cisco ASA 5505 Getting Started Guide Software Version 7.2(USA:Cisco Systems,2006), p 4-12.）

表二 Cisco ASA 5505 設備背面板說明

編號	連接埠或裝置名稱	使用目的
1	電源連接埠	連接電源線。
2	保密服務卡插槽	保留未來使用。
3	本地端設定連接埠	使用命令列指令來管理裝置用。
4	設備鎖裝置	保留未來使用。
5	重置開關	保留未來使用。
6	兩個 USB2.0 連接埠	保留未來使用。
7	乙太網路裝置連接埠編號 0 到 5	第二層交換連埠，可提供彈性的 VLAN 設定。
8	網路供電裝置(PoE)連接埠編號 6 和 7	可以連接網路供電的裝置(例如：IP 電話)，這種裝置電源由此介面提供。

（資料來源：作者繪製）

二、Cisco ASA 5505 硬體防火牆特色

Cisco ASA 5505 硬體防火牆可協助單位更有效地保護內部網路，增進內部網路之安全，其重要功能特色包括[7]：

(一)廣獲市場接受的安全性與虛擬私有網路功能

Cisco ASA 5505 硬體防火牆是全功能、高效能的防火牆，它包含了入侵防禦系統(IPS)、網路防毒、IPSec 虛擬私有網路等技術，可提供強固的應用程式安全性。

(二)先進的 **Anti-X** 功能

[7] Cisco Systems, http://www.cisco.com。

在 Cisco ASA 5505 中，結合了趨勢科技(Trend Micro)在威脅防護與內容安全監控領域上的專業技術與 Cisco 經過市場考驗的成熟安全解決方案，提供了一個全面性的防毒、反間諜程式、檔案阻擋、垃圾郵件、反網路釣魚、URL 網站過濾與內容過濾安全方案。

(三)先進的入侵防禦保護

提供具預防功能的完整入侵防護系統以阻擋大規模的威脅，包含病毒、應用程式層級與作業系統層級的攻擊、後門程式、間諜程式、點對點檔案分享以及即時訊息。

(四)完備的管理與監控服務

在防火牆的管理上，可藉由內建的自適型安全裝置管理員(Adaptive Security Device Manager, ASDM)提供直覺式圖形化、單一設備的管理與監控服務，並透過 Cisco Security Manager 提供企業等級之多元、多台設備管理服務。

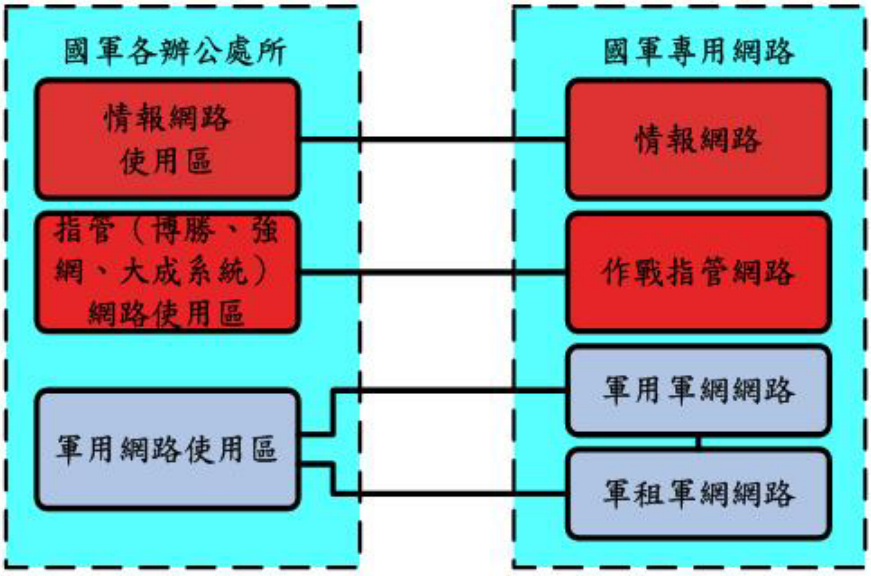
(五)降低建置與維運成本

Cisco ASA 5505 這套多功能的硬體防火牆，可讓平台、組態及管理作業標準化，協助降低佈署成本及例行的運作成本。

硬體防火牆運用於國軍網路系統架構

一、國軍網路架構簡介

現行國軍網路依照辦公處所使用專區的不同，區分為情報網路、作戰指管網路及軍用網路等三類，如圖七國軍網路架構示意圖。



圖七 國軍網路架構示意圖
（資料來源：作者繪製）

圖七中情報網路為情報部門間情資傳遞之資傳平台；作戰指管網路為迅安系統、強網系統、大成系統等指管系統通資平台；而軍用網路為國軍各級單位運用範圍最廣之網路，提供各類編裝、人事、後勤、醫療、財務、公文行政及電子郵件等服務。而軍用網路主要由兩類網路組成，一類為軍用軍網，就是國軍自力管理之資訊網路；另一類為建立國軍骨幹網路備援機制，同時補強軍用軍網無法到達之偏遠地區單位，委託民間固網公司籌建國軍專用之軍租軍網[8]。

目前軍用軍網主幹廣佈全島，由 6 個主要網路中心節點連結，形成國軍資訊網路光纖主幹；軍租軍網網路遍及全國，分別與國軍 4 個主要網路交換中心構連，形成幅員更加廣闊網路涵蓋面，主要服務網路建設較不足之基層單位。各單位區域網路設備依地理位置就近收容至鄰近網路中心設備，與各單位進行作戰訊息傳達與作業資料互通[9]。

二、運用架構探討

國軍主幹網路建置成熟已通連全島，然而網路缺乏主動阻絕防護能力，近年來國軍持續推動網路實體隔離政策，但仍舊有資料外洩的情事發生，探究原因，大多數都是內部人員的不當連線，因此在單位內部網路及外部網路之間建置適當之防火牆系統，來增進單位內部網路之連線防護，預防資安事件之發生，確實有其必要性。由於情報網路及作戰指管網路的安全機制有其建置考量，本文所討論之運用架構僅就以大多數人使用之軍用網路為範圍，說明以 Cisco ASA 5505 硬體防火牆運用在軍用網路架構上，增加單位內部網路之安全。以下提出幾種可運用之系統架構型態：

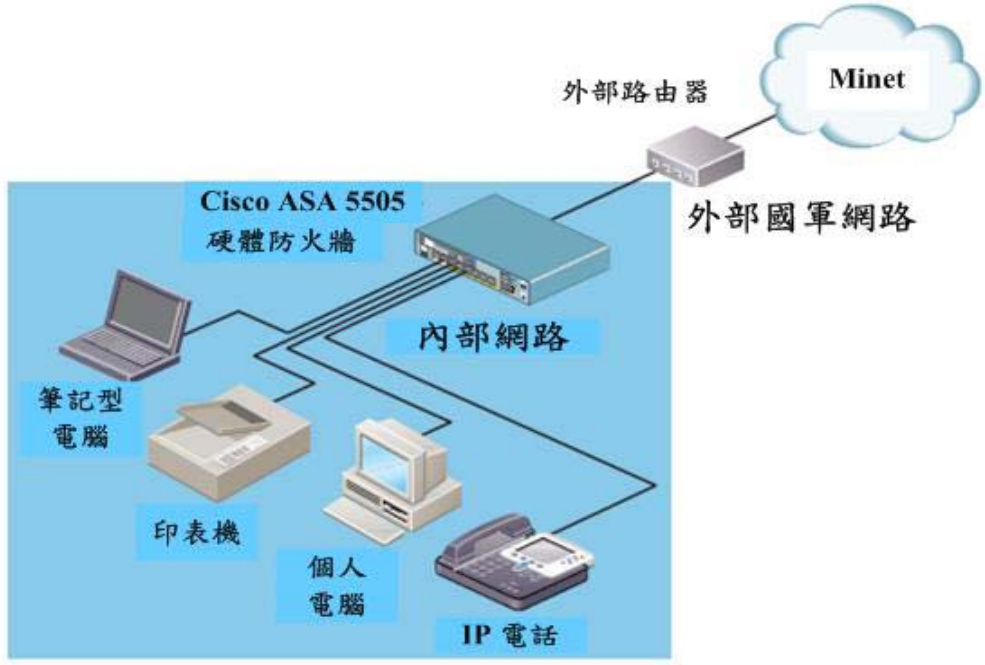
(一)基本架構型態

下圖八為一個很基本的防火牆架構型態示意圖，其中 Cisco ASA 5505 硬體防火牆連接內部網路及外部路由器，然後再連接到外部國軍網路，扮演著內部網路及外部國軍網路之間的一道牆，而防火牆連接的內部網路可以依照 Cisco ASA 5505 所提供的連接埠的不同，可以連接筆記型電腦、印表機、個人電腦、IP 電話等設備，當然也可以連接到集線器(Hub)或交換器(Switch)來收容內部區域網路，可以隨內部網路架構之不同，可彈性運用。

圖八這種架構能夠保護內部網路的安全，避免外部入侵者存取內部網路資源，凡是要存取內部網路的資源都得經過防火牆驗證，至於內部網路的使用者，經由防火牆的設定，可以適度的開放允許的服務讓內部網路的使用者存取外部網路的資源，避免內部的使用者隨意存取外部網路資源，造成內部網路之漏洞。

[8] 國軍新一代軍網架構發展指導綱要計畫（台北：國防部，96 年），頁 1-2。
[9] 同註 8。

這種架構算是防火牆運用上最基本的架構型態。



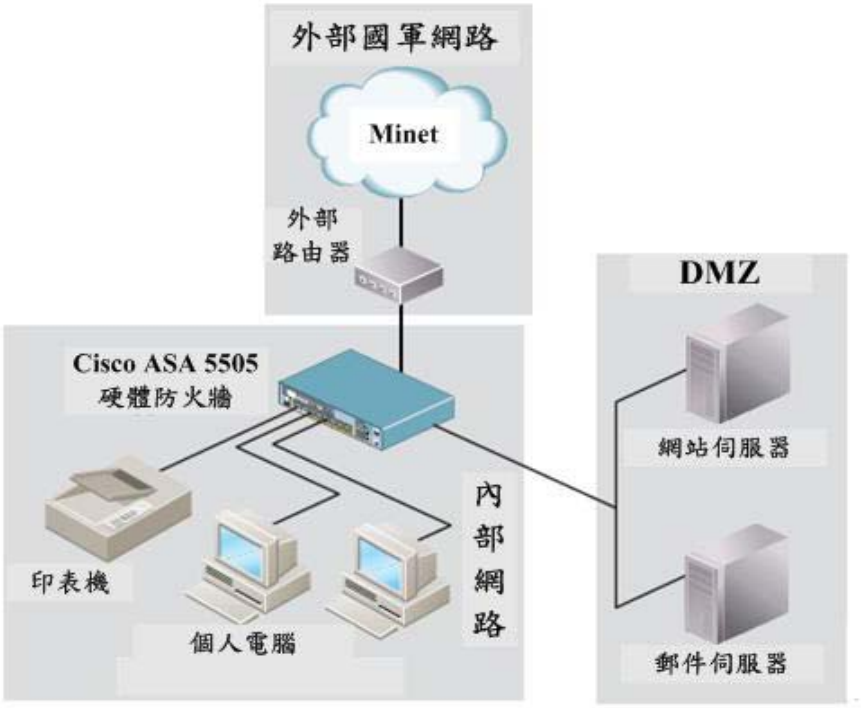
圖八 基本防火牆架構型態示意圖
（資料來源：San Jose,Cisco ASA 5505 Getting Started Guide Software Version 7.2(USA:Cisco Systems,2006), p 4-12.）

(二)外圍三向架構型態

下圖九為外圍三向防火牆架構型態示意圖，其中 Cisco ASA 5505 硬體防火牆連接三個區域，第一個區域連接內部網路；第二個區域連接外部路由器，然後再連接到外部國軍網路；第三個區域連接周邊網路(Perimeter Network)。周邊網路又稱為非軍事區域(Demilitarized Zone, DMZ)或是屏障子網路(Screened Subnet)，一般我們習慣使用 DMZ 這個名稱。

在圖九中內部網路的連接方式如同基本架構型態所述，而在非軍事區域中可以架設單位對外開放的應用網路服務，例如單位的網站伺服器(Web Server)、郵件伺服器(Mail Server)等。在此架構型態中，內部網路與外部國軍網路是完全隔離，透過防火牆的設定，開放內部網路的使用者可以存取外部資源，但外部國軍網路的使用者，經由防火牆的設定，限制外部的使用者存取內部網路的資源，如此一來內部網路的資源便受到防火牆的保護；至於放在非軍事區域的應用網路服務資源，可經由防火牆的設定，開放內部及外部的使用者存取防火牆所開放的特定服務資源，但是防火牆設定非軍事域內的使用者是限制存取內部網路資源，如此一來外部網路的使用者也無法透過非軍事區域進入到內部網路，因此，內部網路之資源便可完全受到防火牆的保護。相較之下，上述基本

防火牆架構型態中，內部網路若有應用網路服務（如網站伺服器或郵件伺服器等）要開放給外部網路使用者存取時，防火牆必須設定開放給外部網路存取，如此便會造成內部網路安全上的漏洞，外部的非法入侵者就可透過此一管道，進入到內部網路，經由應用伺服器進行跳板攻擊，入侵內部網路的資訊系統。因此，就安全運用上來說，外圍三向防火牆架構，算是一個不錯的選擇架構。



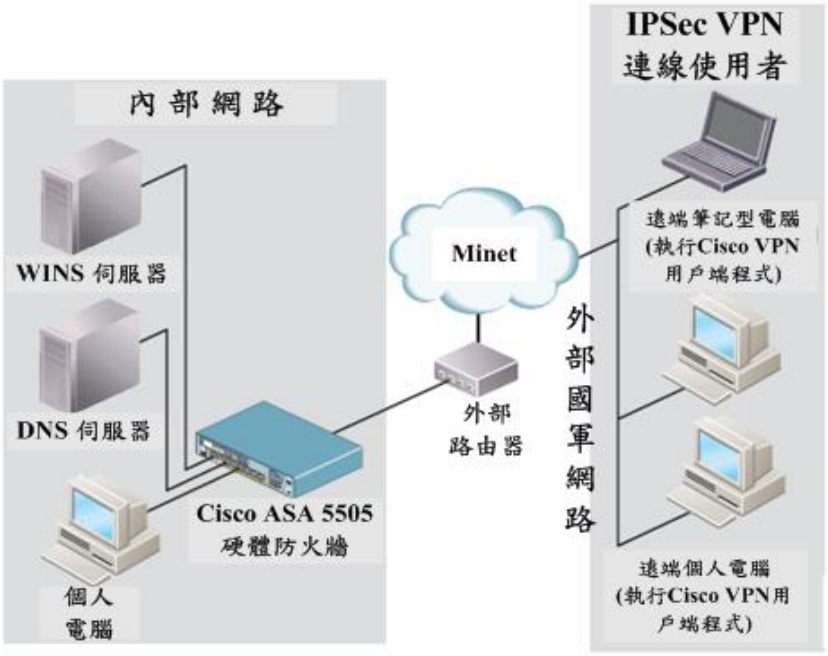
圖九 外圍三向防火牆架構型態示意圖
（資料來源：San Jose,Cisco ASA 5505 Getting Started Guide Software Version 7.2(USA:Cisco Systems,2006), p 4-12.）

(三)IPSec 虛擬私有網路連線架構型態

Cisco ASA 5505 硬體防火牆在安全連線的考量上，可以設定 IPSec 虛擬私有網路功能，讓外部虛擬私有網路連線使用者執行虛擬私有網路用戶端程式，透過外部國軍網路與內部網路建立虛擬私有網路，讓使用者與內部網路之間能夠安全的溝通。

下圖十為 IPSec 虛擬私有網路連線架構型態示意圖。在圖中內部網路的連接方式如同基本架構型態所述，只是增設提供內部網路使用之應用伺服器（如 WINS 伺服器、DNS 伺服器），而連接外部國軍網路的 IPSec 虛擬私有網路連線使用者，在遠端執行 Cisco VPN 用戶端程式，就可以透過外部國軍網路來與 Cisco ASA 5505 硬體防火牆建立虛擬私有網路連線，建立一條安全的通道傳送資料，這種連線方式，讓遠端使用者連線上感覺就像是在內部網路連線的使用者一

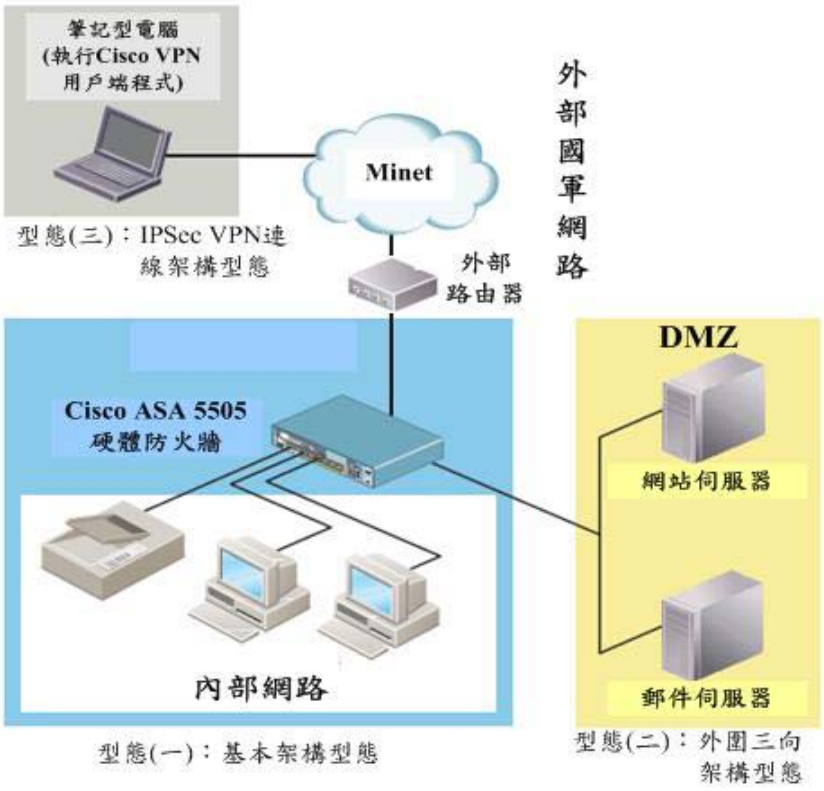
般。然而，此種連線方式是使用 IPSec 通訊協定，彼此之間必須經過驗證程序，然後建立一個加密的安全通道，資料傳送的時候也都經過加密，增加資料傳輸的保密性。因此，遠端的使用者若有必要存取內部網路資源時，可以透過外部國軍網路，運用此連線方式來達到安全的連線。



圖十 IPSec 虛擬私有網路(VPN)連線架構型態示意圖
（資料來源：San Jose,Cisco ASA 5505 Getting Started Guide Software Version 7.2(USA:Cisco Systems,2006), p 4-12.）

三、架構分析比較

由上面章節之架構說明，在運用架構上可以歸納表示成如圖十一，在選擇防火牆架構時，首先應考量本身單位的網路架構，接下來就是要考量安全需求。假若單位的網路架構簡單，且內部也沒有對外提供服務的應用伺服器，那麼建置防火牆時，可選擇運用型態（一）：基本架構型態；如果單位內具有應用網路伺服器（如網站伺服器或郵件伺服器等），那麼就應該考量使用型態（二）：外圍三向架構型態，將應用網路服務放置於非軍事區域中；若外部網路的連線用戶端須要存取內部網路的資源時，應選擇使用型態（三）：IPSec VPN 連線架構型態，讓外部網路與內部網路連線時建立安全的通道，增加連線的安全性。



圖十一 綜合架構型態示意圖
（資料來源：San Jose,Cisco ASA 5505 Getting Started Guide Software Version 7.2(USA:Cisco Systems,2006), p 4-12.）

因此，在圖十一中每種架構型態都有其可用之處，最重要的就是網路作業人員是否能夠靈活運用，依照單位內部網路架構及安全需求，選擇建置單位之防火牆系統架構。

結論

本文以 Cisco ASA 5505 硬體防火牆為基礎，運用到國軍網路架構中，首先介紹防火牆概論，說明防火牆的定義、技術型態與種類，其次介紹 Cisco ASA 5505 硬體防火牆功能及特性，再以簡單扼要的方式提出如何將硬體防火牆運用到國軍網路架構中，在系統運用架構上提出三種架構型態，第一種為基本架構型態、第二種為外圍三向架構型態，第三種為 IPSec 虛擬私有網路連線架構型態，三種架構型態都可依照單位內部網路特性及需求，來加以靈活運用。因此，希望透過本文提出之架構型態，使其成為兼具安全與實用之防火牆系統，以提供網路作業人員之參考依據及一般使用者之基本認知。