財團法人台灣網路資訊中心

台灣網路資訊中心委託執行計畫

「Native IPv6 連網環境建置及 IPv6 用戶安全防護研析」

IPv6 企業資通安全防護 技術手冊

計畫委託機關：台灣網路資訊中心

中華民國 109 年 10 月

摘要

隨著 IPv6 的發展，IPv6 安全風險開始浮現，亦挑戰 IPv6 網路防護能力，如何建構安全的網路防護機制，確保企業 IPv6 用戶資通安全，也是部署 IPv6 不可或缺的重要關鍵。本手冊除參考 IETF IPv6 相關資通安全 RFC 標準外，亦針對 IPv6 企業資通安全防護相關議題進行研析，探討設備 IPv6 網路安全防護功能與機制，並針對企業網路 IPv6 網路安全管理提出建議。本手冊可做為我國企業網路推動與部署 IPv6 的參考依據。

目次

圖目錄

表目錄

前言

隨著 Internet 的迅速發展，連接公眾 Internet 的用戶終端設備數量不斷激增，現階段數量有限的 IPv4 位址愈顯得捉襟見肘，嚴重影響了網路的發展。而對於擁有幾百台甚至上千台終端用戶的大型網路或是企業用戶來說，如何有效的分配網路的 IP 資源，建構安全的網路環境並有效管控用戶終端裝置的連網行為，是企業網路發展的首要目標。此外，礙於 IPv4 位址空間的不足，也影響了企業網路未來的發展，而 IPv6 除有充足的位址空間，能滿足企業網路位址空間的需求外，也具備自動配置與區分位址類別的特徵，使得企業網路升級與佈署 IPv6 成為發展的趨勢。

本報告主要針對企業網路進行IPv6資通安全防護相關議題研析，探討企業網路 IPv6 安全議題與解決方案，並針對企業網路 IPv6 資安防護提出建議，可供企業網路佈署 IPv6 與建立企業網路安全連線的參考。

壹、 目的及應用範圍

本報告目的在於研究企業網路 IPv6 安全佈署相關議題，因企業網路安全連線技術領域涵蓋範圍廣泛，故本報告主要針對企業網路安全議題，安全防護以及防護架構機制進行研析，期可作為企業網路發展與部署企業內部 IPv6 網路安全與用戶連線的參考。

貳、 企業網路 IPv6 安全議題與解決方案

本章首先將分析引進 IPv6 之後，可以強化哪些資安功能而又會引進哪些新的資安議題。其次面對過去既有的許多 IPv4 資安問題，本章將從 IPv6 的角度，提出相對應的建置建議。

一、 IPv6 協定在網路安全上的強化

針對 IPv6 在網路安全上的強化摘要說明如下：

- 端到端的安全保證： IPv6 最大的優勢在於保證端到端的安全，可以滿足用戶對端到端安全和移動性的要求。IPv6 移走 NAT，允許所有的網路節點使用其全球惟一的位址進行通信。IPv6 可利用 IPSec 封裝完成對通信端的驗證和對資料的加密保護[1]，使得重要的資料可以在 IPv6 網路上安全地傳遞，因此，無需針對特別的網路應用部署

應用層閘道器 ALG，就可保證端到端的網路透明性，有利於提高網路服務速度。

- 可聚集的(aggregate-able)而階層化的位址結構：由於 IPv6 位址構造是可聚集的，而且具有層次化的特性，因此 IPv6 接入路由器可以很容易地在用戶進入時對用戶進行來源位址檢查，使得 ISP 可以驗證其客戶位址的合法性。
- 有效防止未授權的接取： IPv6 強化了防止未授權接取的能力，更加適合於那些對敏感資訊和資源有特別處理要求的應用。
- 強化的網域名稱系統 DNS： 以 IPv6 為基礎的 DNS 系統未來可作為公共密鑰基礎設施(PKI)系統的基礎，有助於抵禦網路上的身份偽裝與偷竊，若進一步採用可以提供認證和完整性安全特性的 DNS 安全擴展(DNS Security Extensions)協定，將可進一步增強目前針對 DNS 的新攻擊方式的防護能力，例如“網路釣魚(Phishing)”攻擊、“DNS 中毒(DNS poisoning)”攻擊等，這些攻擊會控制 DNS 伺服器，將合法網站的 IP 位址篡改為假冒以及惡意網站的 IP 位址。
- 有效防止網路掃描與病毒蠕蟲傳播：當病毒和蠕蟲在感

染了一台主機之後，就開始對其他主機進行隨機掃描，在掃描到其他有漏洞的主機後，會把病毒傳染給該主機。這種傳播病毒的速度在 IPv4 環境下非常迅速。但這種傳播方式因為 IPv6 的巨大位址空間而變得不適用，病毒及網路蠕蟲在 IPv6 的網路中傳播將會變得很困難。

- 有效防止網路放大與碎片(Fragment)等攻擊：ICMPv6 在設計上不會回應群播位址和廣播位址的訊息，所以只需要在網路邊緣過濾群播封包即可有效阻止由攻擊者向廣播網段發送封包而引發的網路放大攻擊。而 IPv6 認為 MTU 小於 1280 位元組的封包是非法的，處理時會丟棄 MTU 小於 1280 位元組的封包(除非它是最後一個封包)，這有助於防止碎片攻擊。

綜合以上所述，IPv6 協定確實比 IPv4 的安全性有所改進，例如 IPv4 中常見的一些攻擊方式，在 IPv6 網路可能失效或是降低其威脅性，例如網路偵察、表頭攻擊、 ICMP 攻擊、碎片攻擊、假冒位址、病毒及蠕蟲等。

二、 引入 IPv6 可能引發的安全問題

針對 IPv6 可能引發的安全問題摘要說明如下：

- IPv4 與 IPv6 共存的架構可能存在新資安風險：由於 IPv6 與 IPv4 網路將會長期共存，網路必然會同時存在兩者的安全問題，或由此產生新的安全漏洞。目前已經發現從 IPv4 向 IPv6 轉移時出現的一些安全漏洞，例如駭客可以利用 IPv6 對同時具備 IPv4 和 IPv6 兩種協定的 LAN 網路進行非法接取，而惡意攻擊者亦可以透過雙堆疊的 IPv6 主機，建立由 IPv6 到 IPv4 的隧道，繞過防火牆對 IPv4 網路進行攻擊。IPv6 協定轉移與採用其他任何一種新的網路協定一樣，其安全措施必須重新經過慎重的考慮和測試。
- IPv6 的網管設備和網管軟體尚未成熟：IP 網路中許多不安全問題主要是管理造成的。IPv6 的管理與 IPv4 在思路上有可借鏡之處。但對於一些網管技術，如 SNMP 等，不管是移植還是另起爐灶，其安全性都必須從本質上有所提高。由於目前針對 IPv6 的網管設備和網管軟體支援 IPv6 仍然有限，因此缺乏對 IPv6 網路進行監測和管理的有效方法，亦缺乏對大範圍的網路故障定位和性能分析的機制。
- IPv6 的資安產品尚未成熟：IPv6 網路同樣需要防火牆、

VPN、IDS、漏洞掃描、網路過濾、防止病毒閘道器等網路安全設備。事實上 IPv6 環境下的病毒已經出現，但這方面的安全技術研發還尚需時日。IPv6 防火牆需面對以下的一些挑戰： (A) 封包表頭的差異：在 IPv4 中並沒有擴充表頭，因此在設計 IPv6 防火牆時，需特別注意到擴充表頭，在做封包過濾時，要能辨識出含擴充表頭的封包。(B) End-to-End：網際網路最初的概念就是 End-to-End，由於 IPv4 位址不足，因而破壞了這個架構， IPv6 解決了這個問題，而回歸到 End-to-End 的概念。但是防火牆需要做封包過濾與執行安全政策，又似乎必須剪斷 End-to-End，因此在設計 IPv6 防火牆時，就需要找出解決方法。(C) Mobility：在 IPv6 的行動能力應用上，一個外地的主機看起來都會是本地的，因此在做封包過濾時，需解決面對一個移動節點而不能把它當成外地主機的問題。(D)相對於 IPv4，IPSec 在 IPv6 扮演更重要的腳色。在 IPv6 的環境中要使用 IPSec，必須解決如何過濾在加密的通道中傳遞資訊的問題。 (E) Path MTU：IPv6 封包只在來源主機進行封包分割，它利用 ICMPv6 協定來找出 Path MTU，因此 IPv6 防火牆需要具備辨識和處理

ICMPv6 封包的能力。

- 其他新的安全挑戰：IPv6 協定仍需在實踐中持續做改進的動作，例如 IPv6 群播認證、用戶限制以及行動管理也存在很多新的安全挑戰。

綜合以上所述，與 IPv4 相比，雖然 IPv6 在網路保密性、完整性方面有了更好的改進，但 IPv6 不可能徹底解決所有安全問題，同時還會伴隨而產生新的安全問題。目前多數網路攻擊和威脅大都來自應用層而非 IP 層，因此，保護網路安全與資訊安全，只靠一兩項技術並不夠，還需配合多種手段，諸如認證體系、加密體系、密鑰分發體系等方可竟全功。

三、 IPv6 面對資安弱點的解決方案

目前在 IPv4 網路環境中，各種可能的資安攻擊方式可概分為十一大項，分別為：偵查、非法接取、表頭的篡改與封包的分片、第三層和四層資訊的欺騙、arp 和 dhcp 攻擊、廣播放大攻擊(smurf)、路由攻擊、偵聽、應用層攻擊、中間人攻擊、泛洪(flooding)。以下將就從 IPv6 的角度，摘要說明如何利用 IPv6 來解決上述的各種攻擊。

- 偵查：網路偵查在 IPv4 中很簡單，駭客可以使用 Ping sweep、Port scan、Application and vulnerability scan 輕易達到目的，但在 IPv6 的環境不同，由於一個 IPv6 子網的 IPv6 位址很多，通常為 2 的 64 次方，掃描起來相當費力，幾乎不可能，因而降低了被掃瞄的機會與意願。
- 非法接取：在 IPv4 網路環境下，通常會執行以下的動作來避免非法的存取:ACL on border FW 以及 ACL on host FW。在 IPv6 網路環境下，基本上亦是利用相同的動作來避免非法的存取，在引進 IPv6 網路環境後，可進一步啟動 IPSec，對於存取控制將有所助益。
- 表頭的篡改與封包的分片：在 IPv4 網路環境下，可能存在以下資安危機：(A)利用 fragmentation 來困惑或是 bypass 路由器或防火牆的存取控制，(B)利用 overlapping data/header 來 bypass 路由器或防火牆的存取控制 (C)利用 fragmentation 來癱瘓 IDS 等資安工具。引進 IPv6 網路環境後，RFC 8200 中明定[2]，在 IPv6 網路中 fragmentation 只能在 end 端執行，任何中間經過 fragmentation 的 packet 均可被視為攻擊發生而直接 drop，而 Overlapping fragments 在 IPv6 中是不被允許的。

- 第三層和四層資訊的欺騙：在 IPv4 網路環境下，可能存在以下資安危機: DOS、DDOS、spam、worm 以及 virus attacks 等等。在 RFC 2827 明定應實現 ingress filtering 的功能[3]，將欺騙的 L3 traffic 擋在它的源頭，但若駭客使用 subnet 內的 IP 位址，則 RFC 2827 仍無法防範。此外，RFC 2827 對於 Layer 4 spoofing 的幫助並不大。引進 IPv6 網路環境後，由於 IPv6 位址具有 globally aggregated 的特性，此特性可讓 ISP 更容易實現 RFC 2827 filtering 的功能，使得整個欺騙的 L3 traffic 停留在客戶端而不會無限制的擴散。
- ARP 和 DHCP 攻擊：在 IPv4 網路環境下，可能存在以下資安危機: (A) 駭客竄改 IP-MAC 之間的對應，使無辜的使用者與駭客對話，進而啟動 man-in-the-middle attack，(B) 駭客假冒 DHCP server，進而啟動 man-in-the-middle attack，(C) 駭客利用 flooding 攻擊，癱瘓合法的 DHCP server。引進 IPv6 網路環境後，由於 ARP 已被 ICMPv6 的 ND 所取代，所以 IPv4 網路環境下的 ARP 資安問題自然消失，但是 IPv6 的 ND 仍繼承了既有的 ARP 資安問題。IPSec 是一個可能的解決辦法，或是實現 RFC 3971

的 SEND (SEcuring Neighbor Discovery)亦可解決[4]。

- 廣播放大攻擊：在 IPv4 網路環境下，可能存在以下資安危機:駭客利用 ICMP Echo 訊息、一個 subnet 的 broadcast destination 位址、一個假冒的 source 位址即可執行”smurf”攻擊。引進 IPv6 網路環境後， IP-directed broadcast 的動作已被移除，而若 IPv6 終端用戶實際實現 RFC 2463，則”smurf”攻擊或其他類似的 Attacks 可被有效減緩[5]。
- 路由攻擊：在 IPv4 網路環境下，一般使用 MD5 來保護路由器之間的路由交換訊息，引進 IPv6 網路環境後，可啟動 IPSec，對於預防路由攻擊有所助益。
- 偵聽：可以使用 IPSec 降低被竊取資料的機會。
- 應用層攻擊：Virus and Worm 均屬於此類，使用 IPSec 之後，相關的安全檢查與防護將落到 host 身上，因為 FW 看到的是加密過的資料。
- 中間人攻擊:可以使用 IPSec 降低被攻擊的機會，建議使用 IKE main mode。
- 泛洪：針對 Flooding，IPv6 並無新增之防護方法，建議沿用 IPv4 既有方法予以防範。

四、 IPv6 面對資安弱點的解決方案

本節主要參考國際 RFC 標準針對企業網路導入 IPv6 部署需求進行探討，並摘要企業網路部署 IPv6 參考指引。針對企業網路部署 IPv6 網路的需求可參考 RFC 4057 Enterprise IPv6 Scenarios [6]摘要說明如下。

- DNS 網域名稱伺服器：必須同時提供 IPv4 和 IPv6 服務且要配合做好相關設定以確保連線。
- 路由協定 Routing：內部和外部路由需同時支援 IPv4 和 IPv6 路由協定交換，確認 IPv6 路由拓撲在內的狀況，以及哪些與外部連接的介面、供應商網路、過渡機制等。
- 終端用戶配置:企業終端用戶應採固定的 IPv6 網路設定，或採用 DHCPv6 來進行位址設定，企業也需要確認上游供應商網路是如何分配。
- Security 安全:管理單位需要檢視手上的資安工具是否支援 IPv6，並研擬企業網路導入 IPv6 的資安防護計畫。
- 應用服務：現有的應用服務需要移植或提供新的替代服務，確保同時提供 IPv4 和 IPv6 服務的能力。
- 網路管理：新增的 IPv6 網路基礎設施元件需要被納入管理。管理單位必須確認網路管理平台是否提供 IPv6

版本，同時需要規劃 IPv6 網路用以監控網路內的節點。

- 位址規劃：資訊管理單位需要擬定 IP 申請發放的規定。同時為了應付 IPv6 導入初期的轉換需求，建議保留一組 IPv4 位址提供轉換服務使用。

企業網路部署 IPv6 指引則是參考 RFC 7381 Enterprise IPv6 Deployment Guidelines 的標準[7]，針對內部以及外部兩個階段來討論。在企業內部 IPv6 部署階段指引摘要說明如下 ：

- Security 安全政策：內部所有現存於 IPv4 安全策略必需同步擴展支援 IPv6。
- 網路基礎架構：企業網路必須為用戶提供備援路徑。
- 終端用戶裝置：主要的作業系統均已支援 IPv6，唯仍應注意個別用戶終端裝置 IPv6 啟動狀態。
- 系統環境：部署 IPv6 應整體考量 IT 環境部署情況，每個系統如 email、VoIP 或 DNS 等均應有詳細的 IPv6 部署計畫。

針對企業部署外部 IPv6 階段指引摘要說明如下 ：

- 網路接取：企業需要與一個或多個服務供應商合作取得網路的連接，並考慮優先以 Native IPv6 連接。

- Security 安全政策：外部網路 IPv4 與 IPv6 安全政策需一致，同時也必須提供過濾與監控的機制。
- 網路監控：IPv6 應做到監控網路連接的使用狀況，比照 IPv4 的網路連接監控， 報告異常的流量模式（例如：連接阜的掃描，SYN Flooding 以及相關的 IP 來源）。
- 服務與應用伺服器：連接網路服務所經路經上之設備如防火牆、負載平衡裝置、資安設備以及相關伺服器建議啟用 DualStack。
- IPv6 NPT 轉換機制：須了解 NPT 機制部署的必要性與涵義。

參、 企業網路 IPv6 資安防護建議

本章主要由不同層面探討企業網路 IPv6 的整體安全性議題，並摘要企業網路設備與主機 IPv6 的安全防護，期可作為企業網路部署 IPv6 之參考指引。

一、 企業網路導入 IPv6 安全指引

IPv6 網路的整體安全性至少必須透過四個層面實現：移轉安全、協定安全以及網路安全，以下將逐項地予以說明。

(一)移轉安全

由於 IPv6 與 IPv4 網路將會長期共存，網路必然會產生新的安全漏洞。向 IPv6 協定轉移與採用其他任何一種新的網路協定一樣，其安全措施必須經過慎重的考慮和測試。目前，IPv4 向 IPv6 過渡技術以雙堆疊、隧道和協定轉換三種為主。建議向 IPv6 轉移應儘量採用雙堆疊技術，避免採用協定轉換，若需使用隧道技術則儘量採用靜態隧道，避免採用動態隧道。以下提供三轉轉移機制的使用時機建議，如表 1 所示。

表 1 IPv6 企業網路移轉方案優缺點比較

方案	說明	
DualStack	優點	➢ 容易設置與易懂。 ➢ 端點對端點連線模式未遭破壞。 ➢ 雙堆疊主機可與其它雙協定堆疊主機、純 IPv4 主機或純 IPv6 主機互連。
	缺點	➢ 擴展性(scalability)差。因為每個節點需 1 個 IPv6 位址及 1 個 IPv4 位址。 ➢ 系統複雜度及負擔增加，需維持 2 個 IP 協定個別的 routing table 及相關網管資訊。 ➢ 無法提供純 IPv4 主機與純 IPv6 主機的互通。
Tunnel	優點	➢ 節點對節點的連線方式未遭破壞。 ➢ 利用現有 IPv4 網路，可降低成本。
	缺點	➢ 需要 IPv4 網路架構。 ➢ 封裝及解封裝增加網路額外負擔。 ➢ 人工的設定與維護，增加網管者沈重的工作負擔。
Transition	優點	➢ 可建構在 IPv4 與 IPv6 網路交界位置，提供純 IPv4 與純 IPv6 間的通訊，免除將主機升級為雙 IP 協定堆疊的麻煩。
	缺點	➢ 經由 NAT-PT 處理的 session，在整個 session 過程中，所有封包均需流經此 NAT-PT。因此 NAT-PT 轉換器可能成為網路運作的瓶頸點，會危及整體網路運作。 ➢ 需借助 DNS-ALG、FTP-ALG 以及各種應用程式 ALG(Application Layer Gateway)方能處理封包酬載中位址的轉換，達成應用層雙向互連。

(二)協定安全

網路受到的安全威脅是來自多層面的，包括實體層、資料鏈路層、網路層、傳輸層和應用層等各個部分。在實體層以上層面，安全性隱憂主要有來自於針對各種協定的安全威脅，以及意在非法佔用網路資源或者耗盡網路資源的安全隱憂，諸如雙 802.1Q 封裝攻擊、廣播包攻擊、MAC Flooding、生成樹攻擊等二層攻擊，以及虛假的 ICMP 訊息、ICMP 洪泛、來源位址欺騙、路由振盪等針對三層協定的攻擊。在應用層，主要有針對 HTTP、FTP/TFTP、Telnet 以及通過電子郵件傳播病毒的攻擊。對於這些攻擊，可以採用的防護手段包括：

- 通過 MAC 位址和 IP 位址綁定、限制每個 port 的 MAC 位址使用數量、設立每個 port 廣播封包流量門限、使用基於 port 和 VLAN 的 ACL、建立安全用戶隧道等來防範針對第二層的攻擊。
- 透過路由過濾、對路由資訊的加密和認證、定向組播控制、提高路由收斂速度以減輕路由振盪影響等措施，來加強第三層網路安全性。
- IPv6 的 AH(Authentication Header)和 ESP(Encapsulating Security Payload)中的擴充表頭結合多樣的加密演算法可

以在協定層面提供安全保證。在 AH 認證方面，可以採用 hmac_md5_96、 hmac_sha_1_96 等認證加密演算法；在 ESP 封裝方面,經常採用的演算法有 3 種:DES_CBC、3DES_CBC 及 Null 。目前的網路環境仍以手工提供密鑰配置管理的方式，但為適應將來大規模安全網路組建要求，應同時預留 IKE（Internet 密鑰交換）協定介面。

- 通過 AAA、 TACACS+、RADIUS 等安全接取控制協定，控制用戶對網路的接取許可權,防患針對應用層的攻擊。

(三)網路安全

IPSec 隧道和傳輸模式的各種組合應用，可以提供網路各層面的安全保證。諸如：端到端的安全保證、內部網路的保密、通過安全隧道構建安全的 VPN 等等。端到端的安全保證在兩端主機上對資料進行 IPSec 封裝，中間路由器實現對有 IPSec 擴充表頭的 IPv6 資料透通，從而實現端到端的安全保證。在內部網路保密方面，由於 IPSec 作為 IPv6 擴充表頭不能被中間路由器而只能被目的節點解析處理，因此，可以透過 IPSec 來保證內部網路的安全。在利用 IPSec 安全隧道實現 VPN 方面，路由器之間建立 IPSec 安全隧道以構成安全的 VPN，是最常用的安全網路建置方式。

(四)其他

綜合以上所述，安全的網路是眾多安全技術的綜合，而 IPv6 IPSec 機制是其中重要的組成部分，它提供了協定層面上的一致性解決方案，這也是 IPv6 相比 IPv4 的重大優越性。同時，為了構建安全網路，還應該採取以下安全措施：

- 結合 AAA 認證、NAT-PT、二/三層 MPLSVPN、基於 ACL 標準的接取列表和靜態擴展接取列表、防止封包分組攻擊等來實現安全預防。
- 通過路由過濾、靜態路由、策略路由和路由負荷分擔來實現安全路由。
- 通過 SSHv2 （SecureShell 第 2 版）、SNMPV3（簡單網路管理協定第 3 版）、EXC，提供進程接取安全、線路接取安全。
- 通過分級管理、實施特權級管理等手段來實現網路的安全管理。
- 通過完善的告警、日誌和審計功能實現網路時鐘的安全。
- 提供接取列表和關鍵事件的日誌、路由協定事件和錯誤記錄等，以供網路管理人員進行故障分析、定位和統計。

二、 網路設備與主機 IPv6 安全防護建議

本節係針對資安設備，網路設備與主機摘要 IPv6 建議，期能作為企業網路部署與建置 IPv6 的參考。

(一)資安設備

資安設備如防火牆，IDS，IPS 等均屬此類。茲摘要 IPv6 安全防護建議如下：

- 清查既有防火牆是否支援 IPv6，透過汰舊換新過程逐步更換。
- 取得支援 IPv6 的能力如以韌體升級方式支援 IPv6，須注意檢查 CPU 負載及記憶體的消耗狀況，避免效能不足防火牆。
- 支援 IPv6 後可參考 IPv4 規則設定 IPv6 的過濾方式(ACL)，再依據觀測的 IPv6 流量資訊，逐步完善 IPv6 的防禦規則。過濾政策 Checklist 可參考附錄。

另針對流量與紀錄 Log 部分:

- 可依服務類別/個人使用統計流量：Inbound、Outbound、FTP 連線、SSH 連線、網路芳鄰、遠端桌面連線、遠端程序呼叫、Proxy、Mail、ICMP 等進行統計。
- OS 如本身可正常支援 IPv6，則 System Log 一般均可正

常顯示；AP Log 則需視 AP 對 IPv6 支援度而定，建議先行測試。

(二)網路設備

網路設備係以路由器與交換器為主，在路由器部分，Ipv6 防護建議如下：

- 對外建議使用/127 點對點連線。
- 僅允許正面表列的訊務流量通過，其餘禁止。
- 關閉發送 RA。
- 過濾非必要之 ICMPv6 訊息，只處理合法網段訊務轉送。
- 依據 scope 範圍過濾群播封包。
- 禁止 Routing Header Type 0(RH0)與未知 IPv6 延伸表頭。
- 啟動 unicast Reverse Path Forwarding (uRPF) 。
- 啟動 Secure Neighbor Discovery (SEND) 。
- 停用 IPv6 轉移機制，如 6to4, ISATAP, Configured Tunnel 等。

針對交換器部分，建議是以 IPv6 First Hop Security 為主，設備本身須可支援 RA guard，DHCP guard，IPv6 Snooping，Source/Prefix Guard 以及 Destination Guard 等基本 IPv6 防護功能。

(三)伺服器與終端設備

在伺服器部分 IPv6 防護建議如下：

- 部署入侵偵測系統來監督 Link-local 的流量，監督一些可疑流量型態的門檻值(threshold) 。
- 強化主機系統及應用程式本身之安全。
- 定期做作業系統之 patch、安裝主機型/網路型的入侵偵測系統、主機型防火牆及防毒軟體等。
- 停用 IPv6 轉移機制，如 6to4, ISATAP, Configured Tunnel 等。
- 主動監測 IPv6 資安防護狀態，偵測到異常攻擊儘快通報

針對終端主機部分部分，建議如下：

- 避免將每個用戶的 IP 位址指定成連續的 IP 位址，應該儘量分散其 IP 的指定，及使用隨機產生的位址前綴。
- 使用私有擴展位址（Privacy extensions），來達到防禦外部對內進行偵蒐攻擊的目的。
- 使用代理伺服器，如 HTTP Proxy，以避免 Web 客戶端的 IP 被 Cache，或使用暫時的 Privacy Address。
- 所有電腦支援 IPv6 與 host-based 防火牆。
- 強化主機系統及應用程式本身之安全，如定期做作業系

統之 patch、安裝主機型的入侵偵測系統、主機型防火牆及防毒軟體等。

- 建議使用 IPSec AH 來作為兩端連線的相互認證。
- 停用 IPv6 轉移機制，如 6to4, ISATAP, Configured Tunnel 等。
- 主動監測資安防護狀態，偵測到異常攻擊儘快通報。
- 定期做作業系統之 patch、安裝主機型/網路型的入侵偵測系統、主機型防火牆及防毒軟體等。
- 停用 IPv6 轉移機制，如 6to4, ISATAP, Configured Tunnel 等。

簡要來說，企業網路 IPv6 的安全佈署基本上除了防火牆必須能完整支援 IPv6 外，網路設備也需要能有效過濾與稽核 IPv6 位址，可預防未經授權的 IPv6 用戶存取企業網路的內部資源，此外，對於用戶網路終端設備的管理則可以考慮透過 Static 或 DHCPv6 用戶定址技術來有效管理企業網路內部主機或設備，透過有效的網路管理機制以及用戶定址技術能有效提昇企業佈署 IPv6 的安全性。

三、 IPv6 網路安全管理建議

在 IPv6 網路安全管理方面，首要任務也是基本原則就是加強網管人員之 IPv6 專業知識教育訓練，以藉此強化 IPv6 安全相關議題之管理。IPv6 網路安全管理相關建議，茲簡要說明如下：

- IPv6 的 128 位元位址設計可提供極大的位址空間，雖然可以有效遏阻針對 IPv6 子網段所進行的網段掃瞄暴力攻擊。但是如果網路管理員不會善用 IPv6 位址特性，這項優點也無用武之地。因為很難記住完整的 IPv6 位址，網路管理員通常只會使用小而易記的 IPv6 位址(如::1)，駭客也是可能輕鬆掃瞄到這類 IPv6 節點而進行攻擊。建議使用加入 16 位元表示方法(如 ABCDEF)之 IPv6 位址，增加位址的安全度及掃瞄的困難。
- 慎重考慮所支援的服務及可允許之擴展標頭。如果非必要，絕對不要提供不必要的服務，例如如果不支援 Mobile IPv6 則不要允許此類封包進入網路。
- 決定有效的 ICMP 封包過濾執行及 RFC 2827 所建議之封包篩選規定，尤其在網路入口/出口節點執行有效封包篩選(例如網路端口組絕 Type 0 Routing Header)及捨棄 MTU 小於 1280 位元的分割封包(除非是最後一個分割封

包)。

- 為了確保路由器管理介面的安全，網路管理員都應該使用安全的遠端存取 SSH(Secure Shell)機制和確保本通信介面不使用預設密碼。
- 重要資訊系統為了管理方便建議考慮採用固定 IPv6 位址並使用加密認證機制(IPsec 或是其他類似機制)。
- 現有的路由協定如 OSPFv3、RIPng、BGP and IS-IS 也應使用加密認證機制加強保護。
- 為了管理方便，最保險之網路部署建議使用雙協定(dual stack)機制，一旦出現資安漏洞，至少追查時比較方便。
- 收集實際 IPv6 運作經驗的相關資訊和記錄，以提供更多 IPv6 資料封包篩選原則和防火牆控制管理項的實作經驗分享。
- 由於現有 IPv6 應用軟體及支援 IPv6 防火牆尚嫌功能不足等因素考量，大部分企業及 ISP 大都以現有設備進行 IPv6 網路安全防護，所以防護功能可能不足應付駭客利用 IPv6 而進行之惡意攻擊。建議做好個人端資安防護(定期更新修補檔案及使用防毒軟體)。
- 目前多數網路攻擊和威脅來自應用層而非 IP 層，IPv6 網

路同樣需要防火牆、VPN、IDS、漏洞掃描、網路過濾、病毒防護等網路安全設備。需要等到這些設備都支援IPv6，才能真正有效保障 IPv6 服務安全需求。

- 對用戶而言，安全不能等而且服務才是重點，網路安全管理範圍遲早將擴大涵蓋網路各層級。與其消極等待設備都支援 IPv6，不如趁早進行 IPv6 資安服務規劃及在商用網路大規模實際演練，加強實戰經驗，方可徹底保障用戶上網安全需求及加強社會大眾對 IPv6 服務之信心。

總結來說，為了降低導入 IPv6 投資成本與風險為主要目標，企業網路導入 IPv6 應考慮提供 IPv6 資安服務行動方案，重點應包括 IPv6 安全能力調查、安全策略規劃、安全管理制度、資安防護技術以及人員教育訓練等，如表 2。

表 2 IPv6 企業企業網路資安工作重點

名稱	說明
IPv6 安全能力調查	進行現有相關資訊系統與網路設施之 IPv6 安全防護現況資訊調查，包括 Firewall/IPS/IDS 等。
IPv6 安全策略規劃	針對各公司機關或商用服務規劃 IPv6 網路資安防護導入策略，提高部署效率。
IPv6 資安技術研究	研究前瞻性 IPv6 網路安全防護技術，提高安全防護品質。
建立 IPv6 安全管理制度	訂定與完善 IPv6 網路安全管理制度，提昇管理有效性。

名稱	說明
IPv6 網路安全教育訓練	定期安排 IPv6 網路資訊安全專業訓練。

肆、 企業網路設備基礎 IPv6 防護機制測試

一、 企業網路 IPv6 測試架構

企業網路接取架構係以中華電信 HiNet 固定制為例，企業用戶可經由企業內架設的交換器、防火牆、路由器再透過中華電信 HiNet 光世代網路連接至外部網路。

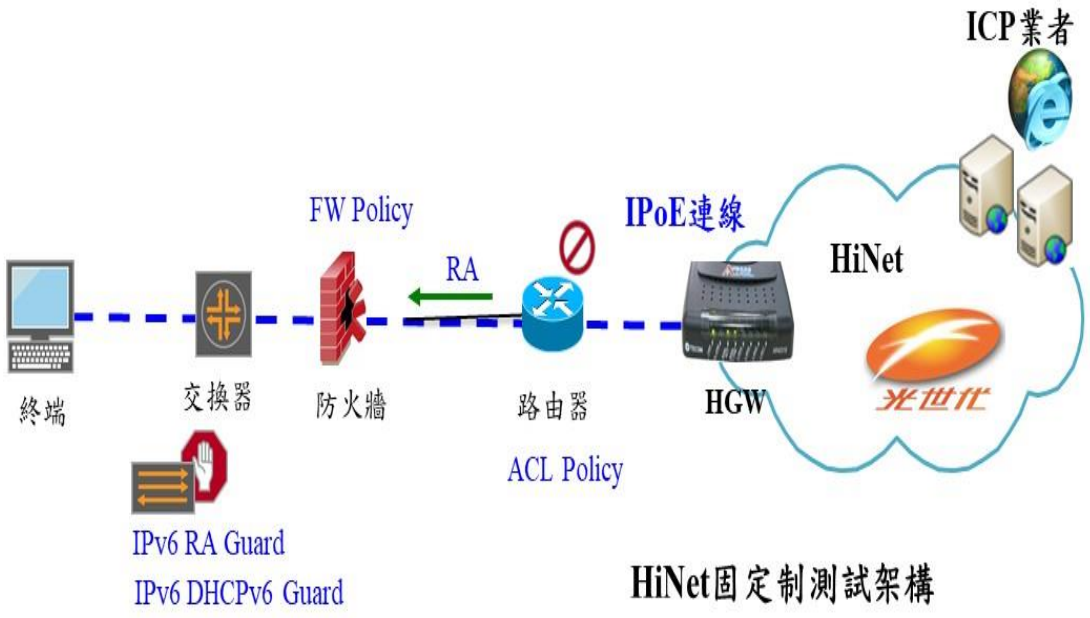

圖 1 IPv6 企業網路測試架構

二、 企業網路 IPv6 設備安全防護功能測試

本節主要針對交換器、防火牆以及路由器等三項企業網路基

礎網路設備進行 IPv6 安全防護功能測試。

(一)交換器 Switch

交換器為企業網路用戶連接的第一道防線，因此 First Hop Security 的安全防護功能便扮演關鍵的腳色。由於 RA 防護、DHCPv6 安全以及來源端驗證是企業網路基礎的安全防護機制，因此以下主要針對該三種 First Hop Security 機制進行驗證測試。

(1) IPv6 Router Advertisement Guard

IPv6 RA Guard 測試結果如圖 2 所示。

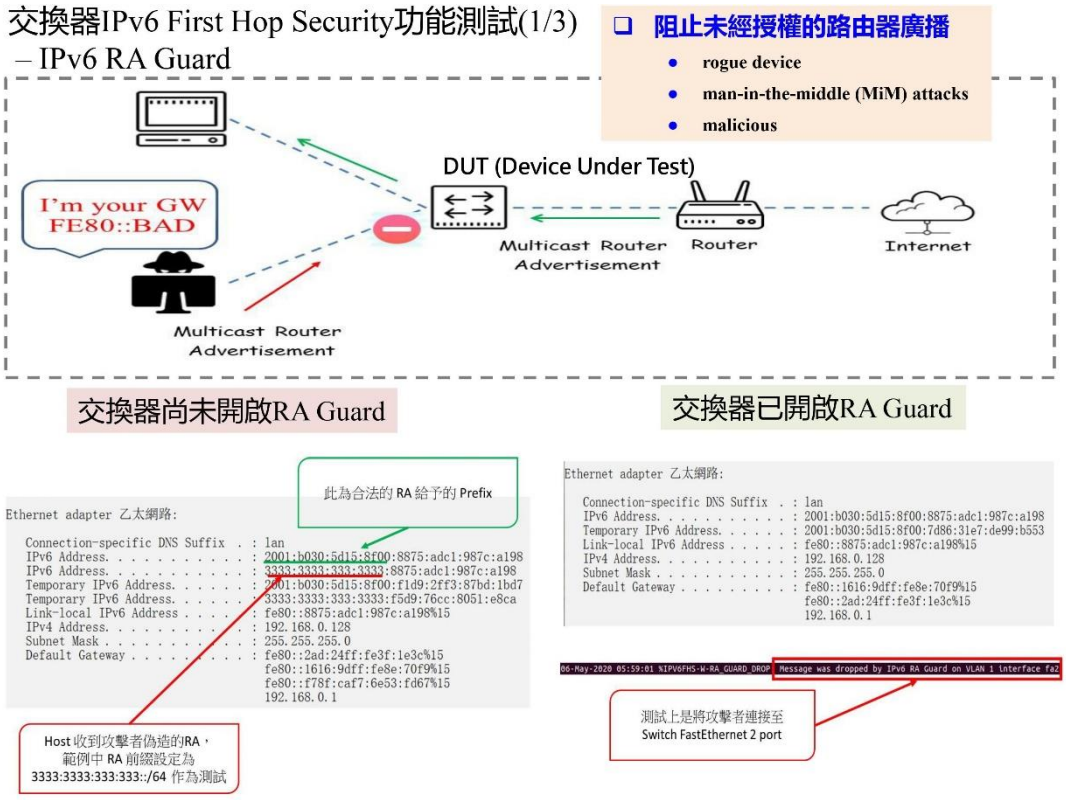

圖 2 IPv6 RA Guard 測試結果

圖 2 上方的部分為測試架構，下方的左右兩張截圖皆為被攻擊的 host 的網路資訊。左下的圖為尚未使用 RA Guard，使用紅色表示受害主機收到 3333:3333:3333:3333 作為前綴，作為攻擊者主機所送出的偽造 RA。使用綠色表示受害主機實際上收到的正確 RA，設有正確的前綴。右下方的圖為已使用 RA Guard，受害主機的網路資訊為正確的，並且於圖的下方附上交換機 log 的資訊，顯示交換機 FastEthernet 2 port 的 Message 被 RA Guard 丟棄。

(2) IPv6 DHCPv6 Guard

IPv6 DHCPv6 Guard 測試結果如圖 3 所示。

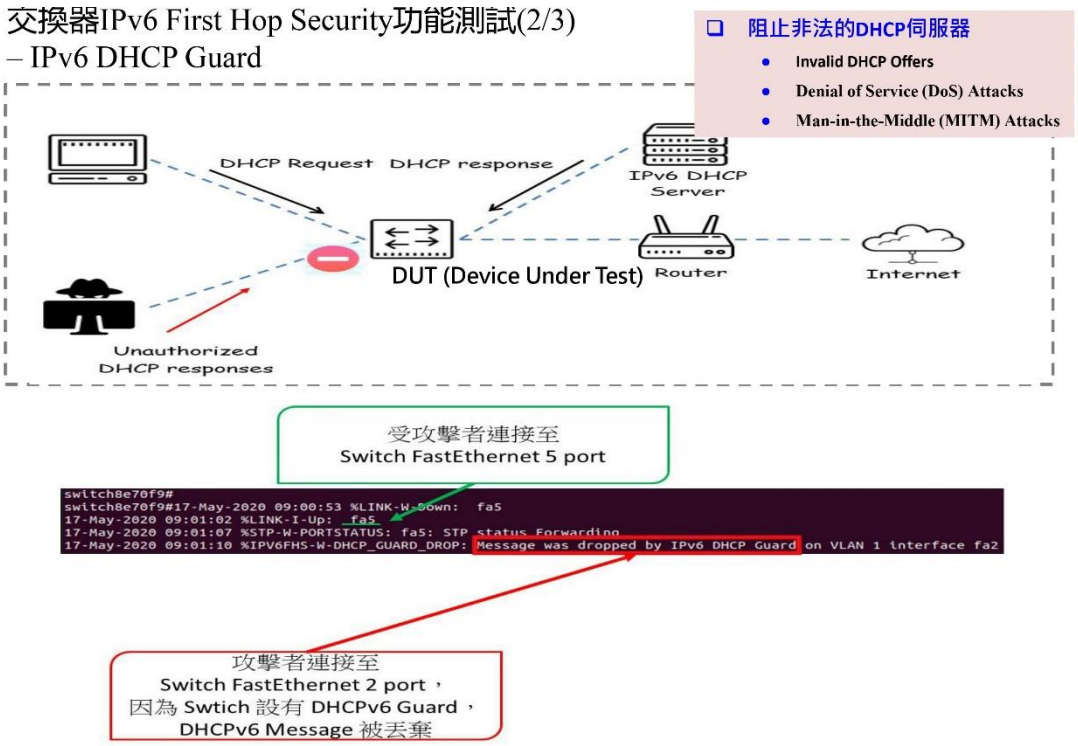

圖 3 IPv6 DHCPv6 Guard 測試結果

圖 3 上方的部分為測試架構，下方的圖為交換機 log 資訊的截圖，圖中內容為攻擊者所連接至的 FastEthernet 2 port 的訊息被交換機的 IPv6 DHCP Guard 丟棄，測試的結果顯示 IPv6 DHCP Guard 可有效管控異常 DHCPv6 訊務的發送。

(3) IPv6 Source Guard

IPv6 Source Guard 測試結果如圖 4 所示。

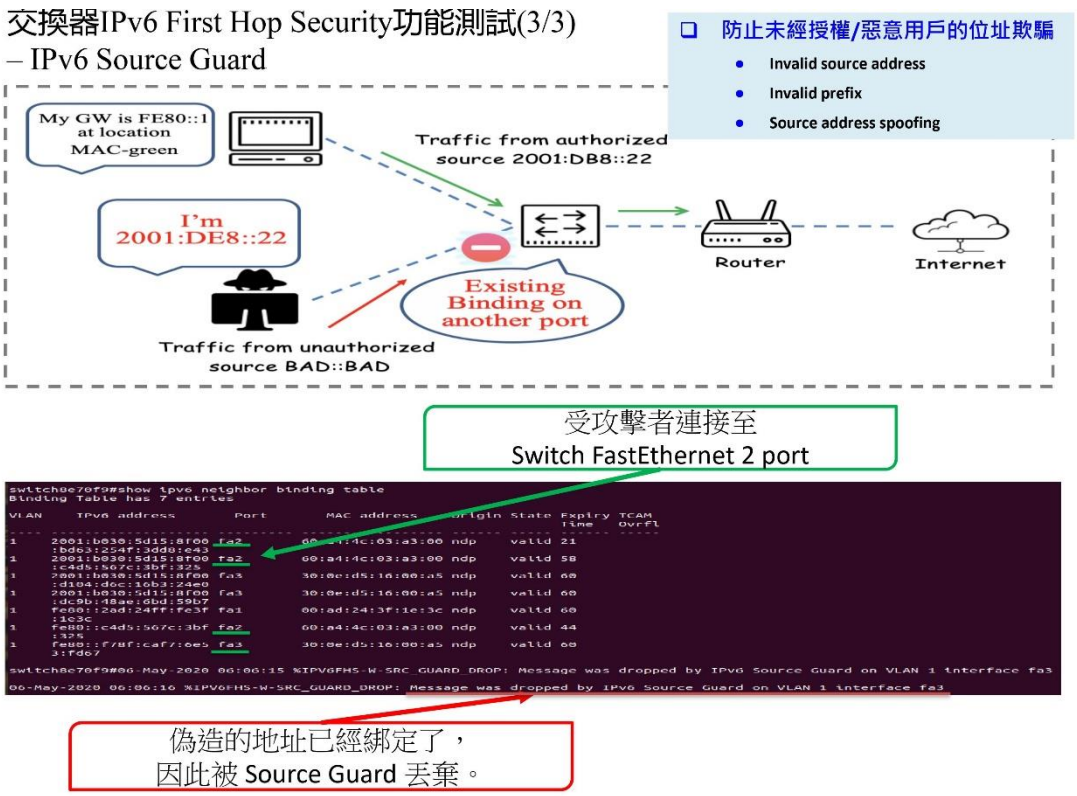

圖 4 IPv6 Source Guard

圖 4 上方的部分為測試架構，下方的圖為交換機 log 資訊的截圖，圖中內容為交換機 binding table 的資訊，綠色的部分表示為受害者已經連接至 FastEthertnet 2 Port，並且紅色為攻擊者因為偽造受害者的 IPv6 位址，因為 Switch 中的 binding table 攻擊者想偽造的 IPv6 位址已經綁定在其他 port 上，使得攻擊者的訊息被交換機 Source Guard 丟棄，測試的結果顯示 Source Guard 可有效依據 IPv6 攻擊來源的位址加以管控。

(二)防火牆 Firewall

由於市售企業用戶防火牆 IPv6 支援能力不一，因此本節針對防火牆 IPv6 功能測試部份，以 Address Scope、TUP/UDP Port、Extension Header 以及 Rogue RA 等功能為主。

本計畫以 Juniper SSG5 安全服務閘道器為例，由終端測試主機經由防火牆針對測試目標進行連線，防火牆管理介面 IPv6 設定畫面如圖 5 所示，除判斷廠牌設備型號規格實際支援能力外，也透過觀察管理介面的選項設計評估其 IPv6 資安功能與 IPv4 的差異。

圖 5 Juniper SSG5 防火牆 IPv6 功能設定介面

表 3 企業網路 IPv6 防火牆 SSG5 測試摘要

項次	測試項目	結果說明
1	IPv6 Address Scope	可阻擋 IPv6 invalid source address
2	Extension Header	不管封包正確性，一率 forward
3	Rogue RA	無法測試 Rogue RA
4	Application	無法指定 TCP/UDP port，只能使用預設 port 的 application

測試結果彙整如表 3。測試的結果顯示雖該防火牆指定過濾 IPv6 的位址格式，但針對指定 Port 以及 Rouge RA 等 IPv6 基礎防火牆的過濾規則仍有待加強，這同時也顯示 RFC 標準、FW 支援能力及防護設定之間仍可能存在差異，網管者需了解此差異，以評估是否需採取額外措施。

(三)路由器 Router

本節企業網路路由器 Router IPv6 測試主要以 Cisco 網路設備 ACL 為主，其他不同廠牌型號之設備，除可參考設備使用手冊外，也建議可請設備廠商提供對應的操作程序與範例，以作為實際設備設定 IPv6 功能的參考。圖 6 為 Cisco 2811 IPv6 ACL 設定範例。

```
R2>
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 access-list ncu2811
R2(config-ipv6-acl)#deny ipv6 host 2001:4860:4860::8888 any
R2(config-ipv6-acl)#exit
R2(config)#inter fa0/1
R2(config-if)#ipv6 traffic-filter ncu2811 out
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

圖 6 Cisco 2811 IPv6 ACL 功能設定範例

圖 7 終端設備訊務經路由器 IPv6 ACL 測試結果

終端設備經過路由器 ACL 管控測試結果如上圖 7。上半部分為尚未設定 ACL，測試的目標主機為 Public Google DNS 位址，

來自 IPv6 終端用戶的 ICMP 訊務連到目標主機;若啟動 IPv6 ACL 則測試終端的訊務就會如圖 7 下半部分備路由器 IPv6 ACL 規則阻斷。

三、 企業網路 IPv6 安全防護檢核清單

有關 IPv6 網路安全部署與規劃，建議可參考 RFC 4942[8]與 Cisco B.C.P 文件[9]制訂整體 IPv6 網路安全防護策略（IPv6 ACL 的原則)。以下提供企業網路對外啟動 IPv6 連線基本的檢核清單，期能提供企業網路 IPv6 安全佈署之指引參考。

表 4 企業網路導入 IPv6 安全防護 Check List

項次	說明	備註
1	研擬企業網路 IPv6 資安工作計畫。制定 IPv6 安全策略、盤點設備/系統 IPv6 支援能力、建立 IPv6 安全管理制度以及加強 IPv6 網路安全教育訓練等	
2	避免企業外部電腦設備直接存取企業內部的網路主機或設備	
3	防火牆設備必須能完整支援 IPv6	
4	重要資訊系統建議採用固定 IPv6 位址並考慮使用加密認證機制(IPsec 或是其他類似機制)	
5	管理者需使用安全的遠端存取 SSH(Secure Shell)機制和確保本通信介面不使用預設密碼	
6	強制使用 FQDN 與 DNS 定址，本地端使用者建議使用固定 IPv6 位址或採 DHCPv6 方式	
7	決定有效的 ICMP 封包過濾執行及 RFC 4890 所建議之封包篩選規定	
8	採用 IPv6 unicast reverse path forwarding 來拒絕所有不明來源位址的封包	

項次	說明	備註
9	阻止一切來自於不安全 IPv6 網路來源位址的訊務流量	
10	檢查 Outbound traffic 以及目的位址回應的匹配條件，檢測用戶是否有無意間夾帶任何殭屍網路流量或者惡意訊務	
11	攔截所有 Inbound SSL/TLS IPv6 訊務流量，並進行必要的檢查	
12	通過 IPS 的訊務需進行網路傳輸速率的限制，以避免網路設備流量超載	
13	路由協定如 OSPFv3、RIPng、BGP and IS-IS 應使用加密認證機制加強保護	
14	建議禁止使用 Tunnel 技術，(例如 IP Protocol 41、UDP 3544 teredo 等)	
15	建議啟動 First Hop Security 機制確保 IPv6 用戶接取網路安全	

伍、 結論

本報告主要探討企業網路導入 IPv6 安全議題與解決方案，並針對網路設備與主機 IPv6 資安防護提出摘要建議並針對企業網路設備基礎 IPv6 防護機制進行測試。此外，為強化企業網路 IPv6 安全，本計劃亦針對企業網路導入 IPv6 安全防護需求提出檢核清單，可作為我國企業網路未來部署 IPv6 安全管理之參考。

參考文獻

[1] RFC 4301 - Security architecture for the Internet protocol，

Available: https://tools.ietf.org/html/rfc4301

[2] RFC 8200 - Internet Protocol, Version 6 (IPv6) Specification，

Available: https://tools.ietf.org/html/rfc8200

[3] RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing，Available: https://tools.ietf.org/html/rfc2827

[4] RFC 3971 - SEcure Neighbor Discovery (SEND)，Available: https://tools.ietf.org/html/rfc3971

[5] RFC 2463 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification，Available: https://tools.ietf.org/html/rfc2463

[6] RFC 4057 - IPv6 Enterprise Network Scenarios，Available: https://tools.ietf.org/html/rfc4057

[7] RFC 7381 - Enterprise IPv6 Deployment Guidelines，Available: https://tools.ietf.org/html/rfc7381

[8] RFC 4942 - IPv6 Transition/Coexistence Security Considerations，

Available: https://tools.ietf.org/html/rfc4942

[9] IPv6 and IPv4 Threat Comparisions and Best Practice Evaluation(v1.0) Cisco Systems

附錄一、企業網路 IPv6 過濾政策參考指引

名稱	說明
IPv6 存取控制 (Inbound 與 Outbound 都建議阻斷)	■ The loopback address (e.g., ::1/128) ■ The unspecified address, similar to the IPv4 address 0.0.0.0 (e.g., ::/128) ■ The IPv4-mapped address (e.g., ::ffff:0:0/96) ■ Link-local unicast address (e.g., fe80::/10, fe90::/10, fea0::/10, feb0::/10) ■ Site-local address (e.g., fc00::/7) ■ The documentation address (e.g., 2001:db8::/32) ■ Overlay routable cryptographic has identifiers address (e.g., 2001:10::/28) ■ IPv6 Benchmarking address (e.g., 2001:2::/48) ■ Discard-only prefix for remote triggered blockhole routing address (e.g., 0100::/64) ■ IANA Special Purpose address Block (e.g., 2001:0000::/29 – 2001:01f8::/29) ■ Address ranges reserved by the IETF (0000::/8, 0100::/8, 0200::/7, 0400::/6, 0800::/5, 1000::/4,a000::/3, e000::/4, f800::/6, fe00::/9, fec0::/100, 3ffe::/16, etc)
IPv6 路由表頭過濾 (should be able to block)	■ Type 0 – routing header extensions (source routing) ■ Type 1 – routing header extensions (NIMROD routing) ■ Type 43 variant 0 – routing header extensions (Type 0) ■ Type 4-252 – unassigned ■ Type 253 & 256 – experimental ■ Type 255 – reserved
ICMPv6 訊務管控 (should be able to block)	■ Should be able to block ICMPv6 message types as follows: ■ Type 150 - Seamoby Experimental Protocol ■ Types 5-99 and 102-126 – Error messages not currently defined by IANA ■ Types 154-199 and 202-254 - All informational messages currently unassigned by IANA ■ Type 138 - Router Renumbering ■ Type 139 - ICMP Node Information Query ■ Type 140 - ICMP Node Information Response ■ Type 100, 101,200, and 201 – Experiment message types ■ Type 127 and 255 – Reserved Extension types

名稱	說明
IPv6 延伸表頭過濾 (should be able to block)	■ Next Header Code 0 – Hop-by-Hop Options ■ Next Header Code 60 – Destination Options (with Routing Options) ■ Next Header Code 43 – Routing Header ■ Next Header Code 44 – Fragment Header ■ Next Header Code 51 – Authentication Header ■ Next Header Code 50 – Encapsulation Security Payload Header ■ Next Header Code 50 – Encapsulation Security Payload Header ■ Next Header Code 60 – Destination Options ■ Next Header Code 135 – Mobility Header
其他 (No special attention needed IPv6 traffic SHOULD be dropped)	■ Address Configuration and Router Selection messages (must be received with hop limit = 255) ➢ Router Solicitation (Type 133) ➢ Router Advertisement (Type 134) ➢ Neighbor Solicitation (Type 135) ➢ Neighbor Advertisement (Type 136) ➢ Redirect (Type 137) ➢ Inverse Neighbor Discovery Solicitation (Type 141) ➢ Inverse Neighbor Discovery Advertisement (Type 142) ■ Link-local multicast receiver notification messages (must have link-local source address): ➢ Listener Query (Type 130) ➢ Listener Report (Type 131) ➢ Listener Done (Type 132) ➢ Listener Report v2 (Type 143) ■ SEND Certificate Path notification messages (must be received with hop limit = 255): ➢ Certificate Path Solicitation (Type 148) ➢ Certificate Path Advertisement (Type 149) ➢ Multicast Router Discovery messages (must have link-local source address and hop limit = 1) ➢ Multicast Router Advertisement (Type 151) ➢ Multicast Router Solicitation (Type 152) ➢ Multicast Router Termination (Type 153)