網際網路交換中心之黑洞路由系統設計與實作

陳品瑄　陳俊傑　王洋銘
財團法人國家實驗研究院國家高速網路與計算中心
{2303127, jjchen, addis} @narlabs.org.tw

摘要

國家高速網路與計算中心（NCHC）配合政府政策，建立了整合性的公共服務網路交換中心—福爾摩沙開放網際網路交換中心（以下簡稱FOX）。網路交換中心是不同網路之間進行資料交換和連通的樞紐，但由於網路架構的日益複雜和網路威脅的持續增長，網路安全問題成為了交換中心的首要挑戰之一。傳統的網路防護方式難以快速應對攻擊，因此需要更加即時和高效的防禦策略。隨著網路攻擊技術的不斷演進，網路交換中心所面臨的攻擊也更加多樣和複雜。FOX作為台灣的主要網路交換樞紐，保護其運營效率和安全性至關重要。因此，本研究旨在開發和實施一種能夠快速攔截惡意流量的防禦機制，保障交換中心成員的網路安全。本系統以遠端黑洞路由（Remote Black Hole Routing, RTBH）技術為核心，能夠在路由層面快速攔截和丟棄惡意流量。交換中心的成員可通過Web介面提交已知的攻擊源或異常流量來源，系統會根據黑名單進行路由驗證，並即時更新路由策略，將惡意流量導向黑洞。RTBH的實施不僅能夠集中化管理，還能降低每個成員配置和管理的負擔，減少資源消耗與複雜性。

本研究研究貢獻在於為網路交換中心提供了一種可行的即時防護機制，保護成員免受惡意流量攻擊，從而提升整體防護效率，達到了聯防機制的預期效果。

關鍵詞：RTBH、BGP、Blackhole、FOX。

Abstract

The National Center for High-Performance Computing (NCHC), in line with government policies, has established an integrated public service network exchange center—the Formosa Open Exchange (hereinafter referred to as FOX). As a critical hub for data exchange and connectivity between different networks, the network exchange center faces increasing challenges from the growing complexity of network architectures and the rising threats to network security. Network security has thus become one of the primary challenges for the exchange center. Traditional network protection methods are insufficient in quickly responding to attacks, necessitating more immediate and effective defense strategies. With the continual evolution of network attack techniques, the attacks faced by network exchange centers have become more diverse and complex. As one of Taiwan's primary network exchange hubs, protecting FOX's operational efficiency and security is of utmost importance.Therefore, this research aims to develop and implement a defense mechanism capable of rapidly intercepting malicious traffic, ensuring the network security of exchange center members. The core of this system is the implementation of Remote Black Hole Routing (RTBH), which allows for the quick interception and disposal of malicious traffic at the routing level. Members of the exchange center can submit known attack sources or abnormal traffic sources through a web interface, and the system will verify routes based on a blacklist, promptly updating routing policies to redirect malicious traffic into a black hole. The implementation of RTBH not only enables centralized management but also reduces the burden on individual members for configuration and management, thus lowering resource consumption and complexity.

The contribution of this research lies in providing a feasible real-time protection mechanism for network exchange centers, safeguarding members from malicious traffic attacks, enhancing overall defense efficiency, and achieving the intended outcomes of a collaborative defense mechanism.

Keywords: RTBH、BGP、Blackhole、FOX

1. 前言

網際網路交換中心(Internet Exchange IX) 交換中心是一個供網路供應商（ISP）和內容提供商(ICP)交換流量的實體設施。其主要為連線不同的網路供應商（ISP）或內容提供商，藉由網路交換中心交換訊務，可減少訊務繞境國外、轉訊成本、降低網路節點數及傳輸延遲，同時改善使用者的連線速度和服務品質，提供更高品質服務予使用者。在無IX架構下（如圖1所示），使用者和內容提供者訂閱的ISP必須互相連線，因此，可能需建置高達N*(N-1)/2條電路。但是若ISP透過IX介接(如圖2所示)，僅需租用少數大頻寬線路到IX，並於IX機房內跳線即可完成互連，除可大幅降低ISP互連線路成本外，亦可節省建置時間並減少網路傳輸延遲及頻寬消耗。

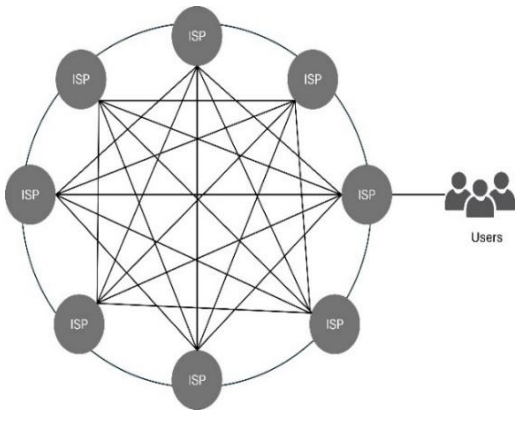

圖 1無 IX 架構連接方式

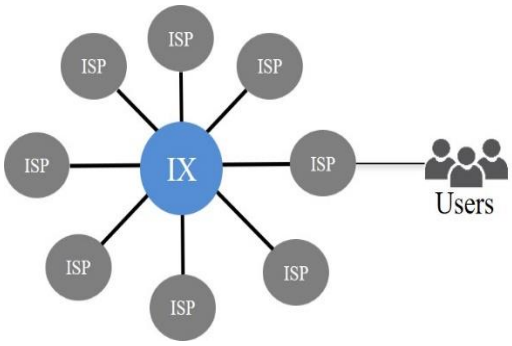

圖 2. IX 架構連接方式

本研究以 FOX 網路交換中心為例實作黑洞路由，以提供交換中心成員透過本系統遠端啟動黑洞路由，因此，本文採取與各交換中心成員情資交換、協同聯防的新思維，將攻擊流量直接於 FOX 網路交換中心協助攔阻，以達最理想的防禦機制。於第2章節介紹國內現行網路交換中心，第3章節進行黑洞路由文獻和技術探討，第4章節以實例說明 FOX 交換中心自動化路由黑洞機制系統架構與實作，第5章節說明系統現況與結論。

2. 國內網際網路交換中心介紹

目前台灣經審查認可通過的 IXP 共 4 家，分別為台灣網際網路交換中心 (Taiwan Internet Exchange, TWIX)、中華民國網際網路交換中心 (Taiwan Network Access Point, TWNAP)、台北網際網路交換中心(Taipei Internet Exchange, TPIX)及亞太網際網路交換中心 EBIX。TWIX 為我國第一個成立的網際網路交換中心，由中華電信負責建設維運，TWNIC 予以指導協助，於 1997 年開始提供服務。

TPIX 是由是方電訊公司所設置營運，於 2002 年開始提供服務。為會員數及交換訊務量最大之台灣網際網路交換中心，有多條海纜接入，故許多國外的網路服務供應商、網際網路內容業者、內容傳遞網路 CDN 業者，以及其他國際知名跨國企業如 Amazon、CloudFlare、Facebook、Microsoft 等皆已經接入，並在此進行公用互連與專用互連之訊務交換。EBIX 由遠傳電信所建置的亞太網際網路交換中心。提供路由交換服務(Peering)、轉訊服務(Transit)等項目。TWNAP 由國家通訊傳播委員會公布的「113 年第 1 季網際網路交換中心 (Internet Exchange IX) 統計資訊」顯示，TWNAP 現已無網路交換業務。

2.1 FOX 交換中心

FOX 網路交換中心[1]是由國家高速網路與計算中心(以下簡稱國網中心)配合政府政策為建立先進網路建設、以優化公共網路所建置，已於111年完成建置，並於112年加入國際路由安全共同協議規範 MANRS (Mutually Agreed Norms for Routing Security)，以共同維護全球互聯網的穩定和安全。FOX 串接國內四大公共服務網路，包含政府服務網路(GSN)、臺灣學術網路(TANet)、台灣高品質學術研究網路(TWAREN)以及中研院(ASNet)。除提升政府公共服務及教育研究所需雲端運算、儲存與資料治理服務之韌性，亦可透過網路交換中心建立與國際大型雲端服務及內容服務業者接取，以期提升公共服務跨網傳輸效率，降低國內網路交換成本。FOX 分別於台北、國網中心新竹節點資料中心、國網中心台中節點資料中心、國網中心台南節點資料中心四地建置機房以進行異地網際網路交換中心(IXP,Internet Exchange Point)。FOX 提供互連型態可分為多方互連（public peering）和雙方互連（private peering）兩種：

- 多方互連（public peering）：網際網路公共互連，為網路供應商（ISP）或內容提供商之間透過網路交換中心進行互連之行為。
- 雙方互連（private peering）：係指兩個 ISP 網路透過專屬線路直接進行封包交換，不與其他 ISP 共用，兩 ISP 之專屬電路可各自連接至交換中心，再由機房跳線完成；或由兩 ISP 間專屬電路完成。

3. 網路防護技術

黑洞路由（Blackhole Routing）和遠程觸發黑洞（Remote Triggered Black Hole, RTBH）都是用來應對網路攻擊的技術，儘管兩者都涉及丟棄惡意流量，但在實現和使用方式上仍存在一些顯著的差異。

3.1 黑洞路由（Blackhole routing）

Black Hole 主要是一種用於保護網路避免或減緩 DDoS 攻擊的機制，一般透過靜態路由或 ACL（Access Control List）來實現。目的是集中控制某一個地址或地址段的路由。首先定義一個指向 Null0的靜態黑洞路由，將 next-hop 導向到一個空的 IP 位址(黑洞)，也就是將目標路由間接指向 NULL。以圖3為例，當路由器收到動態或靜態路由欲往 172.68.1.1 傳送時，事先已於觸發路由器設定路由指向欲往該 IP 時，其下一節點（Next-Hop）必須往 192.0.2.1 轉送，而網路內所有邊緣路由器已知 192.0.2.1 的下一節點即為 Null0，此時路由器便自動將所有往 172.68.1.1 的封包直接丟棄。

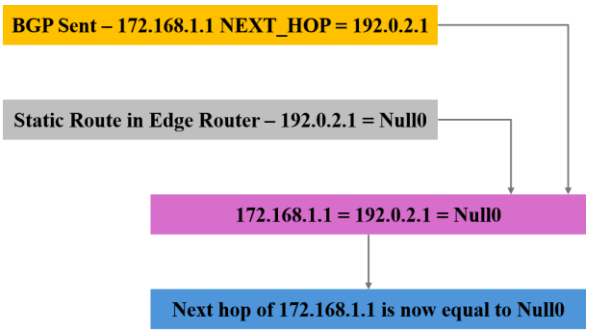

圖 3. Blackhole 啟動模式[2]

Null0為路由器的預設虛擬介面。預設為啟用狀態，但實際上無法轉發或接收流量。每當封包被路由到 Null0時，將被丟棄。Null0的運作方式類似於 UNIX 作業系統中的“/dev/null”目錄，主要目的在於捨棄不需要的流量。

3.2 RTBH (Remotely Triggered Black Hole)

RTBH 為更靈活和自動化的黑洞路由技術，主要透過 BGP Community 標籤來遠端觸發黑洞路由，無需手動配置每個路由器，使得特定的 IP 流量在整個網路中被丟棄，適合大規模、跨多自治系統的網絡攻擊防禦需求。網管維運人員在出現攻擊或異常流量時，遠端觸發路由器的黑洞行為，可以在多個路由器間快速傳播。RTBH 技術使管理員能夠基於攻擊來源或目的地自動調整路由，主要可分為2種:

- 目的導向

基於特定目的地主機保護方式，也就是事先定義欲保護的網路或主機。透過無法存取目的地主機伺服器，有助於保留剩餘網路內的路由基礎設施資源（CPU、記憶體等）。然而最大缺點是無法區分來源，即正常流量、攻擊流量都會被丟棄。一旦威脅減弱，再將目的地主機解除，重新投入服務。

- 來源導向

基於來源的 RTBH 根據特定的來源地址，在網路邊緣丟棄流量。這種方法使用與基於目的地的 RTBH 相同的觸發機制。在網路邊緣對攻擊者的來源 IP 位址進行黑洞封鎖。目標主機仍能處理其他請求。同時只有來自可信任的、已經過驗證的外部 BGP 連接的請求，才能觸發黑洞路由來封鎖指定的來源 IP 地址。這可以防止未經授權的或惡意的 BGP 鄰居誤導網路，避免錯誤封鎖合法流量，提升網路的安全性和穩定性。

4. 系統架構與實作

在本系統中使用 RFC 7999[3] 所定義標準的 BGP Community ‘BLACKHOLE’，通常表示為 65535:666實作 RTBH 機制。透過統一的 BGP community，使得不同運營商和自治系統之間能夠協同工作，簡化配置和管理，快速觸發黑洞路由及部署，立即阻止攻擊流量。同時，本系統結合 IP prefix 和 ASN 來驗證路由正確性，可以更精確地識別是否有來源地址欺騙行為，從而提高攻擊源識別的準確性，防止誤將正常流量當作攻擊流量處理，以有效防禦網絡攻擊。並在實作前確保所有網路交換中心各成員都了解並同意黑洞路由的策略和執行細節。

4.1 系統開發緣由

由第3章節說明黑洞路由運作方式後,本節將說明系統開發原因及以網路交換中心應用 RTBH 如何可以避免遭受攻擊所造成的影響。

網路交換中心各成員的防禦策略可能與其他成員不同，導致部分攻擊流量未被有效攔截，或過度攔截合法流量，影響到正常的網路操作，並且，若每個成員需要自行管理其路由器的資源和配置，這可能導致資源的重複使用或浪費，並且增加了對路由器的效能要求，透過網路交換中心實施 RTBH 可以減少重複配置，並確保防禦措施的協同效應，減少對整體網路的壓力。當成員 Member-A 下的系統主機遭受攻擊時(以圖6所示)，IX Route Server 發布路由資訊到交換中心上網路上，同時所有其他成員將接收 IX Route Server 的 BGP 路由，並根據其路由政策調整(以圖7所示)。透過網路交換中心 Route Server 政策制定，攻擊來源流量將被重新導向將 Next-Hop 指向 blackhole ，以確保攻擊流量在到達成員 Member-A 網路之前在交換中心架構上丟棄該流量。由網路交換中心執行黑洞路由可以在惡意流量到達網路交換中心各成員網路之前將其攔截並丟棄。因此，惡意流量不會進入任何各網路交換中心成員的網路，從而不會占用這些網路的入口頻寬減輕網路交換中心各成員的負擔。

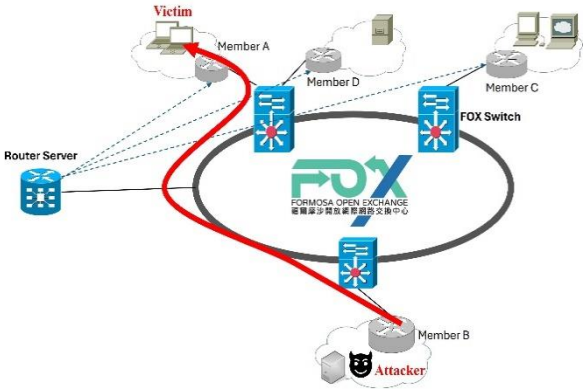

圖6. 網路交換中心攻擊情境示意圖

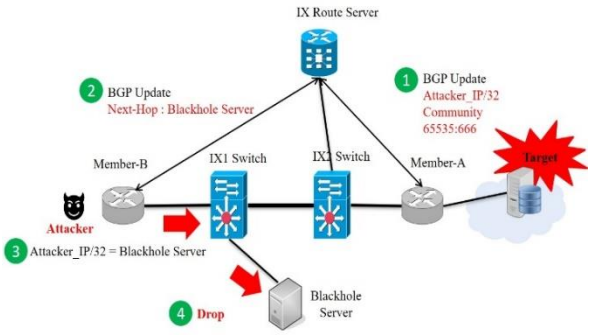

圖7. 網路交換中心攻擊流量防護示意圖

透過網路交換中心統一實作 RTBH 能夠提供更有效的防禦協調、更一致的防禦措施，以及更好的影響範圍控制，這些都可以減少對整體網絡和下游使用者的負面影響。相比之下，成員各自實作 RTBH 會增加管理的複雜性和防禦措施的不一致性，從而加大對網絡穩定性的潛在風險。因此，若由各 ISP 成員自行啟動黑洞路由並非最佳解法，故本系統以 FOX 網路交換中心為例採取與上游各成員協同聯防的新思維，透過各成員提供，遠端驅動將攻擊流量直接網路交換中心 Router Server 協助攔阻並藉由 BGP 技術與各交換中心成員交換網路，以達最理想的防禦機制。

4.2 系統架構

因此，為提供 FOX 網路交換中心各成員更好的防禦保護機制，透過成員間合作以達到資安聯防，歸結上述開發緣由與相關技術文獻採討。本系統架構開發以 FOX 網路交換中心為實例整體建置架構如圖8所示。透過本系統開發建置黑洞路由系統，成員可以遠端自行啟動黑洞路由。首先，與 FOX 網路交換中心各成員達成協議接受 Blackhole BGP community[3]後 ，並只接受黑洞路由的 prefix 為/32（IPv4），避免過度攔截，以確保只對特定的 IP 地址進行流量丟棄，而不會誤傷其他合法的 IP 範圍。當成員遭受攻擊時，可以透過本系統 Web 使用者介面輸入(如圖9所示)，遠端驅動 FOX 交換中心 Route Server ，Route Server 自動會透過 BGP 路由交換協定自動發送到 FOX 交中心各成員，並將攻擊流量在進入交換中心時,則會自動導到 blackhole 丟棄。

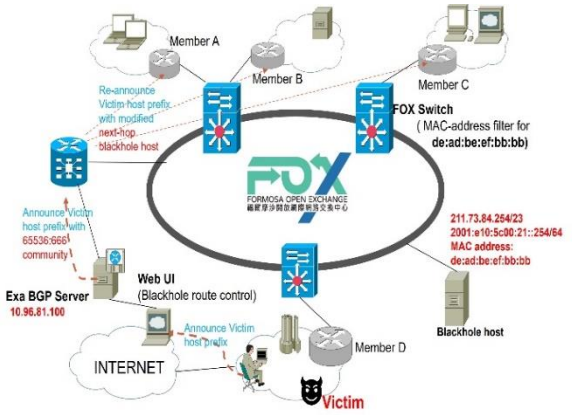

圖8. FOX 交換中心 RTBH 系統架構

Search Search...

#	Date ▼	IP	ASN	User	Status	Action	Tag
1	2024-09-26 10:49:03	211.79.63.8/29	7539	twarentest	enable	Unblock	router
2	2024-09-19 13:21:18	103.186.142.1	18423	hsuan-RAID	disable	Block	web
3	2024-09-19 13:10:22	211.79.63.52	9681	hsuan	disable	Block	web

第 1 頁 / 共 1 頁 上一頁 下一頁 第 1 頁

圖9. FOX Blackhole Service

4.2.1 Triger Router 配置

將與各成員協議好的 Blackhole BGP community (65535:666)事先設定在所觸發的路由器 FOX Route Server 上，設定如圖10所示。例如:基於在 Route Sever 設定 Blackhole BGP 政策設定(如圖11所示)，當收到 ExaBGP server 所發送的路由 211.79.63.52/32帶有65535:666 tag 時。Route Server 辨識為該 tag 為 blackhole community 時，透過在 Route Server 上所配置的政策，為會自動變更 next-hop(如圖12所示)。再由 next-hop IP 所設定的 static route 將攻擊流量導到黑洞丟棄。

```
-----------------------------------------
            entry 10
                from
                    community "blackhole"
                exit
                action accept
                    next-hop 211.73.84.254
                exit
            exit
            default-action accept
            exit
```

圖10. Blackhole BGP policy

```
==============================================================================
BGP IPv4 Routes
==============================================================================
Original Attributes

Network        : 211.79.63.52/32
Nexthop        : 211.73.85.240
Path Id        : None
From           : 10.96.81.100
Res. Protocol  : INVALID              Res. Metric    : 0
```

圖11. 原始發送路由

```
Modified Attributes

Network         : 211.79.63.52/32
Nexthop         : 211.73.84.254
Path Id         : None
From            : 10.96.81.100
Res. Protocol   : STATIC                Res. Metric     : 1
```

圖12. Next-hop 修改後的路由

4.2.2 ExaBGP 與路由驗證

ExaBGP[4]主要用於 BGP 協定。在網路架構中，ExaBGP 用於實作邊界閘道協議（BGP）路由管理和策略控制，ExaBGP 支援可從配置設定或 Script 中讀取路由資訊，並提供 API 讓使用者能以程序化的方式與 ExaBGP 進行進行路由操作和配置，能夠根據自定義的策略進行路由公告和過濾。由於其高度的可擴展性和靈活性，ExaBGP 成為進行 BGP 路由策略調整和網路安全防護的理想工具。本研究系統流程架構如圖13所示。建置 ExaBGP Server 與交換中心的 Route Server 之間的連線是確保網路路由訊息同步和更新的關鍵步驟。連線過程中需設置 BGP 的鄰居關係，通常包括以下步驟：

- 建立 TCP 連接：配置 ExaBGP 伺服器的 BGP 鄰居參數，指定交換中心 Route Server 的 IP 地址和 AS 編號，並設置必要的驗證和連接參數。
- 路由訊息交換：在連接建立後，ExaBGP Server 會開始接收來自 Route Server 的路由更新，並根據配置的策略處理這些信息。

路由驗證模組，是一種確保網路安全性的重要機制。在此模組流程中，當系統接收到一個 IP 的宣告時，它會先檢查驗證該 IP prefix 是否由該自治系統（ASN）所合法擁有。具體步驟如下：

- 查詢 ASN 的 prefix 列表：透過 API 向 RIPE NCC[5]的 RIPEstat 服務發出，請求來獲取指定 ASN 的 IP prefix 列表。解析 API 返回的 JSON 格式資訊中包含該 ASN 所宣告的所有 prefix，這些 prefix 表示該 ASN 合法擁有和管理的 IP 範圍。
- IP prefix 驗證：將該 IP 地址與之前獲取的 prefix 列表進行比較。比較的過程中，會檢查該 IP 地址是否在 ASN 宣告的任一 prefix 範圍內。如果屬於其中一個 prefix，則表示該 IP prefix 屬於該 ASN。

對於路由驗證過濾模組。這一過程對於本系統研究來說至關重要，因為它可以確保只有合法的 IP prefix 被用來進行 BGP 路由宣告，從而保護網路免受未經授權的路由操作。提高網路安全性和可靠性，防止路由劫持等攻擊行為。

最後，為了實施遠端黑洞路由（RTBH）技術，當收到要發佈或撤回的 IP，使用 Express 框架在 Node.js 中新增一个 API，透過新增的 API 呼叫 FOX-exabgp 函數，啟動 RTBH 處理宣布路由的命令；否則，執行發布撤銷路由的命令。

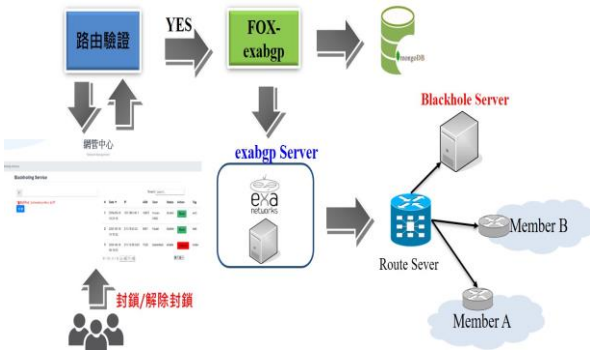

圖 13. FOX ExaBGP 服務系統架構

5. 結論與未來挑戰

RTBH（Remote Triggered Black Hole）作為一種重要的網路安全機制，在阻斷分散式阻斷服務（DDoS）攻擊方面發揮著重要作用。本系統將 RTBH 防護機制導入至 FOX 網路交換中心，透過引導攻擊流量至黑洞，幫助 FOX 網路交換中心迅速部署好黑洞路由環境，減少維運人員郵件往來和電話聯繫，即可快速隔離攻擊流量，從而保護交換中心網路和服務可用性。

隨著網路攻擊手法不斷演進和變化。因此，在網路交換中心的環境中，結合 RTBH 技術與其他先進的網路安全技術變得至關重要。未來，可以透過與資訊安全網路設備或攻擊偵測系統的合作，進一步提高 RTBH 的效益。例如，透過與流量攻擊偵測分析結合，監控網路流量和攻擊模式，實現更智慧化的攻擊偵測和應對。或是與網路防火牆、威脅情報共享平臺整合，可以更快速地更新攻擊規則和黑名單，加強對新型威脅的應對能力。同時與事件管理系統整合，提高 RTBH 的監控和報警追蹤功能，確保對異常流量的及時警示和處理。

總結而言，未來 RTBH 可以透過與資安網路設備或攻擊偵測系統整合，進一步提高對 DDoS 攻

擊的預防和應對效能，讓網路安全防護更加全面和完善。透過跨系統的協同作戰，可以建立更強大的網路安全生態系統，應對日益複雜的威脅挑戰，以維護網路交換中心網路環境的安全和穩定。

參考文獻

[1] FOX,https://www.fox.net.tw

[2] Chris Morrow, Tim Battles, and Danny McPherson, Customer-Triggered Real-Time Blackholes, North American Network Operators' Group 30th Meeting (NANOG 30), 2004.

[3] Thomas King, Christoph Dietzel, Job Snijders , Gert Döring, and Greg Hankins,BLACKHOLE Community,2016

[4] ExaBGP, https://github.com/Exa-Networks/exabgp

[5] RIPEstat,https://stat.ripe.net/about/

[6] Nick Hilliard, and David Freedman, A Discard Prefix for IPv6, 2012

[7] 張聖翊、李慧蘭、古立其、李柏毅、陳敏, 公共服務網路交換中心規劃與建置, TANET2021 臺灣網際網路研討會, 台中, 2021

[8] 陳俊傑,網際網路交換中心路由安全實作探討以 FOX 交換中心為例, TANET2023 臺灣網際網路研討會, 台北, 2023

[9] TWNIC RPKI 服務，https://rpki.tw/RPKI_service.html

[10] W. Kumari, and D. McPherson,Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF) ，2009

[11] Kleffman, Michael D., Analysis of Effects of BGP Black Hole Routing on a Network like the NIPRNET,2005