教育部113年度補助國立圖書館發展館藏特色及強化營運服務計畫

國圖網路安全升級計畫

執行成果報告

執行單位：國家圖書館

114年2月14日

壹、計畫目標

一、計畫背景

鑑於網路技術與通訊科技不斷的推陳出新，資訊安全持續受到高度重視，唯有建構安全的資通訊環境與完整的資料安全防護，才能提供讀者便利安全的資訊服務，也才能面對未來資安議題的各種挑戰與衝擊。本館為重要的關鍵基礎設施，存有多個全國唯一且重要的資料及系統，常為測試攻擊目標，為提高防禦能力，期藉由計畫的推動來強化本館骨幹網路及端點設備的安全防護力。

本館對外提供且持續維運的資訊系統與服務平臺近 60 個，每年進行資訊資產盤點及資安風險評估作業，並持續地就具有資安問題的系統與設備進行安全漏洞的修補、作業系統及資料庫版本的升級等作業。在補助經費的支持下 111 年完成官網主機架構調整、伺服主機及存儲設備升級；完成端點資安防護、網路管理及資訊系統日誌管理所需軟體購置；完成「 數位影音服務系統」、「臺灣華文電子書庫」系統架構調整及資安問題處理；完成「電子書刊送存閱覽服務系統」會員認證機制改善資安防護控制措施……等工作；112 年完成臺灣博碩士論文知識加值系統、圖書自動化管理系統暨全國新書資訊網、電子書刊送存閱覽服務系統、自修室及團體討論室預約系統、政府公報及政府統計資訊網、臺灣書目整合查詢系統等六項資安防護升級與功能優化案，符應教育部資訊系統向上集中、資訊安全等政策各項措施，將具有資安問題的資訊系統進行安全漏洞的修補、作業系統及資料庫版本的升級、主機架構優化等作業，並提供系統日常維護等服務。以建置安全穩定的網站環境。

113 年將持續配合資訊資源向上集中政策，除以本館有限的經費投入系統及資安問題改善外，仍有數個系統需補助經費，進行功能維護及優化、系統框架調整及移機等工作，尚未完成向上集中或預計留置館內之系統仍需依本館資安防護計畫持續維運。

二、預期目標

本案計畫目標有二：

(一)防火牆及核心交換器設備汰換，確保網路安全

資訊安全在現代數位化社會中變得至關重要。隨著數位環境的發展及企業和組織日益依賴資訊科技，資訊安全的維護變得迫切。組織面臨著越來越複雜和多樣化的資訊安全威脅。惡意軟體、網路攻擊和數據洩漏等問題日益嚴重，使得保護資訊資產變得極為重要。防火牆作為資訊安全的第一道防線，扮演著不可或缺的角色，通過監控、過濾和控制網路流量，為組織提供了強大的安全防護。

在現代組織環境中，網路連通性是業務運作的基礎，核心交換器作為網路的中樞，負責管理數據流量的轉發和路由，對於確保網路的穩定運作和資訊安全至關重要，為網路架構的重要組件，對於資訊安全具有關鍵性的作用。

網路安全威脅不斷演進，新的威脅、漏洞和攻擊技術不斷出現。汰換防火牆及核心交換器是維護網路安全、提高性能和確保合規性的關鍵措施。

(二)資訊系統版本升級，確保系統安全

主要辦理出版品國際交換資訊管理/出版品國際交換選書／捐贈機構查詢／臺灣漢學資源中心圖書資源等系統作業系統及資料庫版本升級、資安弱點修補、系統防護基準控制措施改善、系統移置教育部雲平臺等作業。

三、內容要項

(一)汰換防火牆及核心交換器，以強化網路安全

本館防火牆採用 FortiGate 240D，原廠將於 114 年 7 月 15 日終止服務，且 DMZ 區核心交換器亦已於 112 年 6 月 30 日終止更新服務，為確保本館網路資訊安全，預計將於 113 年汰換防火牆設備及核心交換器。

本館防火牆採用 HA 高可用性架構，2 臺防火牆互為備援，故需汰換 2 臺設備，並安裝所需軟體及服務。DMZ 區核心交換器目前以 2 臺 24port 設備作堆疊，擬於 113 年以館內實際需求狀況進行評估汰換，以強化網路安全。

(二)強化系統資安防護力，完成系統向上集中

出版品國際交換資訊管理/出版品國際交換選書／捐贈機構查詢／臺灣漢學資源中心圖書資源等4個系統於105年規劃建置，隨著資訊環境及技術的更迭，主機作業系統Windows 2012 R2已於112年10月終止支援安全修補程式，日後無法被告知系統潛在的漏洞及進行相關套件漏洞的修補，增加被攻擊、惡意軟體感染的可能性，亟需辦理版本升級，以符合資安政策。

依教育部112/10/11教育部網站弱掃報告，目前系統仍存在1個高風險及2個中風險問題；此外，為符合教育部防火牆政策的要求，須重新調整系統架構，關閉非必要的服務埠，達成系統向上集中至教育部雲平臺的目標。

因應軟體升級及資安問題改善的需要，預計辦理資安弱點修補、系統程式架構調整、資料搬移及參數重新設定等，此外，系統多為業務單位內部使用並以帳號密碼管制，將依實際權限授與相對之執行功能及資料存取權限，確保相關資料安全防護。

貳、成果內容

一、執行方式

(一)評估本館目前網路流量及設備使用狀況，依評估結果整理合適之防火牆與交換機規格，並分別辦理防火牆及核心交換機設備汰換採購案。後續在不影響核心資訊服務之前提下，進行新設備設定與更換，並檢視網路狀態是否正常。

(二)辦理資訊系統(出版品國際交換資訊管理/出版品國際交換選書／捐贈機構查詢／臺灣漢學資源中心圖書資源等)資安問題處理及向上集中作業。

(三)剩餘經費辦理本館無線網路增設點位與調整資安設定，無線涵蓋範圍擴大為本館閱覽空間及會議室，縮減不必要之訊號提供。在符合本館資安要求與網路需求性的考量下，保留iTaiwan、ncl_reader、ncl_staff、ncl_device四組訊號。

二、績效成果

(一)本館防火牆從 FortiGate 240D 2 臺升級至 FortiGate 201F 2 臺做 HA 架構，核心交換器從 Extreme BlackDiamond 8806 2 臺替換成 HPE Aruba 8360 2 臺及 HPE Aruba 8100 2 臺（共 4 臺）做雙 HA 架構，目前全館網路穩定運行中。

(二)出版品國際交換資訊管理／出版品國際交換選書／捐贈機構查詢／臺灣漢學資源中心圖書資源等系統完成向上集中作業，並強化系統資安防護力。

(三)重新檢視本館無線網路政策，並介接館員帳號認證，已取代傳統密碼驗證，提供資安防護更高的無線網路連接。

參、成效檢討

一、防火牆是網路安全的第一道防線，有助於防止未經授權的訪問、減少網路威脅、保護資料和資源，並維護網路的完整性和可用性，得以提供資訊資產管理系統及使用者電腦一安全使用環境。效益如下：

(一)資料安全保護

1. 攔截惡意流量：防火牆可以監控網路流量，擋住來自惡意攻擊者的入侵企圖，包括病毒、惡意軟體、釣魚攻擊等。
2. 濾除有害內容：透過深度封包檢測和內容過濾，防火牆能夠阻擋包含有害代碼的數據包，減少惡意程式進入網路的機會。

(二)網路資源管理

1. 流量控制：防火牆可以實施流量控制策略，確保合法的數據和應用程序優先獲得網路資源，提高整體網路效能。
2. 存取控制：通過存取控制列表等機制，防火牆確保僅授權的用戶和設備能夠訪問組織內部資源。

(三)攻擊預防

1. 入侵防禦：防火牆可檢測和阻擋入侵嘗試，包括異常的連線行為、多次錯誤的登入嘗試等，提高網路的安全性。
2. 阻擋 DDoS 攻擊：防火牆可以過濾大量的無效流量，防止分散式阻斷服務（DDoS）攻擊影響網路的正常運作。

(四)隔離和保密性

1. 虛擬區網（VLAN）隔離：透過 VLAN 技術，防火牆可將不同部門或用途的設備隔離，減少內部威脅的影響範圍。
2. 加密流量保密性：防火牆支援加密通訊的解密和再加密，確保敏感資料在網路上的傳輸過程中保持保密性。

(五)合規性和法規遵從

監控和報告：防火牆能夠生成詳細的日誌和報告，有助於組織遵守各種合規性要求。

(六)未來擴展性

整合新技術：先進的防火牆系統具有擴展性，能夠整合新的安全技術和更新，以因應不斷演進的威脅環境。

二、核心交換器須具備高頻寬和處理能力，汰換後可支援大量的資料流程量確保網路快速和高效地傳輸資料。並將流量均勻分佈到多個伺服器或資源，以確保最佳性能和資源利用率。效益如下：

(一)高效的數據傳輸

快速的數據轉發：核心交換器通常具有高速數據轉發能力，確保快速而可靠的數據傳輸，有助於提高內部和外部通信的效率。

(二)簡化網路管理

1. 集中式管理：核心交換器提供中央管理，使網路管理人員能夠更輕鬆地設定和監控網路設備，提高管理效率。
2. 集中化配置：透過核心交換器，組織能夠實現統一的網路配置，簡化了網路設備的管理和維護工作。

(三)流量控制和優先級處理

1. 流量管理：核心交換器可以實施流量控制，確保關鍵數據和應用程序的高效運作，同時防止濫用網路資源。
2. 優先級處理：核心交換器支援 QoS（Quality of Service），使網路能夠基於應用程序的需求對流量進行優先級處理。

(四)虛擬區域技術

資源隔離：透過 VLAN 技術，核心交換器能夠在同一物理網路上實現多

個邏輯網路，提供資源隔離，減少內部威脅的影響範圍。

(五)提升安全性

1. 存取控制：核心交換器能夠實現存取控制，確保僅授權的設備和用戶能夠訪問特定資源，增強網路的安全性。
2. 攻擊防禦：進階的核心交換器支援入侵檢測和防禦（IDS/IPS）功能，有助於阻擋各種網路攻擊。

(六)彈性擴展性

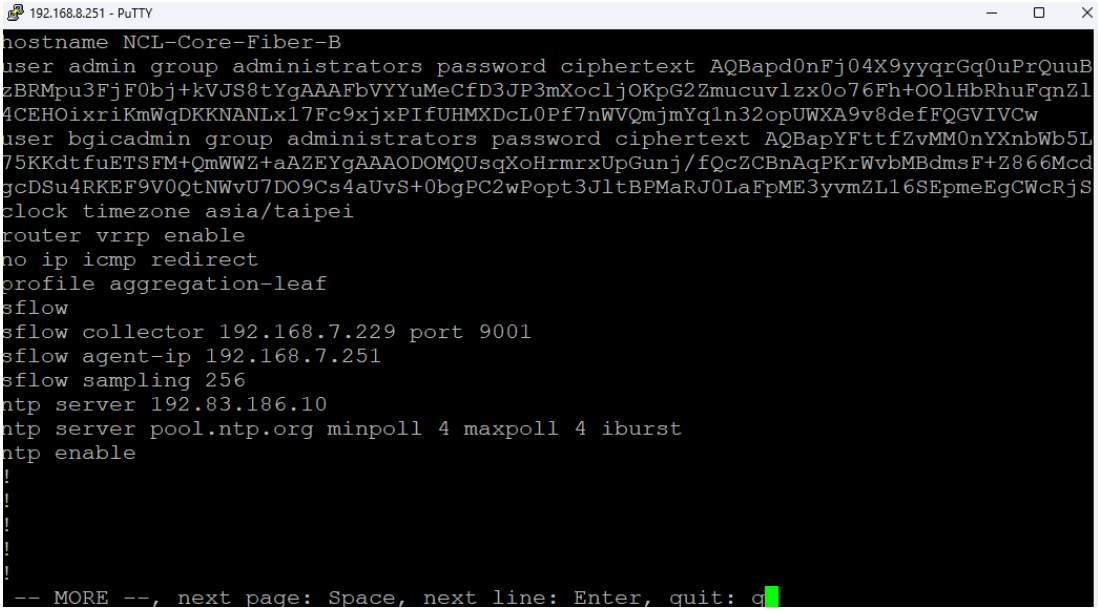
支援新技術：先進的核心交換器支援多種網路協議和標準，有助於整合新的技術和擴展網路能力，滿足不斷變化的需求。

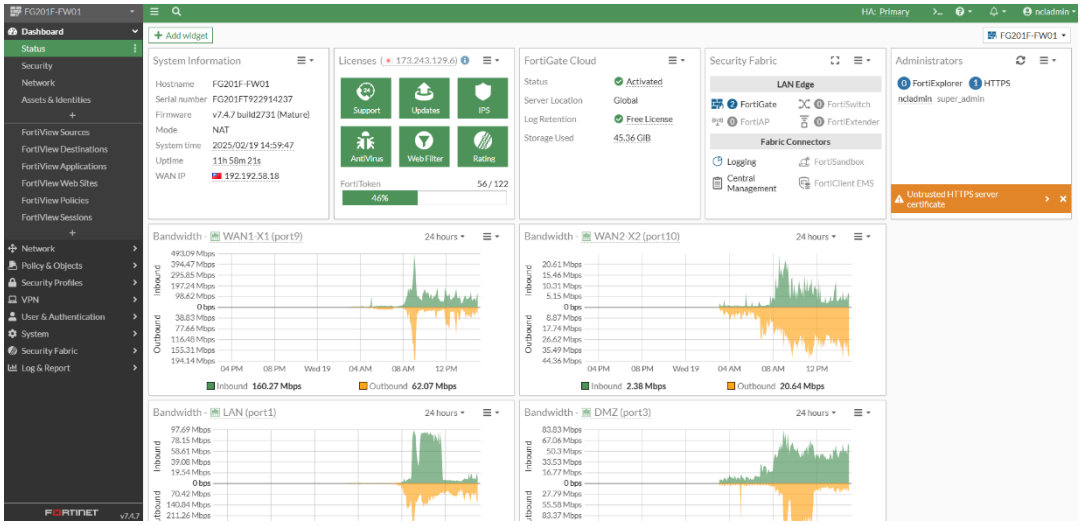
(七)提高整體網路可用性

冗餘和備援：核心交換器支援冗餘設計和備援連接，減少單點故障對整個網路的影響，提高網路的可用性。

三、完成出版品國際交換資訊管理/出版品國際交換選書／捐贈機構查詢／臺灣漢學資源中心圖書資源等系統向上集中之系統弱點修補，並完成向上集中所需資安問題處理及向上集中作業。

肆、附件(成果照片)


192.168.8.251 - PuTTY
hostname NCL-Core-Fiber-B
user admin group administrators password ciphertext AQBapd0nFj04X9yyqrGq0uPrQuuB
zBRMpu3FjF0bj+kVJS8tYgAAAFbVYYuMeCfD3JP3mXocljOKpG2Zmucuvlzx0o76Fh+OOlHbRhuFqnZl
4CEHOixriKmWqDKKNANLx17Fc9xjxPIfUHMXDcL0Pf7nWVQmjmYq1n32opUWXA9v8defFQGVIVCw
user bgicadmin group administrators password ciphertext AQBapYFttfZvMM0nYXnbWb5L
75KKdtfuETSFM+QmWWZ+aAZEYgAAAODOMQUsqXoHrmrxUpGunj/fQcZCBnAqPKrWvbMBdmsF+Z866Mcd
gcDSu4RKEF9V0QtNWvU7DO9Cs4aUvS+0bgPC2wPopt3JltBPMaRJ0LaFpME3yvmZL16SEpmeEgCWcRjS
clock timezone asia/taipei
router vrrp enable
no ip icmp redirect
profile aggregation-leaf
sflow
sflow collector 192.168.7.229 port 9001
sflow agent-ip 192.168.7.251
sflow sampling 256
ntp server 192.83.186.10
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
!
!
!
!
!
-- MORE --, next page: Space, next line: Enter, quit: q


FG201F-FW01
Dashboard
Status
Security
Network
Assets & Identities
FortiView Sources
FortiView Destinations
FortiView Applications
FortiView Web Sites
FortiView Policies
FortiView Sessions
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
HA: Primary
ncladmin
Add widget
System Information
Hostname FG201F-FW01
Serial number FG201FT922914237
Firmware v7.4.7 build2731 (Mature)
Mode NAT
System time 2025/02/19 14:59:47
Uptime 11h 58m 21s
WAN IP 192.192.58.18
Licenses
Support
Updates
IPS
AntiVirus
Web Filter
Rating
FortiToken 56 / 122
46%
FortiGate Cloud
Status Activated
Server Location Global
Log Retention Free License
Storage Used 45.36 GiB
Security Fabric
LAN Edge
FortiGate
FortiSwitch
FortiAP
FortiExtender
Fabric Connectors
Logging
FortiSandbox
Central Management
FortiClient EMS
Administrators
FortiExplorer
HTTPS
ncladmin super_admin
Untrusted HTTPS server certificate
Bandwidth - WAN1-X1 (port9)
Inbound 160.27 Mbps
Outbound 62.07 Mbps
Bandwidth - WAN2-X2 (port10)
Inbound 2.38 Mbps
Outbound 20.64 Mbps
Bandwidth - LAN (port1)
Bandwidth - DMZ (port3)


首頁 | ENGLISH | 網站地圖 | 國圖首頁
TAIWAN
Taiwan Resource Center for Chinese Studies
臺灣漢學資源中心
中心簡介
最新消息
書目查詢
資源介紹
> 資源介紹 > 相關網站
臺灣研究
漢學研究
研究獎助金
數位人文資源
第 0/0 頁
網站名稱
網址