



智慧雲端 – AI高速運算平台

AI High Performance Computing (HPC) Platform

台灣智慧雲端服務股份有限公司
Taiwan Web Service Corporation

Agenda

- TWS 公司簡介
- 產品簡介 Overview
- TWCC 使用者見證
- Infra 資安防禦: 國家級資安防禦系統

TWS 公司簡介



20TH
計算能量

全球超級電腦
(TOP 500)

10TH
能源效率

全球綠能超級電腦
(Green 500)



資料來源：2018年11月的全球排名・國網中心NCHC



台灣杉二號
TAIWANIA 2

科技部
4年投資

耗資
50億

政府
x
民間業者

TWCC TAIWAN
COMPUTING
CLOUD

Hello, we're



是



唯一運營商。

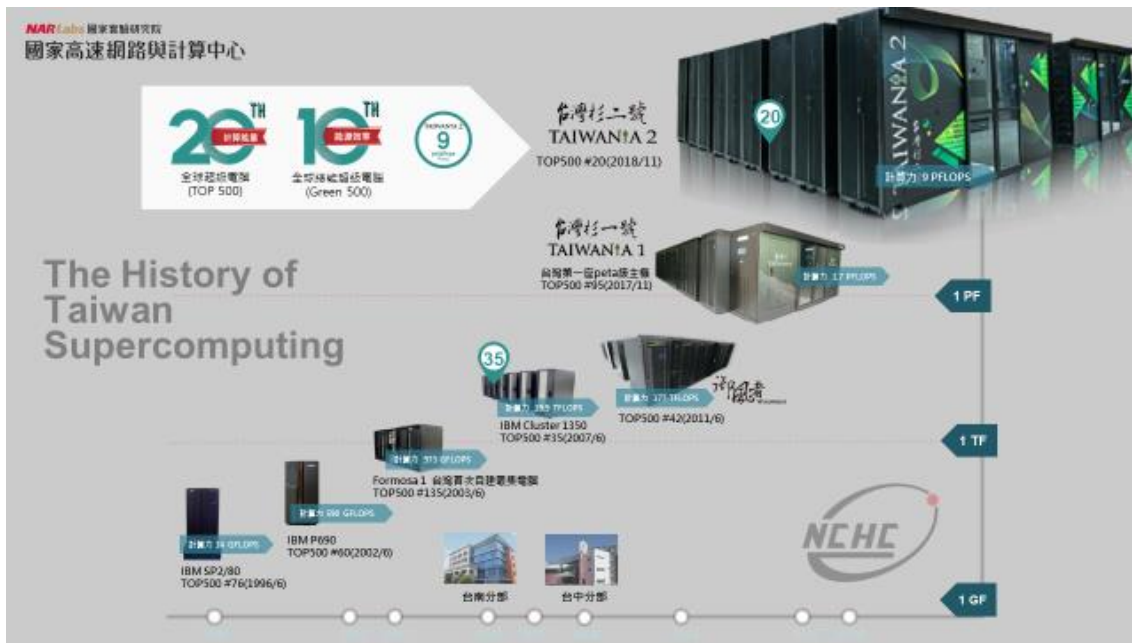
國家級超級電腦

提供產業數位發展所需的 AI智慧應用服務 及 雲架構解決方案

提升數位資料價值、推動 AI Ecosystem 合作共生

- Local · Secure · AI Enabler -

TWS 緣起與 TWCC 產品



TWS 團隊組成：

- 成員主要來自於 TWCC 核心建置團隊和 ASUS 在雲端的菁英
- 從技術領域出發，成就更快更好的雲服務

TWCC 建設目的：

- World Class **HPC Cluster** 世界級高級運算電腦
- 透過 AI 使用者需要的大量 GPU 算力，幫助台灣 AI 使用者、產業，提供更快更好的使用！

TWS 4大特色



國家主權雲平台
資料中心服務



本地最大
AI服務雲平台



技術自主
成就AI技術量能



AI Ecosystem
生態圈共榮成長

致力實現智慧應用及推展數位服務，協助客戶創造卓越的商務價值



在地合規高標資安: 助您安全上雲

Local compliance and high standards of information security

Local



機敏資料不出境: 助您關鍵資料防禦落地

Keeping the data of Taiwanese in Taiwan

Secure



推動 AI 產業生態圈: 助您智慧應用加速

Enable Taiwan AI Ecosystem

AI Enabler

產品簡介 OVERVIEW



關鍵資源: TWCC 臺灣AI雲

快速部署

容器運算服務

Container Compute Service

可快速部署 GPU 處理器的人工智慧工作環境，提高 29% 的工作效率



有效統御

高速運算服務

High-performance Computing

部署跨節點、多顆 GPU 的分散式高速平行運算環境，效能提高 30% 以上



智算兼備

虛擬運算服務

Virtual Compute Service

短時間內即能建立安全穩固、彈性應用的虛擬運算個體 (VM)



數據匯集

雲端儲存服務

Cloud Storage Service

安全高效率的多樣儲存選擇，適合各式運算情境，多層備份機制，安心儲存資料





容器運算服務

Container Compute Service, CCS

每個實體運算伺服器配備 8 張 NVIDIA Tesla V100 GPU 卡，支援 5120 個 CUDA 核心與 640 個 Tensor 核心，並支援 NVLink 進行 GPU 間的資料傳輸，加速人工智慧訓練、推論與高效能運算。



不同的容器選擇

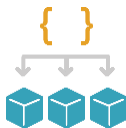
開發型容器 (Interactive Container)：可搭配 Jupyter Notebook 編寫程式，線上除錯、運算，行動裝置也能完成工作，隨時掌握進度。

任務型容器 (Scheduled Container)：能指定運算的開始執行時間，適當排程規劃批次任務使用的資源量，提升工作效率。運算完即回收運算資源，有效節省開發成本。



多樣化的 AI 框架

整合提供 NVIDIA 優化之 TensorFlow、Caffe、CUDA、Torch、PyTorch、TensorRT、CNTK、MXNet、Theano、DIGITS、RAPIDS 等 AI 框架，無需費心安裝問題，並能滿足不同模型訓練與推論的需求。



大記憶體容器，增加效能又快又準

容器最小規格至少配備 1 個 V100 GPU、4 個實體 CPU Core，以及 90 GB 主記憶體，定規資源比例，容易依據需求選定容器大小，並可同時部署與執行大量容器，加速 AI 模型訓練效率，提高預測準確率。



快速部署工作環境

採用 Kubernetes 架構，並導入 NVIDIA 優化 AI 軟體堆疊，用戶可快速複製專案內的 AI 計算環境，短時間內便能備份與快速部署開發工作環境，相較於傳統的方式可節省 3 倍的準備時間，並能彈性地轉換平台。

滿足 AI 訓練與推論需求的強大 GPU



V100 for PCIe



V100 for NVLink

效能

雙精度 7 TFLOPS
單精度 14 TFLOPS
深度學習 112 TFLOPS

雙精度 **7.8** TFLOPS
單精度 **15.7** TFLOPS
深度學習 **125** TFLOPS

頻寬

32 GB/S

300 GB/S

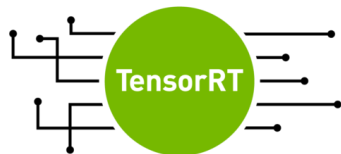
14 種 NGC optimized AI Frameworks



Caffe



PyTorch



mxnet

theano



RAPIDS





高速運算服務

High-performance Computing, HPC

TWCC使用國際開源軟體 Slurm 作為資源調度系統，為一容錯度高、高可擴展性叢集管理系統，適用於大、小型的 Linux 群集，至今已成為許多超級計算機所使用的資源管理器。

Slurm 本身並不需要針對系統內核 (Kernel) 做調整，並且相對獨立。作為一個群集管理系統，Slurm 有三個關鍵功能：

- 可在一段時間內，替用戶分配計算資源的獨佔或非獨佔使用
- 提供管理框架，於計算節點上進行資源的分配、執行與監控
- 可透過排程管理的工作列隊 (Queueing) 來仲裁資源分配



跨節點調度 GPU，實現高速分散式平行運算

支援原生超級電腦 (HPC) 操作介面，透過 Slurm 資源調度軟體，能實現跨節點的分散式平行運算，將高負載的工作量平均分派，提升處理效率，並有效減少虛擬化的額外負擔。



更加安全的容器運算環境

搭配 Singularity 來運行容器，用戶可使用本服務提供的 Docker 映像檔來進行相關 AI 運算，提升安全性。



具備極高吞吐量與極低延遲，資料傳輸更快速

採用 100 Gbs 高速網路串連 GPU 主機群，透過 NVLink 與超高速網路計算 (InfiniBand) 架構的整合，使 RDMA (Remote Direct Memory Access) 技術可大幅提升跨節點的大數據資料傳輸效率，解決傳統乙太網路的缺點。



彈性選用 GPU 數量，可進行多 GPU 平行計算

運算個體配備 NVIDIA Tesla V100 GPU，可加速 AI 訓練、推論的迭代循環，提升生產力。



虛擬運算服務

Virtual Compute Service, VCS

TWCC 提供的傳統一般型主機租用服務，除可以透過自動化工具及流程進行快速部署及回收，並可依需求將加速運算的 GPU 單元加載至虛擬運算個體，專門處理圖形任務的 GPU 核心資源，能快速完成大量運算。

可同時掛載多個虛擬磁碟，建立附加 Volume，自由彈性調配個體的儲存空間，智算兼備、節省成本的最佳選擇。



雲端佈建，多重選擇

提供多種作業系統 (Windows、Linux)、vCPU 數量、記憶體容量、GPU 硬體資源及儲存空間等，可以使用者習慣、需求彈性選擇。



自動平衡負載，服務不中斷

虛擬環境提供掛載負載平衡 (Load Balancing) 與自動擴容 (Auto Scaling) 服務，可設定使用條件自動偵測並彈性擴展縮減運算資源環境，無需時時擔心計算工作因系統超載資源不足而被迫中斷。



更加安全的運算環境

透過安全殼層 SSH 並搭配鑰匙對的安全方式進行連線虛擬運算個體，對敏感性資料傳輸加密並築牆抵禦惡意程式，可確保兩個站點之間安全傳輸。



輕鬆備份，迅速還原

快照備份服務提供您在雲端保存虛擬運算個體的設定、重要資料，並提供多種備份機制，能快速進行復原、重建作業，避免因人為操作不當所引發之損失。



虛擬運算服務—網路及資訊安全服務

Virtual Compute Service, VCS



虛擬網路

Virtual Network, VNW

本服務主要是為提供各虛擬運算個體可自訂虛擬網路及串接至網路的IP管理功能機制。本功能提供專案管理員使用完整存取權限，其轄下租戶使用者僅具讀取權限。



虛擬私有網路

Virtual Private Network,
VPN

TWCC 提供企業級 site-to-site VPN 功能，讓專案成員建立VPN虛擬私有網路，以達到訊息保密、傳送認證與準確性等網路安全功能。



負載平衡

Load Balancing Service,
LBS

本服務支援 TCP、HTTP、HTTPS 等通訊協定，當流量變大時，可以將流量分配到不同的虛擬運算個體上，以維持服務的靈活性、擴充能力及高可用性。



自動擴容

Auto Scaling

本服務是一種自動彈性調整資源機制，能夠在指定條件下動態增加或減少虛擬運算個體的數量，以因應負載增加所造成的資源不足問題，提升服務效能並降低成本。



基礎虛擬防火牆

Basic Virtual Firewall, BVF

本服務提供簡單靈活的架構，透過創建防火牆及資安管理規則，提供租戶網路安全防護機制。



安全性群組

Security Group

本功能提供網路安全性群組相關功能，使用者可透過簡易的規則進行網路安全政策控管。



雲端儲存服務

Cloud Storage Service, CSS

TWCC提供多樣化的儲存選項，包括：高速檔案系統 (HFS)、雲端物件儲存 (COS)、虛擬磁碟服務 (VDS) 多種儲存系統，適用於各式運算情境。可透過終端機、圖形化的入口網站線上存取檔案。



高吞吐量，安全耐久

各式儲存系統讀寫檔案速率快、安全耐久，並可高速處理海量的數據，大規模 AI 平行運算不中斷。



磁帶備份系統，多一層備援措施 **Coming Soon**

多一層自動備份機制，將資料存入磁帶設備，嚴謹對待每一筆資料，降低災難發生的風險。

高速檔案系統

Hyper File System, HFS

- 高性能的平行檔案系統能夠針對大檔案提供高吞吐量的 I/O，並對每筆資料快速存取操作，使用體驗佳。
- 可獨立作為一般資料儲存空間，並適用於 TWCC 各類型容器運算服務，支援 AI 高速運算服務的運算資料存放與傳輸。

雲端物件儲存

Cloud Object Storage, COS

- 可透過網路存放和存取各種資料類型 (支援 S3 協定)，資料儲存安全且經濟實惠。
- 可獨立作為一般資料儲存空間，並適用於 TWCC 容器運算服務、高速運算服務、虛擬運算服務的資料存放與傳輸。

虛擬磁碟服務

Virtual Disk Service, VDS

- 專為 TWCC 虛擬運算服務設計之儲存空間，提供固態硬碟 (SSD) 與標準硬碟 (HDD) 兩種儲存選擇。
- 用戶可使用虛擬磁碟建立多個附加 Volume，自由彈性調配虛擬運算個體的儲存空間。

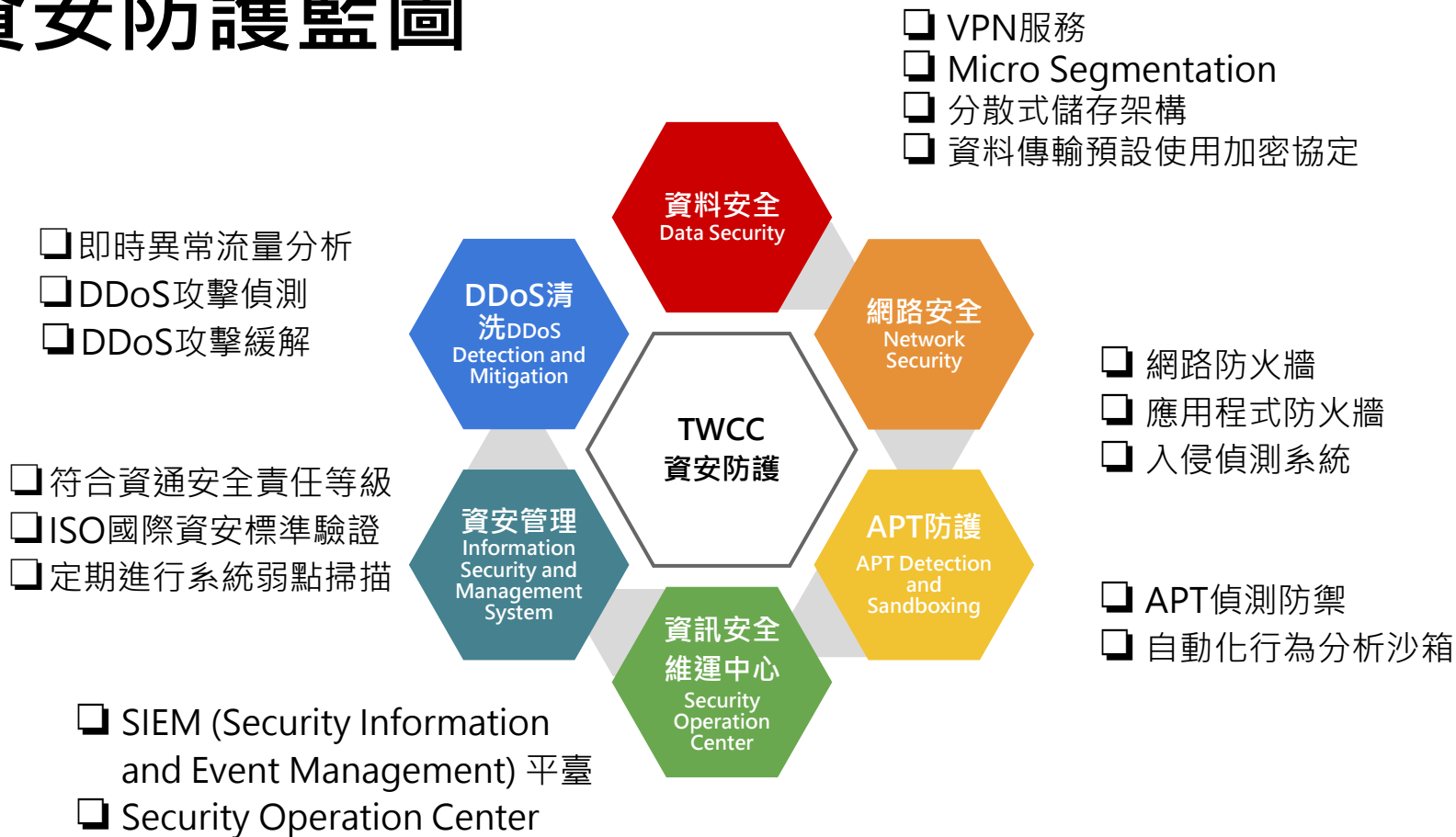
儲存服務比較

	高速檔案系統 HFS	虛擬磁碟服務 VDS	雲端物件儲存 COS
 搭配服務	CCS / HPC	VCS	藉由 TWCC CLI 傳輸資料至其他儲存服務
 容量上限	無	One Volume: 16 TB	無
 檔案限制	無	無	User Portal 單一檔案不得超過 1GB，總檔案數不得超過 1000
 存取限制	僅可透過 CCS / HPC 存取	僅可透過 VCS 存取	可透過 User Portal 或 Internet 存取
 傳輸速度	高	低	中
 價位比較	高	中	低
 資料傳輸	透過 SFTP 上傳及下載檔案	依虛擬運算個體內安裝的工具上傳與下載檔案，如：SFTP、FTP	透過 HTTPS 或第三方軟體上傳及下載檔案

INFRA 資安防禦: 國家級資安防禦系統

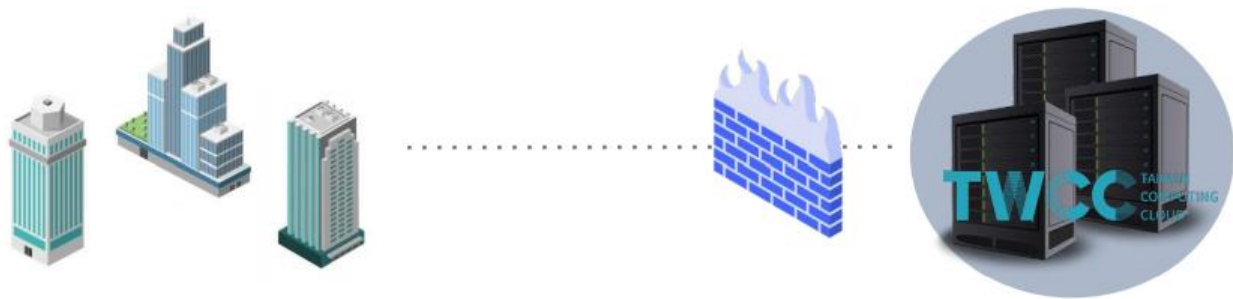


資安防護藍圖



新世代防火牆

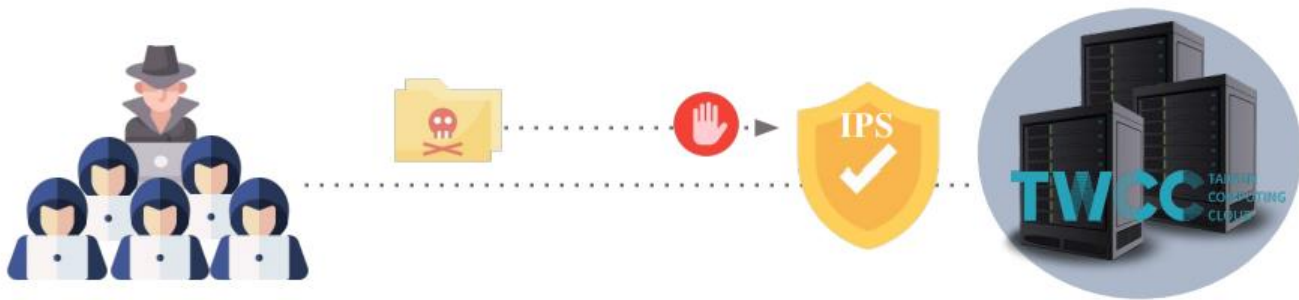
TWCC 部署「新世代防火牆 (Next-Generation Firewall)」網路安全設備，對於進出的網路流量進行資安政策管控，降低服務主機遭到外部攻擊的資安風險。



- **實施存取控制 (Access Control)**：依據資安政策進行流量管控。
- **降低暴險範圍 (Exposed Surface)**：關閉不需要對外開啟的通訊埠。
- **應用服務識別與管理 (Application Identification and Management)**：依據資安政策管理應用服務。

網路型入侵偵測防禦系統

TWCC 為有效降低網路攻擊所帶來的威脅，配置網路型入侵偵測防禦系統(Network Intrusion Prevention System)，監控網路流量，偵測異常行為並即時阻絕網路攻擊，以確保網路服務主機安全。



- 入侵偵測 (Intrusion Detection)：觀察網路流量並偵測可能的網路入侵行為。
- 威脅防禦 (Threat Prevention)：辨識網路攻擊特徵並即時阻絕。
- 網路威脅情資 (Cyber Threat Intelligence)：定期接收並更新最新的網路威脅情資，已識別最新的網路攻擊手法與特徵。

資訊安全維運中心

TWCC擁有專業網路團隊，可提供ISP等級管理與防護。可全天候針對威脅行為進行告警與資安事件通報應變處置，並對於 APT 攻擊發送預警通報。



- 安全資訊與事件管理平臺(SIEM)
 - 設備佈署：國網中心臺中分部
 - 維運位置：國網中心臺南分部
 - 說明：收集網路防火牆、重要主機與設備系統日誌，進行關聯性分析與威脅判斷。一旦發現高風險事件則會發出告警，並由SOC維運人員進行事件追蹤與應變處理

國際資訊安全標準認證

變革創新管理品質典範

2019: ISO 9001 Plus Award 變革創新管理品質典範獎

個資管理系統國際認證

2020: BS 10012:2017 個人資料保護

2020: ISO/IEC 27017:2015 資訊安全管理

2020: ISO/IEC 27018:2014 個人隱私資料保護

資訊安全管理系統國際認證

2019: ISO 20000 資訊服務管理驗證

2020: ISO 27001:2013 資訊安全管理系統 (ISMS)

雲端安全國際認證

2019: ISO 27017 雲端服務資訊安全

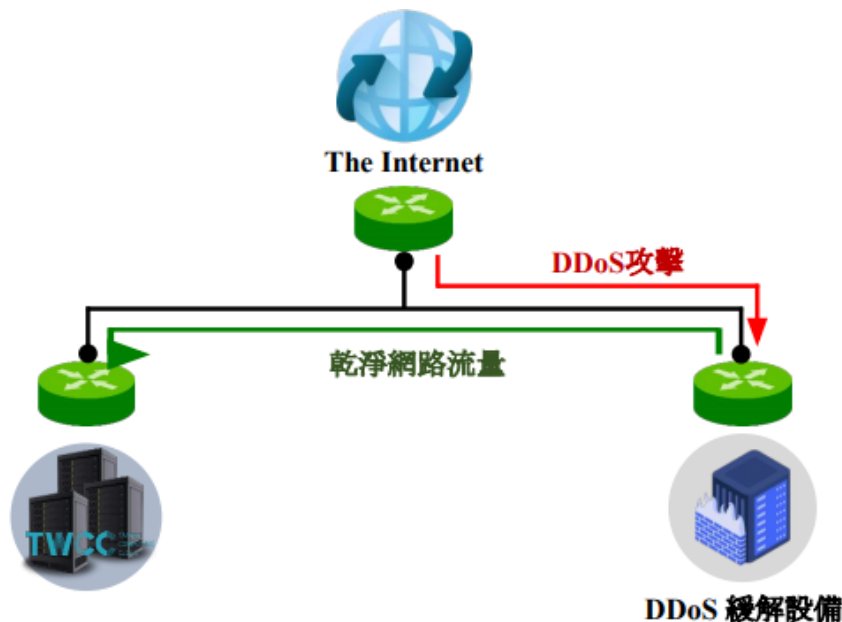
2015: CSA STAR Level 2 金牌



DDoS 攻擊偵測與緩解系統

面對與日俱增的 DDoS 攻擊，於骨幹網路建立 **DDoS 攻擊偵測與緩解系統**，保護 TWCC 重要對外網路服務，確保網路連線品質與服務可用性。

- **DDoS 攻擊偵測**：收集 Netflow 資訊並即時偵測網路攻擊行為。
- **DDoS 攻擊緩解**：使用 Clean-Pipe 技術，將 DDoS 攻擊流量導引至清洗機進行過濾，再將清洗後的乾淨流量放回原本的路由。





Thank You