RDSecurer

重新定義網路傳輸秩序

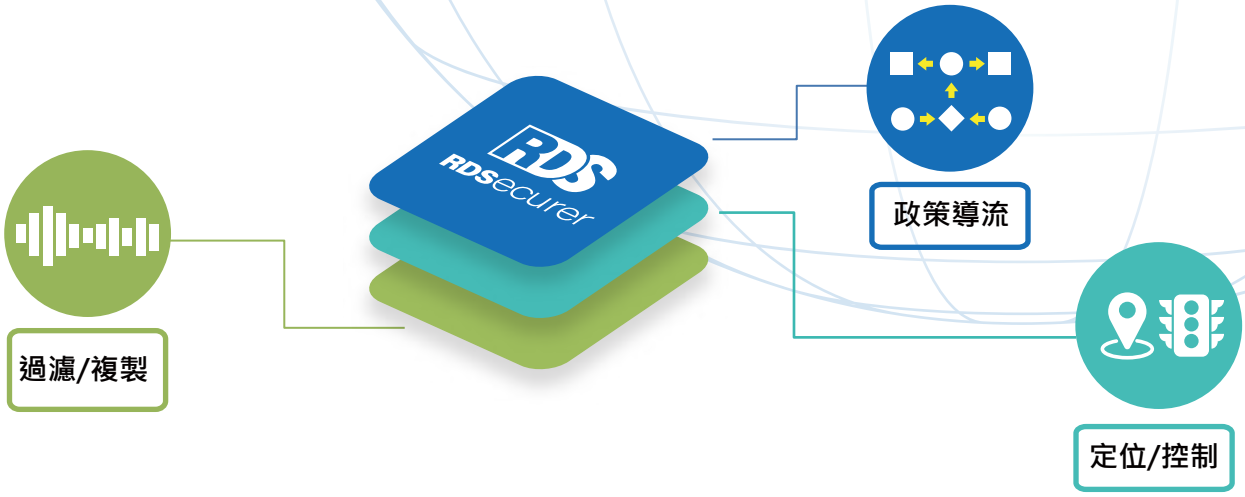
流量定義控制系統
RDSecurer Traffic Defined Controller

人類疫情與數位疫情為 IT 營運管理帶來三重夾擊

2019年的某天，COVID-19病毒摧毀地球上與人相關的各類連結，範圍廣及差旅移動，糧食生產、物流運輸、產品製造，甚至是學校教育等活動均被迫延宕，甚至停止！且影響至今已超過兩年仍尚未結束，這是人類文明史上非常罕見的！為此，各行各業冀望透過數位技術的大量運用，如：遠距辦公與教學、智慧製造，零售OMO等數位應用及轉型來突破眼前難關，卻也面臨巨量數據的匯聚/過濾/複製/導流等各類問題。

然而，網路犯罪組織也嗅到全球大量數位化應用可帶來的鉅額犯罪收益，極力探勘各營運系統、IoT裝置、網路設備，甚至是資安產品上已存在的各種弱點，並以最短的時間將其武器化，搭配近年極為盛行的勒索病毒，大舉攻陷全球各類型組織，其衍生的營運癱瘓，資料外洩，生命威脅及形象聲譽等鉅額損失已無法估計！為此，須儘速完成各類重要系統弱點評估及修復的目標同時，所衍生而來的經常性服務停頓的狀況，將是另類的數位災害！

總結上述，現今組織 IT 營運管理將同時面臨**巨量資訊處理 + 數位網路攻擊 + 修復性服務停擺**引發的**三重夾擊**，猶如面對職業格鬥家的連續技襲擊，如果仍以傳統管理思維及網路框架應對，將難以招架!



突破既有網路藩籬，另闢數據傳輸新道路

RDSecurer Traffic Defined Controller 可針對 OSI Layer 1 ~ Layer 4 通訊協定中絕大多數的參數提供辨識、引用及變更等**流量自定義控制**能力，如：依據管理需求定義流量管理政策，當網路流量經過 TDC Platform 時，依政策要求特定流量執行過濾、重新套用VLAN ID 並複製成多分流量後，分別將各流量導流至不同 Interface 傳送，如此獨特且強大的引流能力，適用於包含內網東西向存取控制，流量定義服務鏈及大範圍流量複製等各類不同應用場景，將有效協助組織重新制定內網傳輸應用的各類需求！

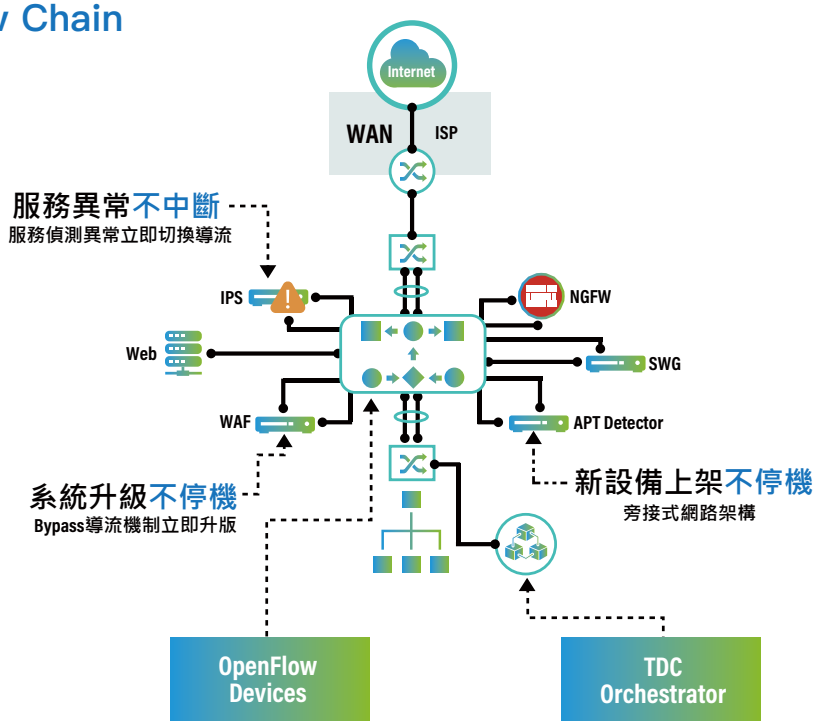
部署 TDC 優勢

- 降低服務停擺的隱性成本
  - 系統更新與漏洞修補
  - 新服務上線
- 建立零信任存取架構
  - 裝置自動定位
  - 端末設備存取控制
- 彈性管理網路流量
  - 過濾/匯聚/複製
- 最佳化投資效益
  - 降低資安產品負載
  - 彈性分配線路頻寬

改善傳統資安骨幹架構缺陷 – Flow Chain

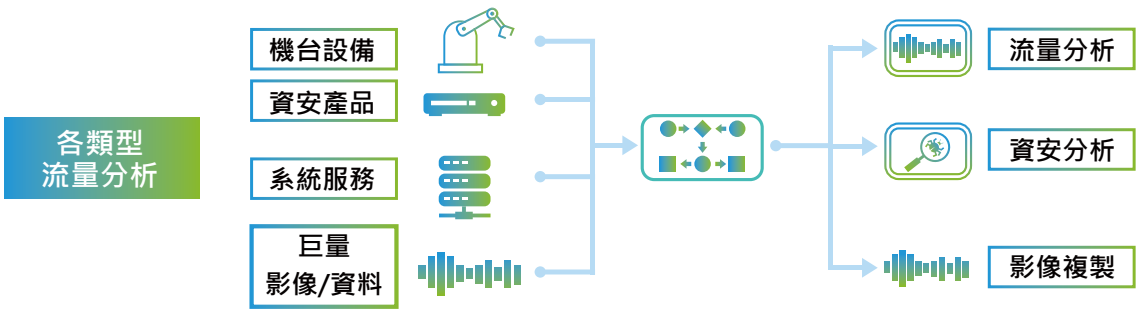
傳統串接式資安骨幹網路架構存在著單一設備故障即斷線；系統更新或新產品上線時須中斷組織聯外服務，且服務測試失敗恐需面臨Roll-Back 窘境；更別提資安設備常需處理自己無法辨識的服務流量類型，而衍生無效投資的浪費發生！

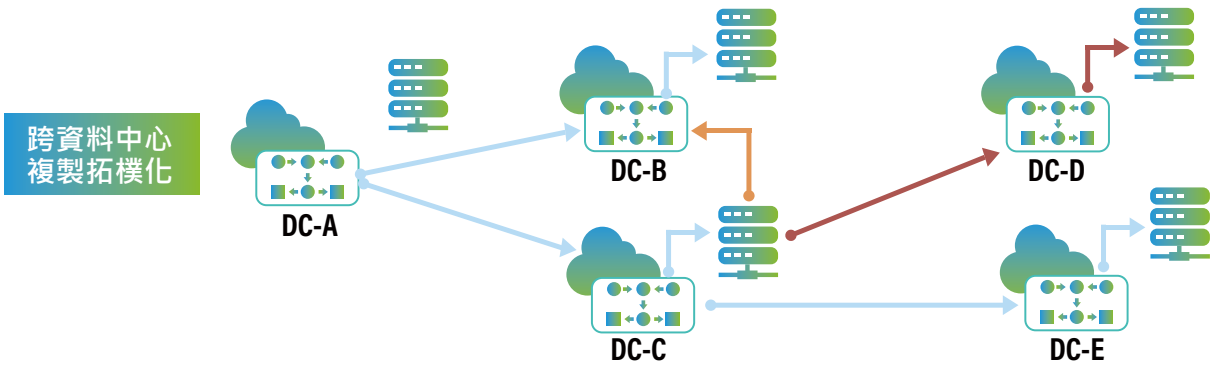
TDC Flow Chain以 OpenFlow Devices 可佈建於任何有網路及資安設備需整合導流的現場，常見於Internet出口與核心網路交換器之間，將原有串接式資安骨幹網路上的各資安設備，採並聯旁接架構接入OpenFlow Device上，結合TDC Orchestrator 集中化管理平台，依據管理政策需求或資安產品特性，派發專屬的流量定義鏈政策，徹底改善上述提及傳統資安骨幹網路設備的各項缺陷，且因服務停止的次數大幅減少，進而降低潛藏其中的巨大隱性管理成本。



大數據時代的資料傳導利器 – Flow Tapping

數位化時代，數據即是黃金，數據即是武器！數據萃取的各類需求也因應而生，無論是生產數據、消費習慣，乃至於資安鑑識分析等各類需求，皆需由遍布各處且零散的資料進行匯聚/過濾後，依據政策需求複製到分析器的所在處，而目的地甚至需要跨越資料中心或廠區，具備拓樸化流量管理介面，可更友善的提供Tapping管理者正確的制定流量傳導複製政策，而TDC Flow Tapping已具備您未來或是現在的使用需求！

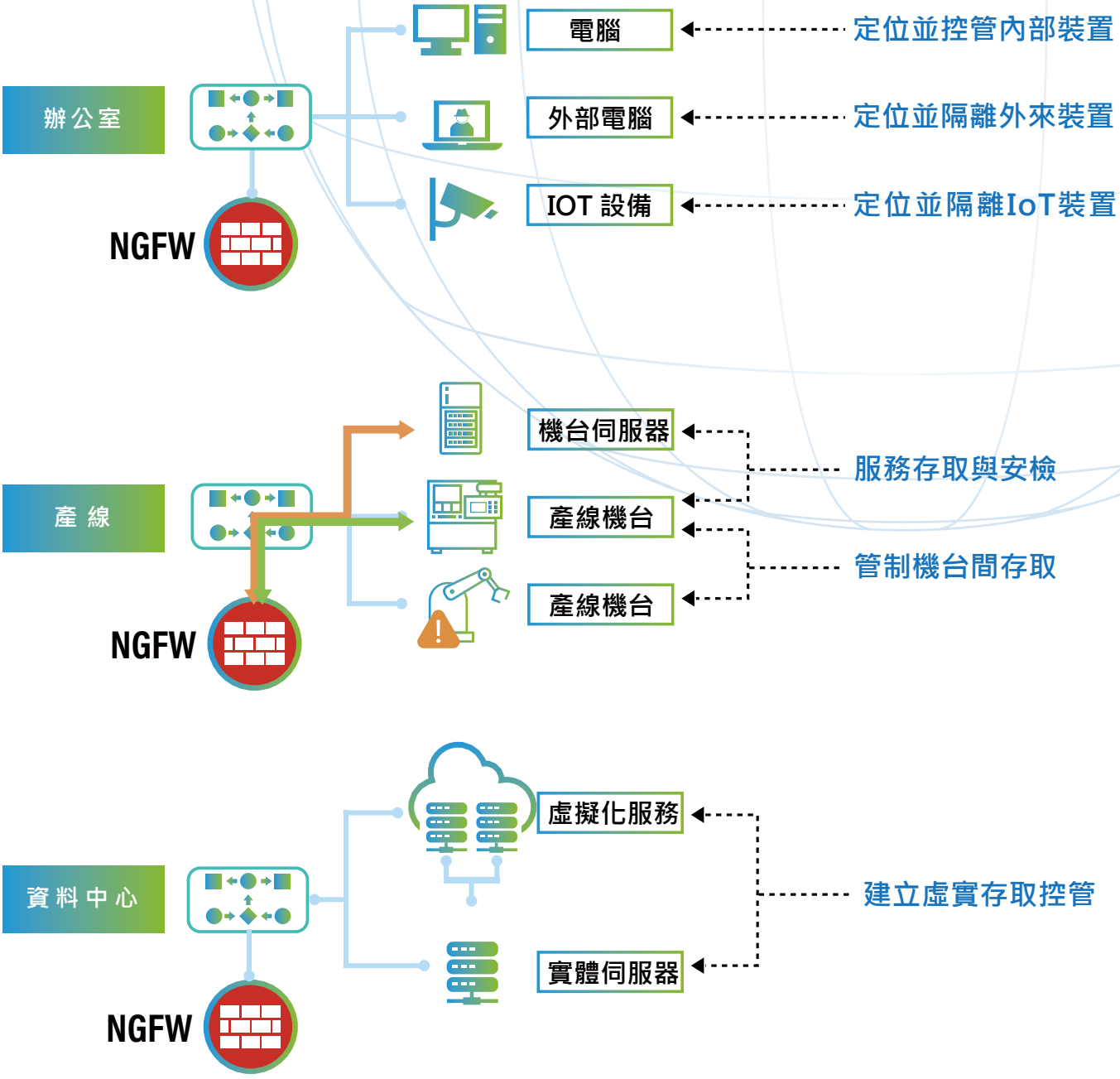




更智慧且彈性的東西向存取控制 – Flow Guard

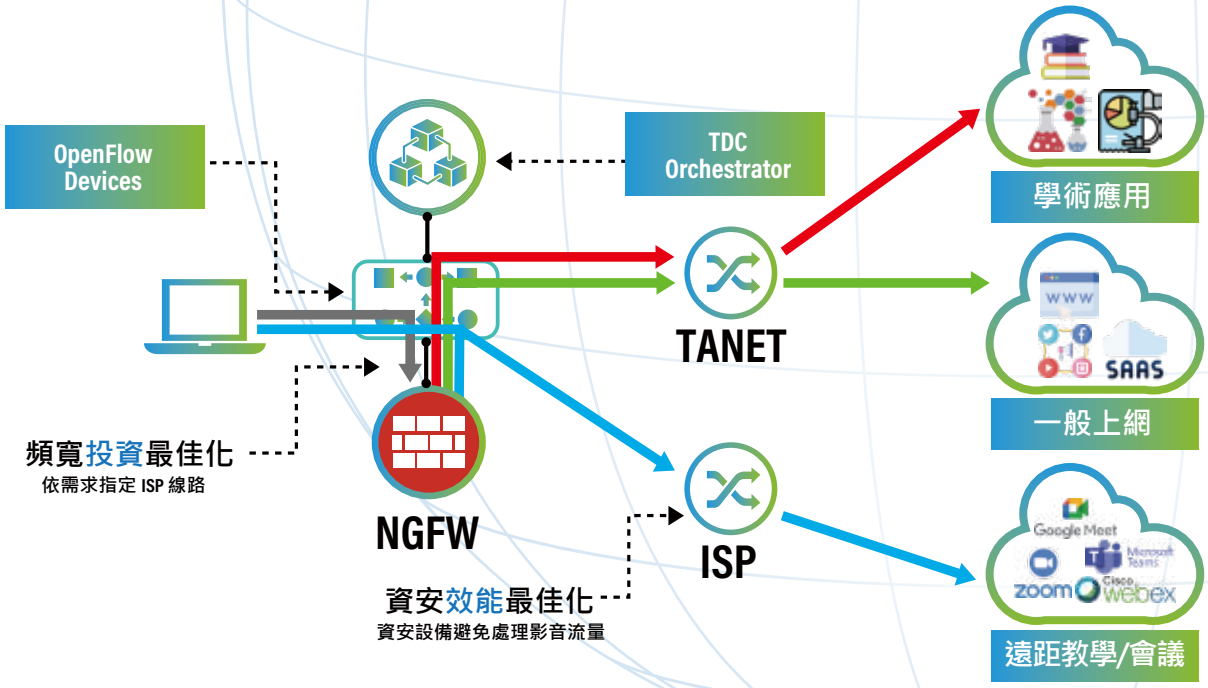
有別於傳統存取控制需要手動定義裝置元件，TDC Flow Guard 可藉由 OpenFlow Device自動學習並定位末端接入的裝置資訊，除了常見的IPv4+MAC 資訊綁定，更領先業界提供 **IPv6 +MAC 定位**能力，記錄位於OpenFlow的通訊，進而定位該裝置使用位置，有效解決政府、學校及電信等已投入大量IPv6應用場域的裝置定位及管控困擾。

上述應用場景亦可應用於智慧製造現場，管制各機台間東西向流量存取，當機台如需連線控制器或伺服器時，可導流至資安設備進行資安檢查，避免發生產線遭駭勒索等憾事。
最重要得是資料中心內的**虛實整合**服務間的**存取管控**，無論是實體與虛擬機間存取管控，或虛擬機與虛擬機存取管控，均可達成管理要求！



智慧分流領航員 — Smart Navigator

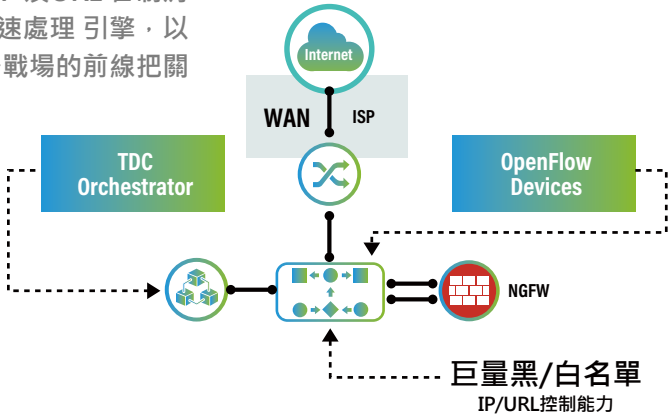
因疫情急遽升溫，導致各行各業大量採用遠距視訊雲端服務，作為教學/會議/辦公的新景 象，也帶來頻寬投資增加及資安檢測設備的負載加重現象，而資安設備負載變高的根源， 竟也是大量視訊流量湧入的無效處理! TDC Smart Navigator 依據 IP 及 URL 不同條件， 在無須改變現行網路架構情況下，以透通模式將指定流量重新導向至專用線路上網，例如: 教育學術相關流量即導向學術專用線路;可整合具備網路應用程式辨識之網路資安設備， 達成以應用服務分類進行導流，如:視訊相關網路應用可導流至一般等級線路，並繞過特定資安設備，以增進線路及資安設備投資效益。



巨量拒絕/信任名單 — Negative / Permit List

網路攻擊強度逐日提升，第一線存取控管顯得極為重要! 整合各方資安情資換得的管制清單量體已嚴重影響現行防火牆吞吐效率及清單管理難度。

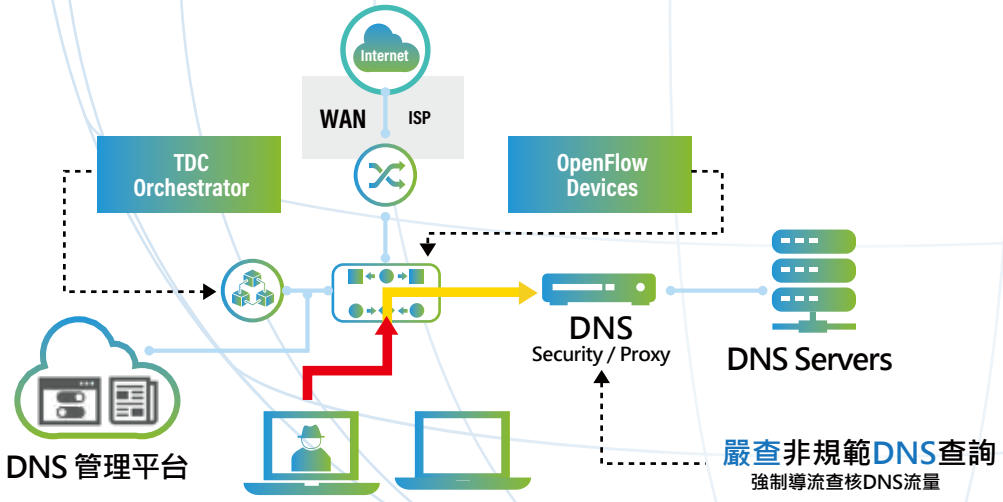
TDC Negative / Permit List 具備可處理 百萬筆 IP 及URL 管制清單能力，搭配OpenFlow Device 具備網路硬體加速處理 引擎，以近乎網路延遲的處理效能，協助 組織企業在網路戰場的前線把關網路威脅， 並有效緩解防火牆負載。



杜絕非規範DNS查詢流量 – DNS Broker

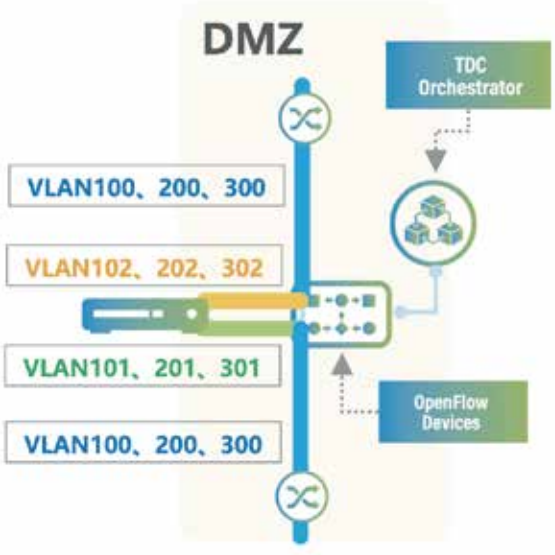
網路犯罪組織在內網發動一連串攻擊前，大多間諜程式先建立駭客中繼站報到作業，以取　得更多相關武器及工具，而建議駭客惡意中繼站連線的第一部，通常需先向 DNS 服務查 詢特定的網址，方可進行連線。組織企業建立 DNS 防護系統，以阻擋上述的惡意 DNS 資訊取;而駭客也非省油的燈，藉由指定特定的 DNS 服務主機 IP 地址，試圖繞過組織建 置的 DNS 防護系統。

TDC DNS Broker 以透通模式架構，將所有DNS查詢流量強制導向 DNS 防護設備，進而 杜絕任何使用非規範的DNS 查詢流量所衍生的攻擊入侵威脅。 TDC DNS Broker 提供友 善的 DNS 集中化管理平台，除提供多租戶管理架構(Multi-Tenancy)，可依據不同網域名稱建立階層式管理介面，並完善整合如:F5 Networks 等現今 DNS 防護產品大廠， 透過TDC DNS Broker 即可設定 DNS 相關設定至 DNS 防護產品，及查詢組織現有裝置 IP 地址 已遭受 DNS 資安威脅等，大幅提昇DNS 安全及管理效率。



VLAN ID 重新編譯 – VLAN Compiler

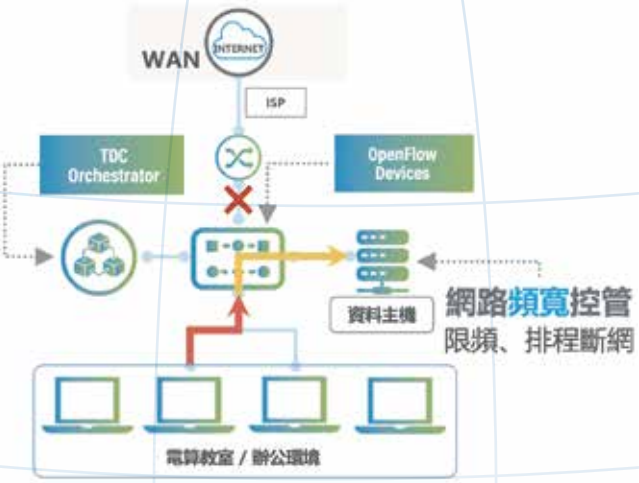
VLAN 劃分是最常見的網路區塊化管理中最基礎且 重要的技術，而我們發現越來越多的在特定應用場　景，需要彈性的動態調整網路流量原有的VLAN ID 配置，如:終端裝置存取控管及隔離、IEEE 802.1ad QinQ 網路封裝傳輸，或如 :F5　Networks　等特定網路設備架構介接需求...等。TDC VLAN Compiler 提供政策式管理機制，搭配採用透通架構模式的 OpenFlow Device 攔截網路流量，執行 VLAN ID 重新配置後，接續導流至特定目的地。



流量頻寬限制 — Rate limiting

網路頻寬管理議題已式微了嗎?其實應用 面向更廣泛了!除了以往網路頻寬控管因 頻寬費用昂貴因素，而最常見於 Internet 出口外，現今頻寬控管可能因管理實務、 資安政策等更多面向因素進行頻寬管控。 如教學現場的上課限制學生使用 Internet 頻寬電腦，及上機考試時需要進行排程中 斷Internet連線等管理需求。

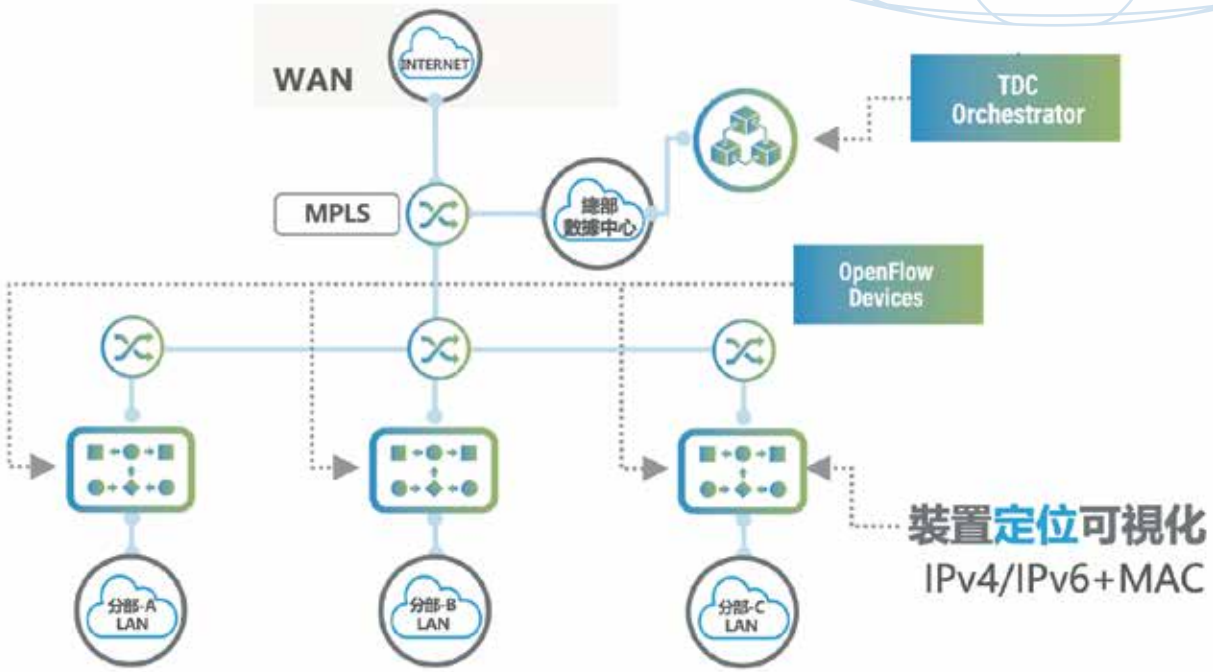
TDC Rate limiting 提供政策式管理機制， 搭配採用透通架構模式的 OpenFlow Device 直接管理網路頻寬，達成各種頻寬管制需求。



裝置定位可視化 — Device Positioning

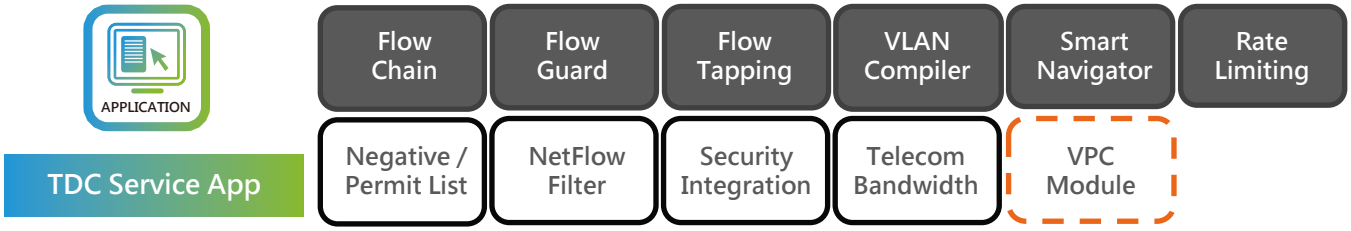
IT、IoT，甚至是OT裝置都已具備 IP 網路通訊能力，以往經常透過 DHCP 派發機制管理 裝置識別機制，最常見的莫過於 IPv4 + MAC 綁定管理了。但，因 IPv4 資源匱乏衍生的 IPv6 時代興起，連網裝置可視性變的非常困難，起因為連網裝置 IPv6 配發大多採用無狀 態配發機制，配發者不再是以往的DHCP 服務主機，取而代之的是核心網路路由器/核心 網路交換器執行 IPv6 配發角色，對於連網裝置辨識及管理變的相當困難!

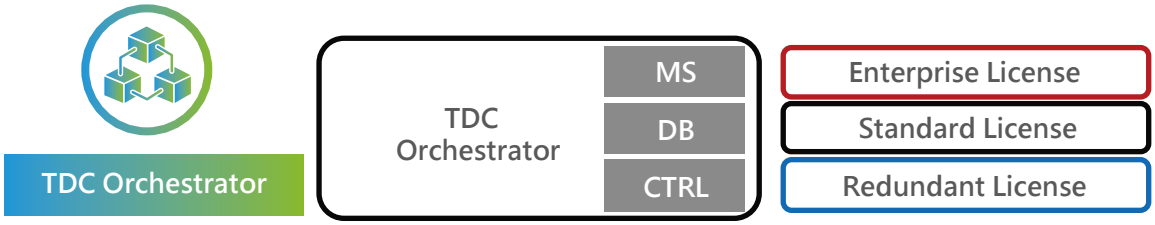
TDC Device Positioning 採用視覺化管理平台，並配置 OpenFlow Device 於連網裝置與 核心網路路由器/核心網路交換器間，以透通模式架構，辨識並建立網路流量中 IPv6/IPv4 地址與 MAC 地址之間關連性，可搭配 TDC Flow Guard 或 TDC Flow Chain 模組，以更 精準的連網裝置可視性能力達成各種流量管理需求。

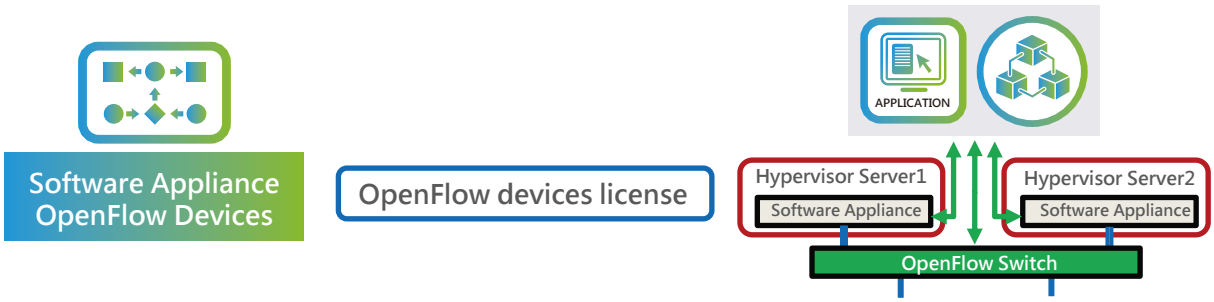


RDSecurer TDC Platform

RDSecurer TDC Platform 由三元素組成，分別是具備多樣化功能的 TDC Service APP，其次是 TDC Orchestrator集中化管理平台，採虛擬化平台設計，相容於現今主流虛擬化作業平台；亦可直接安裝於 Red Hat Linux 作業系統 。 TDC Orchestrator 負責將 TDC Service APP 套件功能所制訂的政策，配發至第三個元件OpenFlow Device。 OpenFlow Device 包含 OpenFlow Switch 及 TDC Virtual Software Appliance，適用於主流虛擬化作業平台環境，協助運行TDC 於虛擬化環境內的流量管理需求。







RDSecurer TDC Orchestrator 系統資源需求

VMware 平台軟硬體支援規格：

- 支援 vSphere 5.5 (含)以上版本
- 虛擬化環境數量： 3 x 虛擬化環境
- MS - CPU : 4Core, RAM : 16G, Disk : 40G
- DB - CPU : 4Core, RAM : 16G, Disk : 40G+200G
- CTL - CPU : 2Core, RAM : 8G, Disk : 40G

Ret Hat Linux 平台安裝硬體規格:

- 19吋標準機架式專用機型
- Intel® Xeon® 3.5GHz Series
- 64G RAM
- 500G(含)以上Disk
- 1G Ethernet port * 4

RDSecurer