RDsecurer

TDC
Virtual Private Cloud Controller

私有雲網路流量調度系統

DATA SHEET

企業邁向數位轉型成功時的巨大障礙–網路攻擊威脅

數位轉型浪潮之下，各行各業藉由提高數位技術運用達成營運目標，為尋求有效分享資料、運算力與應用服務等資源， 企業欲將傳統資料中心升級為私有雲需求也日益增加，打造具備分散式敏捷運算架構，並可輕鬆跨越地理位置共享重要數據能力等各類型數位應用需求，如雨後春筍般興起。
然而，當企業開始享有大量應用數位科技所帶來的成效與便利時，卻也需要正視其衍生而來更多引發網路攻擊威脅！

網路犯罪組織也嗅到全球數位化應用浪潮下的潛在可衍生鉅額犯罪收益，極力探勘各類營運系統、IoT裝置、網路設備，甚至是資安產品上的各種弱點，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企業組織，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，企業除了急須儘速完成各類重要系統弱點評估及修復的目標同時，更需考量為防範資安攻擊而產生非預期性系統漏洞修補升級，所衍生營運及服務停頓的增加隱性營運成本，將是另類的數位災害！

企業為抑制惡意威脅橫向感染發生，部署零信任網路存取管控機制（Zero Trust Networks Access, ZTNA）已然成為現今資安防護主流思維，企業組織在即有網路系統架構下大範圍部署該機制時卻面臨諸多挑戰，尤其是握有重要應用服務的私有雲服務！以虛擬化系統架構搭建的私有雲服務為企業數位資產的主要聚集地，但因為虛擬化平台種類繁多，且虛擬機之間的網路存取大多不設防，如虛擬機遭惡意威脅入侵後，恐造成快速感染至同一虛擬化平台內的其他虛擬機風險。

缺乏全盤管控機制

- 缺乏虛擬機之間存取控制
- 缺乏跨虛擬化主機之間管控
- 缺乏跨虛擬化平台之間管控

缺乏自動化安全通訊管道

- 跨資料中心通訊服務
- 跨租戶通訊傳輸機制

虛擬化防護成本高昂

- 虛擬存取控制成本高
- 跨虛擬化平台無整合

智慧且彈性的私有雲網路控制方案 – TDC Virtual Private Cloud Controller

TDC Virtual Private Cloud Controller 私有雲網路流量調度系統，提供企業自定義網路流量傳導架構，採用極具彈性的 OpenFlow 協議，透過自動化政策管理機制，打造橫跨多種類型虛擬化平台之網路橫向存取控制能力、動態建立跨資料中心專屬安全通道等之私有雲零信任網路存取架構，協助企業強化數位資產保護。

虛擬化系統橫向存取控制

虛擬化橫向存取控制可建置於常見虛擬化系統的網路環境，管理細緻度可達以單一虛擬化機為控管單位。虛擬化平台除可採用 NFV 網路功能虛擬化架構，整合常見的系統虛擬化平台外，針對特定系統虛擬化平台更可直接管理其 Open–vSwitch（OVS），兼具效能與管理便利性。

點對點隔離傳輸機制

TDC VPCC 採用 **OpenFlow 軟體定義網路**技術，將每個虛擬機建立隔離網路通訊架構，透過管理政策放行機制，放行虛擬機與虛擬機之間，或虛擬機與實體裝置之間的網路通訊，建立零信任網路存取控制結構。

階層式分權管理

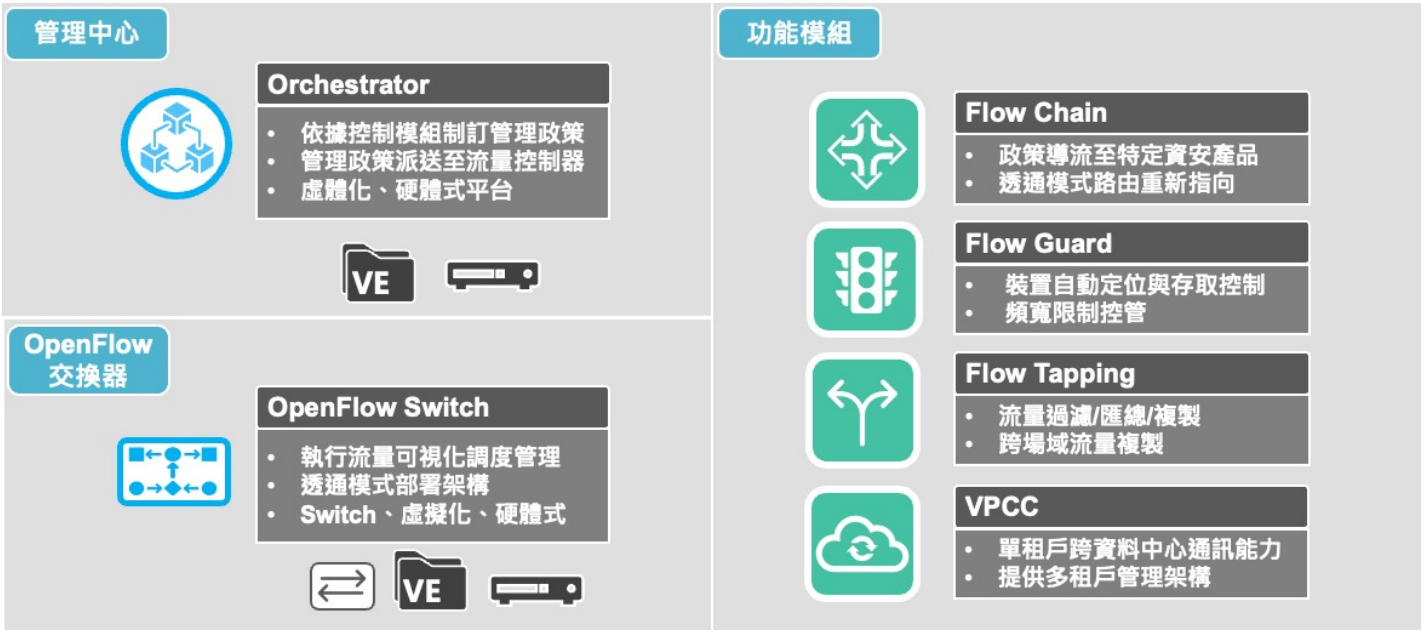
提供多租戶管理架構（Multitenancy），可依據不同虛擬化系統，不同實體主機，不同租戶或不同資料中心進行管理分權，達成管理分權目標。

強化進階威脅防護

提供網路流量再指向導流能力，可將 OpenFlow 交換器完成存取控制過濾後的流量，導流到具備進階資安防護能力的次世代防火牆專注於進階資安威脅防護任務。
亦可將特定流量複製到 ATP 或 NDR 進行網路流量行為辨識，滿足各類資安防護網路架構需由。

TDC Virtual Private Cloud Controller

TDC Virtual Private Cloud Controller由三元件組成，分別為**管理中心 (Orchestrator)** 提供單一集中管理介面，並搭配多樣化**功能模組（Service APP）**制定網路自定義管理政策，透過具備 OpenFlow 協定之虛擬化網路交換器(Open vSwitch, OVS)、虛擬化控制器 NFV 組成的 **OpenFlow 交換器**，達成客戶各種網路自定義流量管控需求。



	功能	說明
TDC VPCC	OpenFlow 協定支援	支援 OpenFlow Protocol Ver. 1.3.0，以建立Software define network 網路架構。
	虛擬化網路路由器	• 提供 Internet、MPLS VPN及資料中心網路交換器等各類線路與設備介接，Public IP 及 Private IP等通訊路由交換能力 • 提供 GRE Tunnel 功能，以利跨資料中心通訊存取
	獨立管理通訊埠	具備 Out-of-Band 網路管理架構，採用獨立管理通訊埠建立網路管理控制機制（control Plane），與資料傳遞流量（Data Plane）分離，避免管理通訊與資料傳替通訊間發生交互影響。
	Spine—Leaf 網路架構支援	OpenFlow Switch支援 Spine—Leaf 網路架構，當存在於不同 Leaf OpenFlow Switch下的兩台資訊裝置建立通訊時，需跨越 Spine 角色之OpenFlow Switch，以利控制與預測網路延遲與效能。
	系統虛擬化平台支援	• NFV支援：VMware vSphere ESXi, Microsoft Hyper-V • OVS支援：Citrix XenServer Hypervisor, KVM
	網路連接埠高可用及裝置橫向擴充	因應不同 OpenFlow Switch廠商支援LACP、LAG、MLAG、Device Stacking 等多種網路通訊高可用架構及裝置虛擬化橫向擴充能力
管理中心	加密圖形化管理介面	具備 TLS V1.3 之 SSL 圖形化加密網頁管理介面
	網路流量統計顯示	即時顯示已納管之 OpenFlow Switch流量資訊，可依據其獨立通訊埠流量得知實體或虛擬化資訊系統之網路通訊流量現況，並可依據查詢結果會出相關資訊
	集中化網路管理能力	可於單一管理介面納管大量 OpenFlow Switch，設定並派送網路存取控制（ACL）政策至 OpenFlow Switch
	多租戶管理分權架構	具備多租戶階層式存取控制管理架構，系統管理員可依據不同服務或區域配置獨立管理介面，各分權管理介面可獨立設定存取控制及網路配置等相關設定
	分權管理機制	具備多種帳號分權管理群組，系統管理者可依據不同的管理帳號及群組對象套用特定管理權限
	管理稽核記錄	提供管理帳號登入管理稽核事件記錄、查詢及匯出功能
	設定檔管理	具備管理設定檔備份及還原等管理功能
	告警發送	具備 SNMP-Trap, E-Mail, Syslog 等多種類型告警發送機制
	API 支援	提供管理用通訊介面RESTful API 整合外部管理系統，以利自動化管理
	管理系統高可用架構	具備系統高可用架構，以達成服務不中斷目標： • 管理系統：提供 High-Availability (HA) 高可用架構，並提供專屬Virtual-IP 作為統一管理 IP 位址 • 資料庫：提供 High-Availability (HA) 高可用架構，並提供專屬Virtual-IP 作為統一管理 IP 位址 • OpenFlow 控制器：提供 N+1 橫向擴充高可用架構，具備 Active-Active 高可用架構，單一台 OpenFlow 控制器可管理 30台（含）以上之 OpenFlow Switch
	平台安裝支援	虛擬化平台： • VMware vSphere Ver.5.5 （含）以上、Microsoft Hyper-V 2016 以上 • 管理系統：CPU：4x Core, RAM：16GB, Disk：40GB • 資料庫：CPU：4x Core, RAM：16GB, Disk：40GB+200GB • OpenFlow 控制器：CPU：2Core, RAM：8GB, Disk：40GB • * 上述為最低硬體效能

	功能	說明
網路存取控制功能	網路自動定位	透過OpenFlow Switch自動辨識並記錄網路流量上 IPv4/IPv6 + MAC 地址配對。
	實體資訊系統存取控制	採用具備 OpenFlow 協定之網路實體交換器進行網路存取控制，可依據 OSI Layer1 ~Layer4 的各種不同條件定義專屬存取控制政策，例如：實體通訊埠、Ethertype、來源/目的地 IP 位址/網路區段，IP Protocol、來源/目的地 TCP 通訊埠、來源/目的地 UDP 通訊埠作為存取控制條件。
	虛擬化資訊系統存取控制	• 架構1：採用具備OpenFlow 協定之網路虛擬化交換器進行網路存取控制，可依據 OSI Layer2 ~Layer4 的各種不同條件定義專屬存取控制政策，例如：Ethertype、來源/目的地 IP Address，IP Protocol、來源/目的地 TCP Port Number 、來源/目的地 UDP Port Number 作為存取控制條件，制定阻擋（Deny）或允許(Allow) 等管理政策。 • 架構2：將單一系統虛擬化平台內的各虛擬化系統間網路通訊流量，強制導流至與系統虛擬化平台網路實體連接埠介接之具備 OpenFlow 協定之網路實體交換器進行網路存取控制，再依據 OSI Layer2 ~Layer4 的各種不同條件定義專屬存取控制政策，例如：Ethertype、來源/目的地 IP Address，IP Protocol、來源/目的地 TCP Port Number 、來源/目的地 UDP Port Number 作為存取控制條件，制定阻擋（Deny）或允許(Allow) 等管理政策。 • 在尚未設定任何存取控制政策前，預設單一系統虛擬化平台內的各台虛擬機網路通訊均為隔離狀態，即使使用相同 IP 網段與路由設定，均不影響網路通訊運作。 • 跨資料中心存取控制設定，如遇兩資料中心之虛擬化系統發生相同 Private IP 狀況時，可透過SNAT機制完成兩資料中心間之虛擬化系統通訊。
	存取控制網路通訊協定支援	• 符合 RFC791 之 IPv4 標準規範之存取控制能力，子網路遮照管控之最小網路位元組為30 （子網路遮照：255.255.255.252），最大網路位元組為8 （子網路遮照：255.0.0.0） • 符合 RFC1918之 IPv4 標準虛擬化網段規範之存取控制能力，子網路遮照管控之最小網路位元組為30 （子網路遮照：255.255.255.252），最大網路位元組為8 （子網路遮照：255.0.0.0） • 符合 RFC2460 之 IPv6 標準規範之存取控制能力，最大字首度為為/64 （2001:db8:abcd:0012::0/64）
	特定網路服務導流支援	依據管理政策獨立開通並導流常用通訊協定服務之指定 IP 地址網路通訊 • DNS • DHCP • NTP • Internet Gateway，如來源 IP 為 Private IP，則依據管理政策配置 SNAT 功能

	功能	說明
RESTful API	存取控制政策設定	制定 IPv4 存取政策，包含存取管理政策之新增/修改/刪除等功能，OSI Layer2 ~Layer4 的各種不同條件定義專屬存取控制政策，例如：Ethertype、來源/目的地 IP Address，IP Protocol、來源/目的地 TCP Port Number 、來源/目的地 UDP Port Number 作為存取控制條件，制定阻擋（Deny) 或允許(Allow) 等管理政策。
	路由設定	路由政策設定管理
	NAT設定	NAT政策設定管理
	用戶端總表	查詢現有實體或虛擬化用戶端列表
	單一存取控制用戶端 IPv4 細項資訊	查詢已設定存取控制管理政策之用戶端 IPv4 網段之分配狀態，顯示已配置及未使用之 IPv4 IP 地址
	單一存取控制用戶端 IPv6 細項資訊	查詢已設定存取控制管理政策之用戶端 IPv6 網段之分配狀態，顯示已配置及未使用之 IPv6 IP 地址
	單一存取控制用戶端路由生效資訊	查詢已設定存取控制管理政策之用戶端之路由設定已生效資訊
	單一存取控制用戶端NAT生效資訊	查詢已設定存取控制管理政策之用戶端之 IP 轉址設定（NAT）設定已生效資訊
	用戶套用存取控制政策列表	查詢已設定存取控制管理政策之實體或虛擬化用戶端列表
	用戶套用 Public IP 列表	查詢已設定存取控制管理政策之實體或虛擬化用戶端 Public IP 使用對照列表
	OpenFlow Switch列表	查詢納管之實體及虛擬化 OpenFlow Switch列表名稱資訊
	OpenFlow Switch網路介面資訊	查詢納管之單一實體及虛擬化 OpenFlow Switch網路通訊埠介面傳輸資訊，包含封包數（Packet TX/RX）及流量（Byte TX/RX）等資訊