VMWARE NSX

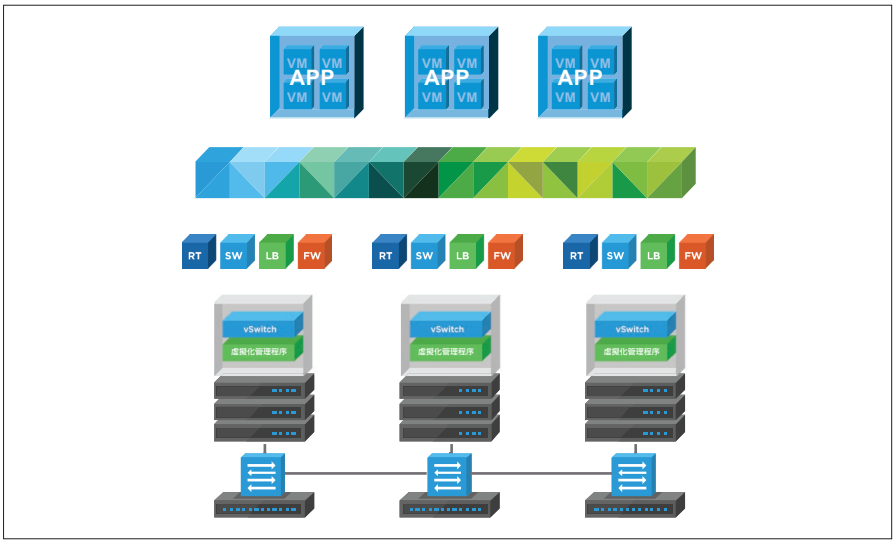
網路虛擬化及安全平台

概觀

VMware NSX® 是專為軟體定義的資料中心所打造的網路虛擬化及安全平台，提供整個網路的虛擬機運作模式。在 NSX 上，包括交換、路由與防火牆保護在內的網路功能都內嵌在虛擬化管理程序裡，並分散在環境中。這個模式有效地建立了「網路虛擬化管理程序」，可以做為虛擬網路與安全服務的平台。虛擬網路和虛擬機運作模式類似，會透過程式完成佈建與管理，且不受底層的網路硬體限制。NSX 以軟體重建整個網路模型，而能夠在幾秒之內建立和佈建任何網路拓撲，包括從簡單到複雜的多層級網路。使用者可以利用透過 NSX 提供的服務組合，建立具有不同需求的多個虛擬網路，以創造本質上更安全的環境。

主要優點

- 為個別的工作負載提供微分段與精密的安全性
- 網路佈建時間從數天減少至數秒，以及透過自動化改善營運效率
- 不受實體網路拓撲限制，在資料中心之間或內部都享有工作負載行動化
- 透過領先業界的協力廠商商業網路，提供強化安全性與進階網路服務



網路虛擬化、安全性與軟體定義的資料中心

VMware NSX 為網路提供全新的運作模式，網路再進而形成軟體定義的資料中心的基礎。因為 NSX 以軟體建立網路，資料中心操作員可以達到過去實體網路無法達到的靈活性、安全性與經濟效益程度。NSX 提供一套完整的邏輯網路元件與服務，包含邏輯交換、路由、防火牆保護、負載平衡、VPN、服務品質 (QoS) 與監控。任何運用 NSX API 的雲端管理平台都可以在虛擬網路中提供這些服務。虛擬網路在任何現有網路硬體上進行部署時都不需要中斷。

NSX 的重要功能

交換	能夠在資料中心之內或之間的路由 (L3) 結構上建立邏輯的第 2 層層疊延伸。支援 VXLAN 的網路層疊。
路由	在虛擬化管理程序核心中，以分散形式執行的虛擬網路之間的動態路由，可以透過使用實體路由的主動-主動式容錯移轉做到水平擴充。支援靜態路由與動態路由 (OSPF、BGP) 協定。
分散式防火牆保護	內嵌於虛擬化管理程序核心的分散式具連線狀態防火牆保護，每個虛擬化管理程序主機能提供高達 20 Gbps 的防火牆承載量。支援 Active Directory 與活動監控。此外，NSX 也可以透過 NSX Edge™ 提供南北向的防火牆承載量。
負載平衡	L4–L7 負載平衡器，附加 SSL 降低工作負載與直通功能、伺服器運作狀況檢查功能，並有應用程式規則提供可程式性和流量操控性。

VPN	站點對站點與遠端存取的 VPN 功能，並針對雲端閘道服務提供未受管理的 VPN。
NSX 閘道	支援 VXLAN 對 VLAN 的橋接，可緊密地連接到實體的工作負載。此功能是 NSX 的原生功能，同時也可藉由商業網路合作夥伴的機架頂端交換器來提供。
NSX API	RESTful API 提供的整合性能夠連接到任何雲端管理平台或自訂自動化作業。
作業	原生的作業功能，例如中央指令行介面 (CLI)、traceflow、SPAN 與 IPFIX 可排除問題並主動監控基礎架構。與 VMware vRealize® Operations™ 和 vRealize Log Insight™ 等工具整合，提供進階分析與疑難排解。 NSX Application Rule Manager 和端點監控可提供最多到第 7 層的端對端網路流量視覺化，應用程式團隊能夠用來辨識資料中心內部和資料中心之間的端點，進而建立適當的安全規則來進行回應。
情境感知的微分段技術	NSX 能讓您依據 IP 位址與 MAC 位址以外的更多因素（包括 VMware vCenter™ 物件與標籤、作業系統類型與第 7 層應用程式資訊）建立動態安全性群組及相關聯原則，以利在應用程式情境中進行微分段作業。 透過來自虛擬機、Active Directory 與行動裝置管理整合的登入資訊所建立的身分識別原則，可方便建立個別使用者的安全性，包括遠端與虛擬桌面環境中的工作階段層級安全性。
雲端管理	與 vRealize Automation™ 以及 OpenStack 原生整合。
與協力廠商合作夥伴整合	支援協力廠商合作夥伴多種類別產品與管理、控制平台和資料轉發平台之間的整合，這些產品類別包括新一代防火牆、IDS/IPS、無代理程式的防毒保護、應用程式交付控制器、交換、作業與能見度、進階安全性等等。
跨 vCenter 網路與安全性	不受底層實體網路拓撲限制，跨越 vCenter 與資料中心界限延伸網路與安全性，提供災難復原與主動-主動式資料中心等功能。
日誌記錄管理	利用 vRealize Log Insight for NSX 提供的額外能見度，協助更快速地解決問題。具體呈現事件趨勢、觸發警示等等，這些全都能夠即時進行。

使用情境

安全性

NSX 使組織能以邏輯的方式將資料中心分為不同的安全性區段，可細分到個別的工作負載，且不受工作負載的網路子網路或虛擬區域網路 (VLAN) 限制。於是 IT 團隊可以根據動態的安全性群組，針對每個工作負載定義安全性原則與控管，而工作負載可確保針對資料中心內的威脅做出即時反應，並針對個別的虛擬機執行。與傳統網路不同，如果攻擊者穿越資料中心的周邊防禦，威脅並不能在資料中心中水平移動。

自動化

NSX 透過將勞力密集、容易出錯的工作自動化，解決了冗長的網路佈建、組態設定錯誤和代價高昂的處理程序所帶來的難題。NSX 以軟體建立網路，排除了以硬體為基礎的網路所造成的瓶頸。

NSX 與 vRealize Automation 或 OpenStack 等雲端管理平台的原生整合，可促成更進一步的自動化。

應用程式延續性

因為 NSX 將網路從底層硬體抽離，網路與安全性原則就附加在其相關的工作負載上。組織可以輕易的將整個應用程式環境複寫到遠端的資料中心做為災難復原的準備，在企業資料中心之間移動，或是將其部署到混合雲環境中。所有動作都能在幾分鐘內完成，完全不需要中斷應用程式，而且完全不需要觸碰實體網路。

VMware NSX 版本

Standard

專為需要網路靈活性與自動化的企業組織提供

Advanced

適用於除了 Standard 版本功能外，亦需要以微分段達成本質更安全的資料中心之企業組織

Enterprise

專為除了 Advanced 版本功能外，亦需要跨多網域的網路與安全性功能的企業組織提供

ROBO

適用於希望在遠端辦公室或分公司虛擬化應用程式並提供安全保障的企業組織

進一步瞭解

如需詳細資訊，請造訪 http://www.vmware.com/tw/products/nsx/。

有關 NSX 授權版本功能的其他詳細內容，請參閱 https://kb.vmware.com/kb/2145269。

若要取得其他資訊或購買 VMware 產品，請致電 +886-2-8758-2804、造訪 www.vmware.com/tw/products，或線上搜尋授權經銷商。

	STANDARD	ADVANCED	ENTERPRISE	ROBO
分散式交換	•	•	•	•*
分散式路由	•	•	•	
NSX Edge 防火牆	•	•	•	•
NAT	•	•	•	•
軟體 L2 橋接到實體環境	•	•	•	
透過 ECMP（主動-主動）的動態路由	•	•	•	•
API 驅動的自動化	•	•	•	•
與 vRealize 和 OpenStack 整合	•	•	•	•
利用 vRealize Log Insight for NSX 實現日誌記錄管理	•	•	•	•
透過 vRealize 提供安全性原則自動化		•	•	•
NSX Edge 負載平衡		•	•	•
分散式防火牆保護（包括與 Active Directory 的整合）		•	•	•
伺服器活動監控		•	•	•
服務增強（與協力廠商整合）		•	•	•
與 VMware AirWatch® 整合		•	•	•
Application Rule Manager		•	•	•
跨 vCenter NSX			•	
多站點 NSX 最佳化			•	
VPN（IPSEC 與 SSL）			•	•
遠端閘道			•	
與硬體 VTEP 整合			•	
端點監控			•	
第 7 層分散式防火牆保護			•	

*VLAN 支援

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
台北市 110 信義路五段七號台北 101 大樓 57 樓 C 室 電話 +886-2-8758-2804 傳真 +886-2-8758-2708 www.vmware.com/tw
Copyright © 2018 VMware, Inc. 版權所有。本產品係受美國及國際之版權及智慧財產權相關法律保護。VMware 產品係受 http://www.vmware.com/tw/download/patents.html 上所列之一或多項專利的保護。VMware 係 VMware, Inc. 及其子公司在美國和其他管轄區域的註冊商標或商標。此處所提及的所有其他標誌和名稱，可能分別為其相關公司的商標。文件編號：117478wf-vmw-fy18q4-sddc-launch-ds-nsx-a4 1/18