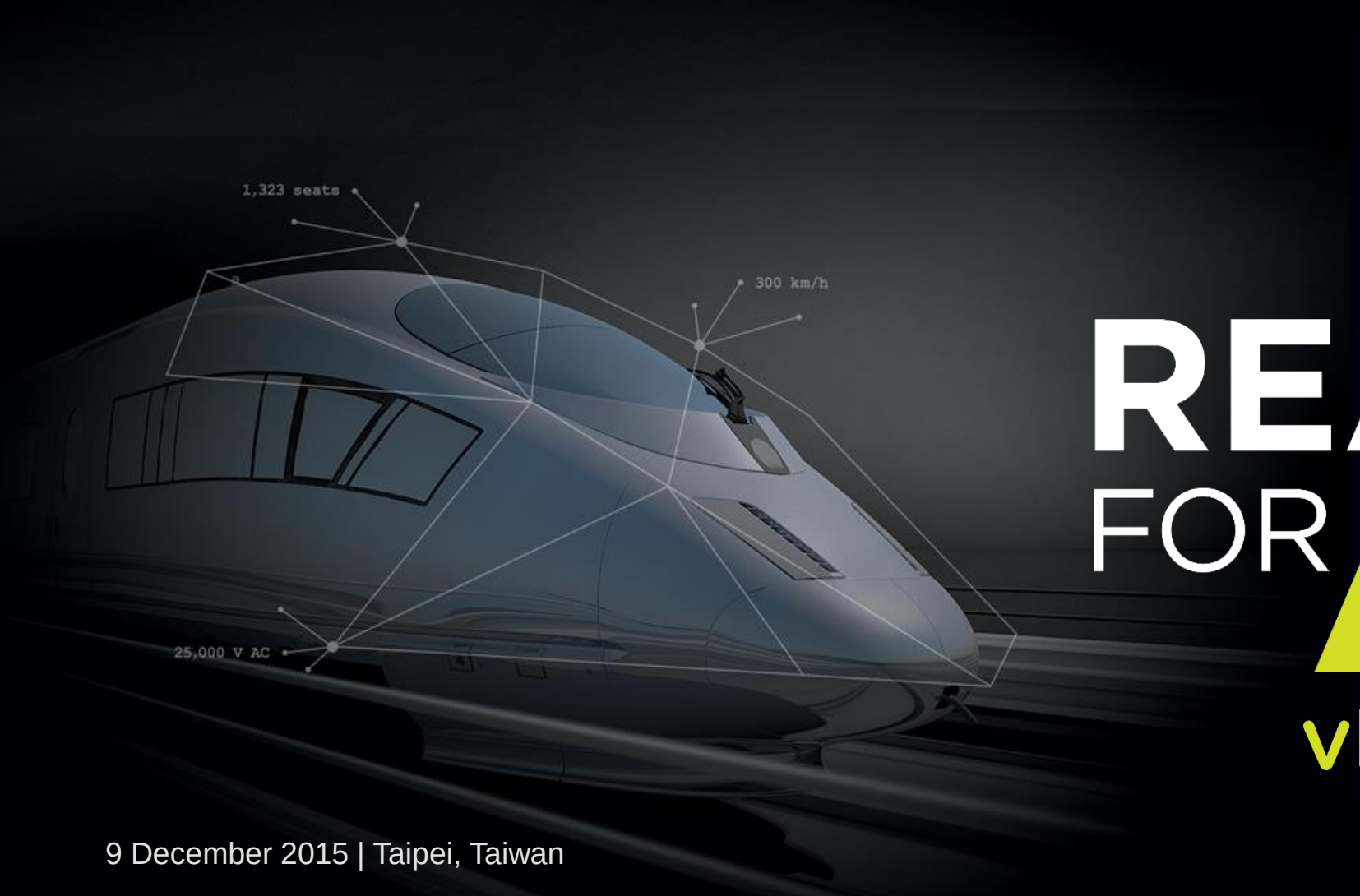


vmware

READY FOR ANY

vForum2015

9 December 2015 | Taipei, Taiwan

長庚大學邁向軟體定義資料中心經驗分享

張永華
資訊中心主任

Agenda

- 長庚大學簡介
- 計畫緣由
- 導入範圍
- 功能驗證
- 未來發展

長庚大學簡介

- 概況 http://www.cgu.edu.tw
  - 地址：桃園市龜山區文化一路259號（鄰近機場捷運A7站）
  - 學生人數：~7000；教職員人數：~1500；生師比：12:1
  - 教學單位：醫學院、工學院、管理學院、通識中心
    - 25+獨立系所、10+研究中心；資訊中心：11人(教服、軟體、網路)
- 資訊系統建置
  - SSO(2014)、DHCP (2015)、行動化ERP (2015)
  - 伺服器虛擬化(2010)、儲存虛擬化(2015)、雲端電腦教室(2015)
  - 虛擬化軟體全校授權(2016)、虛擬平台備份(2016)

長庚大學簡介 – 虛擬化環境現況

軟體

項目	版本	用途
VMware vSphere	- 6.0 / 5.5	校園資訊網站、校務資訊系統、郵件系統、智慧學習系統等數十個關鍵應用系統虛擬化平台主機
vCenter Server	- 6.0 / 5.5	中控管理主機，管理目前所有虛擬化主機

硬體

項目	規格	數量
- VMware ESXi Server	- Intel Xeon E5 -2600 CPU x 2 - 256 GB之記憶體(8台)、128 GB之記憶體(3台)、64GB (3台) - 6 埠 1 GB網卡	- 14台
- 主機端 網路交換器	- Cisco、Brocade L2 Switch	- 4台

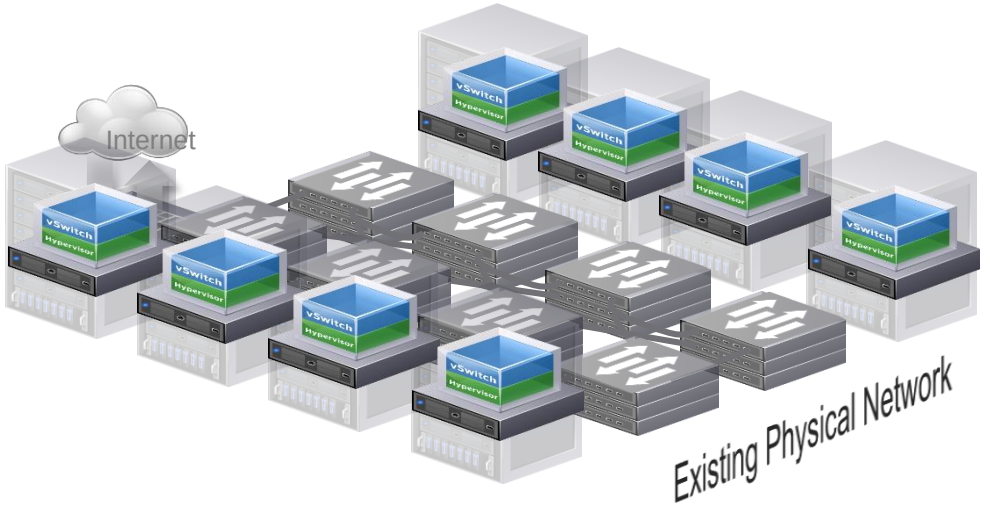
Agenda

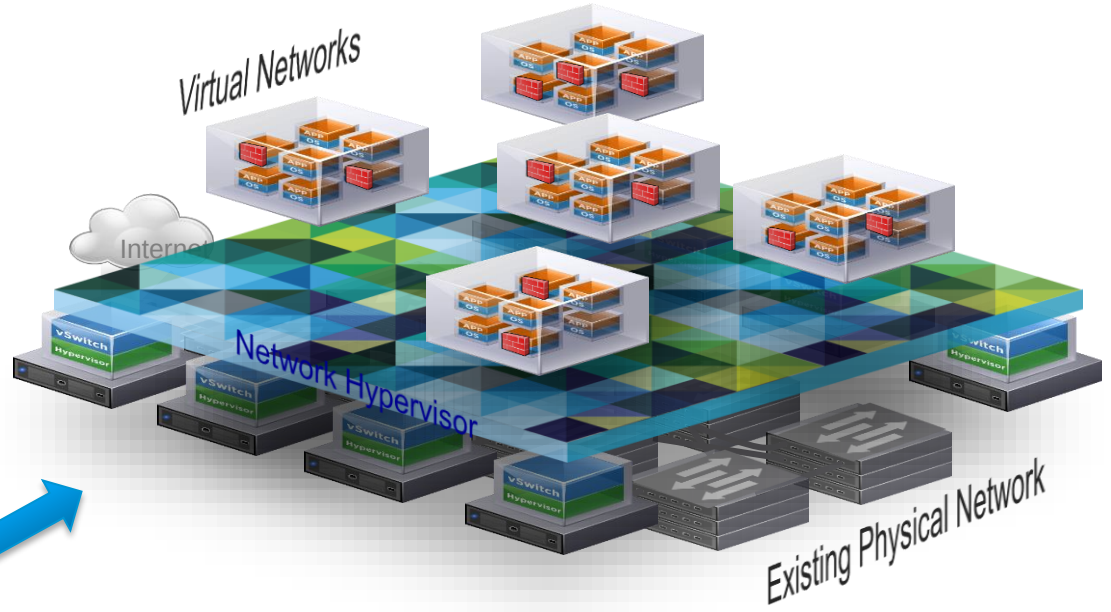
- 長庚大學簡介
- 計畫緣由
- 導入範圍
- 功能驗證
- 未來發展

計畫緣由 – 標準(虛擬)化IT資源 → 軟體定義資料中心

主機與儲存虛擬化

- 資源池
- 穩定且高速的底層環境
- 不受限於廠牌





軟體定義

- 服務導向
- 自動化快速佈署
- 靈活組態變更

vmware

麟瑞科技 RING LINE CORPORATION

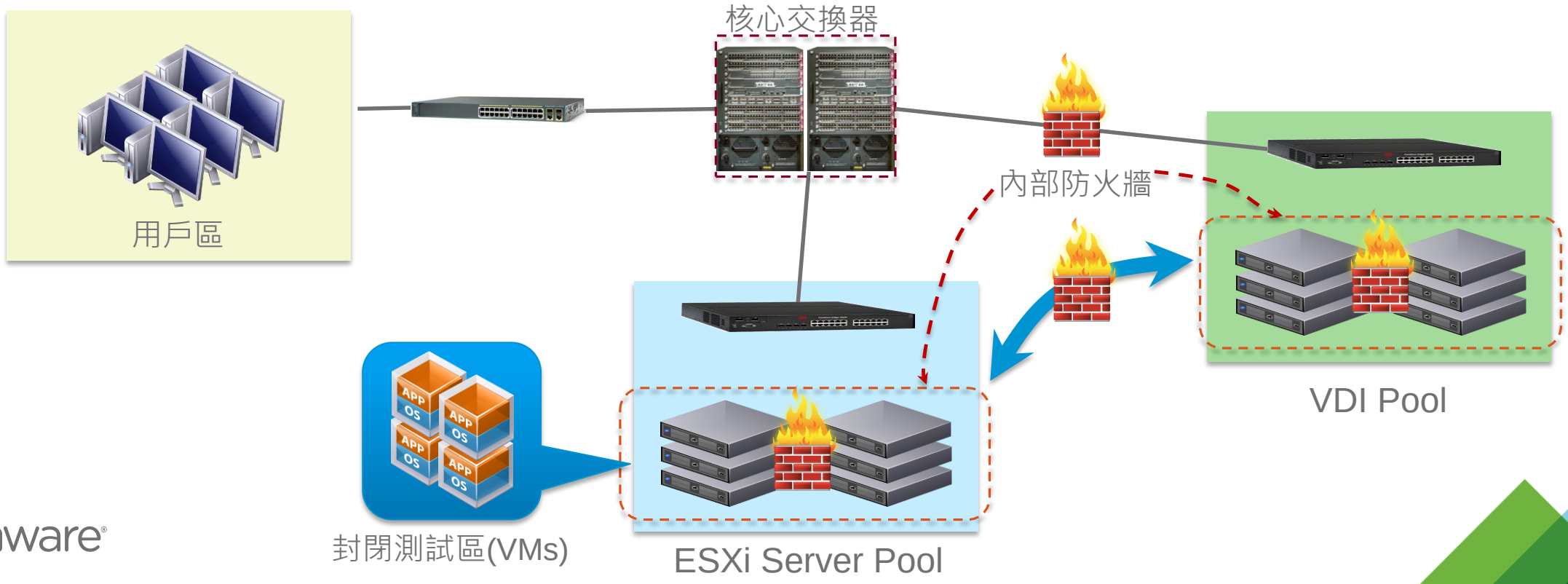
計畫緣由 – 因應資安政策需求

Agenda

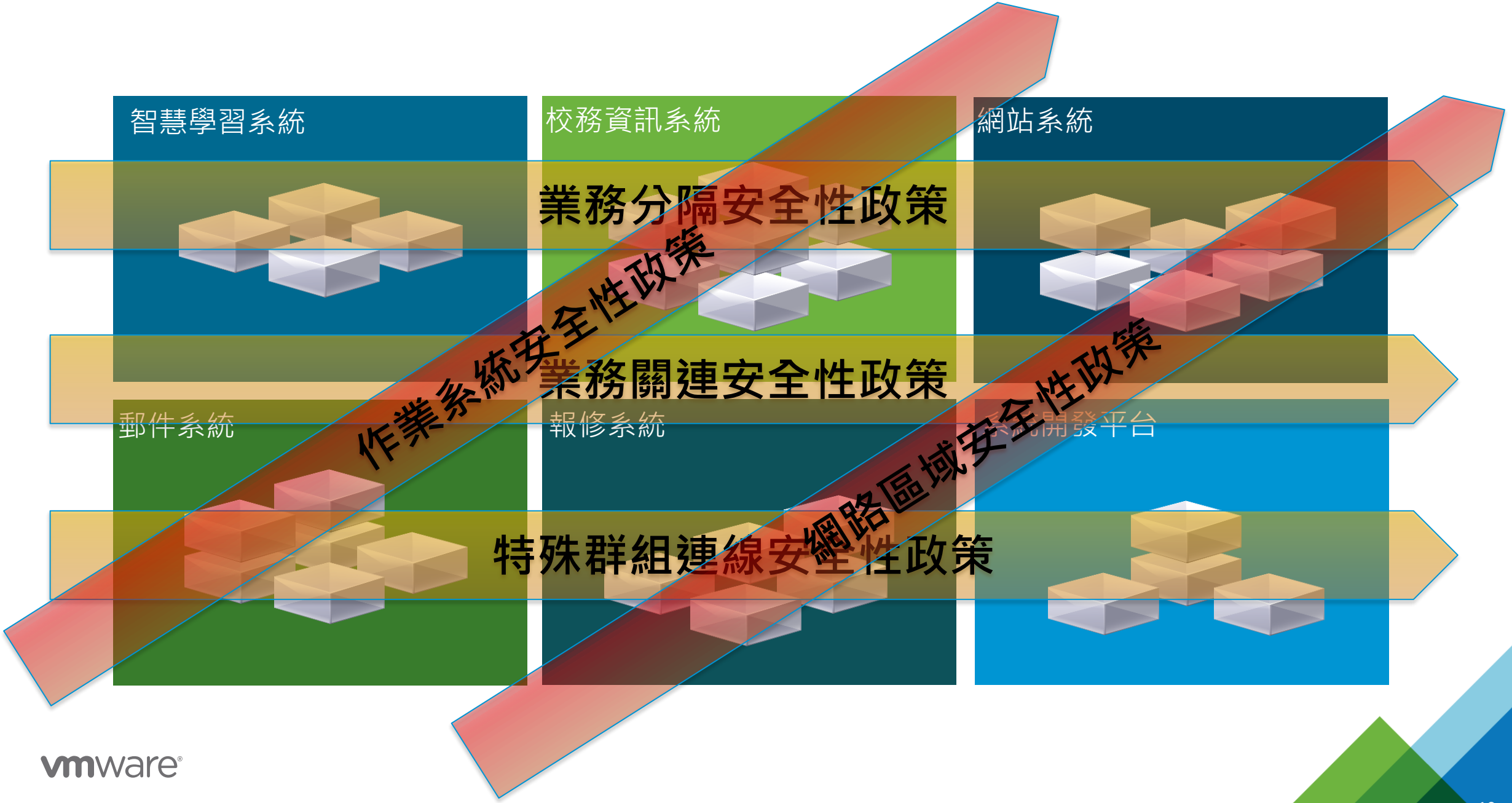
- 長庚大學簡介
- 計畫緣由
- 導入範圍
- 功能驗證
- 未來發展

導入範圍 – 強化虛擬機器安全政策

- 改變傳統按使用年限汰換防火牆設備方式，逐步建立軟體定義資料中心。
- 強化虛擬機器資安管控政策，建立零信任分區。
- 建立虛擬沙箱測試環境，提供業務系統漏洞修補、開發測試之獨立區域。



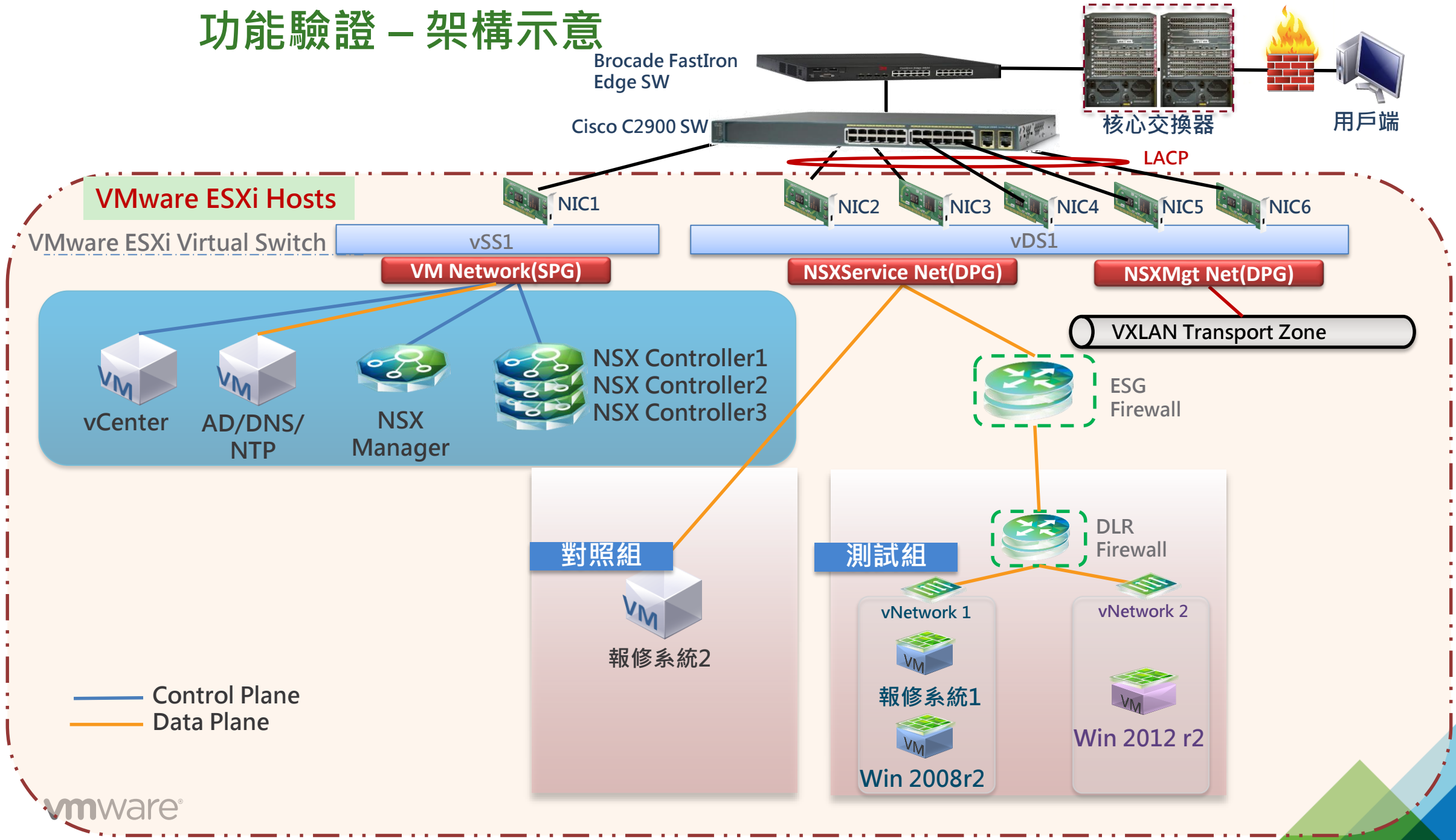
導入範圍 – 強化虛擬機器安全政策



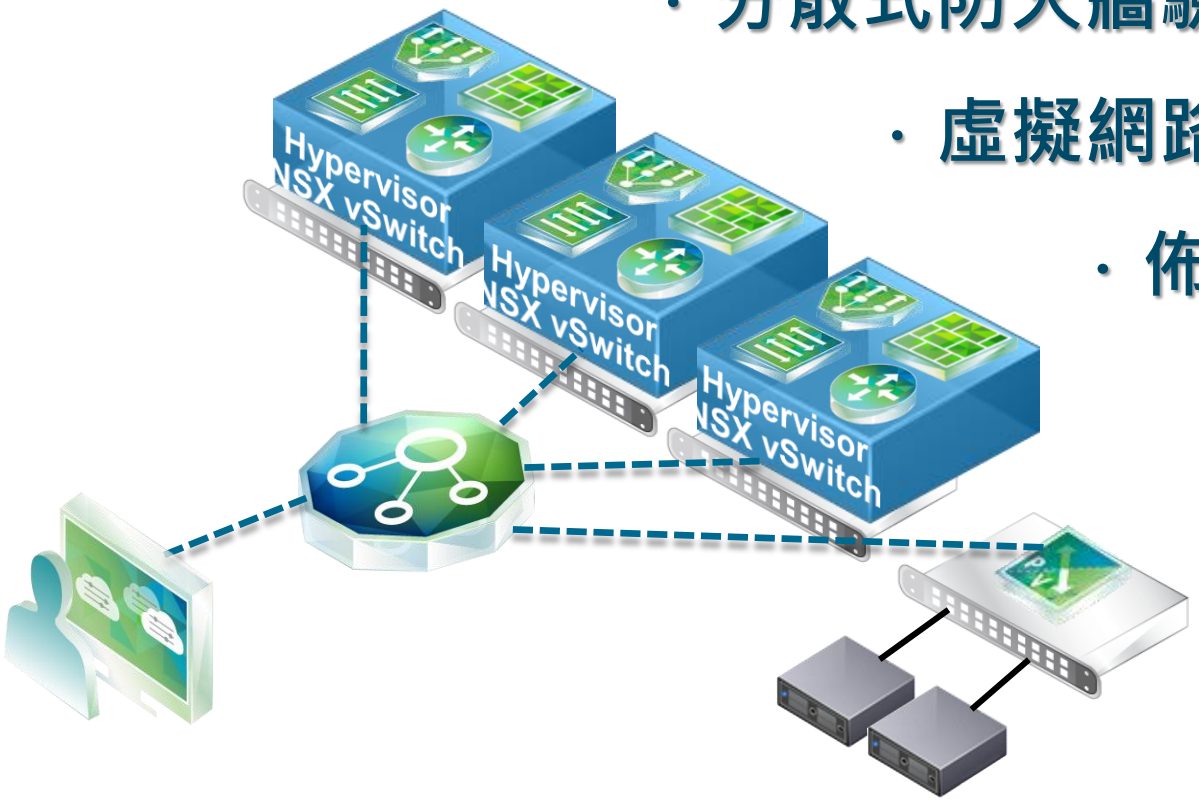
Agenda

- 長庚大學簡介
- 計畫緣由
- 導入範圍
- 功能驗證
- 未來發展

功能驗證 – 架構示意


Brocade FastIron
Edge SW
Cisco C2900 SW
核心交換器
用戶端
LACP
VMware ESXi Hosts
NIC1
NIC2
NIC3
NIC4
NIC5
NIC6
VMware ESXi Virtual Switch
vSS1
vDS1
VM Network(SPG)
NSXService Net(DPG)
NSXMgt Net(DPG)
VXLAN Transport Zone
vCenter
AD/DNS/
NTP
NSX
Manager
NSX Controller1
NSX Controller2
NSX Controller3
ESG
Firewall
DLR
Firewall
對照組
報修系統2
測試組
vNetwork 1
vNetwork 2
報修系統1
Win 2008r2
Win 2012 r2
Control Plane
Data Plane

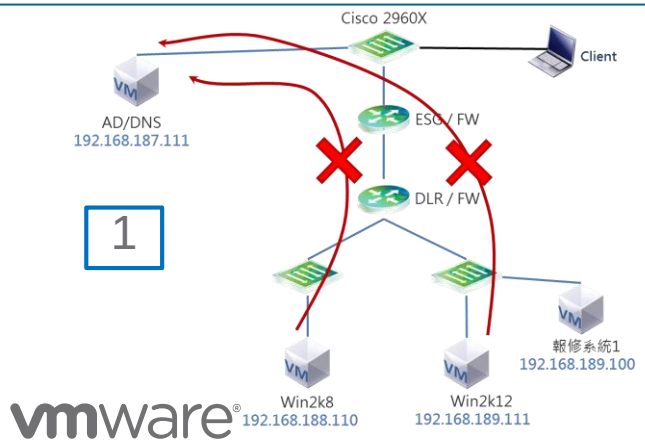
功能驗證 – 驗證項目

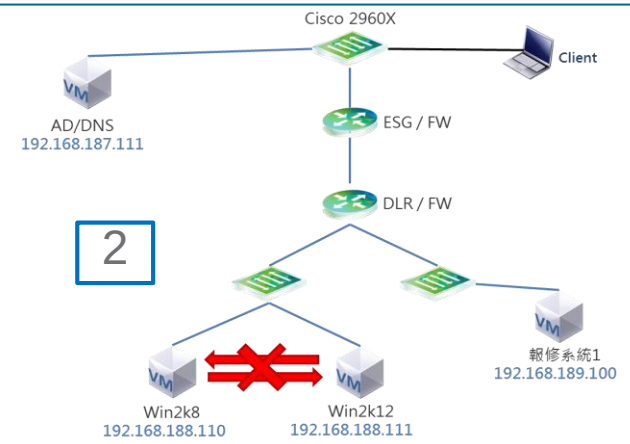


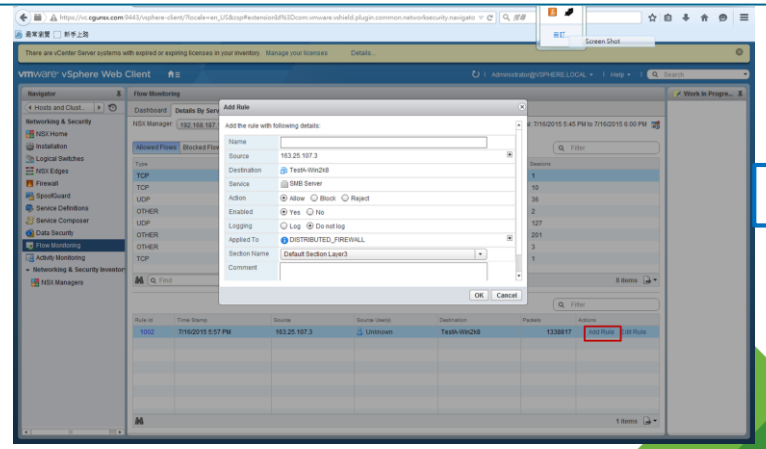
- 分散式防火牆驗證 (為符合服務安全規範)
- 虛擬網路效能驗證
- 佈署與管理驗證

功能驗證 – 防火牆驗證項目與情境

項次	測試項目	測試內容	結果
1	邊界防火牆	· 過濾拒絕或允許特定來源、目的、協定溝通及LOG。 · 政策物件：小至虛擬機器，大至資料中心。 · 可於Edge Service Gateway(ESG)及Distributed Logical Router(DLR)建立防火牆政策。 · 支援Routed、NAT模式。 · 支援靜、動態路由。	■ Yes □ No
2	分散式防火牆	· 過濾拒絕或允許特定來源、目的、協定溝通及LOG。 · 政策物件：小至虛擬網路卡，大至資料中心。	■ Yes □ No
3	Micro-Segmentation(微分割)	· 過濾拒絕或允許同或不同網段虛擬機器特定協定溝通。 · 政策物件：小至虛擬網路卡，大至資料中心。 · 支援動態安全群組，可建立過濾條件，新建虛擬機可直接自動套用至政策。	■ Yes □ No
4	FLOW Monitor	· FLOW監控排名。 · 可由FLOW排名中直接新增防火牆政策	■ Yes □ No



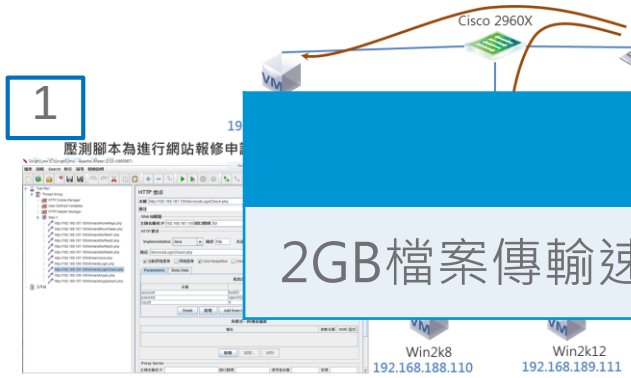




功能驗證 – 虛擬網路傳輸效能

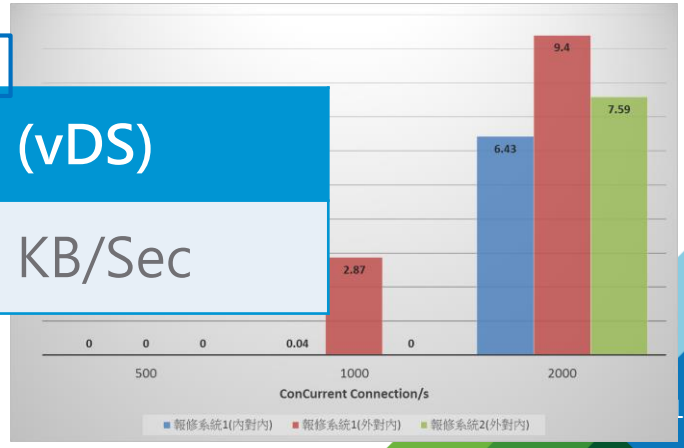
項次	測試項目	測試內容	結果	備註
1	連線數量 壓力測試	· 透過使用Badboy腳本工具及Jmeter壓測工具進行連線壓力測試。 · 模擬Internal LAN用戶端連線至NSX DLR之下之虛擬服務機器。(Internal → NSX Logical LAN) · 模擬NSX DLR一用戶端連線至另一個Virtual Disturbed Switch之下之虛擬服務機器。(Internal → vSphere Virtual LAN)	■ Yes □ No	1000/2000 ConCurrent Connection
2	資料傳輸量 壓力測試	· 透過使用網路芳鄰傳輸大容量檔案。 · 模擬Internal LAN用戶端傳輸檔案至NSX DLR之下之虛擬服務機器。(Internal -> NSX Logical LAN) · 模擬NSX DLR一用戶端傳輸檔案至另一個Virtual Disturbed Switch之下之虛擬服務機器。(Internal → vSphere Virtual LAN)	■ Yes □ No	2GB傳輸檔案
3	高可用性測試	· 檔案傳輸中及ICMP回應狀態，進行ESG、DLR 單一節點模擬故障。 · 節點切換後，檔案持續傳輸，ICMP持續回應。	■ Yes □ No	

1



2

3



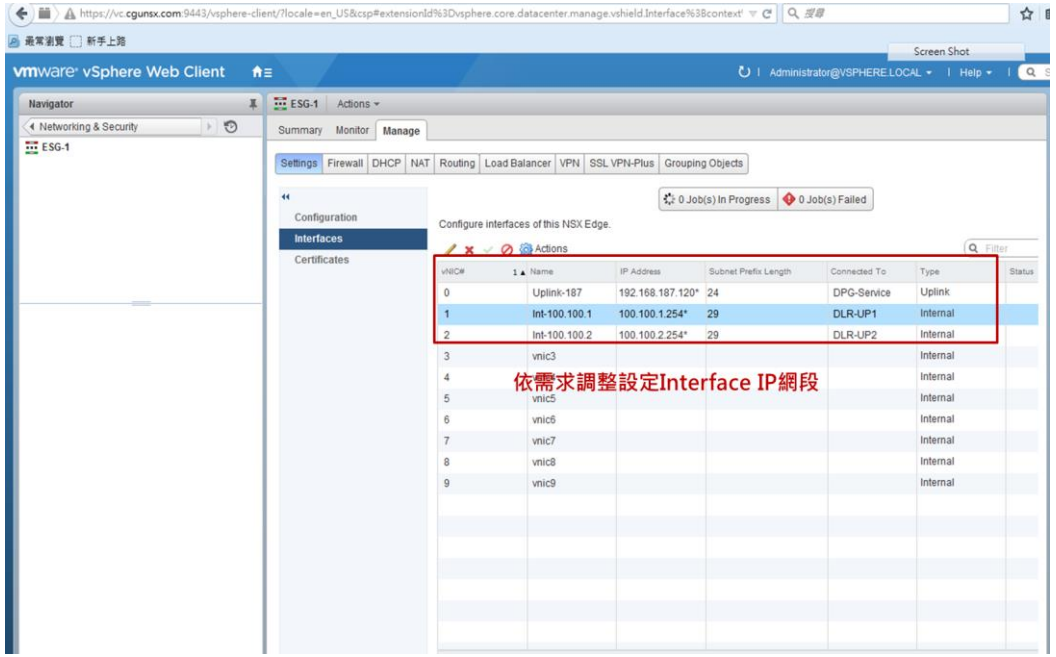
	測試組(NSX ESG/DLR)	對照組 (vDS)
2GB檔案傳輸速率	11448.3 KB/Sec	11534.3 KB/Sec

功能驗證 – 佈署與管理驗證

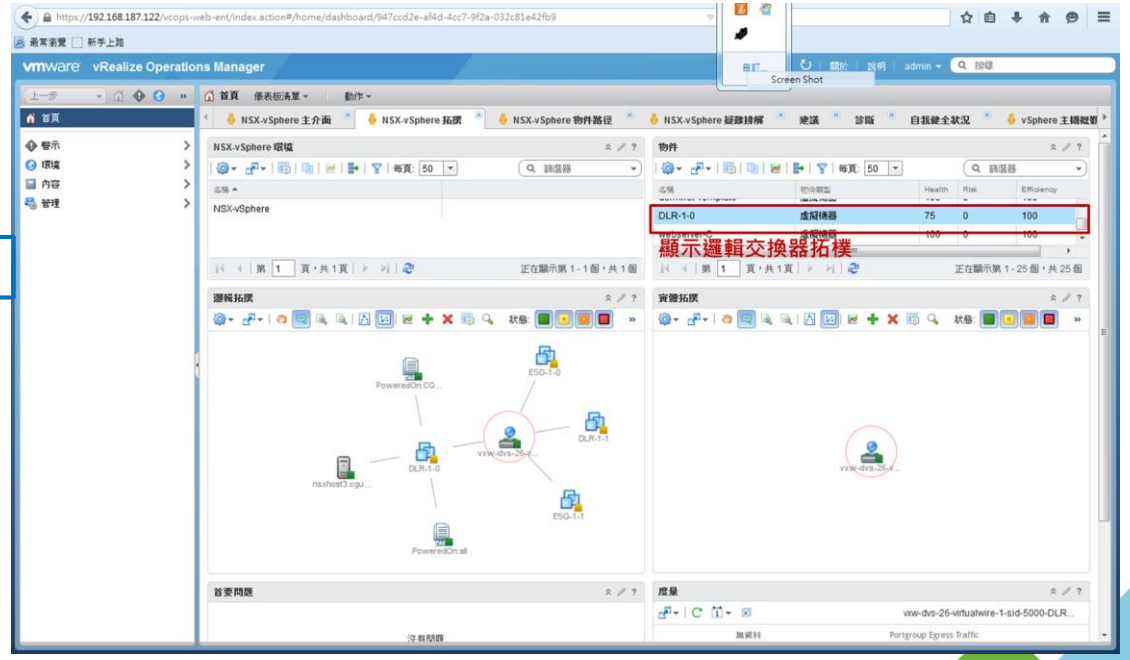
項次	測試項目	測試內容	結果	備註
1	佈署ESG	· 依需求佈署新的ESG及連接既有虛擬網路環境。 · 依需求調整既有ESG網路埠，連接至新建的DLR。	■ Yes □ No	
2	佈署DLR	· 依需求佈署新的DLR及連接既有虛擬網路環境。 · 依需求調整既有DLR網路埠，連接至新建的ESG。	■ Yes □ No	
3	NSX管理監控	· NSX各物件使用率監控。 · NSX架構拓樸、虛擬機器與各節點關係拓樸。	■ Yes □ No	

1

2



3



功能驗證 – 結果效益

業務虛擬機的零信任安全控管

透過微切分安全架構，全面性的涵蓋虛擬環境安全，強化了虛擬網路的資安空白

虛擬網路具備足夠效能

在虛擬網路安全架構下，仍能滿足校務相關業務系統服務效能，釐清虛擬網路效能疑慮

自動化佈署與管理

提供友善管理介面與除錯功能，讓不同專業承辦專員皆能快速進行操作與維護

Agenda

- 長庚大學簡介
- 計畫緣由
- 導入範圍
- 功能驗證
- 未來發展

未來發展

虛擬化資安 → 服務自動化 → 軟體定義資料中心

Phase 1

虛擬環境微切分安全保護暨進階網路服務

- 提供現有虛擬環境零信任等級之安全防護
- 依需求提供VM-Base防火牆、負載平衡器、VPN、路由器功能

Phase 2

服務自動化、邏輯網路接取混合雲或雙中心備援

- 自動將虛擬機器佈署至對應邏輯網路
- 建置私有雲平台，導入混合雲架構
- 建立應用服務維運自動化機制

Phase 3

軟體定義資料中心建立

- 業務服務系統完全虛擬化
- 建立應用服務感知管理流程

vmware

麟瑞科技 RING LINE CORPORATION

READY
FOR ANY
vForum2015