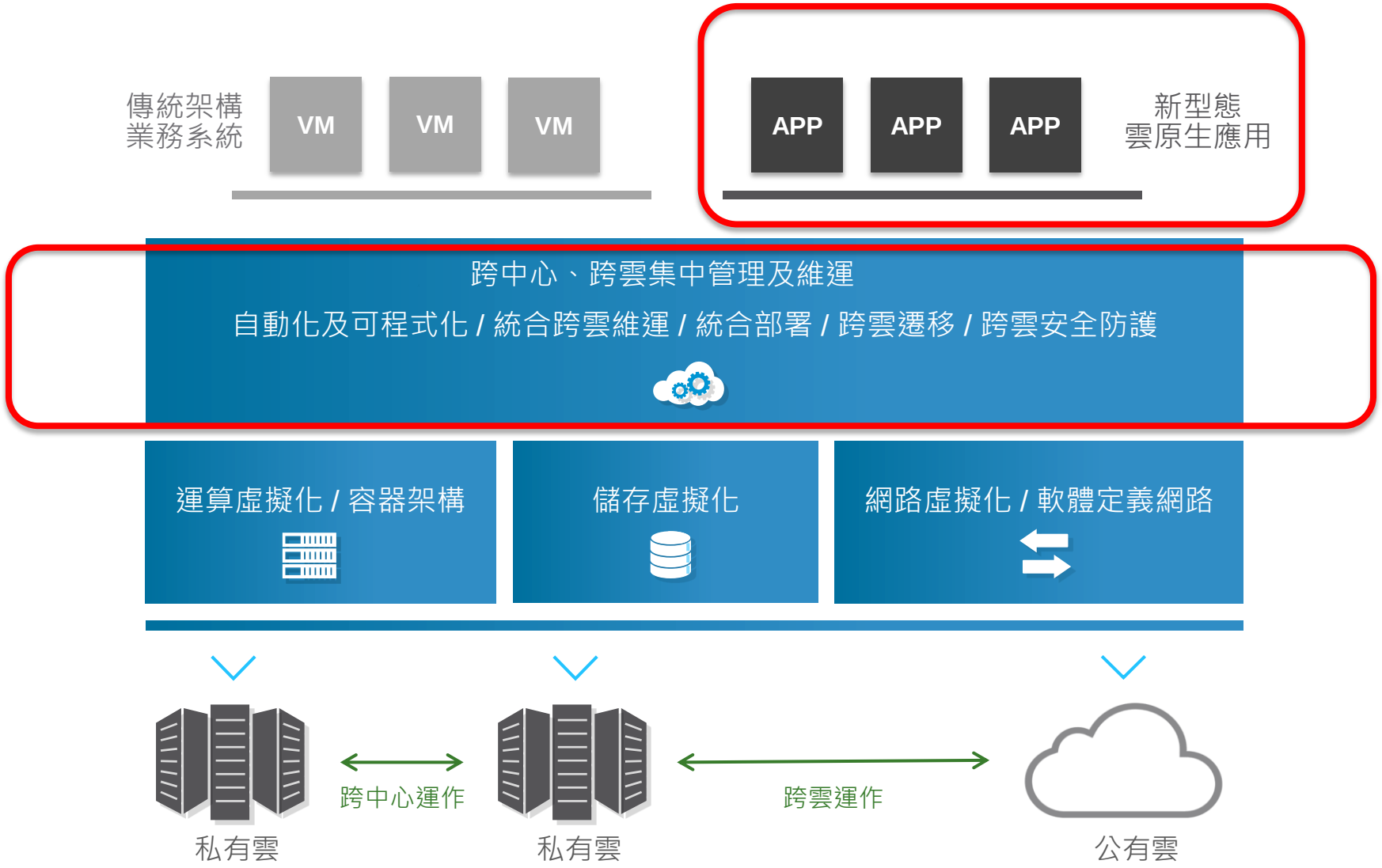
新世代雲原生平台的網路防禦與維運暨香港多所大學的應用分享

Eric NG
資深技術顧問
VMware 網路暨安全部門

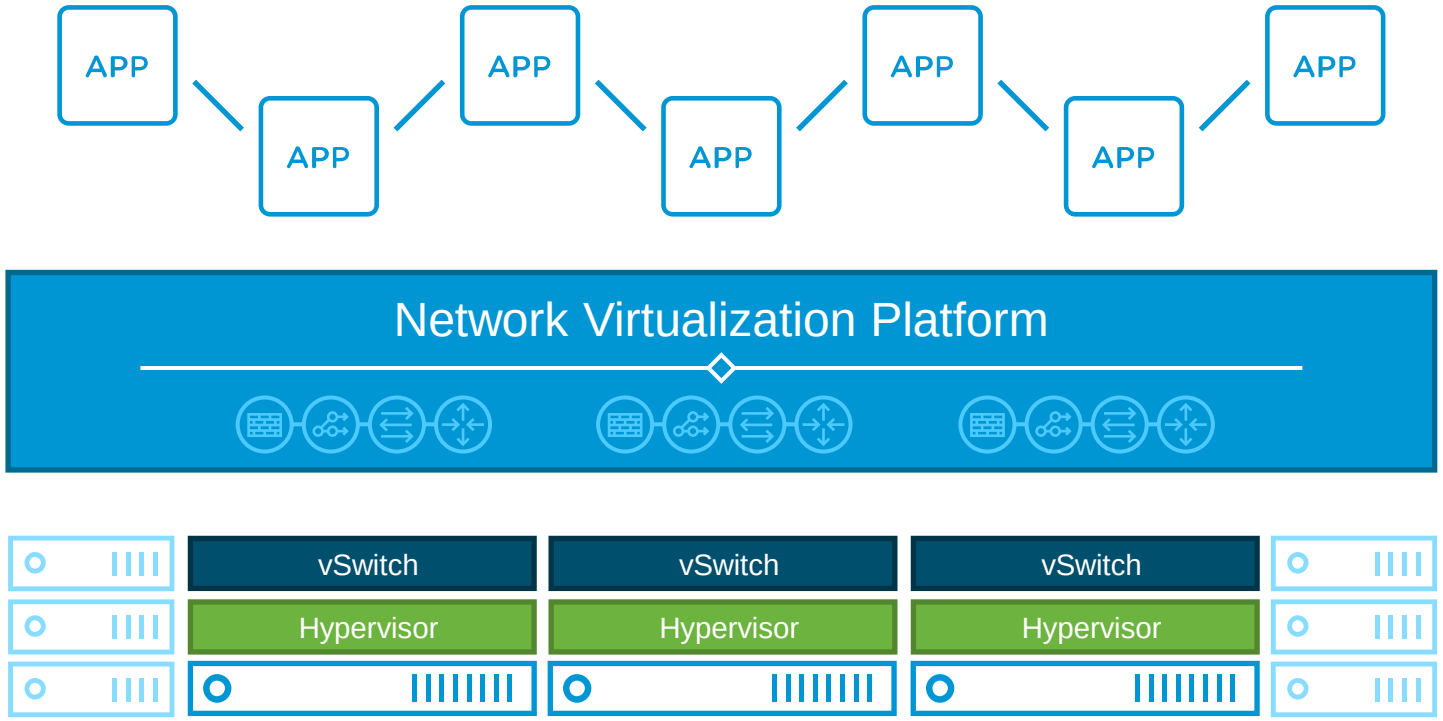
vmware

軟體定義資料中心的重要性



將網路與安全虛擬化

把重要的業務需求功能與底層網路硬體解構



應用部署彈性

網路暨安全虛擬層

資料中心資源池

vmware

VMware NSX 網路暨安全虛擬化的三個核心技術

網路虛擬化 (Network Virtualization) / 軟體定義網路 (SDN)

藉由封裝機制，於企業現有實體網路上隨需建立業務需求的邏輯網路，可跨越地域，並可藉由雲平臺呼叫達成自動化

安全虛擬化：微分段技術 (Micro-Segmentation)

於vSphere直接提供安全功能，可針對至單一虛擬機器，提供完整的防火牆、網路與系統防護

隨需建立的網路服務虛擬機器 (DC VNF)

依據業務需求，無額外成本地建立網路服務虛擬機器，提供路由器、防火牆、負載平衡器、及VPN等網路服務

vmware

NSX希望能解決政府暨企業所遭受的下列挑戰

安全

怎麼在資源整合的同時，
做到完善防護

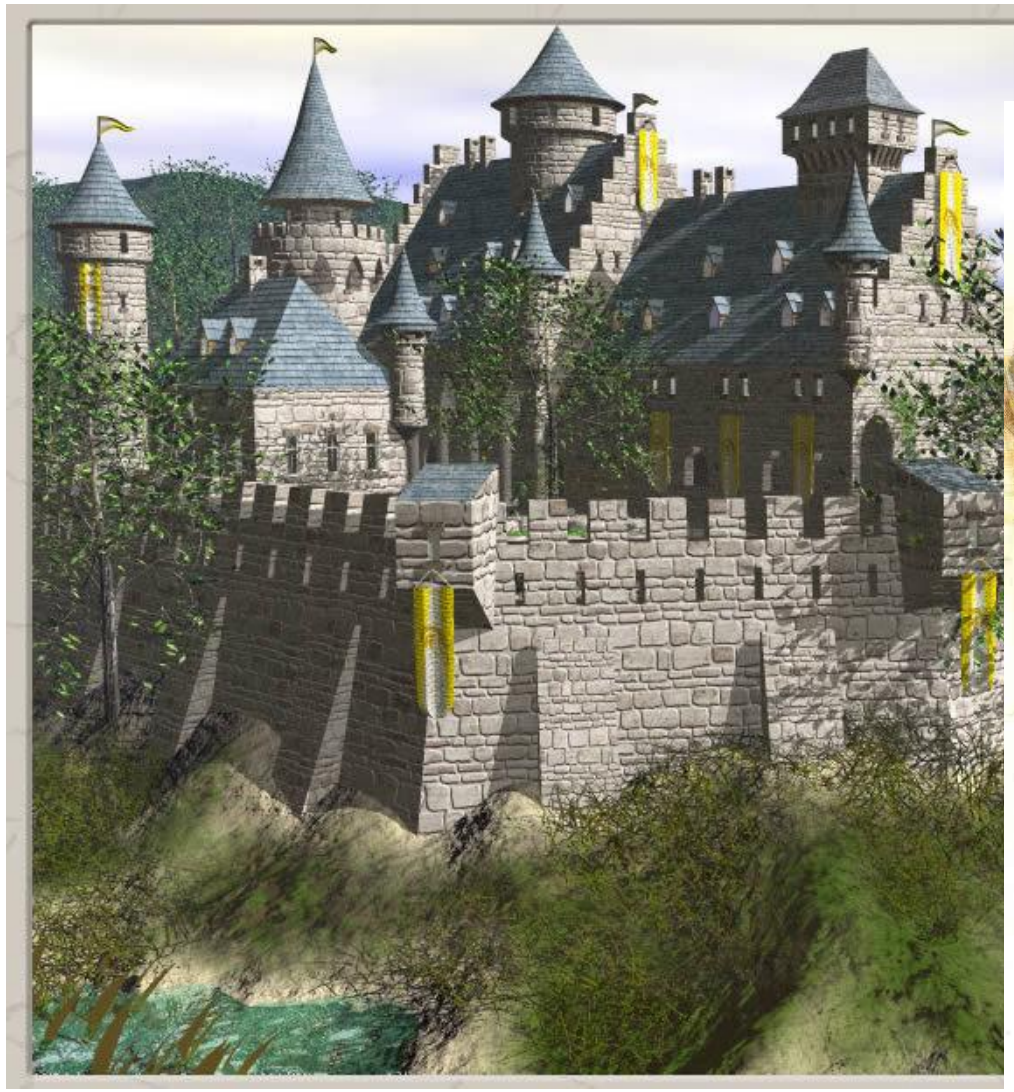
敏捷並正確

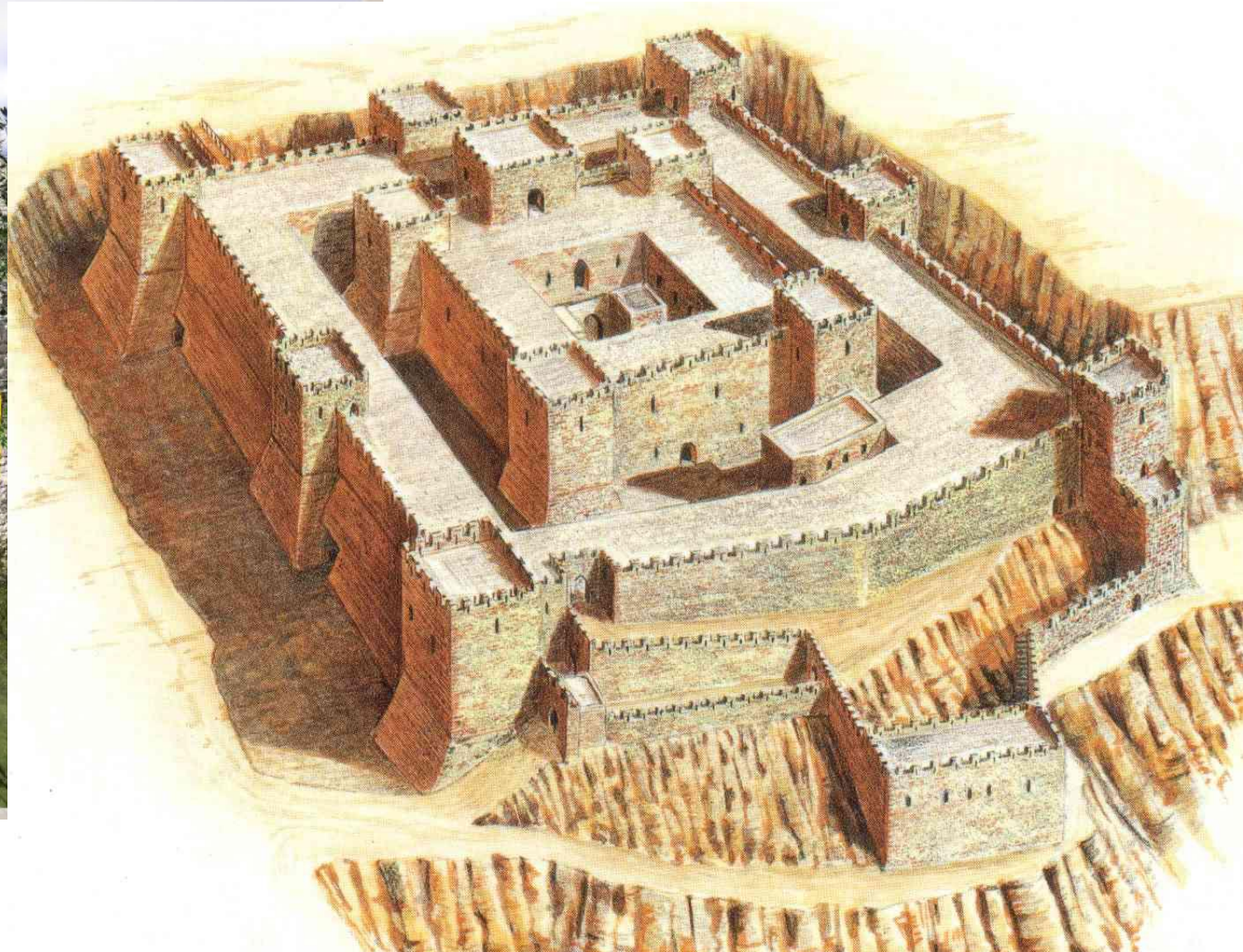
怎麼能夠做到集中管理與
敏捷式部署

跨中心/平臺彈性

怎麼達成跨中心業務
持續性保護與彈性部署？

傳統的安全防禦機制：為資料中心建造又高又厚的邊界城牆





vmware

傳統的安全防禦機制：在外層加入一道又一道的新防護措施

網路地址轉換

防火牆

防毒牆

入侵偵測及防護系統

郵件及社交軟體防護

阻斷服務攻擊防護

網站檢查與過濾

應用程式防火牆

新世代防火牆

高級持續性威脅防禦

vmware

邊界防護功能再強大，為何資料中心還是會遭受入侵？

資料中心前端由強大的網路安全設備進行防護

但駭客仍然時常由**低重要性系統**、或是**合法的系統或應用程式漏洞**入侵

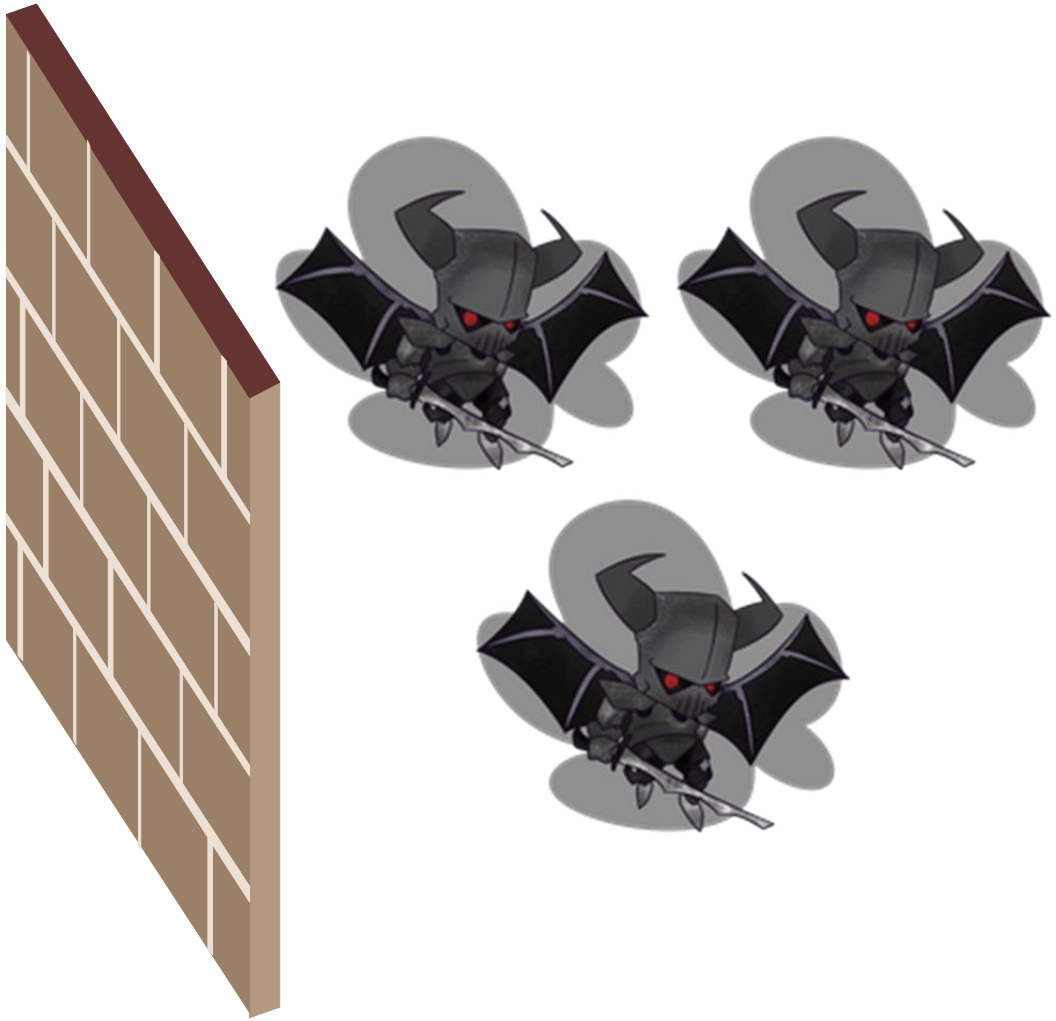
駭客入侵後通常不會聲張，僅會潛伏於現有系統內，或默默進行環境偵測

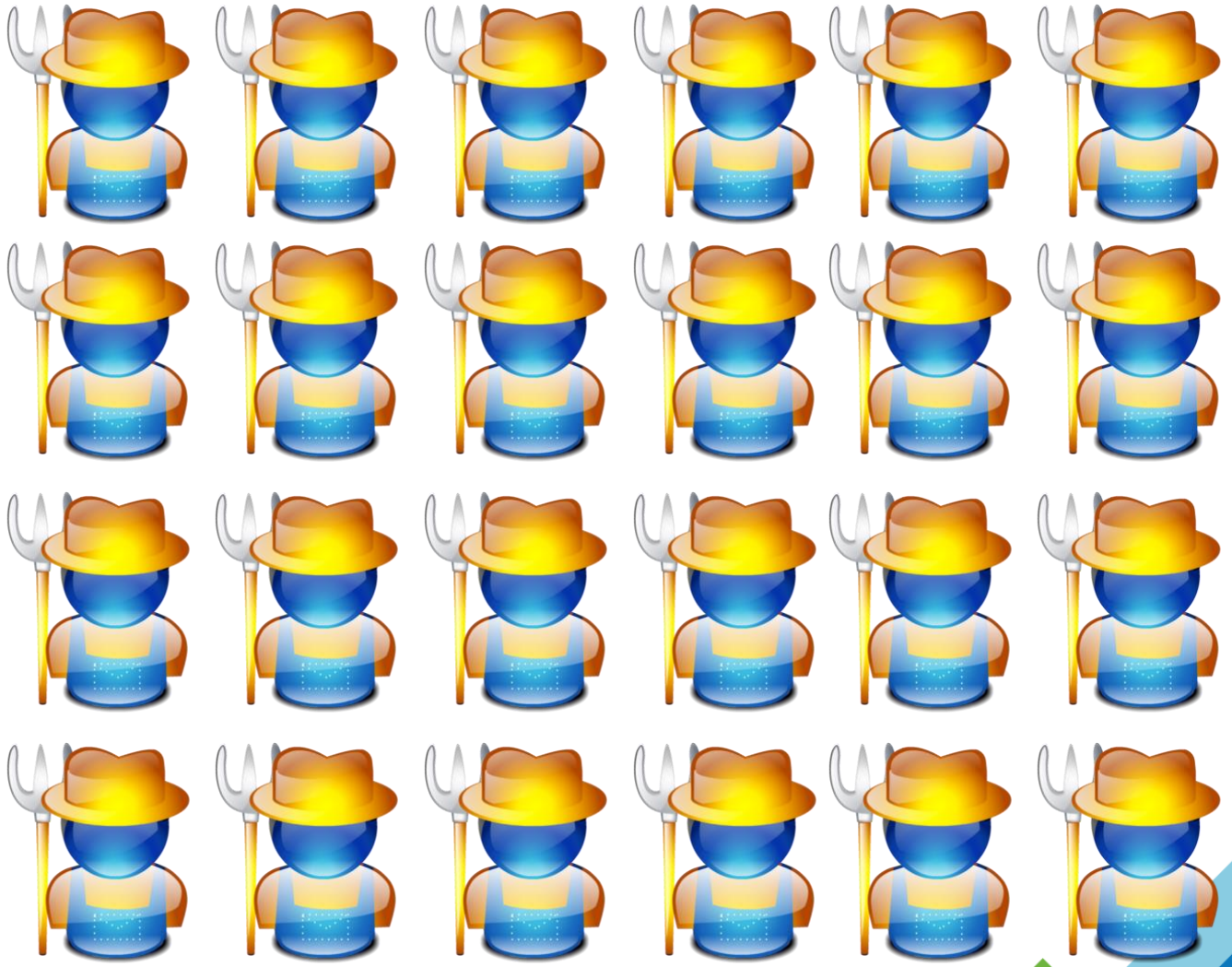
因為資料中心內部安全防護極弱，駭客容易於內部環境進一步感染

東西向Traffic遠大於南北向Traffic，且一般未被完整監控

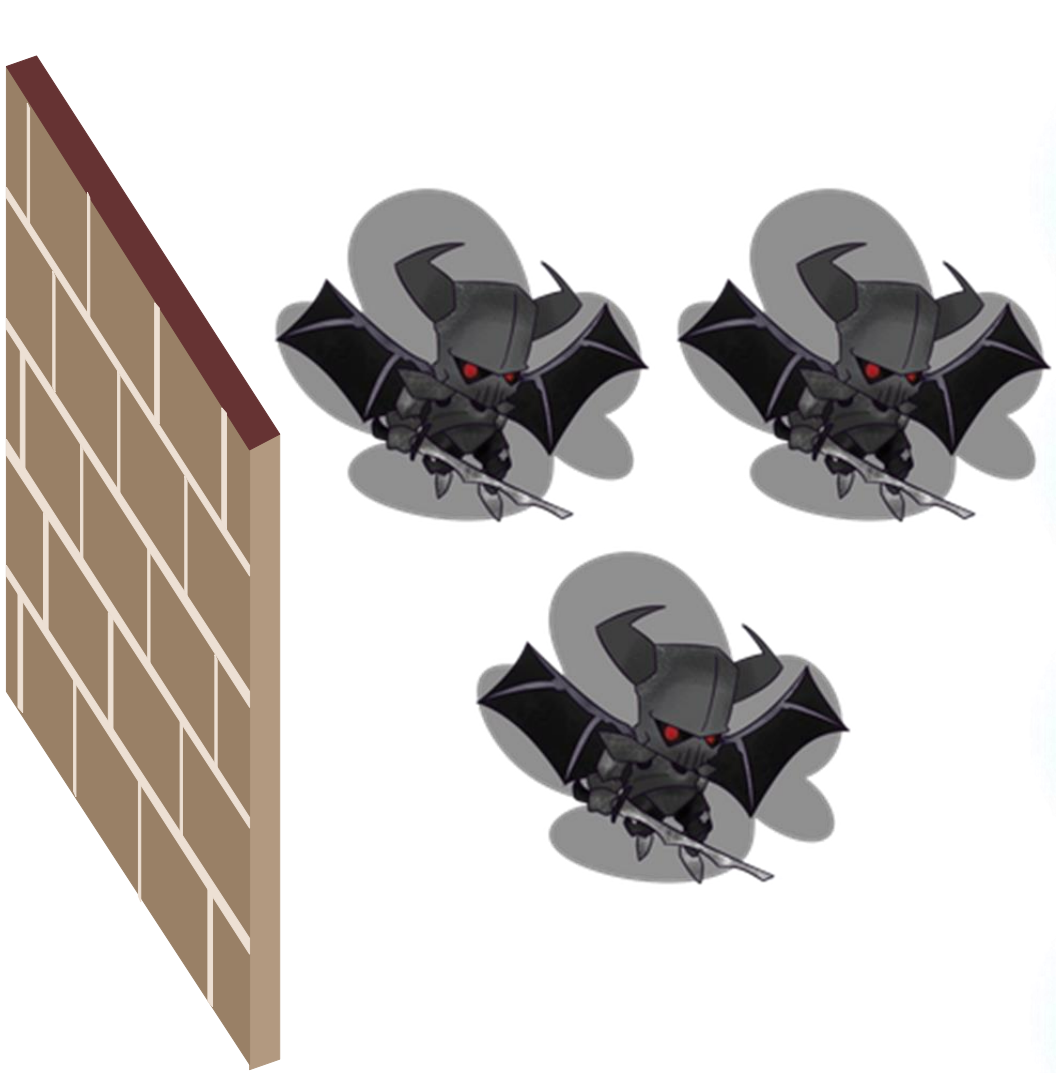
駭客可藉由內部感染或入侵重要系統，進而竊取重要機敏資料

一旦駭客（敵軍）攻進了資料中心（城牆），內部的重要業務是否有任何防護機制？

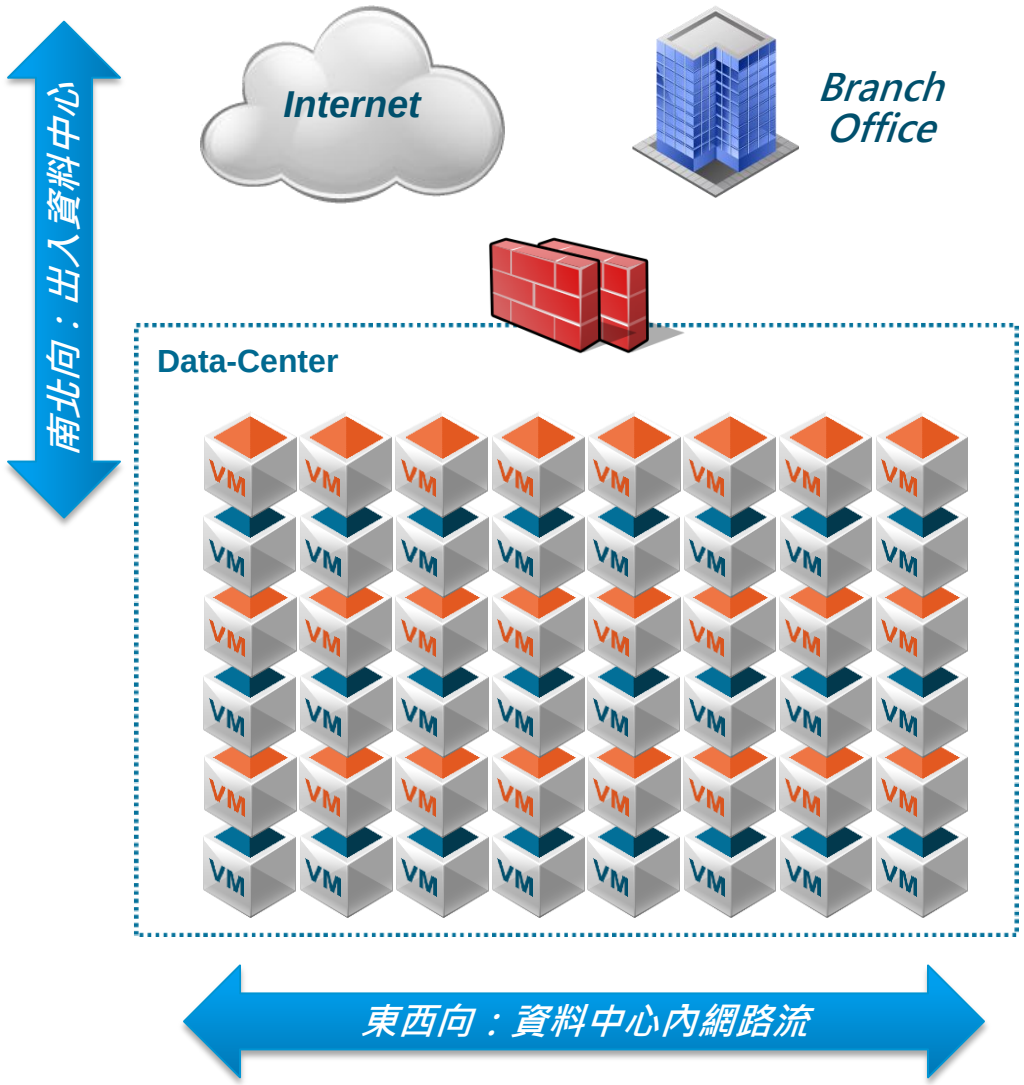




微分段機制替每一個核心業務機器直接提供防禦（穿盔甲）



為何重要的資料中心內必須具備東西向安全防護機制？

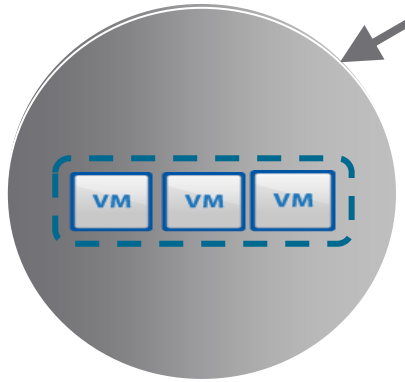


- *南北向防護：*
  - 傳統硬體安全設備
  - 負責防護資料中心來自外部駭客的攻擊

- *東西向防護：*
  - 微分段技術
  - 負責防護當駭客已經攻入資料中心、取得跳板機時，各主要業務間、以及伺服器與伺服器間的防護

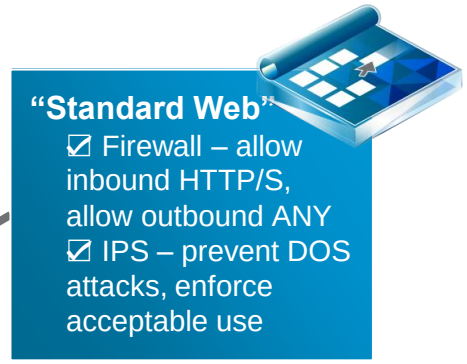
藉由將業務與資訊系統以自動化安全群組建立關聯，可直接指定對應此業務/資訊系統的安全防護政策，與網路完全脫鉤

- 所有名稱以ERP為開頭的虛擬機器
- 所有作業系統為Win 2003的虛機
- 所有設定標籤為人事系統的虛機
- 登入用戶為IT管理者的Windows虛機



Security Group：

哪些業務與系統需要被保護？



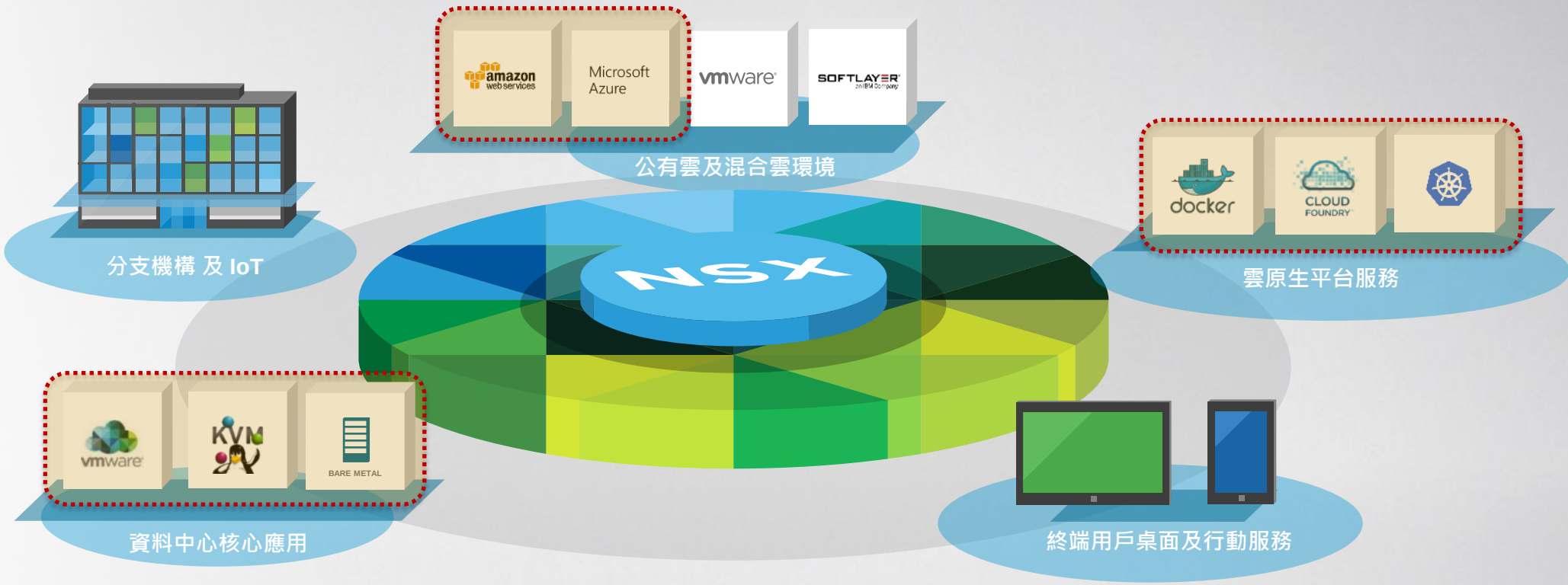
Security Policy：

針對此群組，要提供什麼的安全保護機制？

- 此安全群組的標準防火牆防護規則？
- 此安全群組要採用哪種防毒與系統保護方案？
- 此安全群組要採用哪種入侵防禦或應用程式網路防護方案？

NSX 願景：在每個不同異質平臺上支援安全且自動化部署的網路接取

NSX-T 的
主要使用情境



安全

本質上便安全的
基礎架構

自動化

支援業務需求速度的
IT 服務

業務持續性

任意地點的資料中心

VMware NSX微分段架構對於現行新型態雲資料中心的安全需求回應

達成零信任等級防護

- 每一台虛擬機器都受到保護
- 每一個網路封包都能進行檢查
- 直接於虛擬機器前就能進行最細部的安全控制

基於業務、系統的防護規則

- 安全團隊進行防護時，能夠藉由群組方式指定特定業務、系統、或特定對象
- 資訊系統擴充、變更時，自動套用安全政策無需手動進行資安組態變更

可整合頂尖協力廠商安全機制

- 完整的網路安全保護與IO保護
- 不同方案間之Security Chain管理

NSX虛擬化架構導入：

香港多所大學的應用分享

vmware

軟體定義資料中心：香港理工大學案例

THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

背景：建立新資料中心作為混合雲和災備平臺

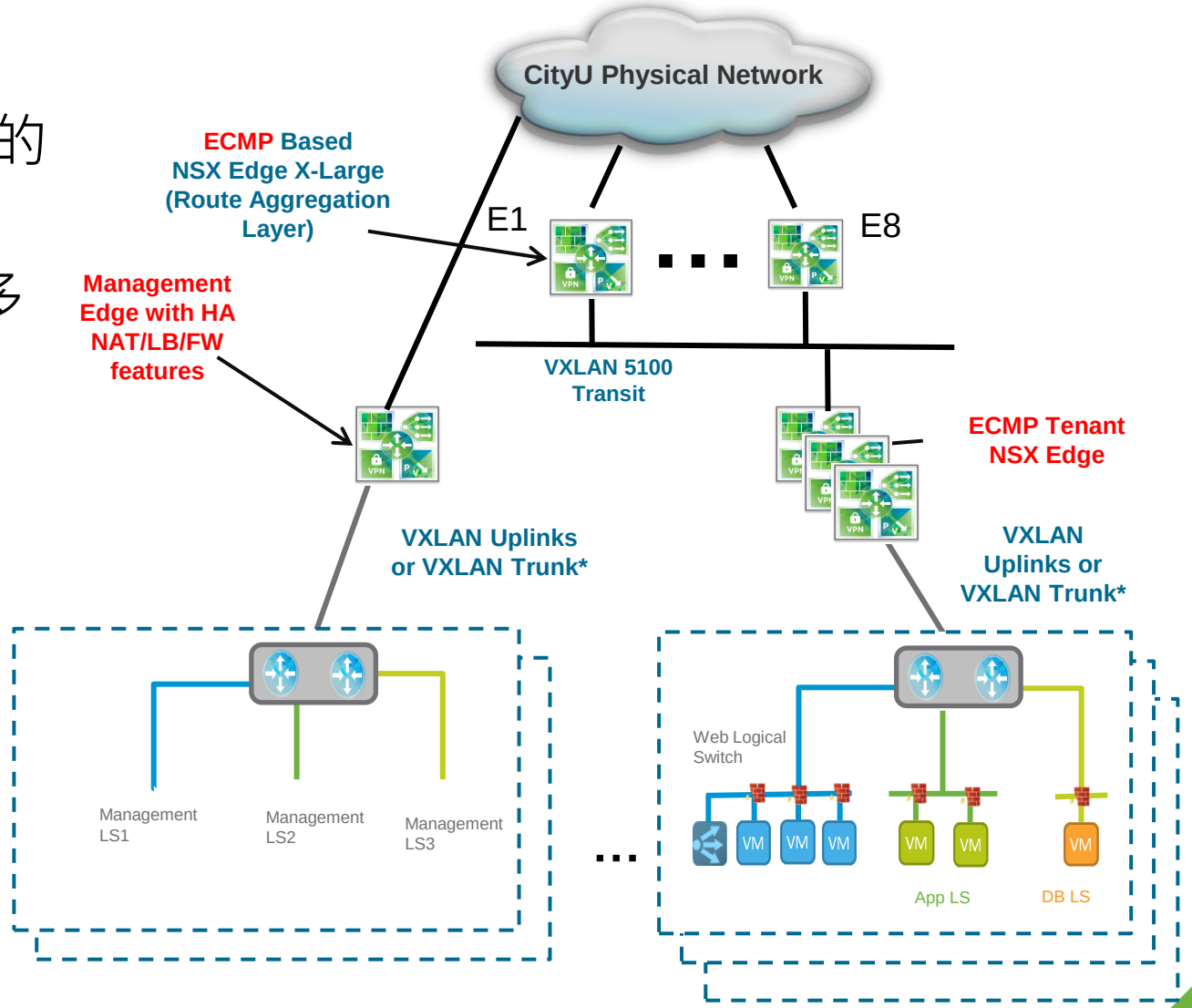
要求：新加伺服器和虛機都不需要改動實體網路

安全自動化

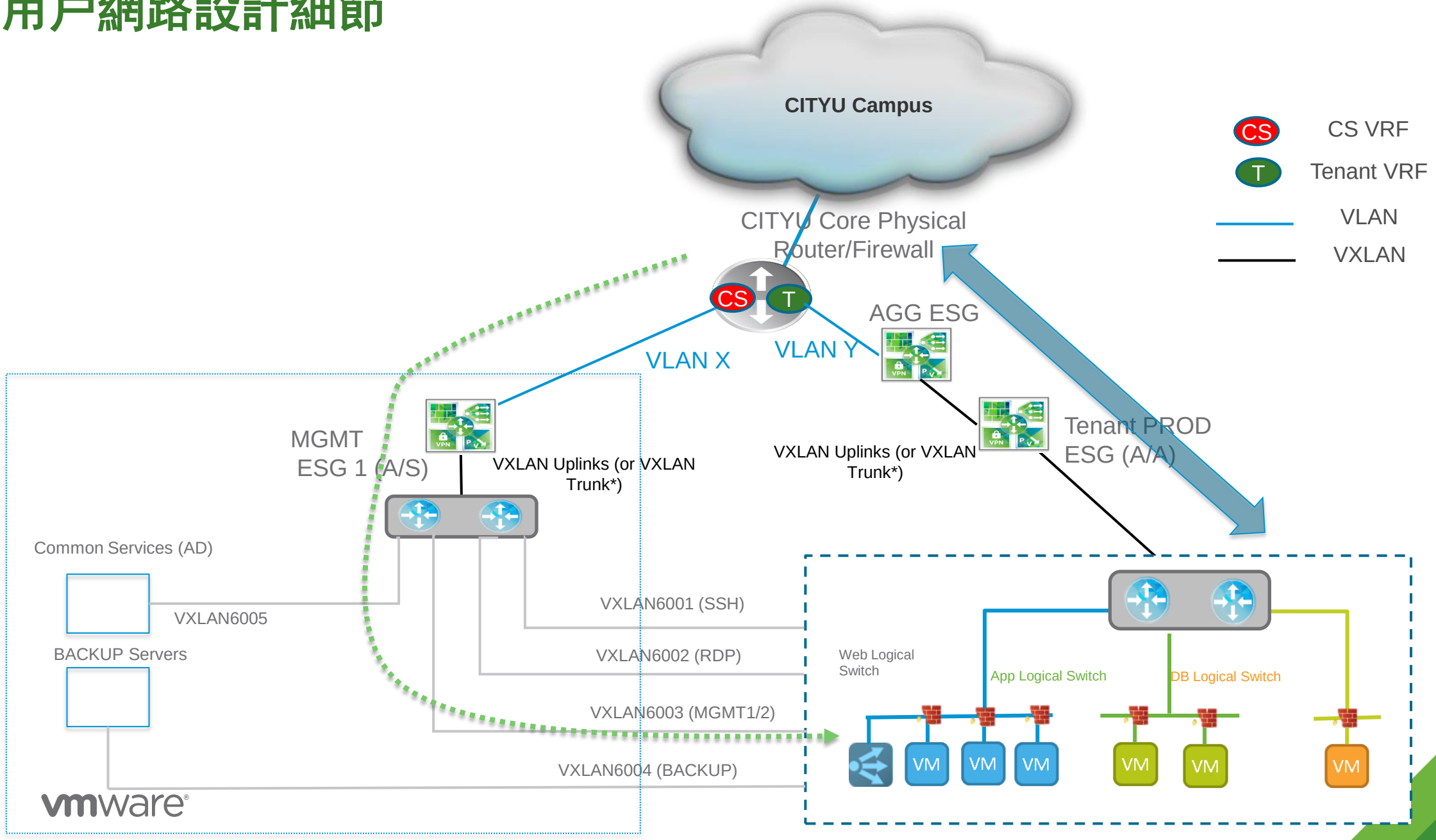
多業務多用戶平臺（相同IP地址）

多用戶虛擬網路架構

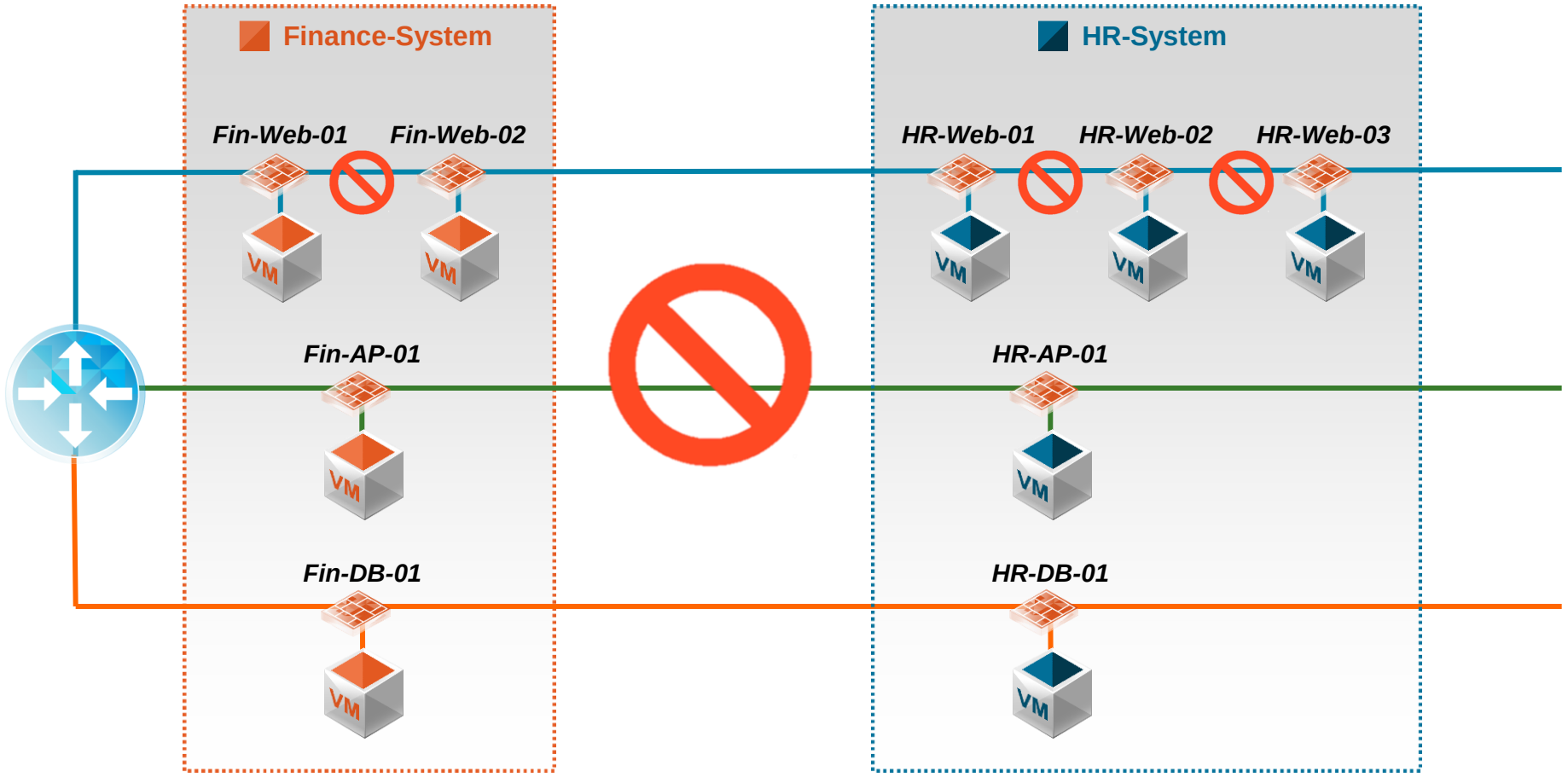
- 高可用性NSX VXLAN 架構
- 兩層 邊際路由器 (ESG) 支援網路的高擴容性而減低實體網路的改動
- 透過 ESG 的NAT 功能去支援多用戶相同IP地址的要求



用戶網路設計細節


CITYU Campus
CS VRF
T
Tenant VRF
VLAN
VXLAN
CITYU Core Physical Router/Firewall
CS
T
AGG ESG
VLAN X
VLAN Y
MGMT ESG 1 (A/S)
VXLAN Uplinks (or VXLAN Trunk*)
VXLAN Uplinks (or VXLAN Trunk*)
Tenant PROD ESG (A/A)
Common Services (AD)
VXLAN6005
BACKUP Servers
VXLAN6001 (SSH)
VXLAN6002 (RDP)
VXLAN6003 (MGMT1/2)
VXLAN6004 (BACKUP)
Web Logical Switch
App Logical Switch
DB Logical Switch
VM
VM
VM
VM
VM
VM
vmware

業務系統擴充時，新的虛擬機器自動加入安全群組，直接套用安全政策



網路和安全虛擬化：香港大學案例

香 港 大 學
THE UNIVERSITY OF HONG KONG

背景：傳統網路和安全方案不足以防禦新的攻擊和應用要求，
自動化方案難以落地

要求: 實體網路虛擬化和統一資源配置

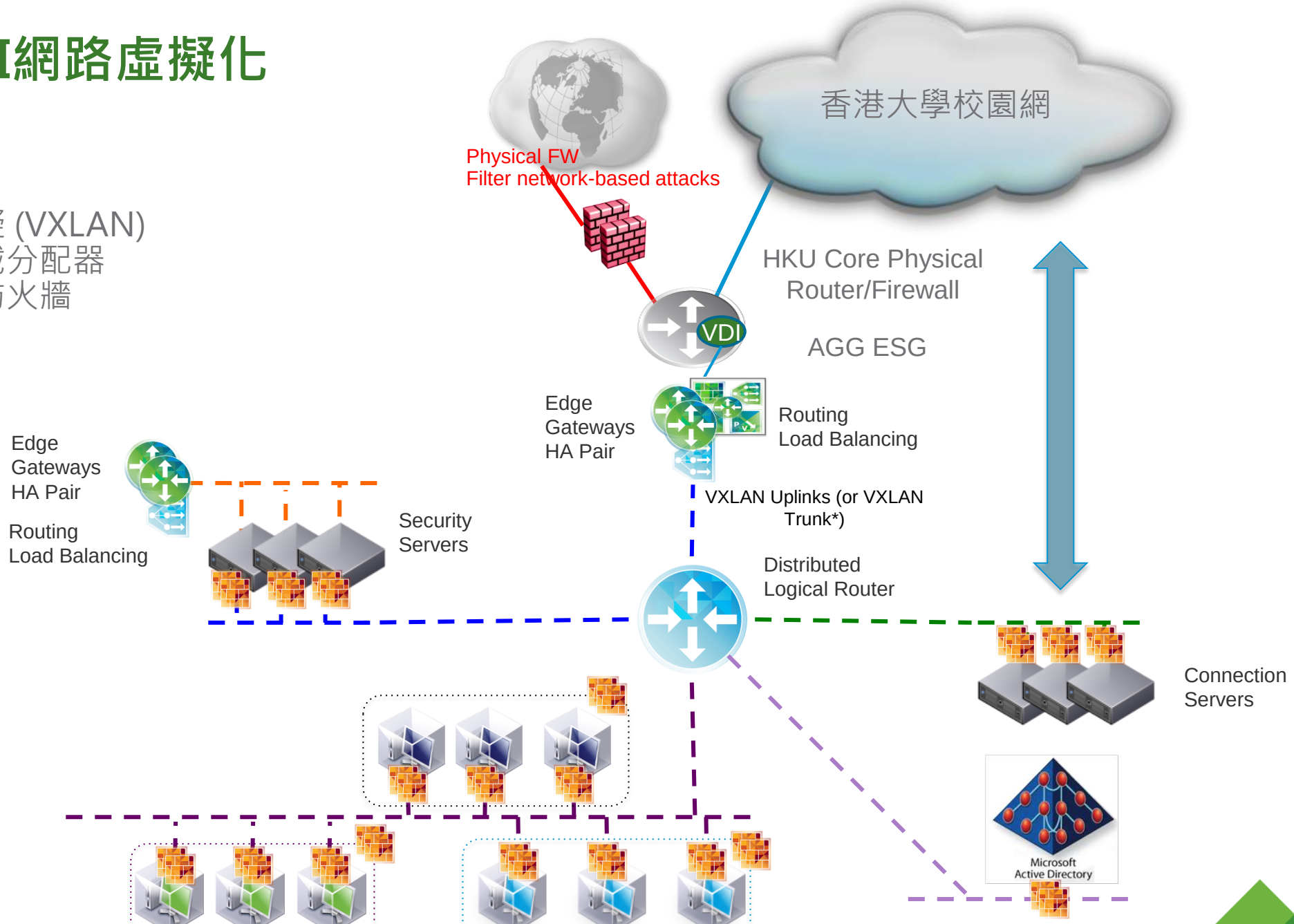
新應用，譬如：VDI 必須達成安全區隔 (同一網路subnet)

一鍵化的網路自動化功能

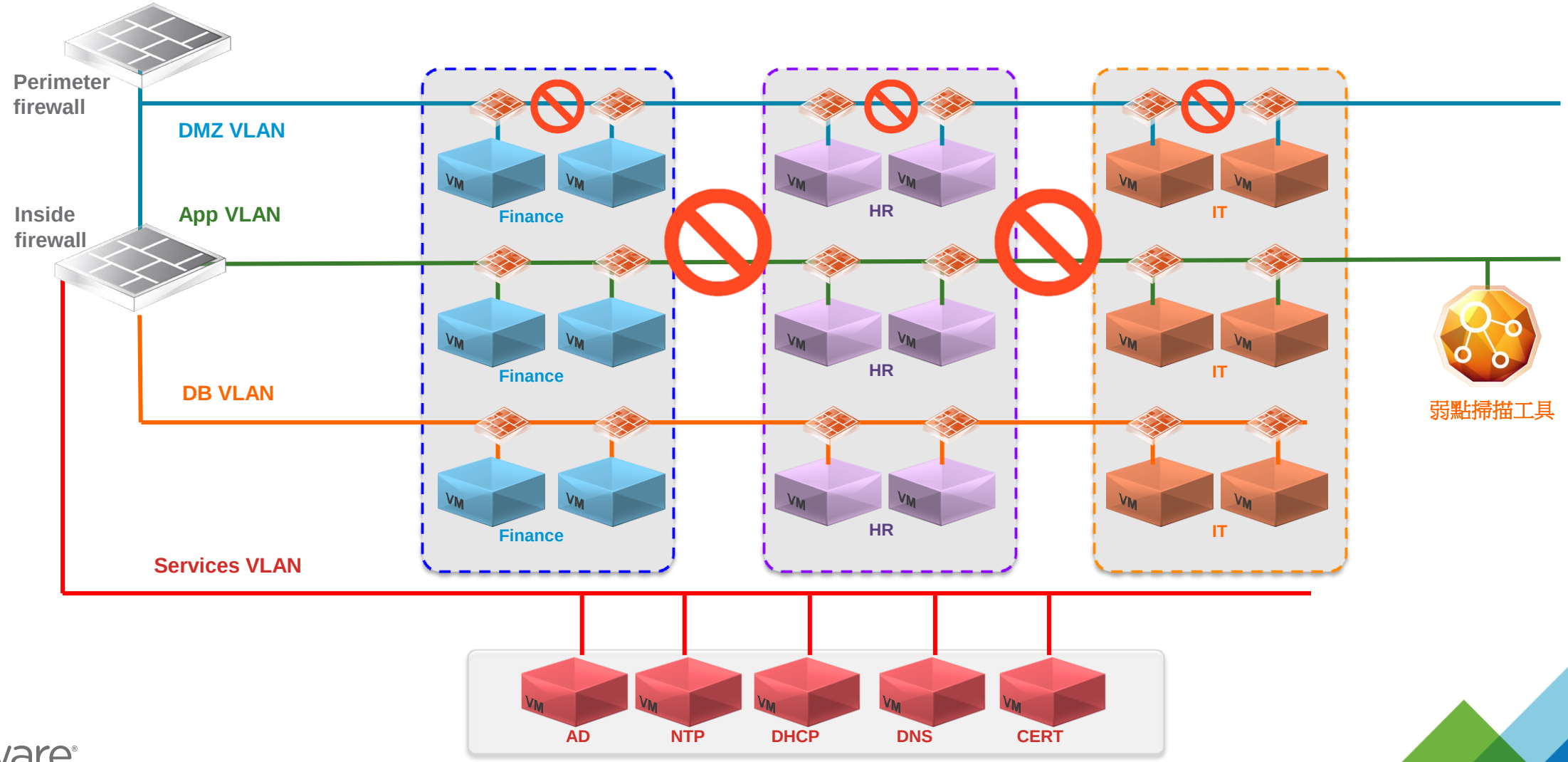
香港大學VDI網路虛擬化

NSX 提供：

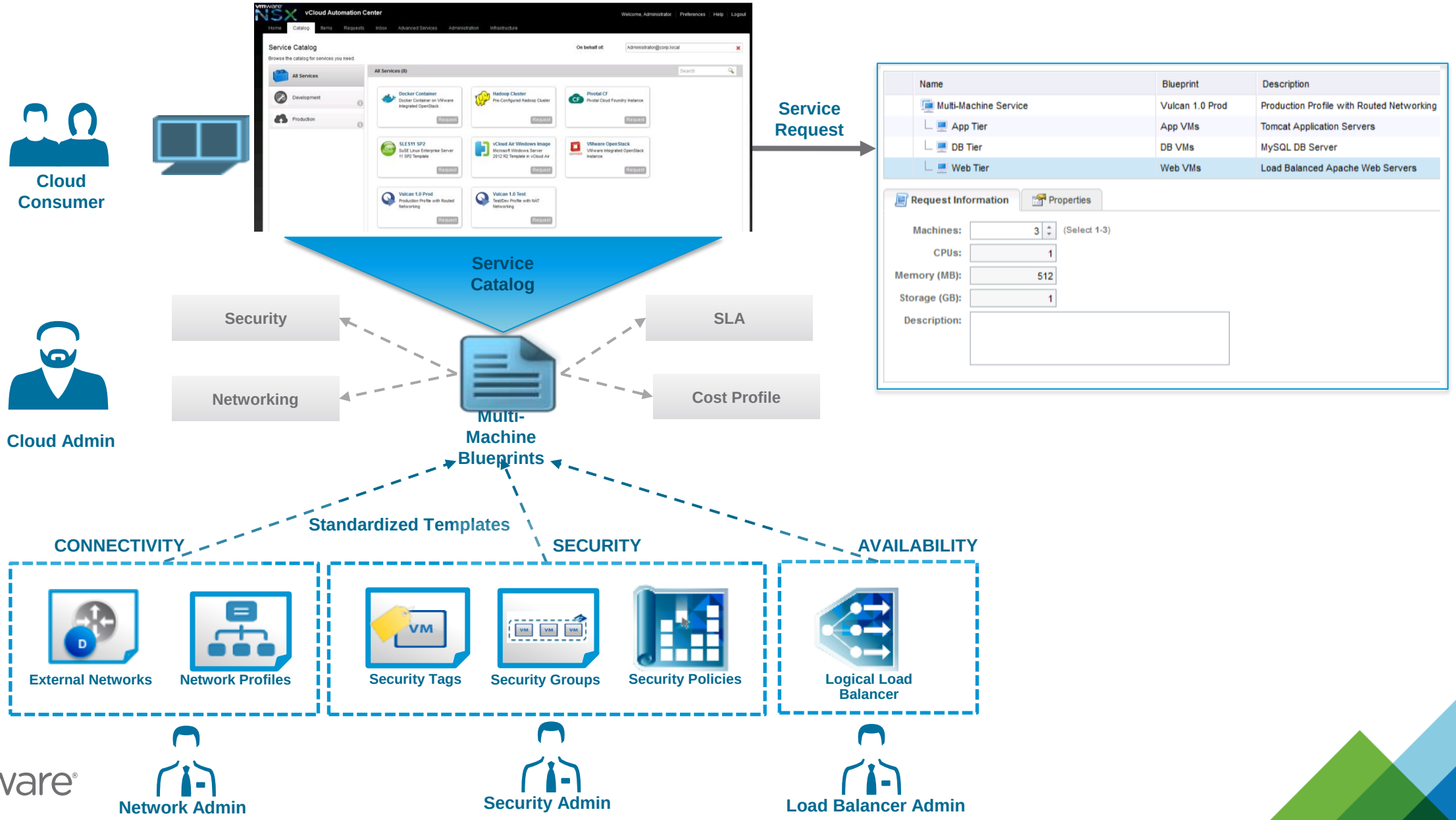
- 網路虛擬 (VXLAN)
- 網路負載分配器
- 分散式防火牆



VMware NSX 微分段技術：
以集中管理、分散防護方式，達成資訊業務間、及同網段機器間的阻隔



跟vRealize Automation整合的IT自動化



安全虛擬化和自動化：香港科技大學案例

香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

背景：安全方案不足以防禦新的攻擊和應用要求，需要一個整合協力廠商安全自動化的方案

要求: 網路微分段安全

Agentless防毒系統和隔離自動化

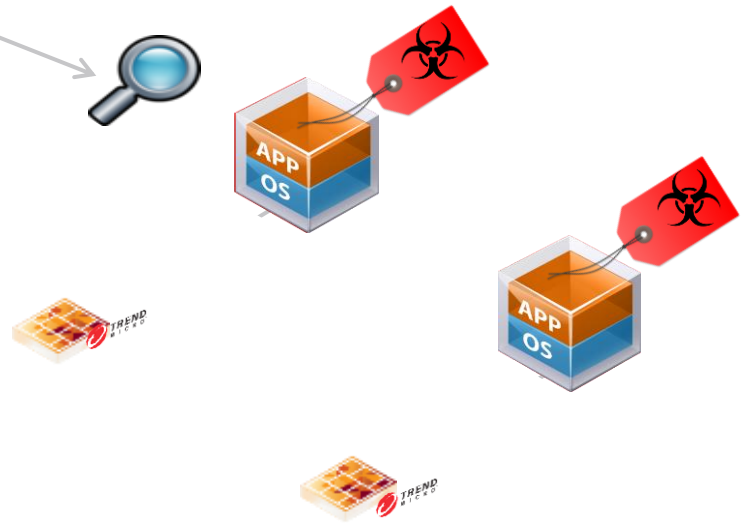
統一維運和除錯平臺，能夠集中進行安全管理，並大幅減低維運Effort

最短期間內鎖定OS虛機並進行升級

安全自動化方案

Security Group = Quarantine Zone
Members = {Tag = ‘ANTI_VIRUS.VirusFound’, L2 Isolated Network}

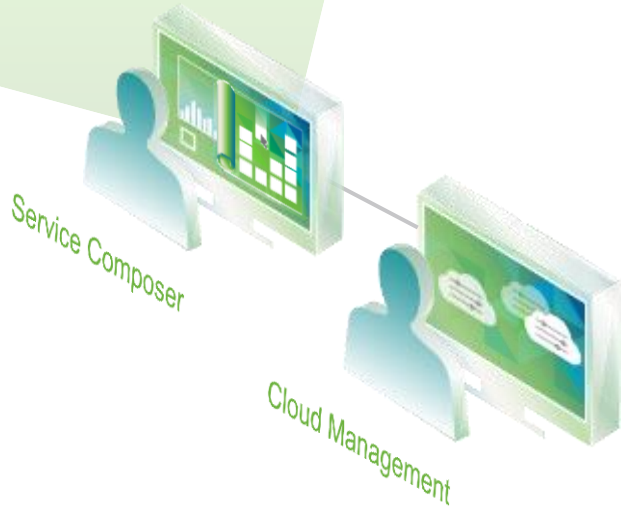
Security Group = Web Tier



Policy Definition

Standard Desktop VM Policy
☑ Anti-Virus – Scan

Quarantined VM Policy
☑ Firewall – Block all except security tools
☑ Anti-Virus – Scan and remediate



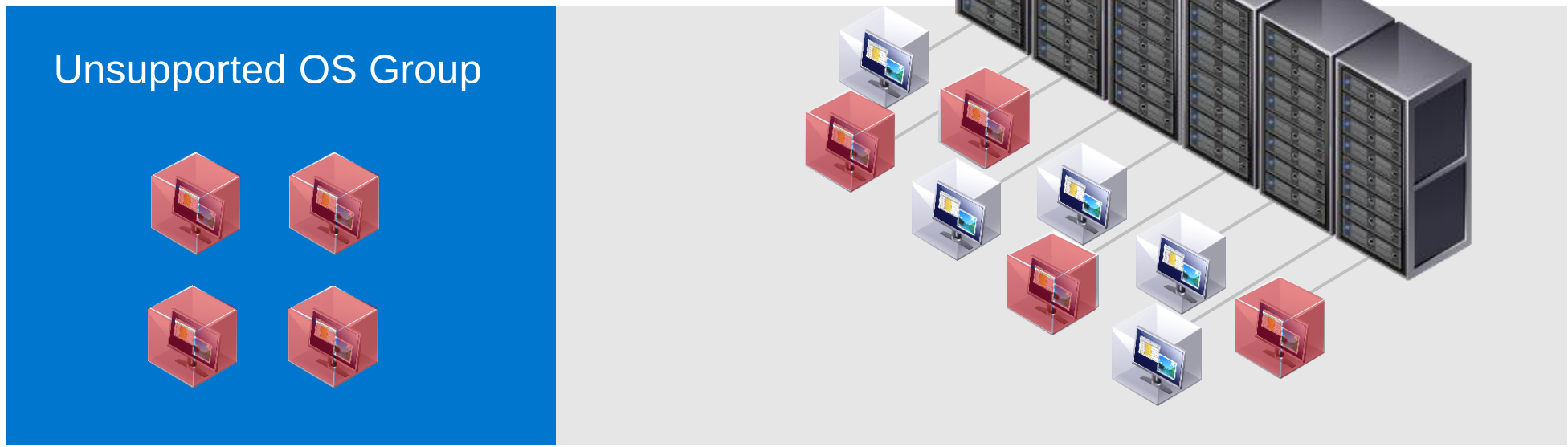
vmware

快速找出已經End-of-Support的作業系統，並禁止存取Internet

客戶狀況

安全政策禁止使用已經End-of-Support的作業系統

若有此類作業系統機器，完成升級前禁止連接至Internet



謝謝

vmware®