vmware

READY FOR ANY

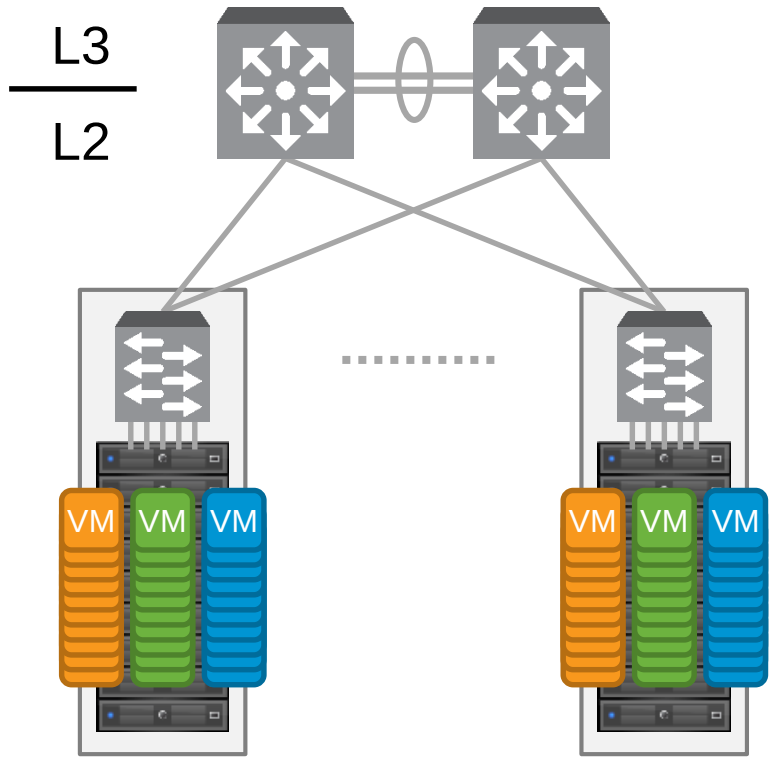
vForum2015

9 December 2015 | Taipei, Taiwan

零信任雲端資料中心資安防護最佳實務

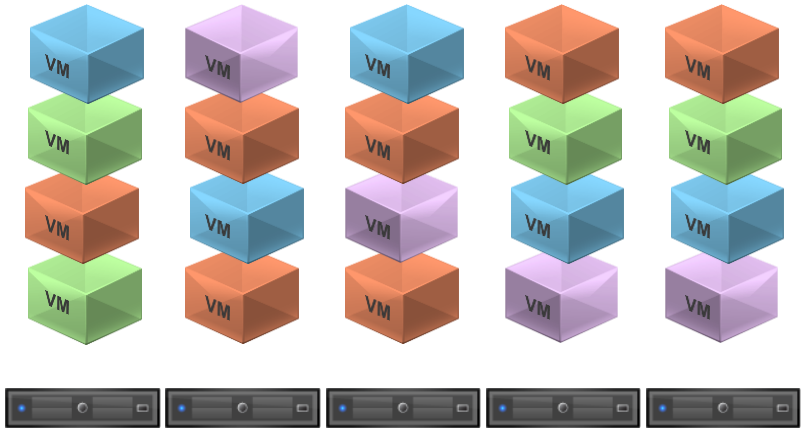
饒康立
VMware技術顧問

虛擬環境及雲架構的特性：資料中心內之虛擬機器數量大幅增加，遠超過原先實體環境規模



安全政策的維運困難性大幅增加

虛擬環境及雲架構的特性：資料中心內之虛擬機器數量大幅增加，遠超過原先實體環境規模

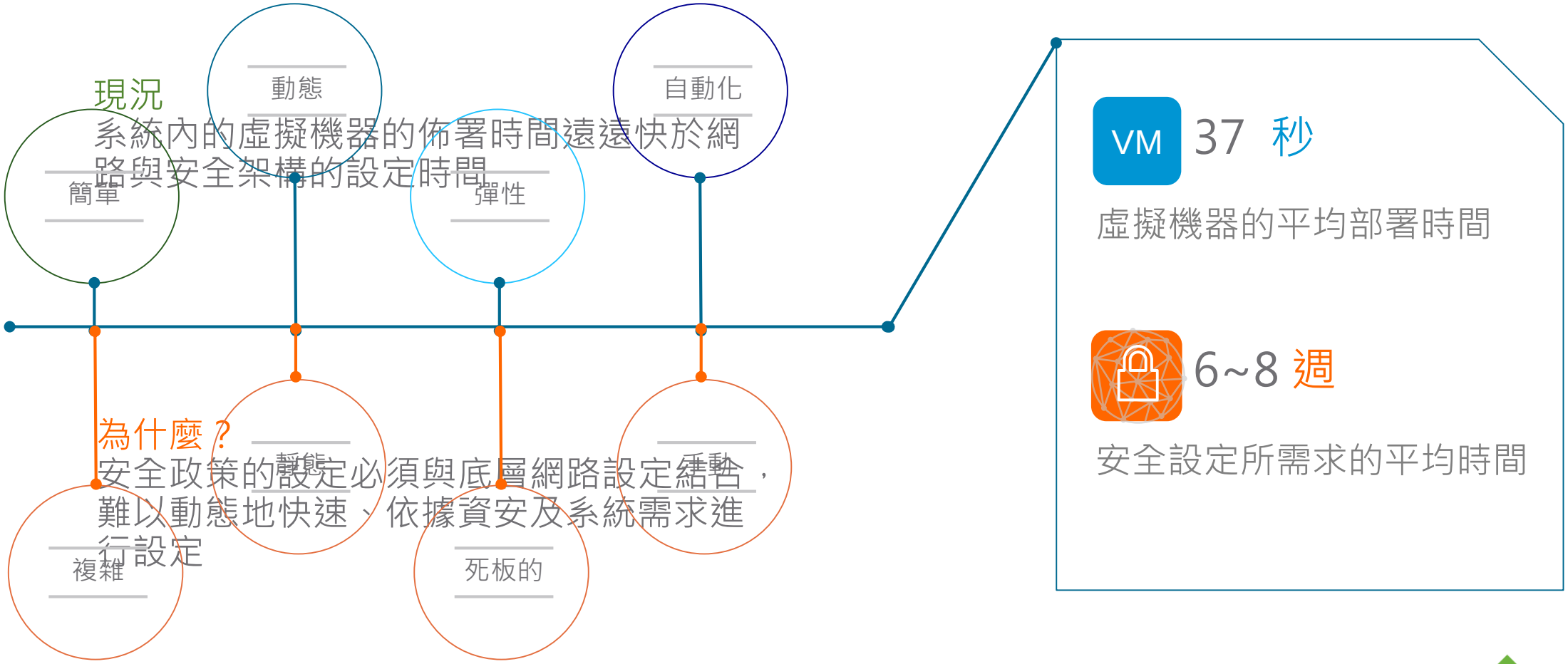


- 環境變動快速，機器的產出與變更隨時發生
- 虛擬機器數目多，且網路位址動態配置
- 不同租戶極可能會有重複的IP或網段

安全政策難以進行手動組態設定

vmware

系統佈署時，安全的設定遠遠超過虛擬機器所部署花費的時間



現況

系統內的虛擬機器的佈署時間遠遠快於網路與安全架構的設定時間

為什麼？

安全政策的設定必須與底層網路設定結合，難以動態地快速、依據資安及系統需求進行設定

VM 37 秒

虛擬機器的平均部署時間

6~8 週

安全設定所需求的平均時間

vmware

業務系統能夠快速地進行部署，但安全政策的設定與組態需要花費極大時間才能完成

vmware

為什麼？現實狀況內，資安需求與網路架構與實體無關，但設定上大部份的時間都需要確認防護目標的網路位置，或是無法執行

資安需求：將不同的資訊系統，比如停車場系統與校務系統間網路阻斷

資安需求：使用者依據身份，僅能夠連接到被授權使用的系統與網路環境

資安需求：所有EoS作業系統如Windows Server 2003不得在生產環境使用

應該要做的是:

能以安全群組直接對應資安政策並進行防護：

- 停車場系統群組機器 不可連線至 校務系統群組機器
- 學生登入的桌面機器，僅能連線到選課或評鑑系統，而非停車場系統或校務系統
- 自動挑出所有Windows Server 2003的虛機

結果去進行的設定是:

找尋系統的 Source / Destination 為

- 172.16.35.244
- 10.42.230.0/24
- FE80::250:56FF:FE8D:8D26
- 00:50:56:8D:CF:93

vmware

結果是：冗長且難以閱讀、不易維護的防火牆規則

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
1	* Any	vWeb_Server	TCP http	accept	- None
2	Email_Server_Internal	Email_Server_DMZ	smtp->outgoing-email	accept	Log
3	net-10.0.0.0-24	Email_Server_DMZ	TCP smtp	accept	Log
4	Email_Server_DMZ	net-10.0.0.0-24	smtp->incoming-email	accept	Log
5	Email_Server_DMZ	net-10.0.0.0-24	TCP smtp	accept	Log
6	net-10.0.0.0-24	vWeb_Server	ftp->web-server-upload	accept	Log
7	net-10.0.0.0-24	vWeb_Server	ftp->web-server-download	accept	Log
8	net-10.0.0.0-24	vWeb_Server	ftp->ftp-scan	accept	Log
9	net-10.0.0.0-24	* Any	TCP http	accept	Log
10	CVP_Server	www.cvp-vendor.com	TCP http	accept	- None
11	UF				
12	* An				

DMZ interface

	Proto	Source	Port	Destination	Port	Description
↑	UDP	DMZ net	*	192.168.1.2	53 (DNS)	Permit DMZ to primary DNS server
↑	UDP	DMZ net	*	192.168.1.3	53 (DNS)	Permit DMZ to secondary DNS server
↑	TCP					
↑	UDP					
✗	*					

Configuration > Firewall > Access Rules

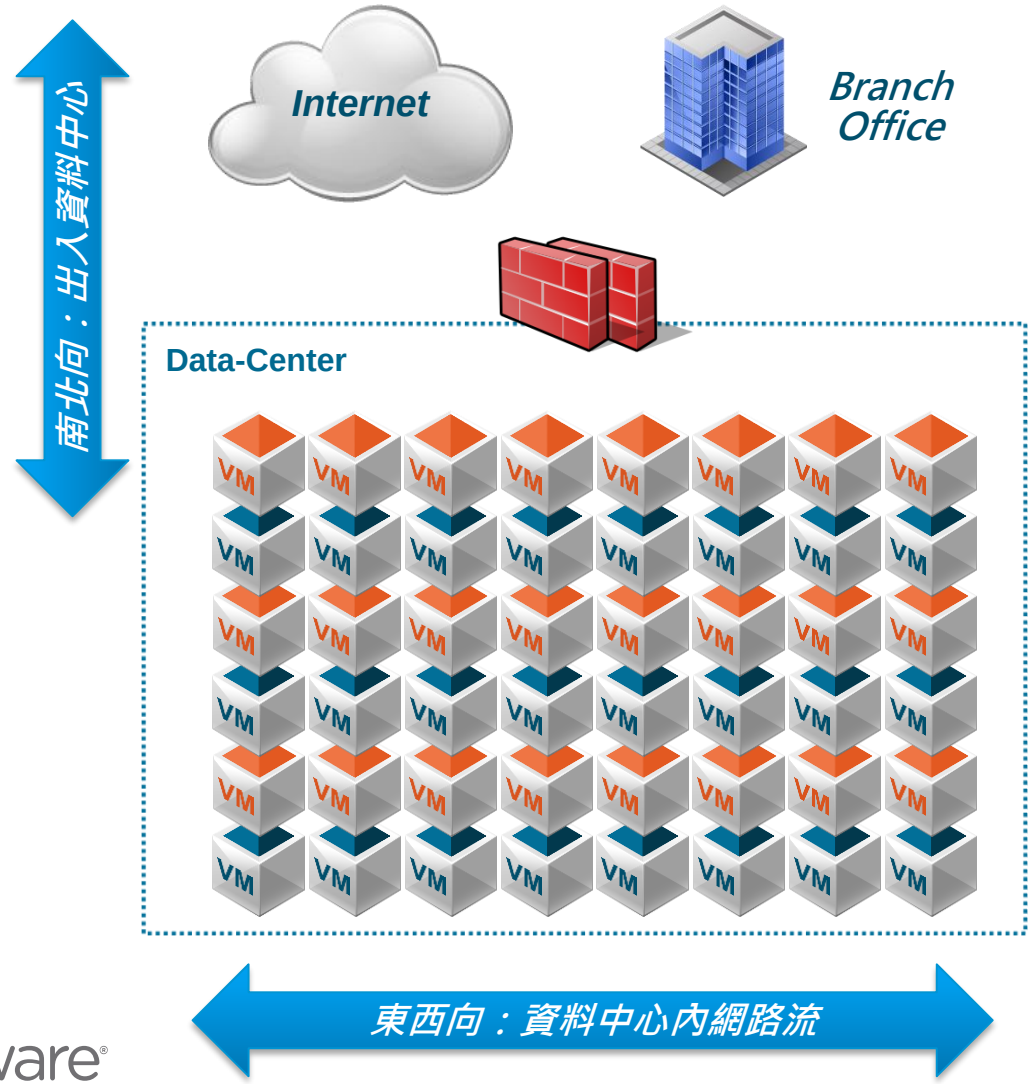
Add | Edit | Delete | Find | Diagram | Export | Clear Hits

#	Enabled	Source	Destination	Service	Action
DMZ (2 implicit incoming rules)					
1		any	Any less secure ne...	ip	Permit
2		any	any	ip	Deny
inside (2 implicit incoming rules)					
			Any less secure ne...	ip	Permit
			any	ip	Deny
			Any less secure ne...	ip	Permit
			any	ip	Deny
			192.168.5.3	smtp	Permit
			192.168.5.5	https	Permit
			192.168.5.4	domain	Permit
			any	ip	Deny

No.	Name	Type	Source	Destination	Service	Action
1	DMZ Access	User	any	172.16.10.11-172.1...	HTTPS HTTP	Accept
2	Web to App	User	172.16.10.11-172.1...	192.168.10.11-192....	Tomcat	Accept
3	App to DB	User	192.168.10.11-192....	192.168.30.10	MySQL	Accept
4	DMZ LDAP, NTP, and DNS access	User	172.16.10.1/24	172.16.40.1/24	any	Accept

vmware

現行資料中心內著重南北向防護，但東西向防護的機制極度欠缺



Cisco Global Cloud Index 對於

資料中心網路流統計資訊:

- *東西向網路流: 76.7%*
- *南北向網路流: 16.7%*
- *資料中心間之網路流: 6.6%*

資料中心內之東西向安全防護刻不容緩

vmware

南北向實體安全設備的功能如此強大，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

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

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

東西向Traffic遠大於南北向Traffic，
且一般未被完整監控

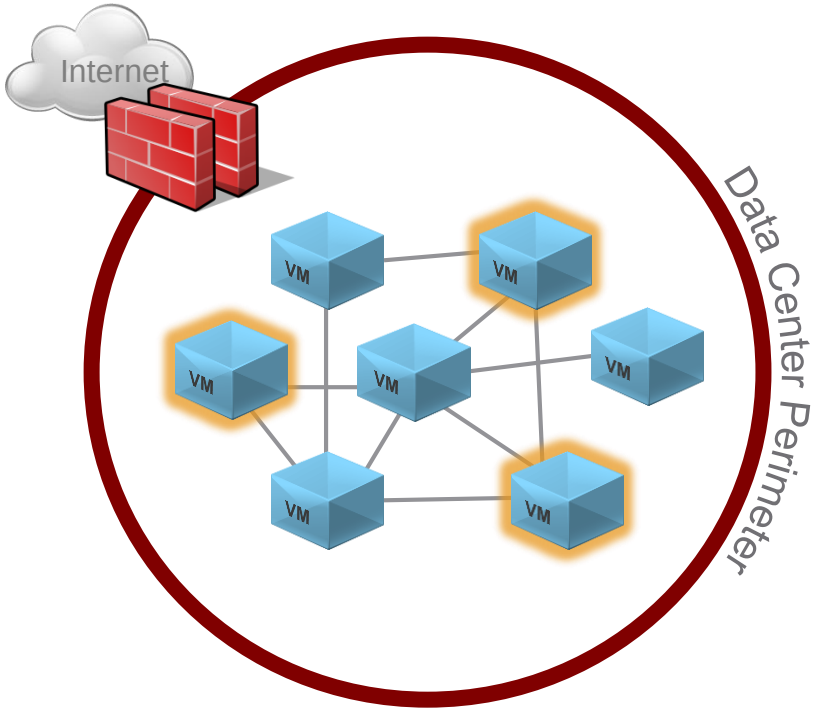
駭客入侵後通常不會聲張，僅會潛伏於現有系統內，或默默進行環境偵測

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

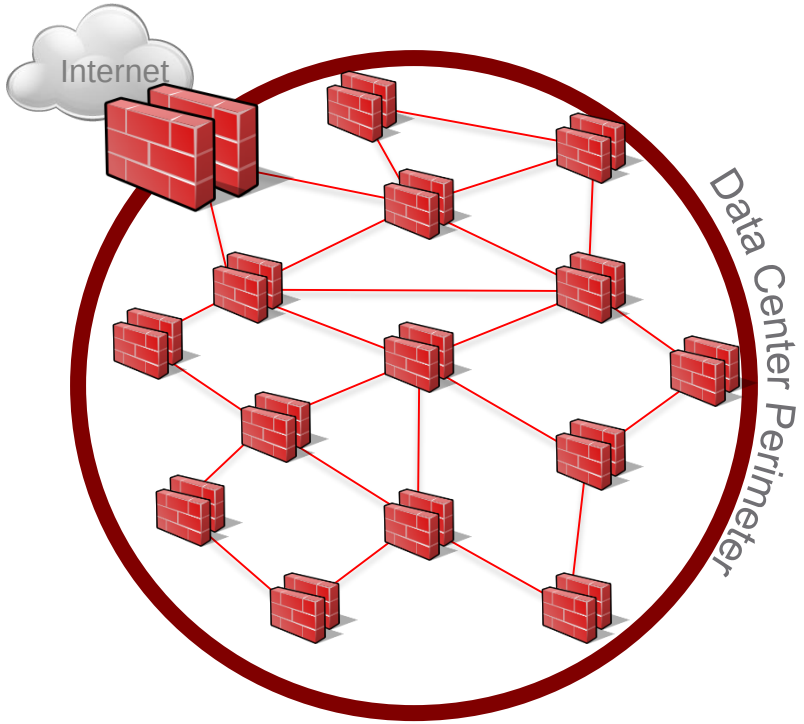
vmware

若需要達成完善的虛擬環境防護，需要能夠在資料中心內的每一個節點都有辦法進行安全防護控制

Now:

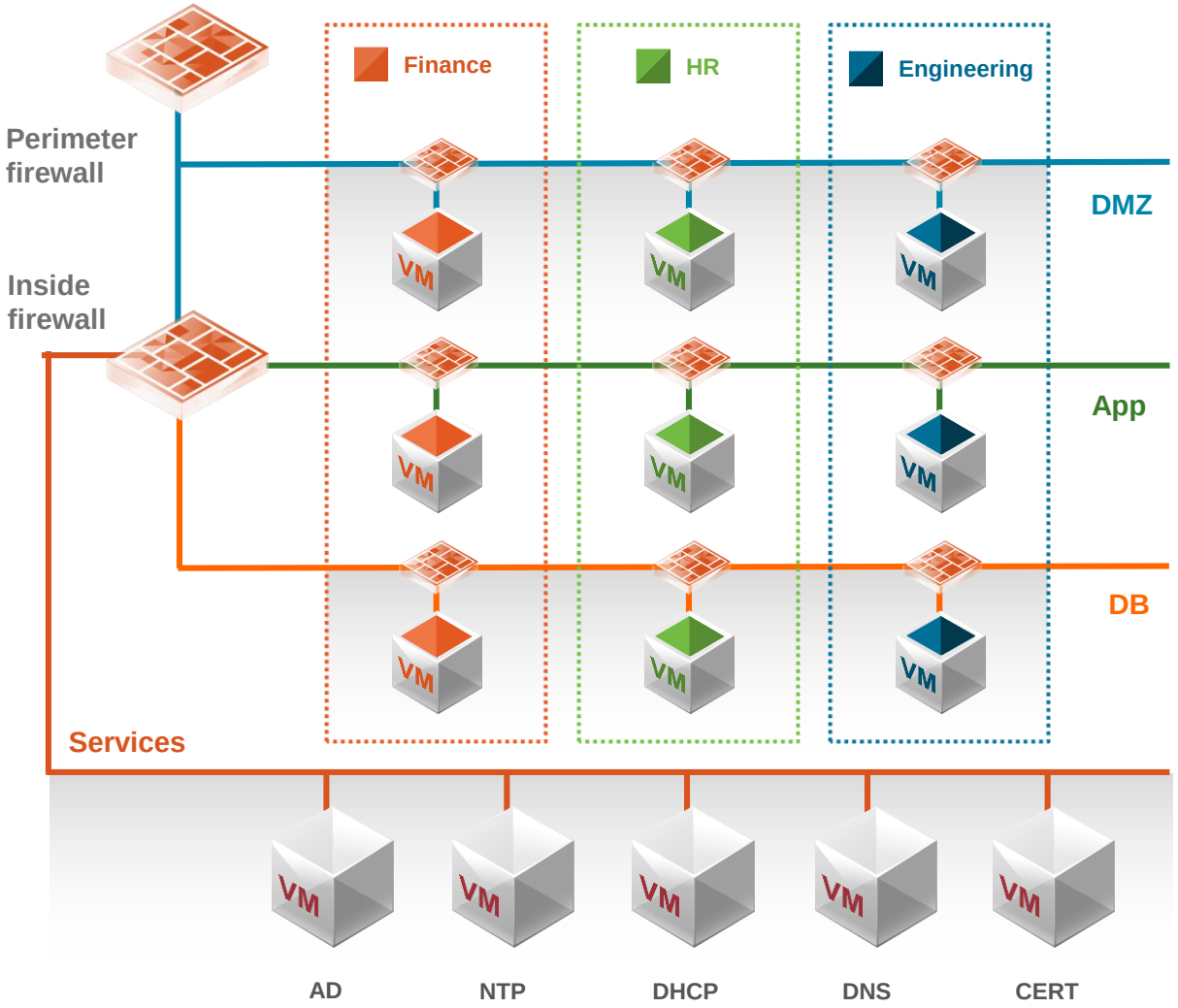


Become:



vmware

必須能夠在每一個機器前都提供安全防護，才能達成資料中心內完整防護機制



- 每一個虛擬機器成為自己的安全防護區，每個封包都能夠得到檢查
- 每一個虛擬機器前均能進行安全控制，無論兩個虛擬機器是位於同一網段或同一vSphere Host

vmware

“We cannot solve our problems with the same way of thinking that created them.”

– Albert Einstein

vmware®

VMware 軟體定義資料中心架構：把系統所需求的功能與硬體設備脫鉤，在軟體內建立並執行

軟體定義資料中心

業務系統

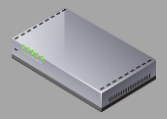
虛擬機器

虛擬網路
及安全

虛擬儲存

資料中心虛擬化

運算容量



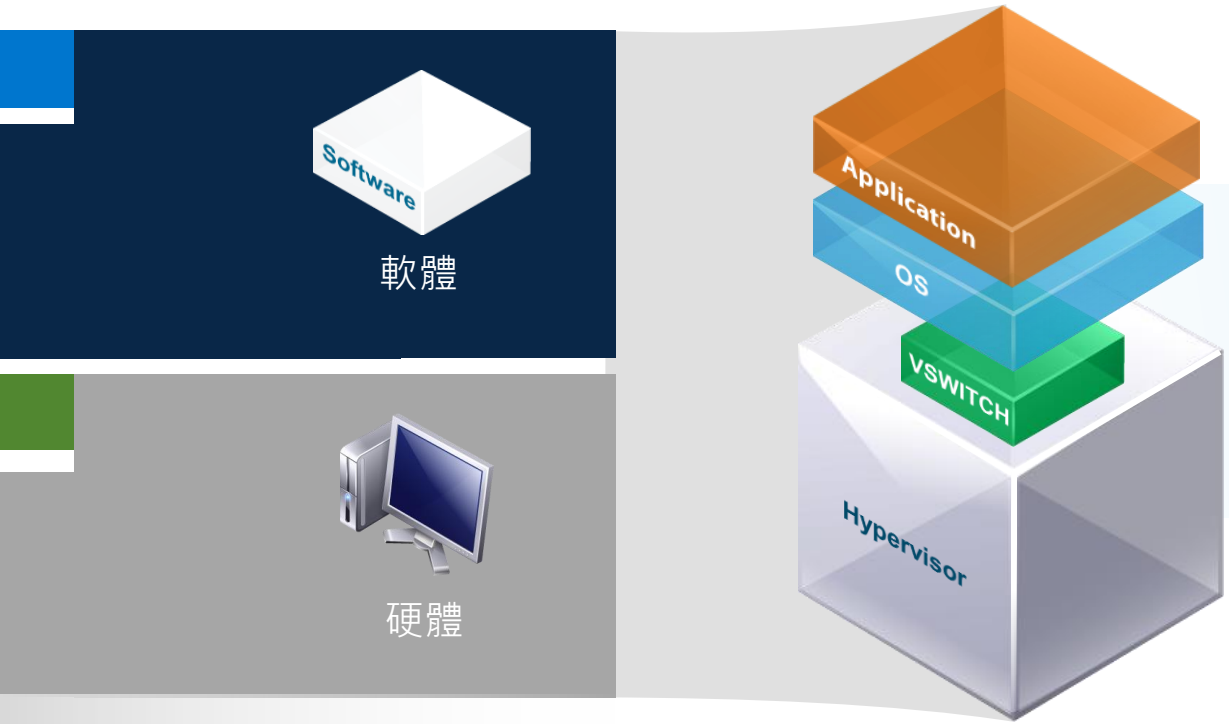
網路容量

儲存容量

不限定採用硬體與佈署位置

vmware

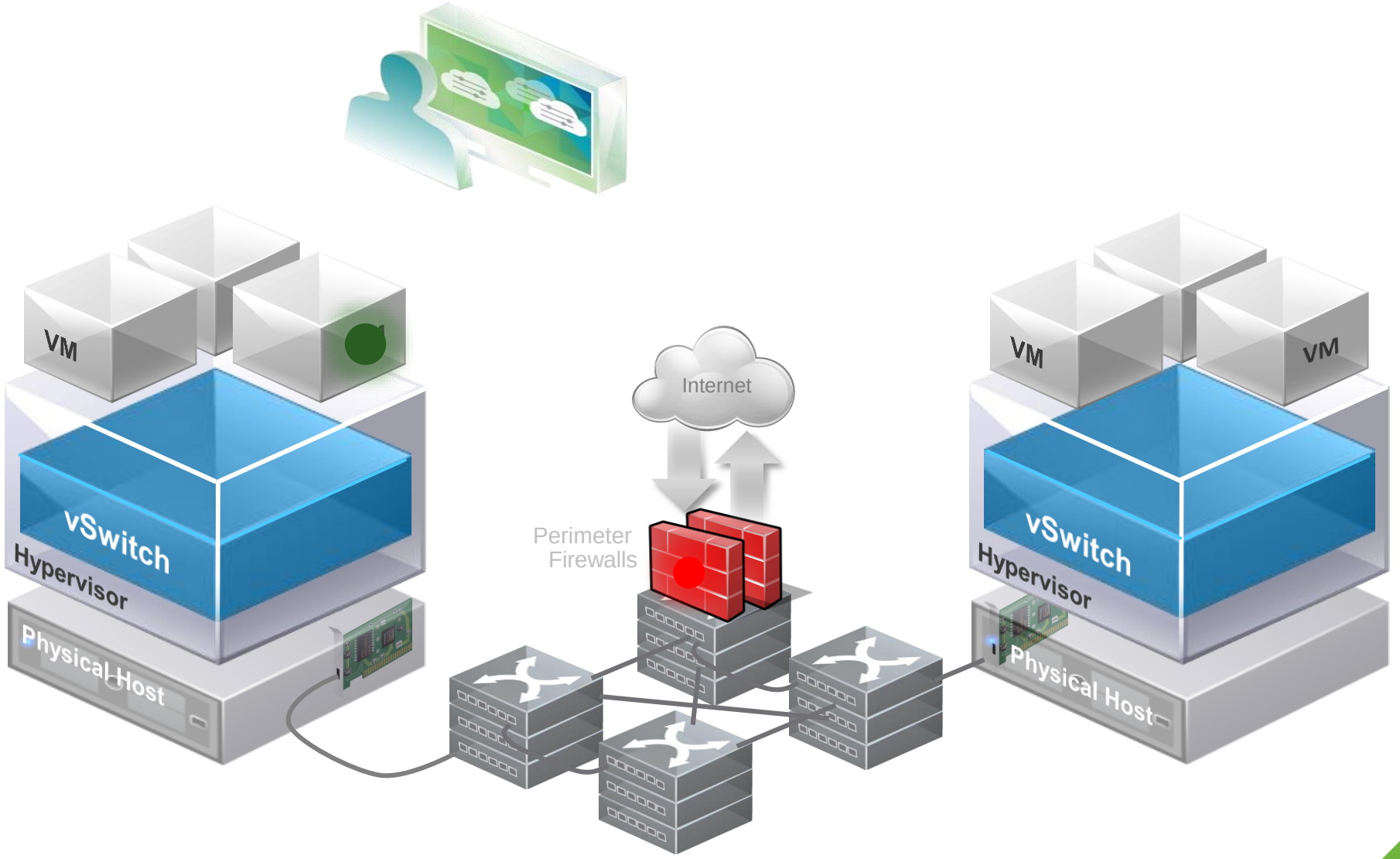
VMware NSX將資料中心所需求的網路與安全功能直接於vSphere Kernel內提供



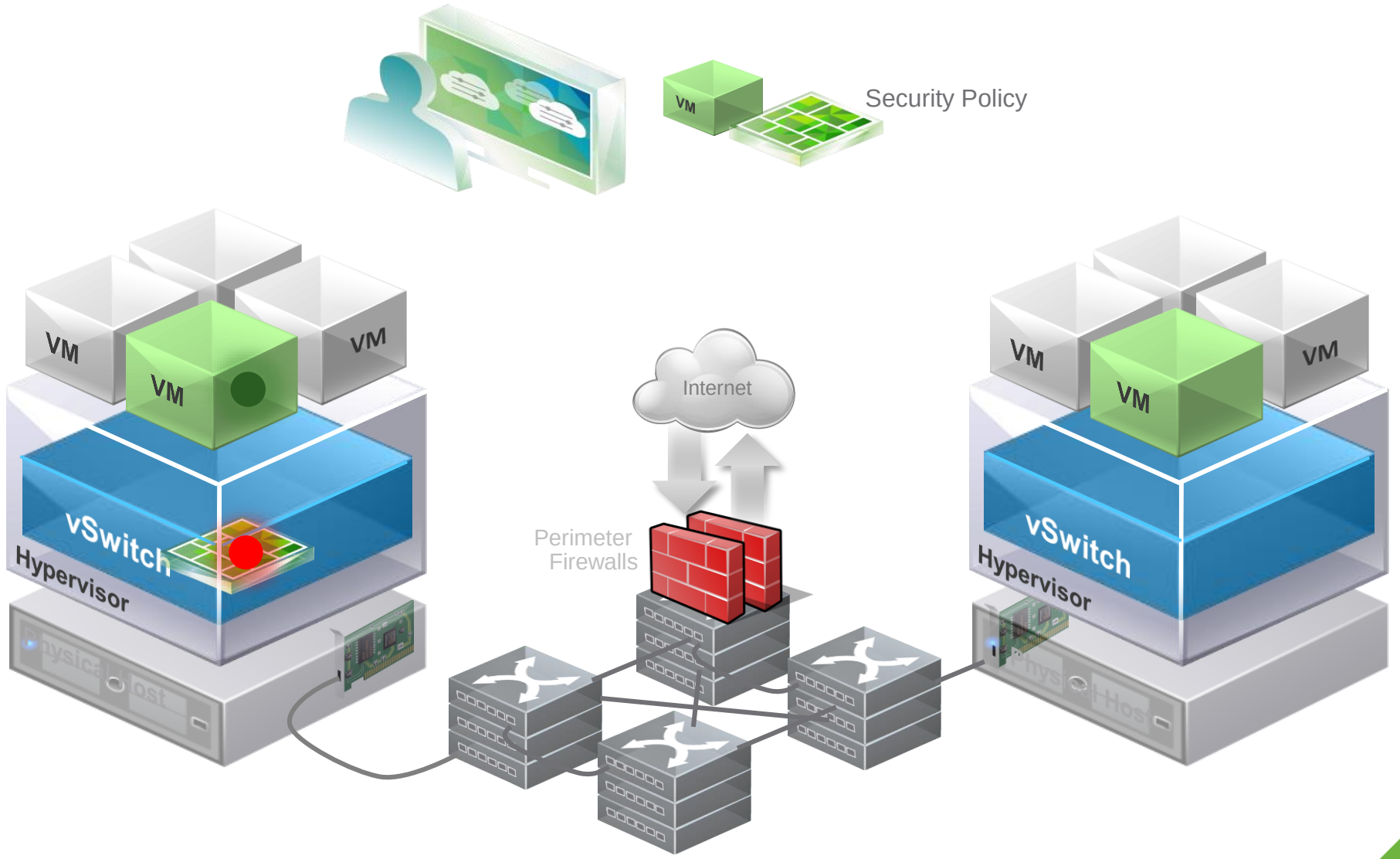
網路與安全功能於vSphere Hypervisor內運作

vmware

傳統實體防護架構：集中於邊界實體防火牆進行防護



微切分安全防護技術：封包檢查直接分散到每一台vSphere Host Kernel內運作，於每台虛擬機器前直接提供防護



vmware

VMware NSX不僅是提供基本的L4 Stateful防火牆防護，可同時搭配頂尖的安全廠商，提供最精細且強大的完整保護

NSX

Built-in Services

Firewall	Data Security
Server Activity Monitoring	VPN (IPSEC, SSL)

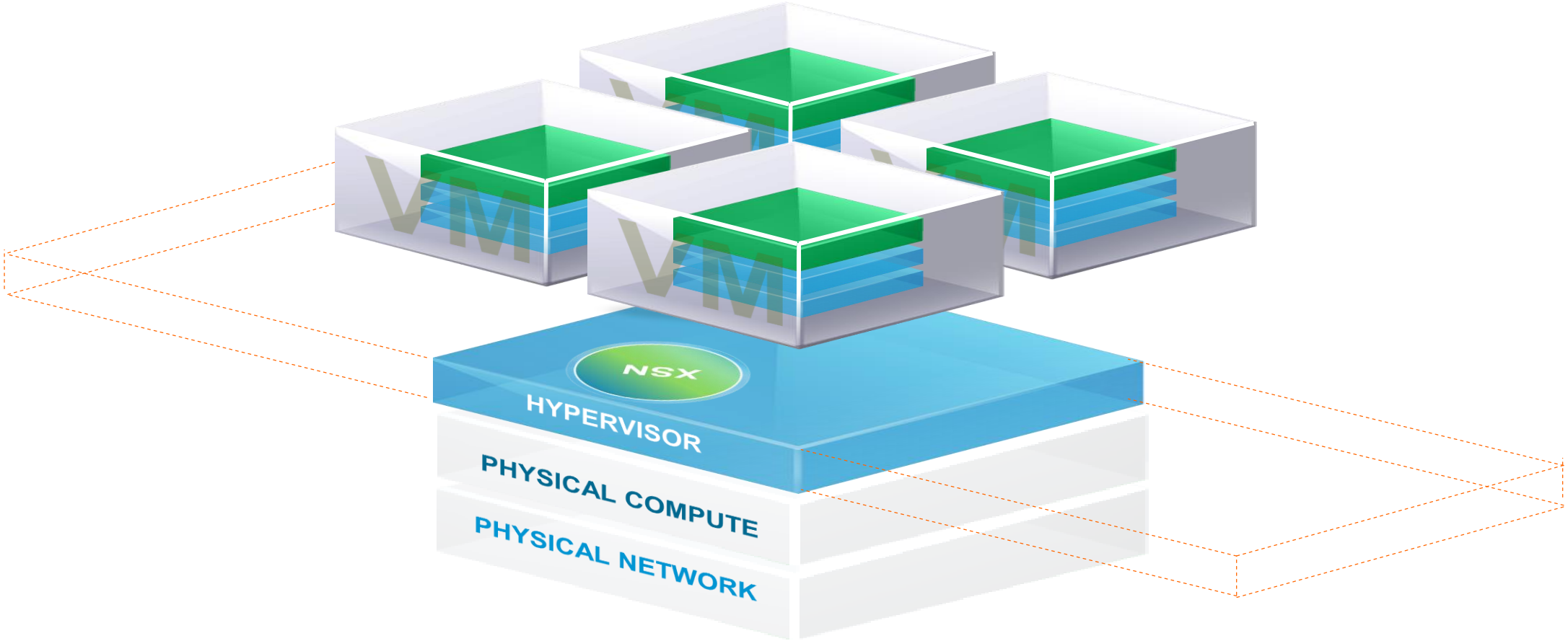
vmware NSX PARTNER

Third-party Services

Antivirus	Firewall	Intrusion Prevention
Security Policy Management	Vulnerability Management	Identity and Access Mgmt
…and more in progress		

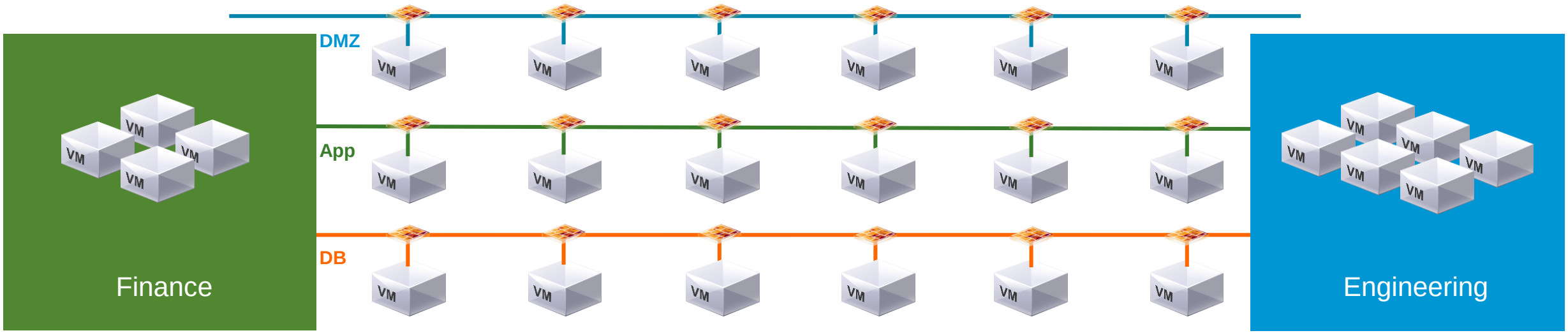
vmware

在vSphere Host Kernel內進行安全防護的另一層意義：安全防護可以與網路脫鉤，直接與業務應用或資訊系統進行對應

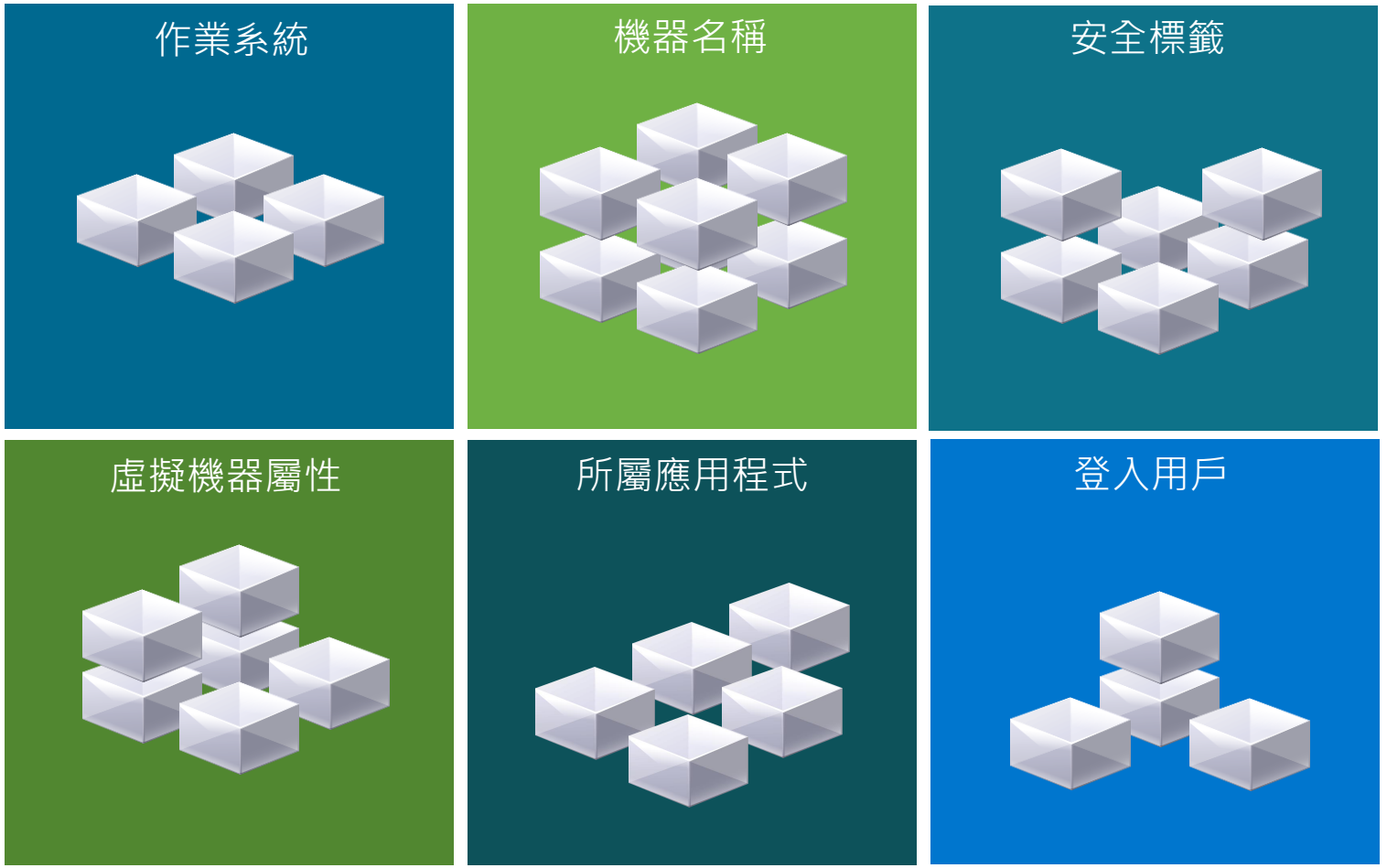


vmware

IT單位能夠直接將要保護的目標以自動化的安全群組形式進行定義，無需再用網路地址的方式進行指定



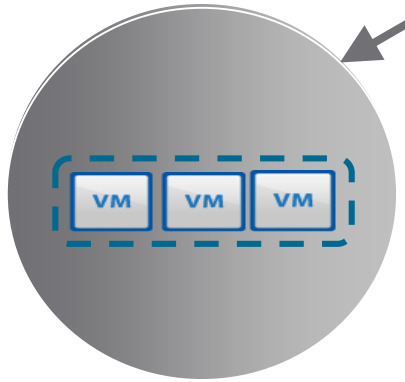
NSX架構內，管理者可以用多樣性的動態條件來建立自動化安全群組



vmware

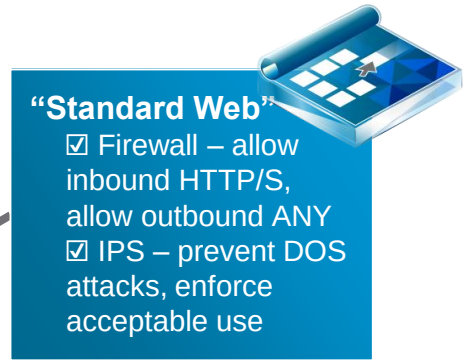
藉由將業務與資訊系統以自動化安全群組建立關聯，可直接指定對應此業務/資訊系統的安全防護政策，與網路完全脫鉤

- 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？



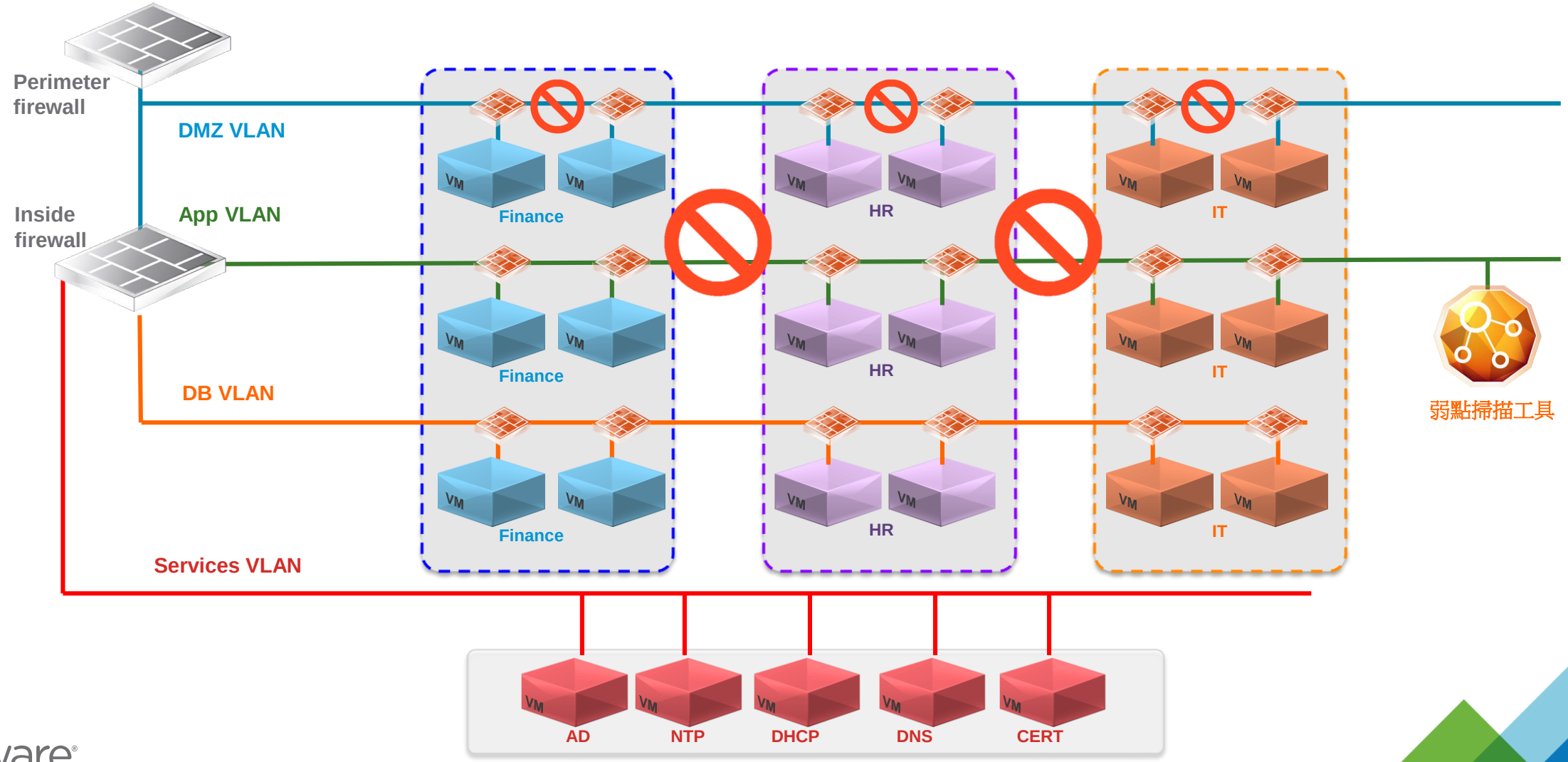
Security Policy：

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？

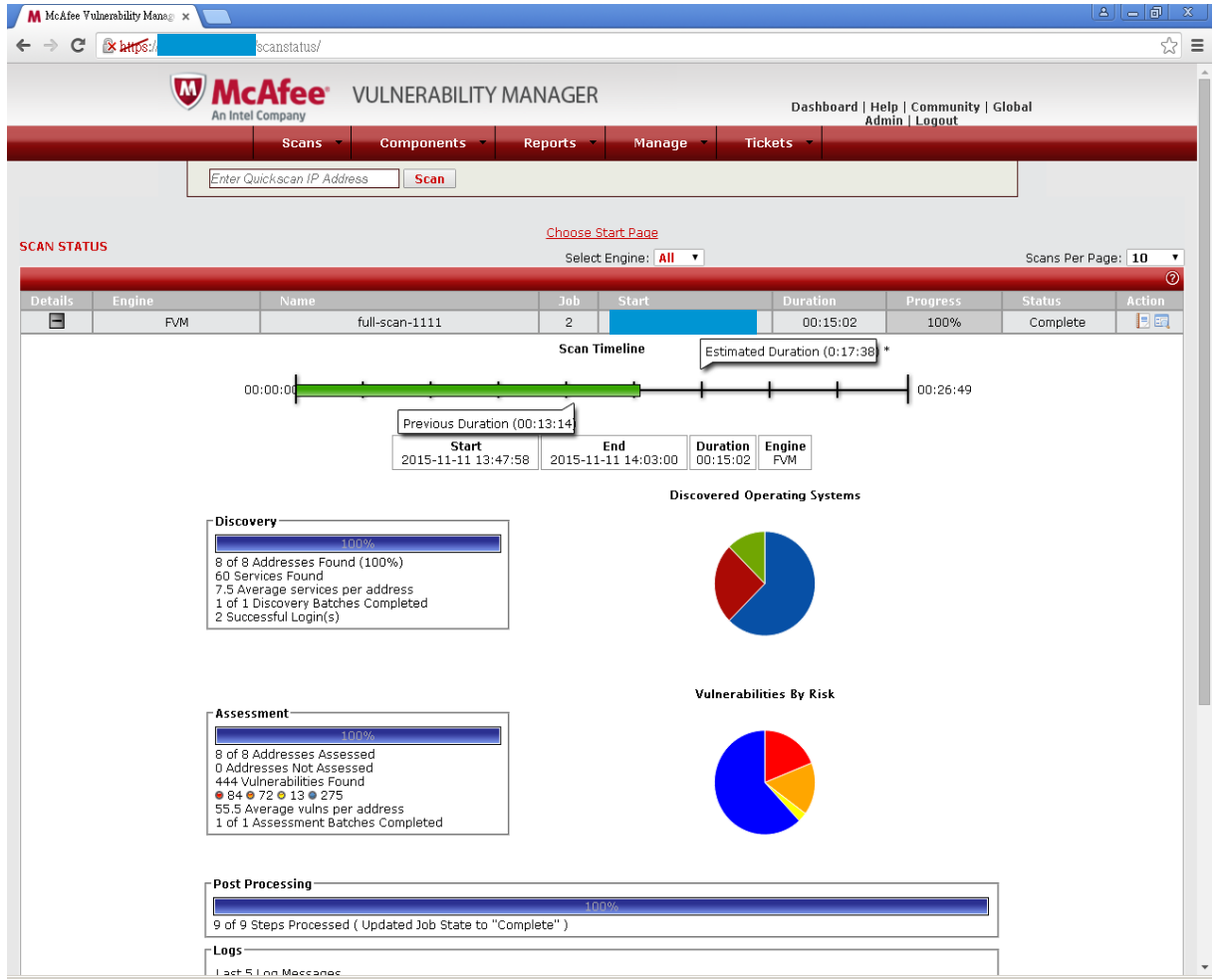
vmware

VMware NSX 微切分技術於台灣客戶實際應用場景：
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

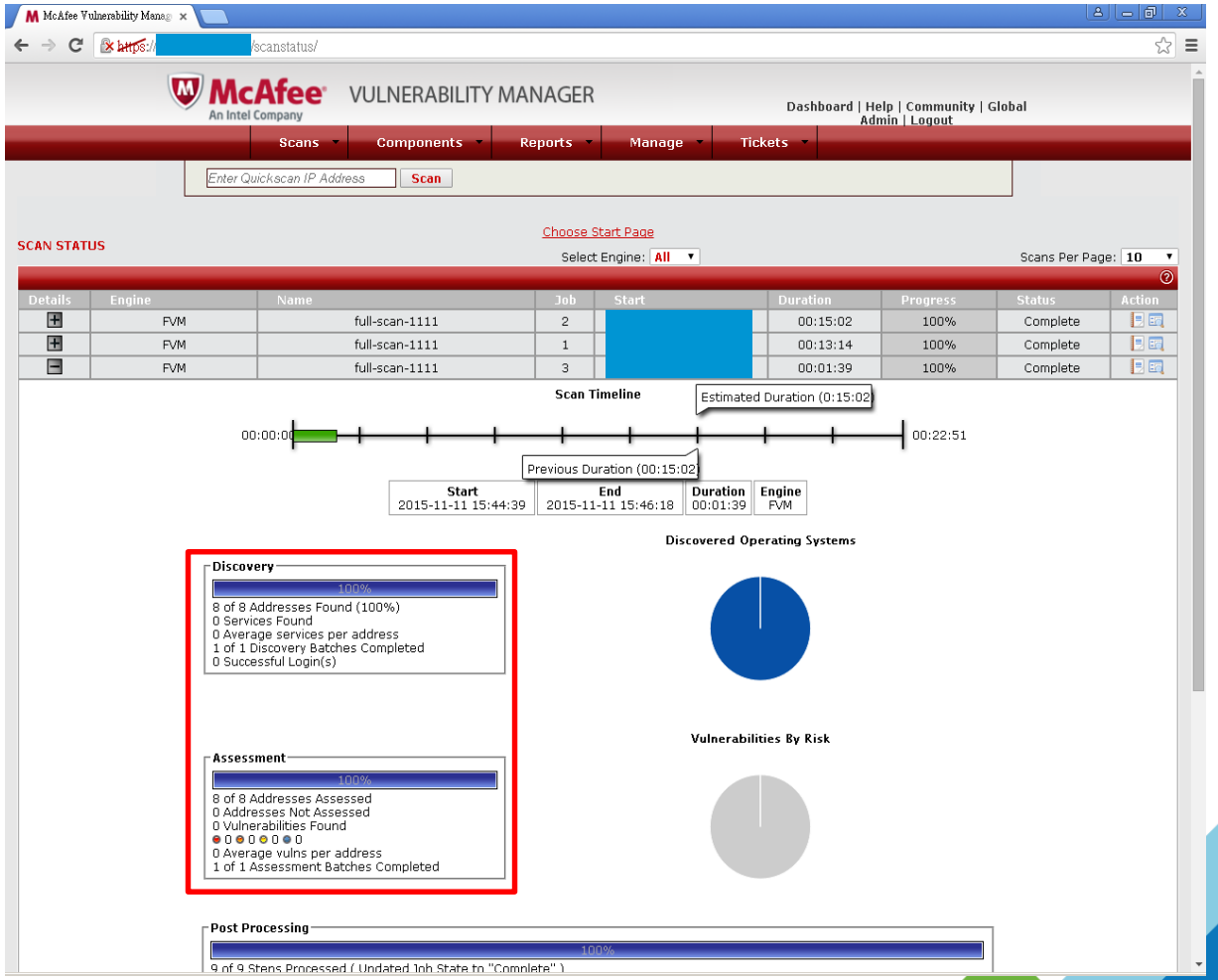


於財金資訊實際驗證：
以VMware NSX完整設定系統網路流白名單，透過標準弱點掃描工具驗證防護功能

NSX 防護前

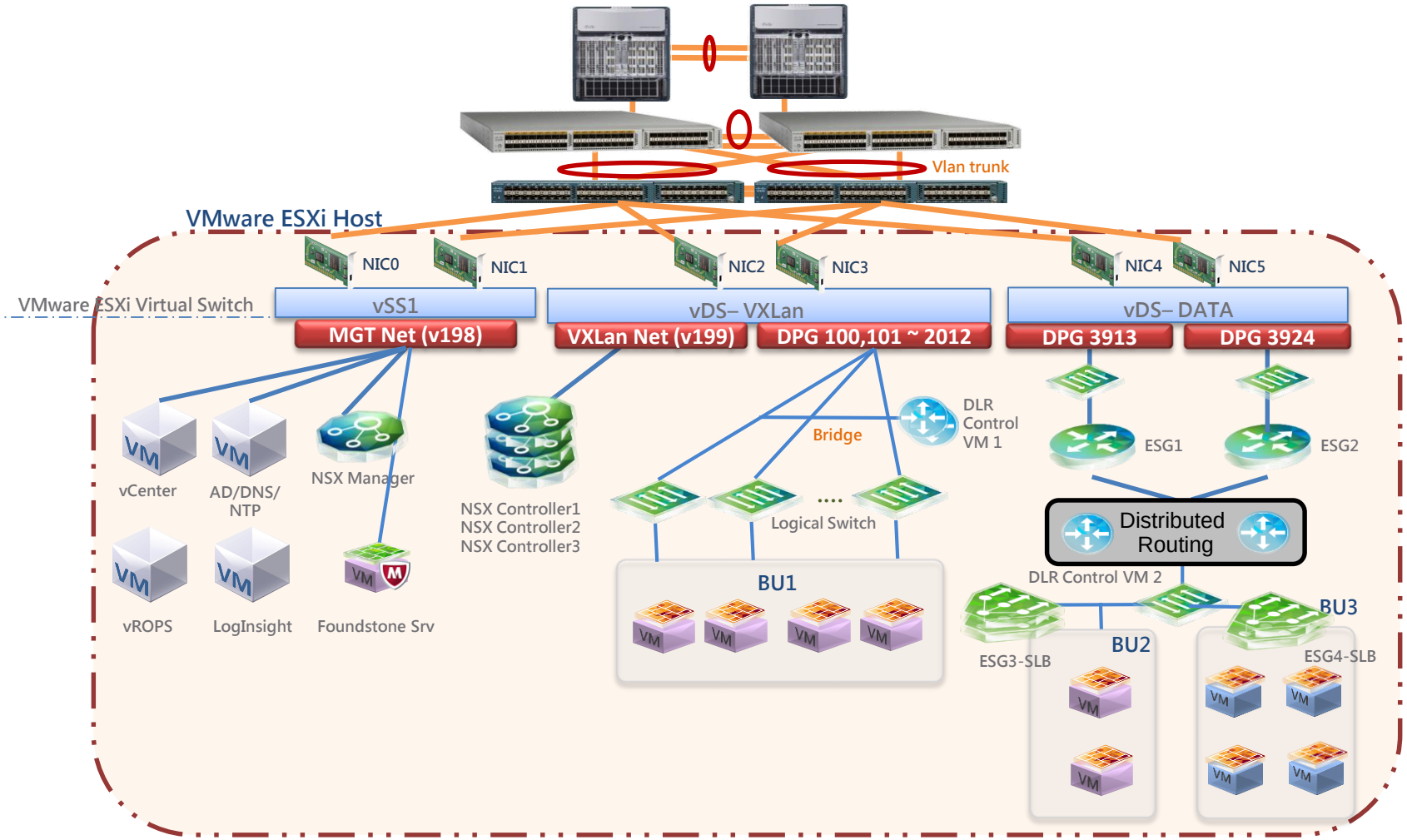


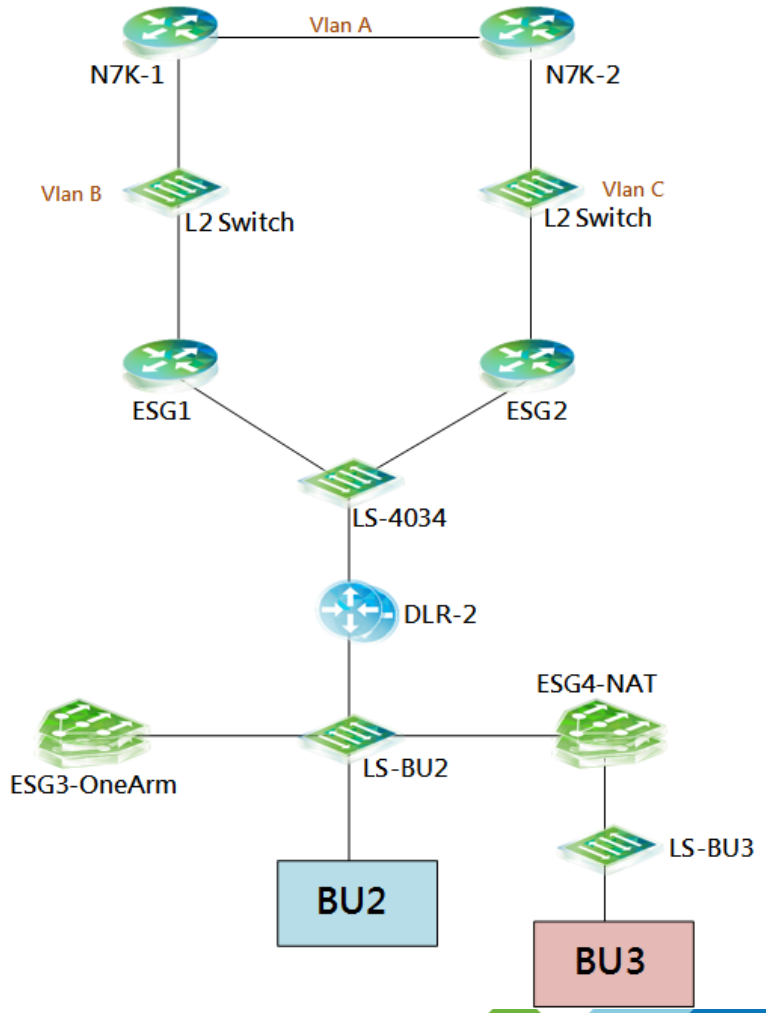
NSX 防護後



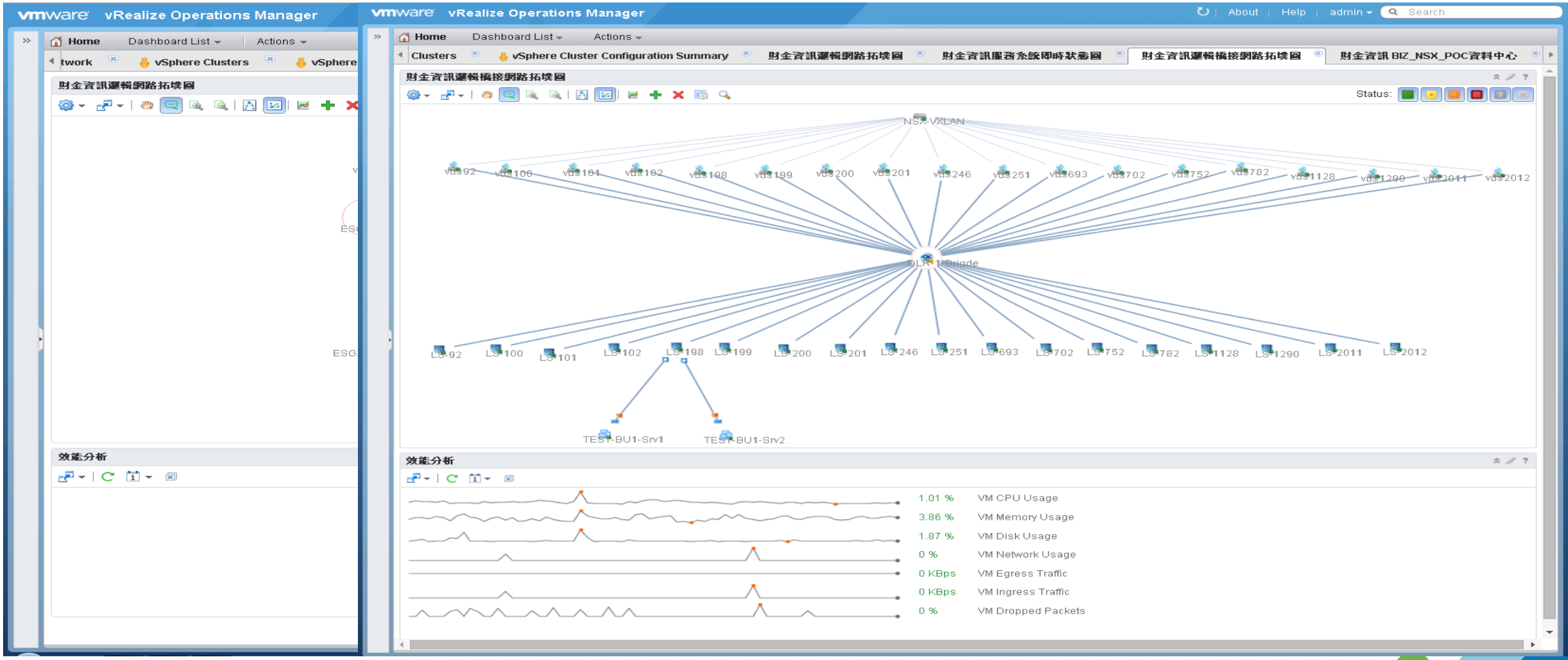
vmware

於財金資訊實際驗證：
於現有的Cisco網路環境與UCS刀鋒交換器內，建立完整的功能測試

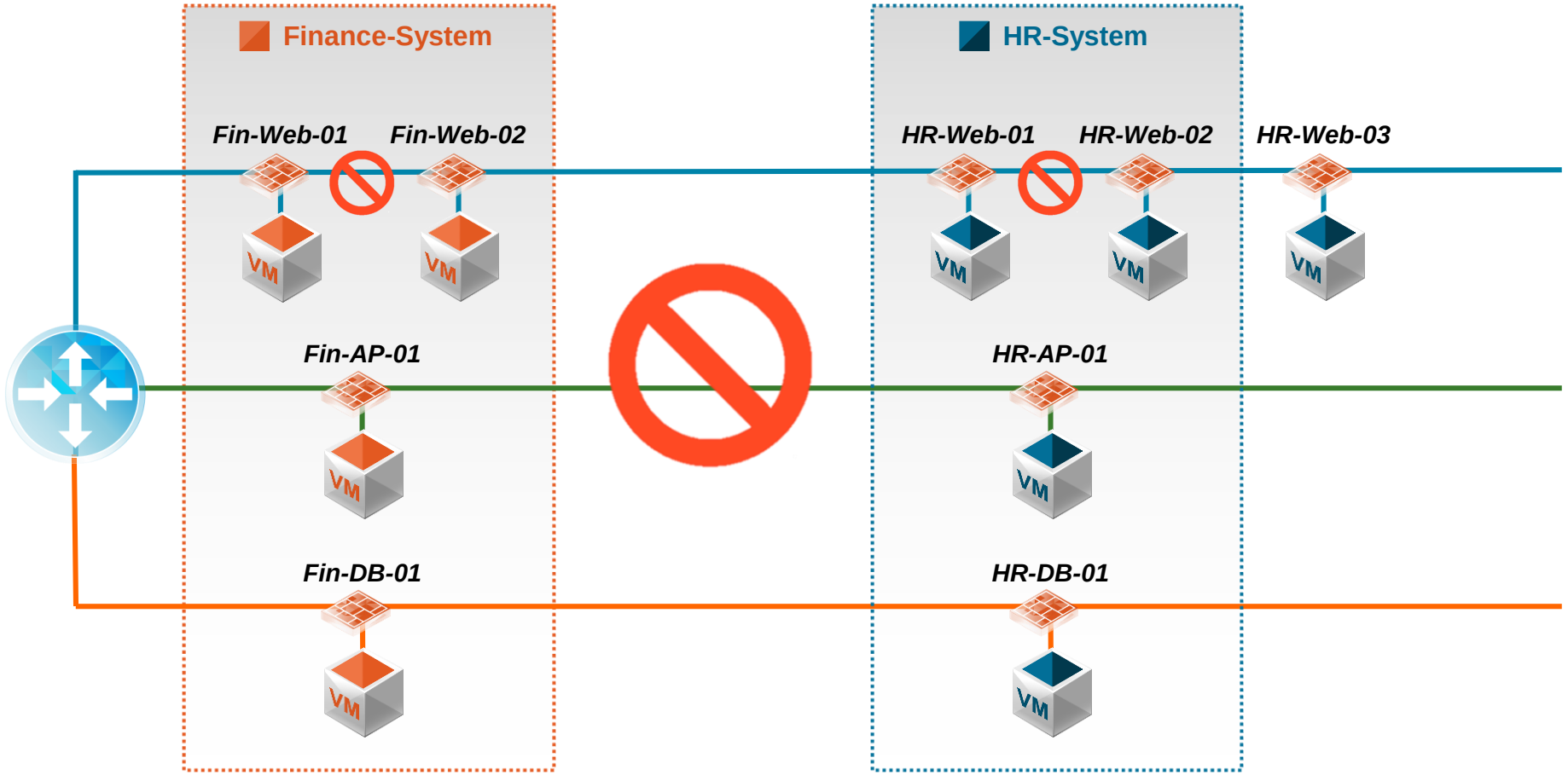




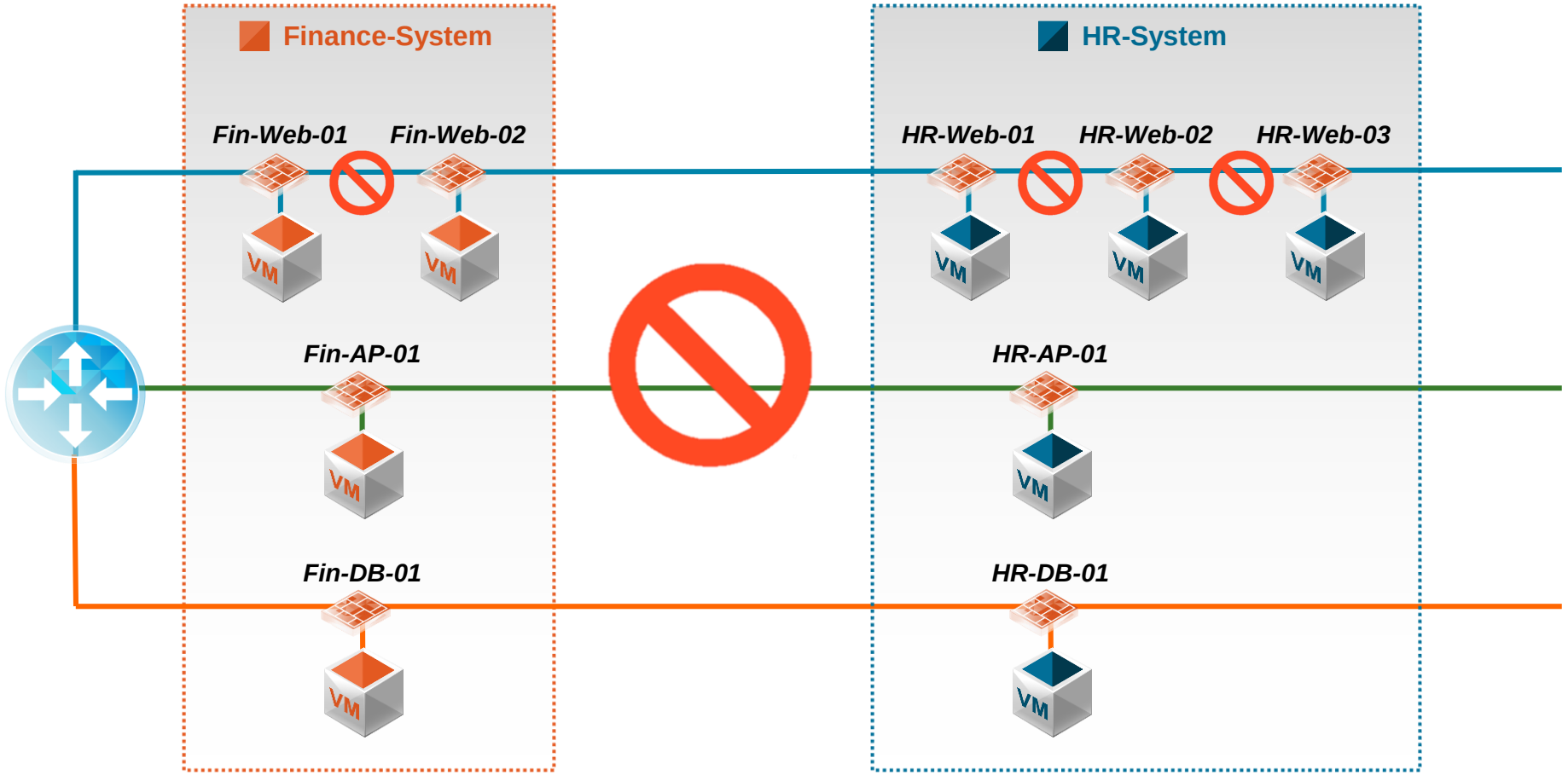
於財金資訊實際驗證：
整合現有軟體定義資料中心構件，快速檢視現有網路架構



VMware NSX 微切分技術於台灣客戶實際應用場景：業務系統擴充時，新的虛擬機器自動加入安全群組



VMware NSX 微切分技術於台灣客戶實際應用場景：
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



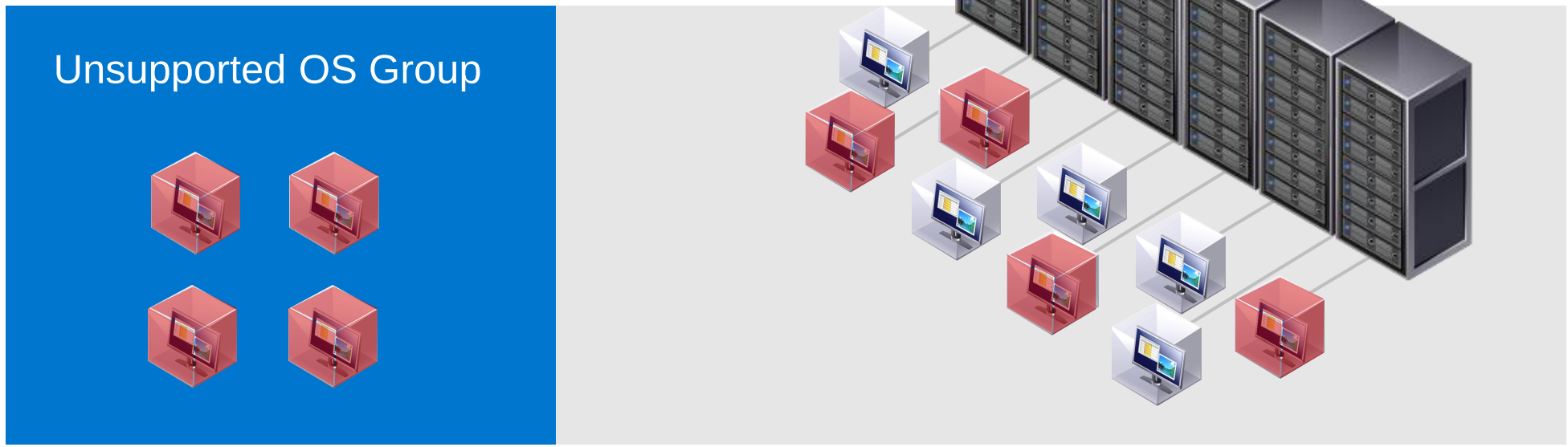
vmware

VMware NSX 微切分技術於台灣客戶實際應用場景：快速找出已經End-of-Support的作業系統，並禁止訪問Internet

客戶狀況

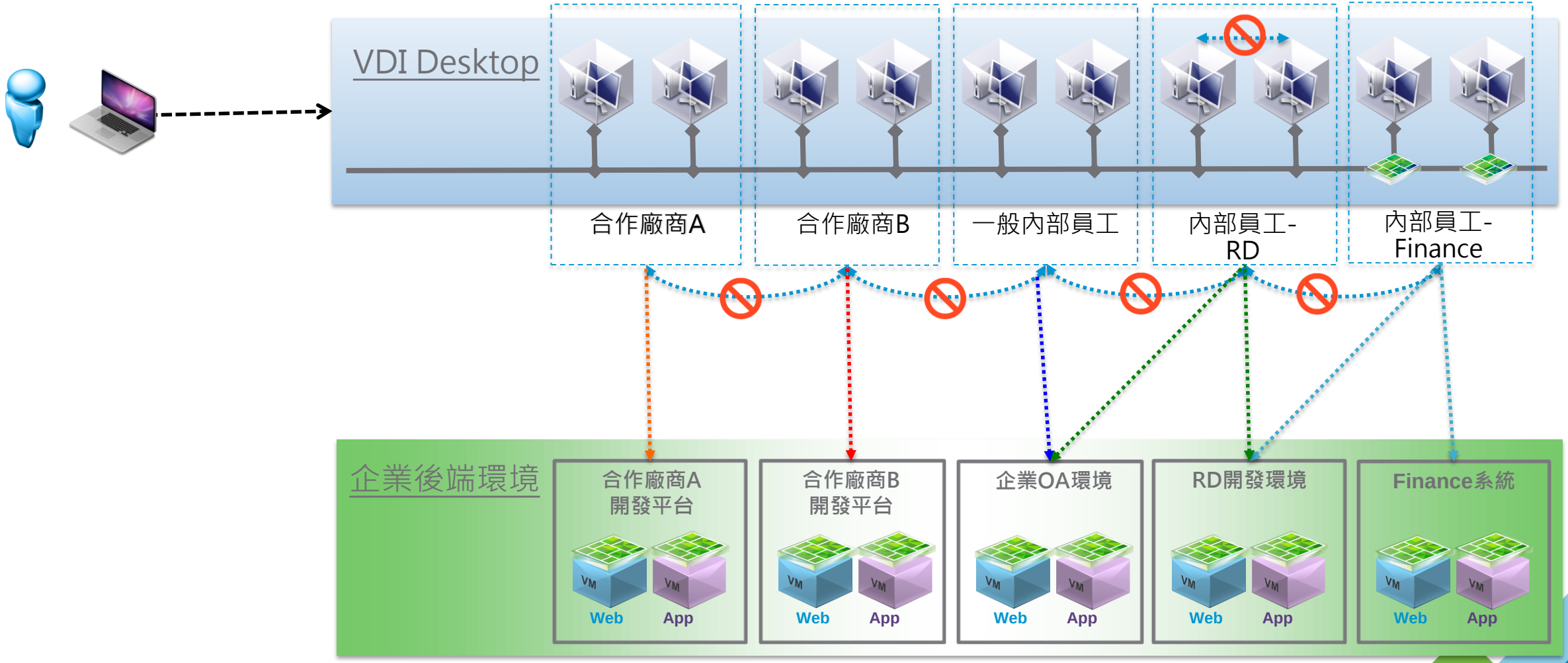
安全政策禁止使用已經End-of-Support的作業系統

若有此類作業系統機器，完成升級前禁止連接至Internet



vmware

VMware NSX 微切分技術於台灣客戶實際應用場景：
搭配虛擬桌面方案，依據用戶身份限制可連入的系統與網路環境



結論：藉由VMware NSX微切分架構，我們能夠協助您的資料中心達成

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
- 或利用虛擬環境內的參數或知識進行設定

自動化達成安全設定

- 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

整合頂尖第三方安全機制

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

vmware

READY
FOR ANY
vForum2015