VMware NSX 保護校園資訊
抵禦外部攻擊的網路安全架構簡述

2017年11月3日
VMware 台灣

林俊谷

vmware

現在 VMware Inc.

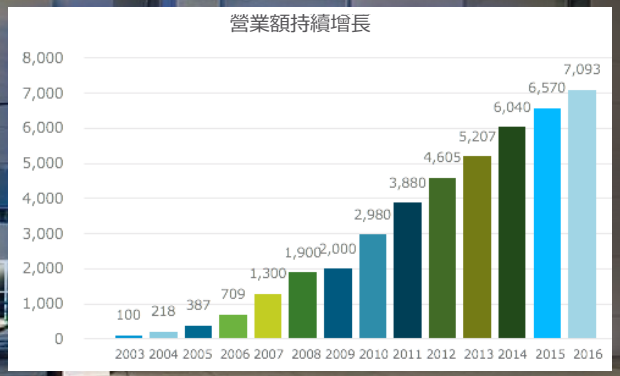
vmware

約71億美金
2016會計年度
營業額

8%
銷售增長率

20,000+人
員工數

約2,400客戶
（同期年增長50%）
網路與安全虛擬化

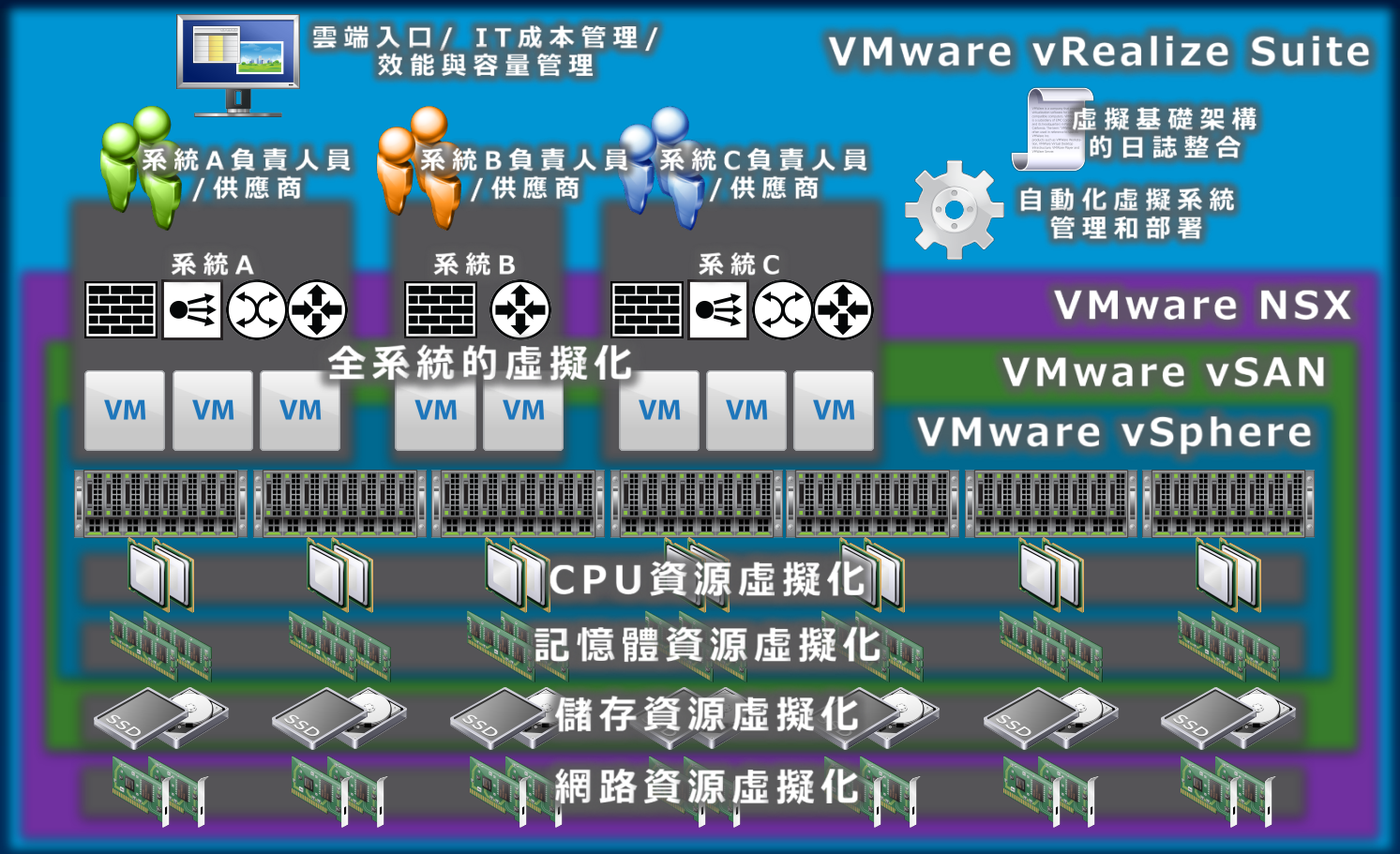


No,1

x86伺服務器虛擬化軟體
客戶端虛擬化軟體
企業行動管理
資料中心自動化軟體
雲端資訊系統管理軟體

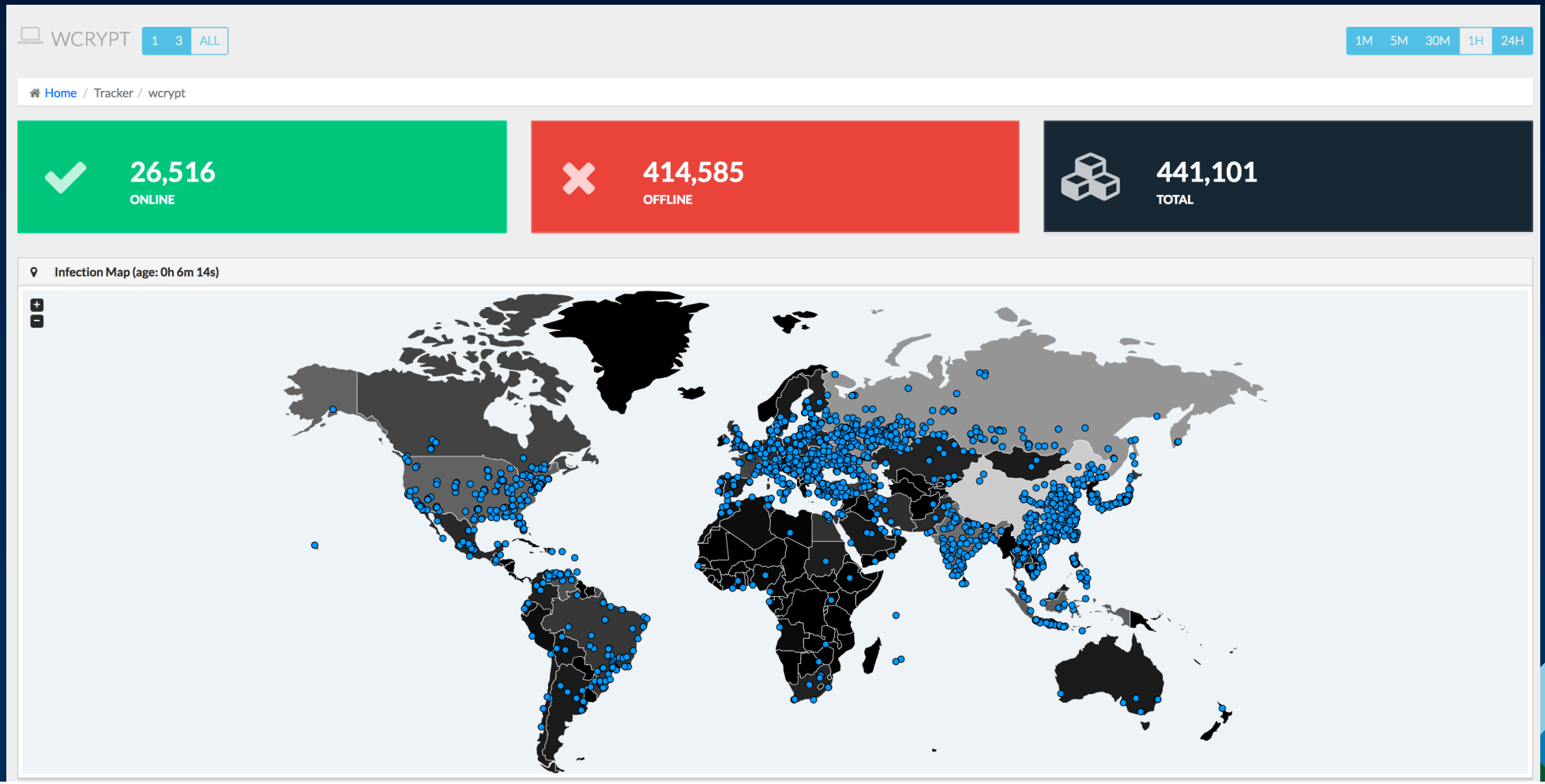
約7,000客戶
（去年150%成長）
儲存虛擬化

通過從實體資源虛擬化的初衷延伸至完整的SDDC雲端架構



全球受到WannaCry病毒(勒索病毒)的衝擊

目前已有100多個國家和地區超過三十萬台電腦被勒索病毒所感染。



標的型攻擊在沒有充足的防範措施下結果

被入侵後反應過慢

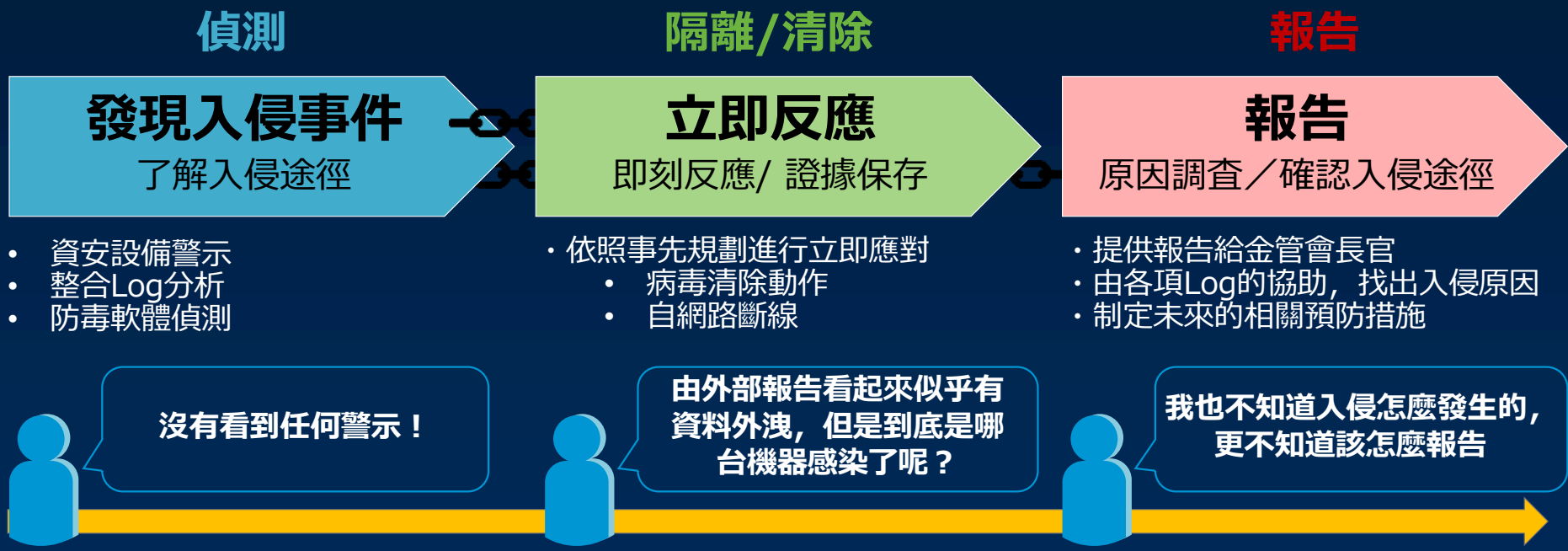
標的型攻擊的侵入
企業能察覺的比例

檢測出來的平均天數

早期發現很困難, 因為內部防範措施是脆弱的

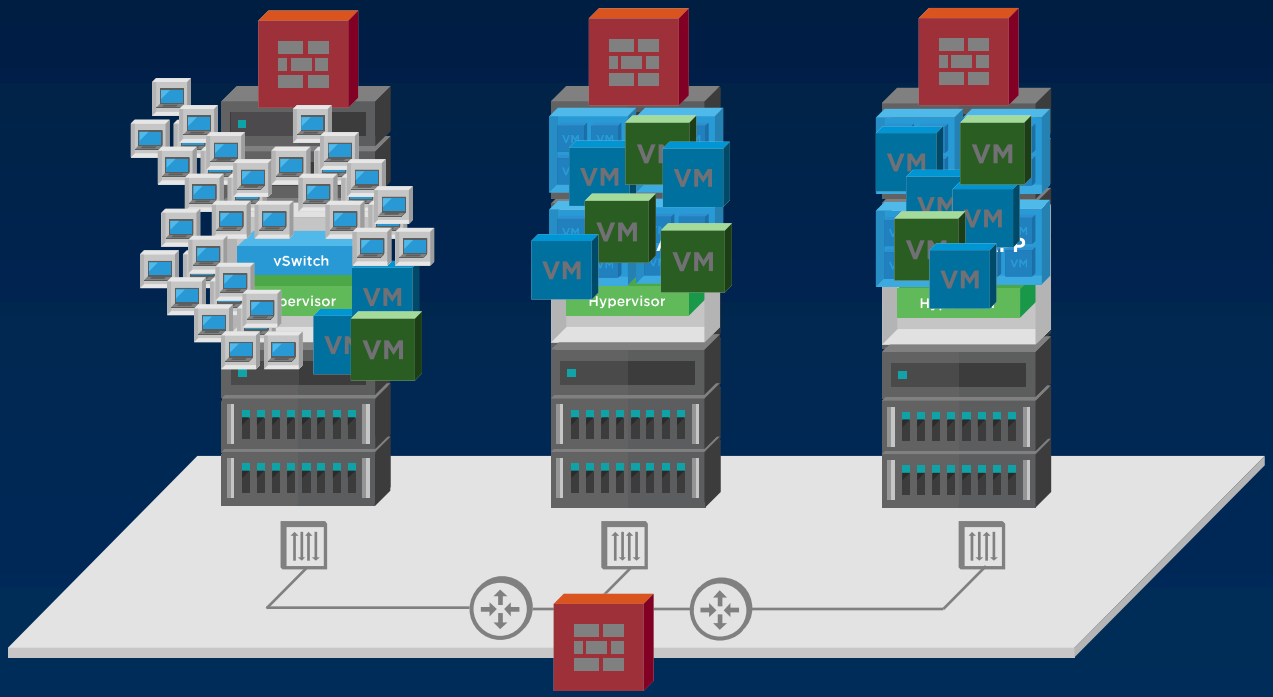
vmware®

為什麼標的型攻擊是個頭痛的問題？



如果無法偵測入侵事件，就無法反應並報告。
當偵測到入侵時，必須立即想到資料外洩的可能

資料中心有什麼問題?



基礎架構的性質已發生變化…

終端用戶基礎架構

應用基礎架構

傳統端末

移動裝置

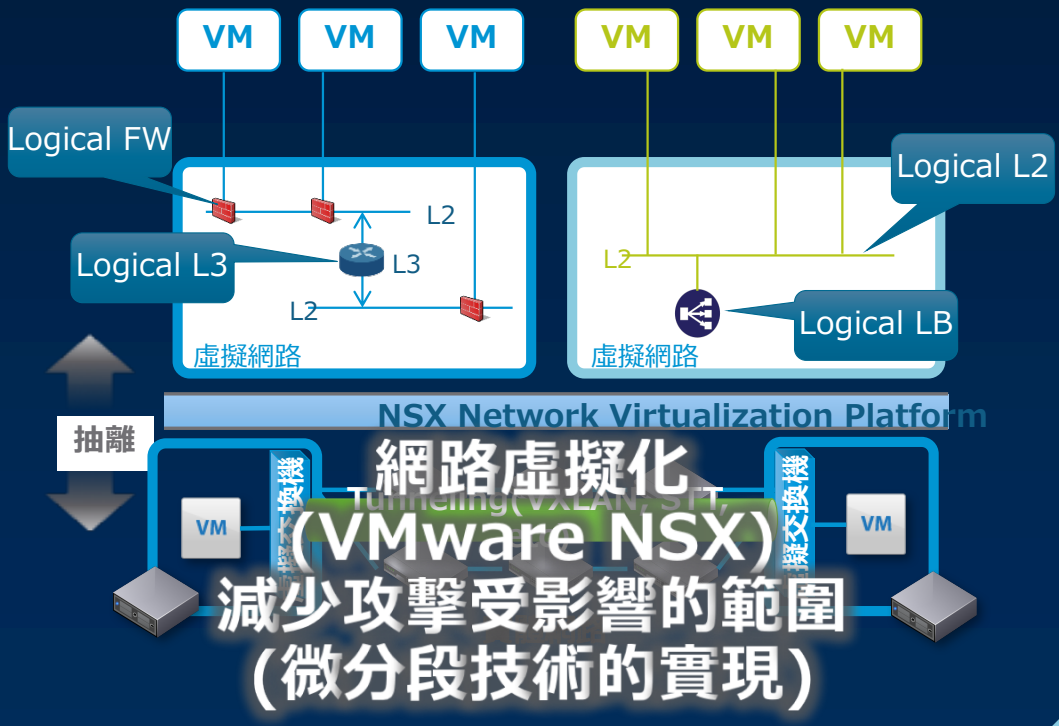
BYOD：自帶設備

COPE：企業所有，個人使用

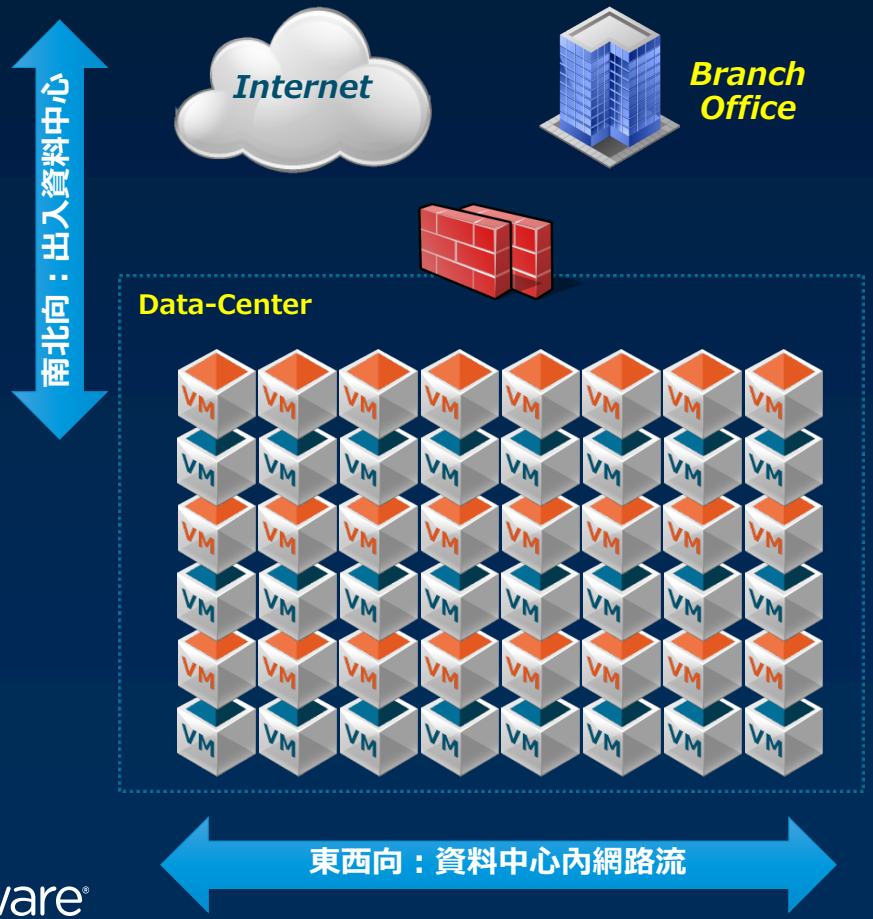
資料中心有其獨特的安全挑戰性


ALIGN
CONTROLS
網路
運算
APP
最適權限
網路
運算

網路犯罪攻擊數據中心因應對策by VMware
～桌面虛擬化和網路虛擬化



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

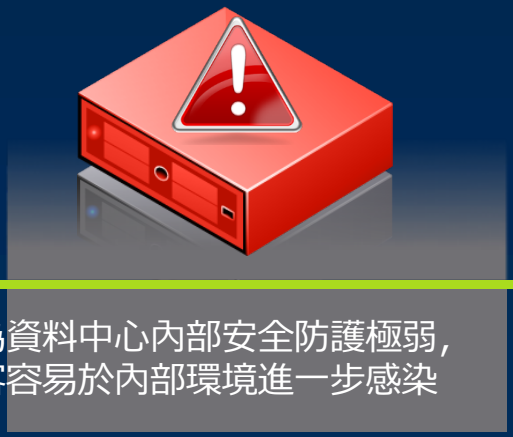
vmware

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



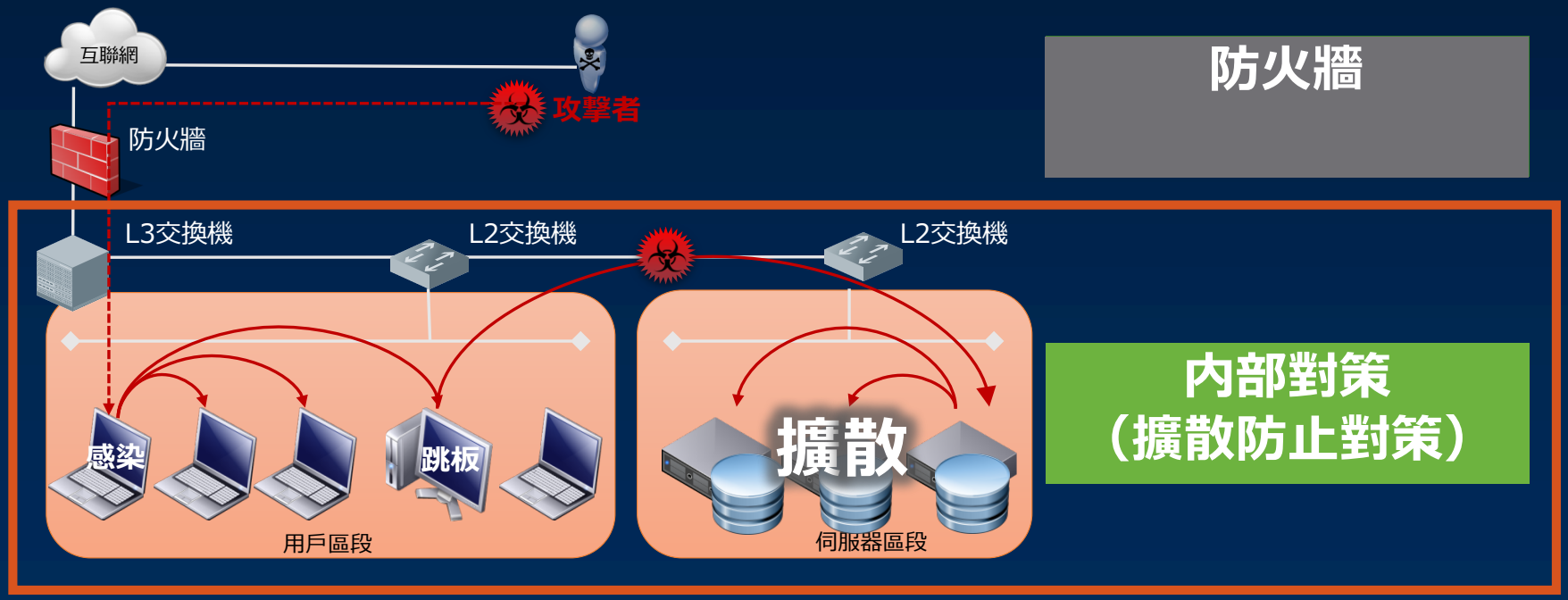
因為資料中心內部安全防護極弱，駭客容易於內部環境進一步感染

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

假設可能被感染前提下如何避免數據洩漏的對策

重要的是在三個層面有明確的措施



防火牆

內部對策
（擴散防止對策）

使用
防毒軟體

vmware

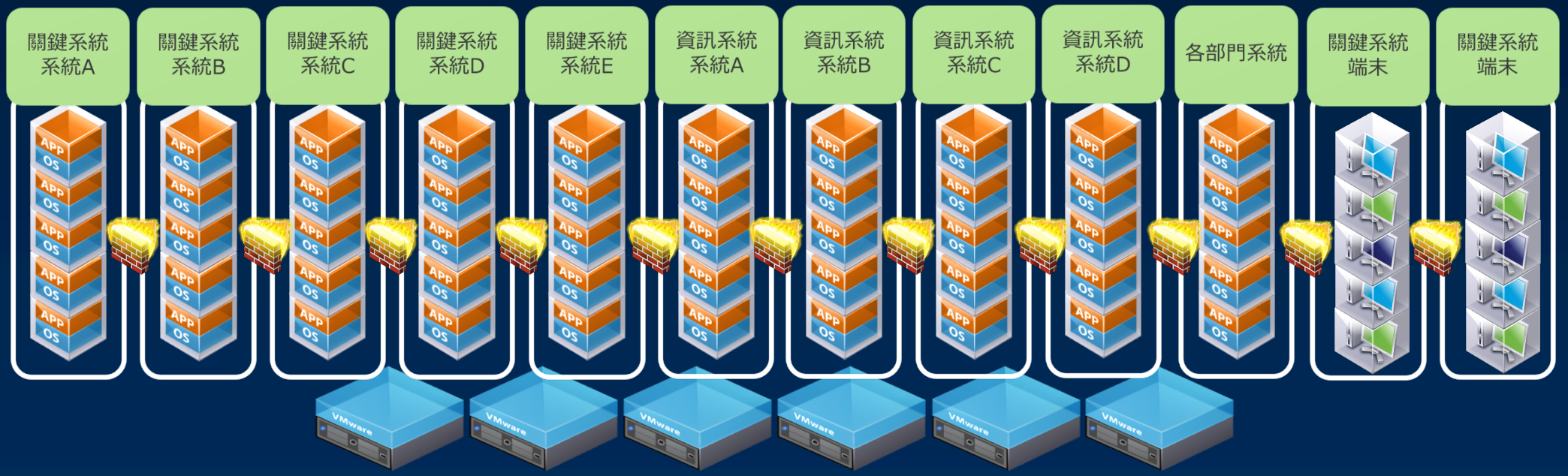
內部對策
（擴散防止對策）

利用網路虛擬化阻隔不必要的網路流量

透過微分段技術防止病毒蔓延

vmware®

網路虛擬化技術
~加強網路安全

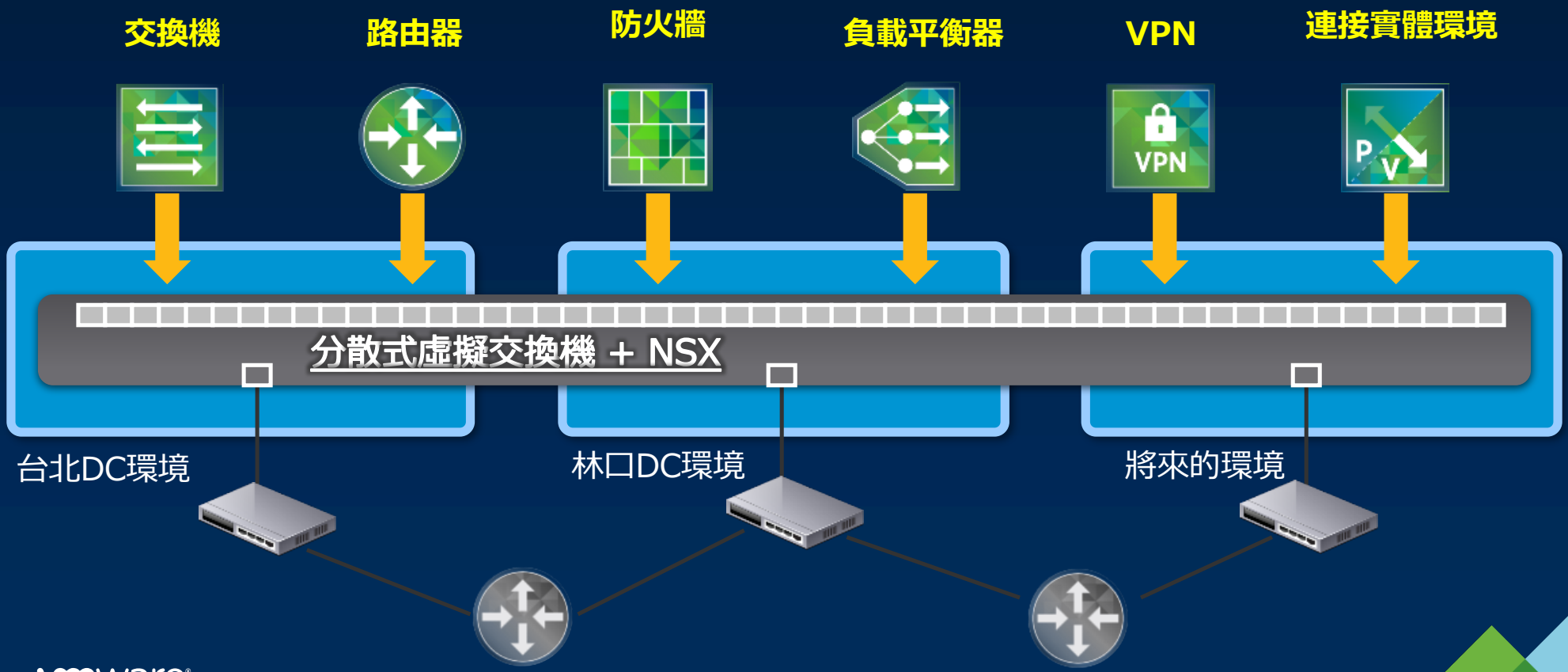


利用網路虛擬化功能的技術（分散式虛擬防火牆）
改進虛擬機彼此間的隔離

vmware®

NSX 將各種網路功能組件進行抽象化

進入SDDC的必然途徑

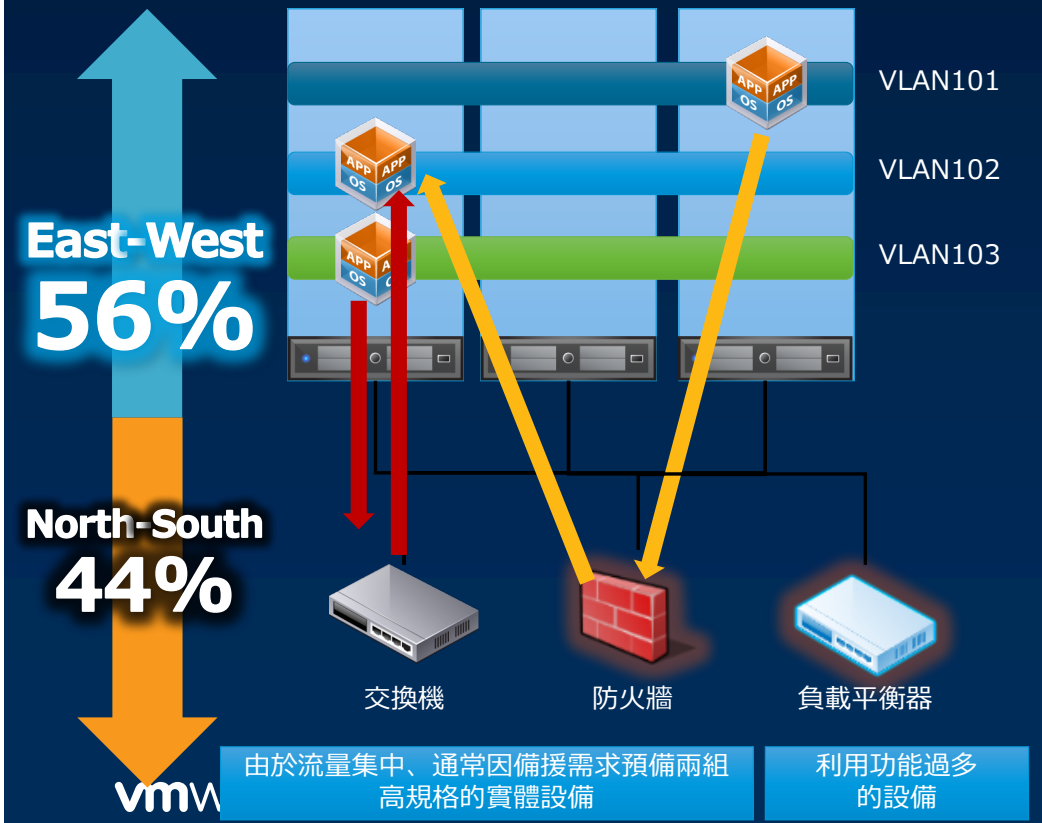


使用網路虛擬化節約成本

減少經過實體網路設備的流量/網路功能的虛擬化(NFV)

僅實現運算資源虛擬化

「一般網路配置」

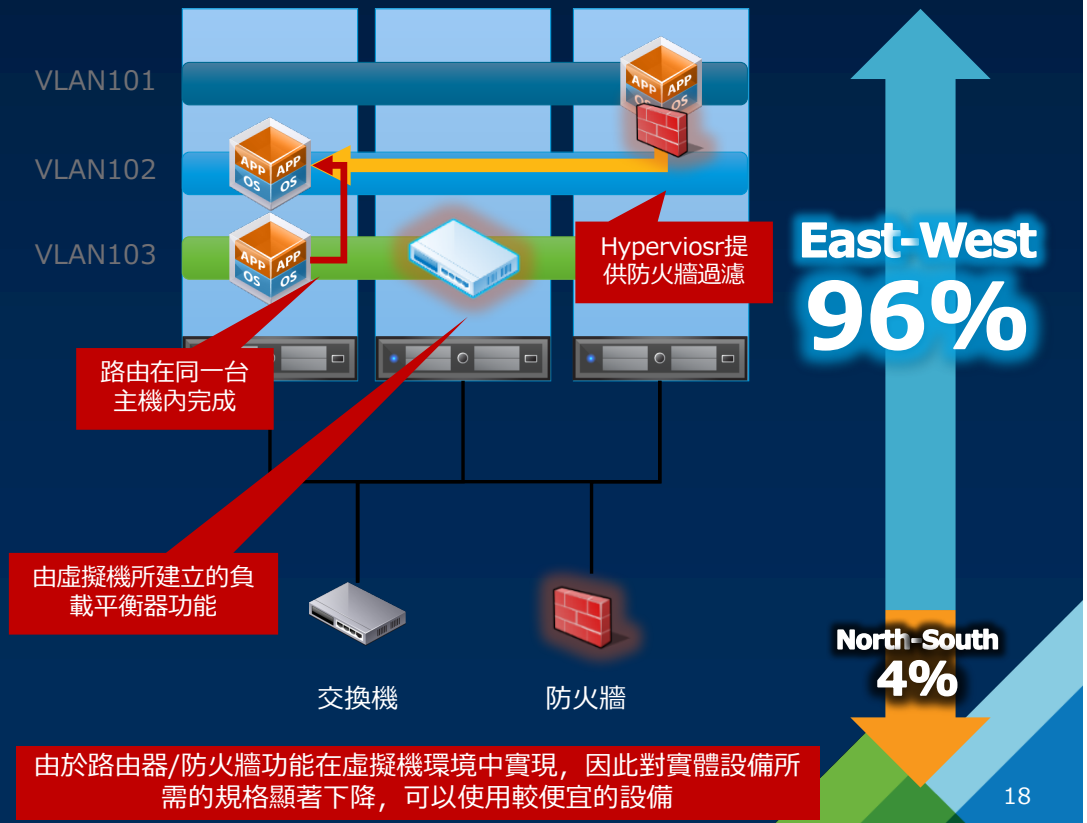


由於流量集中、通常因備援需求預備兩組高規格的實體設備

利用功能過多的設備

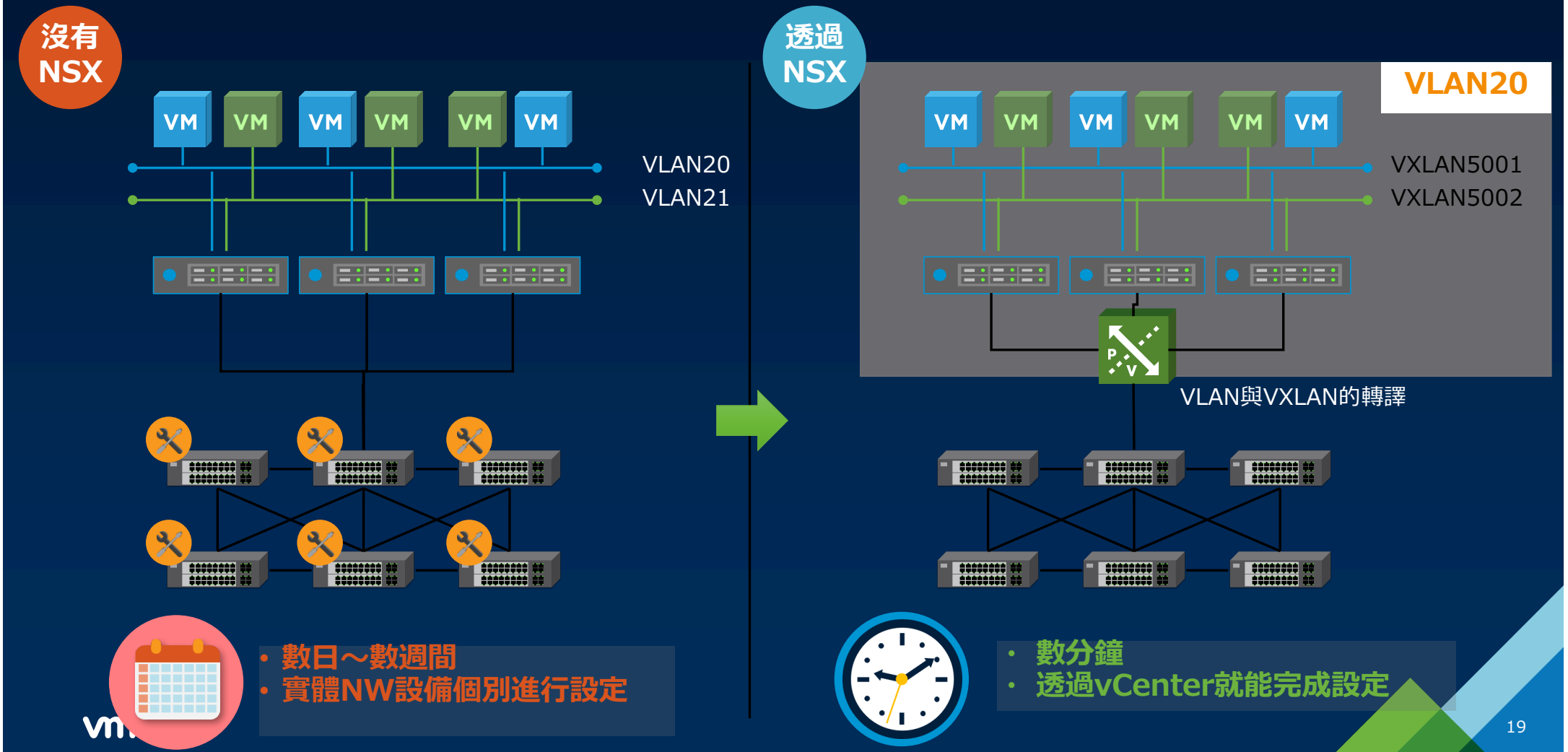
實現運算資源與網路虛擬化

「網路瘦身與優化」



由於路由器/防火牆功能在虛擬機環境中實現，因此對實體設備所需的規格顯著下降，可以使用較便宜的設備

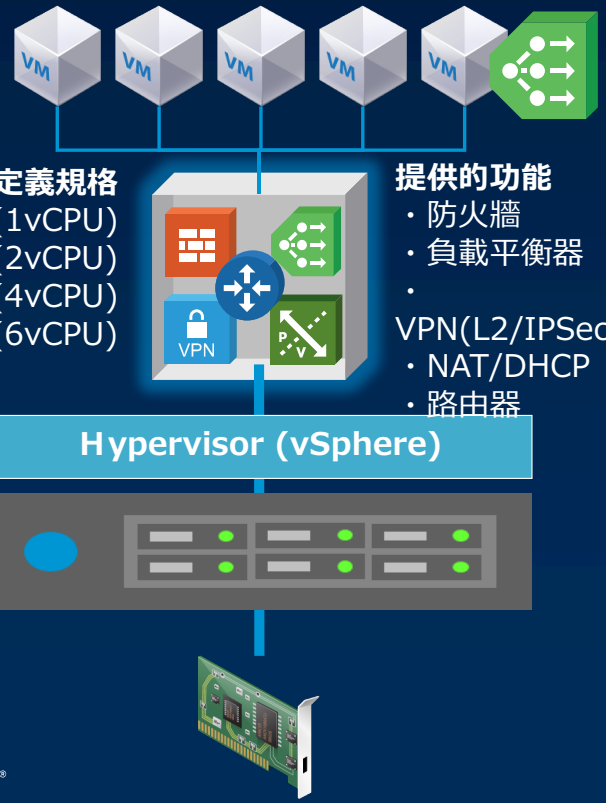
透過NSX、當新的網路需求增加或改變所帶來的自動化效益



NSX網路虛擬化提供形態的比較

虛擬機形式（Virtual Applicance）/Hypervisor形式（分散型）

提供所有功能於一身的虛擬機一體機 – NSX Edge -



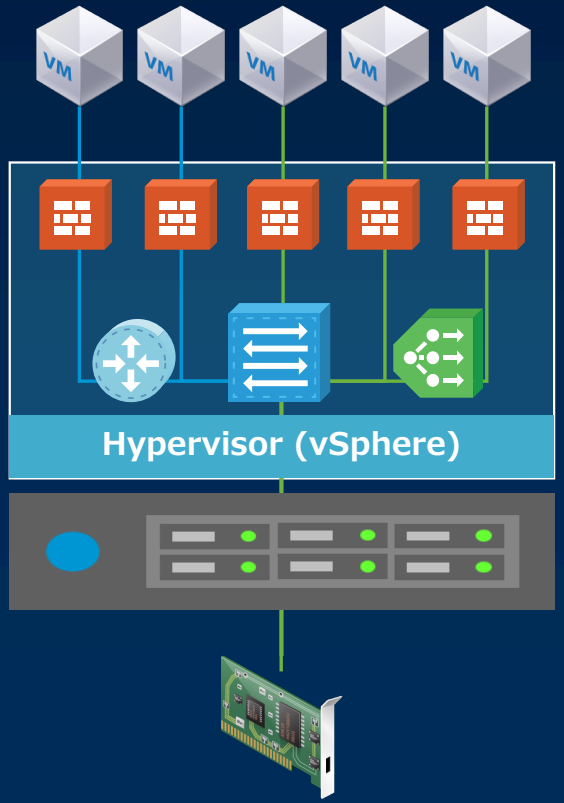
按照需求定義規格

Compact(1vCPU)
Large(2vCPU)
Quad Large(4vCPU)
X-Large(6vCPU)

提供的功能

・防火牆
・負載平衡器
・
VPN(L2/IPSec/SSL)
・NAT/DHCP
・路由器

有效提供高效能的網路功能 Hypervisor形式(分散型)



提供的功能

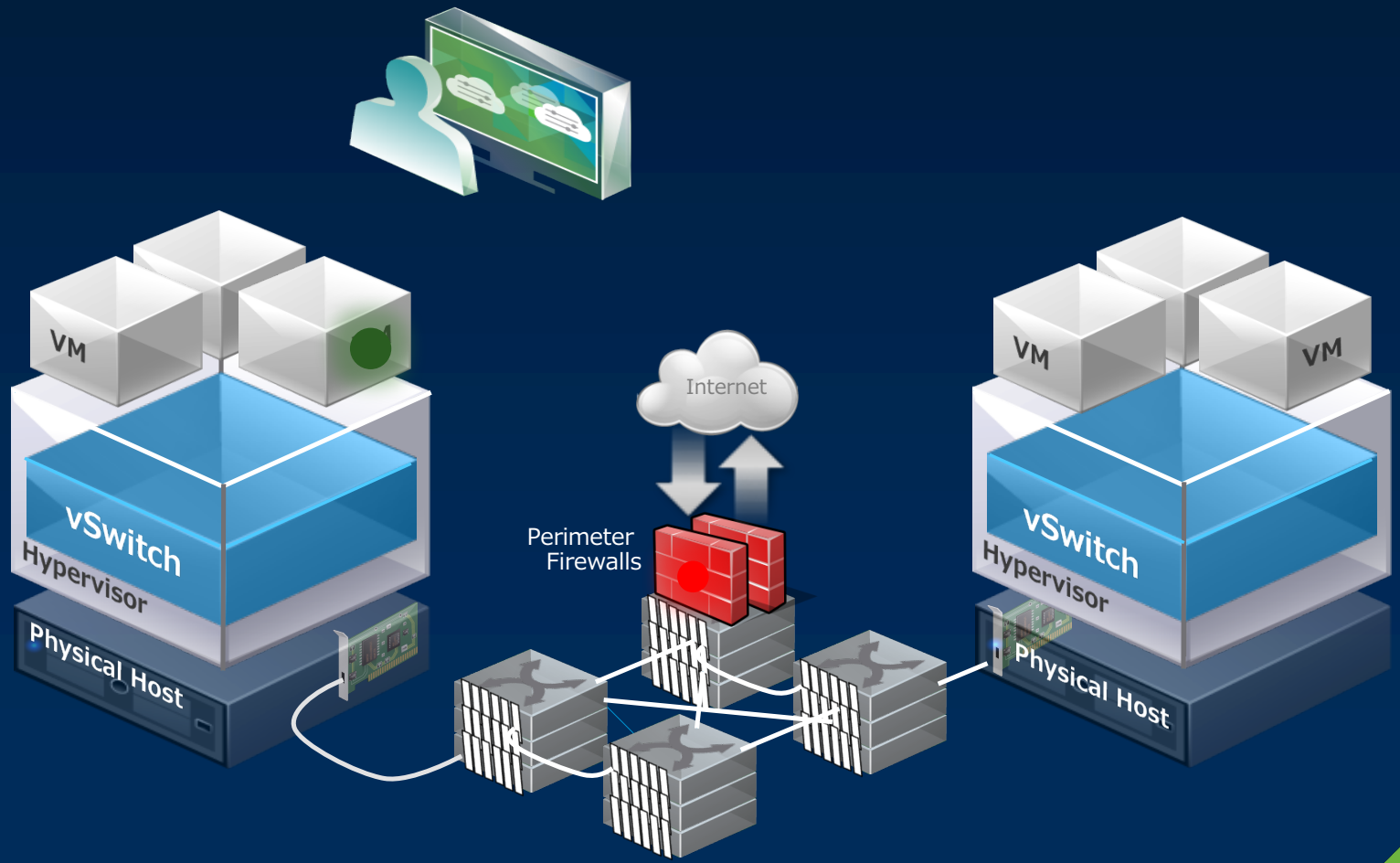
・防火牆
・路由器
・交換機

分散型

・不需要事先預留資源
・由Hypervisor提供資源

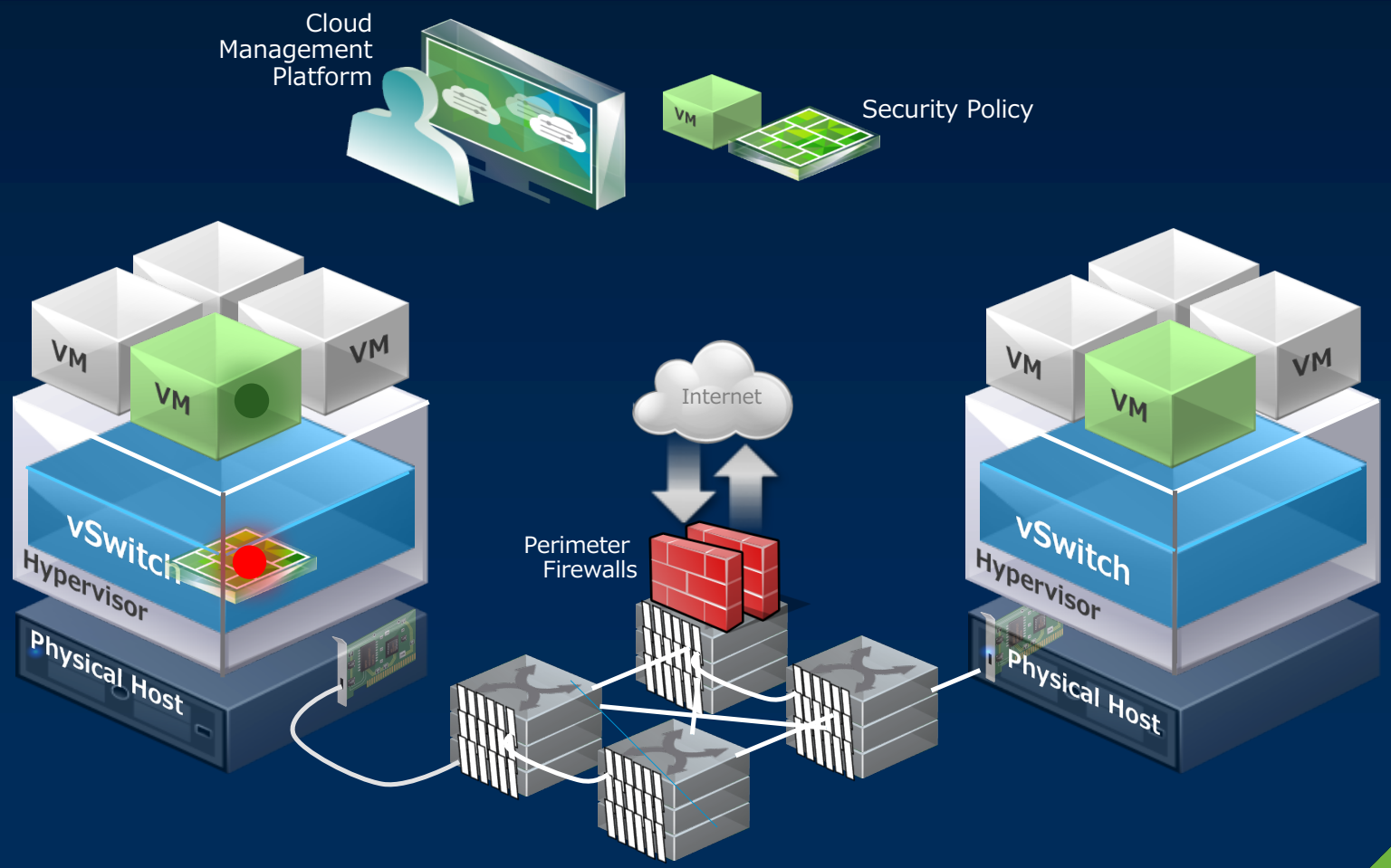
vmware

傳統實體防護架構：集中於邊界實體防火牆進行防護



vmware®

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

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:

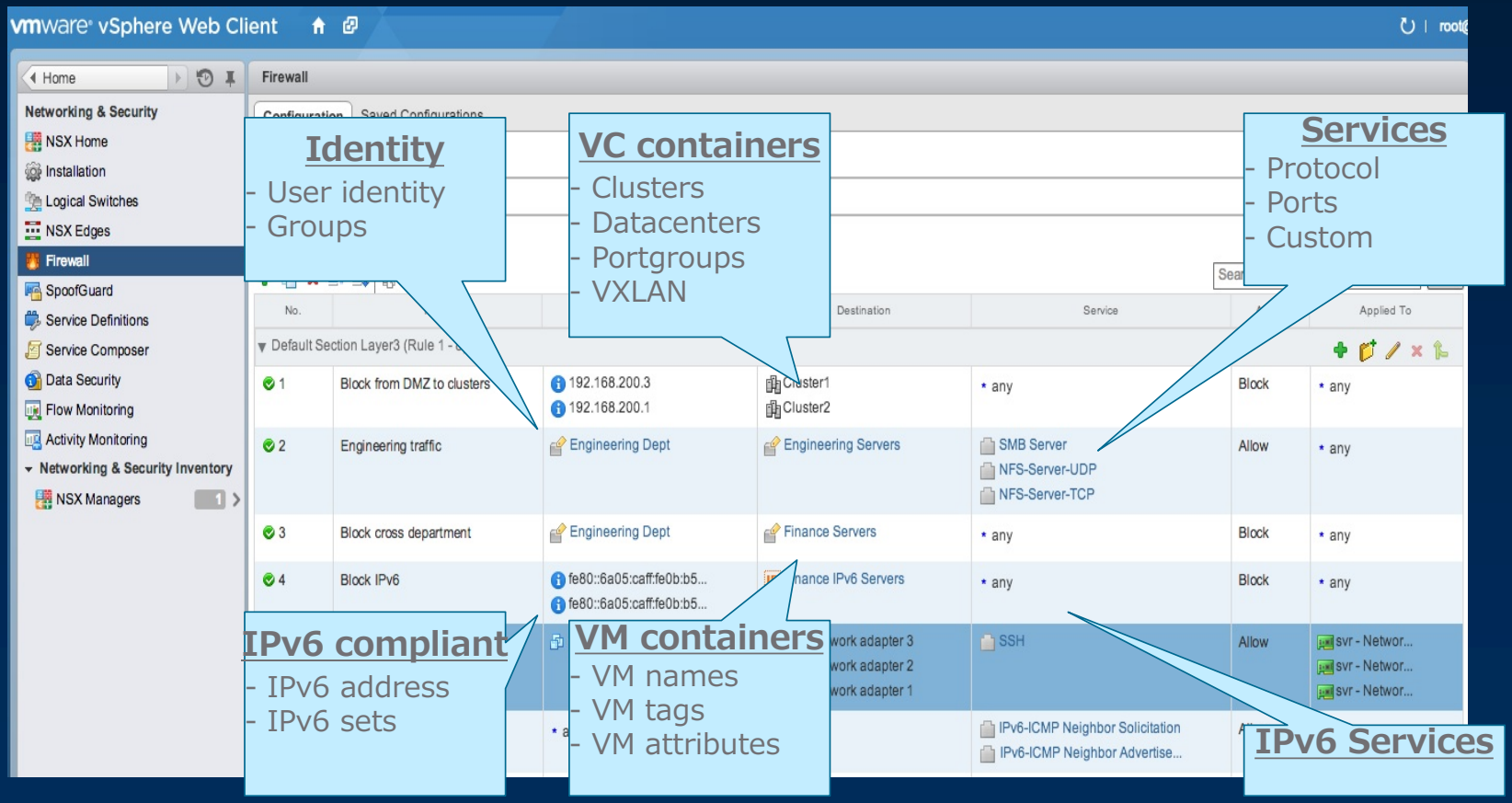
找尋系統的 Source / Destination 為

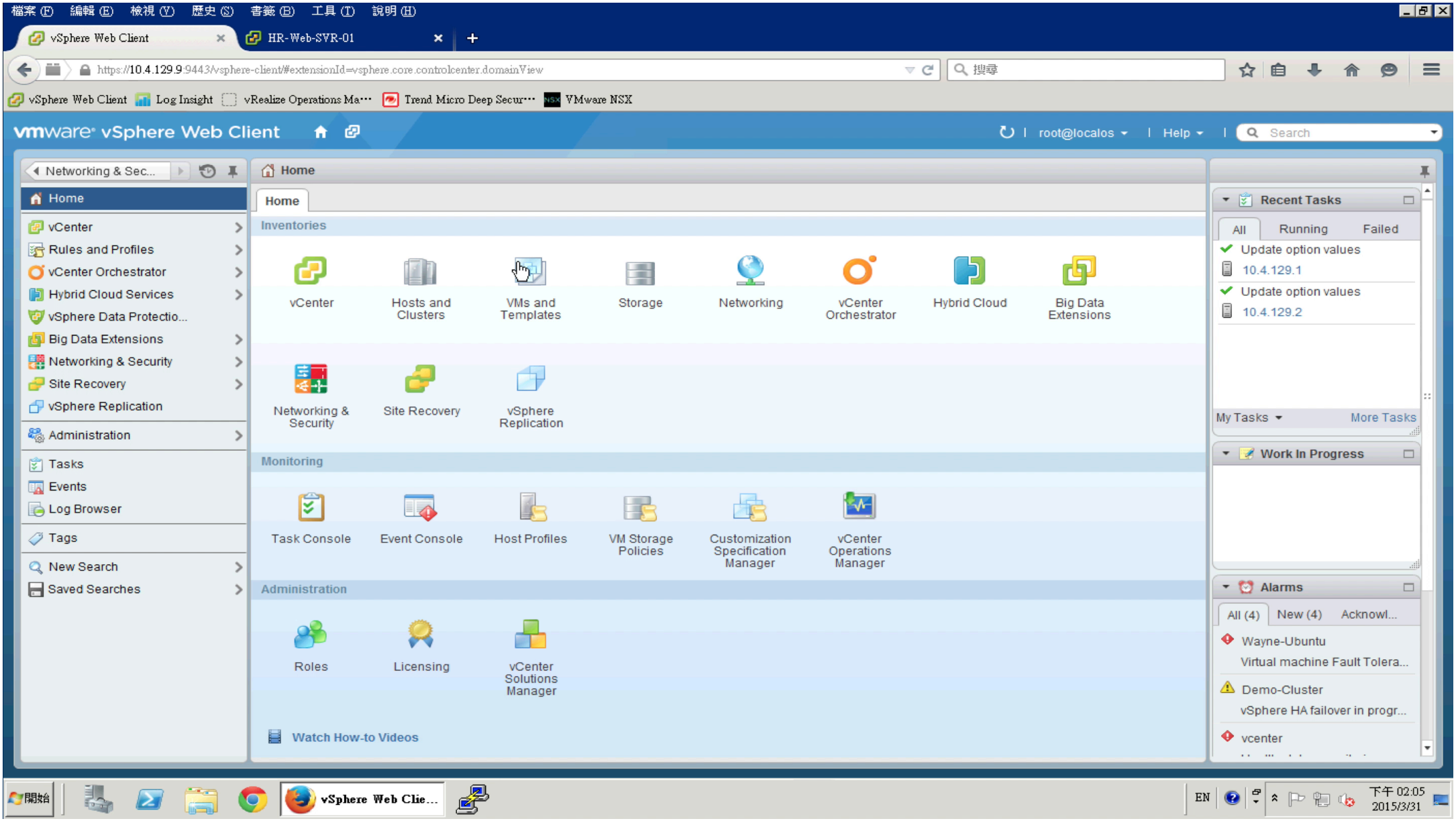
- 172.16.35.244
- 10.42.230.0/24
- FE80::250:56FF:FE8D:8D26
- 00:50:56:8D:CF:93

vmware

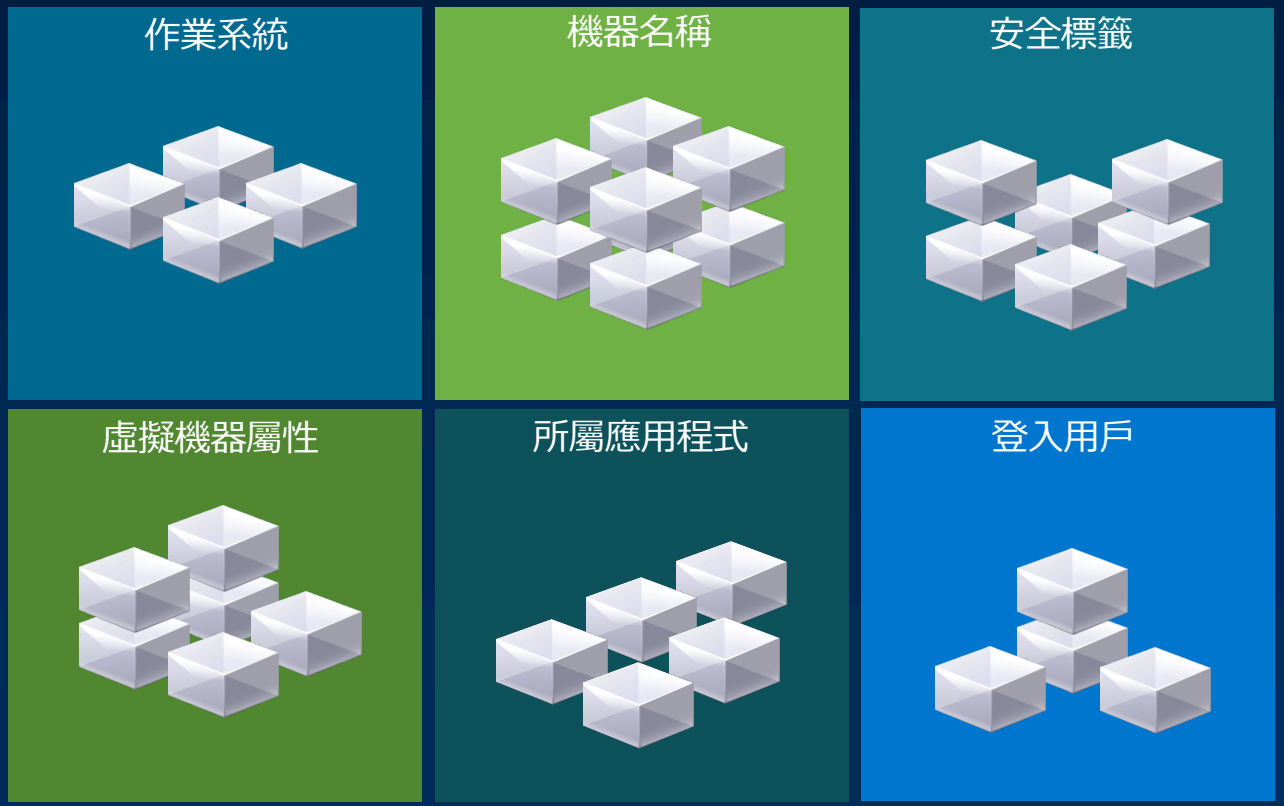
透過設計簡單的NSX防火牆條件，指定群組間的可互通性

NSX支援以各種『特性』建立安全群組




檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)
vSphere Web Client
HR-Web-SVR-01
https://10.4.129.9:9443/vsphere-client/#extensionId=vsphere.core.controlcenter.domainView
搜尋
vSphere Web Client
Log Insight
vRealize Operations Ma…
Trend Micro Deep Secur…
VMware NSX
vmware vSphere Web Client
root@localos
Help
Search
Networking & Sec…
Home
vCenter
Rules and Profiles
vCenter Orchestrator
Hybrid Cloud Services
vSphere Data Protectio…
Big Data Extensions
Networking & Security
Site Recovery
vSphere Replication
Administration
Tasks
Events
Log Browser
Tags
New Search
Saved Searches
Home
Home
Inventories
vCenter
Hosts and Clusters
VMs and Templates
Storage
Networking
vCenter Orchestrator
Hybrid Cloud
Big Data Extensions
Networking & Security
Site Recovery
vSphere Replication
Monitoring
Task Console
Event Console
Host Profiles
VM Storage Policies
Customization Specification Manager
vCenter Operations Manager
Administration
Roles
Licensing
vCenter Solutions Manager
Watch How-to Videos
Recent Tasks
All
Running
Failed
Update option values
10.4.129.1
Update option values
10.4.129.2
My Tasks
More Tasks
Work In Progress
Alarms
All (4)
New (4)
Acknowl…
Wayne-Ubuntu
Virtual machine Fault Tolera…
Demo-Cluster
vSphere HA failover in progr…
vcenter
開始
vSphere Web Clie…
EN
下午 02:05
2015/3/31

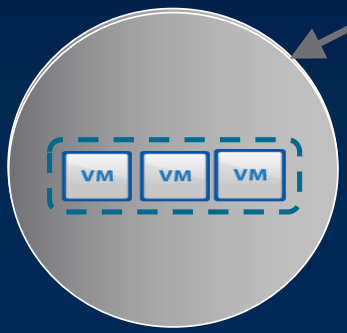
NSX架構內，管理者可以用多樣性的動態條件來建立自動化安全群組



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？

“Standard Web”
☑ Firewall – allow inbound HTTP/S, allow outbound ANY
☑ IPS – prevent DOS attacks, enforce acceptable use

Security Policy：

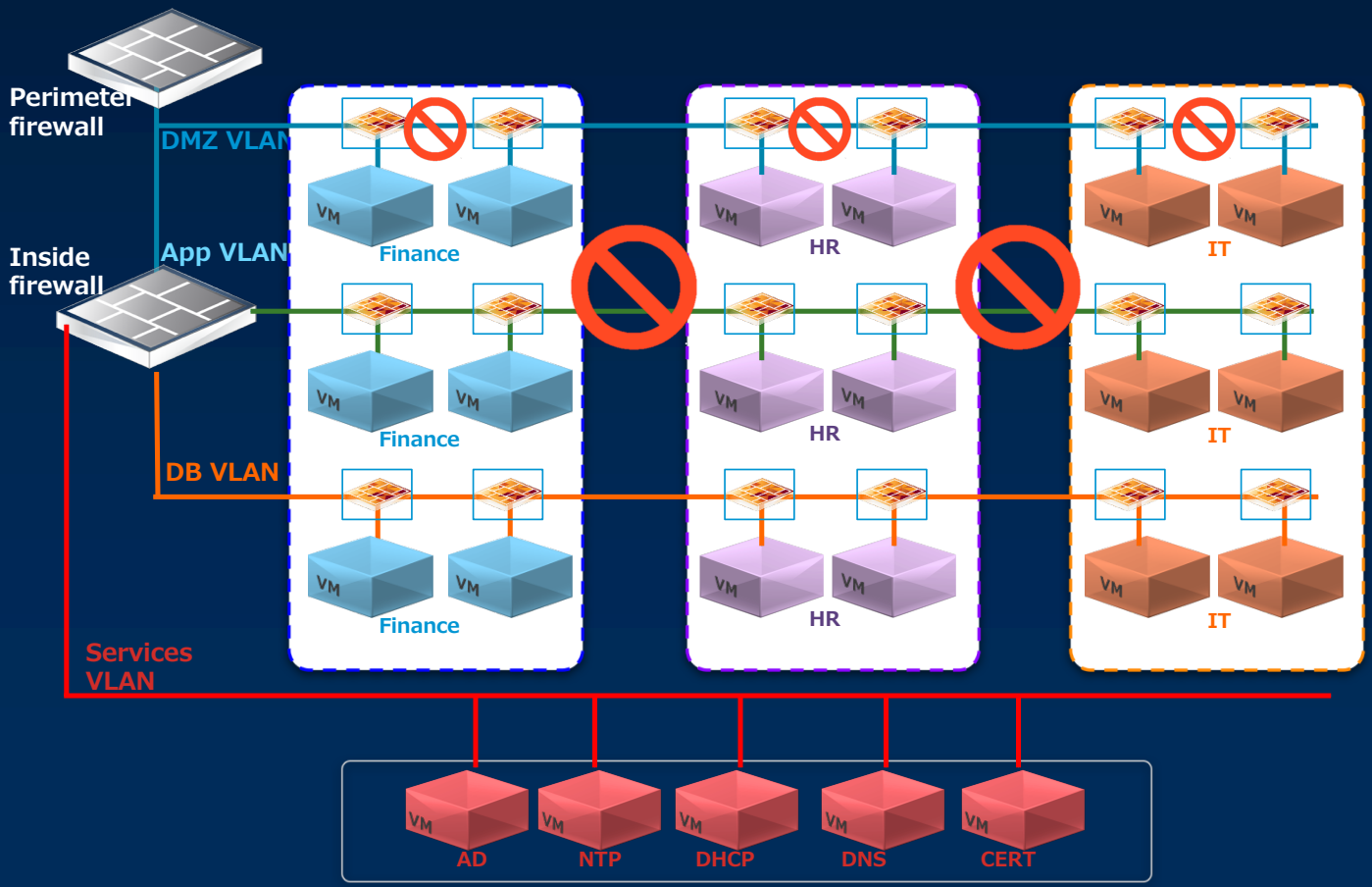
針對此群組，要提供什麼的安全保護機制？

- 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？

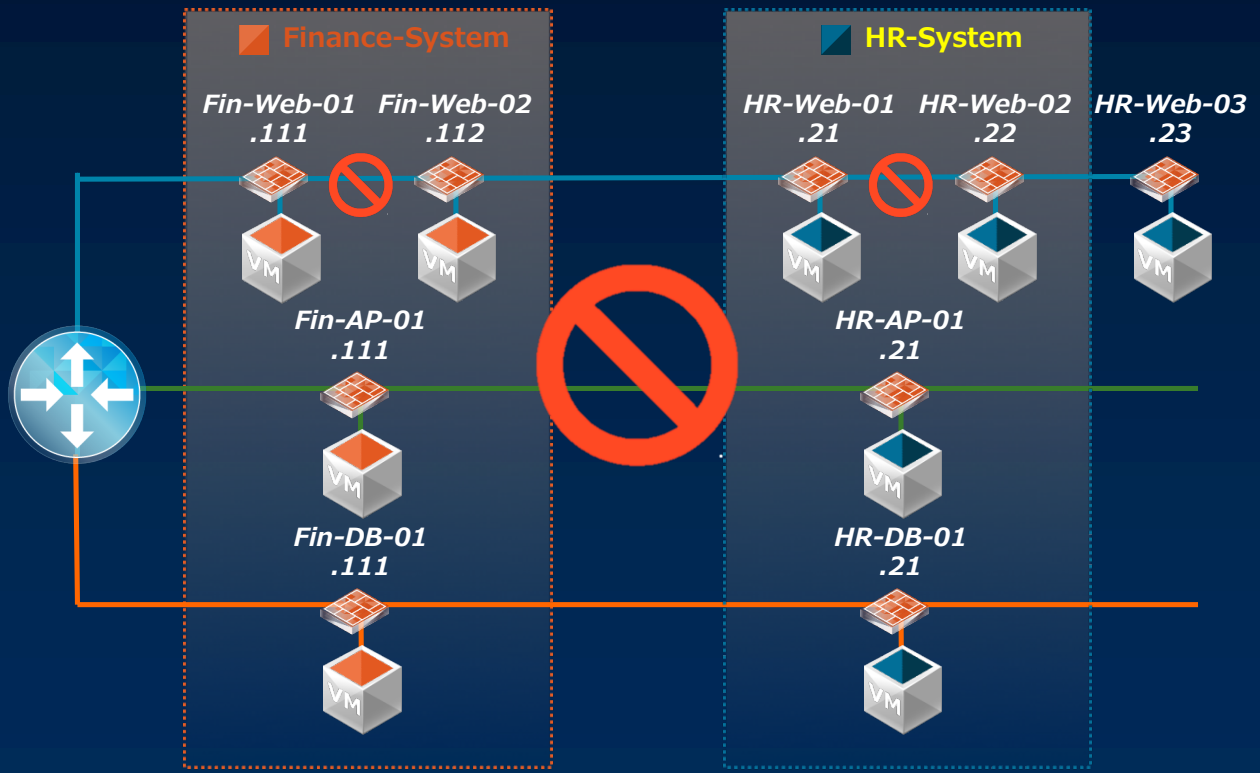
vmware

安全虛擬化技術使用：資料中心內的業務隔離控制

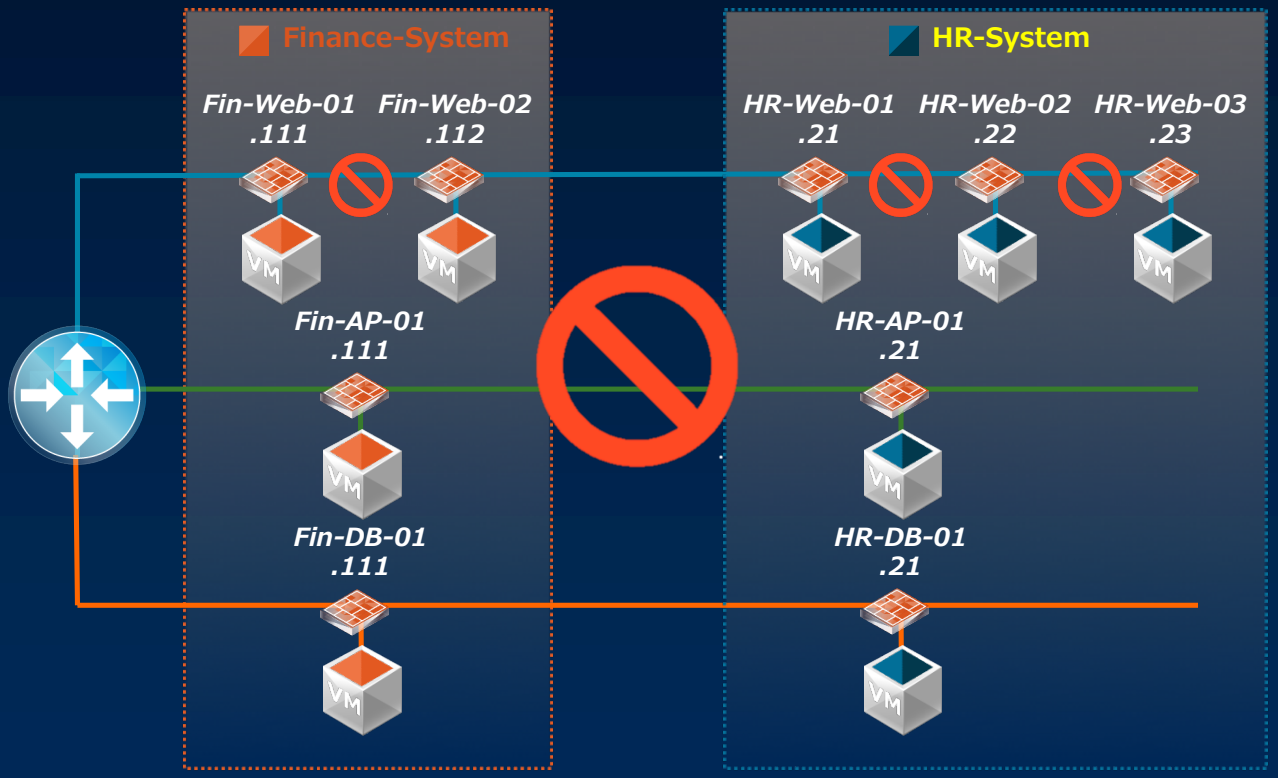
- 即使僅透過防火牆功能，NSX也可透過群組功能進行業務或系統間的防護，並於虛擬機器前直接保護



安全虛擬化：新增之虛擬機器自動套用安全政策

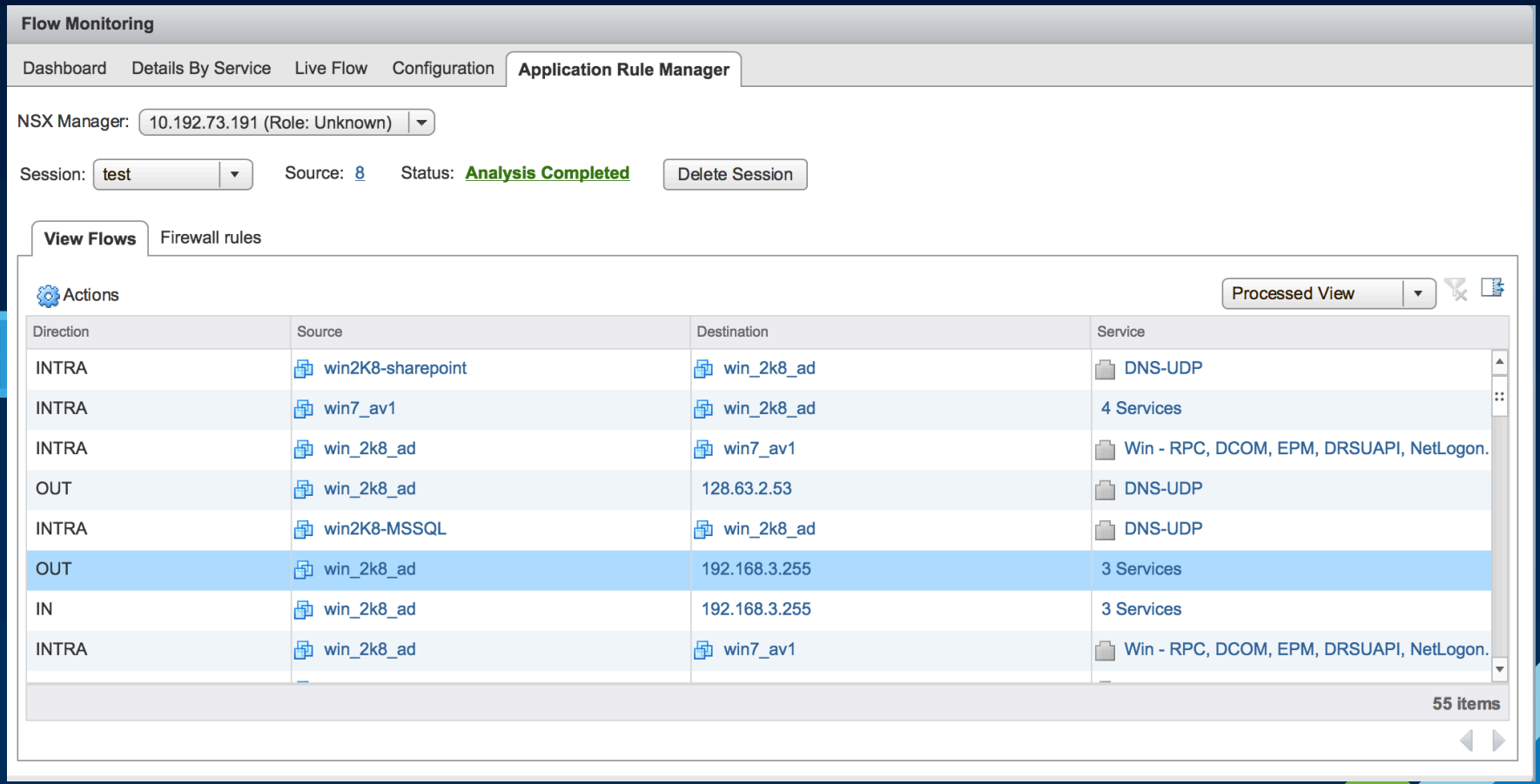


安全虛擬化：新增之虛擬機器自動套用安全政策



新增的Web伺服器，於產出時自動就被納入
對應安全群組，安全防護政策自動生效

運用 NSX Application Rule Manager增加對應用的可視性

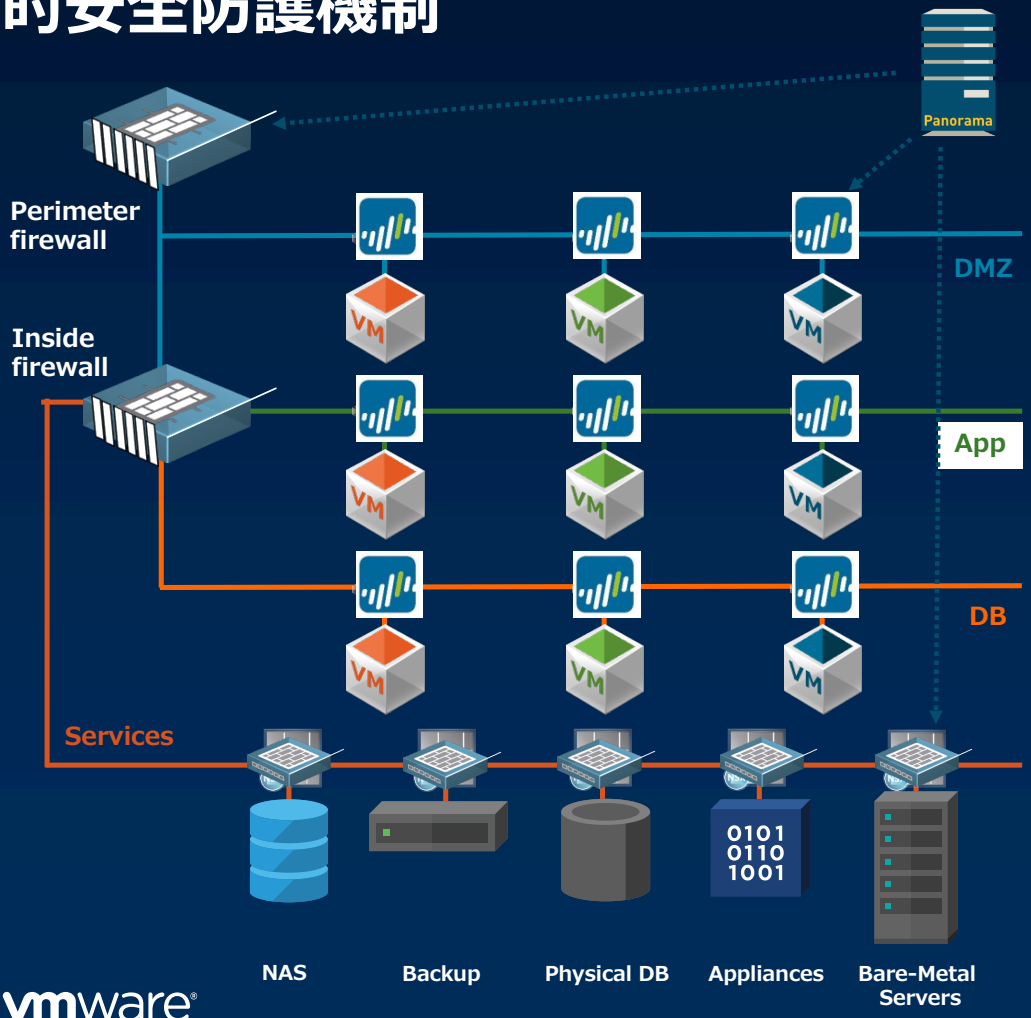


內部對策
（擴散防止對策）

與第三方廠商的整合提供更強化的安全基礎

vmware

NSX作為虛擬環境安全防護平臺，可以搭配不同的安全廠商提供進階的安全防護機制

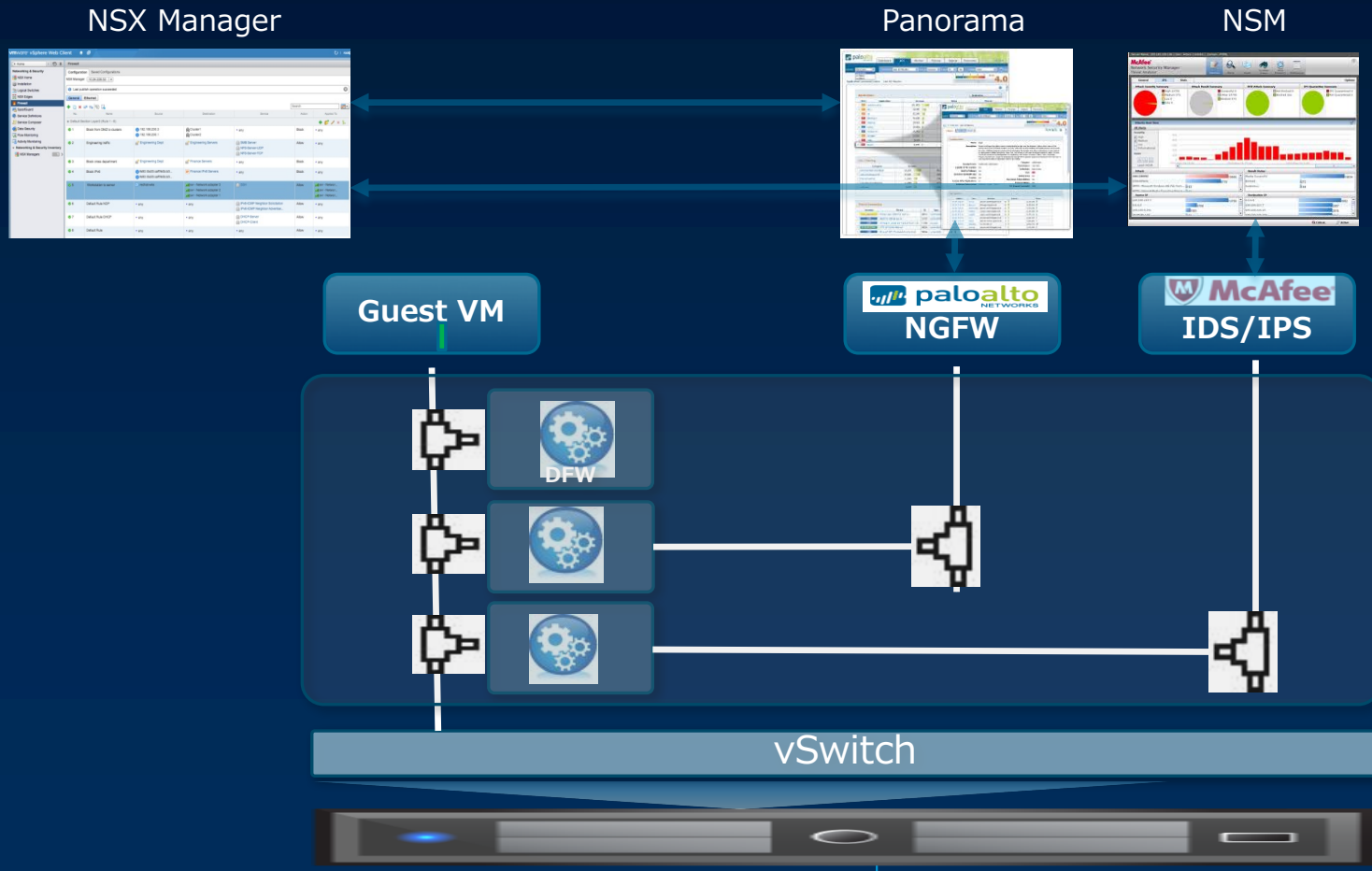


- NSX搭配安全廠商集中進行南北向及東西向之
  - 網路進階安全防護：IPS / Next-Generation Firewall / 網頁控管…
  - 系統防護：防病毒 / 系統檔案安全性檢查
- 安全廠商可使用NSX安全群組進行配置

paloalto NETWORKS
Check Point SOFTWARE TECHNOLOGIES LTD.
TREND MICRO
Symantec
intel Security

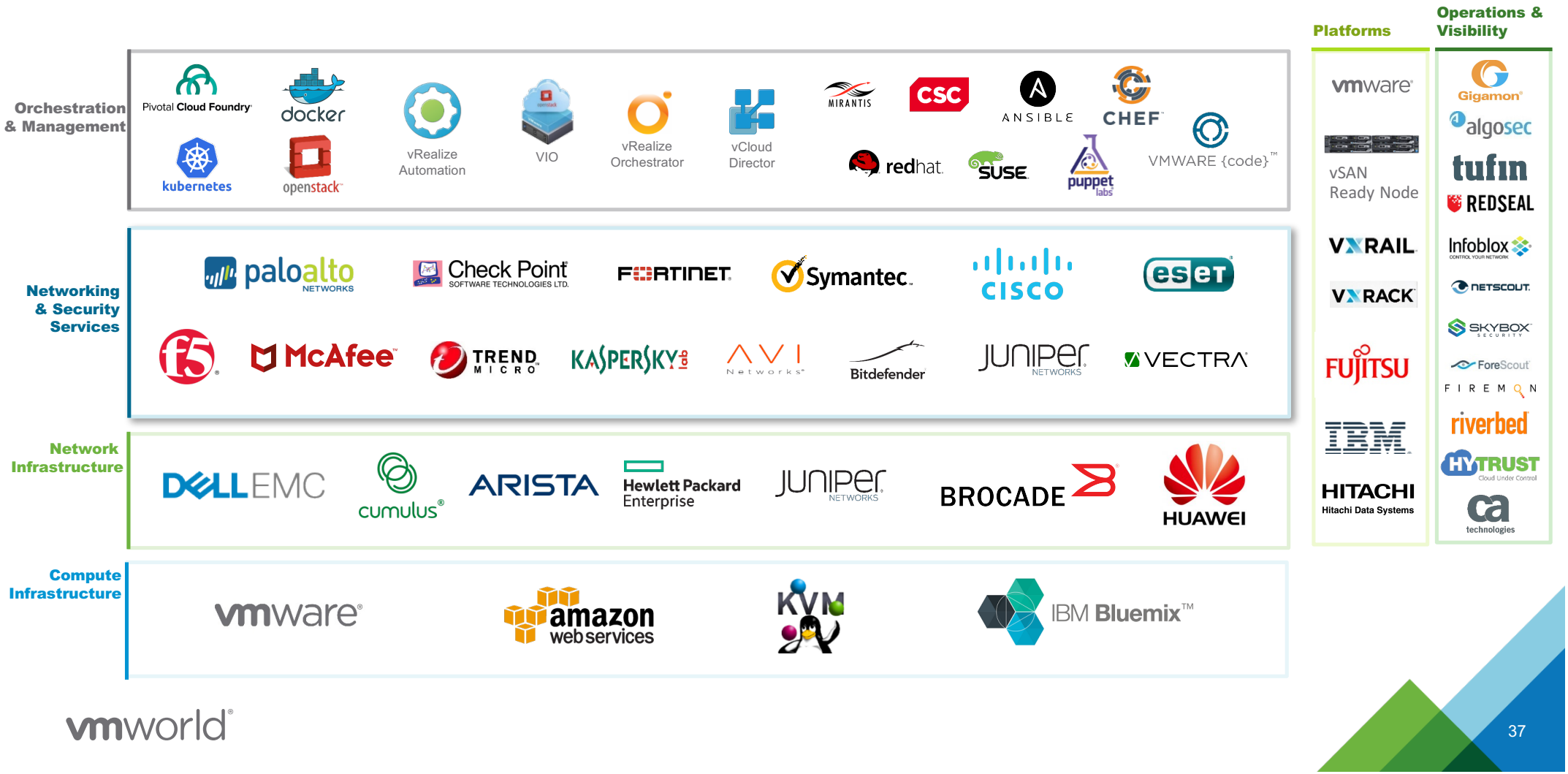
vmware

VMware NSX不僅是提供基本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



VMware NSX不僅是提供基本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 夥伴生態環境


Orchestration & Management
Pivotal Cloud Foundry
docker
kubernetes
openstack
vRealize Automation
VIO
vRealize Orchestrator
vCloud Director
MIRANTIS
CSC
ANSIBLE
CHEF
redhat
SUSE
puppet labs
VMWARE {code}
Networking & Security Services
paloalto NETWORKS
Check Point SOFTWARE TECHNOLOGIES LTD.
FORTINET
Symantec
CISCO
eset
f5
McAfee
TREND MICRO
KASPERSKY lab
AVI Networks
Bitdefender
JUNIPER NETWORKS
VECTRA
Network Infrastructure
DELL EMC
cumulus
ARISTA
Hewlett Packard Enterprise
JUNIPER NETWORKS
BROCADE
HUAWEI
Compute Infrastructure
vmware
amazon web services
KVM
IBM Bluemix
Platforms
vmware
vSAN Ready Node
VXRAIL
VXRACK
FUJITSU
IBM
HITACHI
Hitachi Data Systems
Operations & Visibility
Gigamon
algosec
tufin
REDSEAL
Infoblox
NETSCOUT
SKYBOX SECURITY
ForeScout
FIREMON
riverbed
HYTRUST
Cloud Under Control
ca technologies

Micro-Segmentation微分段技術的亮點

NSX以安全群組直接對應資安政策並進行防護，與網路架構無關。
資安政策設定方式與**業務直接連結**，達成**安全自動化**

微分段技術能防護**每一台虛擬機**，每一張虛擬網卡
虛擬環境內的**所有網路流量**都可以被防護

微分段技術是一個平臺，可以依需求**搭配不同資安廠商的新穎技術**
進行完整的資安防護

內部對策
（擴散防止對策）

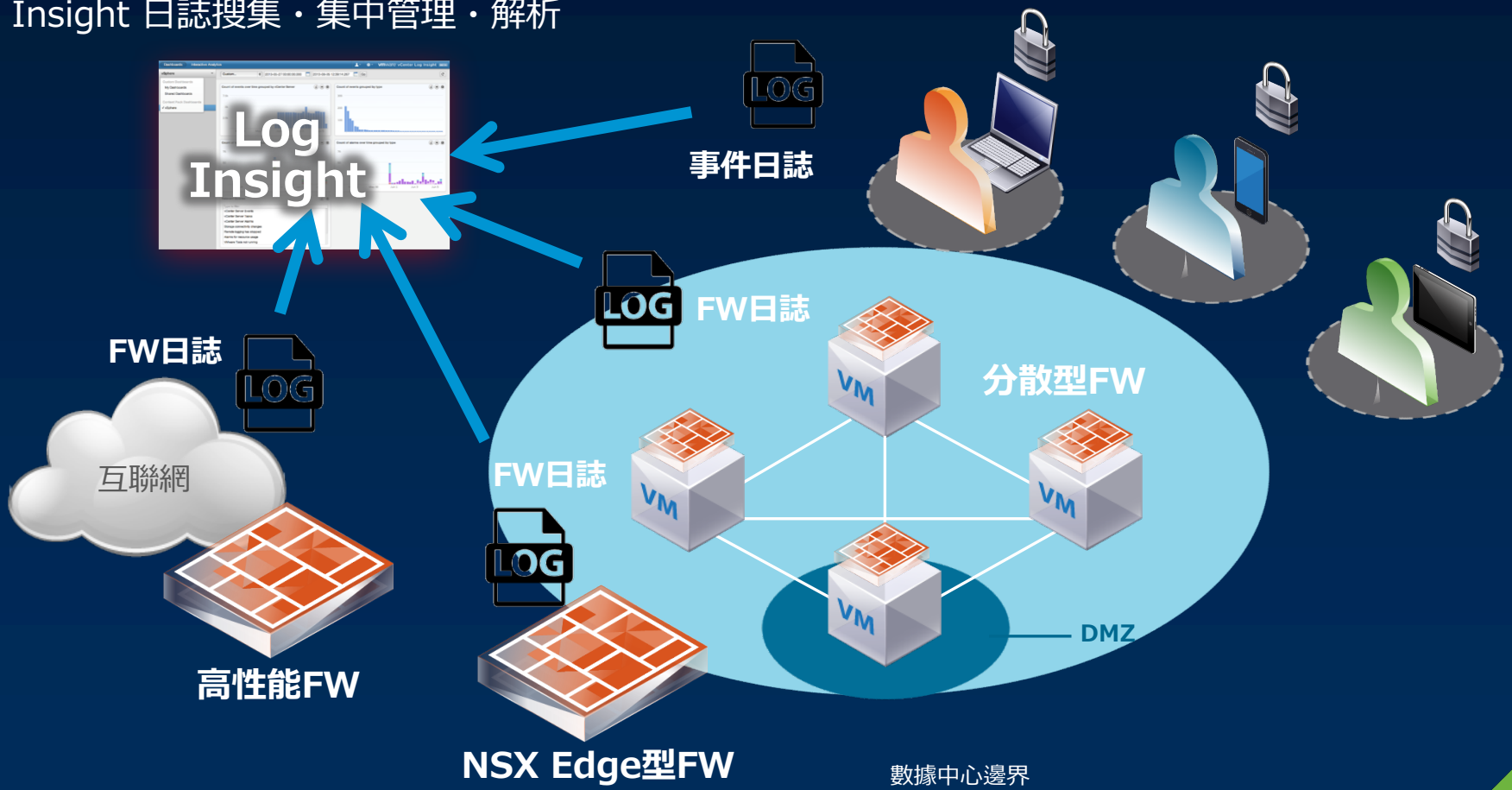
使用管理工具協助對應後續狀況的檢驗

惡意軟體感染的檢測和事故發生原因的快速調查

vmware®

多層FW防禦與惡意軟體感染檢測之日誌分析

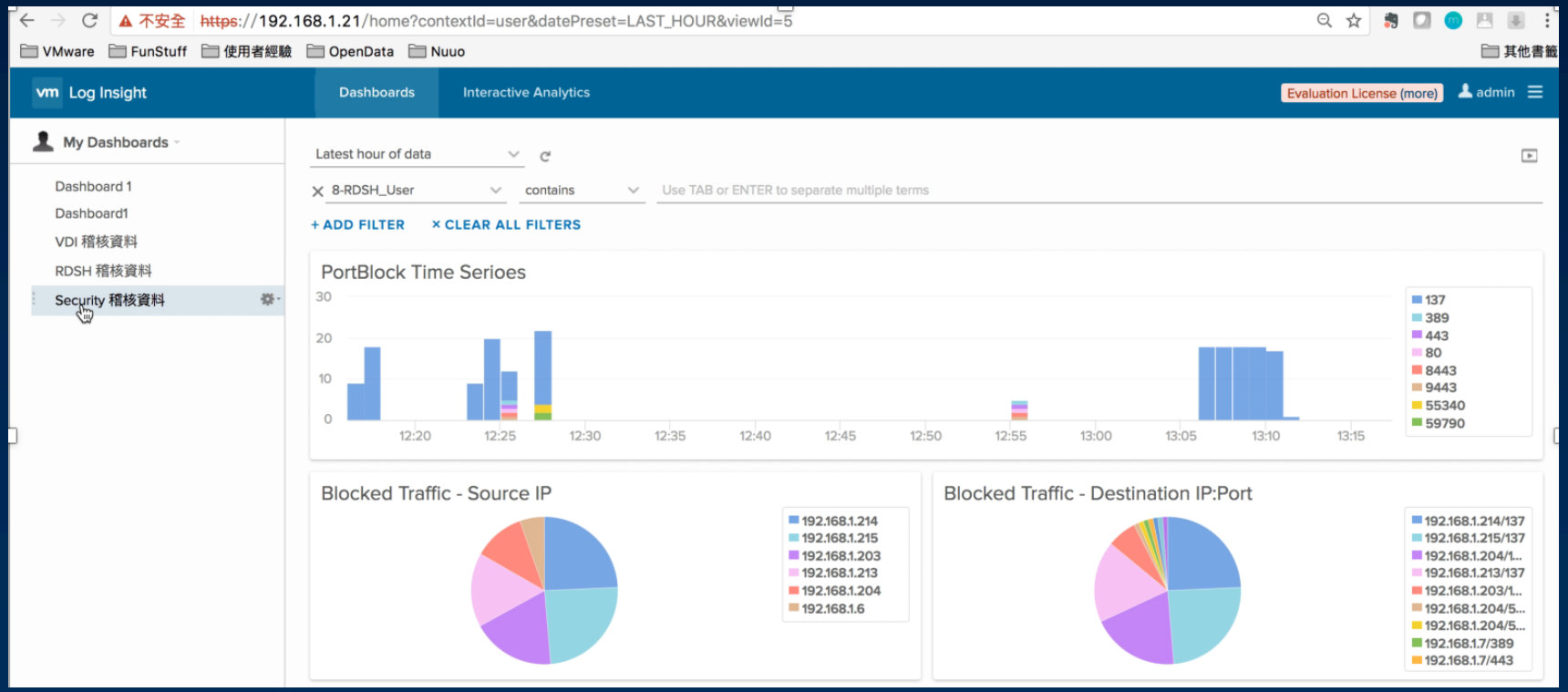
Log Insight 日誌搜集・集中管理・解析



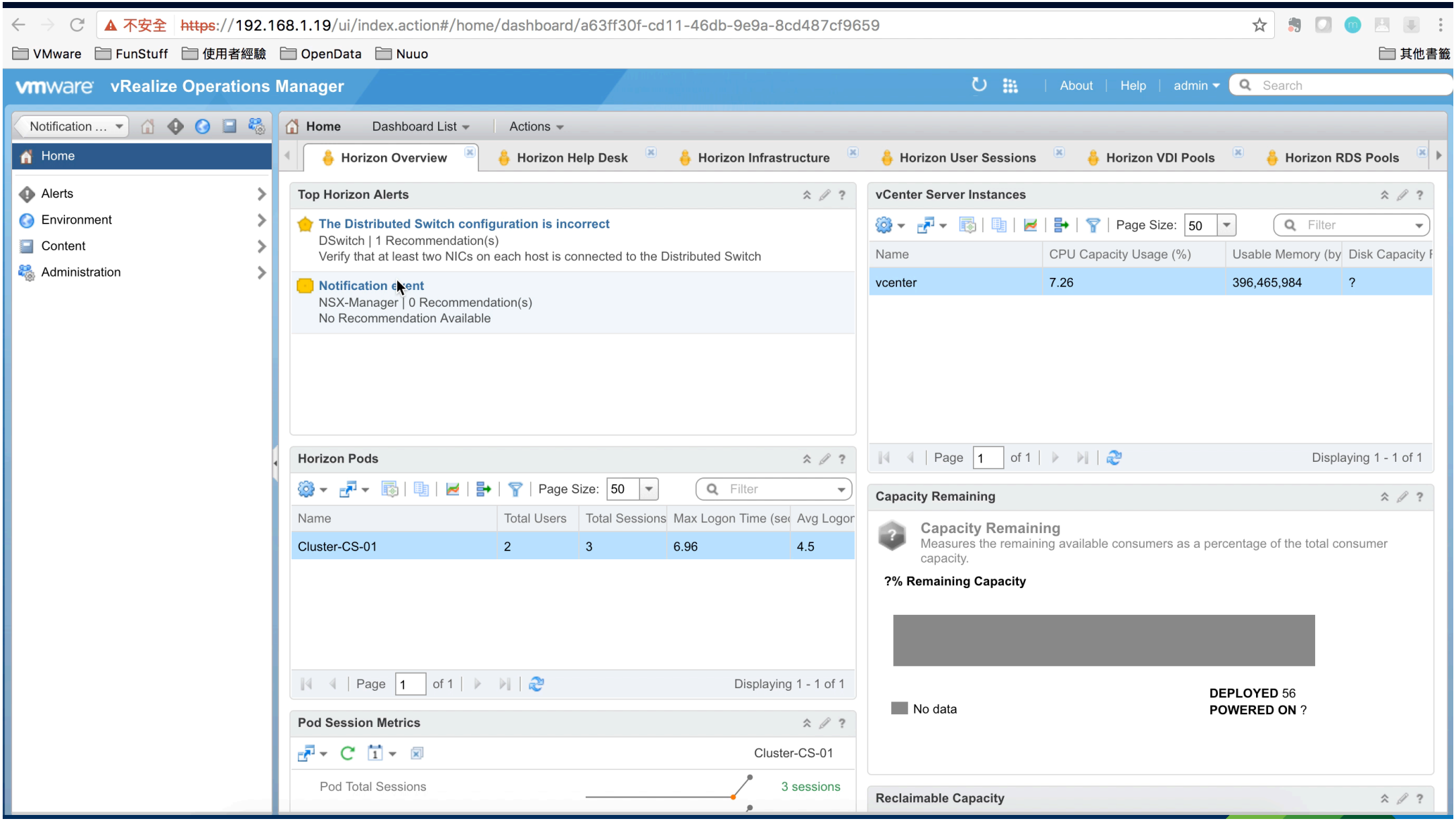
Log Insight 防火牆日誌的可視化

結合東西向防火牆與維運Log的縱深防禦

- 自動帶入Log介面，確認防火牆被攻擊的時間序列與發起來源

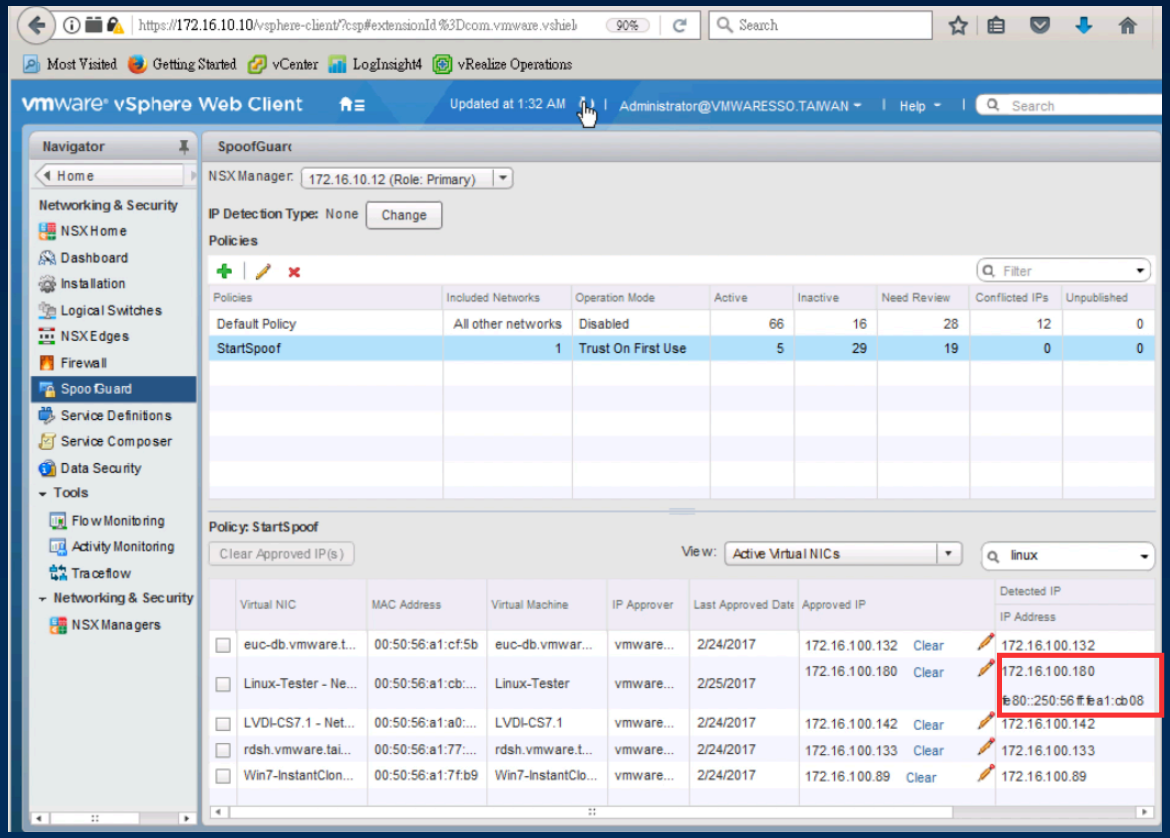


vmware

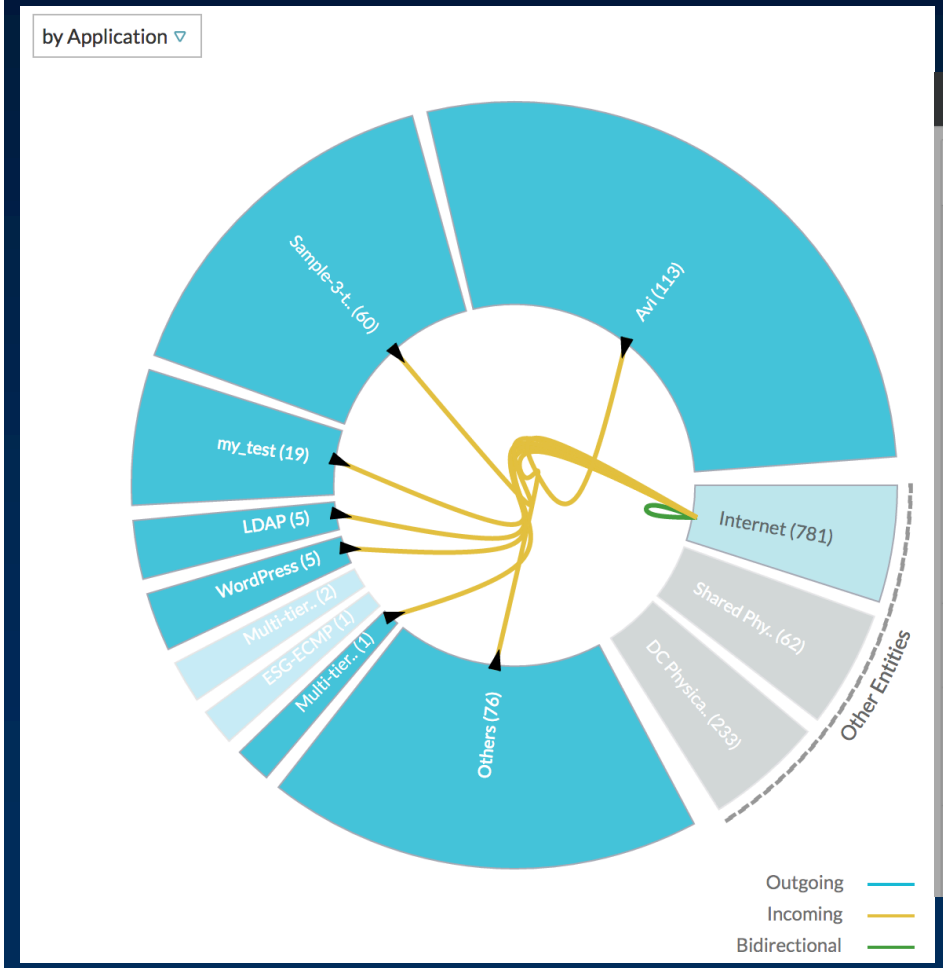

不安全 https://192.168.1.19/ui/index.action#/home/dashboard/a63ff30f-cd11-46db-9e9a-8cd487cf9659
VMware
FunStuff
使用者經驗
OpenData
Nuuo
其他書籤
vmware vRealize Operations Manager
About
Help
admin
Search
Notification ...
Home
Alerts
Environment
Content
Administration
Home
Dashboard List
Actions
Horizon Overview
Horizon Help Desk
Horizon Infrastructure
Horizon User Sessions
Horizon VDI Pools
Horizon RDS Pools
Top Horizon Alerts
The Distributed Switch configuration is incorrect
DSwitch | 1 Recommendation(s)
Verify that at least two NICs on each host is connected to the Distributed Switch
Notification event
NSX-Manager | 0 Recommendation(s)
No Recommendation Available
vCenter Server Instances
Page Size: 50
Filter
Name
CPU Capacity Usage (%)
Usable Memory (by
Disk Capacity
vcenter
7.26
396,465,984
?
Page 1 of 1
Displaying 1 - 1 of 1
Horizon Pods
Page Size: 50
Filter
Name
Total Users
Total Sessions
Max Logon Time (se
Avg Logor
Cluster-CS-01
2
3
6.96
4.5
Page 1 of 1
Displaying 1 - 1 of 1
Capacity Remaining
Capacity Remaining
Measures the remaining available consumers as a percentage of the total consumer capacity.
?% Remaining Capacity
No data
DEPLOYED 56
POWERED ON ?
Pod Session Metrics
Cluster-CS-01
Pod Total Sessions
3 sessions
Reclaimable Capacity

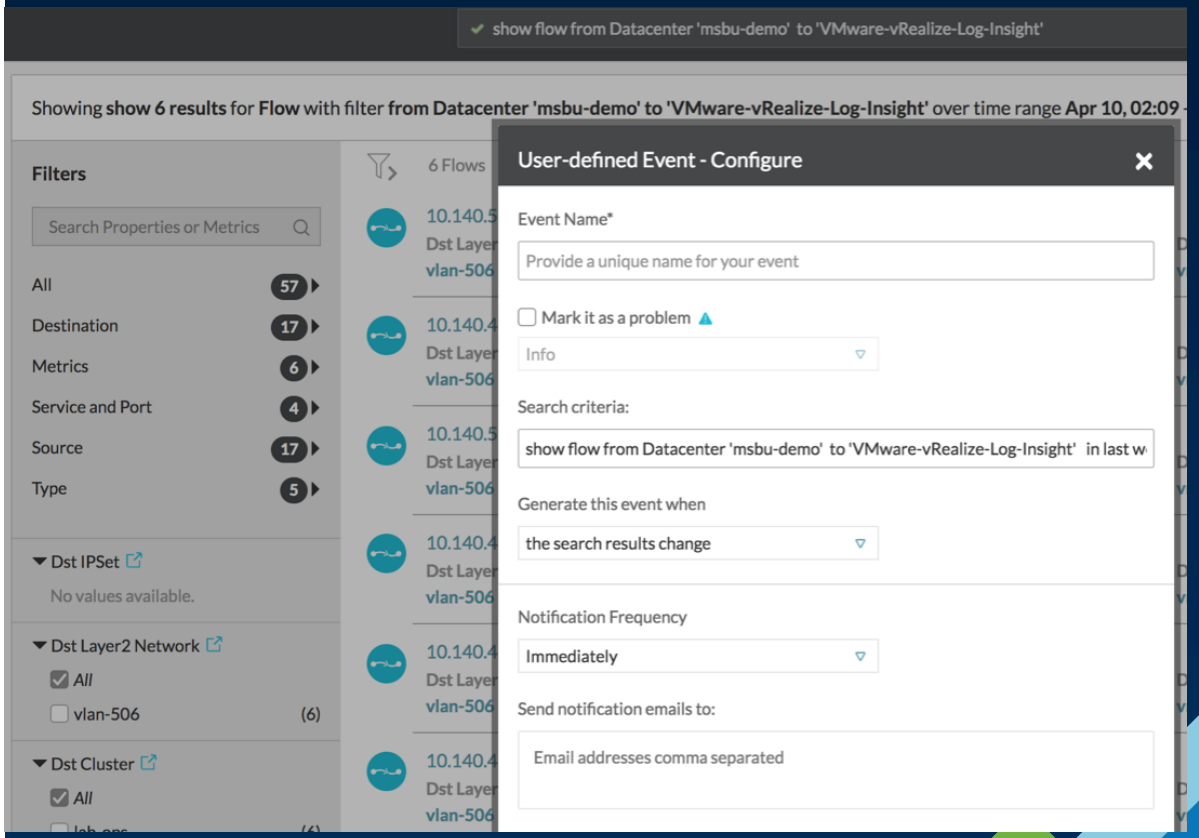
管控各機器的Mac-Address與IP，防止IP被不當竄改

- 任何竄改，必須管理者核准後，該更改方才生效
- 生效前，該機器會處於斷線狀態，避免可能的跳板攻擊



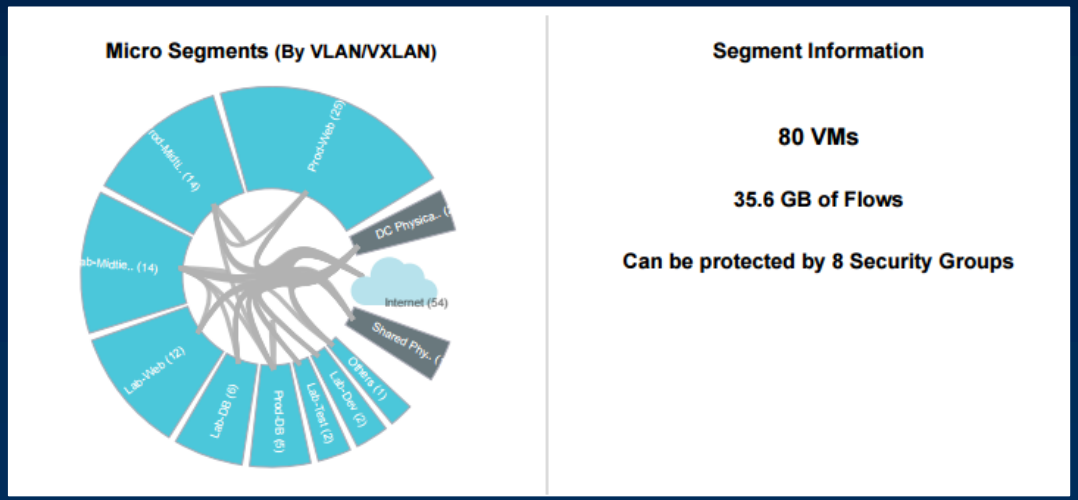
監控不正常的網路流


by Application
Sample-3-t.. (60)
Avi (113)
my_test (19)
LDAP (5)
WordPress (5)
Multi-tier.. (2)
ESG-ECMP (1)
Multi-tier.. (1)
Others (76)
Internet (781)
Shared Phy.. (62)
DC Physica.. (233)
Other Entities
Outgoing
Incoming
Bidirectional


show flow from Datacenter 'msbu-demo' to 'VMware-vRealize-Log-Insight'
Showing show 6 results for Flow with filter from Datacenter 'msbu-demo' to 'VMware-vRealize-Log-Insight' over time range Apr 10, 02:09
Filters
Search Properties or Metrics
All 57
Destination 17
Metrics 6
Service and Port 4
Source 17
Type 5
Dst IPSet
No values available.
Dst Layer2 Network
All
vlan-506 (6)
Dst Cluster
All
6 Flows
User-defined Event - Configure
Event Name*
Provide a unique name for your event
Mark it as a problem
Info
Search criteria:
show flow from Datacenter 'msbu-demo' to 'VMware-vRealize-Log-Insight' in last w
Generate this event when
the search results change
Notification Frequency
Immediately
Send notification emails to:
Email addresses comma separated

利用vRealize Network Insight實現微分段架構建立

不必要的通訊 許可狀態檢視	從實際網路通訊 檢測不必要的溝通	微切分規則 建議演示	不必要的通訊 發生時進行阻隔並舉報
・必要的通訊指認上常有困難 ・不易建立黑名單設定阻隔規則以禁止通訊 ・不必要的通訊發生時常被忽略	・數週到數月的流量記錄 ・時間週期內找出必要的通訊流向	・從通訊結果建議對不要的通訊流向進行遮閉規則的提示 ・規則導入/導出到NSX	・實現白名單系統的NW配置，以防止不必要的通訊 ・不必要通訊發生的情況下，進行示警報並報告



必要的通訊流指認

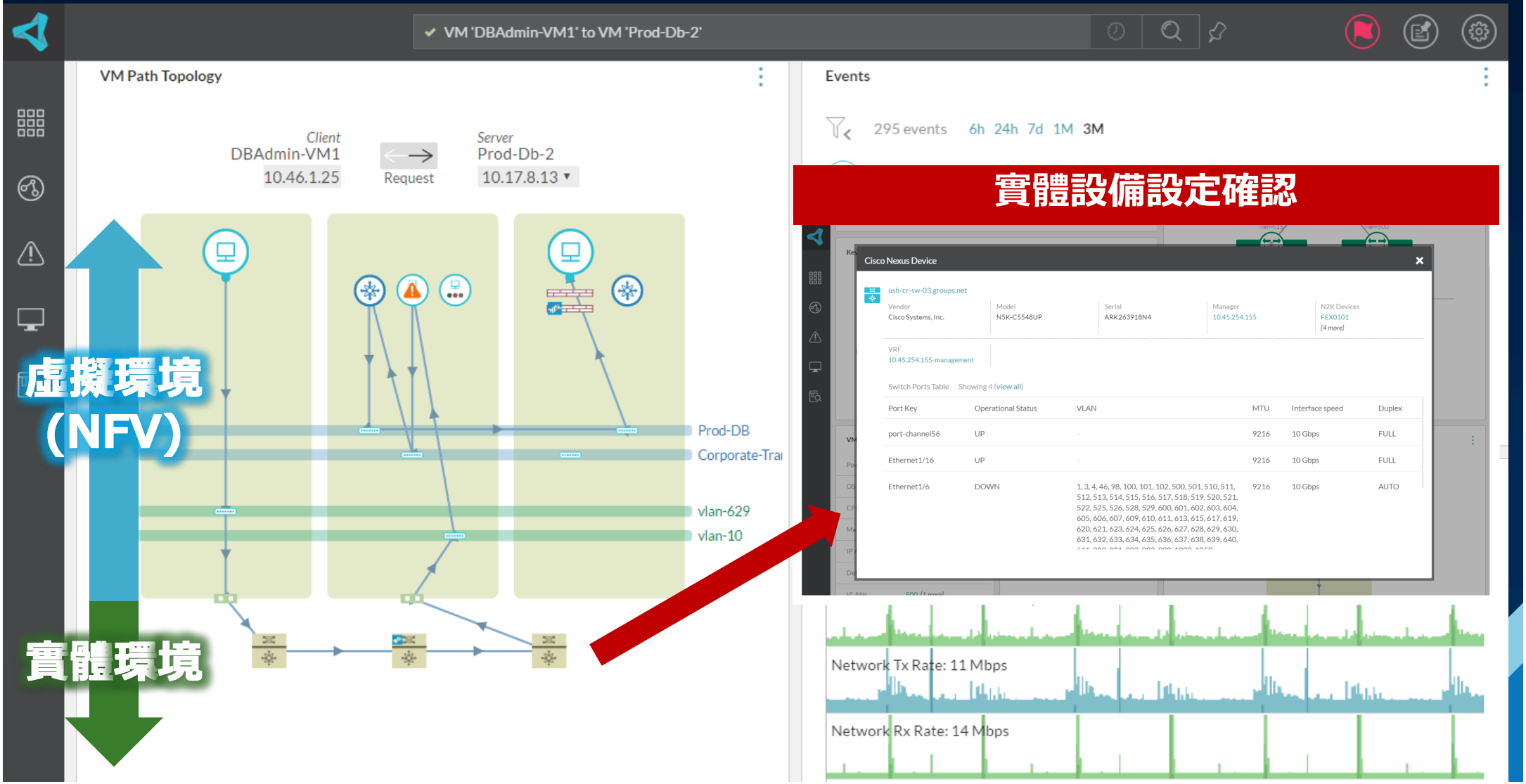
Recommended Firewall Rules

Source	Destination	Services	Action
SG-Lab-Dev	Internet	443 [https]	ALLOW
DC-Physical	SG-Lab-Dev	22 [ssh]	ALLOW
DC-Physical	SG-Lab-Test	22 [ssh]	ALLOW
SG-Lab-Test	Internet	443 [https]	ALLOW
...	...	...	...
ANY	ANY	ANY	DENY

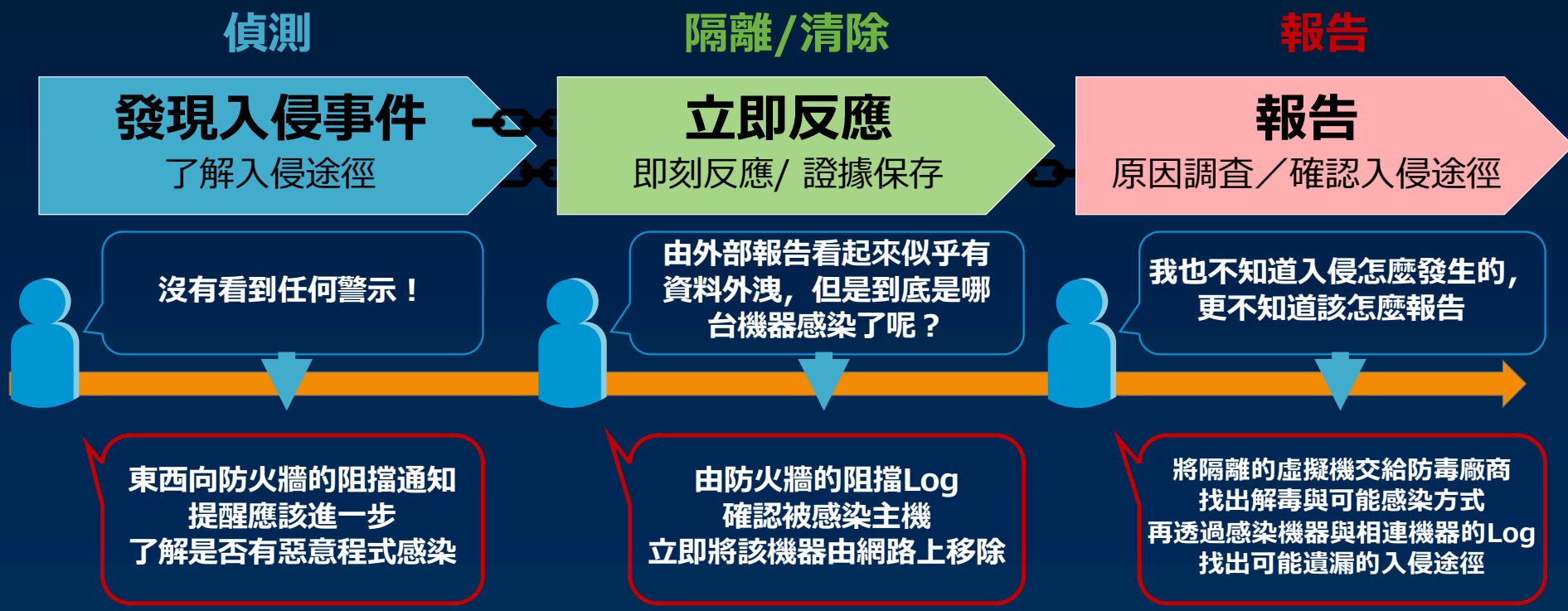
白名單系統

所有不必要的通訊被切斷

利用vRealize Network Insight 進行實體&虛擬環境整合運用管理



遇到標的型攻擊的三階段的現況



NSX已經由美國國防部採用指定為可採購之資訊方案

UNCLASSIFIED

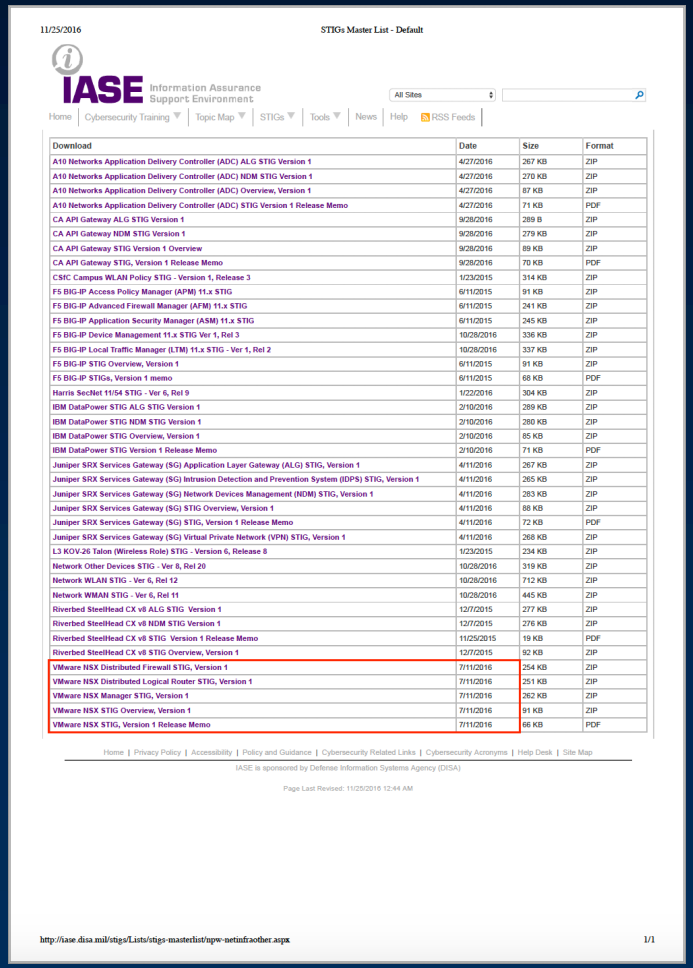
**VMWARE NSX DISTRIBUTED FIREWALL (DFW)
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW**

Version 1, Release 1

27 June 2016

Developed by DISA for the DoD

UNCLASSIFIED



11/25/2016 STIGs Master List - Default

IASE Information Assurance Support Environment

All Sites

Home | Cybersecurity Training | Topic Map | STIGs | Tools | News | Help | RSS Feeds

Download	Date	Size	Format
A10 Networks Application Delivery Controller (ADC) ALG STIG Version 1	4/27/2016	267 KB	ZIP
A10 Networks Application Delivery Controller (ADC) NDM STIG Version 1	4/27/2016	270 KB	ZIP
A10 Networks Application Delivery Controller (ADC) Overview, Version 1	4/27/2016	87 KB	ZIP
A10 Networks Application Delivery Controller (ADC) STIG Version 1 Release Memo	4/27/2016	71 KB	PDF
CA API Gateway ALG STIG Version 1	9/28/2016	289 B	ZIP
CA API Gateway NDM STIG Version 1	9/28/2016	279 KB	ZIP
CA API Gateway STIG Version 1 Overview	9/28/2016	89 KB	ZIP
CA API Gateway STIG, Version 1 Release Memo	9/28/2016	70 KB	PDF
CSfC Campus WLAN Policy STIG - Version 1, Release 3	1/23/2015	314 KB	ZIP
F5 BIG-IP Access Policy Manager (APM) 11.x STIG	6/11/2015	91 KB	ZIP
F5 BIG-IP Advanced Firewall Manager (AFM) 11.x STIG	6/11/2015	241 KB	ZIP
F5 BIG-IP Application Security Manager (ASM) 11.x STIG	6/11/2015	245 KB	ZIP
F5 BIG-IP Device Management 11.x STIG Ver 1, Rel 3	10/28/2016	336 KB	ZIP
F5 BIG-IP Local Traffic Manager (LTM) 11.x STIG - Ver 1, Rel 2	10/28/2016	337 KB	ZIP
F5 BIG-IP STIG Overview, Version 1	6/11/2015	91 KB	ZIP
F5 BIG-IP STIGs, Version 1 memo	6/11/2015	68 KB	PDF
Harris SecNet 11/54 STIG - Ver 6, Rel 9	1/22/2016	304 KB	ZIP
IBM DataPower STIG ALG STIG Version 1	2/10/2016	289 KB	ZIP
IBM DataPower STIG NDM STIG Version 1	2/10/2016	280 KB	ZIP
IBM DataPower STIG Overview, Version 1	2/10/2016	85 KB	ZIP
IBM DataPower STIG Version 1 Release Memo	2/10/2016	71 KB	PDF
Juniper SRX Services Gateway (SG) Application Layer Gateway (ALG) STIG, Version 1	4/11/2016	267 KB	ZIP
Juniper SRX Services Gateway (SG) Intrusion Detection and Prevention System (IDPS) STIG, Version 1	4/11/2016	265 KB	ZIP
Juniper SRX Services Gateway (SG) Network Devices Management (NDM) STIG, Version 1	4/11/2016	283 KB	ZIP
Juniper SRX Services Gateway (SG) STIG Overview, Version 1	4/11/2016	88 KB	ZIP
Juniper SRX Services Gateway (SG) STIG, Version 1 Release Memo	4/11/2016	72 KB	PDF
Juniper SRX Services Gateway (SG) Virtual Private Network (VPN) STIG, Version 1	4/11/2016	268 KB	ZIP
L3 KOV-26 Talon (Wireless Role) STIG - Version 6, Release 8	1/23/2015	234 KB	ZIP
Network Other Devices STIG - Ver 8, Rel 20	10/28/2016	319 KB	ZIP
Network WLAN STIG - Ver 6, Rel 12	10/28/2016	712 KB	ZIP
Network WMAN STIG - Ver 6, Rel 11	10/28/2016	445 KB	ZIP
Riverbed SteelHead CX v8 ALG STIG Version 1	12/7/2015	277 KB	ZIP
Riverbed SteelHead CX v8 NDM STIG Version 1	12/7/2015	276 KB	ZIP
Riverbed SteelHead CX v8 STIG Version 1 Release Memo	11/25/2015	19 KB	PDF
Riverbed SteelHead CX v8 STIG Overview, Version 1	12/7/2015	92 KB	ZIP
VMware NSX Distributed Firewall STIG, Version 1	7/11/2016	254 KB	ZIP
VMware NSX Distributed Logical Router STIG, Version 1	7/11/2016	251 KB	ZIP
VMware NSX Manager STIG, Version 1	7/11/2016	262 KB	ZIP
VMware NSX STIG Overview, Version 1	7/11/2016	91 KB	ZIP
VMware NSX STIG, Version 1 Release Memo	7/11/2016	66 KB	PDF

Home | Privacy Policy | Accessibility | Policy and Guidance | Cybersecurity Related Links | Cybersecurity Acronyms | Help Desk | Site Map

IASE is sponsored by Defense Information Systems Agency (DISA)

Page Last Revised: 11/25/2016 12:44 AM

http://iase.disa.mil/stigs/Lists/stigs-masterlist/npw-netinfraother.aspx 1/1

vmware®

NSX 如何協助您面對安全的威脅與挑戰?

安全威脅使
資料中心的
維護格外困難

對網路環境的**可視性**並
能對於應用的屬性管理

微切分技術提供
無所不在的控制端點

對於多廠商的整合
進行自動化服務串連

對於安全規則, 應用服務提供
完整**生命週期管理**

資料中心的安全
防護變得更容易

vmware

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

vmware

Thank you

vmware®