面向應用服務的私有雲 (Private Cloud/SDN)安全

林揚城(Brook Lin)
blin@paloaltonetworks.com
技術顧問

Agenda

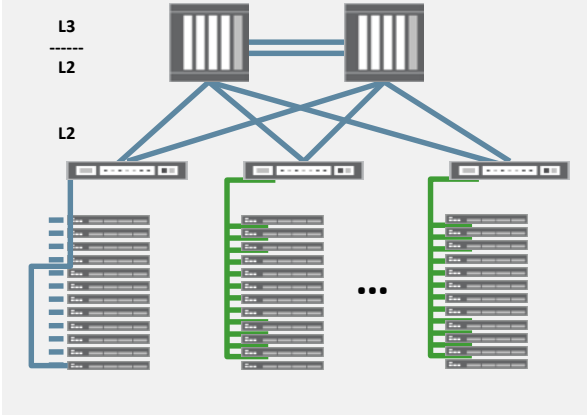
- Private Cloud/SDN 資料中心現狀和挑戰
- 打造面向應用服務的Private Cloud/SDN和自動化的安全維運
- 應用案例分享

現有資料中心的挑戰
(Private Cloud/SDN)

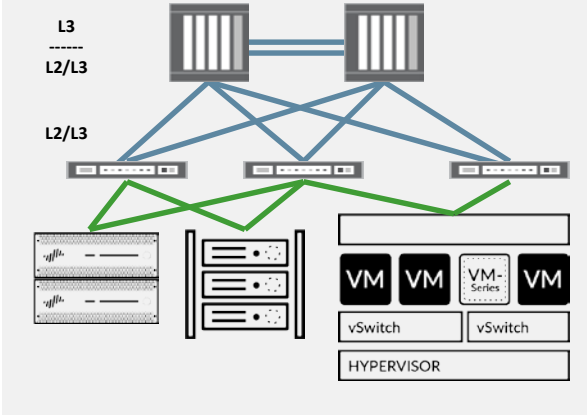
Challenge

資料中心：多層架構逐漸轉變到IP FABRIC

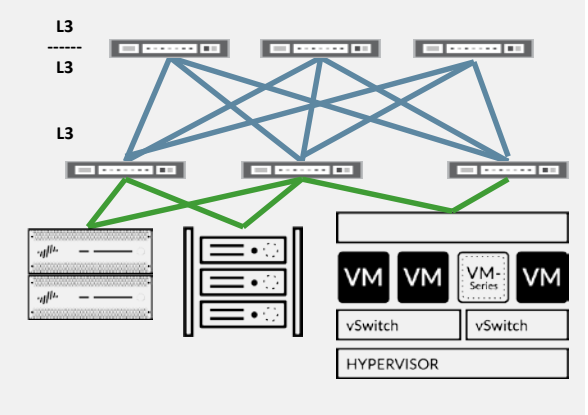
多層設計
傳統架構



資料中心矩陣設計
PortChannel, TRILL



IP Fabric設計
Under + Overlay架構



今天的資料中心：業務和網路的緊密結合(Tightly Coupling)

- 業務與網路的緊密相關：
  - 應用與Port/VLAN/IP地址的結合，意味著應用和位置的緊密綁定，不具備移動性
  - 安全控制與IP地址的結合，意味著無法實現靈活的策略部署
  - 業務的變更意味著基礎網路頻繁的設定修改，反之亦然
  - 從上層業務服務到底層網路的環環相扣，牽一發動全身，之間的橋樑是人來處理
- 業務功能和物理網路的***緊密結合***

網路元素	設計目標	今天用作
VLAN	用於廣播域的隔離	控制伺服器之間互訪的路徑（二層打通）
IP地址	用於端點之間的可達	業務之間的訪問和控制

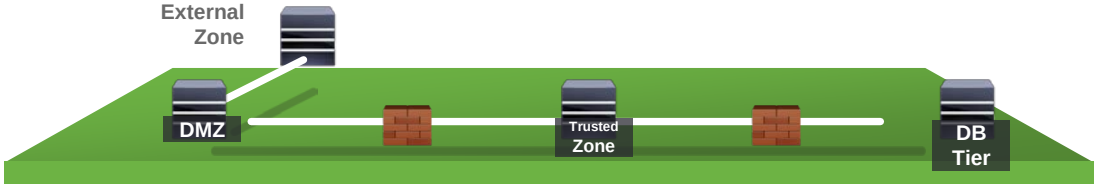
資料中心的維運視角

應用管理員

安全管理員

網路系統管理員

應用系統



安全系統

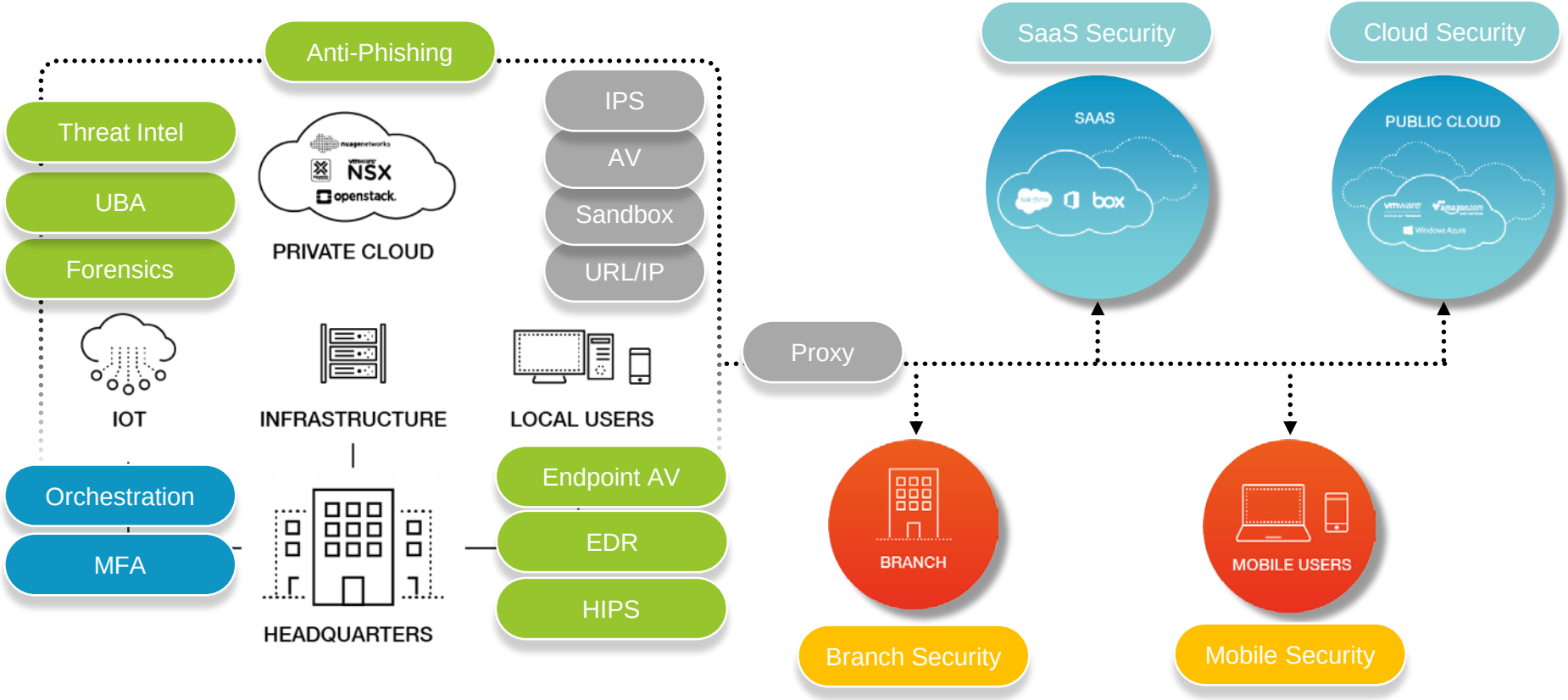
基礎網路

雲平臺管理員

依賴人工的運維模式

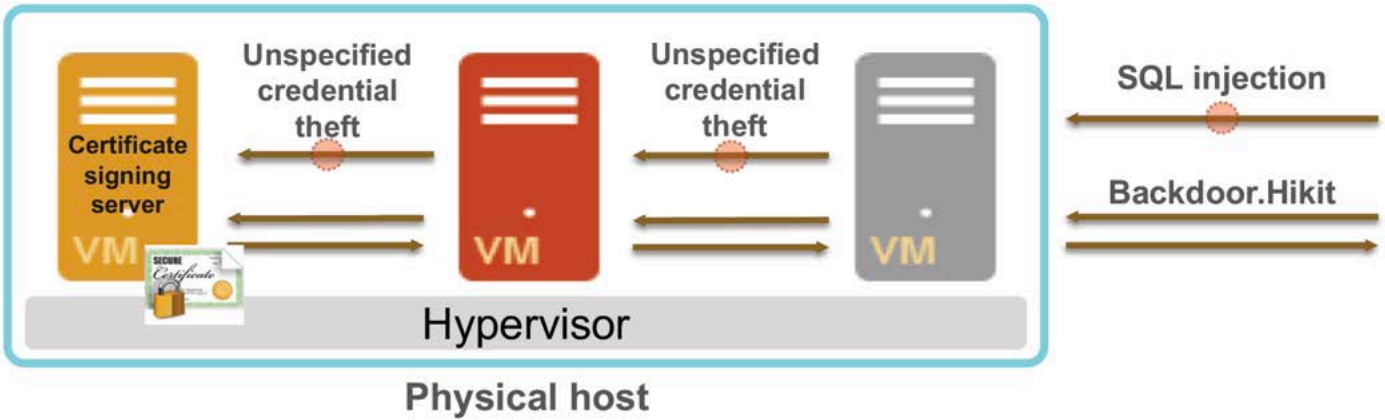
- 面向設備的操作
- 事件觸發，被動維運
- 依賴個人經驗
- 回應時間難以保障
- 人工維運出錯的可能性

服務隨時取得,但服務使用安全嗎? 邊界不復存在



來自“東西向”的安全挑戰

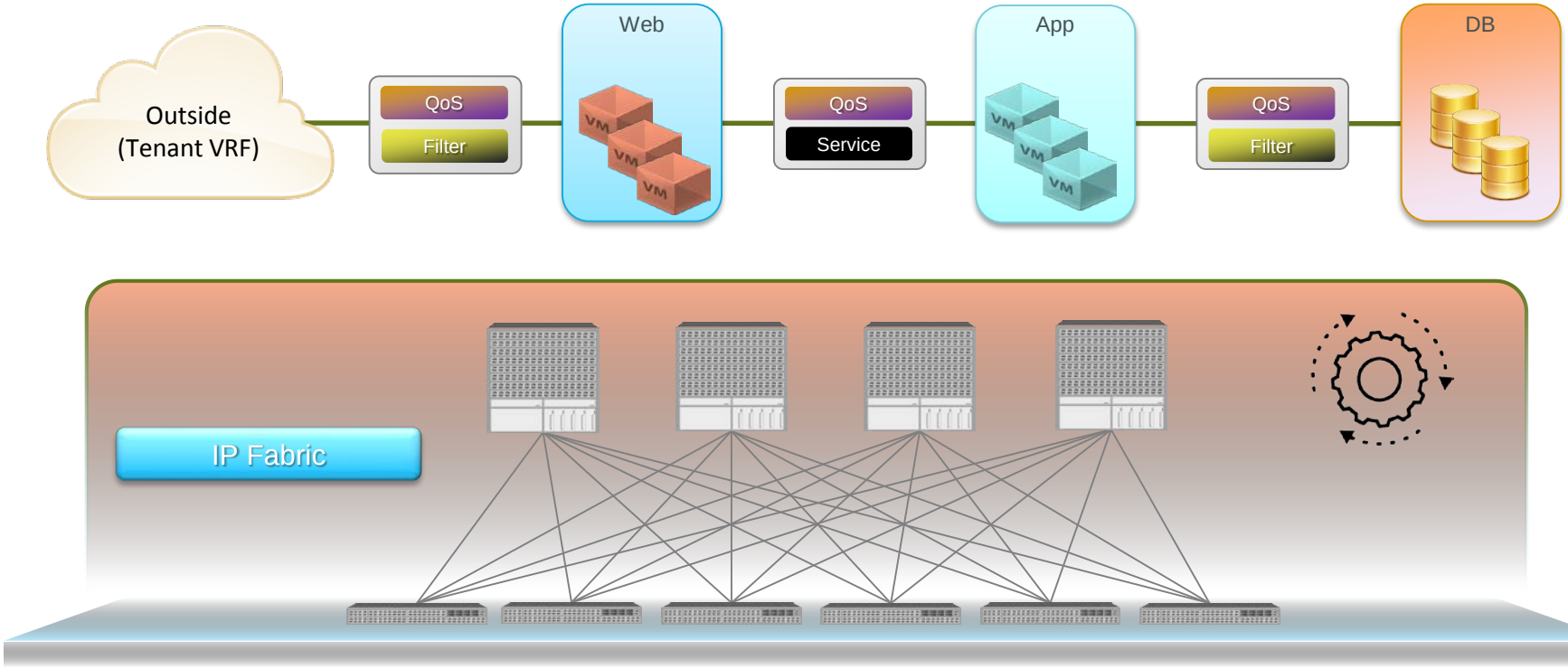
- Hidden Lynx攻擊案例分析
  - Hidden Lynx是一個頂級駭客組織，在過去的5年中發起了多起APT攻擊
  - 針對Bit9的攻擊行動：先是利用SQL注入攻陷Bit9的WEB伺服器，進而通過橫向移動，獲得了一台數位簽章證書的伺服器許可權，對一些木馬和惡意程式碼腳本簽發證書
  - 用戶的Bit9 Agent會將那些惡意程式碼識別為合法的程式，從而讓攻擊者順利進入受害人網路。



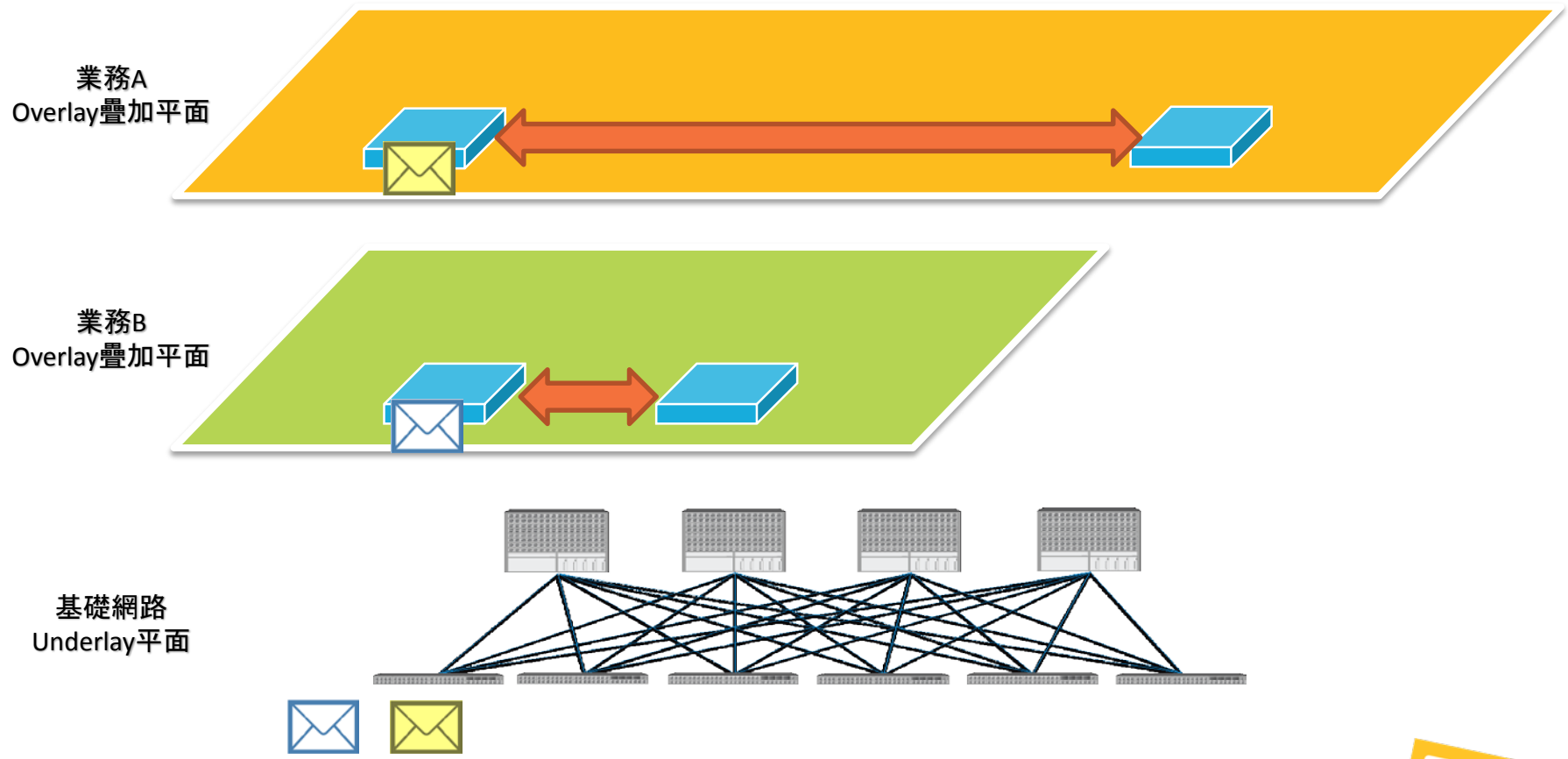
打造面向應用和業務的資料中心
(Private Cloud/SDN)

SOLUTIONS

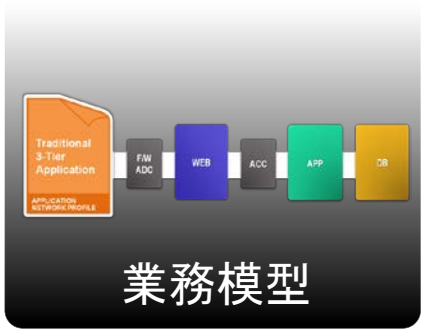
面向應用服務的資料中心



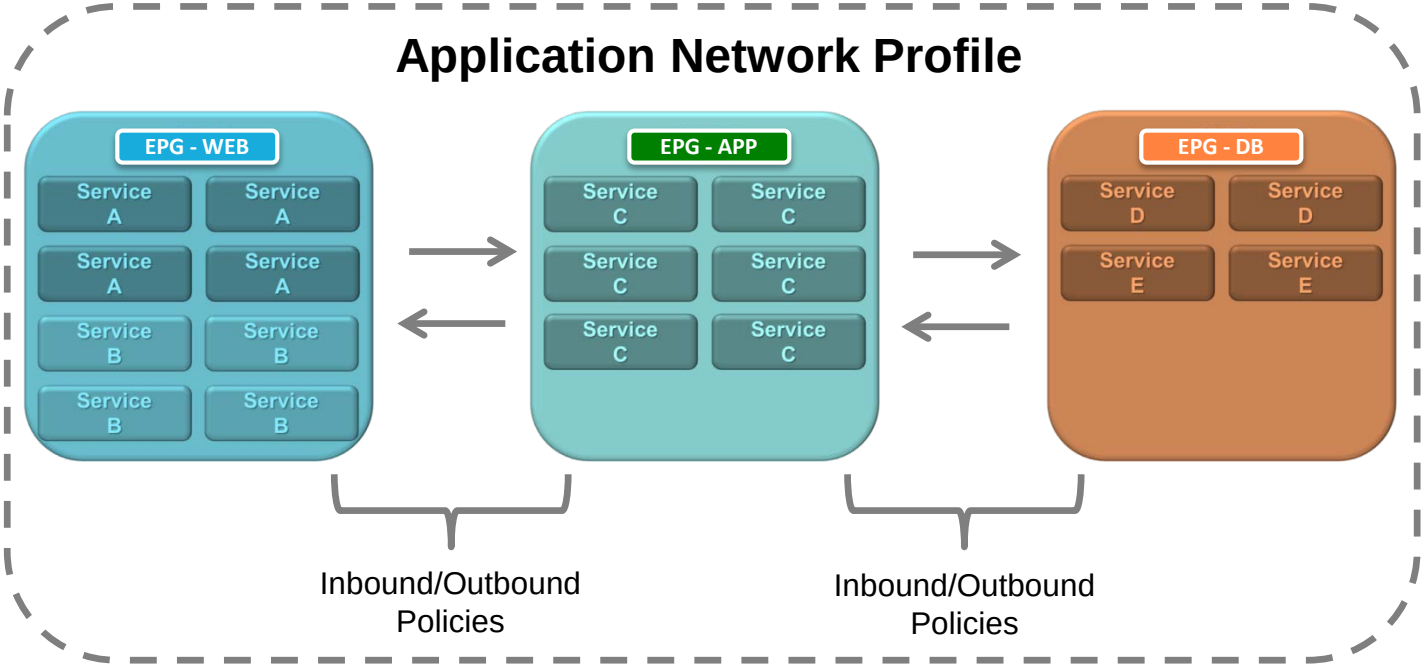
實現機制：構建基於OVERLAY的疊加網路平面



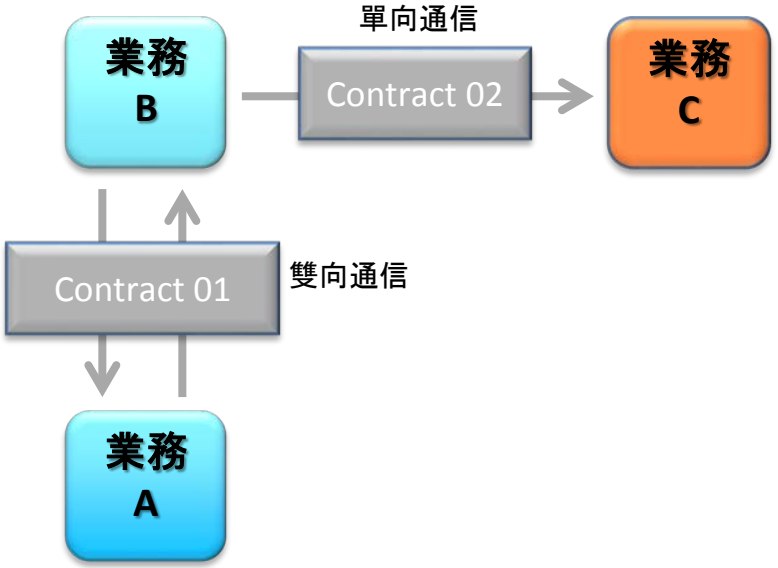
業務邏輯的映射 – 應用服務的辨識

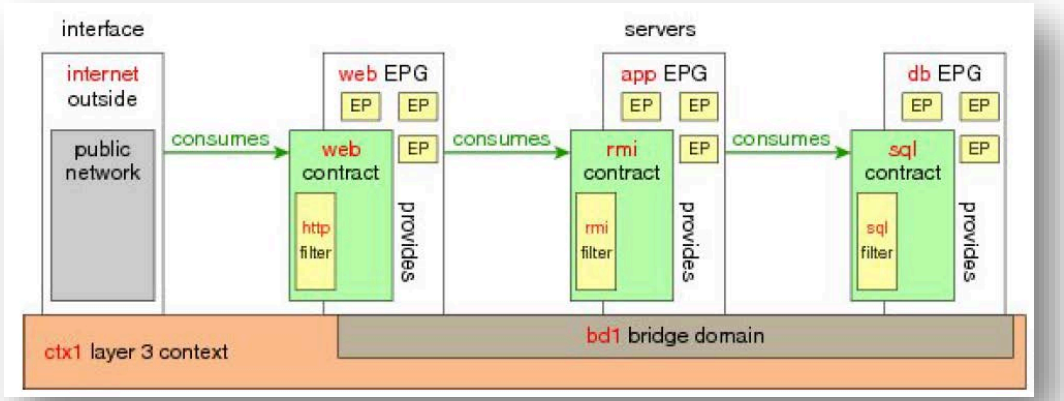


=



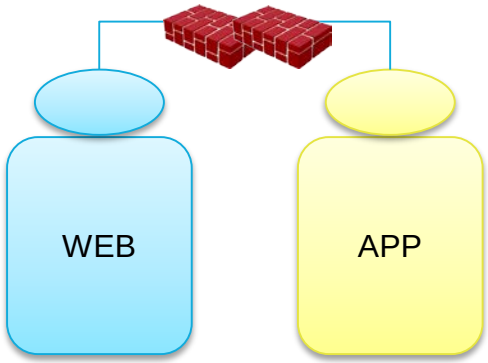
業務之間的訪問策略 – 應用服務之間的安全控管

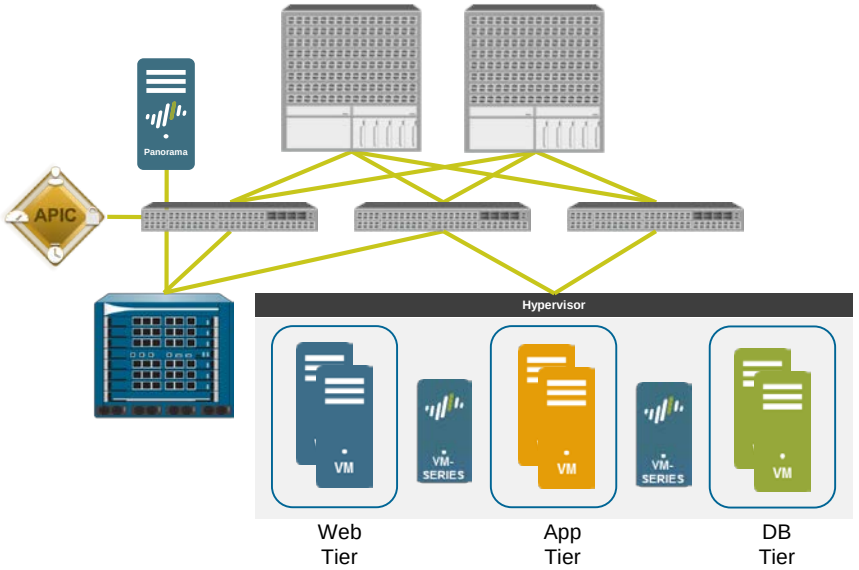




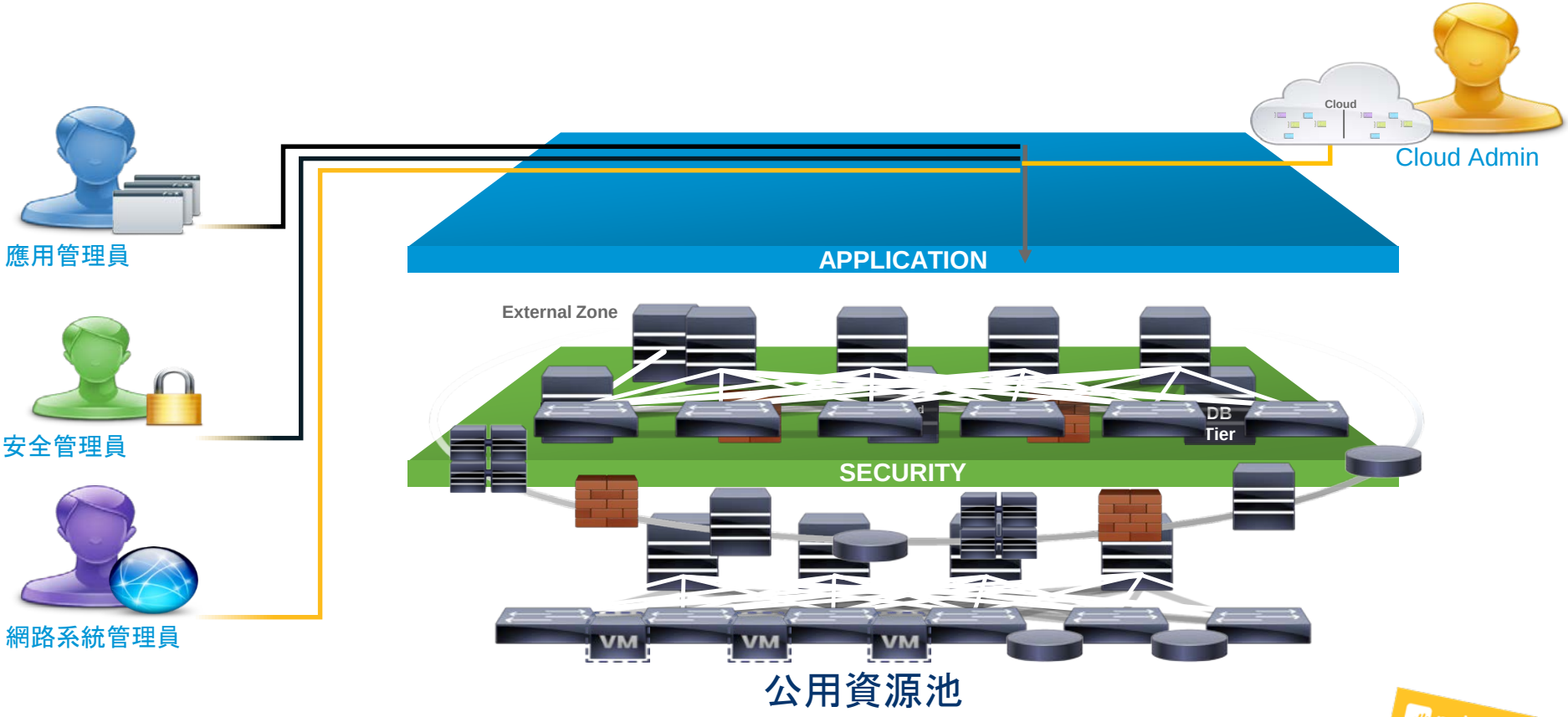
面向應用服務的資料中心安全部署

- 物理防火牆
- 虛擬防火牆
- 可以提供業務之間的L4-L7防火牆





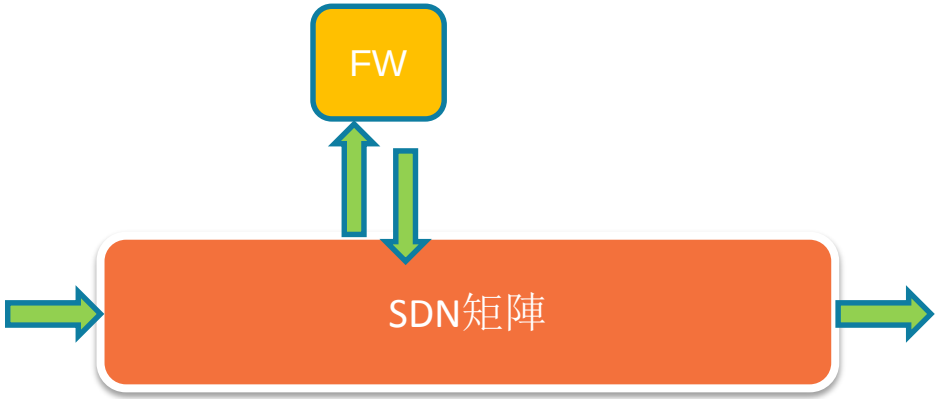
面向應用的數據中心的運維視角

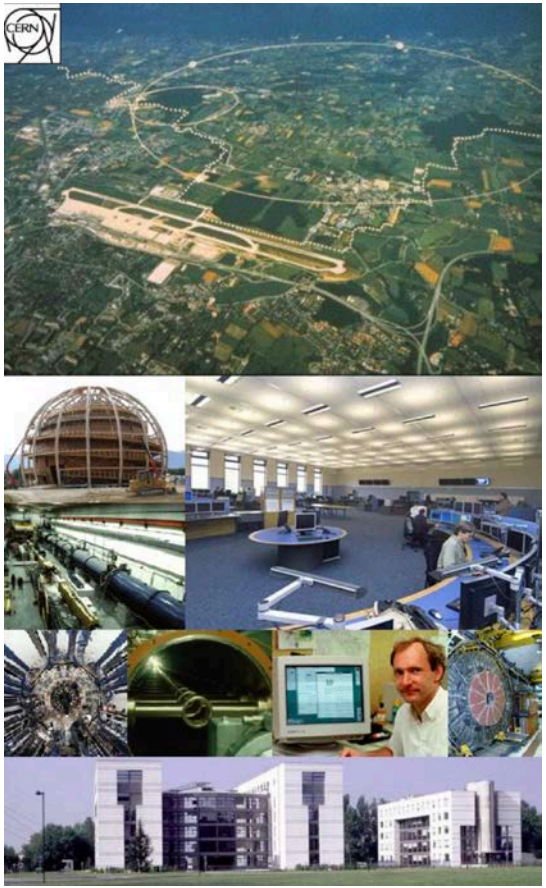


部署

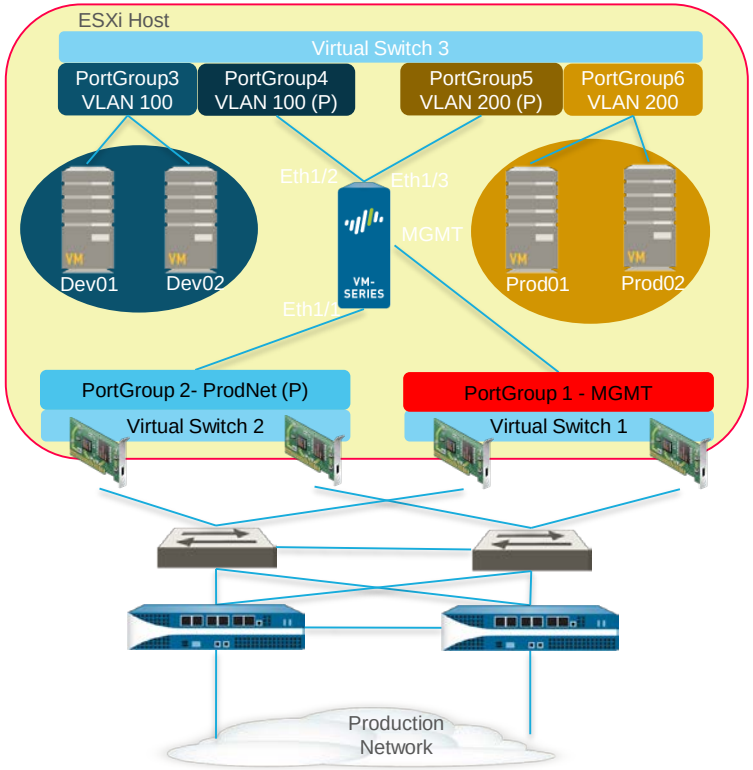
SOLUTIONS

基於SDN的物理防火牆部署方案





虛擬化資料中心防火牆二層部署模型



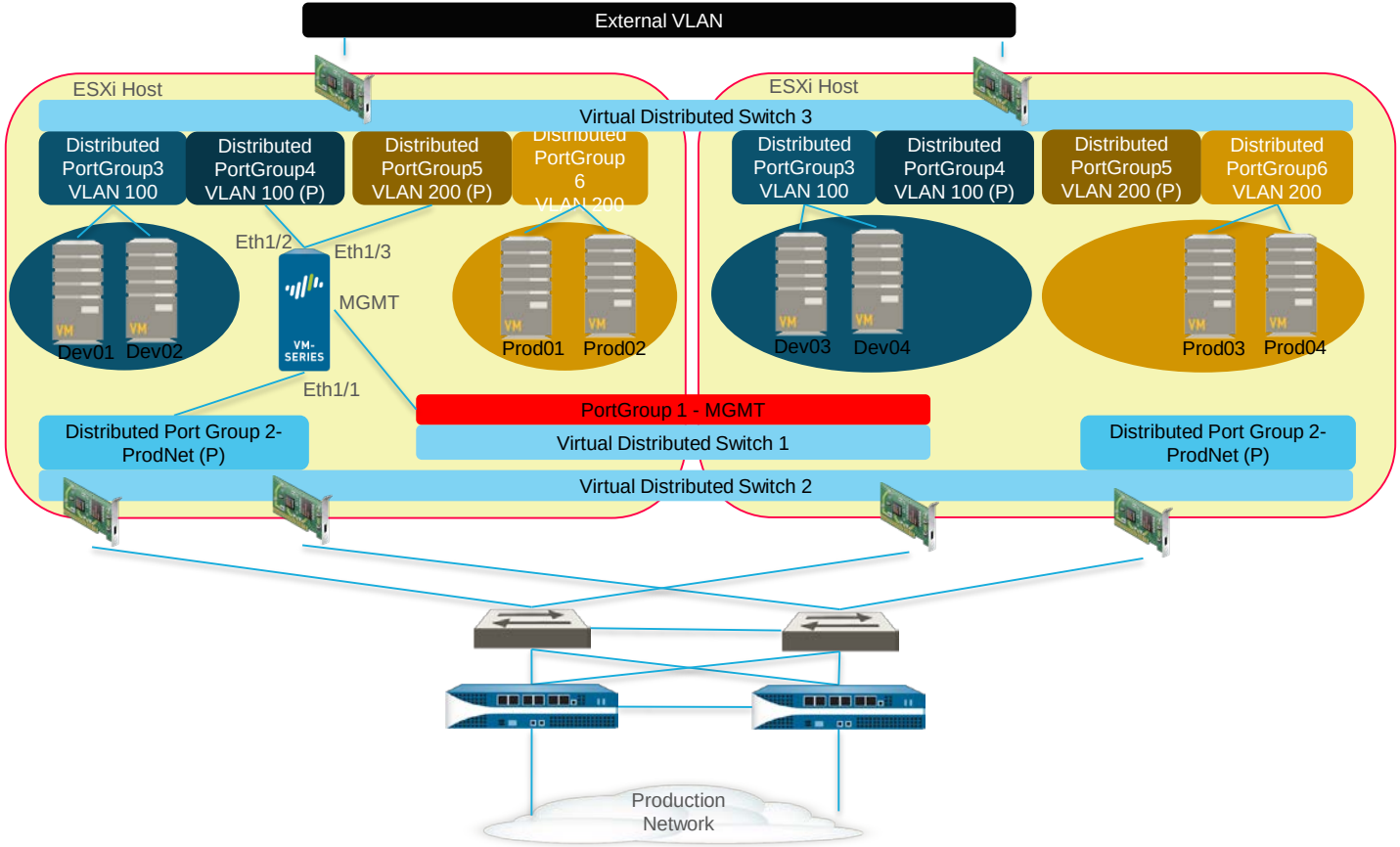
VM-Series配置模型

- 管理埠連接到獨立的vSwitch
- 所有VM在同一個三層子網中
- 所有介面在同一個VLAN中
- Promiscuous PortGroups
- 提供Inter-Zone 流量的安全性原則保護

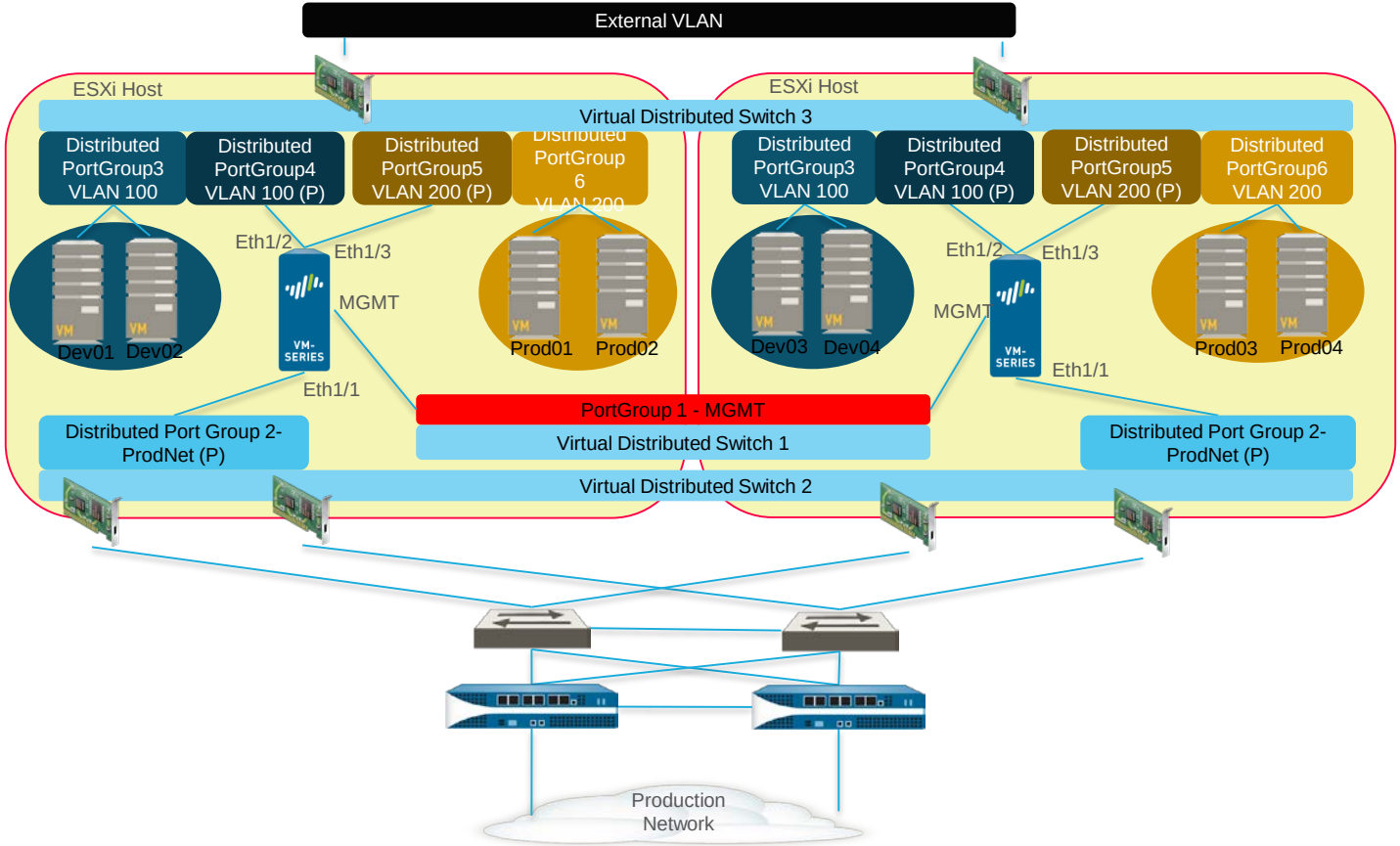
vSphere配置模型

- 只在vSwitch3中設置PortGroup VLAN
- 只有ProdNet 和 MGMT 與外部網路互連

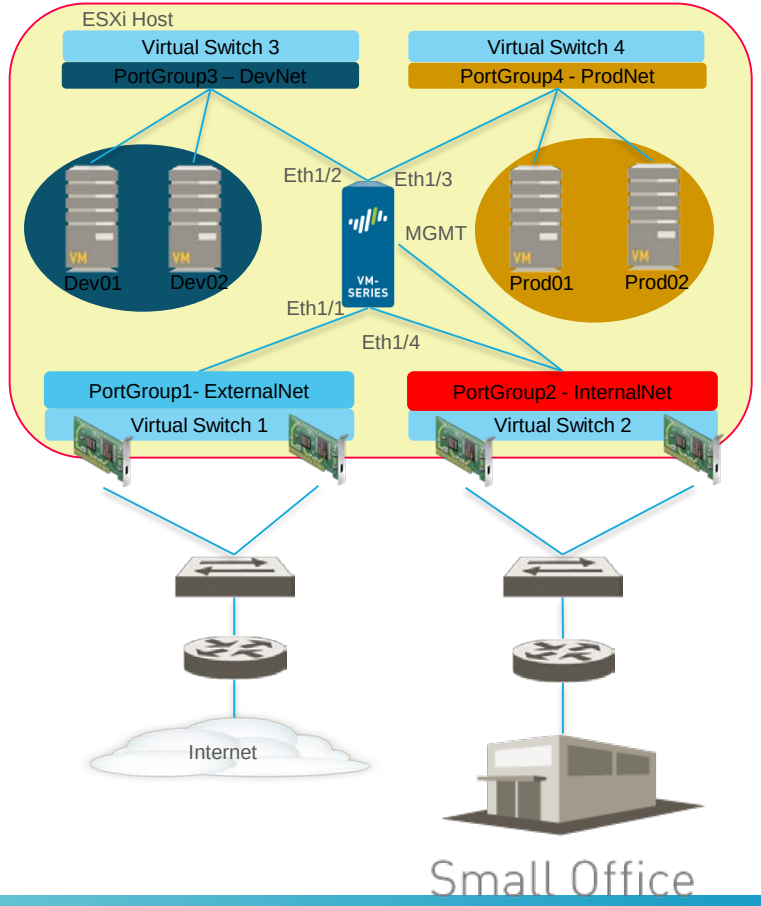
虛擬化資料中心防火牆二層分散式部署模型



虛擬化資料中心防火牆二層分散式HA部署模型



虛擬化資料中心防火牆三層隔離部署模型



VM-Series配置模型

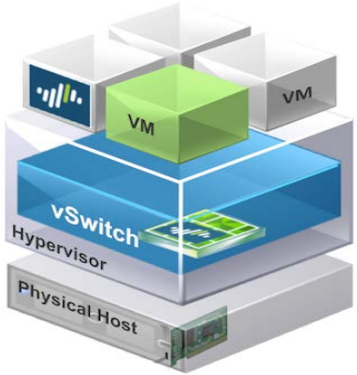
- 所有的介面均為三層介面
- 每個介面連接到不同的vSwitch
- 管理介面連接到專用的管理網路
- VM防火牆作為每個網段的閘道設備

vSphere配置模型

- 每個 vSwitch 都是一個獨立的三層網路
  - vSwitch1 – 10.1.1.0/24
  - vSwitch2 – 10.1.2.0/24
  - vSwitch3 – 10.1.3.0/24
  - vSwitch4 – 10.1.4.0/24

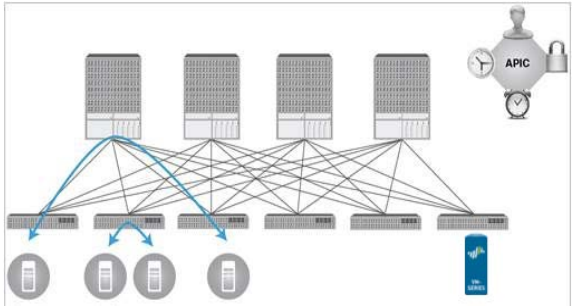
SDN資料中心部署方案

VMware NSX



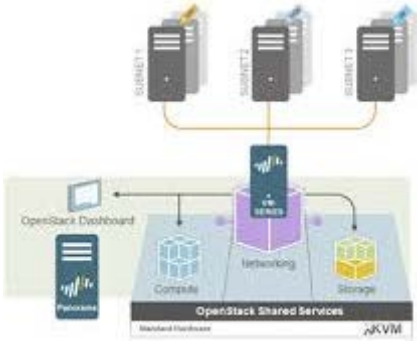
- 網路和安全虛擬化平臺
- 建立在 ESX 虛擬機器管理程式之上，同時集成 vCenter
- 成熟、可用於生產的解決方案

Cisco ACI



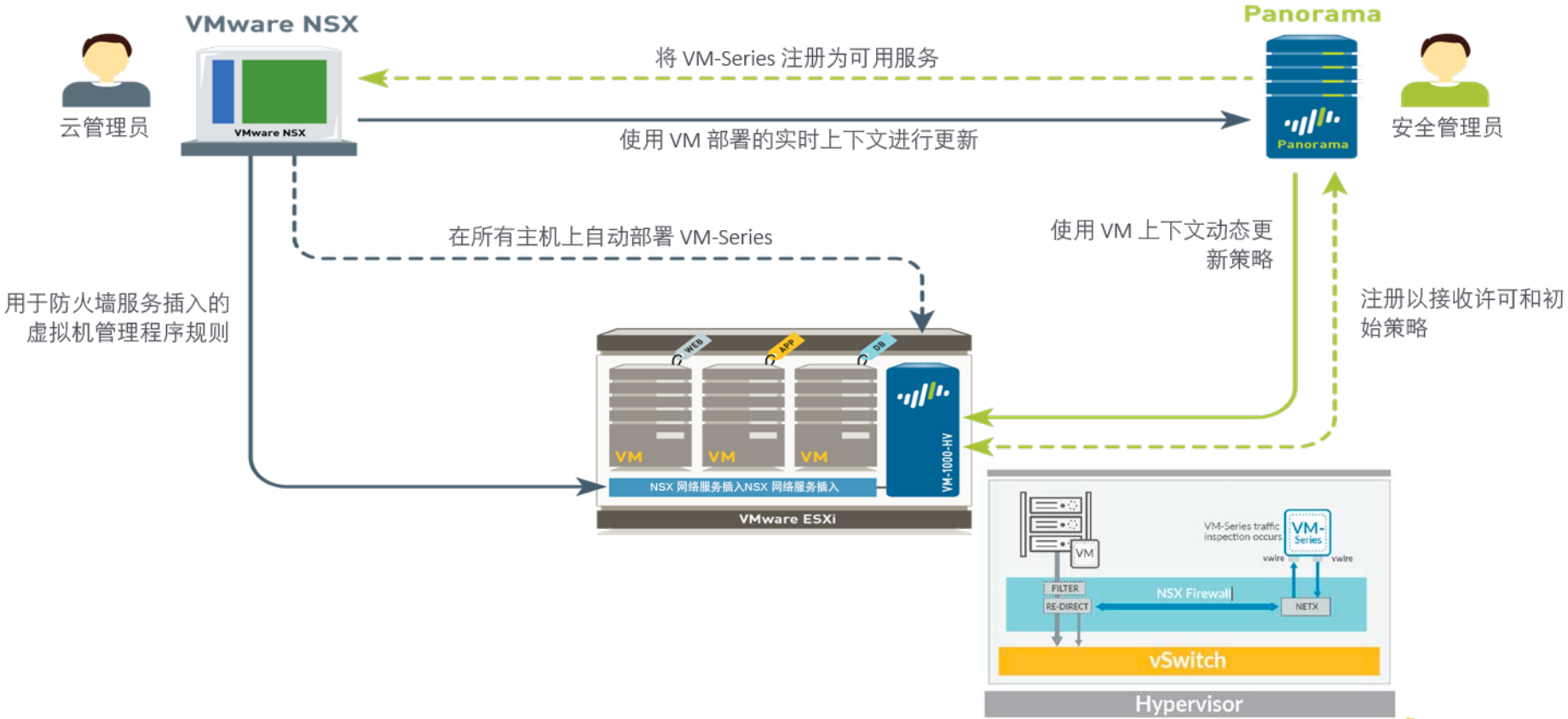
- 基於硬體的解決方案
- APIC 控制器編排網路配置
- 整體式升級安裝用戶群以支援 ACI

OpenStack/KVM

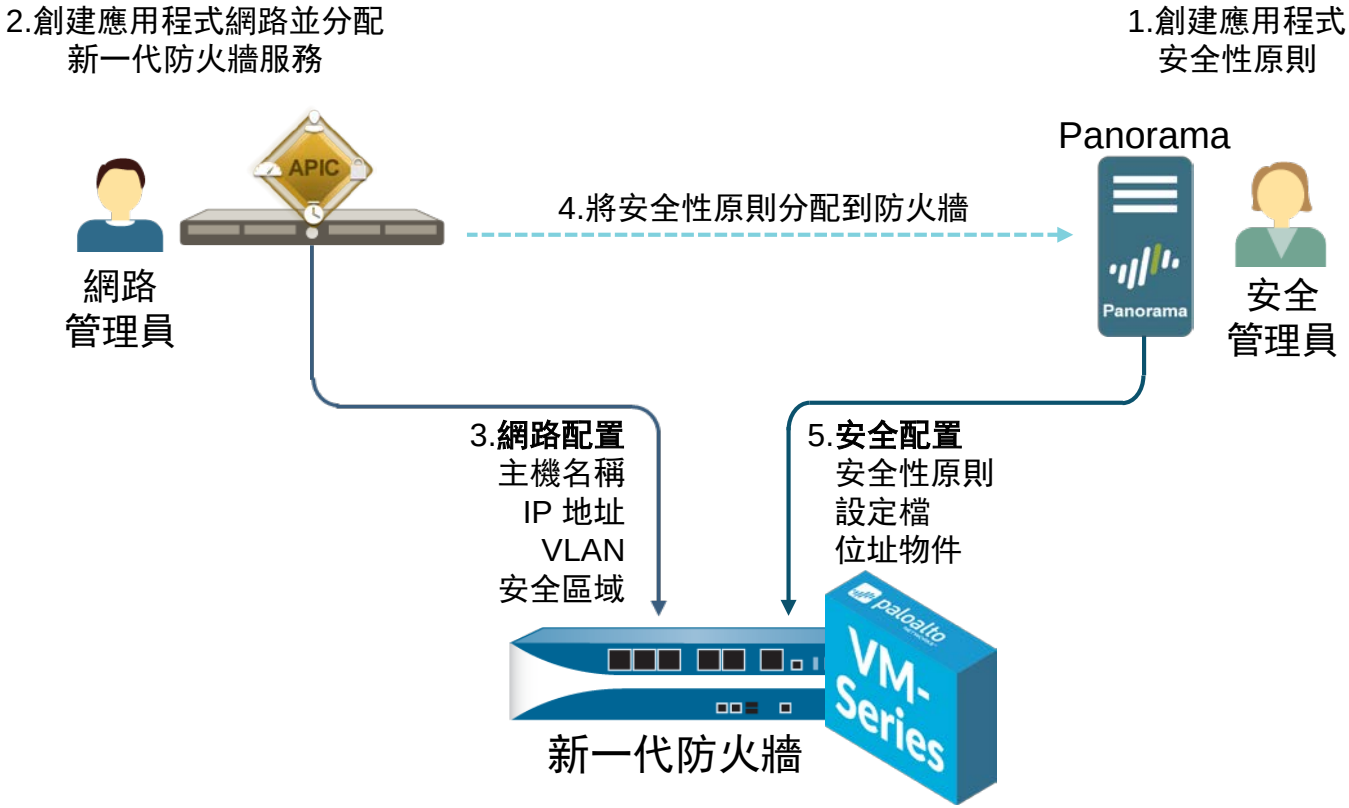


- 雲編排平臺
- 不斷變化
- 需要內部工程人員

與 VMWARE NSX無縫集成



與 CISCO ACI 集成

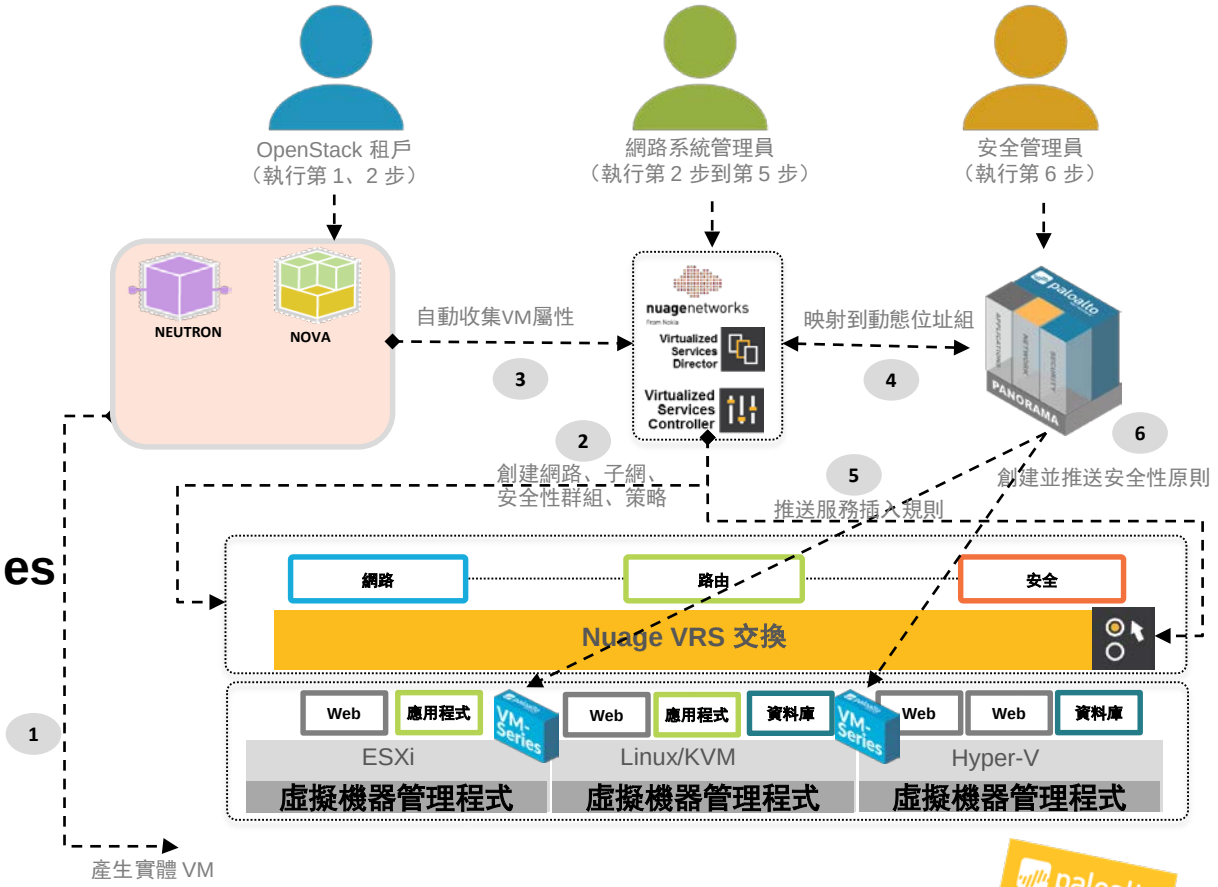


OPENSTACK 工作流示例

商業 OpenStack
- 編排與配置

SDN（例如 Nuage VSP）
- 虛擬網路與微分段
- 服務插入

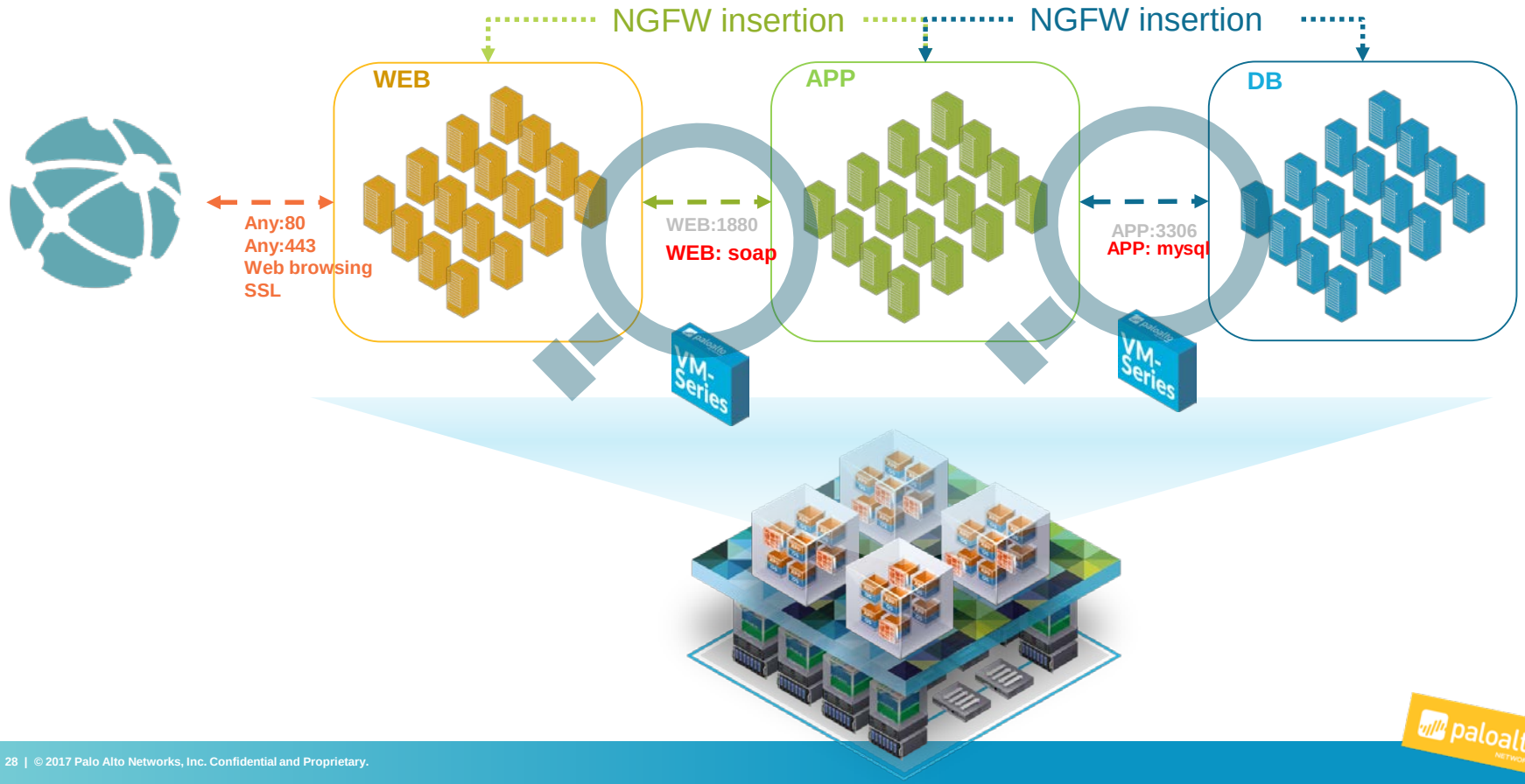
Palo Alto Networks VM-Series
- 應用程式微分段
- 高級威脅防護



應用案列分享

SOLUTIONS

應用案例：東西向流量的視覺化(Visibility)



應用案例：資料中心APT威脅防護(深度分析)

- 保護資料中心東西向流量，實現已知和未知威脅的自動化防禦

1 減少受攻擊面

- 阻斷高風險應用
- 阻止已知病毒和滲透威脅
- 阻斷常用的滲透檔案類型

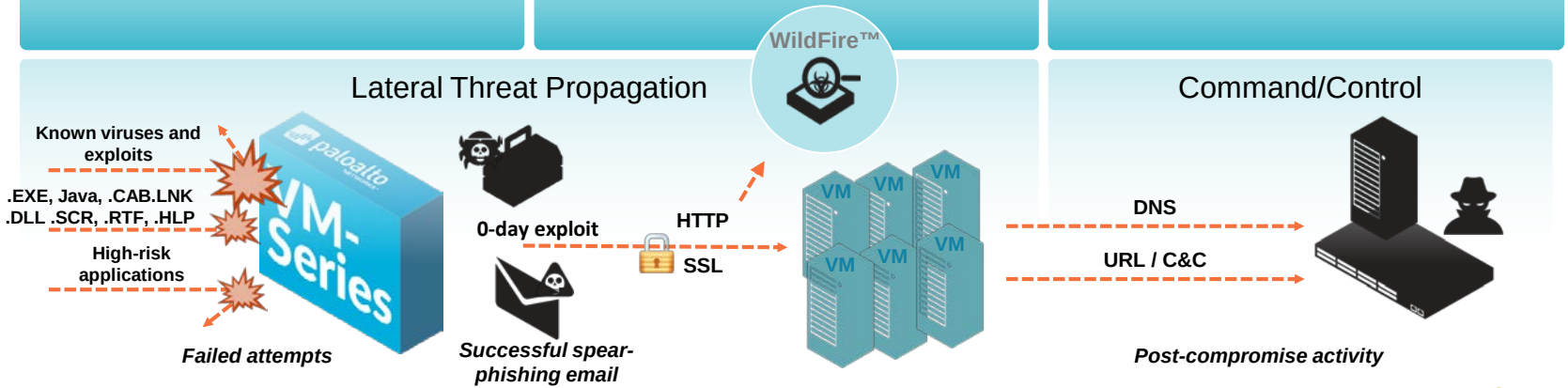
2 檢測未知威脅

- 對所有的應用流量進行識別和分析
- 對SSL流量進行解密和分析
- 通過WildFire沙箱功能識別未知威脅，將未知威脅轉變為已知威脅

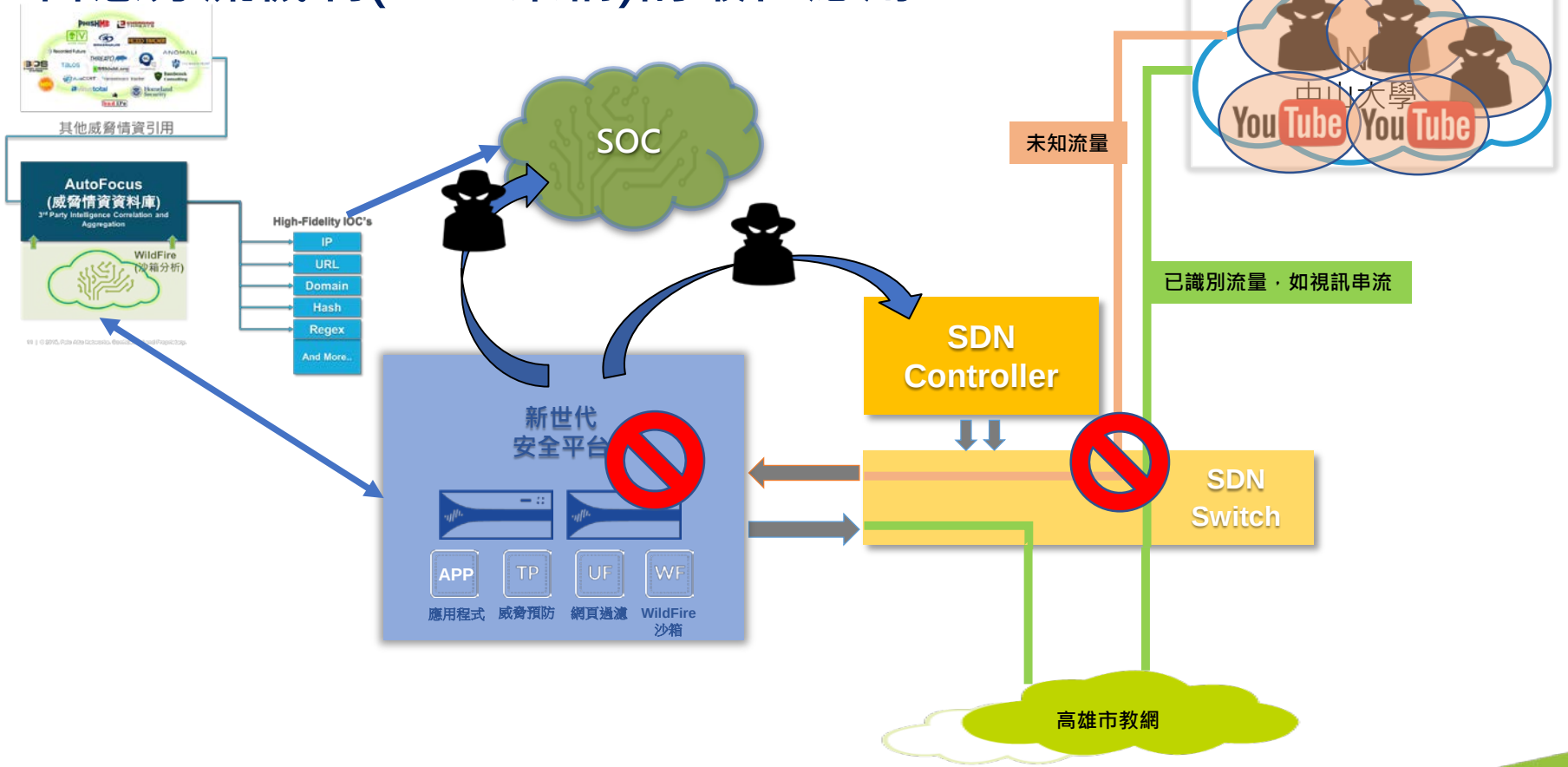
3 自動創建保護

通過以下方式檢測和阻斷C&C攻擊行為:

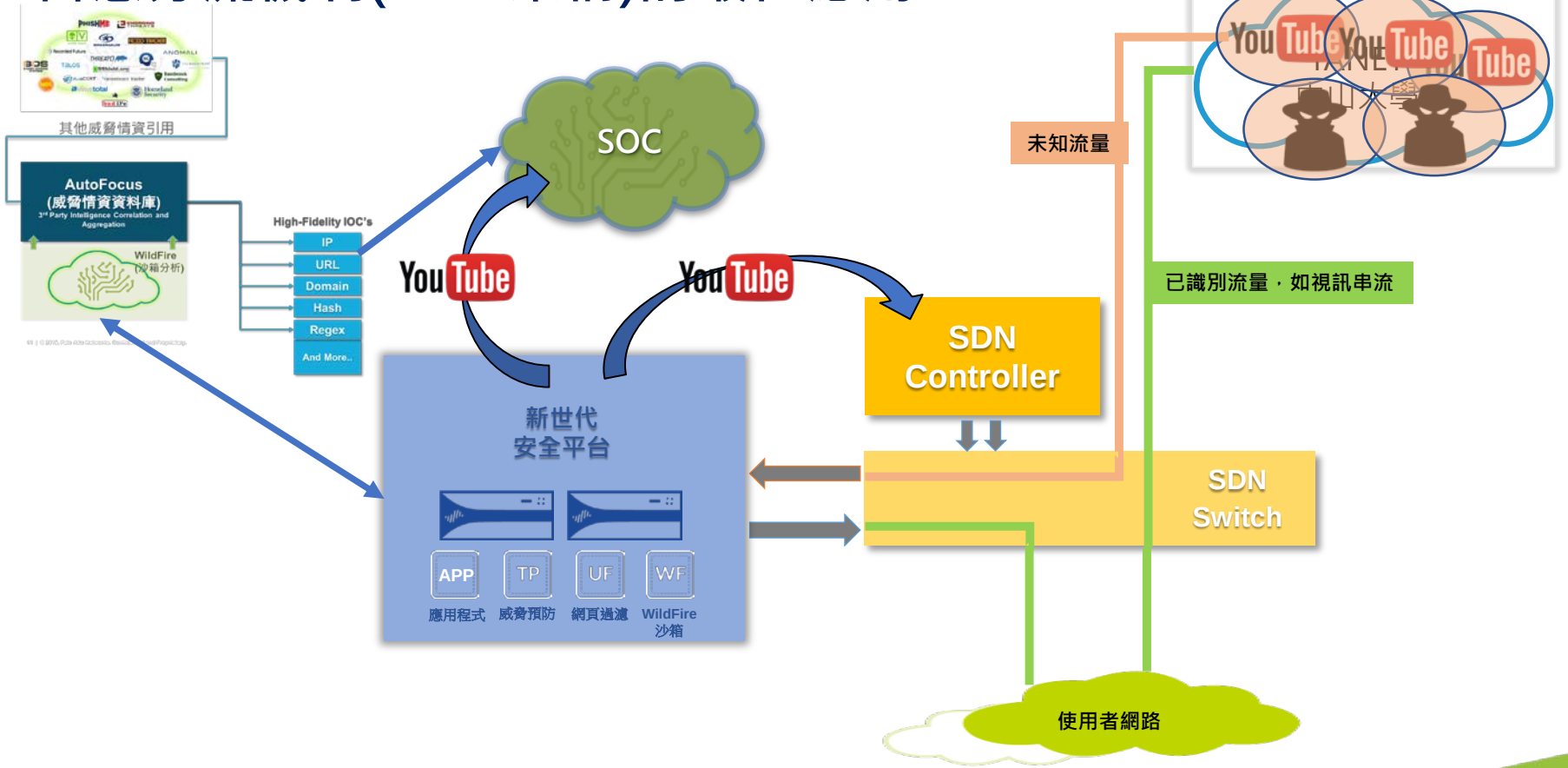
- DNS流量中的惡意功能變數名稱資訊
- URLs (PAN-DB)
- C&C行為特徵分析



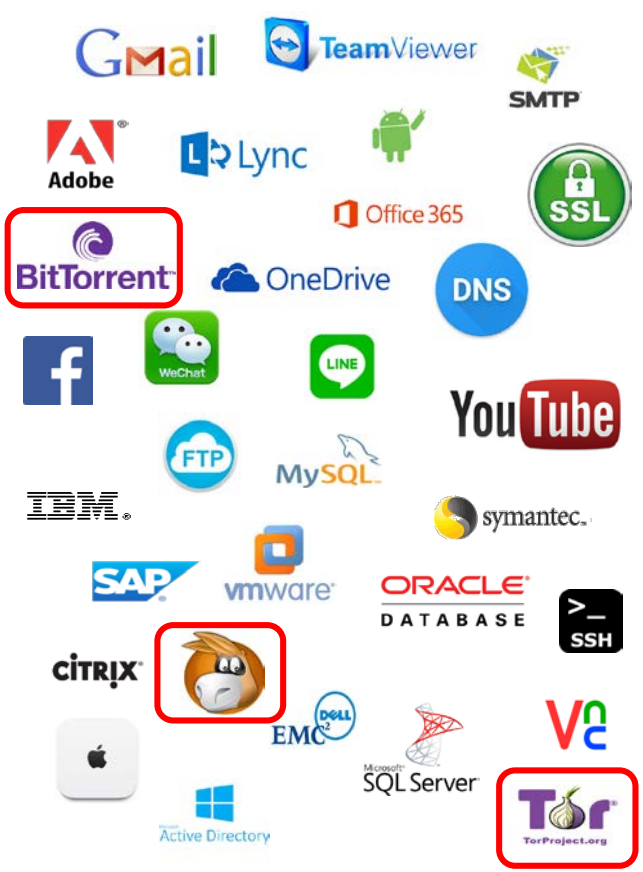
智慧分流機制(SDN架構)的最佳應用



智慧分流機制(SDN架構)的最佳應用



提供新一代應用程式識別機制確保智慧分流機制效益



Protocol Decoders 通訊協定解譯

- Detect Protocol in Protocol within a session
- Provide context for Application Signatures

Application Signatures 應用程式特徵碼

- Detect Layer 7 signatures within a session

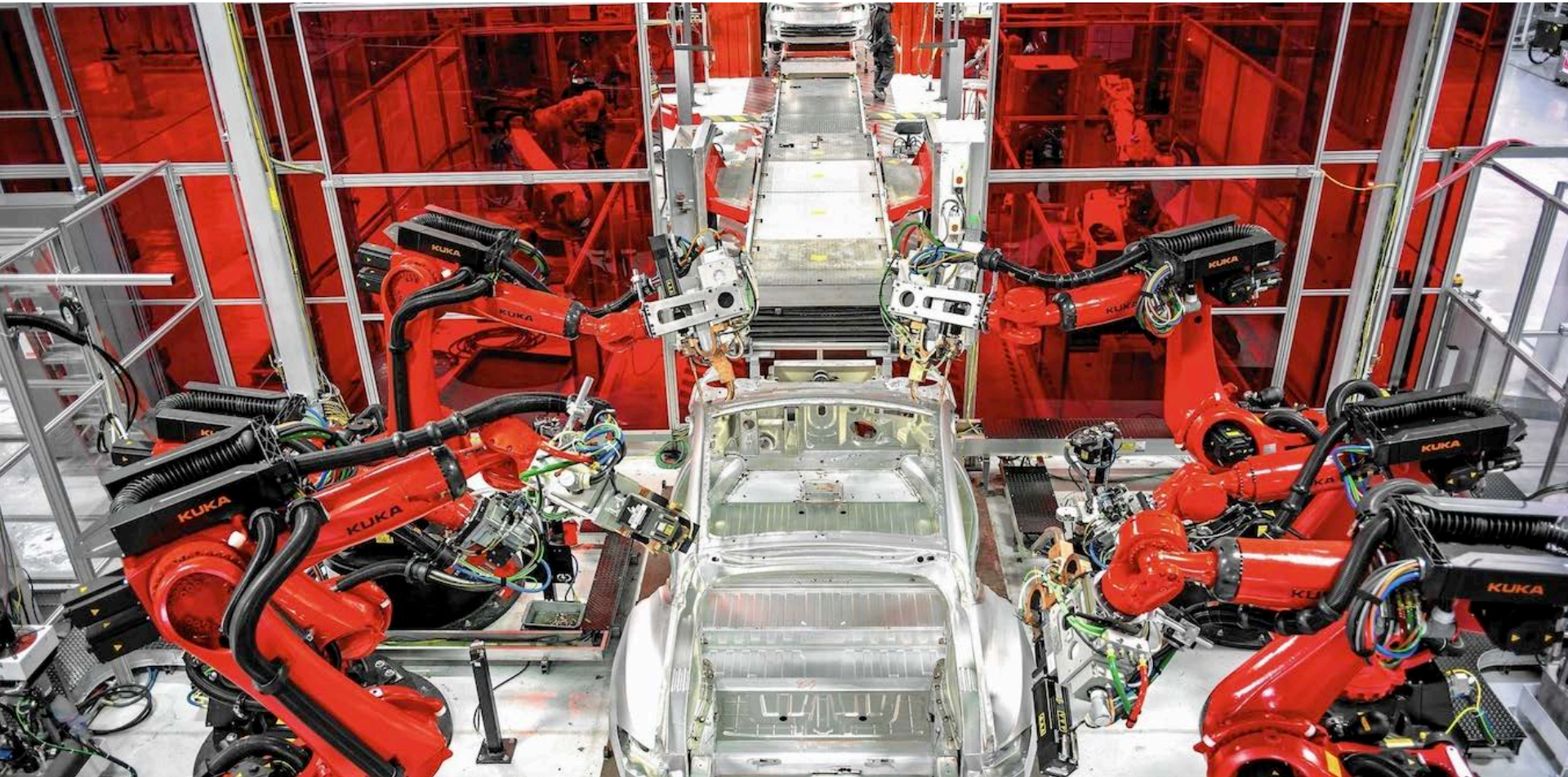
Protocol Decryption 通訊協定解密

- SSL & SSH decryption

Heuristics 啟發式連線行為特徵

- Looks for patterns of communication when no signature exists

API是整合以及自動化的基礎



Secure SDN

Secure Your Data

paloalto NETWORKS®

Appendix

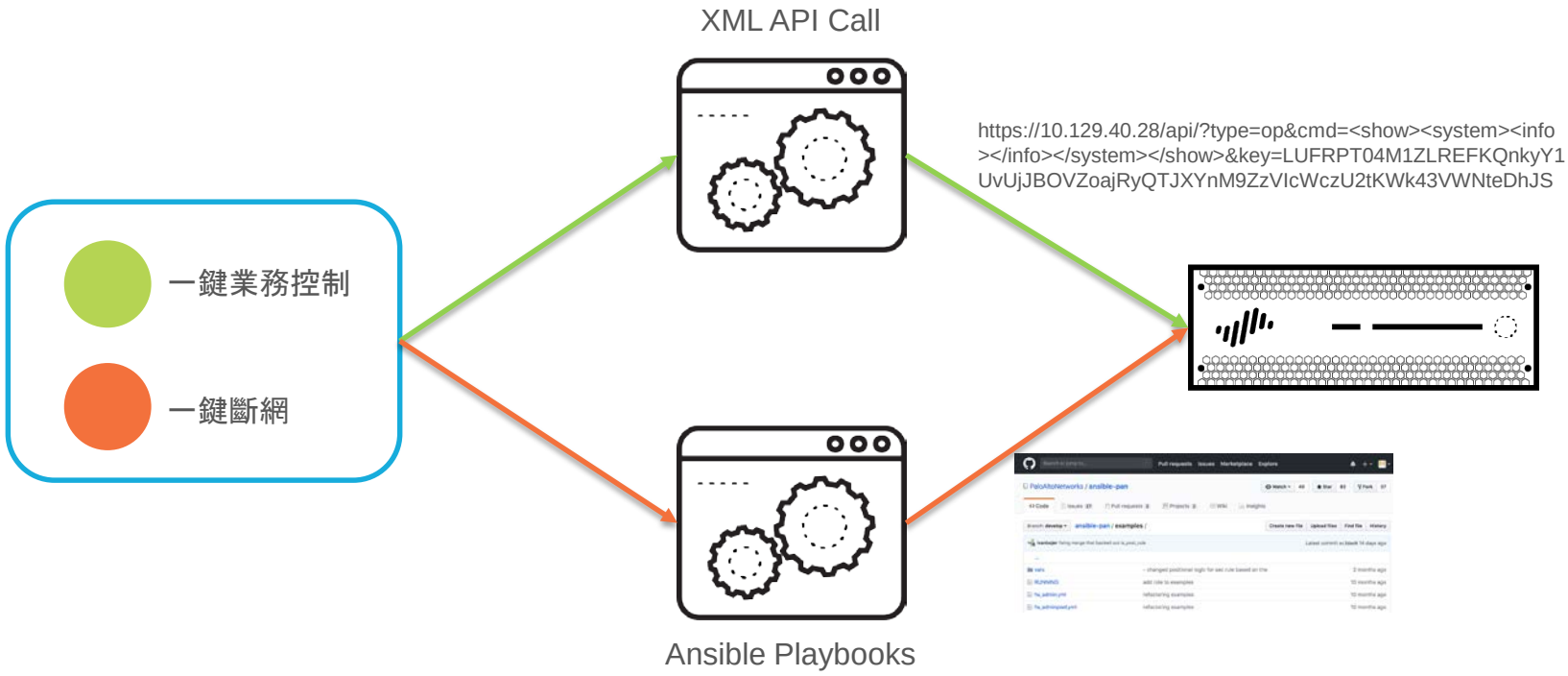
Ansible模組和劇本

- Ansible是新出現的自動化運維工具
  - 實現了批次系統配置、程式部署、運行命令等功能
  - 通過連接外掛程式connection plugins，實現和被監控端通信
  - 通過playbook劇本實現多個任務的自動化執行
- Palo Alto Networks已經構建了一系列Ansible模組，可以說明將安全性無縫集成到DevOps流程中
  - Palo Alto Networks的Ansible模組可用於配置下一代防火牆和Panorama
  - Ansible模組使用Palo Alto Networks XML API與下一代防火牆和Panorama進行通信
  - 提供了社區支援

https://github.com/PaloAltoNetworks/ansible-pan

http://panwansible.readthedocs.io/en/latest/

自動運維：一鍵業務控制



自動運維：多系統聯動

案例：Curtin University

- Curtin is in the global top 20 “Young Universities” (Uni’s under 50 years old)
- 52,000 students
- Campuses in Western Australia (3 locations), Malaysia, Singapore, Dubai and Mauritius
- Local Datacenters and Cloud with AWS
- Integration with ACI – 4 x PA5260s TP,URL,WF

東西向流量通過策略引導到防火牆