越世實業

SDN - SOLUTIONS

主講人　S.C. WANG

WAY SDN

SOFTWRAE-DEFINED NETWORKING

為什麼需要 SDN

NETWORK TROUBLESHOOTING CHALLENGES

MANUAL

- DEPLOY NETWORK TAPS FOR EACH SWITCH
- INCREASE IN COMPLEXITY OF NETWORKS BUT THE TOOL SETS ARE THE SAME
- ERROR PRONE DUE TO THE NATURE OF MANUAL TOOLS

TIME CONSUMING & COMPLEX

- TIME CONSUMING PROCESS
- REQUIRE LOW LEVEL DETAILED INPUTS
- COMPLEX WITH MULTIPLE STEPS TO DIAGNOSE THE PROBLEM

COSTLY

- EXPENSIVE NETWORK TOOLS
- SENDING QUALIFIED RESOURCES TO TROUBLESHOOT IS COSTLY
- TIME WASTED TO TROUBLESHOOT

WAY SDN - 為什麼需要 SND

SDN NETWORK VISUALIZER SDN APP

AUTOMATED AUDITING

- REAL TIME VISIBILITY INTO TRAFFIC
- AUTOMATED AUDITING OF USER' S NETWORK TRAFFIC
- RESTFUL APIS FOR 3RD PARTY SECURITY SOLUTION INTEGRATION

FAST TROUBLESHOOTING

- FAST TROUBLESHOOTING
- LESS STEPS TO GET TO ROOT CAUSE ANALYSIS
- EASE OF ACCESS TO DETAILED DIAGNOSTICS

COST EFFECTIVE

- 40X[1] COST SAVING COMPARED
- TO MANUAL TAPPING TOOLS
- NO ONSITE TECHNICIAN FOR TROUBLESHOOTING

WAY SDN - 為什麼需要 SND

SDN NETWORK DEFENSE DIFFERENT

BEFORE

1. 傳統交換機，傳統路由器組合而成的網路，所有的設定，控制都必需由各個設備控制
2. 管理網路的最小單位為ＩＰ
3. 無法與其它網路設備資訊交換並執行資安區域聯防將災難控制在一個最小的範圍內

NOW

1. 核心層與匯聚層需為SDN交換機
2. 管理網路最小單位為第七層的網路封包
3. 所有封包可以透過第七層ＤＰＩ設備分析後，再決定其網路上的行為
4. 網路行為可以根據讓網使用者有具備的權限，而決放行或拒絕其行為

YESEE 五大方案

新一代網路架構管理願景

SDN INTRANET NETWORK ACTIVE DEFENSE KEY FEATURES

QoS function

- QoS action can be run in MAC / IP / port number / L7 rules

Tapping function

- Specify protocol, ports, IP/MAC addresses to select traffic for capture
- Filter all packets by each rules, then clone they to their switch ports

Access control function

- Network resources manage by l2-l4 / protocol / user id(must integrated with ad server) / application (must integrated with dpi devices).

Smart load balance function

- Each l2-l4 / protocol / user id(must integrated with ad server) / application (must integrated with dpi devices) has it's own gateway to internet.

Service Chain New Function

- By diffident packet, using diffident network device.
- High performance network device,
- Flexible network infrastructure.

QUALITY OF SERVICE 服務品質

WITH SDN-OPENFLOW

適用場景

網路管理

- 限制單日每個IP能夠使用的網路總流量，超過標準時則進行封鎖
- 限制每個網段的網路使用速率，避免小部分人員佔用大部分資源
- 檢測網路內的電腦是否疑似被殭屍網路所感染，讓該電腦的擁有者能夠在參與攻擊前進行電腦的清掃。

公用電腦管理

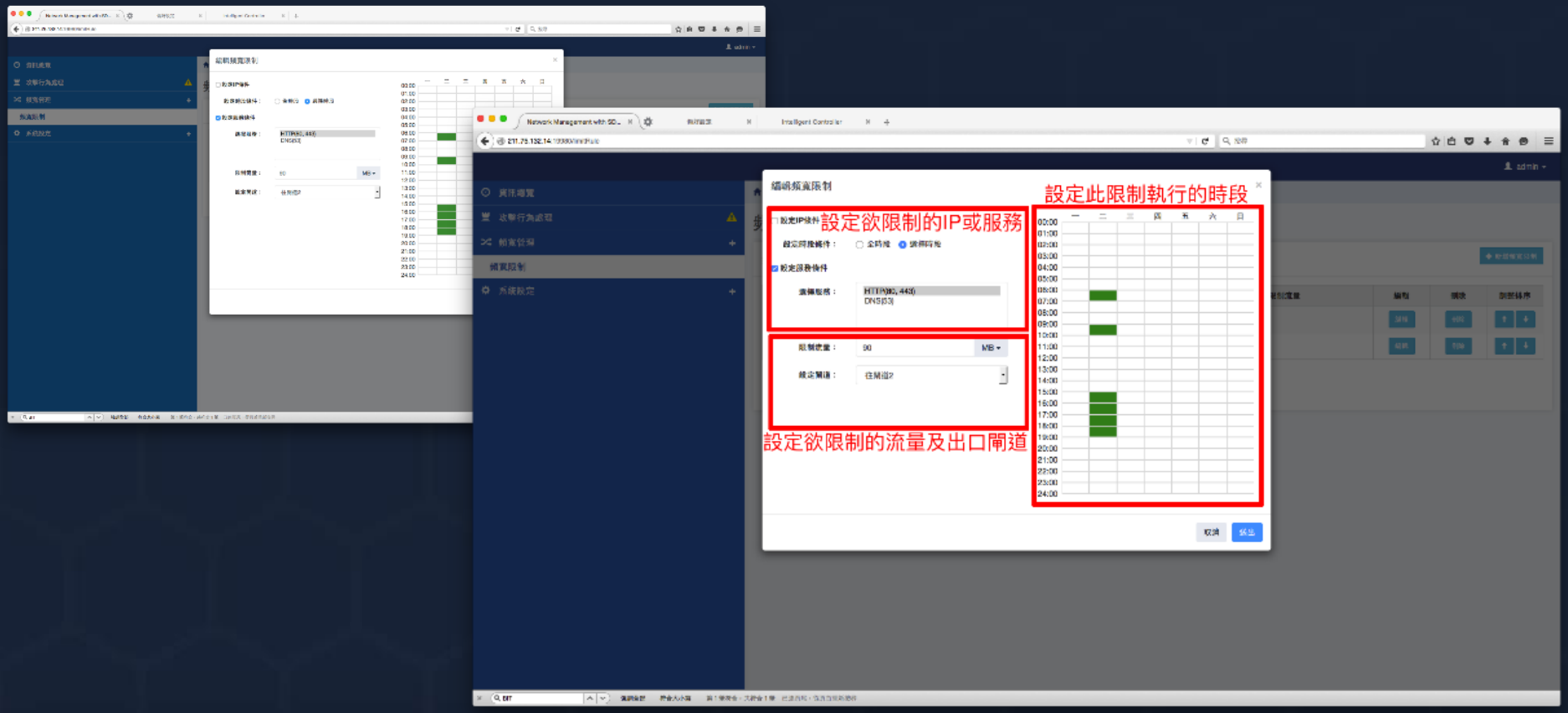
- 限制每個IP的網路使用速率，避免公用電腦被不當使用、或佔用頻寬
- 可在特定時間將特定網段的流量導入不同的閘道，製造隔離的網路環境。

服務品質管理

- 指定特定服務（如VOIP）經由設有專線的閘道線路通行，保障服務使用品質

操作介面

在設定的時段內，可針對特定的網段及網路服務進行流量限制、或指定不同的出口閘道



TAPPING 流量複制

WITH SDN-OPENFLOW

適用場景

大量網路流量需要分析

- 交換機 MIRROR 埠不夠。
- 不同網路流量分析工作系統需要各式各樣不同流量。

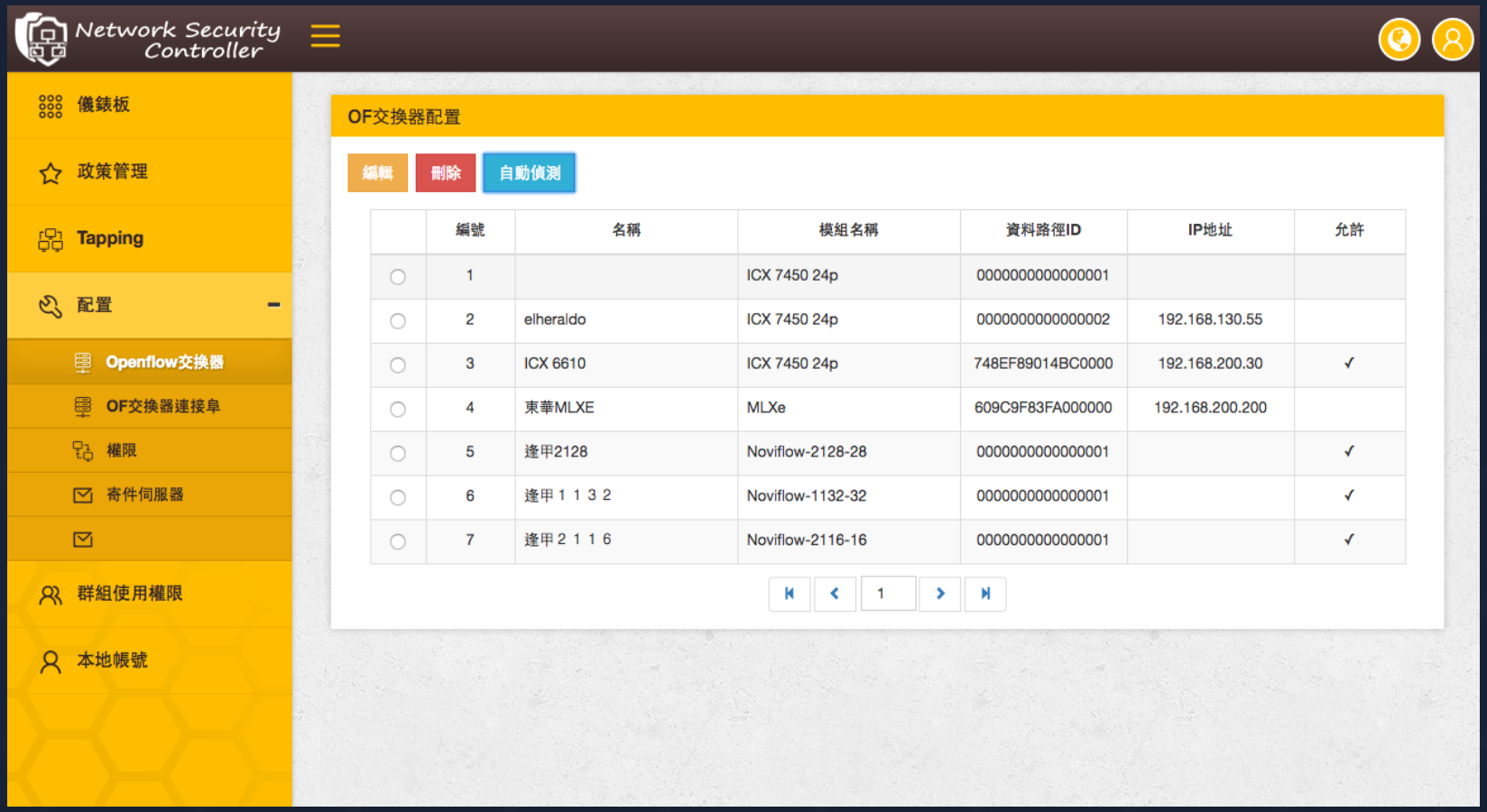
網路流量因不同需要必須增加額外條件

- 多個埠的流量需要匯總到同一個系統。
- 流量需加上網段，L2-L4，VLAN TAG 條件，符合後再進行複制。

不同的單位可以自行複制符合其 IP 的網路流量

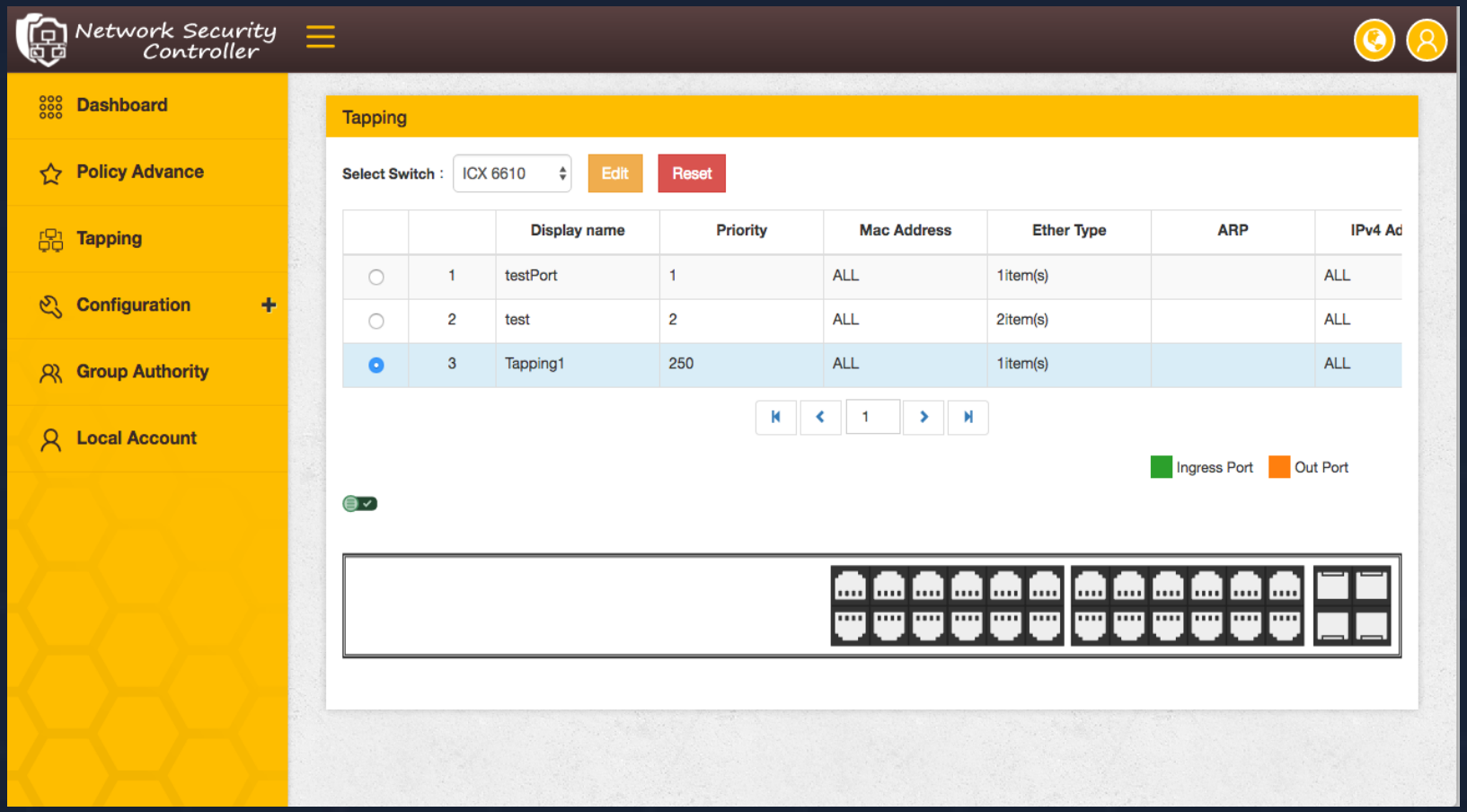
操作介面

SWITCH CONFIG



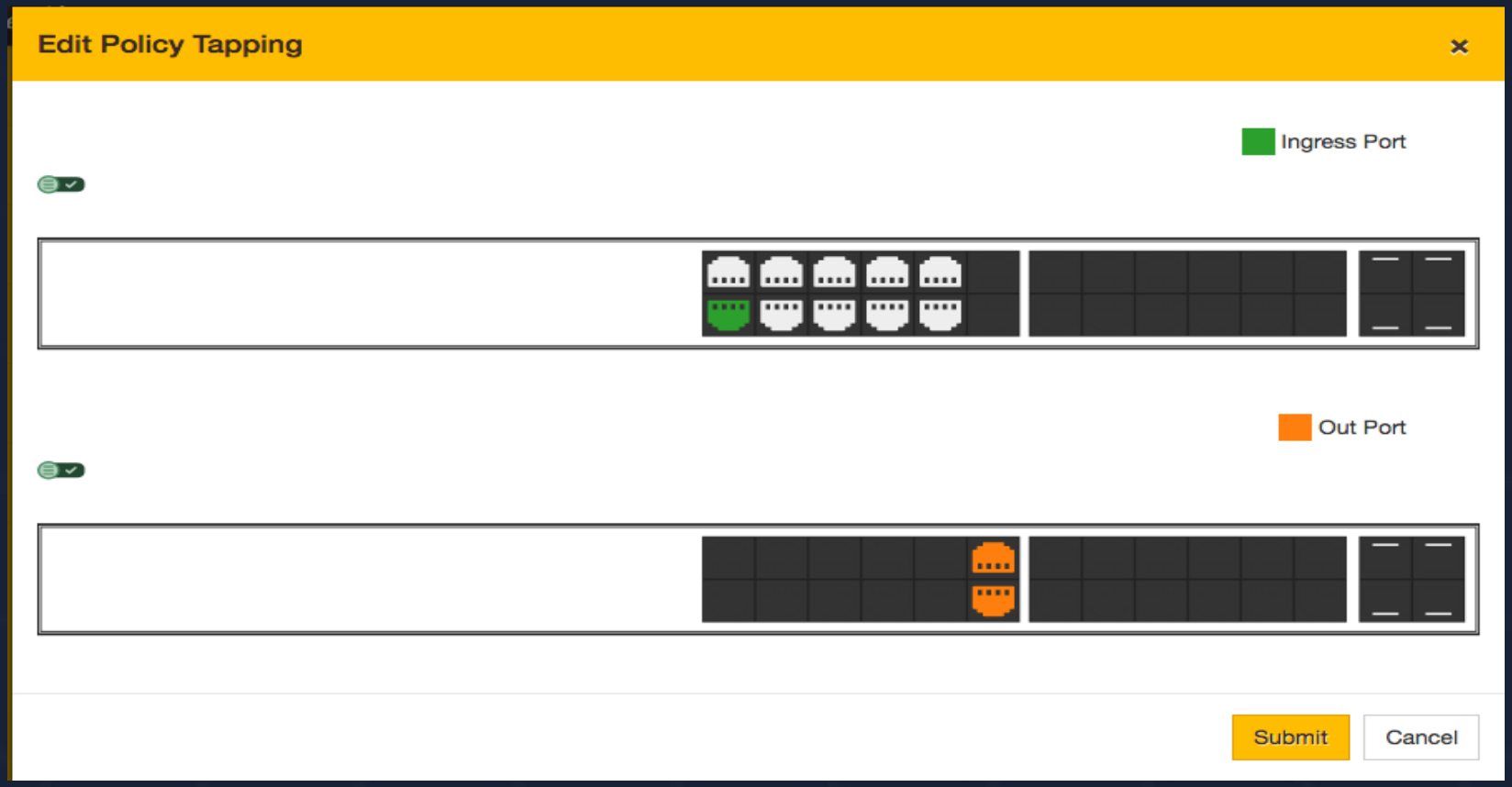
操作介面

TAPPING RULES CONFIG



操作介面

TAPPING RULES CONFIG



ACCESS CONTROL存取控制

WITH SDN-OPENFLOW

適用場景

大量的員工使用網路

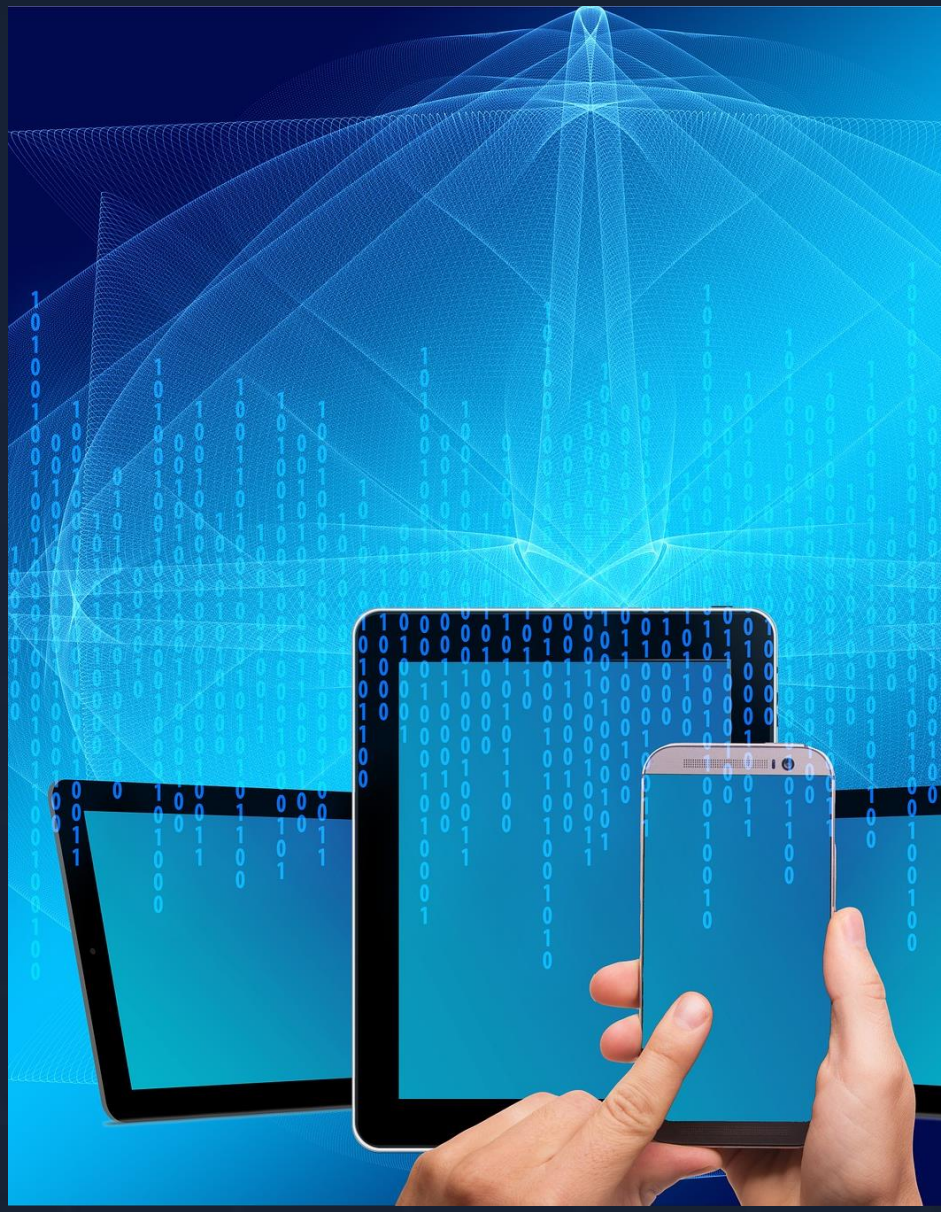
- 限制單日每個IP能夠使用的網路總流量，超過標準時則進行管理
- 限制每個網段的網路使用速率，避免小部分人員佔用大部分資源
- 檢測網路內的電腦是否疑似被殭屍網路所感染，讓該電腦的擁有者能夠在參與攻擊前進行電腦的清掃。

需要能管理能使用網路的帳號

- 固定會有服務人員會一直在處理員工不同裝置要使用學校網路
- 限制每個IP的網路使用速率，避免公用電腦被不當使用、或佔用頻寬
- 可在特定時間將特定網段的流量導入不同的閘道，製造隔離的網路環境，供研發能夠切換成欲使用的開發環境

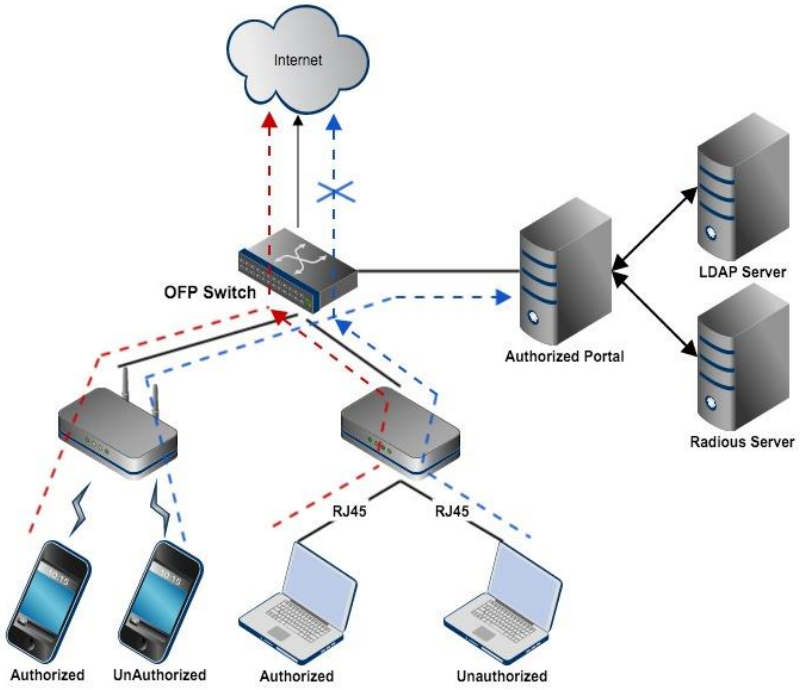
網路頻寬暴衝

IP 相衝問題



系統架構概念

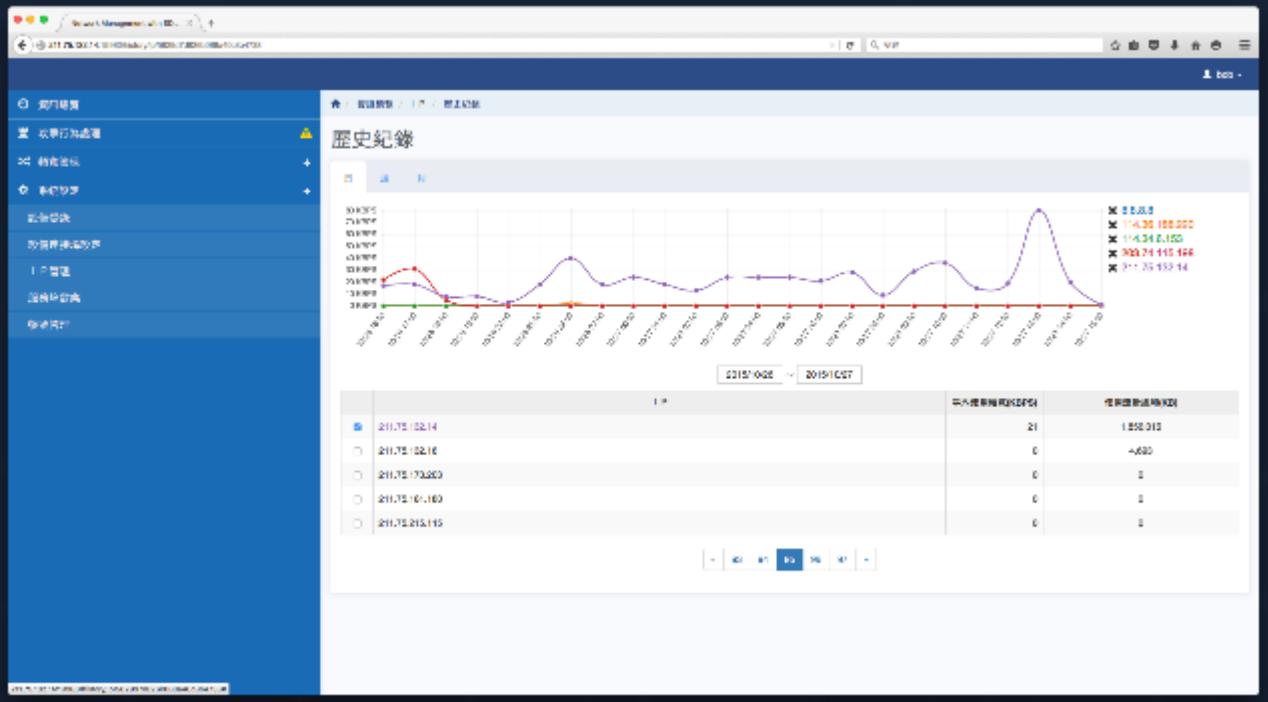
使用者分成授權(AUTHORIZED)與未授(UNAUTHORIZED)，授權者可通過OFP SWITCH連上INTERNET。而尚未通過授權之使用者則會被引導到授權頁面。



操作介面-資訊總覽

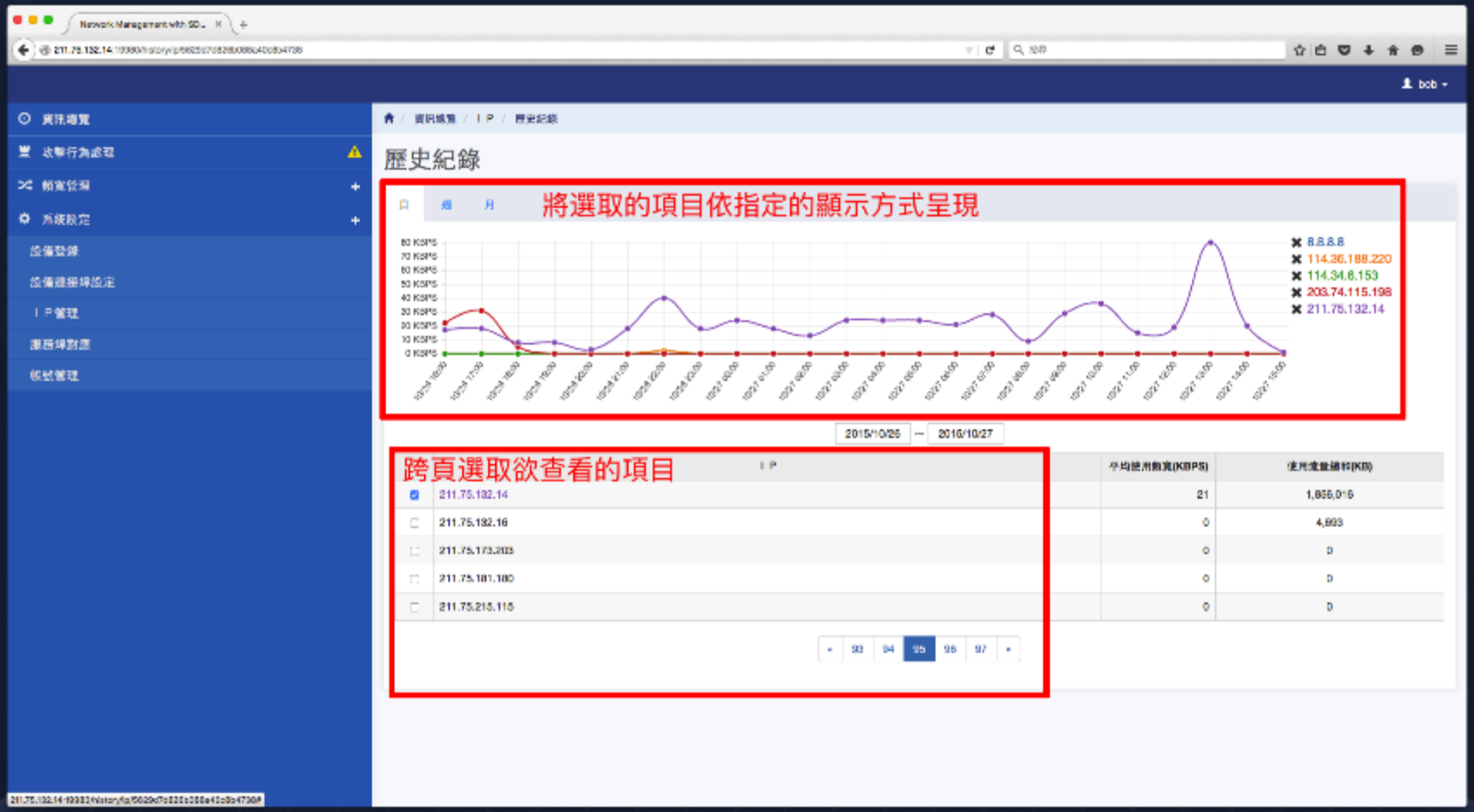
查看各種網路目前使用狀況及其歷史紀錄

- 設備、設備的各個連接埠流通量
- 各種服務的流通量
- 各IP、各設備所涵蓋之IP的網路使用量



操作介面

歷史記錄


歷史紀錄
將選取的項目依指定的顯示方式呈現
跨頁選取欲查看的項目
8.8.8.8
114.36.188.220
114.34.8.153
203.74.115.198
211.75.132.14
2015/10/25
2015/10/27
211.75.132.14
211.75.132.16
211.75.173.203
211.75.181.180
211.75.213.115

SMART LOAD BALANCE智慧路由

WITH SDN-OPENFLOW

適用場景

大量的員工使用網路

- 限制單日每個IP能夠使用的網路總流量，超過標準時則進行管理
- 限制每個網段的網路使用速率，避免小部分人員佔用大部分資源
- 檢測網路內的電腦是否疑似被殭屍網路所感染，讓該電腦的擁有者能夠在參與攻擊前進行電腦的清掃。

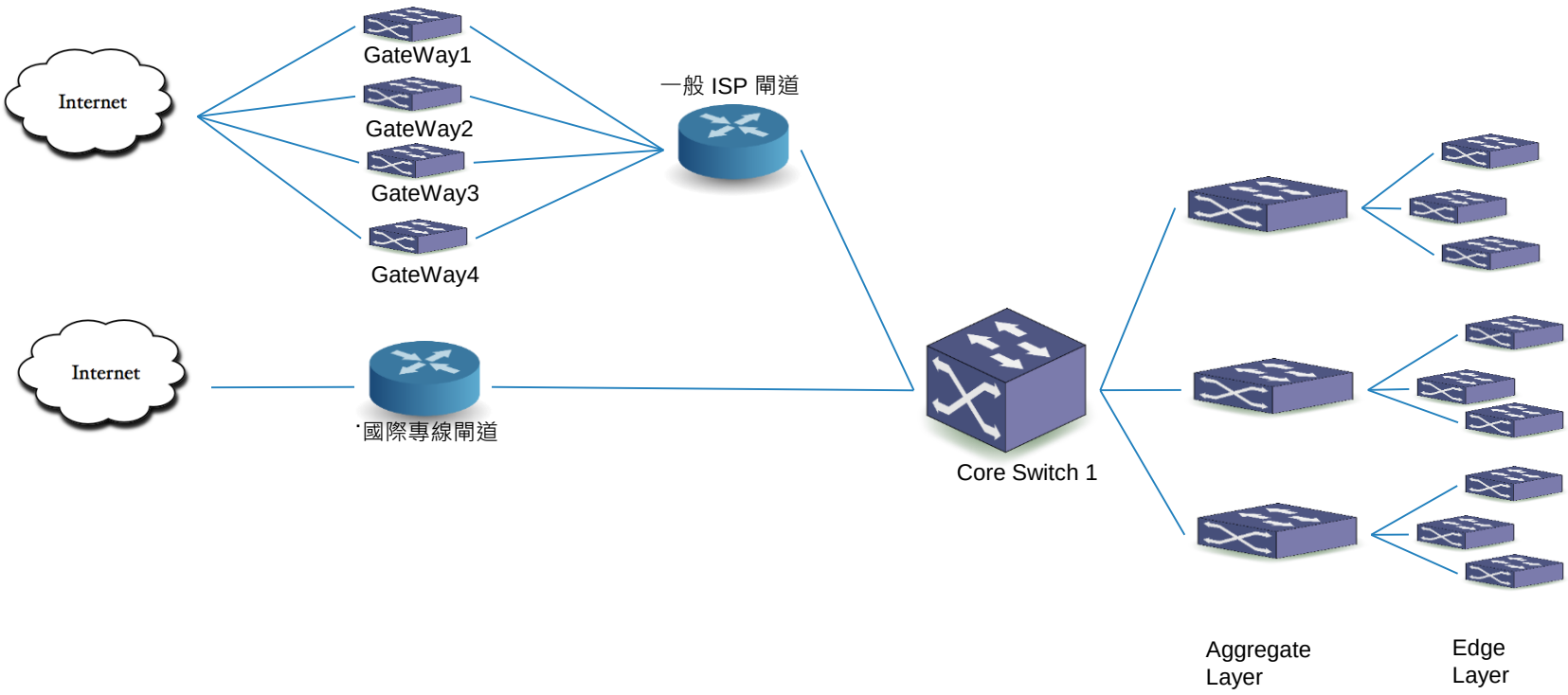
需要能管理能使用網路的帳號

- 固定會有服務人員會一直在處理員工不同裝置要使用學校網路
- 限制每個IP的網路使用速率，避免公用電腦被不當使用、或佔用頻寬
- 可在特定時間將特定網段的流量導入不同的閘道，製造隔離的網路環境，供研發能夠切換成欲使用的開發環境

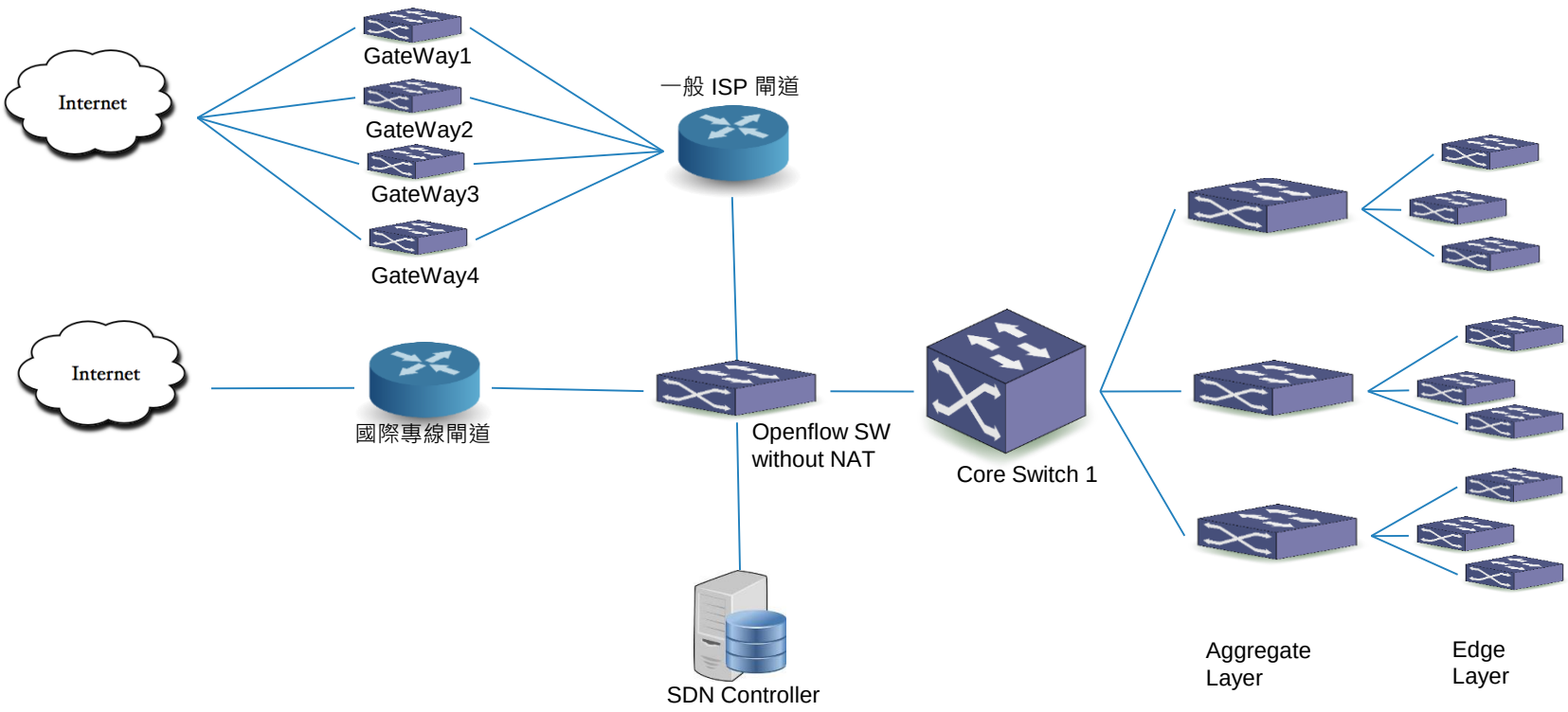
網路頻寬暴衝

IP 相衝問題

現行網路架構說明


Internet
GateWay1
GateWay2
GateWay3
GateWay4
一般 ISP 閘道
Internet
國際專線閘道
Core Switch 1
Aggregate Layer
Edge Layer

建議網路架構說明


Internet
GateWay1
GateWay2
GateWay3
GateWay4
一般 ISP 閘道
Internet
國際專線閘道
Openflow SW
without NAT
Core Switch 1
SDN Controller
Aggregate
Layer
Edge
Layer

操作介面

基本資料設置 – 線路管理

透過此功能進行線路管理, 設定預設通道後沒有符合後續設定任何規則的封包就會通往預設通道。

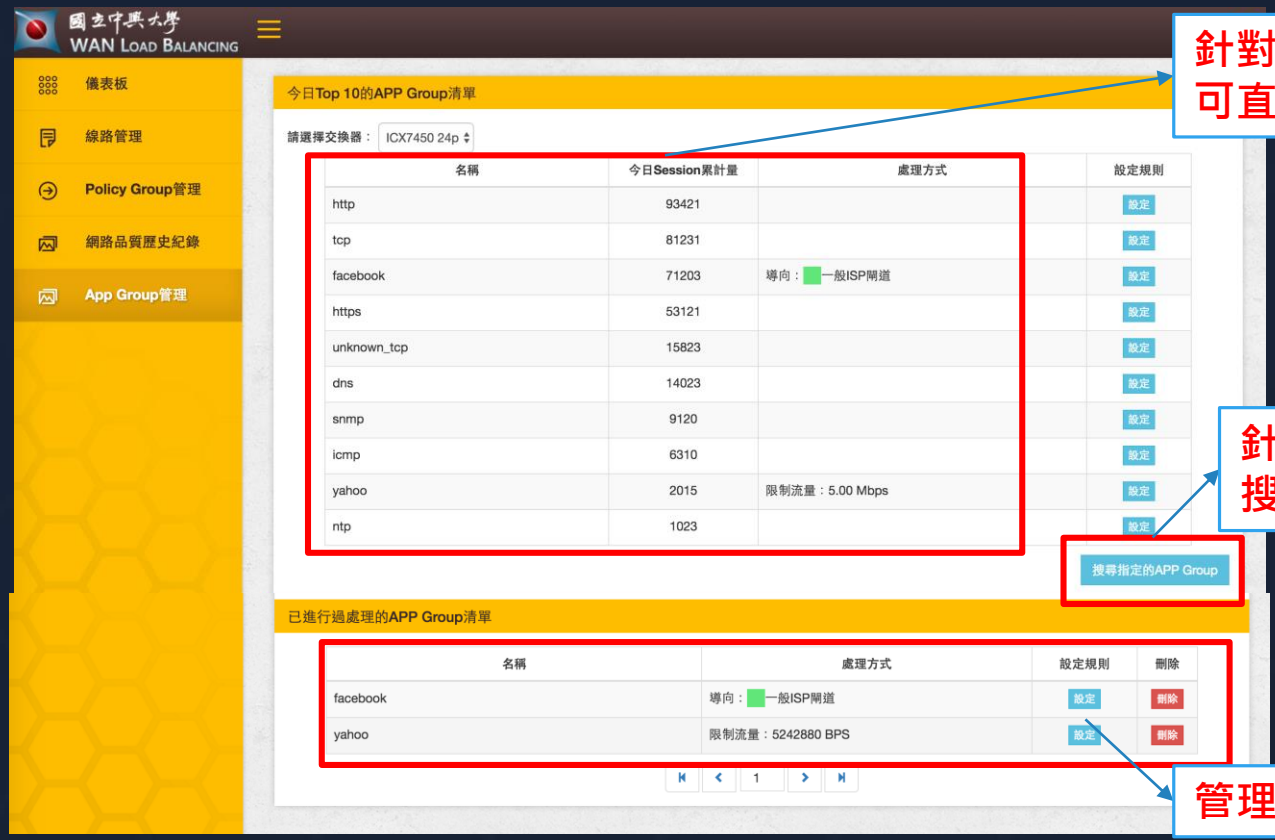
操作介面

導向規則設置 – POLICY GROUP管理

透過此功能進行封包導向的管理, 未符合任何規則的封包會導向「預設」的規則, 若有設定規則則會依照設定的規則導向, 可同時設定內部網段規則與外部網域或網段規則。

操作介面

導向規則設置 – APP GROUP管理



針對今日使用量Top 10的APP
可直接進行導向/限流/停用

針對非Top 10的APP可進行
搜尋後設定導向/限流/停用

管理或改變已設置過的APP策略

操作介面

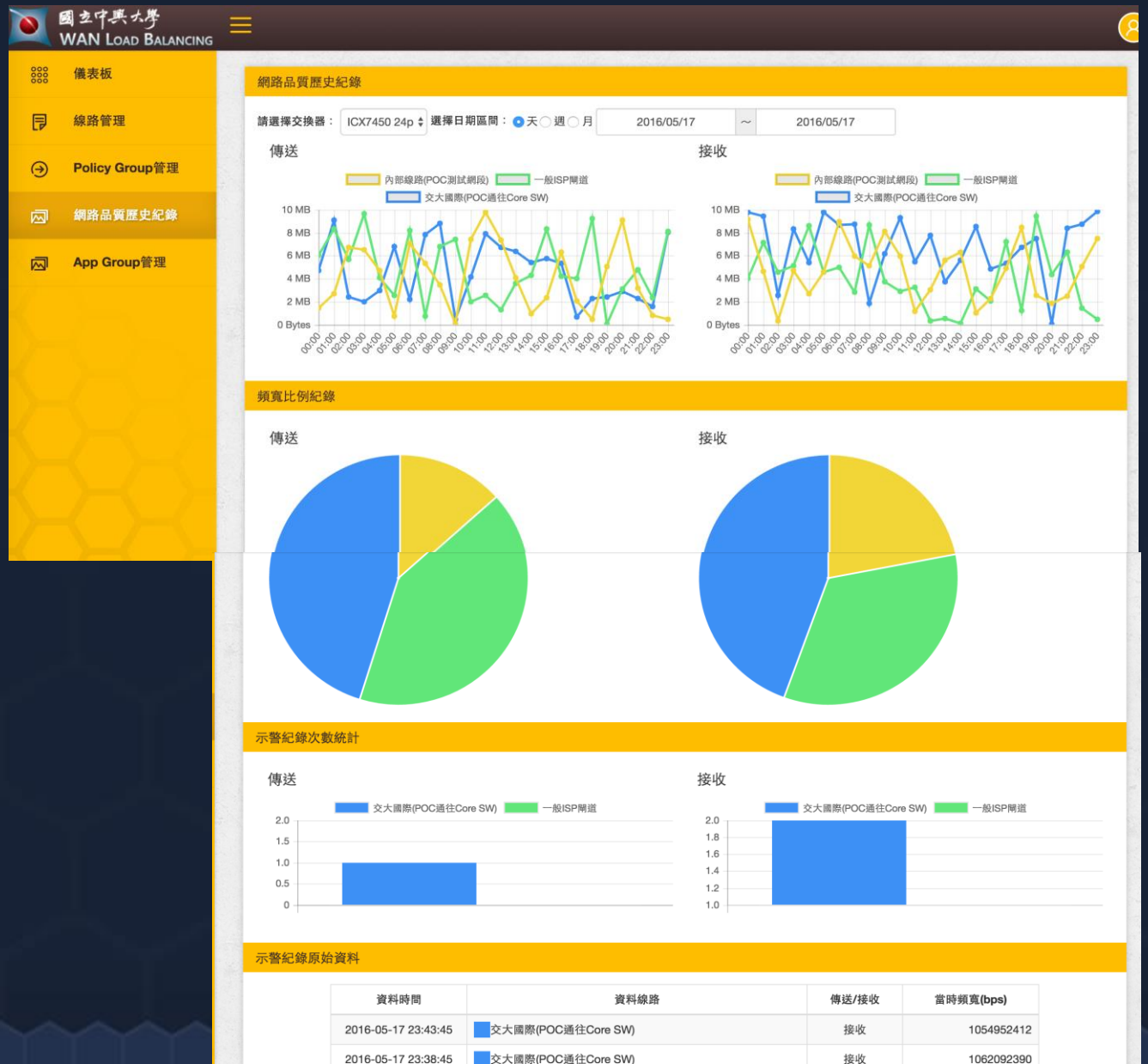
儀表板


線路管理
Policy Group管理
網路品質歷史紀錄
App Group管理
網路品質
請選擇交換器：
ICX7450 24p
即時監控網路孔狀況
傳送
接收
內部線路(POC測試網段)
一般ISP閘道
95 MB
76 MB
57 MB
38 MB
19 MB
0 Bytes
設備狀態異動紀錄
時間
來源
訊息
2016/05/10 19:53:09 連接埠 Switch(ICX7450 24p), Port(10), Status UP -> Down
2016/05/10 19:18:37 連接埠 Switch(ICX7450 24p), Port(5), Status UP -> Down
2016/05/10 19:53:09 連接埠 Switch(ICX7450 24p), Port(10), Status UP -> Down
2016/05/10 19:18:37 連接埠 Switch(ICX7450 24p), Port(5), Status UP -> Down
2016/05/10 19:53:09 連接埠 Switch(ICX7450 24p), Port(10), Status UP -> Down
2016/05/10 19:18:37 連接埠 Switch(ICX7450 24p), Port(5), Status UP -> Down
各種異常狀態的Log

SMART LOAD BALANCE 智慧路由

操作介面

歷史紀錄



SERVICE CHAIN 服務鏈

WITH SDN-OPENFLOW

適用場景

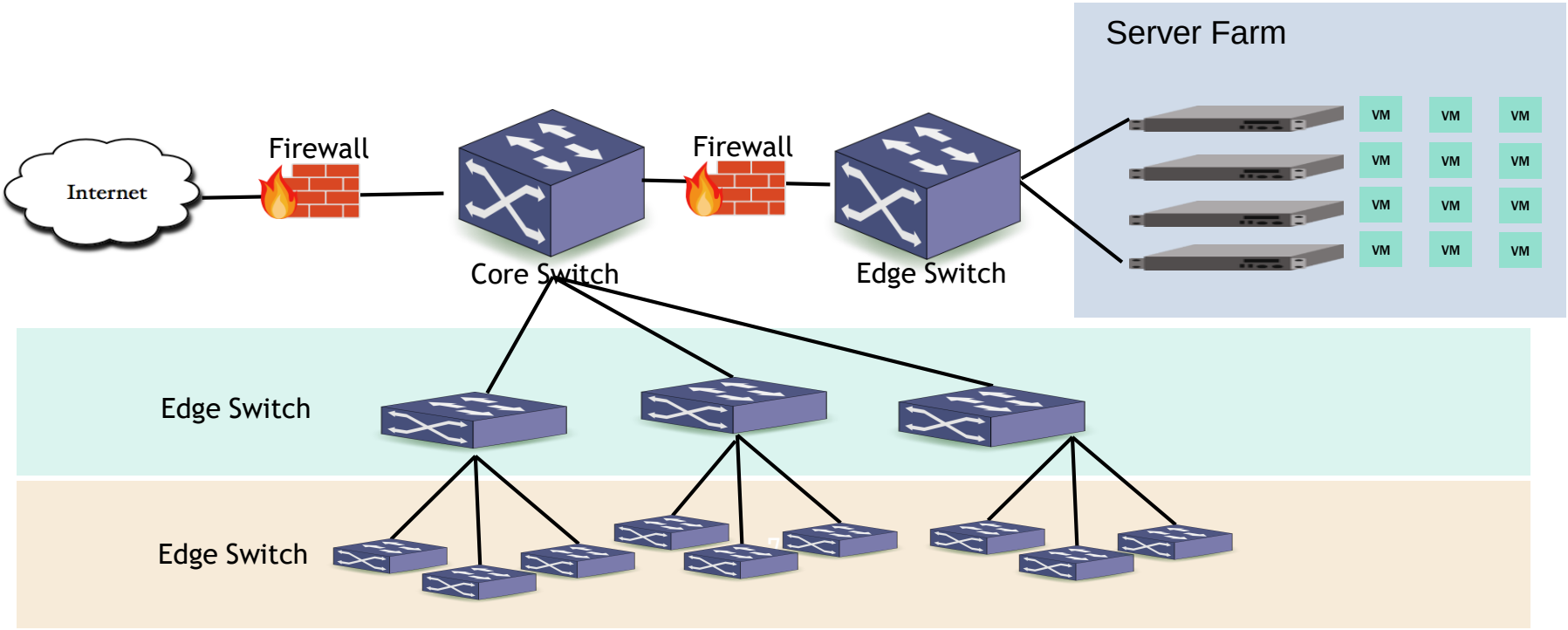
資源最佳運用

- 傳統的網路架構，各機器各司其職，資源使用比重不一。
- SDN架構, 網路設備只專注於傳遞封包, 不做網路管理。

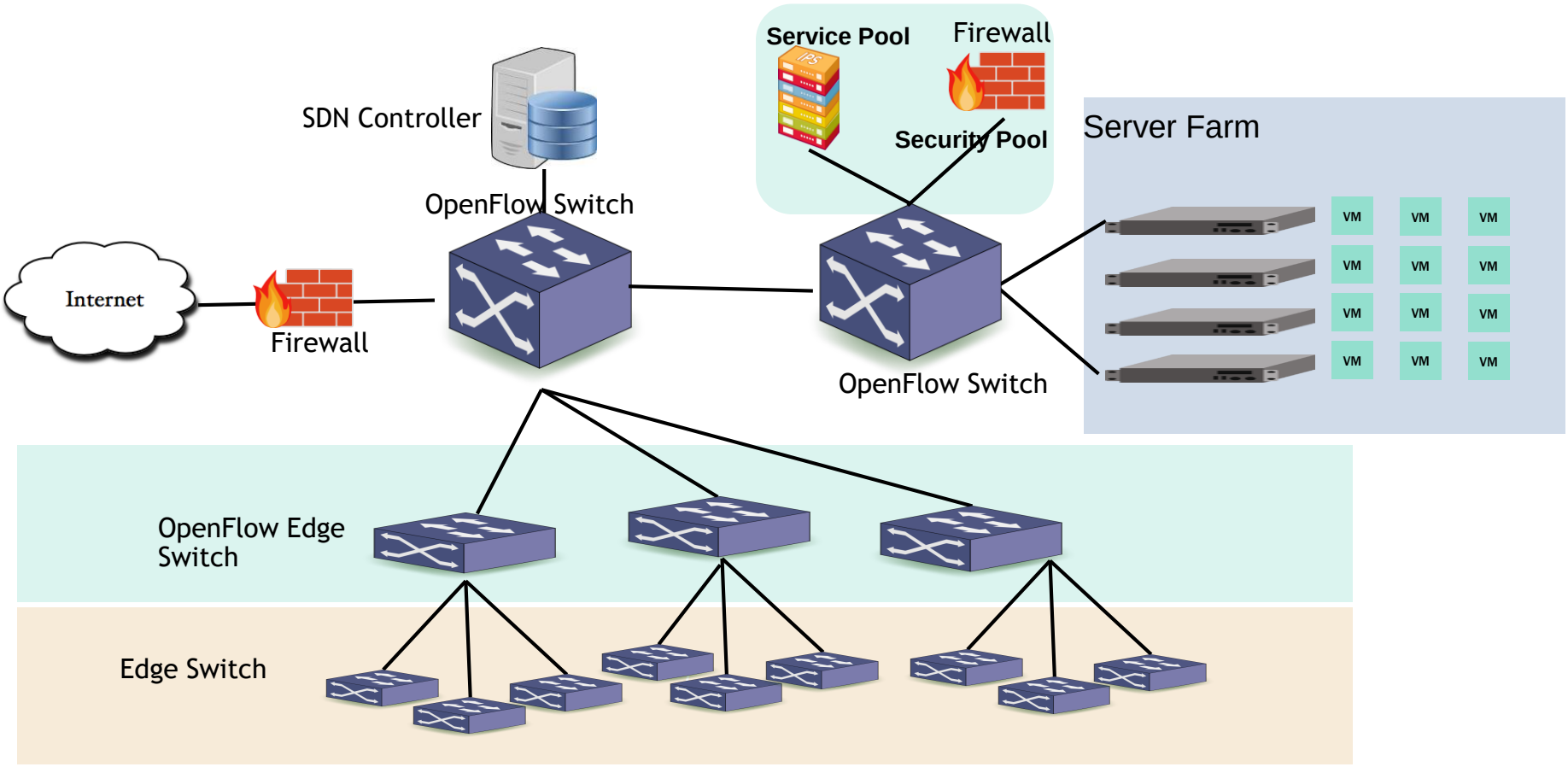
傳輸效率提升

- SDN網路架構就是為了要解決傳統網路的這些問題，SDN的特色是修改了傳統網路架構的控制模式，將網路分為控制層（CONTROL PLANE）與資料層（DATA PLANE），將網路的管理權限交由控制層的控制器（CONTROLLER）軟體負責，採用集中控管的方式。

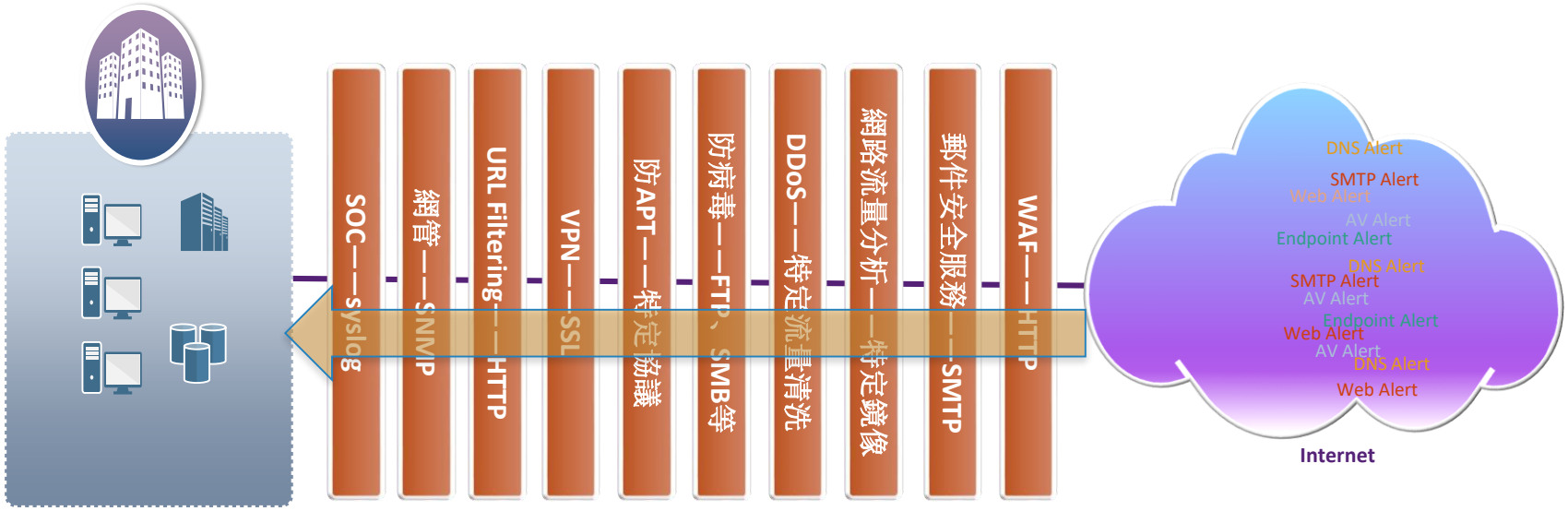
現行網路架構說明


Server Farm
VM
Internet
Firewall
Firewall
Core Switch
Edge Switch
Edge Switch
Edge Switch

建議網路架構說明


Service Pool
Firewall
IPS
Security Pool
SDN Controller
Server Farm
OpenFlow Switch
Internet
Firewall
VM
OpenFlow Switch
OpenFlow Edge Switch
Edge Switch

過往的安全服務鏈架構



企業網路環境

多用戶、多許可權、安全管理

多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

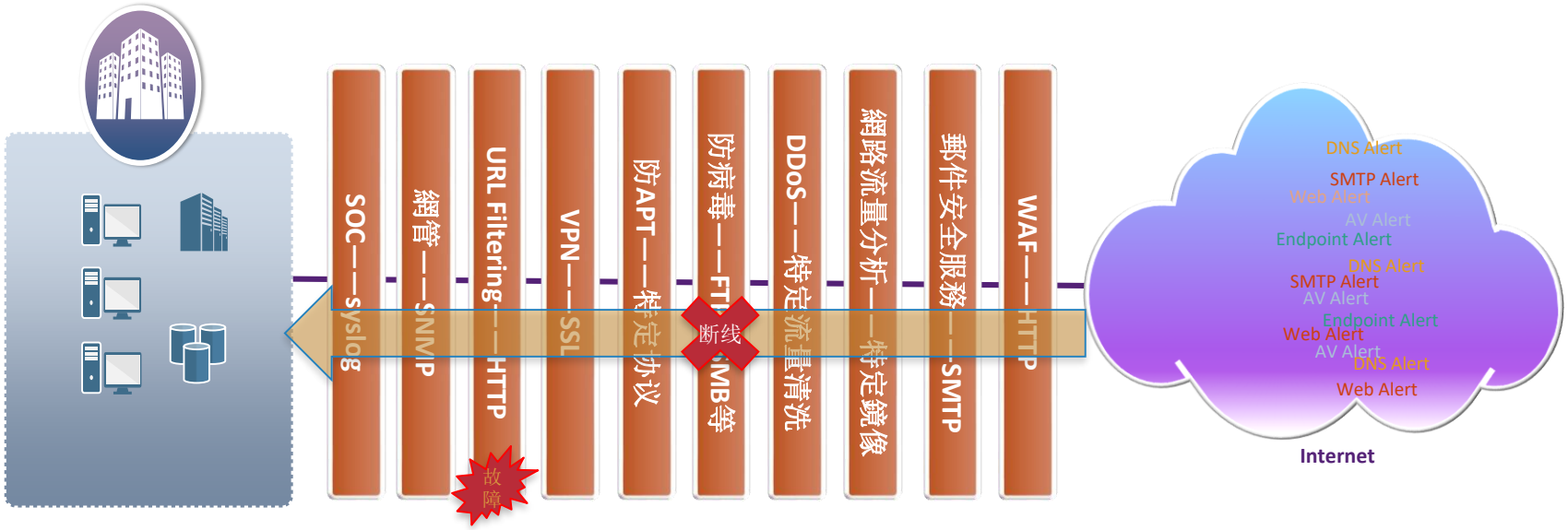
有限的視覺化程度

性能疊加困難，往往面臨性能瓶頸

應急回應變慢

內網或VM之間交互流量難以處理

過往的安全服務鏈架構



企業網路環境

多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

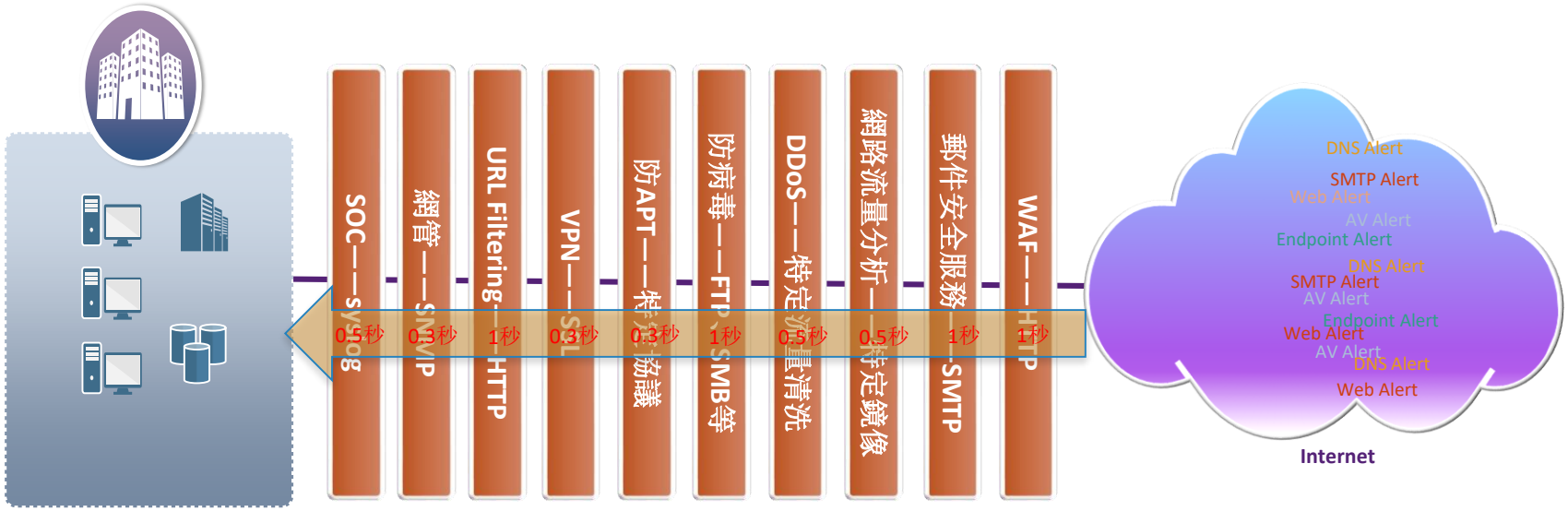
有限的視覺化程度

性能疊加困難，往往面臨性能瓶頸

應急回應變慢

內網或VM之間交互流量難以處理

過往的安全服務鏈架構



企业网络环境

多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

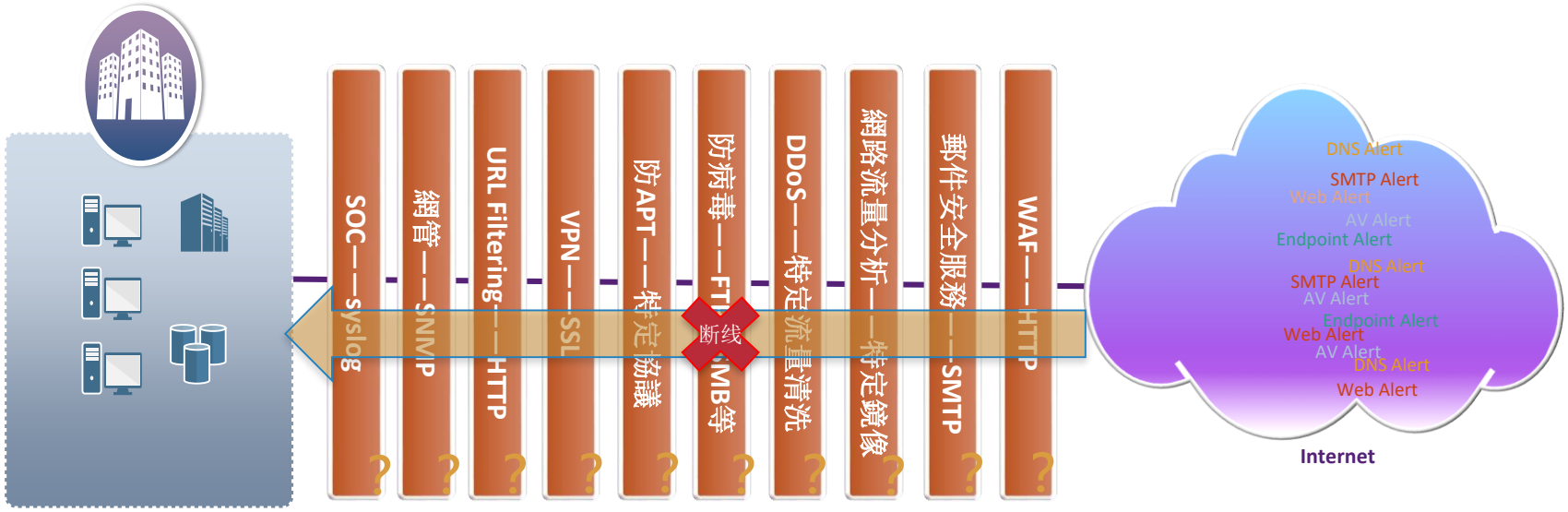
有限的視覺化程度

性能疊加困難，往往面臨性能瓶頸

應急回應變慢

內網或VM之間交互流量難以處理

過往的安全服務鏈架構



企業網路環境

多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

應急回應變慢

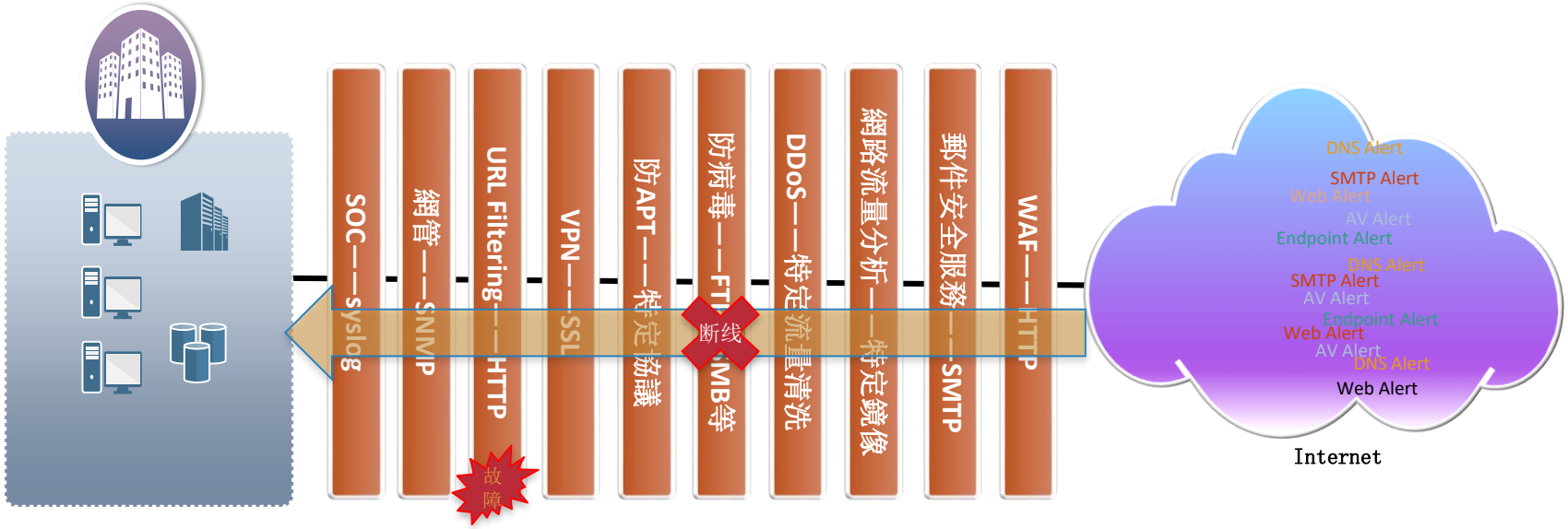
多用戶、多許可權、安全管理

有限的視覺化程度

性能疊加困難，往往面臨性能瓶頸

內網或VM之間交互流量難以處理

過往的安全服務鏈架構



企業網路環境

多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

應急回應變慢

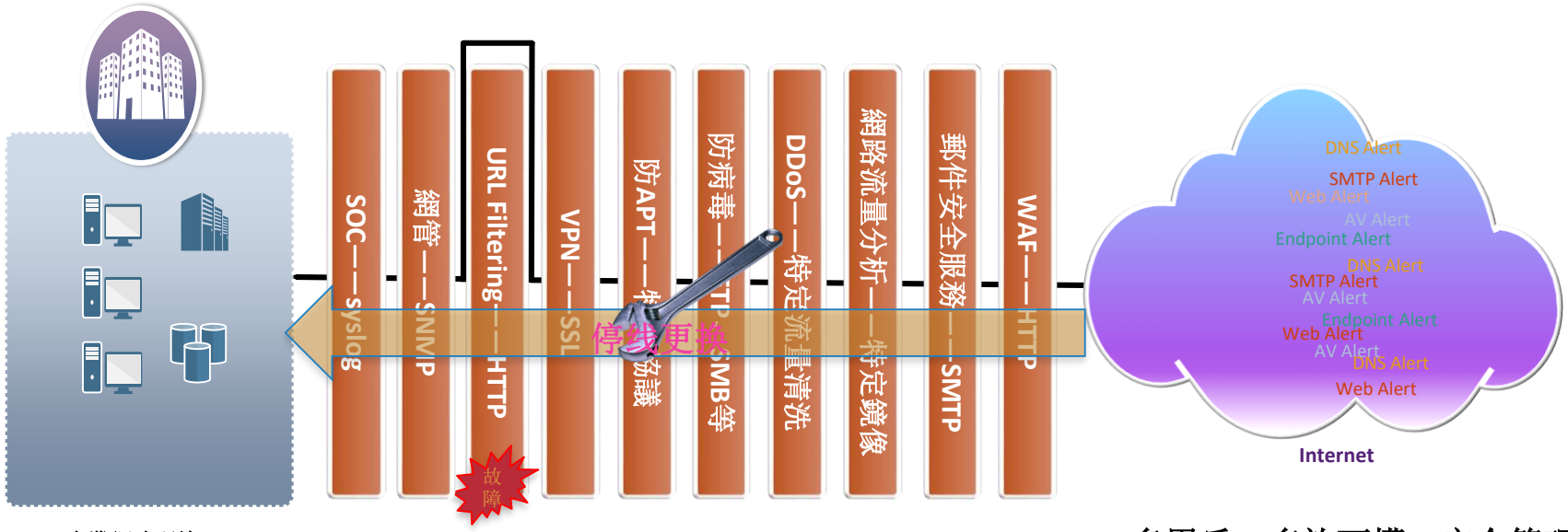
多用戶、多許可權、安全管理

有限的視覺化程度

性能疊加困難，往往面臨性能瓶頸

內網或VM之間交互流量難以處理

過往的安全服務鏈架構



企業網路環境

多用戶、多許可權、安全管理

多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

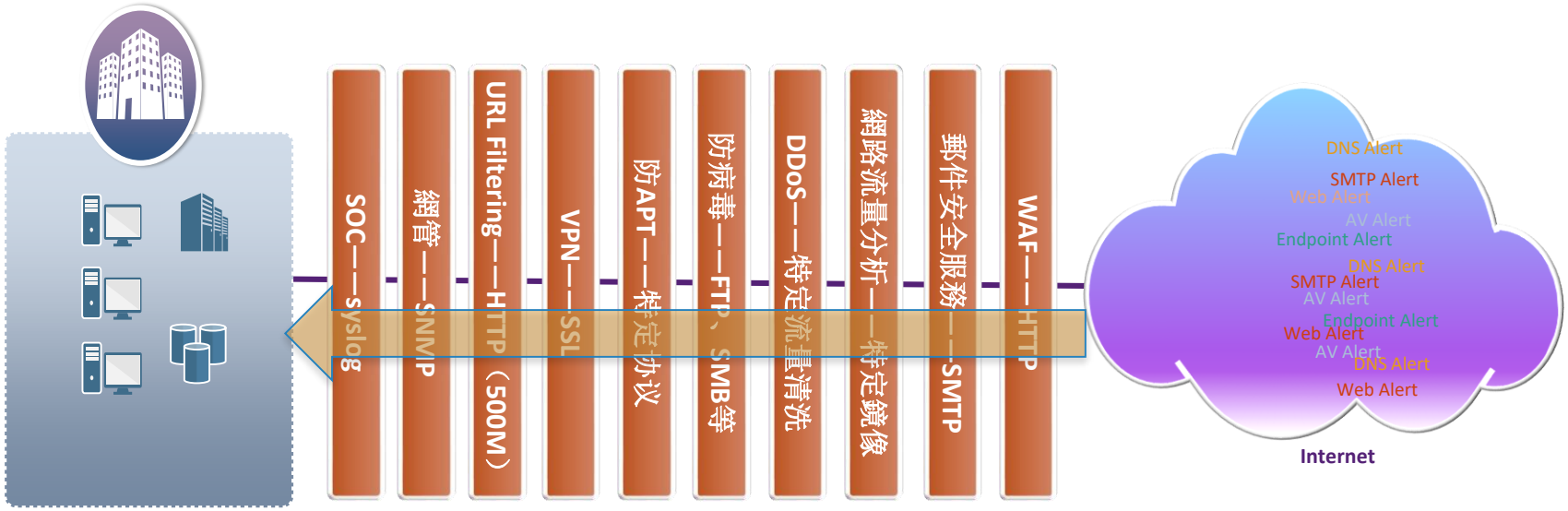
有限的視覺化程度

性能疊加困難，往往面臨性能瓶頸

應急回應變慢

內網或VM之間交互流量難以處理

過往的安全服務鏈架構



企業網路環境

多用戶、多許可權、安全管理

多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

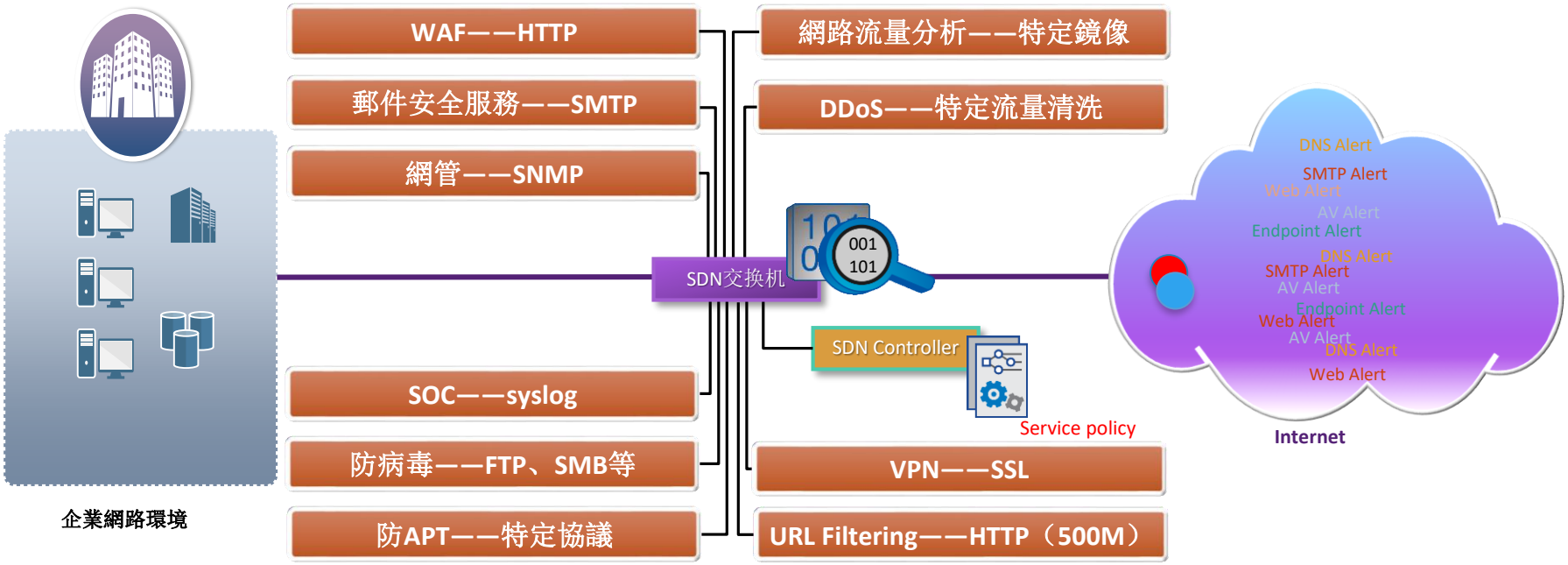
有限的視覺化程度

性能疊加困難，往往面臨性能瓶頸

應急回應變慢

內網或VM之間交互流量難以處理

SDN的安全服務池架構



多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

應急回應變慢

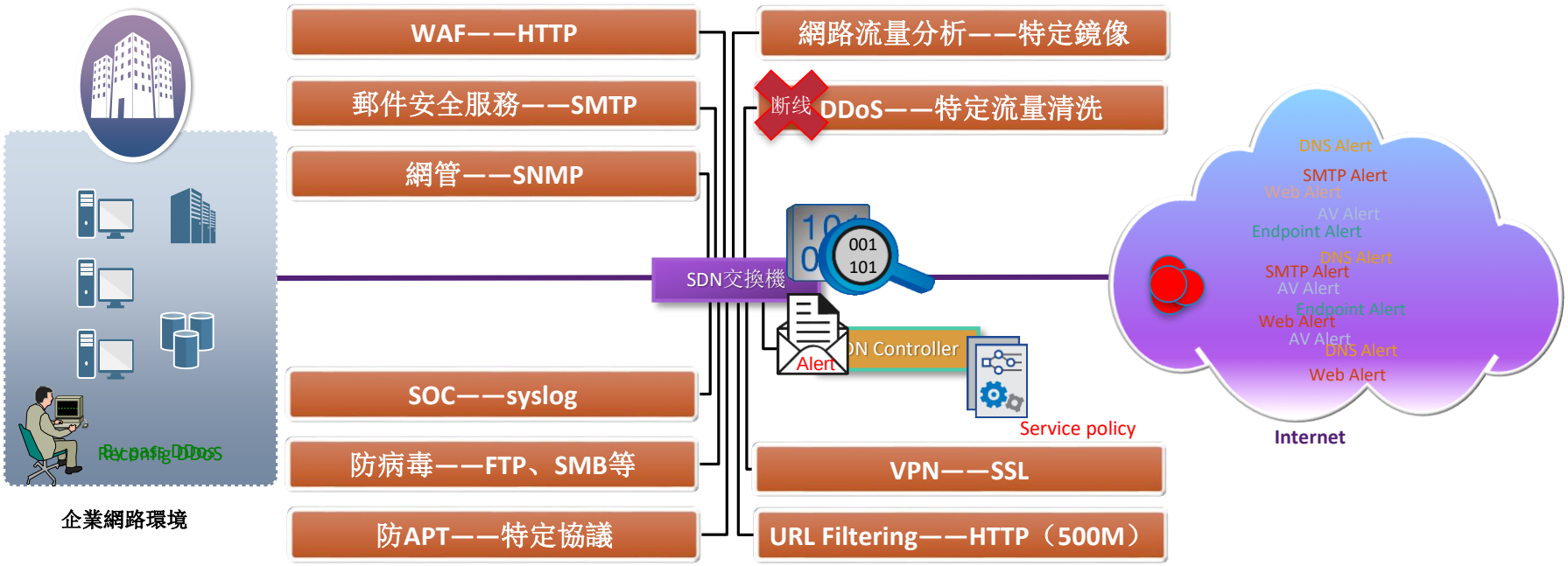
多用戶、多許可權、安全管理

有限的可视化程度

性能疊加困難，往往面臨性能瓶頸

內網或VM之間交互流量難以處理

SDN的安全服務池架構



多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

應急回應變慢

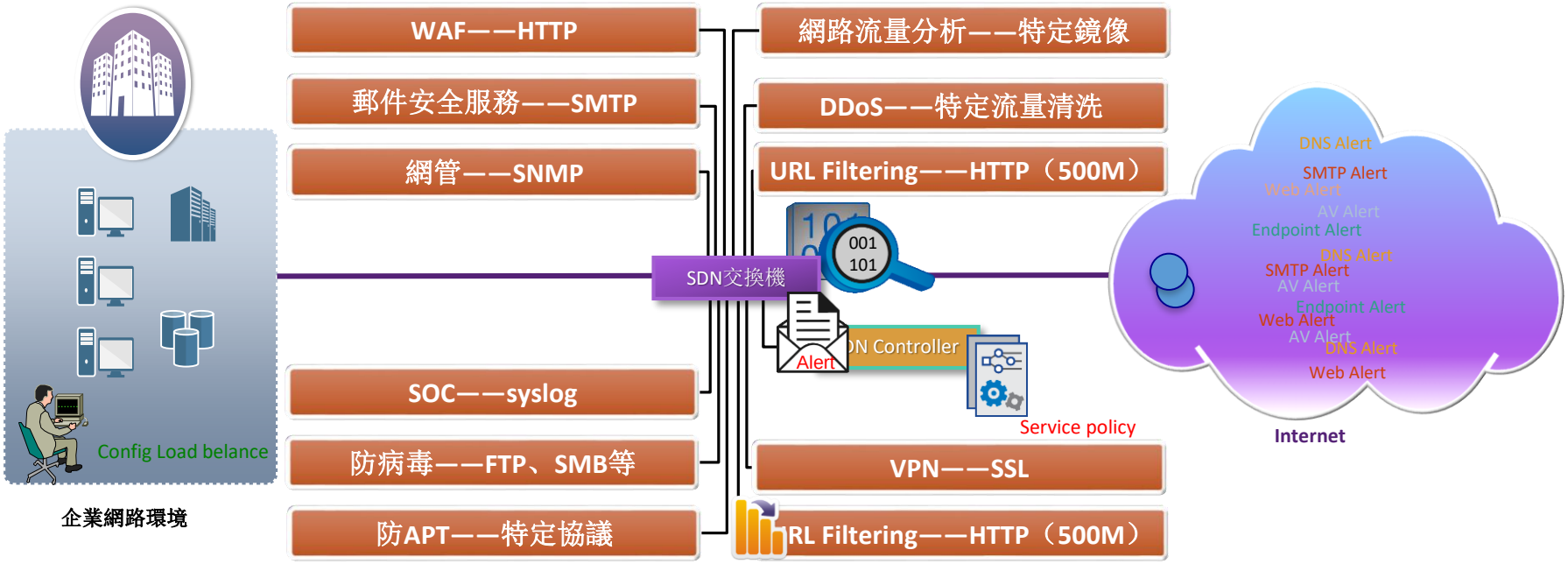
多用戶、多許可權、安全管理

有限的視覺化程度

性能疊加困難，往往面臨性能瓶頸

內網或VM之間交互流量難以處理

SDN的安全服務池架構



多台設備串接，可靠性？

流量經過多次轉發，大延遲？

故障排查複雜，誰來做？

新產品、新功能測試困難

設備故障後，更換困難

應急回應變慢

多用戶、多許可權、安全管理

有限的視覺化程度

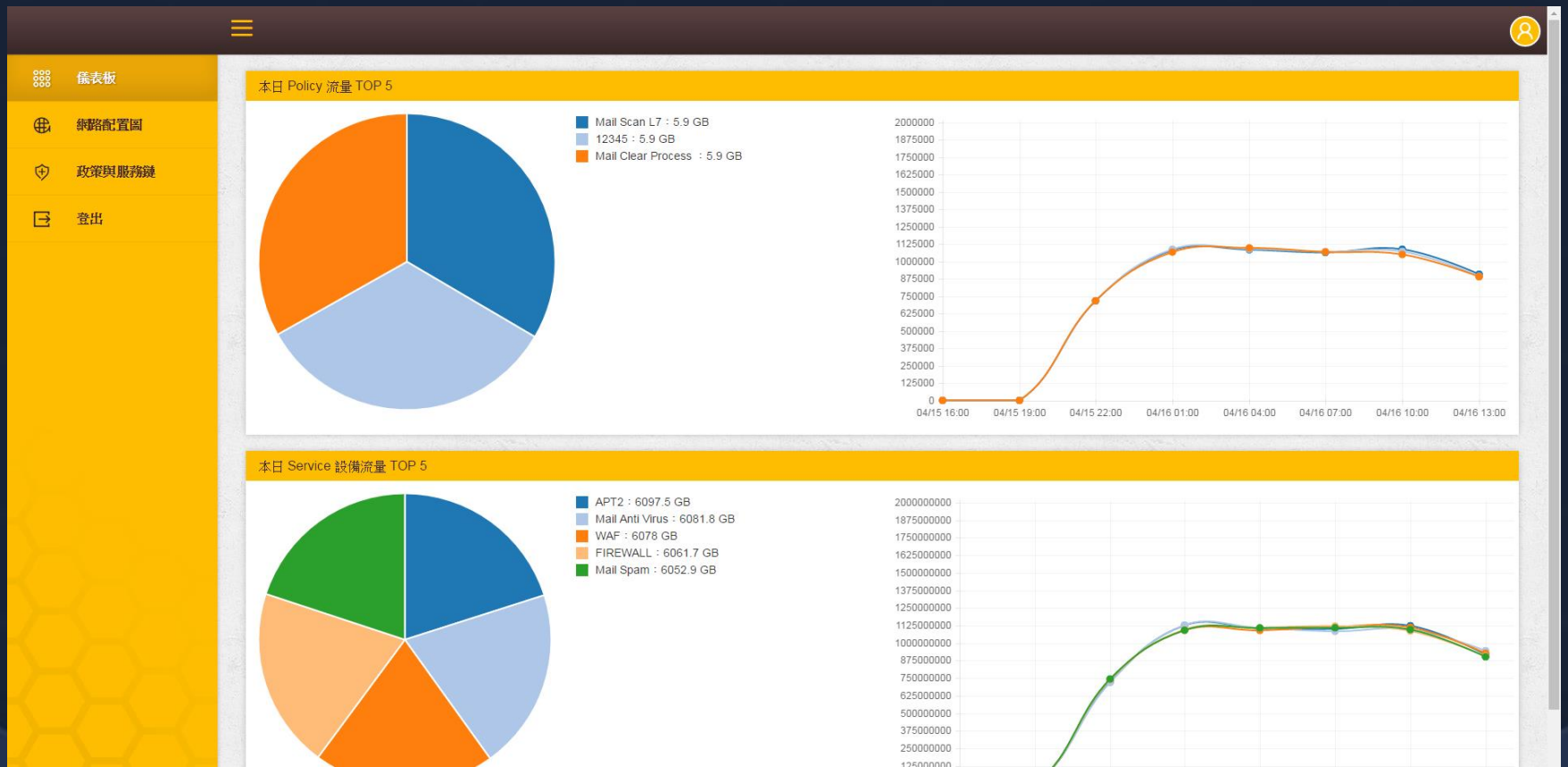
性能疊加困難，往往面臨性能瓶頸

內網或VM之間交互流量難以處理

操作介面

DASHBOARD 統計 ENVIRONMENT SETTING

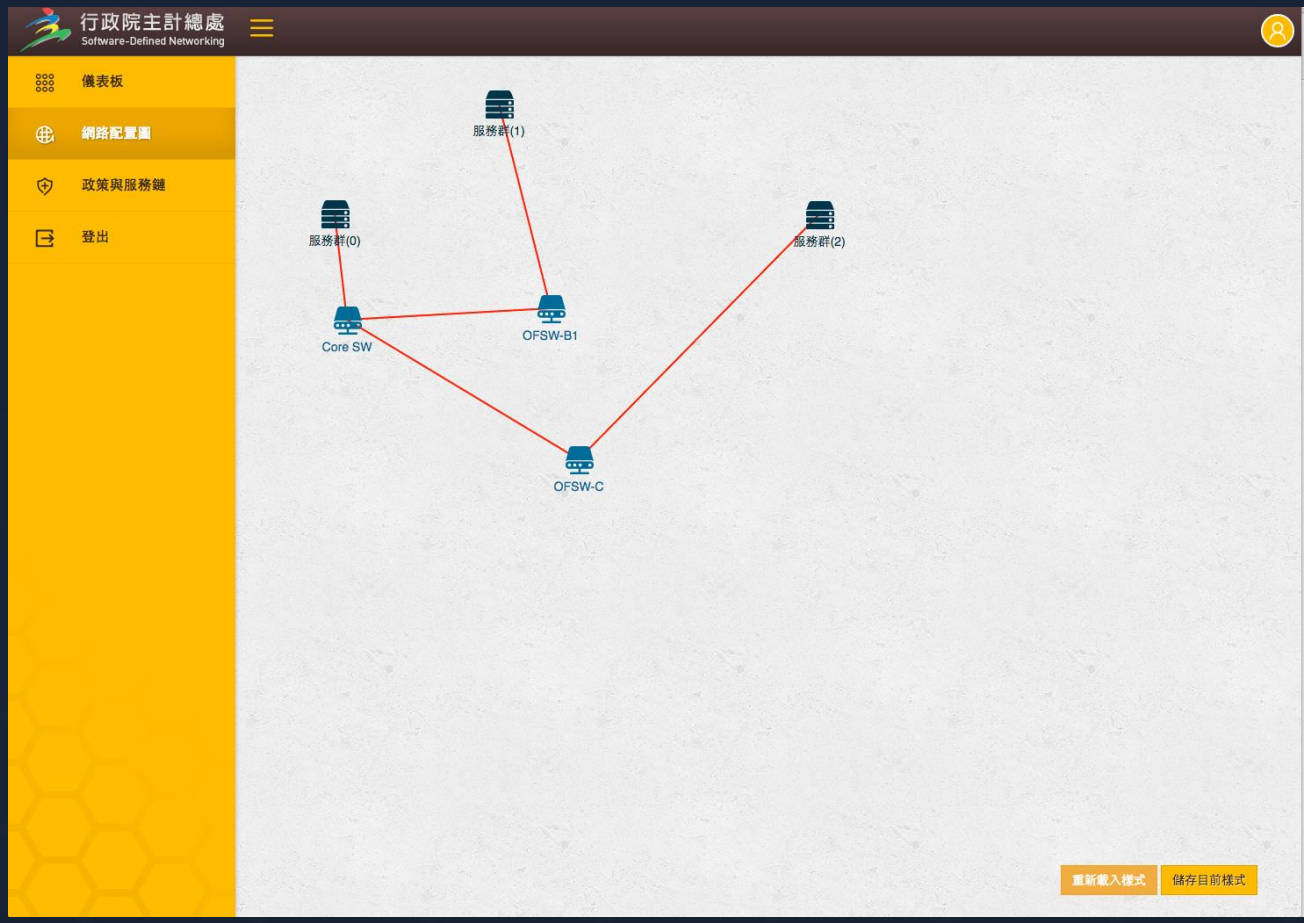
- 顯示 POLICY 流量 TOP 5
- 顯示 SERVICE 流量 TOP 5



操作介面

自動偵測網路拓蹼

- 自動偵測網路拓蹼
- 顯示網路狀態
- 各 SWITCH 連接 SERVICE 的狀態
- 各 SWITCH 上目前執行的 POLICY
- 直覺方式編輯 SERVICE CHAIN 和 POLICY



操作介面

開啟一個 NEW SERVICE CHAINING

OpenFlow Switch - Service Chain

啟用	顯示名稱	服務鏈	輸入埠	輸出埠	來源CIDR	來源埠號	目的CIDR	目的埠號	VLAN號碼
☐	網頁存取檢測-OUT	封包檢測	Port 4	Port 7	不限定	不限定	不限定	80	100
☑	Mail Scan	Mail Scan Servie Chain	Port 3	Port 24	不限定	不限定	不限定	不限定	100
☐	郵件檢測	郵件加密	Port 5	Port 8	不限定	不限定	不限定	25	不使用

Policy名稱 Mail Scan

服務鏈名稱 Mail Scan Servie Chain

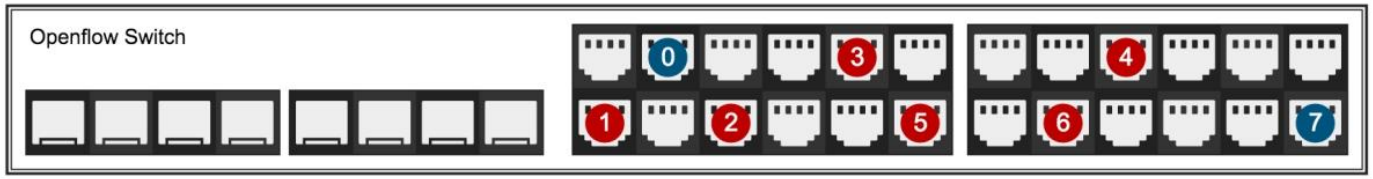
流程

0 > 1 > FIREWALL > 2 > 3 > Mail Spam > 4 > 5 > Mail Anti Virus > 6 > 7

說明：

N 表示 Service 的輸入埠及輸出埠

N 表示 Policy 的輸入埠及輸出埠

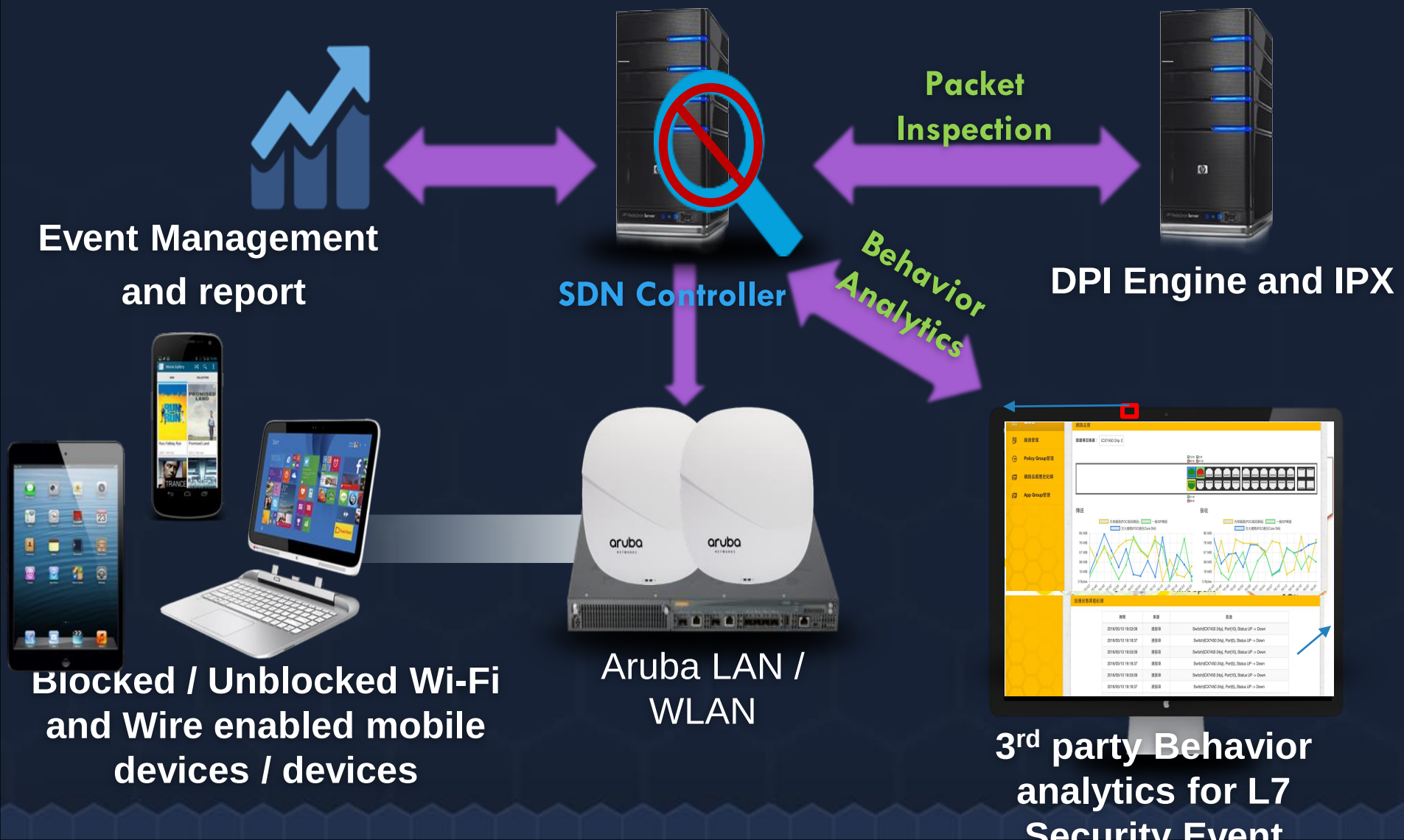


越世實業

Experience Demo

- Aruba Trusted Base 大數據行為分析智能資安分享 (Intelligent SDN Integrated With HPE Aruba)
  - 情境 1 單機試探內部網路機器帳密
  - 情境 2 內部裝置連回駭客基地連線
  - 情境 3 內部連線對內部連線 DDOS (連線癱瘓)

ARUBA TRUSTED BASE 大數據行為分析智能資安分享
(INTELLIGENT SDN INTEGRATED WITH HPE ARUBA)



越世實業

傳統資安事件處理方式

資安事件發生後資安人員才開始分析為何種資安事件，無法防[redacted]發動的攻擊。

越世實業

傳統模式

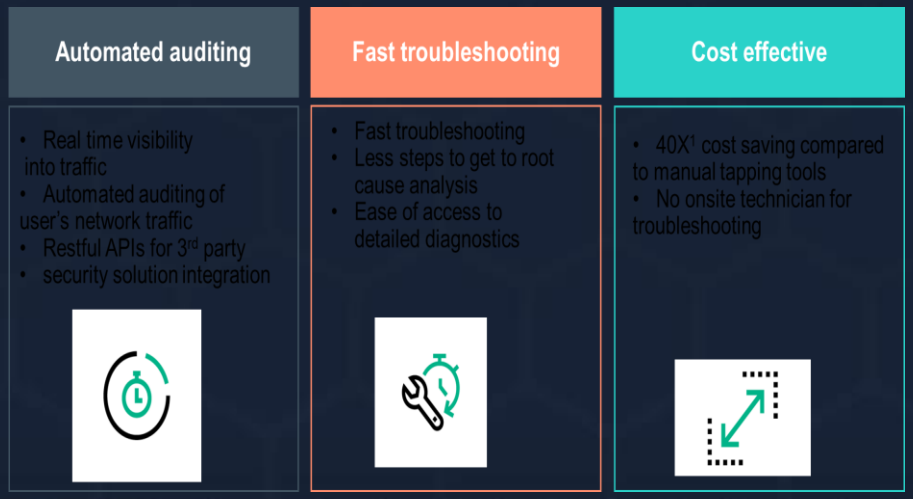
1. 發生資安事件
2. 查閱LOG
3. 找出可能發生的原因
4. 逐一清查

結合 ARUBA OPEN FLOW SWITCH智能資安事件處理方式

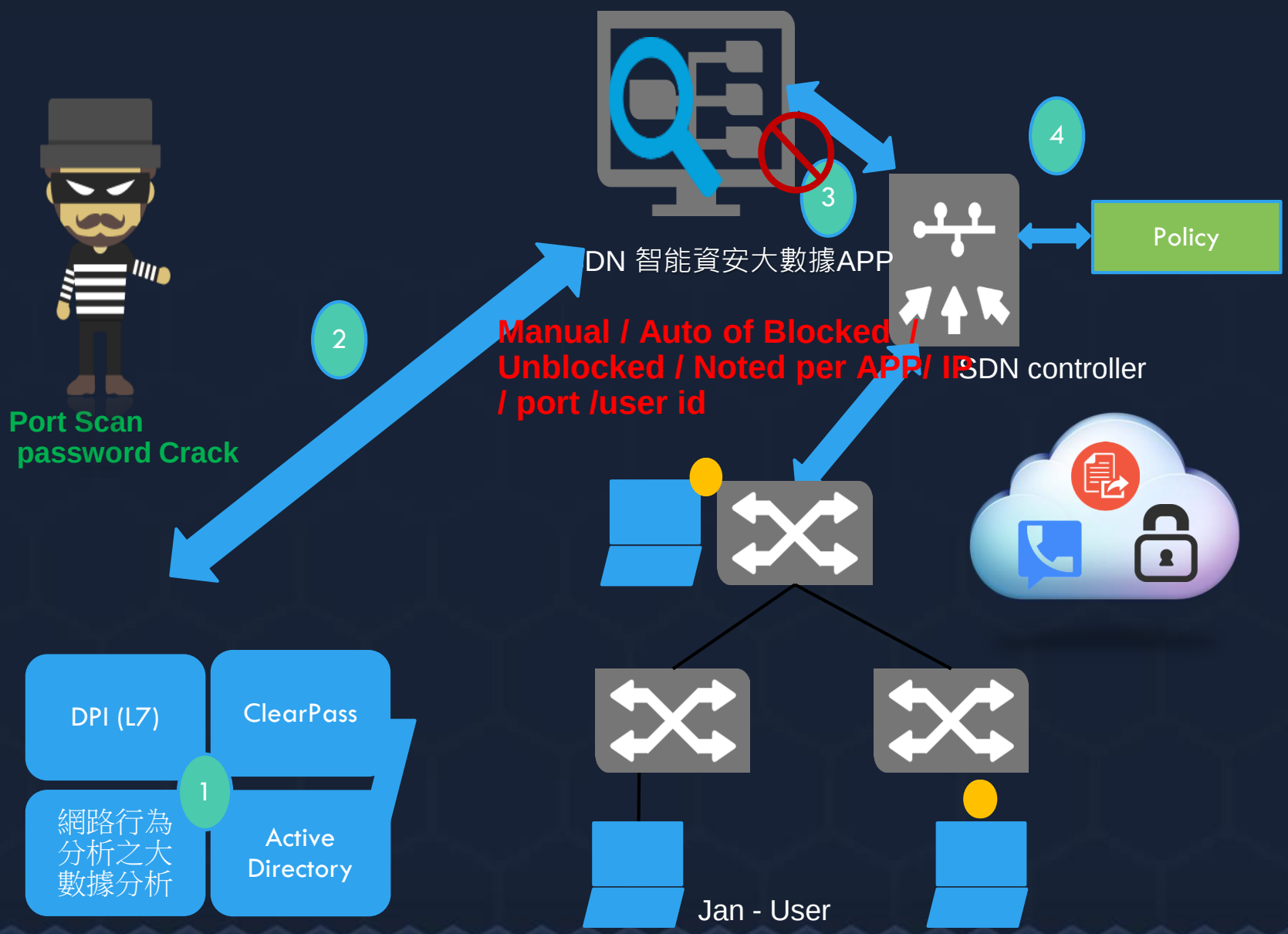
- 事先收集內外封包資訊，針對攻擊內容及行為做一防範

智能資安行為分析模式

1. 資安設備的防護
2. 將所有的網路行為送到資安行為分析系統
3. 主動分析網路行為
4. 將有可能為潛在的攻擊行為過濾出並加以處理



結合Aruba的大數據智能資安防禦Concept



情境 1 單機試探內部網路機器帳密?

– 下班後一般電腦都不關機，該系統可以因被植入木馬程式，自動的會執行 Port Scanning, Password cracker，進而控制該電腦或伺服器之風險，被Hacker為所欲為.....

情境 2 內部裝置連回駭客基地連線?

– 伺服器帳號和密碼被駭客取得後，透由跳板設備將取得的資訊往駭客基地

情境 3內部連線對內部連線 DDOS (連線癱瘓)?

– 駭客會惡意故意癱瘓公司內部某服務，而你的電腦被當成工具，變成協助癱瘓別人網站的幫兇

合作方式

YESEE 提供全方位合作方案

合作方式

越世實業

Q & A