



SDN - SOLUTIONS

主講人 S.C. WANG

WAY SDN

SOFTWARE-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

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

- 40X¹ COST SAVING COMPARED TO MANUAL TAPPING TOOLS
- NO ONSITE TECHNICIAN FOR TROUBLESHOOTING

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 I P
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 D P I 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

即時監控網路孔狀況



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 them to their switch ports

Access control function

- Network resources managed by I2-I4 / protocol / user id (must be integrated with ad server) / application (must be integrated with dpi devices).

Smart load balance function

- Each I2-I4 / protocol / user id (must be integrated with ad server) / application (must be integrated with dpi devices) has its own gateway to internet.

Service Chain New Function

- By different packet, using different 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。

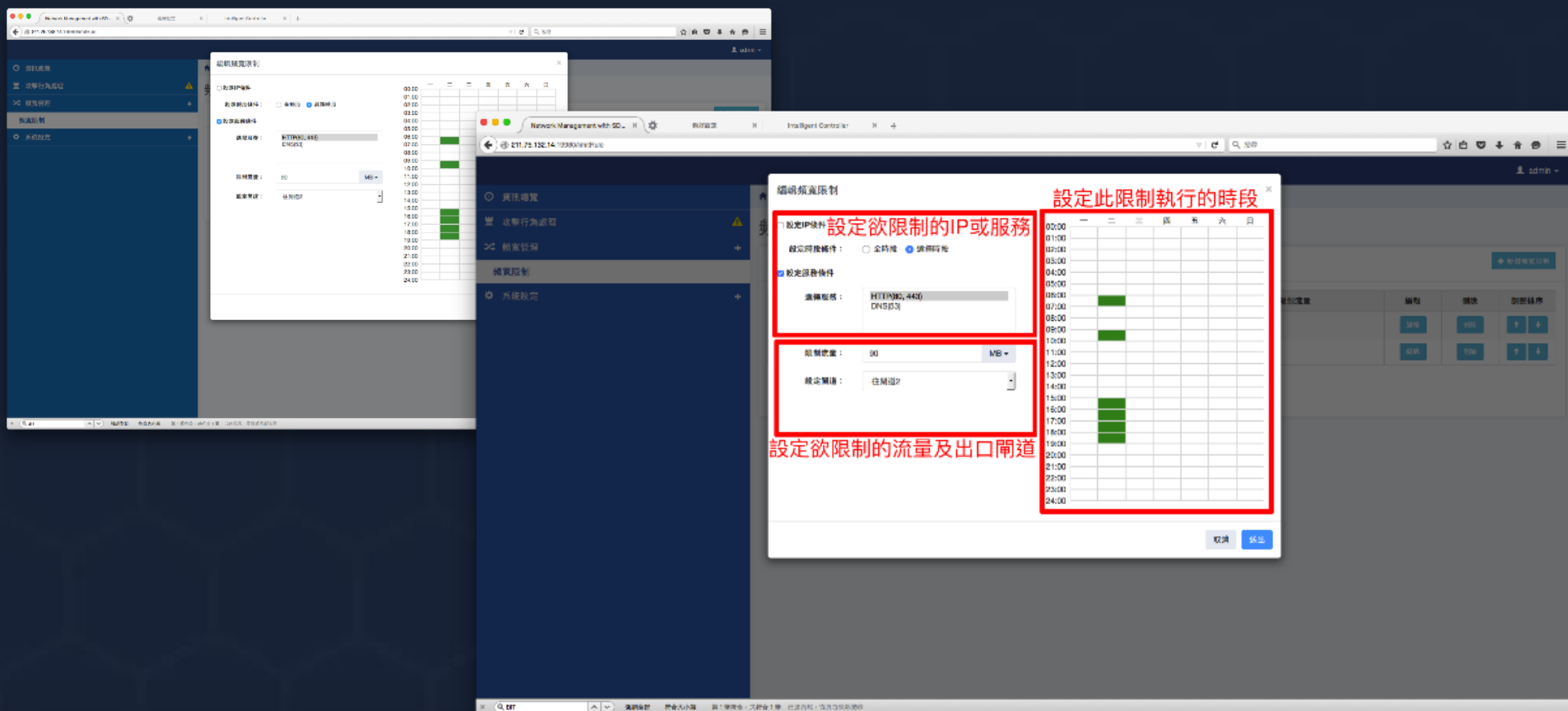
服務品質管理

- 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



The screenshot displays the Network Management v07.50.00 interface. The main window is titled "網路流量限制" (Network Traffic Limitation). It features a sidebar with navigation options: 網路流量限制, 網路服務, 網路設備, 網路監控, 網路分析, 網路安全, 網路管理, 網路維護, 網路故障, 網路優化, 網路性能, 網路質量, 網路可靠性, 網路可用性, 網路穩定性, 網路兼容性, 網路互操作性, 網路集成性, 網路擴展性, 網路靈活性, 網路敏捷性, 網路韌性, 網路容錯性, 網路冗余性, 網路备份性, 網路恢复性, 網路迁移性, 網路克隆性, 網路复制性, 網路分发性, 網路聚合性, 網路路由性, 網路交换性, 網路连接性, 網路连通性, 網路可达性, 網路可访问性, 網路可管理性, 網路可配置性, 網路可升级性, 網路可扩展性, 網路可集成性, 網路可互操作性, 網路可兼容性, 網路可稳定性, 網路可可靠性, 網路可可用性, 網路可质量性, 網路可性能性, 網路可分析性, 網路可监控性, 網路可设备性, 網路可服务性, 網路可限制性.

The "網路流量限制" window is open, showing a configuration form for "設定欲限制的IP或服務" (Set the IP or service to be limited). The form includes the following fields:

- 設定條件:** ☐ 即時性 ☒ 策略性
- 策略名稱:** 網路限制 (444) (DNS [5])
- 限制流量:** 90 MB
- 設定策略:** 在策略P

Below the form is a table for "設定此限制執行的時段" (Set the time period for this limitation to be executed). The table has columns for days of the week (一, 二, 三, 四, 五, 六, 日) and rows for time slots from 00:00 to 24:00. The table is currently empty.

At the bottom of the window, there are buttons for "取消" (Cancel) and "確定" (Confirm).

TAPPING 流量複製

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，符合後再進行複製。

不同的單位可以自行複製符合其 IP 的網路流量



操作介面

SWITCH CONFIG

 Network Security Controller




儀錶板

政策管理

Tapping

配置

Openflow交換器

OF交換器連接埠

權限

寄件伺服器

群組使用權限

本地帳號

OF交換器配置

編輯

刪除

自動偵測

	編號	名稱	模組名稱	資料路徑ID	IP地址	允許
☐	1		ICX 7450 24p	0000000000000001		
☐	2	elheraldo	ICX 7450 24p	0000000000000002	192.168.130.55	
☐	3	ICX 6610	ICX 7450 24p	748EF89014BC0000	192.168.200.30	✓
☐	4	東華MLXE	MLXe	609C9F83FA000000	192.168.200.200	
☐	5	逢甲2128	Noviflow-2128-28	0000000000000001		✓
☐	6	逢甲 1 1 3 2	Noviflow-1132-32	0000000000000001		✓
☐	7	逢甲 2 1 1 6	Noviflow-2116-16	0000000000000001		✓

⏮

⏪

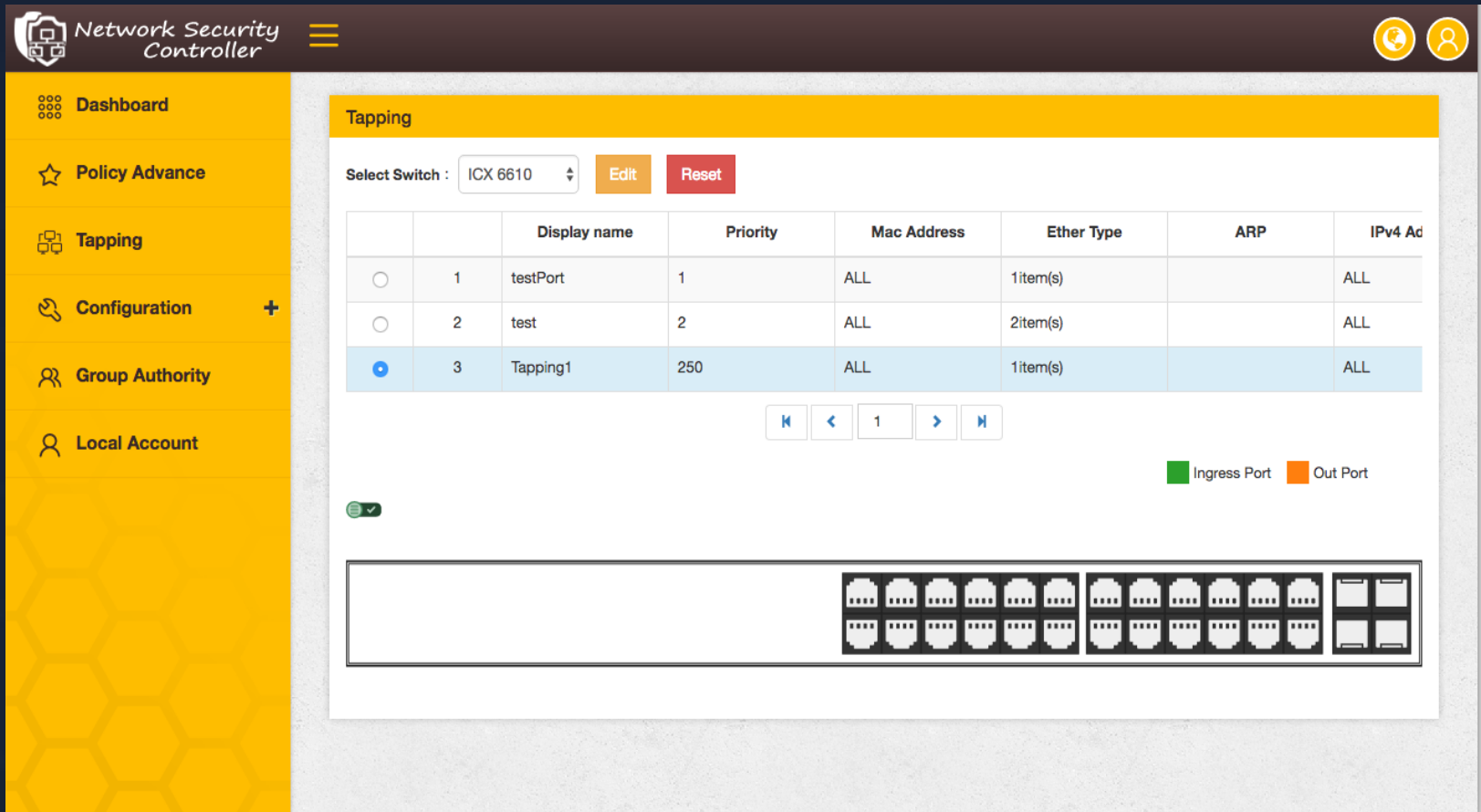
1

⏩

⏭

操作介面

TAPPING RULES CONFIG



The screenshot displays the 'Tapping Rules Config' interface within the Network Security Controller. The left sidebar contains navigation options: Dashboard, Policy Advance, Tapping, Configuration, Group Authority, and Local Account. The main content area is titled 'Tapping' and features a 'Select Switch' dropdown set to 'ICX 6610', with 'Edit' and 'Reset' buttons. Below this is a table of tapping rules. The table has columns for 'Display name', 'Priority', 'Mac Address', 'Ether Type', 'ARP', and 'IPv4 Ad'. Three rules are listed: 'testPort' (Priority 1), 'test' (Priority 2), and 'Tapping1' (Priority 250, selected). Below the table is a pagination control showing '1' of 1 items. A legend indicates 'Ingress Port' (green) and 'Out Port' (orange). At the bottom, there is a diagram of a switch with 24 ports, where the first 20 ports are marked as 'Ingress Port' and the last 4 ports are marked as 'Out Port'.

Network Security Controller

Tapping

Select Switch : ICX 6610 Edit Reset

		Display name	Priority	Mac Address	Ether Type	ARP	IPv4 Ad
☐	1	testPort	1	ALL	1item(s)		ALL
☐	2	test	2	ALL	2item(s)		ALL
☒	3	Tapping1	250	ALL	1item(s)		ALL

1

Ingress Port Out Port

Diagram showing 24 ports (20 Ingress, 4 Out) on a switch.

TAPPING RULES CONFIG

[illegible]

ACCESS CONTROL存取控制

WITH SDN-OPENFLOW

適用場景

大量的員工使用網路

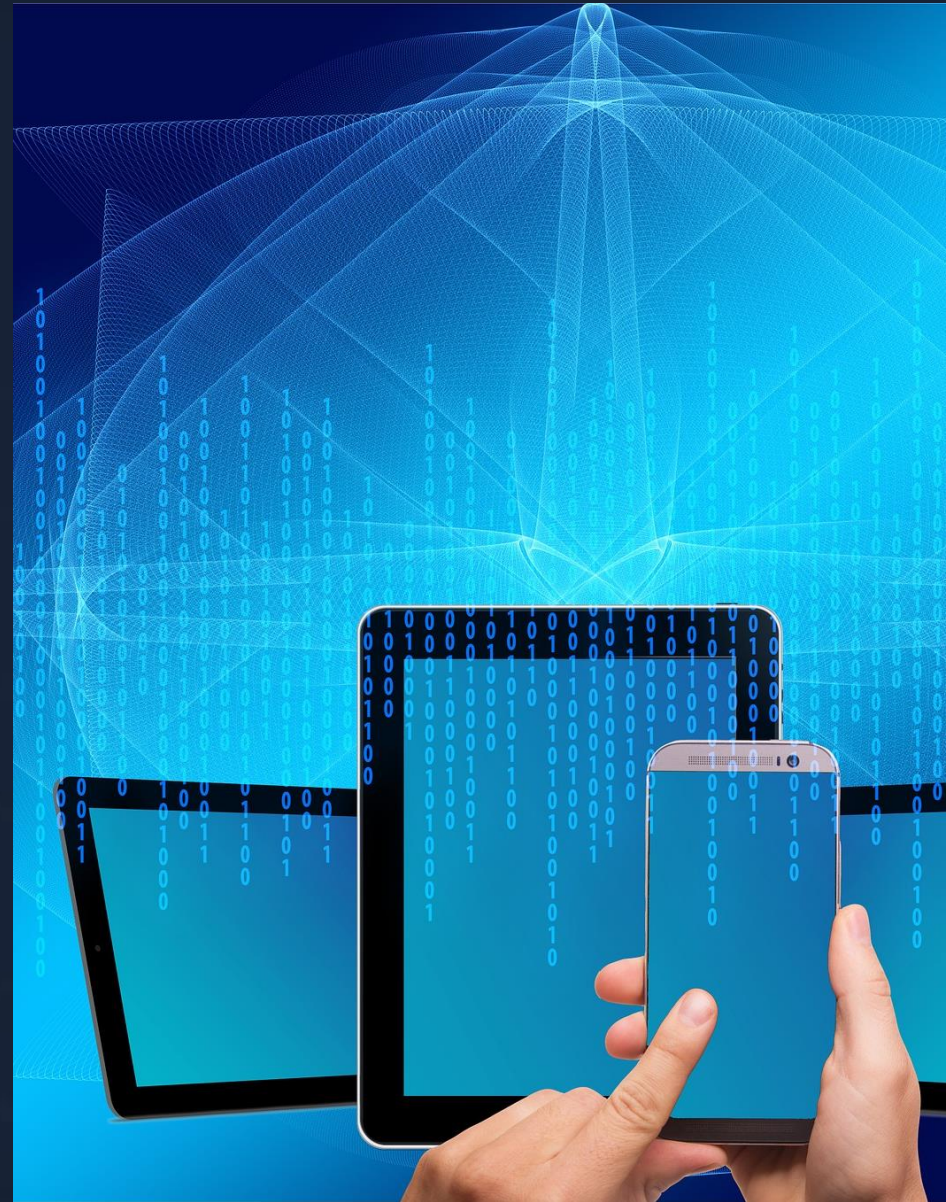
- 限制單日每個IP能夠使用的網路總流量，超過標準時則進行管理
- 限制每個網段的網路使用速率，避免小部分人員佔用大部分資源
- 檢測網路內的電腦是否疑似被殭屍網路所感染，讓該電腦的擁有者能夠在參與攻擊前進行電腦的清掃。

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

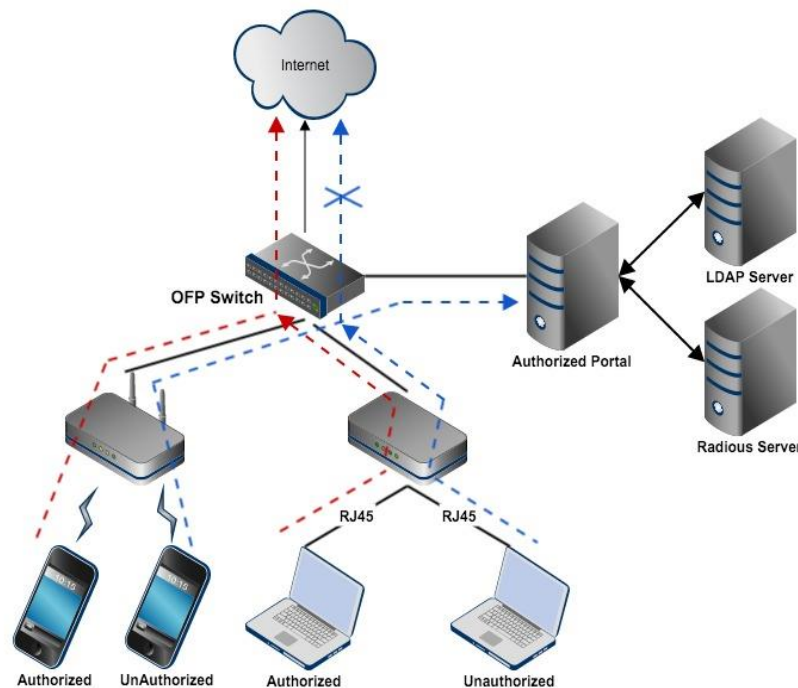
網路頻寬暴衝

IP 相衝問題



系統架構概念

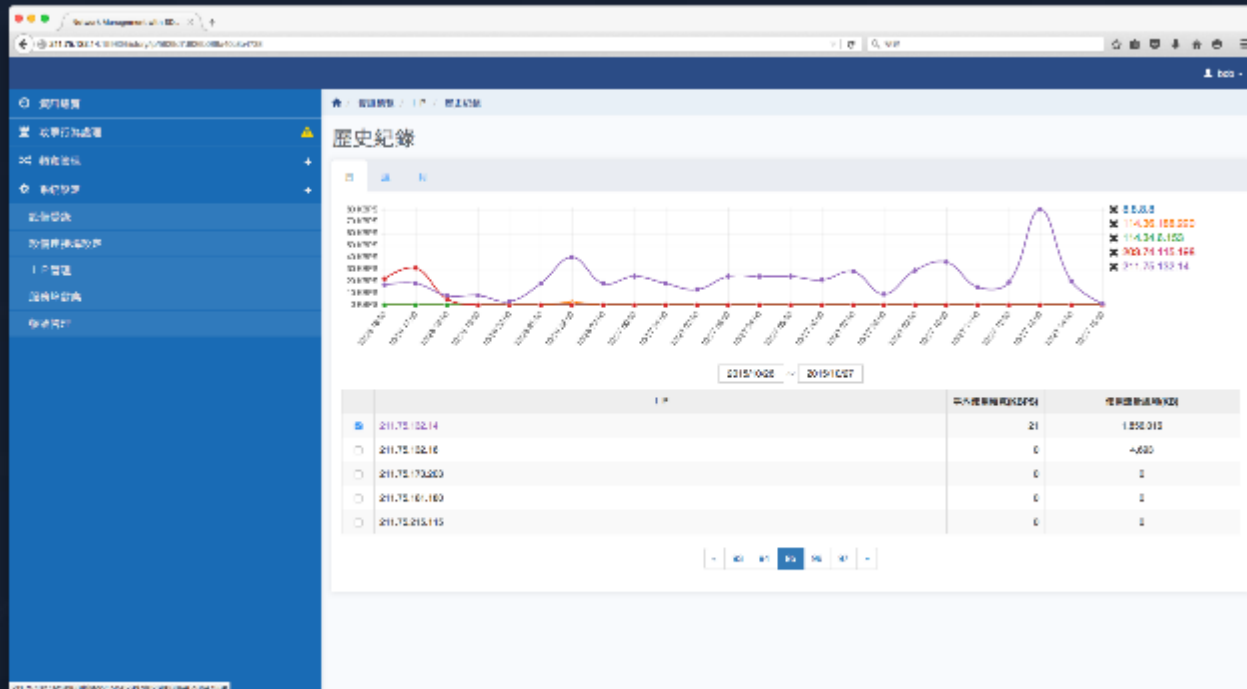
使用者分成授權(AUTHORIZED)與未授(UNAUTHORIZED)，授權者可通過OFP SWITCH連上INTERNET。而尚未通過授權之使用者則會被引導到授權頁面。



操作介面-資訊總覽

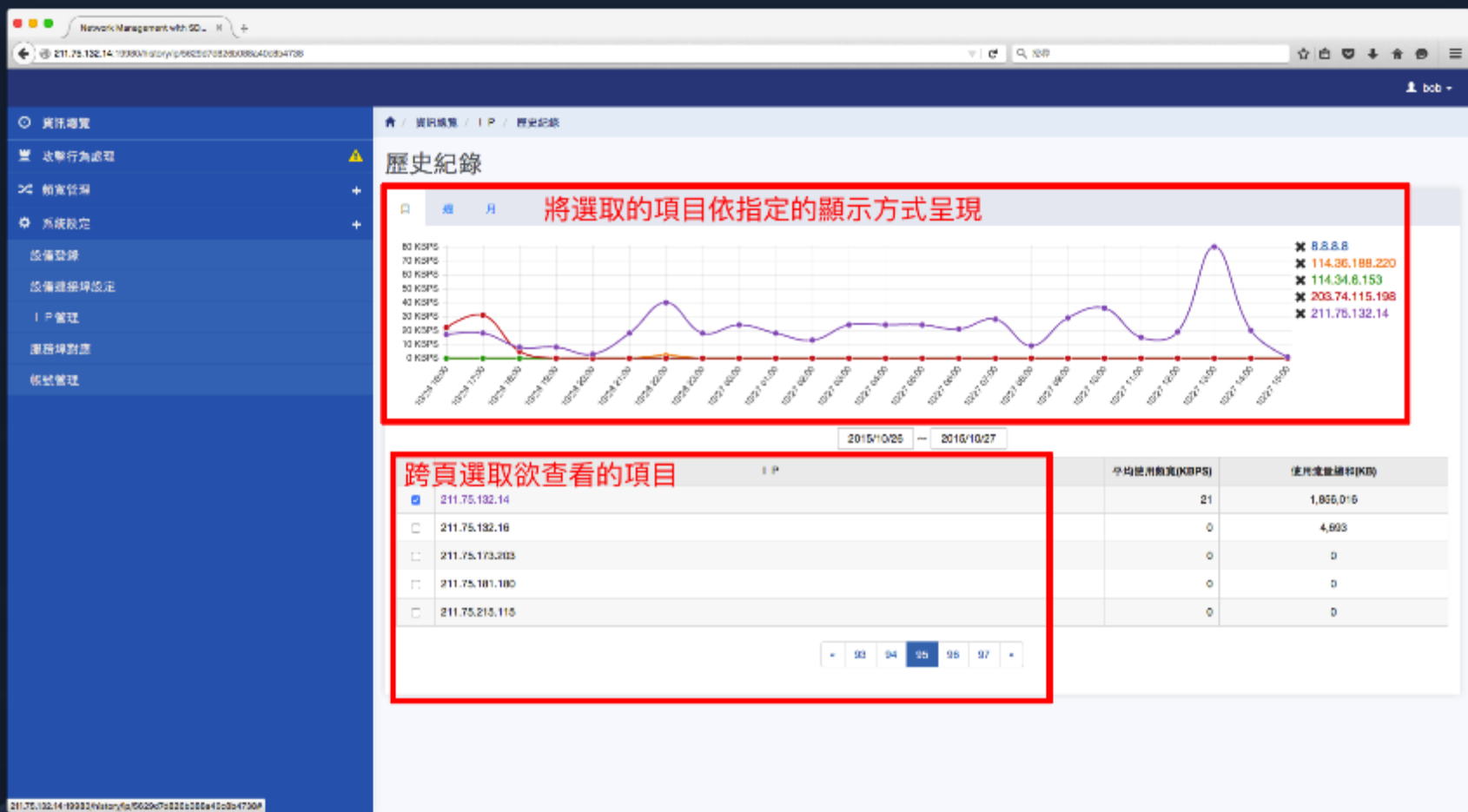
查看各種網路目前使用狀況及其歷史紀錄

- 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



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

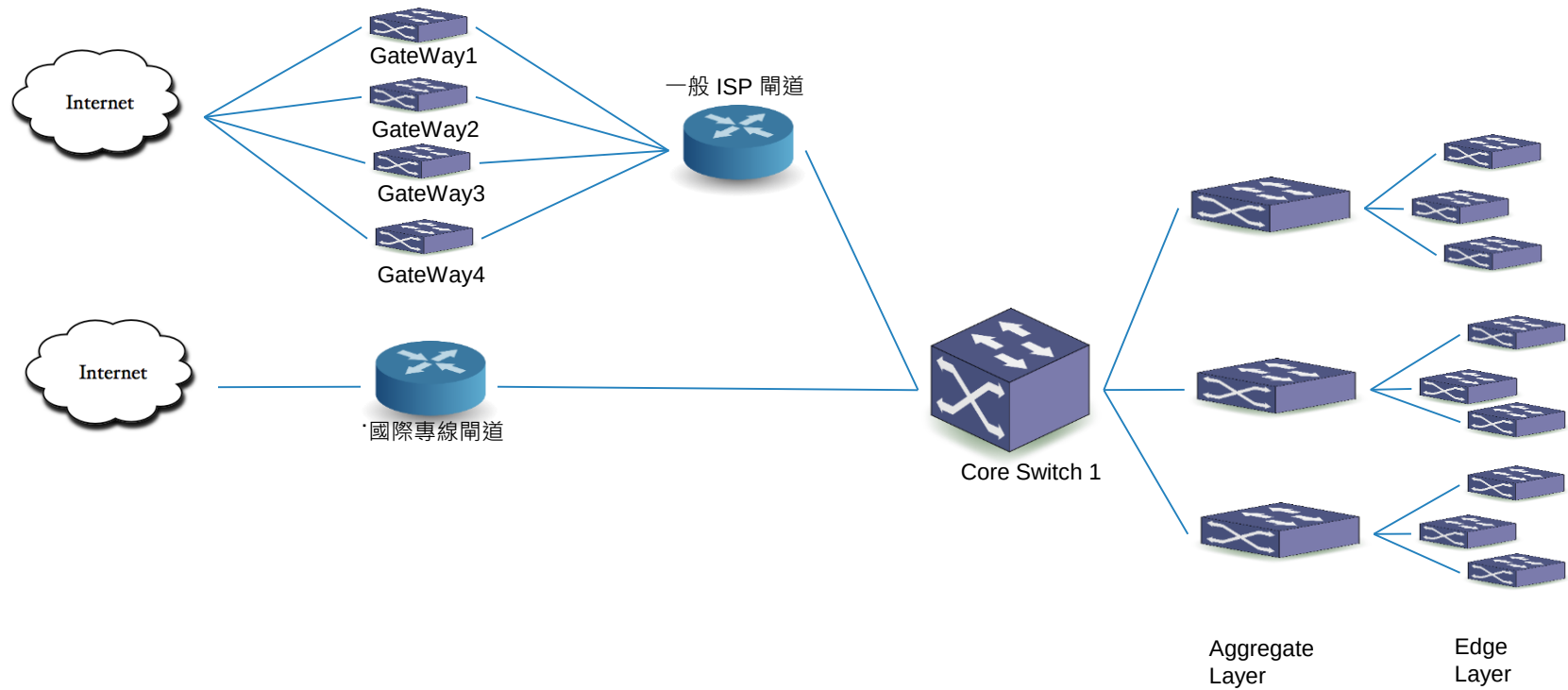
- 固定會有服務人員會一直在處理員工不同裝置要使用學校網路
- 限制每個IP的網路使用速率，避免公用電腦被不當使用，或佔用頻寬
- 可在特定時間將特定網段的流量導入不同的閘道，製造隔離的網路環境，供研發能夠切換成欲使用的開發環境

網路頻寬暴衝

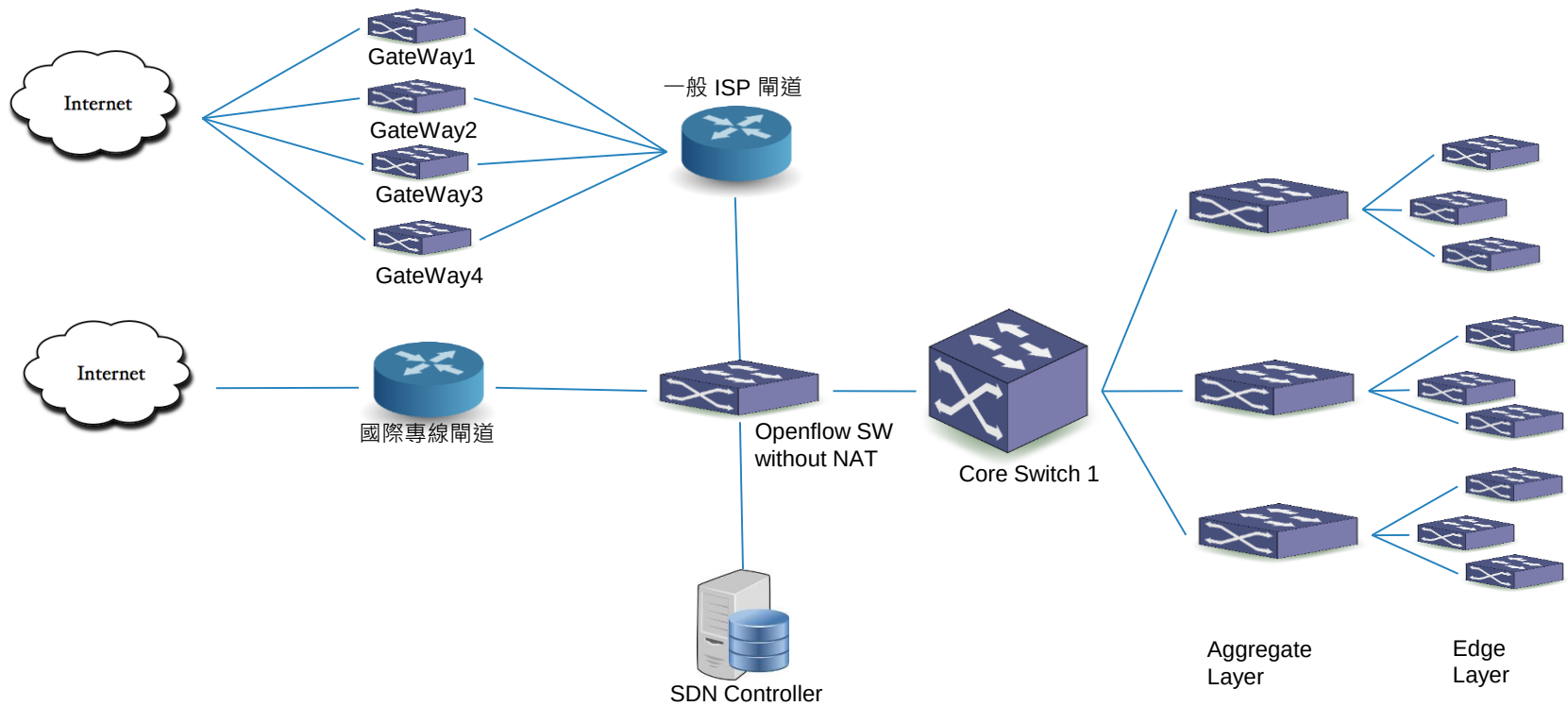
IP 相衝問題



現行網路架構說明



建議網路架構說明



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。


國立中央大學
WAN LOAD BALANCING

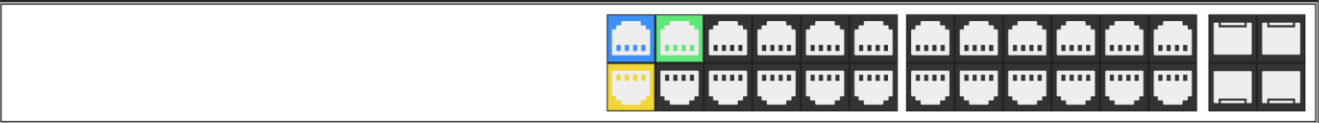
☰



儀表板
線路管理
Policy Group管理
網路品質歷史紀錄
App Group管理

線路管理

請選擇交換器： ICX7450 24p ▾



現有線路清單 +

序號	名稱	閘道器MAC	用途	配置	預設通道	色碼	編輯	刪除
1	交大國際(POC通往Core SW)	00:01:02:03:04:06	external	1	✓		編輯	刪除
2	內部線路(POC測試網段)	00:0C:29:1C:80:...	internal	2			編輯	刪除
3	一般ISP閘道	00:0C:29:1C:80:49	external	3			編輯	刪除



1



操作介面

導向規則設置 – POLICY GROUP管理

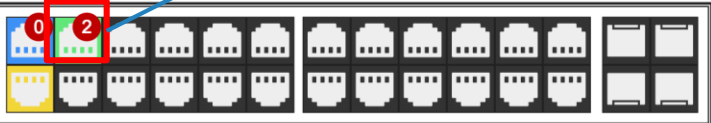
透過此功能進行封包導向的管理, 未符合任何規則的封包會導向「預設」的規則, 若有設定規則則會依照設定的規則導向, 可同時設定內部網段規則與外部網域或網段規則。


國立中央大學
WAN LOAD BALANCING

儀表板
線路管理
Policy Group管理
網路品質歷史紀錄
App Group管理

Policy Group管理

請選擇交換器：ICX7450 24p



Policy Group清單

	名稱	內部網段規則	對外網域規則	導向線路	優先度	編輯	刪除
1	內部測試網段A	192.168.2.0/24	無	一般ISP開道	1	編輯	刪除
2	Google轉往一般ISP開道	無	3個規則	一般ISP開道	2	編輯	刪除
3	預設	無	無	交大國際(POC通往Core SW)	最低	編輯	刪除

網孔上會顯示線路的代表色以及多少Group被導向此線路
滑鼠滑上後會顯示規則內容

操作介面

導向規則設置 – APP GROUP管理


國立中興大學
WAN LOAD BALANCING

儀表板
線路管理
Policy Group管理
網路品質歷史紀錄
App Group管理

今日Top 10的APP Group清單

請選擇交換器： ICX7450 24p

名稱	今日Session累計量	處理方式	設定規則
http	93421		設定
tcp	81231		設定
facebook	71203	導向： 一般ISP開道	設定
https	53121		設定
unknown_tcp	15823		設定
dns	14023		設定
snmp	9120		設定
icmp	6310		設定
yahoo	2015	限制流量： 5.00 Mbps	設定
ntp	1023		設定

搜尋指定的APP Group

已進行過處理的APP Group清單

名稱	處理方式	設定規則	刪除
facebook	導向： 一般ISP開道	設定	刪除
yahoo	限制流量： 5242880 BPS	設定	刪除

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

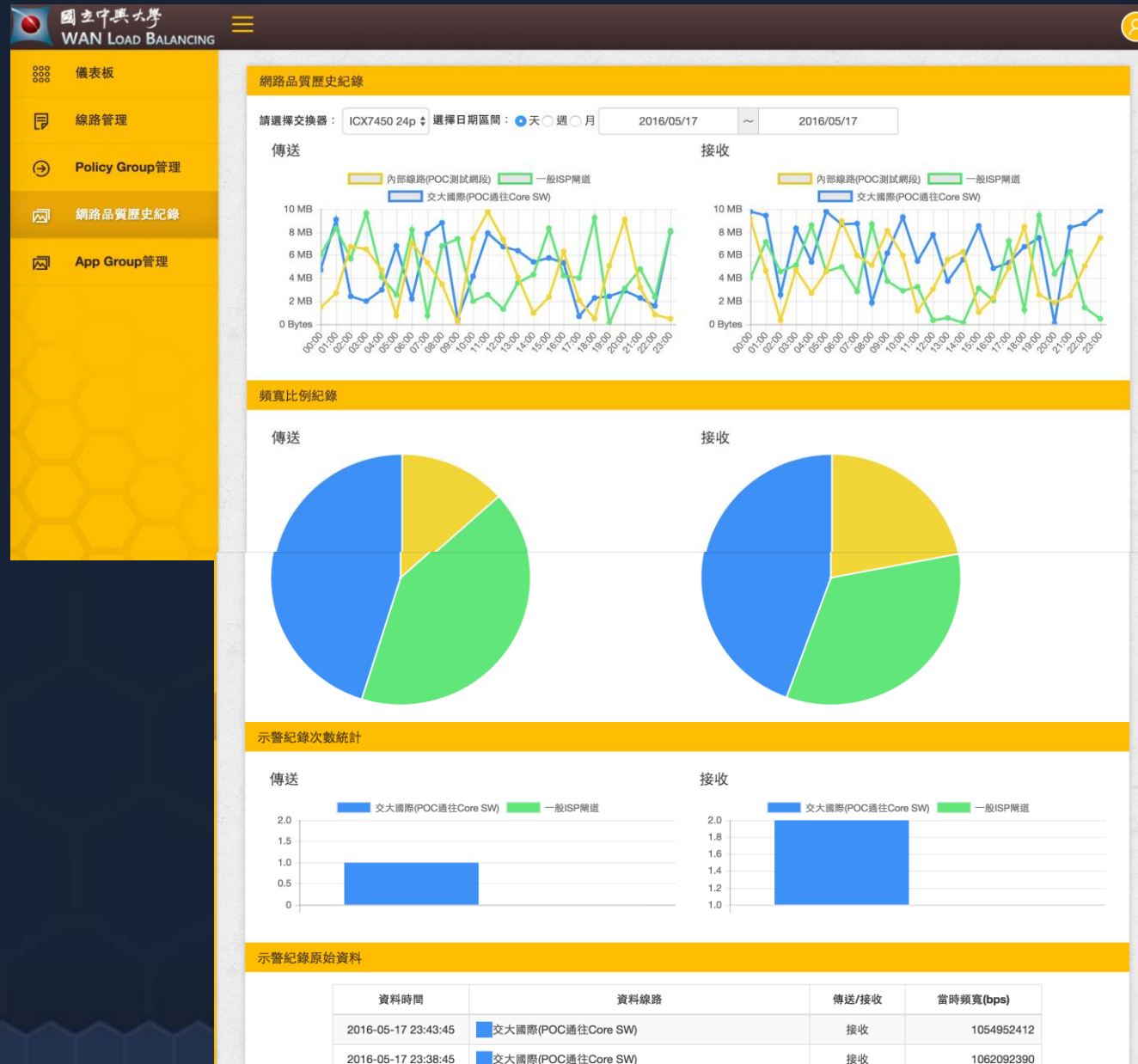
操作介面

儀表板



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

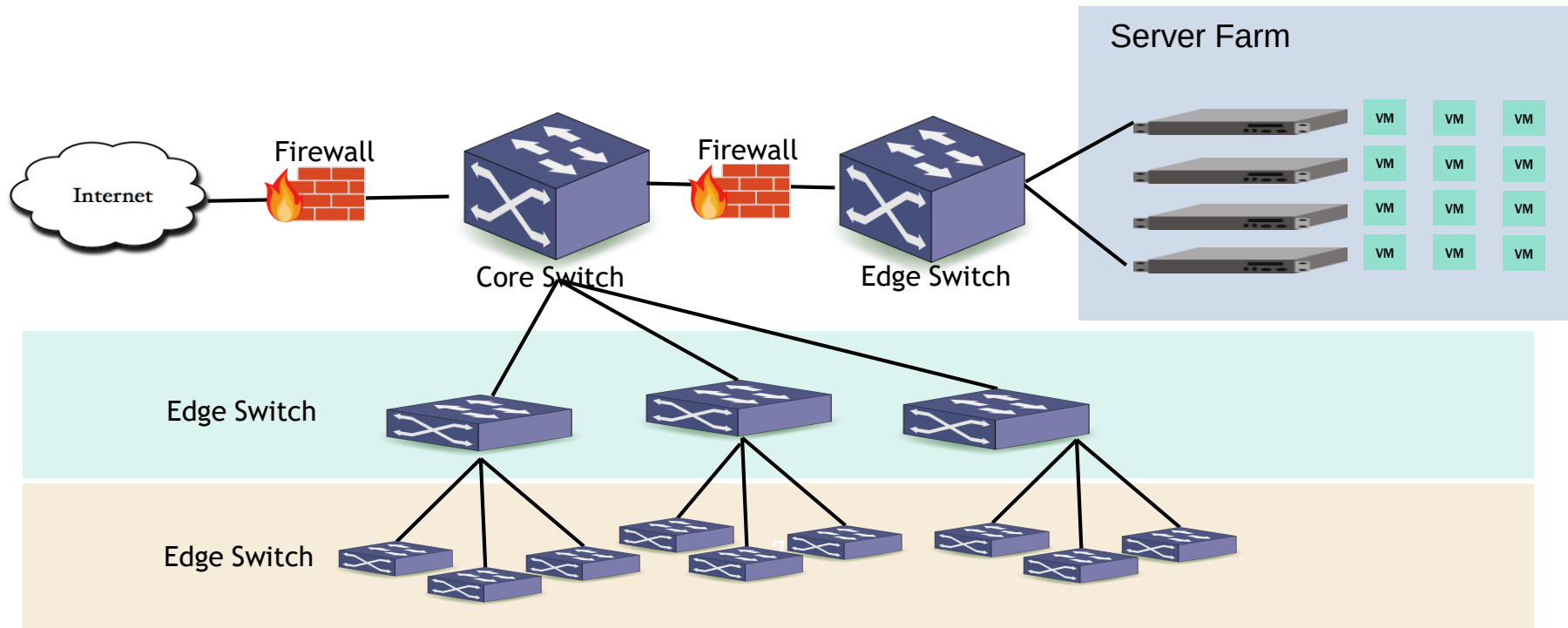
- 傳統的網路架構，各機器各司其職，資源使用比重不一。
- SDN架構，網路設備只專注於傳遞封包，不做網路管理。

傳輸效率提升

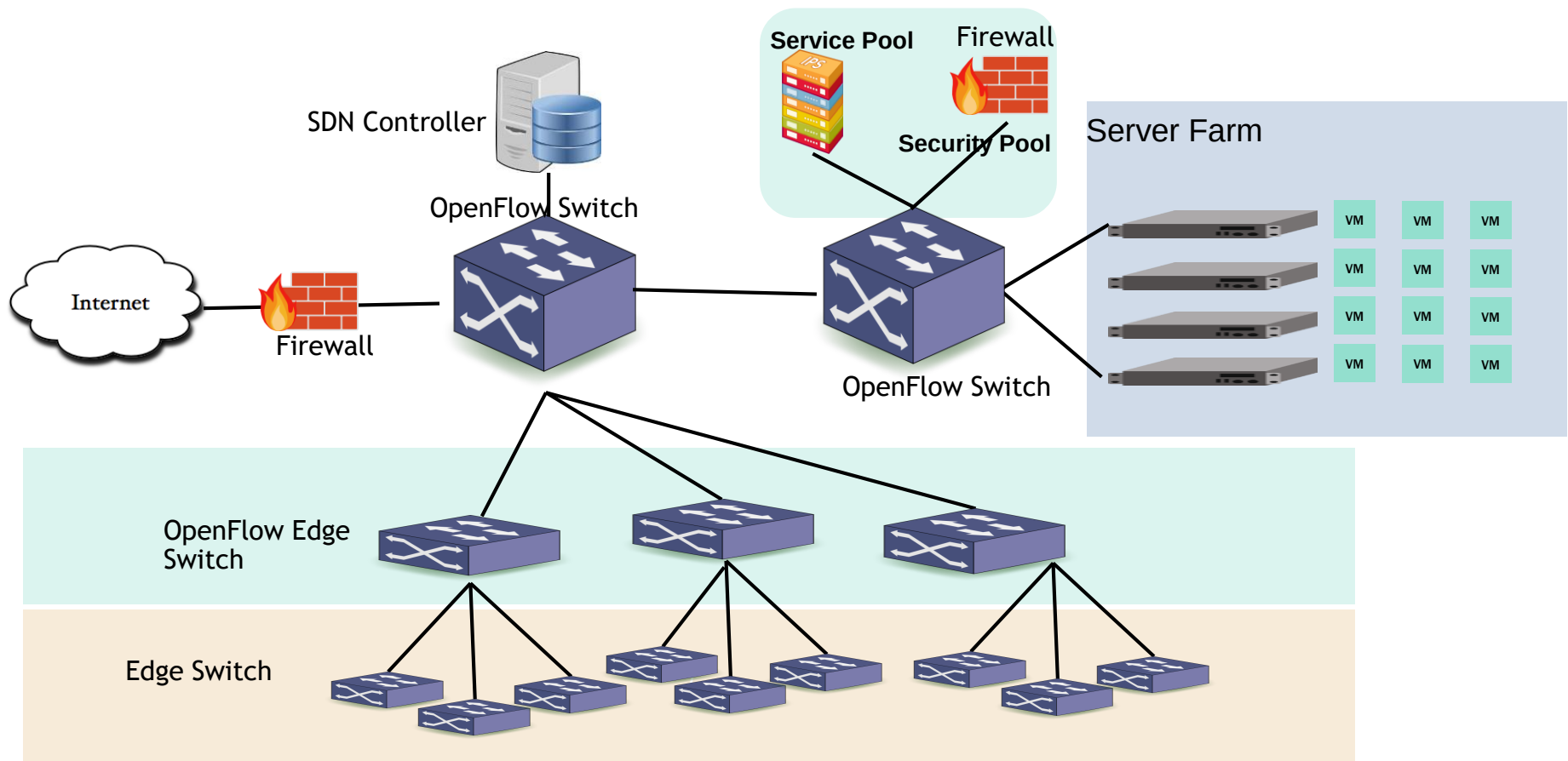
- SDN網路架構就是為了解決傳統網路的這些問題，SDN的特色是修改了傳統網路架構的控制模式，將網路分為控制層 (CONTROL PLANE) 與資料層 (DATA PLANE)，將網路的管理權限交由控制層的控制器 (CONTROLLER) 軟體負責，採用集中控管的方式。



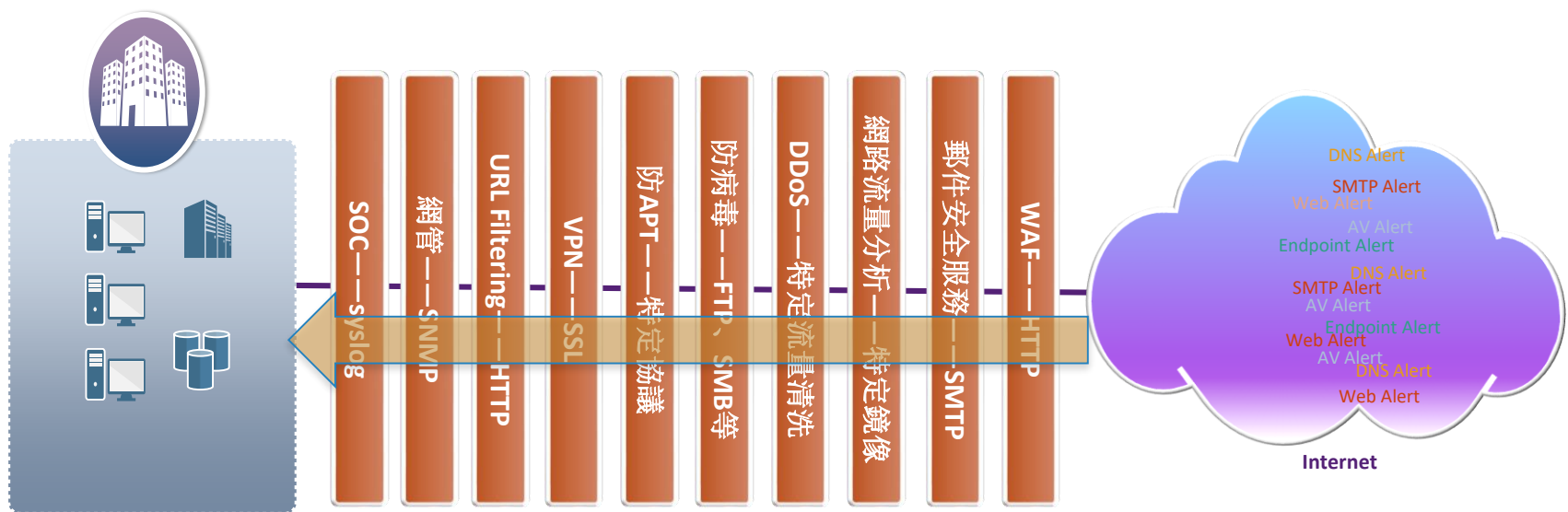
現行網路架構說明



建議網路架構說明



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？

應急回應變慢

新產品、新功能測試困難

設備故障後，更換困難

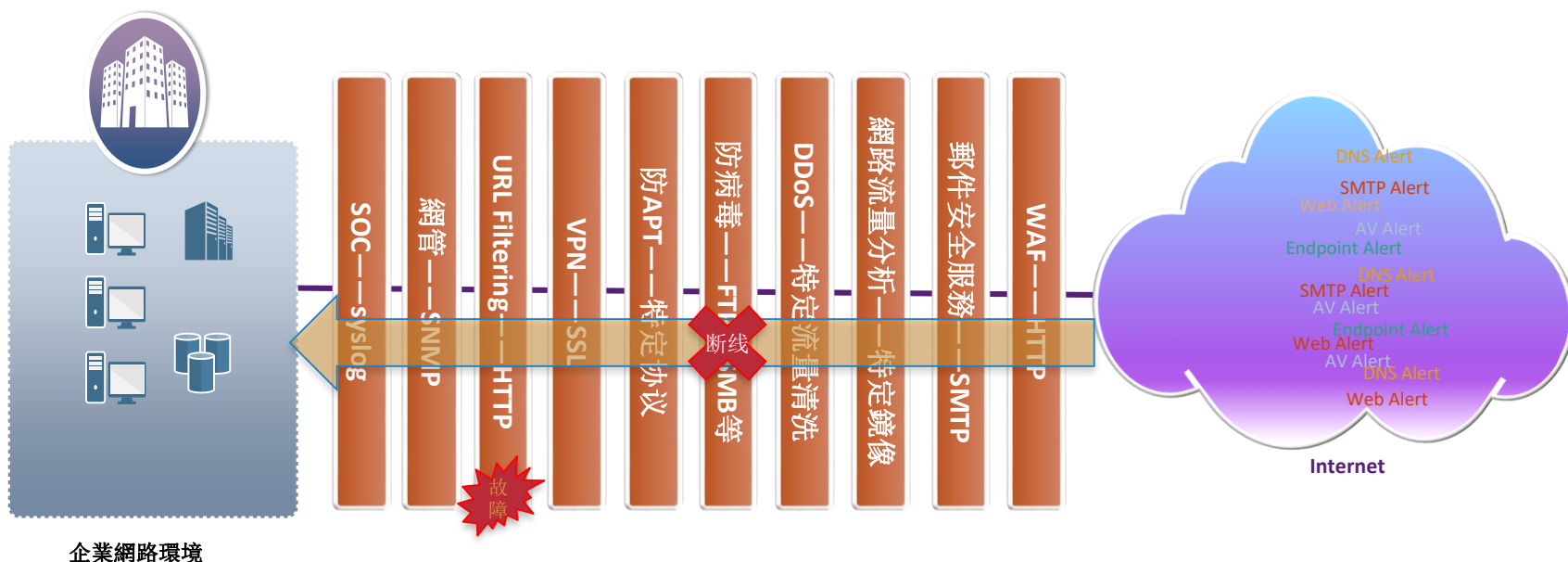
內網或VM之間交互流量難以處理

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

過往的安全服務鏈架構



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

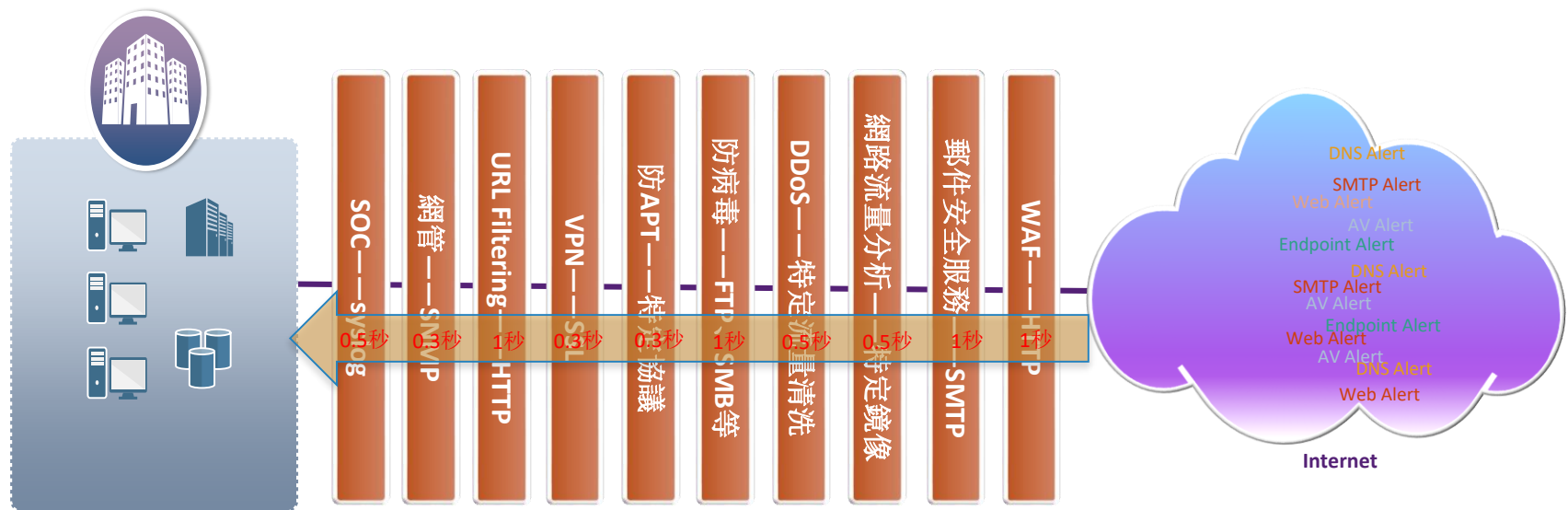
有限的視覺化程度

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

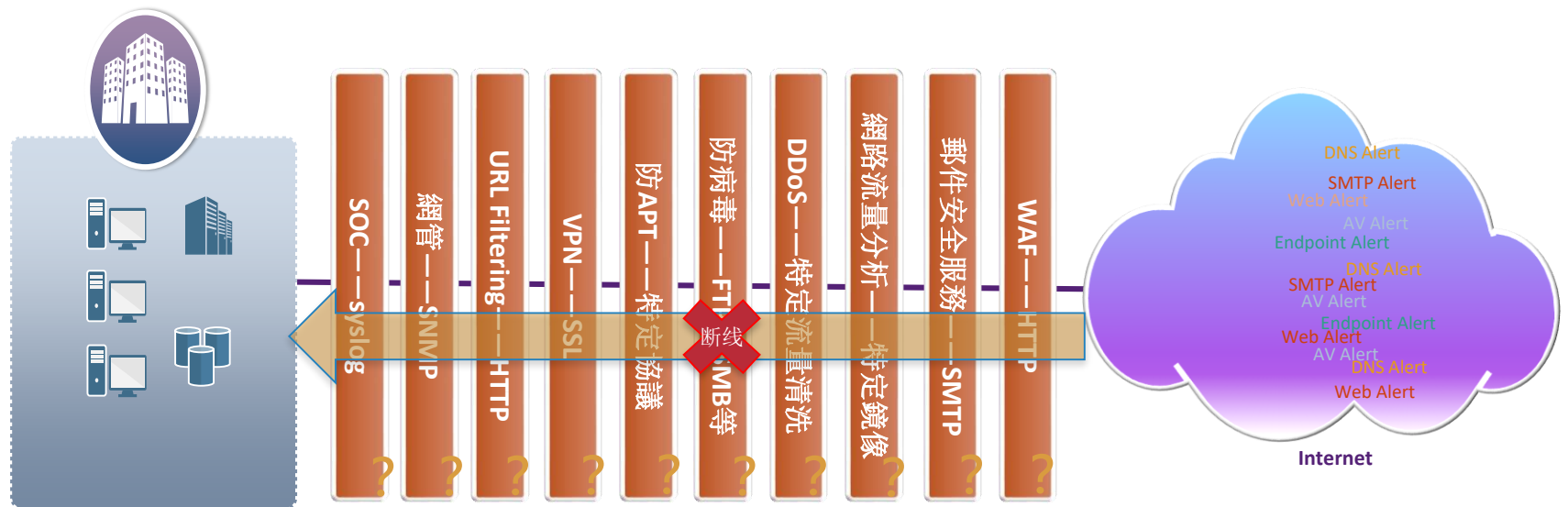
有限的視覺化程度

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？

應急回應變慢

新產品、新功能測試困難

設備故障後，更換困難

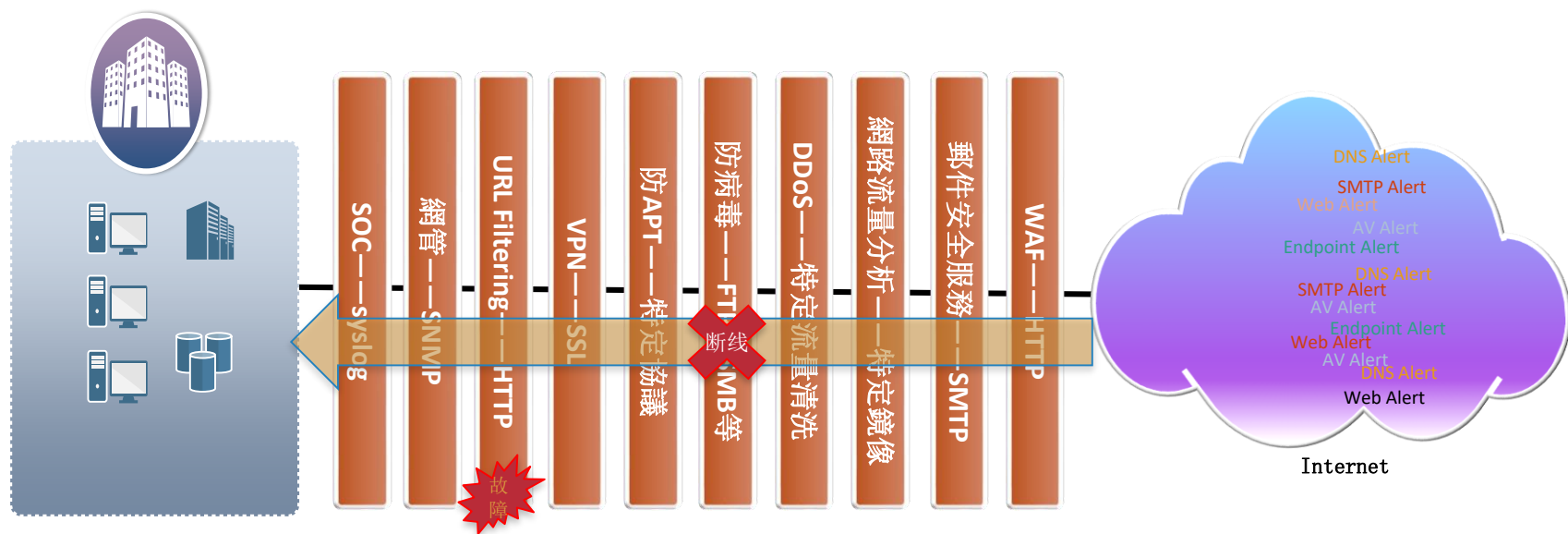
內網或VM之間交互流量難以處理

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

過往的安全服務鏈架構



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？

應急回應變慢

新產品、新功能測試困難

設備故障後，更換困難

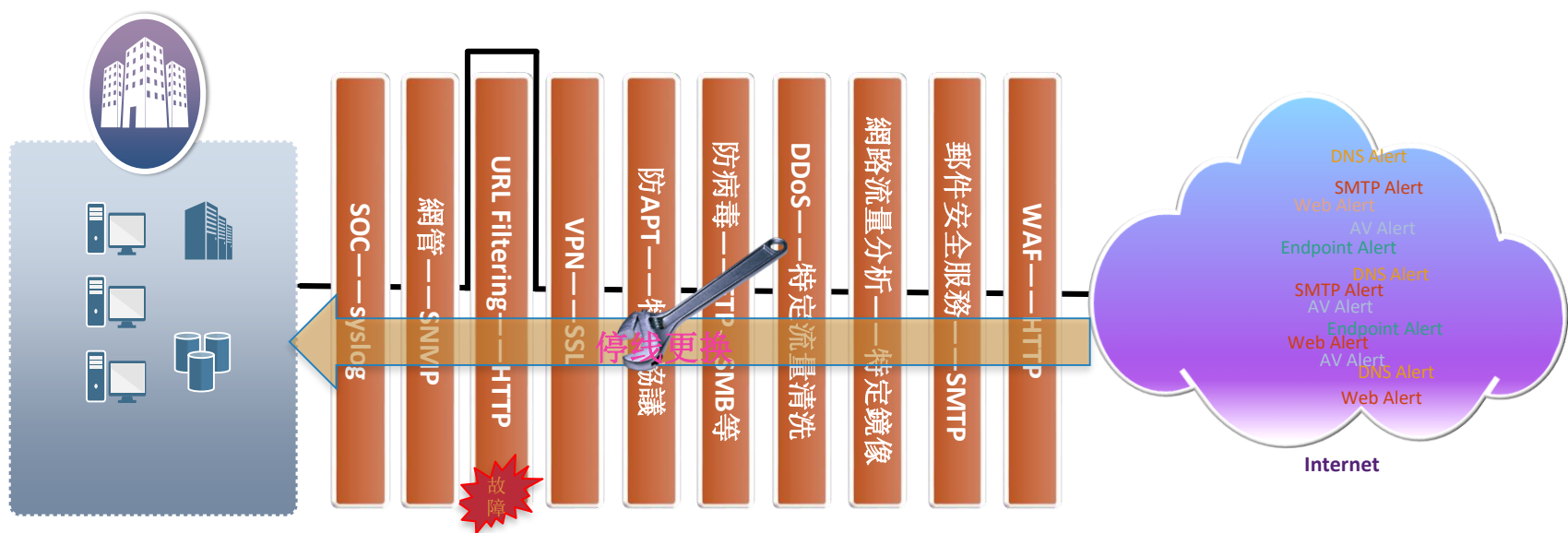
內網或VM之間交互流量難以處理

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

過往的安全服務鏈架構



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？

應急回應變慢

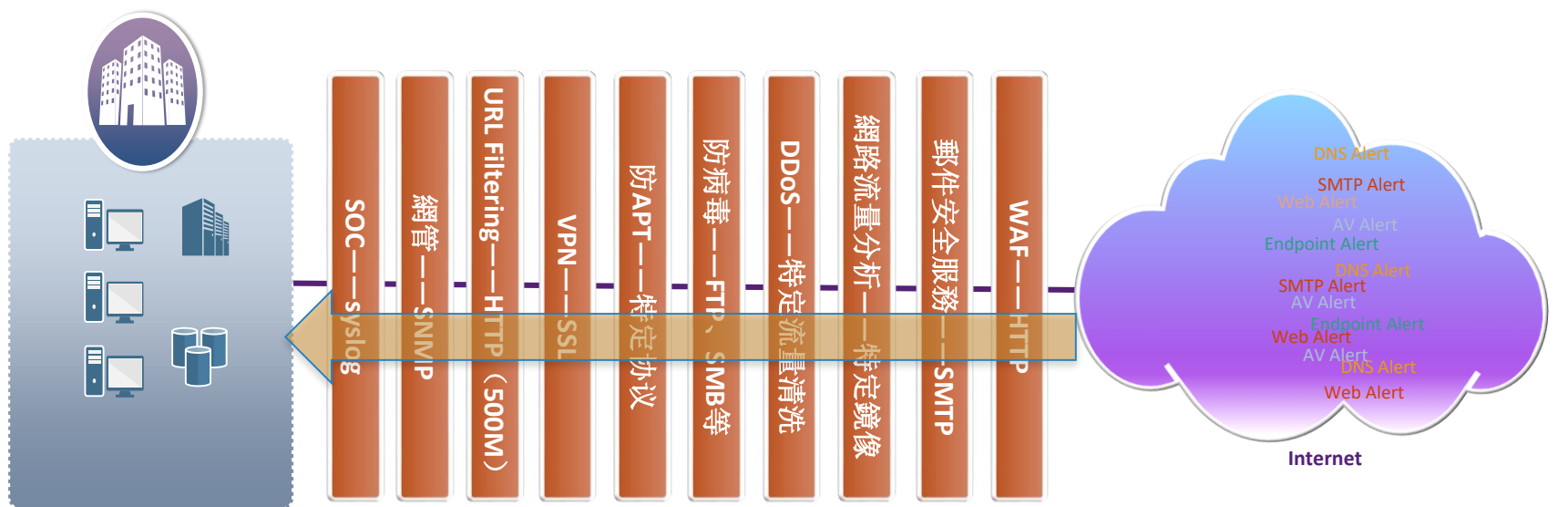
新產品、新功能測試困難
設備故障後，更換困難

內網或VM之間交互流量難以處理

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

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？

應急回應變慢

新產品、新功能測試困難
設備故障後，更換困難

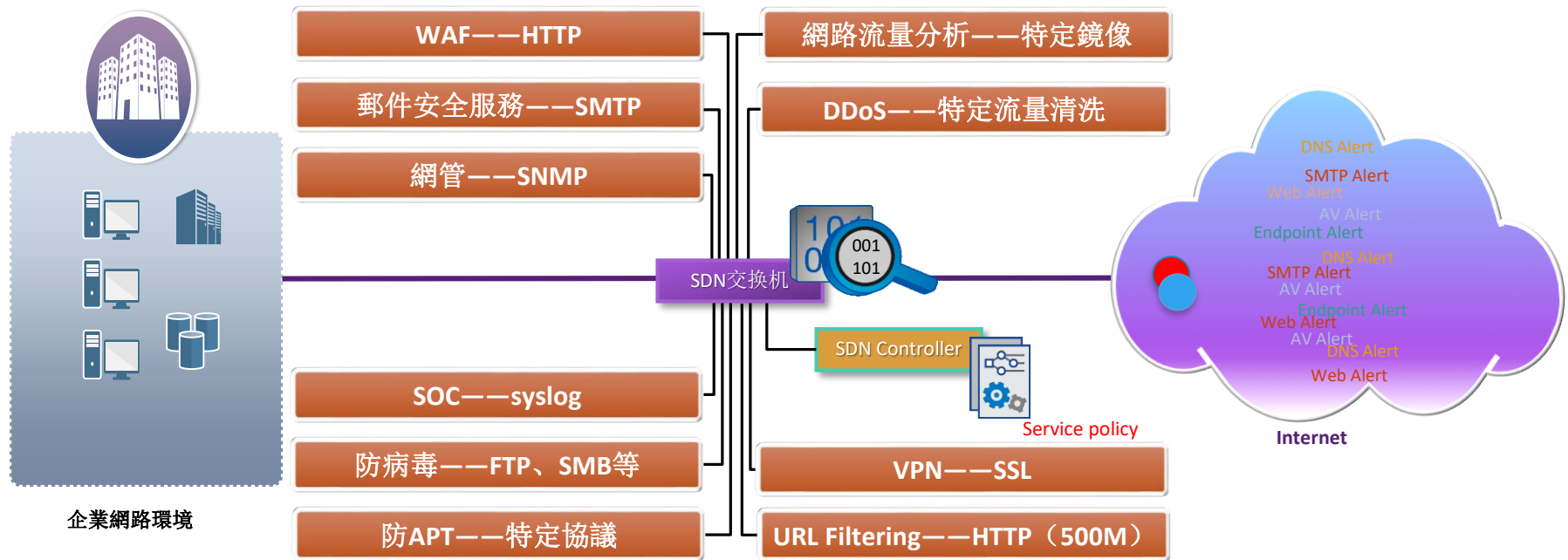
內網或VM之間交互流量難以處理

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

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？

應急回應變慢

新產品、新功能測試困難

設備故障後，更換困難

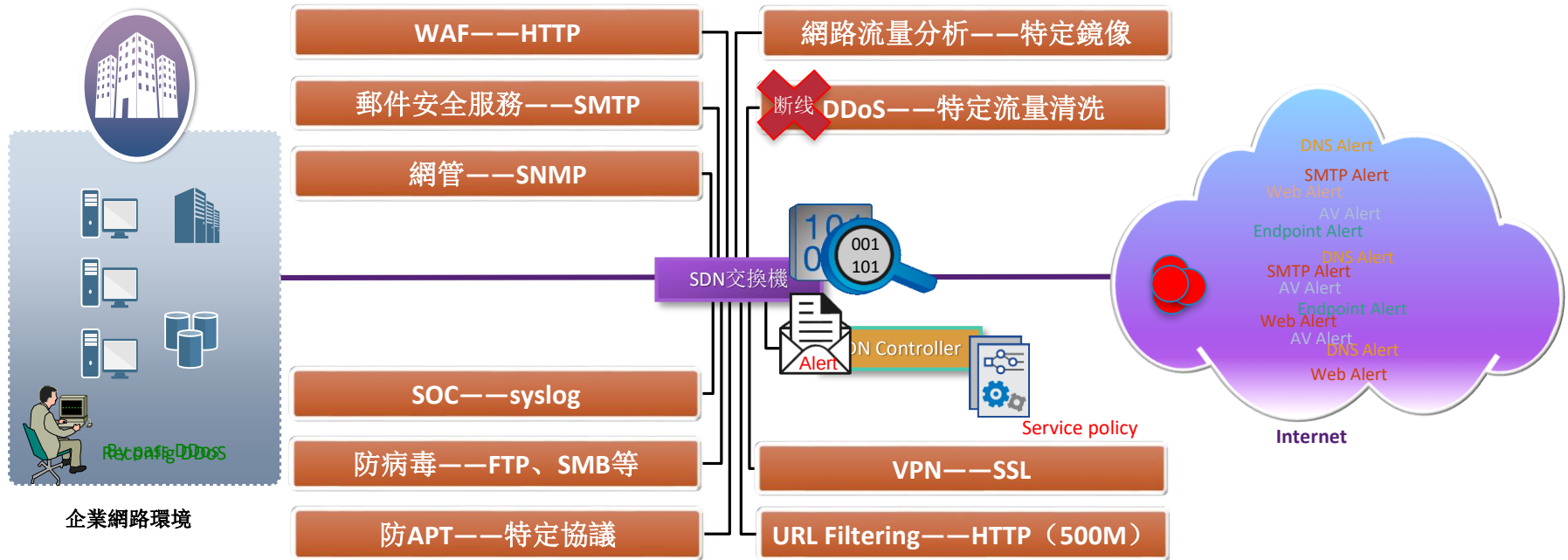
內網或VM之間交互流量難以處理

多用戶、多許可權、安全管理

有限的可視化程度

性能疊加困難，往往面臨性能瓶頸

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？

應急回應變慢

新產品、新功能測試困難

設備故障後，更換困難

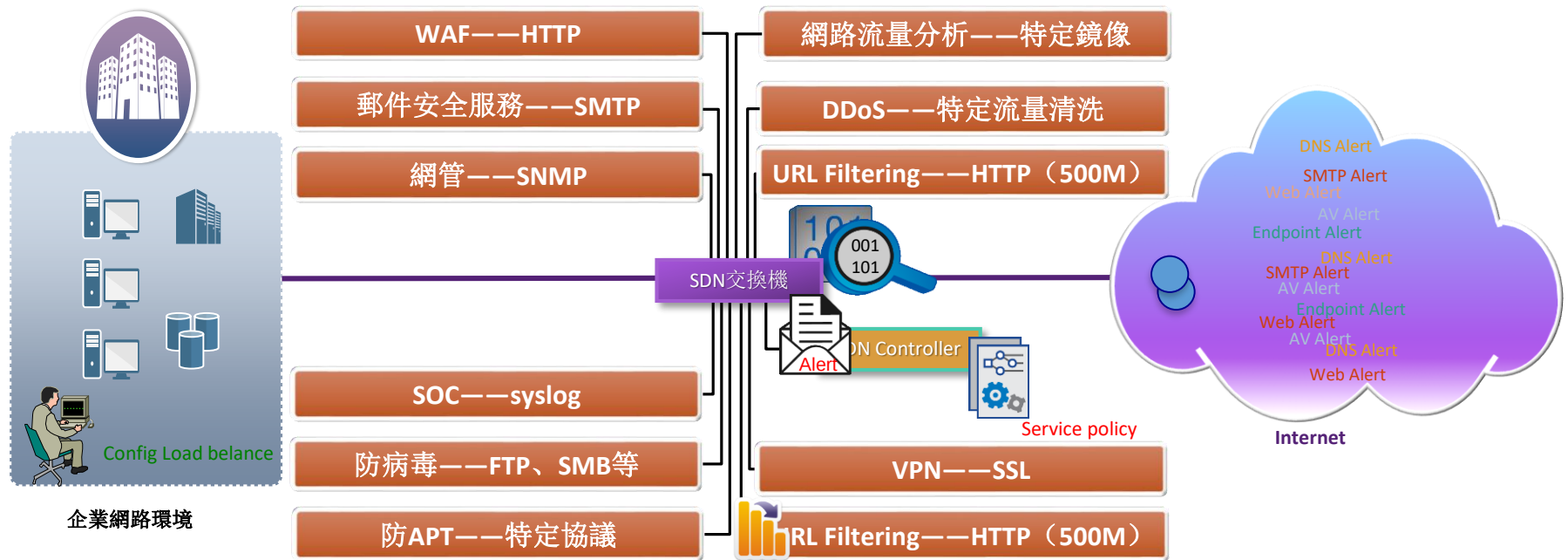
多用戶、多許可權、安全管理

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？

應急回應變慢

新產品、新功能測試困難

設備故障後，更換困難

內網或VM之間交互流量難以處理

多用戶、多許可權、安全管理

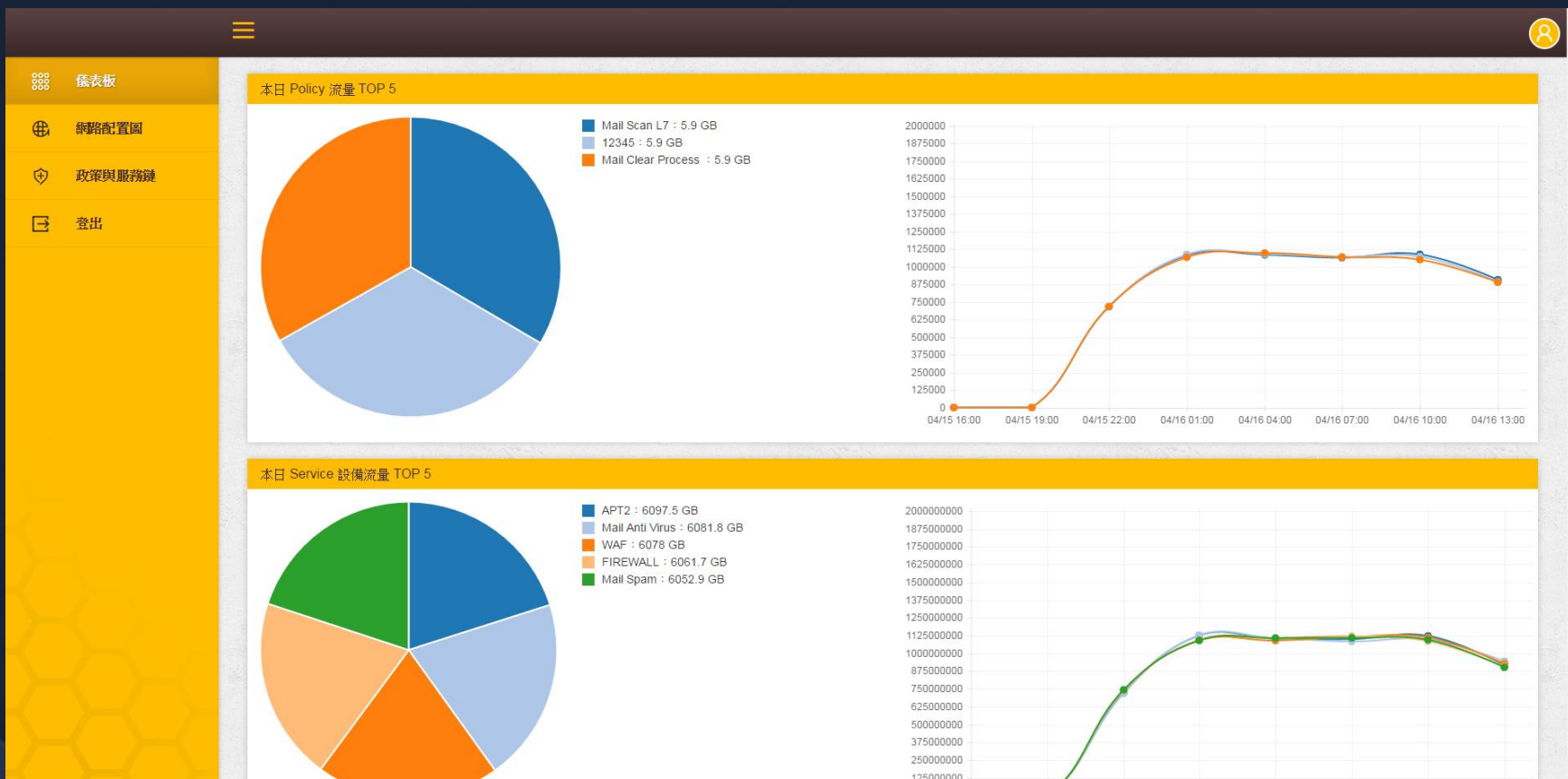
有限的視覺化程度

性能疊加困難，往往面臨性能瓶頸

操作介面

DASHBOARD 統計 ENVIRONMENT SETTING

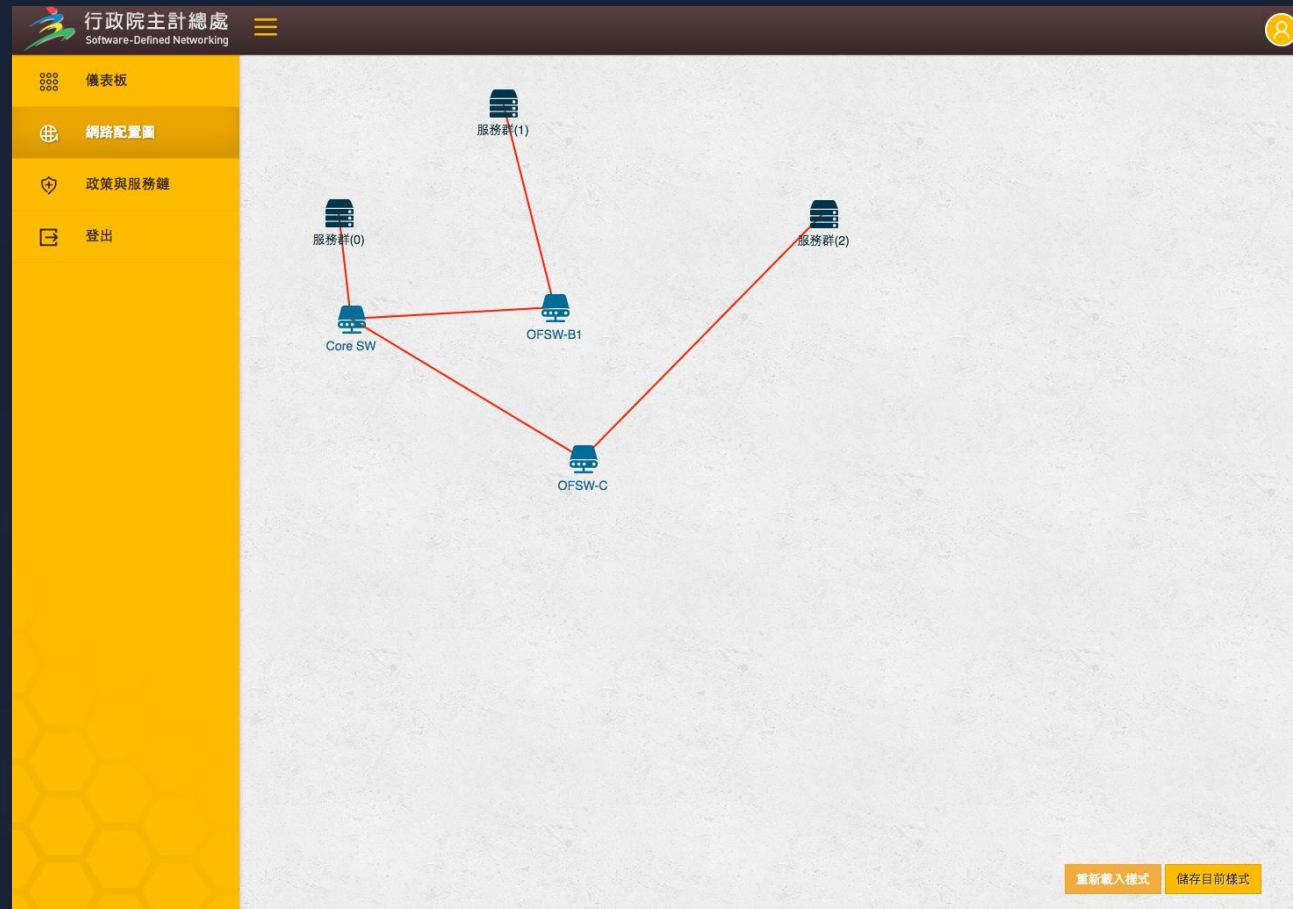
- 顯示 POLICY 流量 TOP 5
- 顯示 SERVICE 流量 TOP 5



操作介面

自動偵測網路拓撲

- 自動偵測網路拓撲
- 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

服務鍊名稱 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

Openflow Switch



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)



越世寬業

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



Event Management
and report



SDN Controller

Packet
Inspection

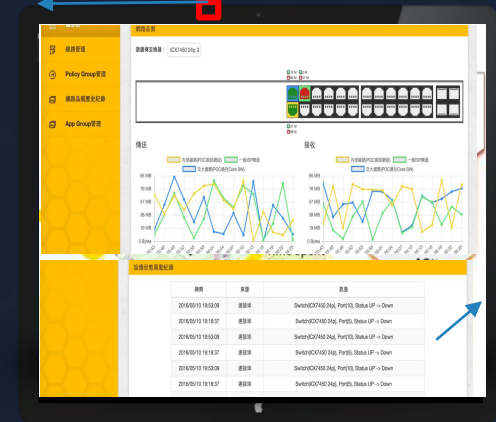


DPI Engine and IPX

Behavior
Analytics



Aruba LAN /
WLAN



3rd party Behavior
analytics for L7
Security Event



Blocked / Unblocked Wi-Fi
and Wire enabled mobile
devices / devices

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，無法防禦已發動的攻擊。



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

Manual	Time consuming & complex	Costly
• 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 processes • Require low level detailed analysis • Complex with multiple steps to diagnose problem 	• Expensive network tools • Sending qualified resources to troubleshoot is costly • Time wasted to troubleshoot 

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



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

Automated auditing

- Real time visibility into traffic
- Automated auditing of user's network traffic
- Restful APIs for 3rd party
- security solution integration



Fast troubleshooting

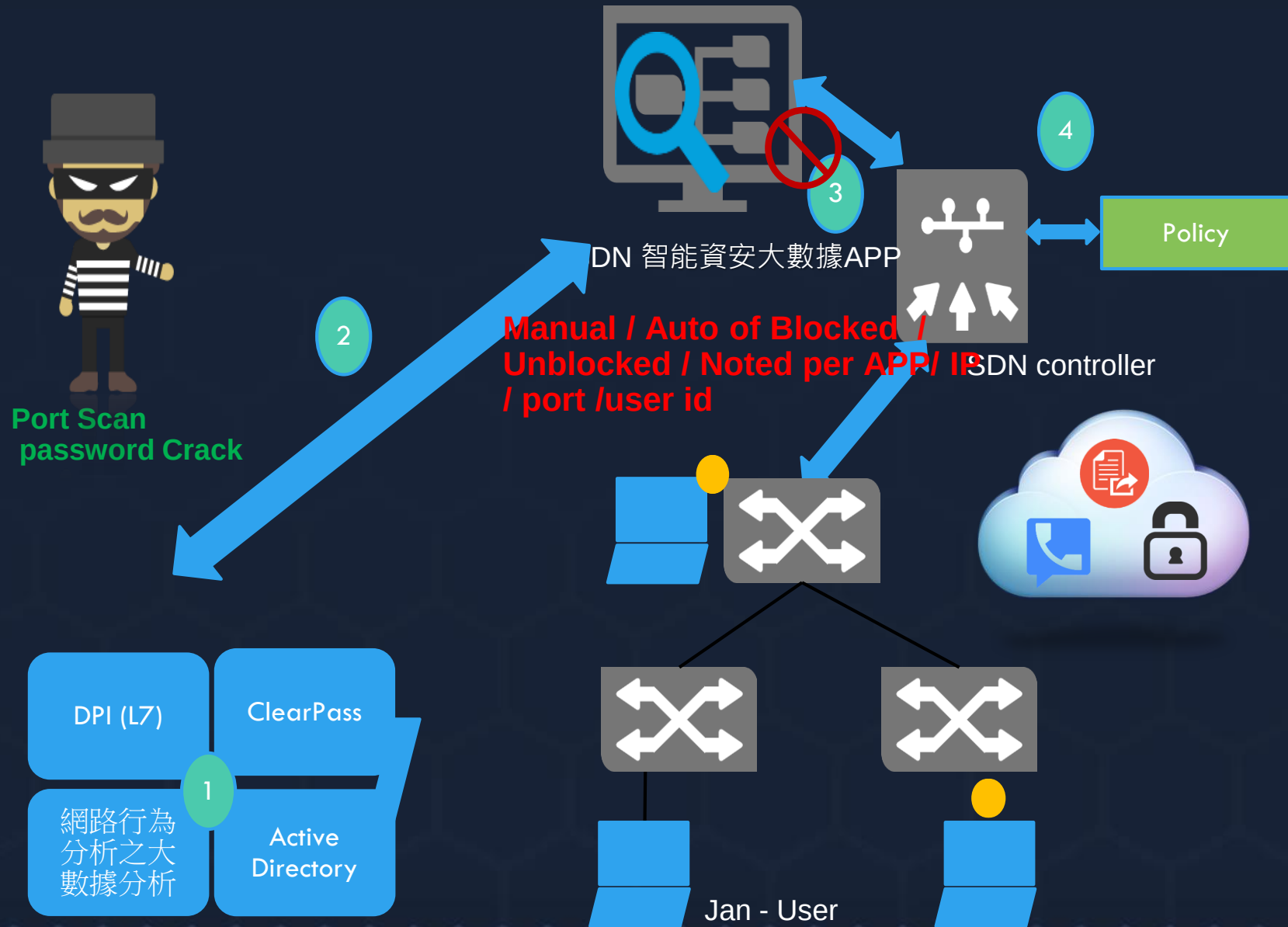
- Fast troubleshooting
- Less steps to get to root cause analysis
- Ease of access to detailed diagnostics



Cost effective

- 40X¹ cost saving compared to manual tapping tools
- No onsite technician for troubleshooting





一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.....



— 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



—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





Q & A