越世實業

SDN - solutions

主講人　S.C. Wang

Why 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

- 40X[1] 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

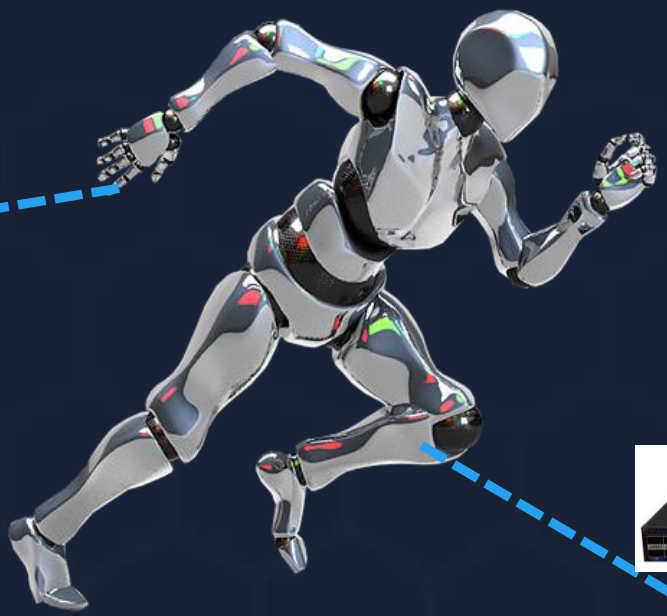
Now

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

越世實業

組成元件

SDN 控制系統



SDN App

SDN Switch

YESEE 五大方案

新一代網路架構管理願景

SDN Intranet Network Active Defense key features

Service Chain 智能分流服務鏈

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

QoS function

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

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.

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

SERVICE CHAIN 智能分流服務鏈

with SDN-Openflow

適用場景

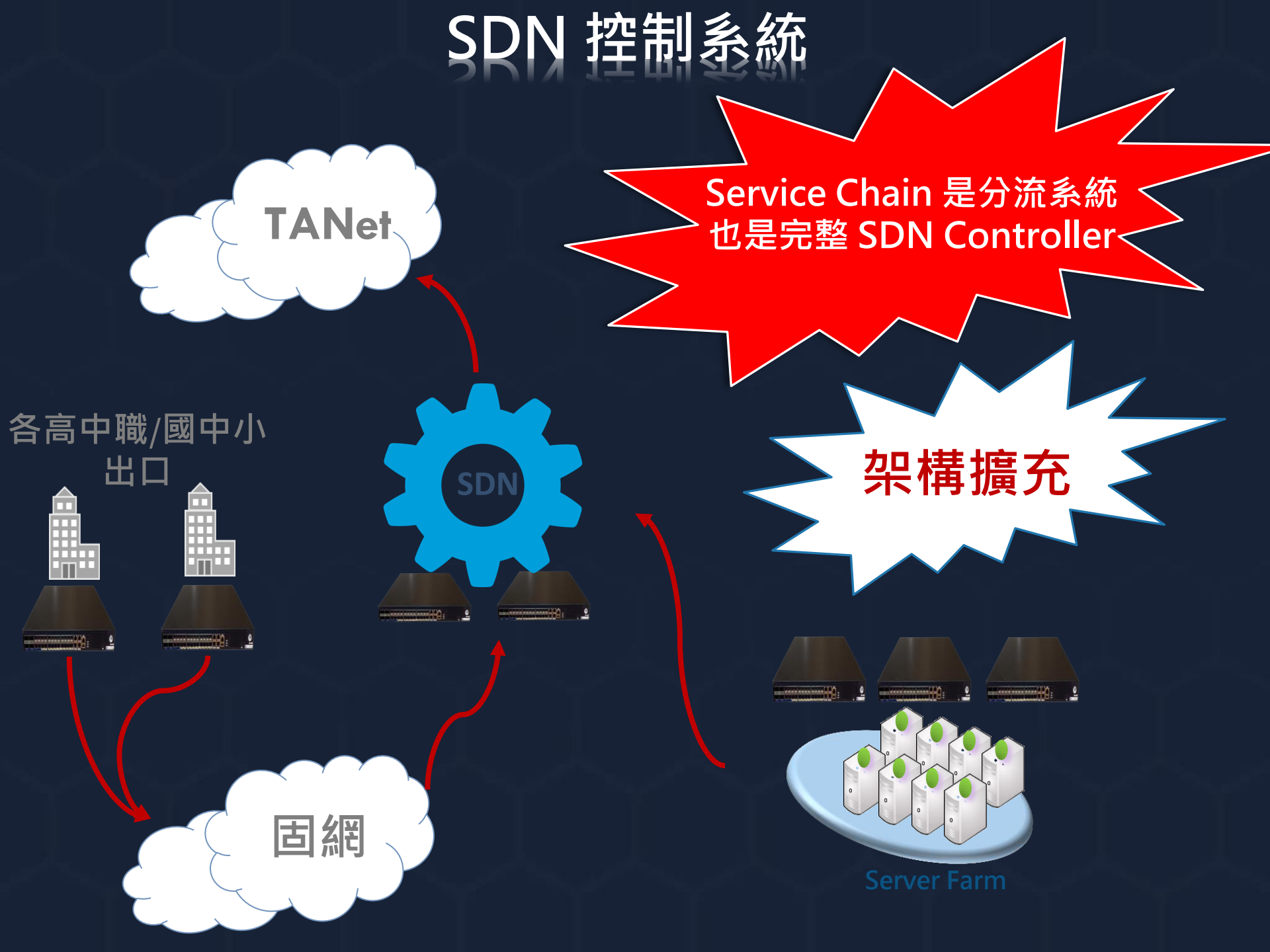
資源最佳運用

- 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。

SDN 控制系統


TANet
Service Chain 是分流系統
也是完整 SDN Controller
架構擴充
各高中職/國中小
出口
SDN
固網
Server Farm

SDN 控制系統

TANet

SDN

智慧分流系統

完整功能
- 白名單功能
- 黑名單功能
- SD 聯防 2.0
- 整合 DPI 應用層資安防禦模組

功能擴充

開放

彈性

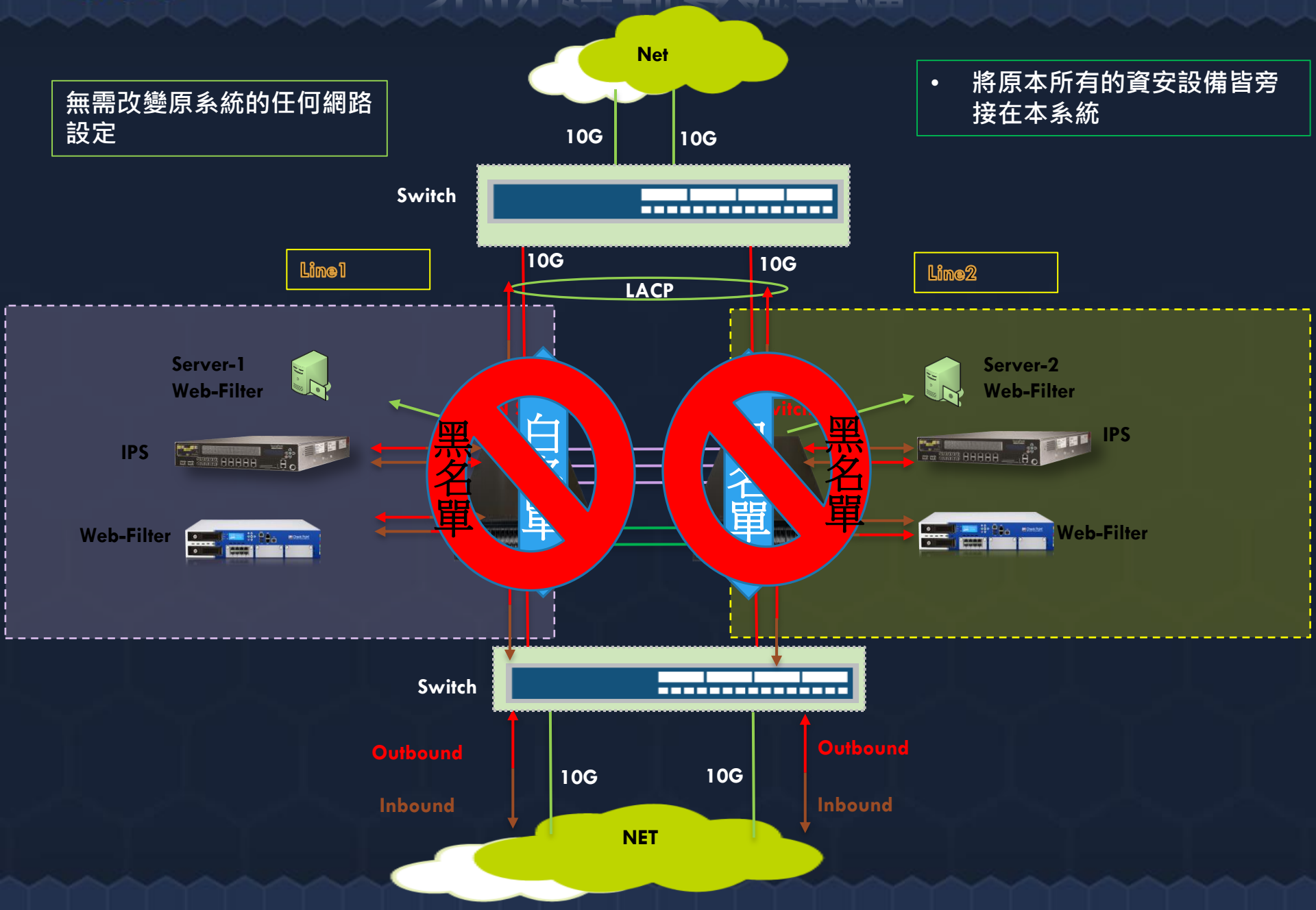
標準

越世實業

SDN 控制系統架構

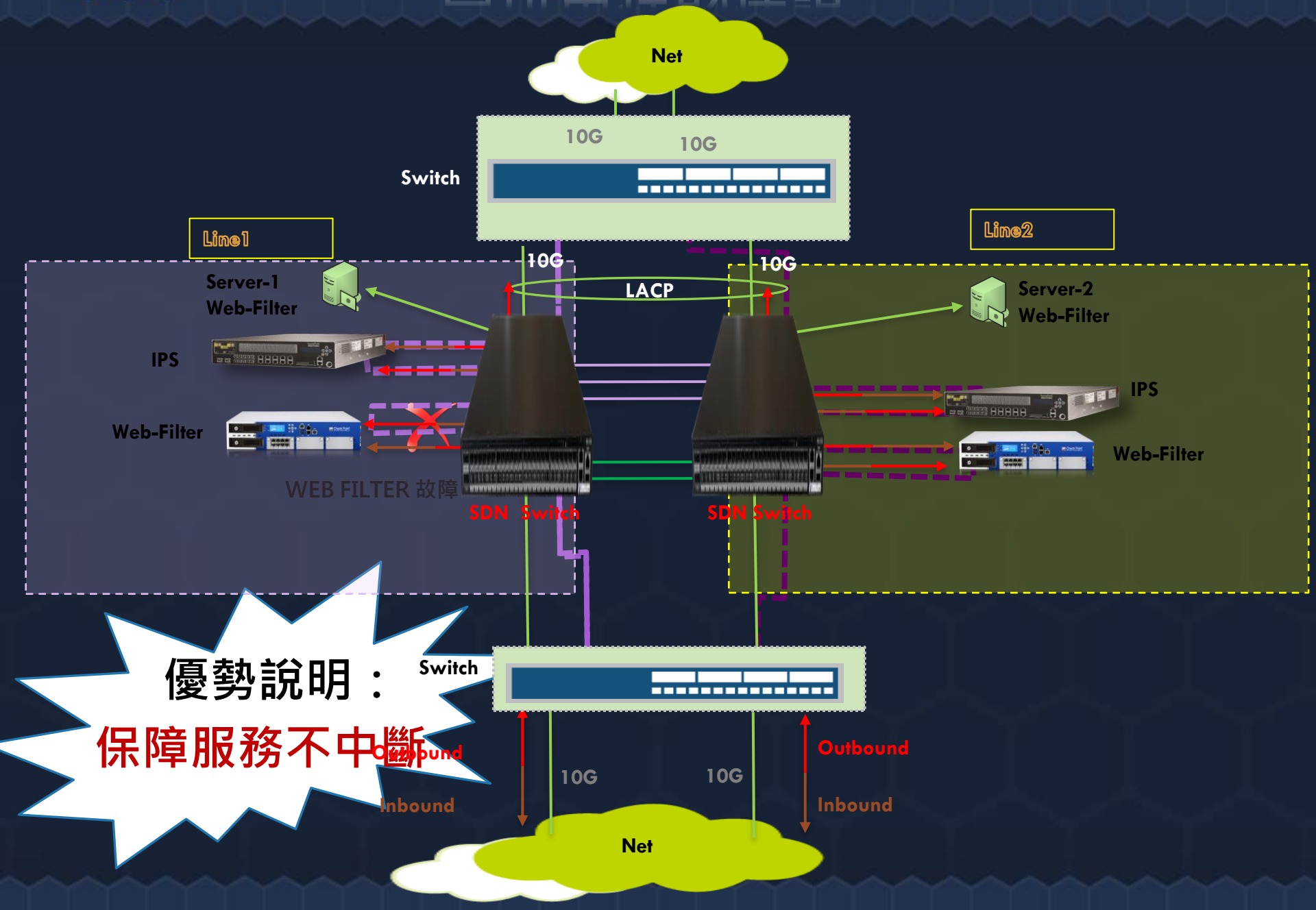
無需改變原系統的任何網路設定

- 將原本所有的資安設備皆旁接在本系統



越世實業

高可用性的保證

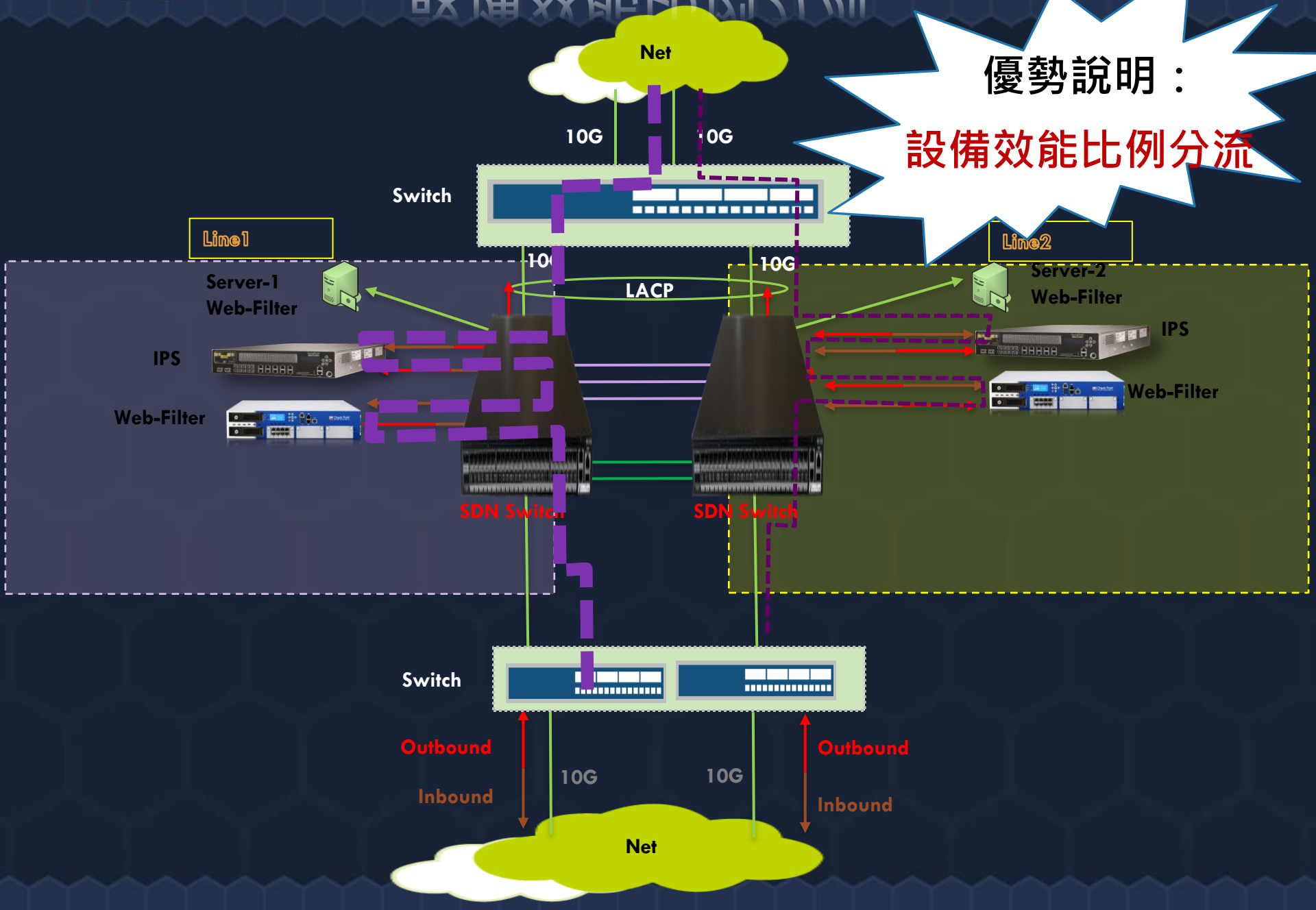


優勢說明：

保障服務不中斷

越世實業

設備效能比例分流



優勢說明：

設備效能比例分流

越世實業

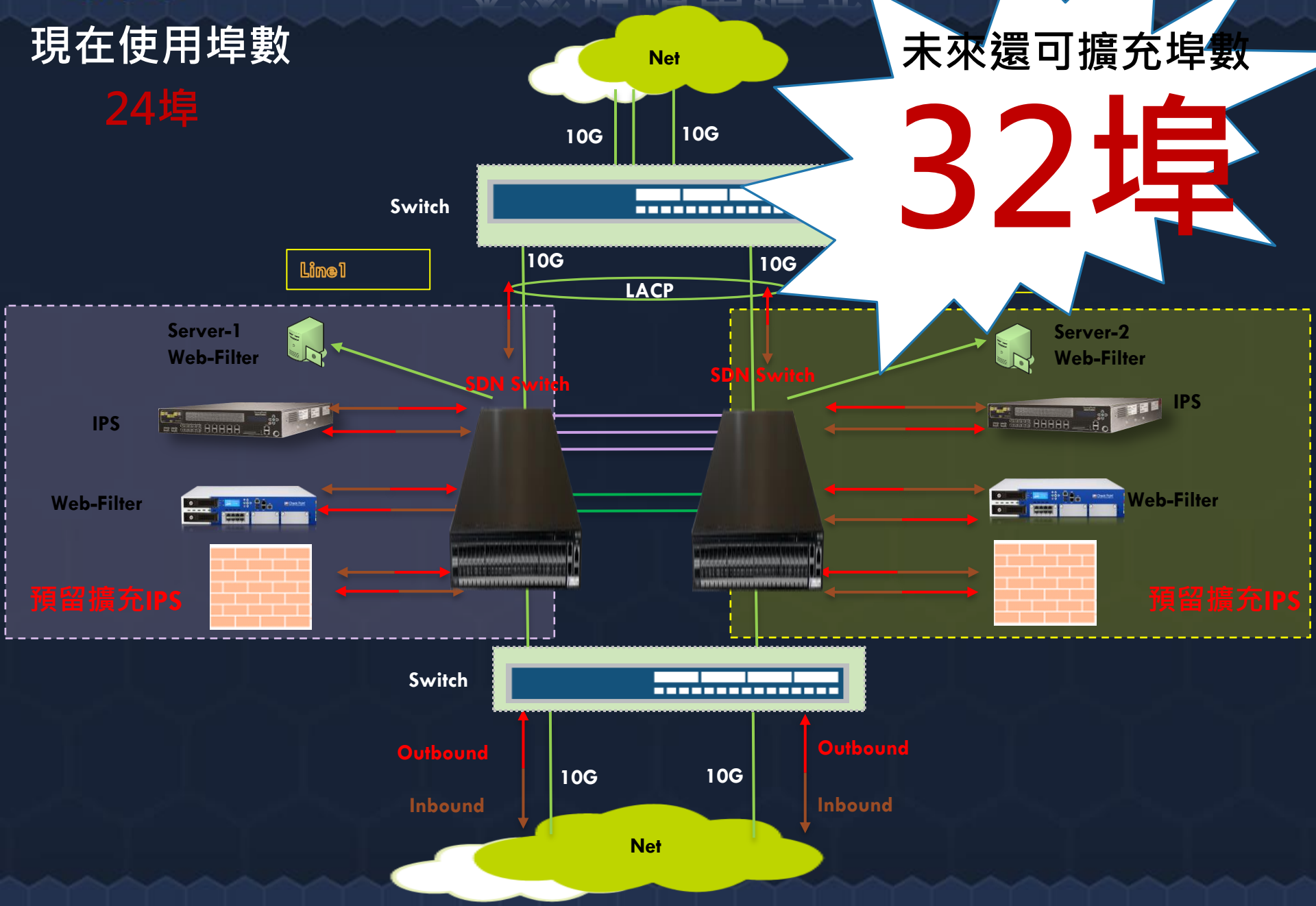
未來埠預留擴充

現在使用埠數

24埠

未來還可擴充埠數

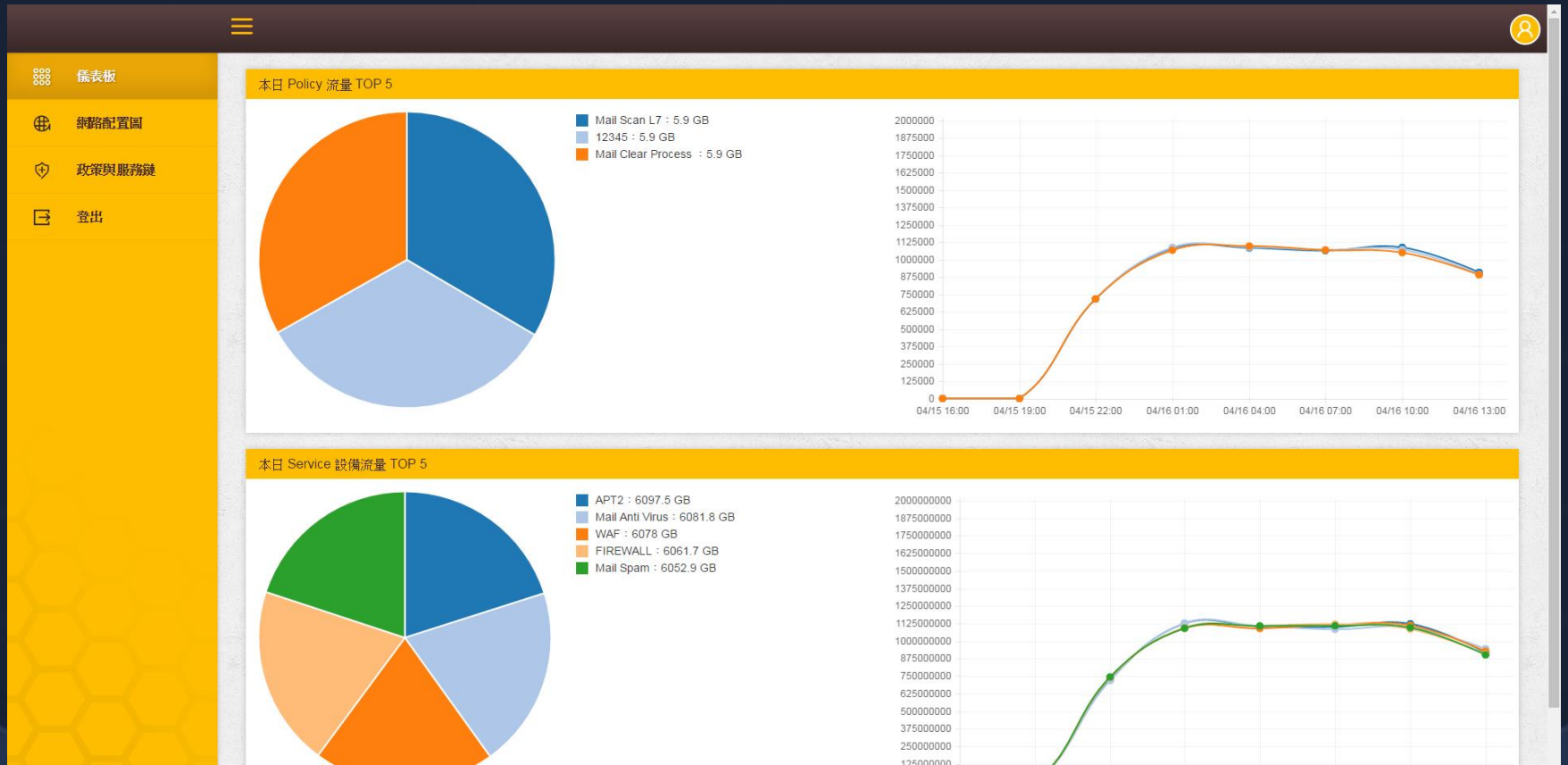
32埠



操作介面

DASHBOARD 統計 ENVIRONMENT SETTING

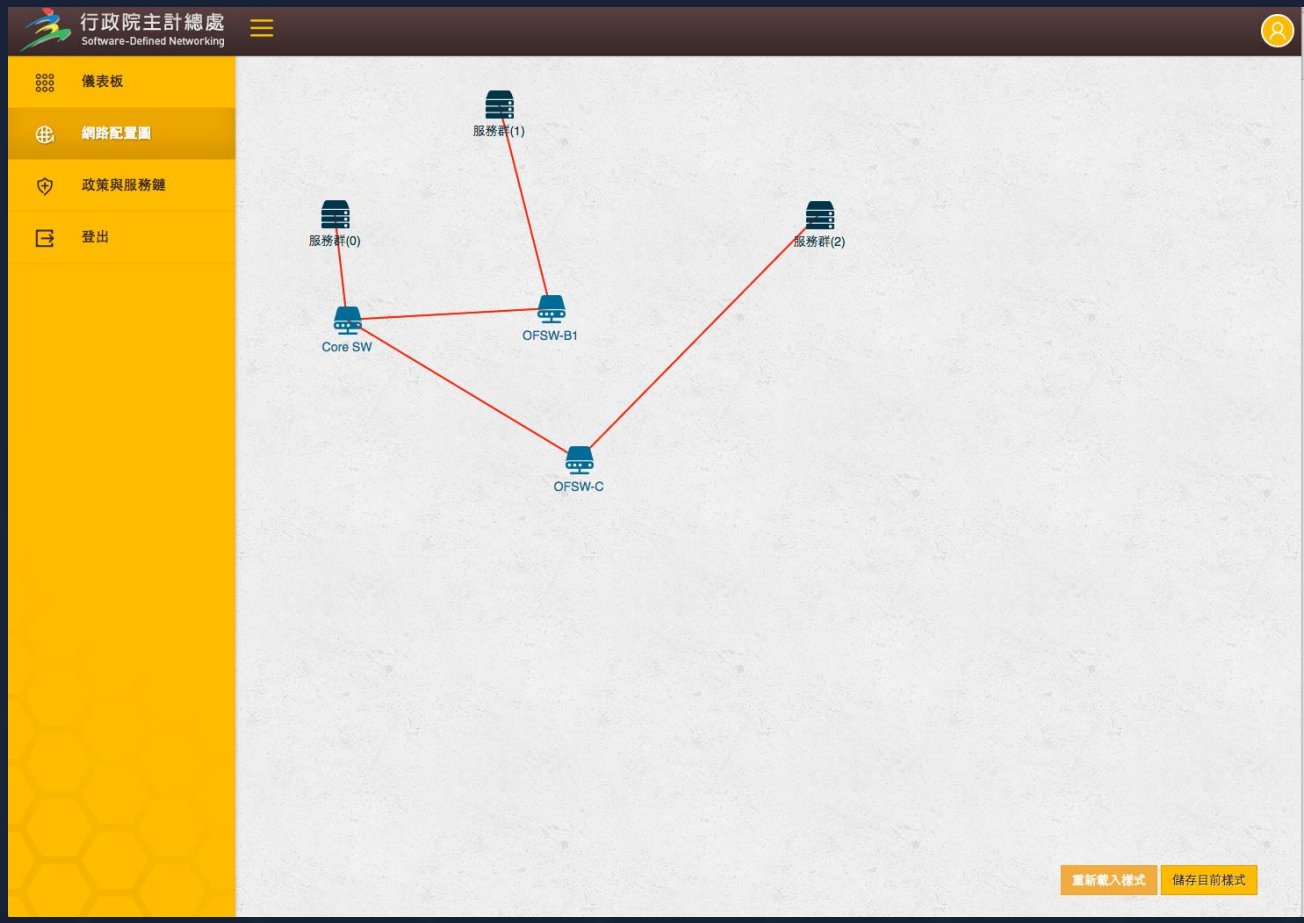
- 顯示 POLICY 流量 TOP 5
- 顯示 SERVICE 流量 TOP 5



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

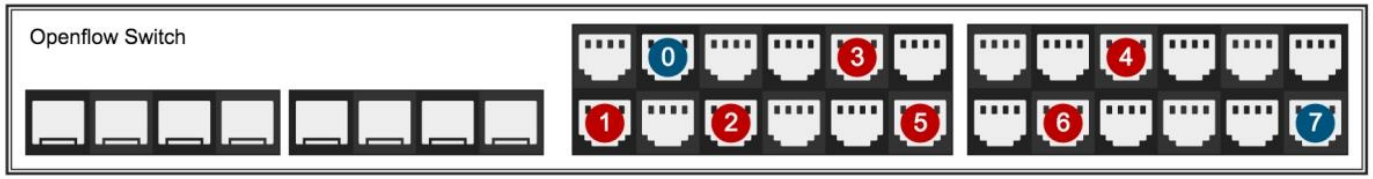
流程

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



SDN 智能分流服務鏈與市場上的分流設備的差異

- 支援整合教育部 SOC 執行資安聯防計劃
- 支援整合L7的防火牆達到資安訊息共享及聯合防禦功能
- 支援整合 AD/LDAP/Radius 達到流量與帳號對應
- 支援依資安設備/網路服務設備的capacity大小做不同流量分流
- 支援多服務連續串接功能

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

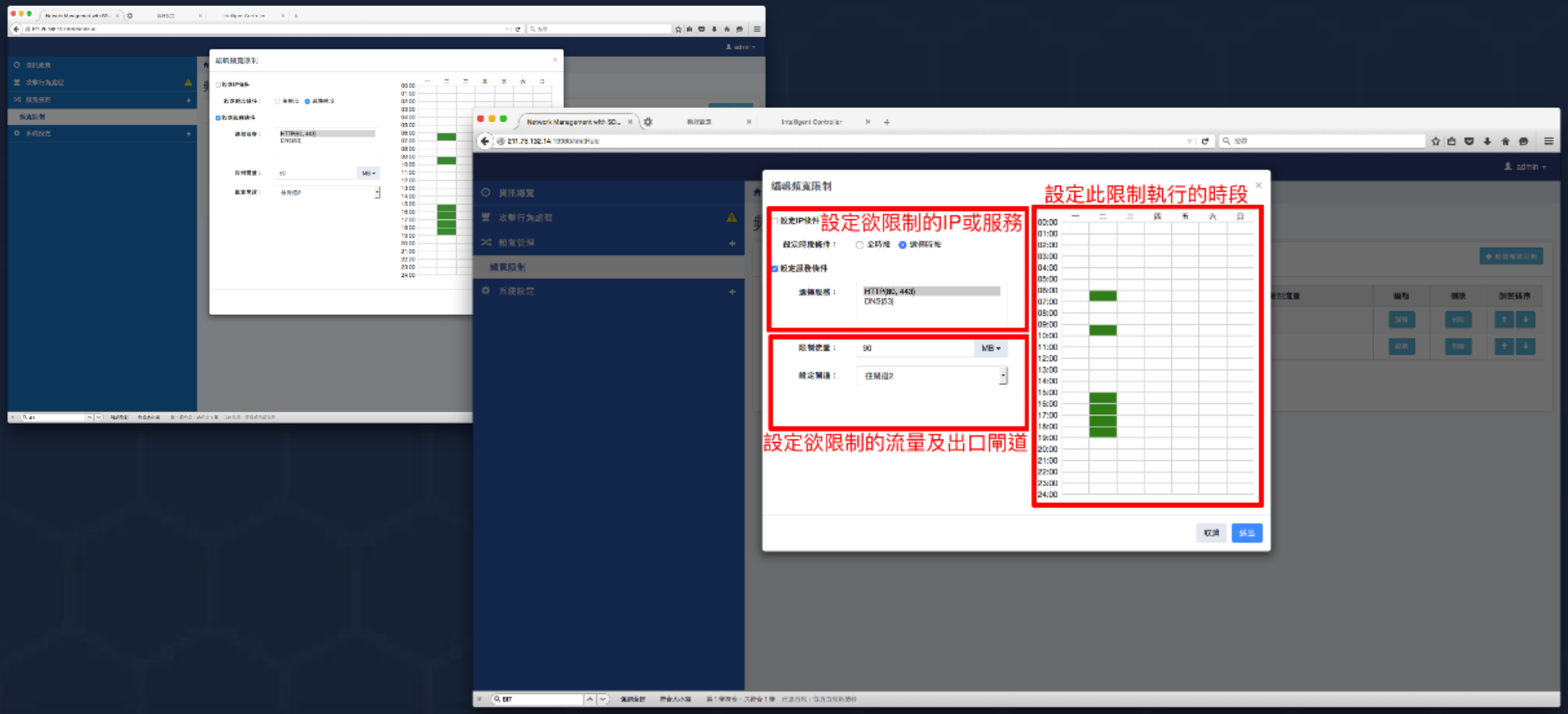
- 限制每個IP的網路使用速率，避免公用電腦被不當使用、或佔用頻寬
- 可在特定時間將特定網段的流量導入不同的閘道，製造隔離的網路環境。

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



ACCESS CONTROL存取控制

WITH SDN-OPENFLOW

適用場景

大量的員工使用網路

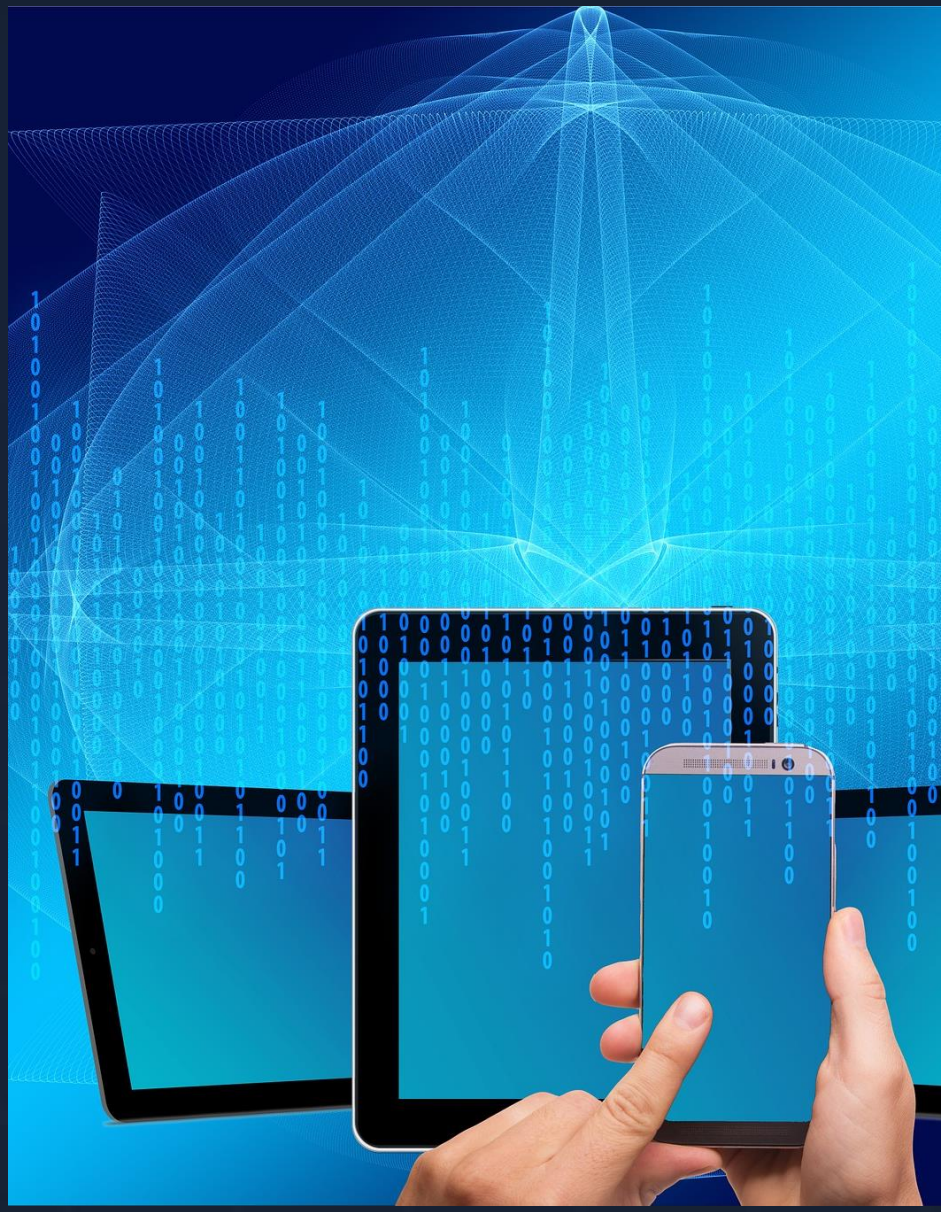
- 限制單日每個IP能夠使用的網路總流量，超過標準時則進行管理
- 限制每個網段的網路使用速率，避免小部分人員佔用大部分資源
- 檢測網路內的電腦是否疑似被殭屍網路所感染，讓該電腦的擁有者能夠在參與攻擊前進行電腦的清掃。

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

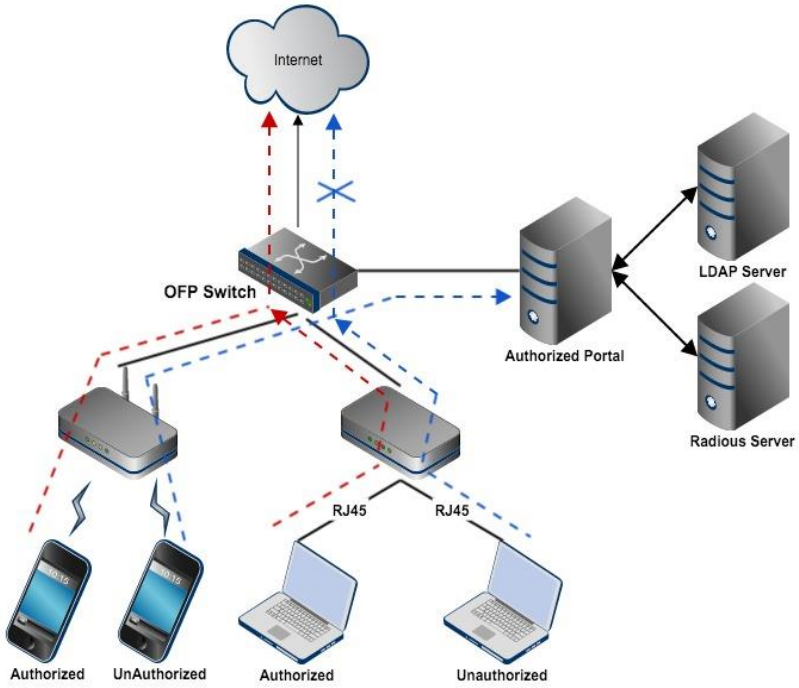
網路頻寬暴衝

IP 相衝問題



系統架構概念

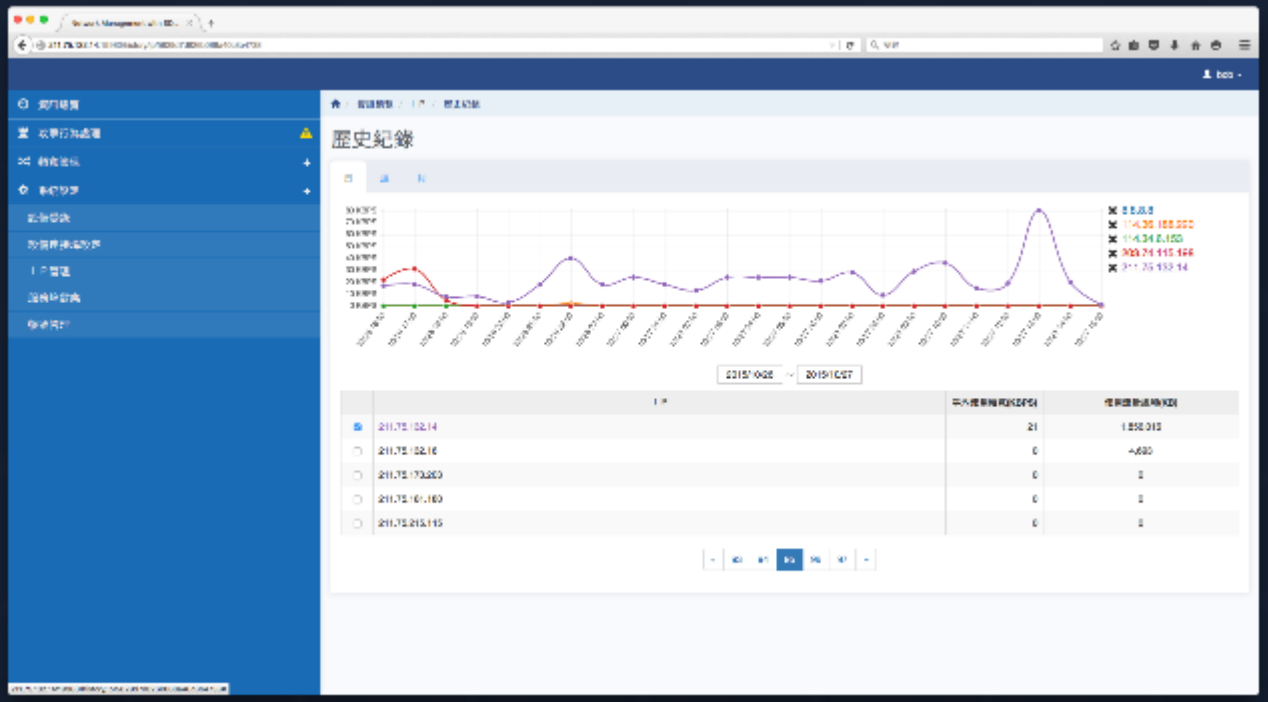
使用者分成授權(AUTHORIZED)與未授(UNAUTHORIZED)，授權者可通過OFP SWITCH連上INTERNET。而尚未通過授權之使用者則會被引導到授權頁面。



操作介面-資訊總覽

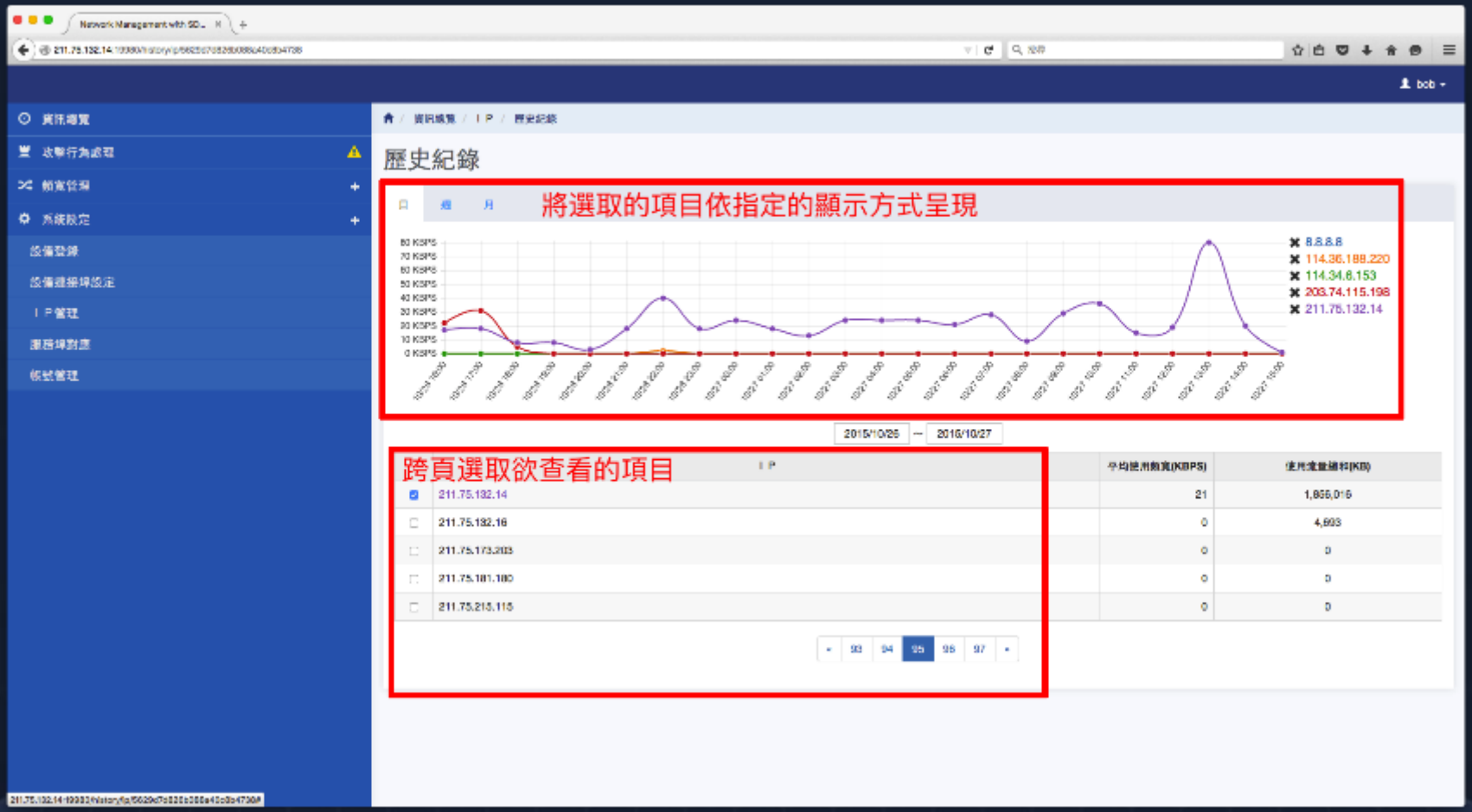
查看各種網路目前使用狀況及其歷史紀錄

- 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

SMART LOAD BALANCE智慧路由

WITH SDN-OPENFLOW

SMART LOAD BALANCE 智慧路由

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。

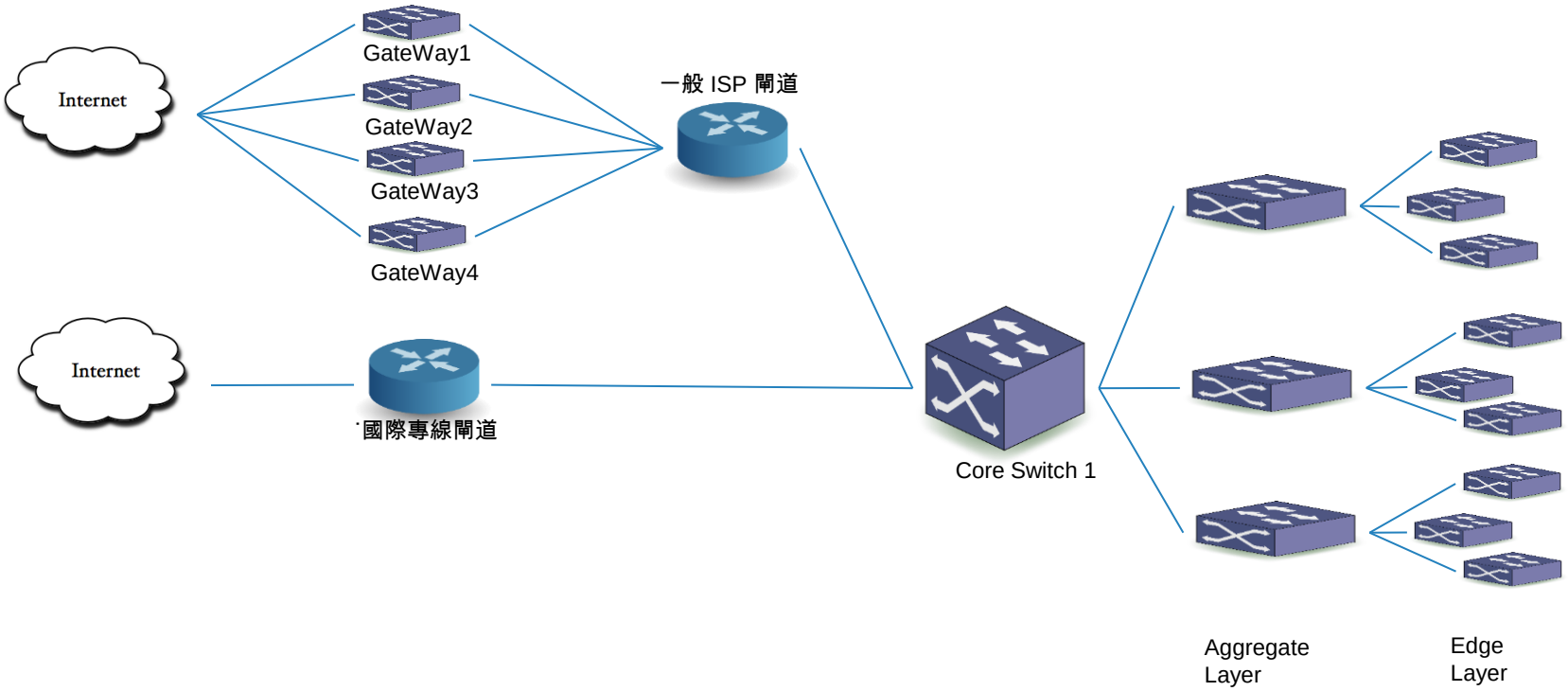
需要能管理能使用網路的帳號

- 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

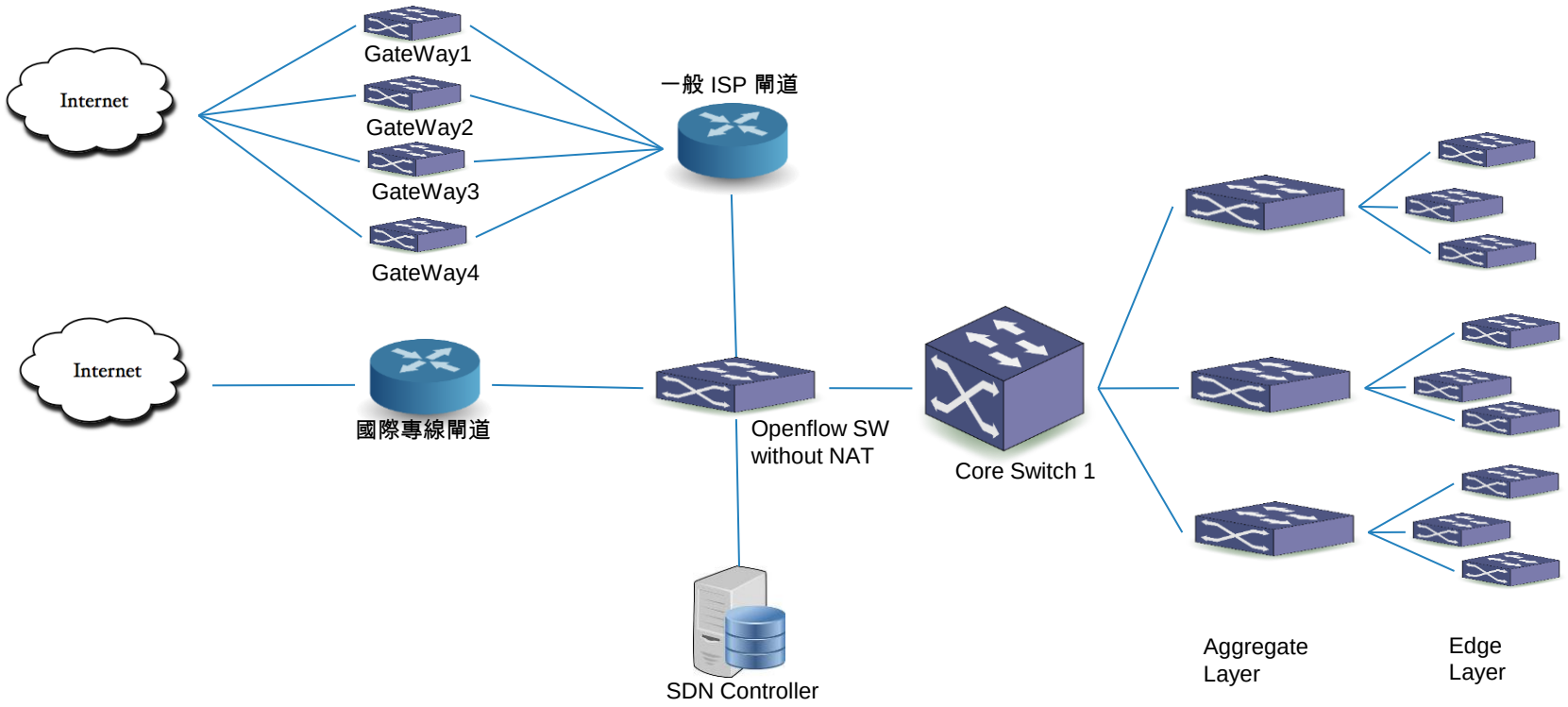
網路頻寬暴衝

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。

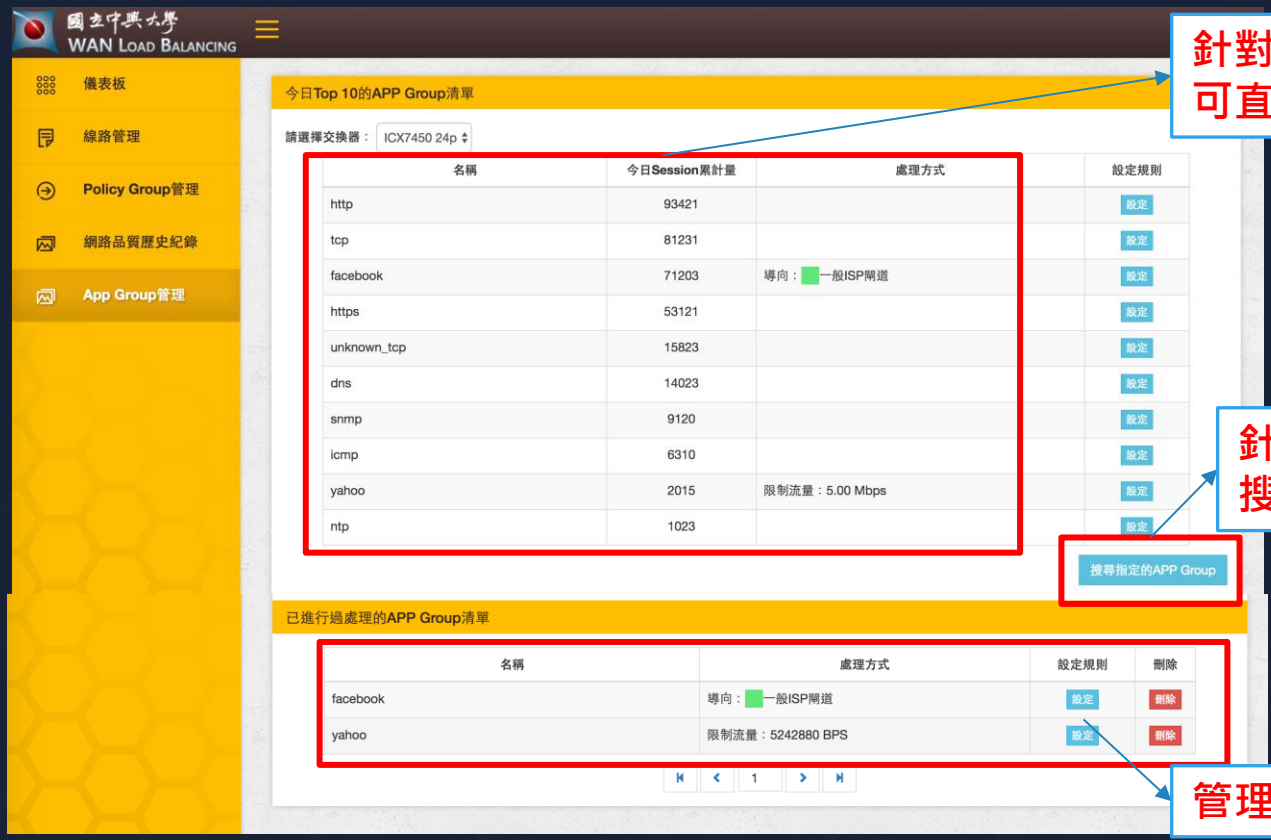
操作介面

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

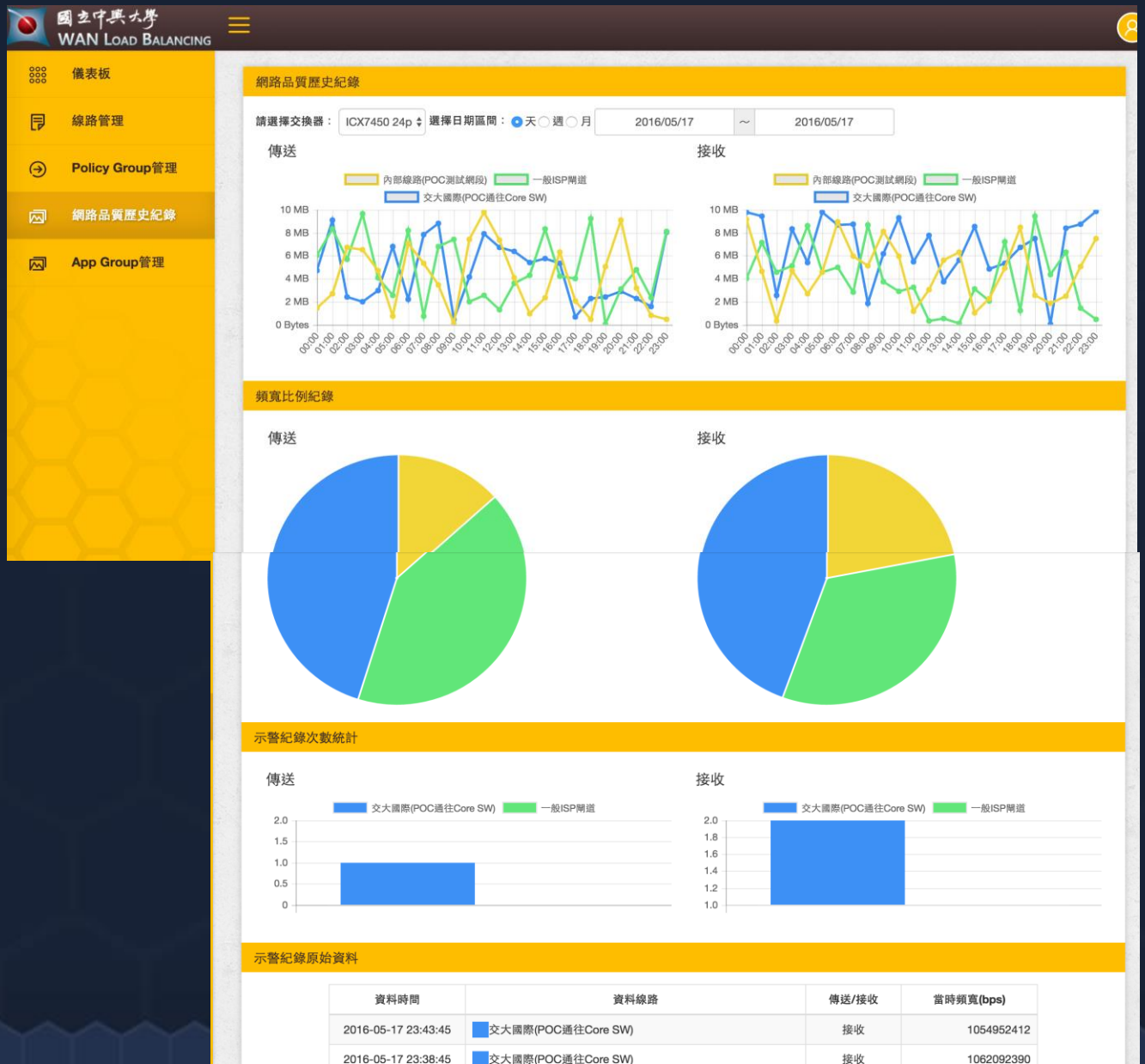
儀表板


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閒道
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



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。

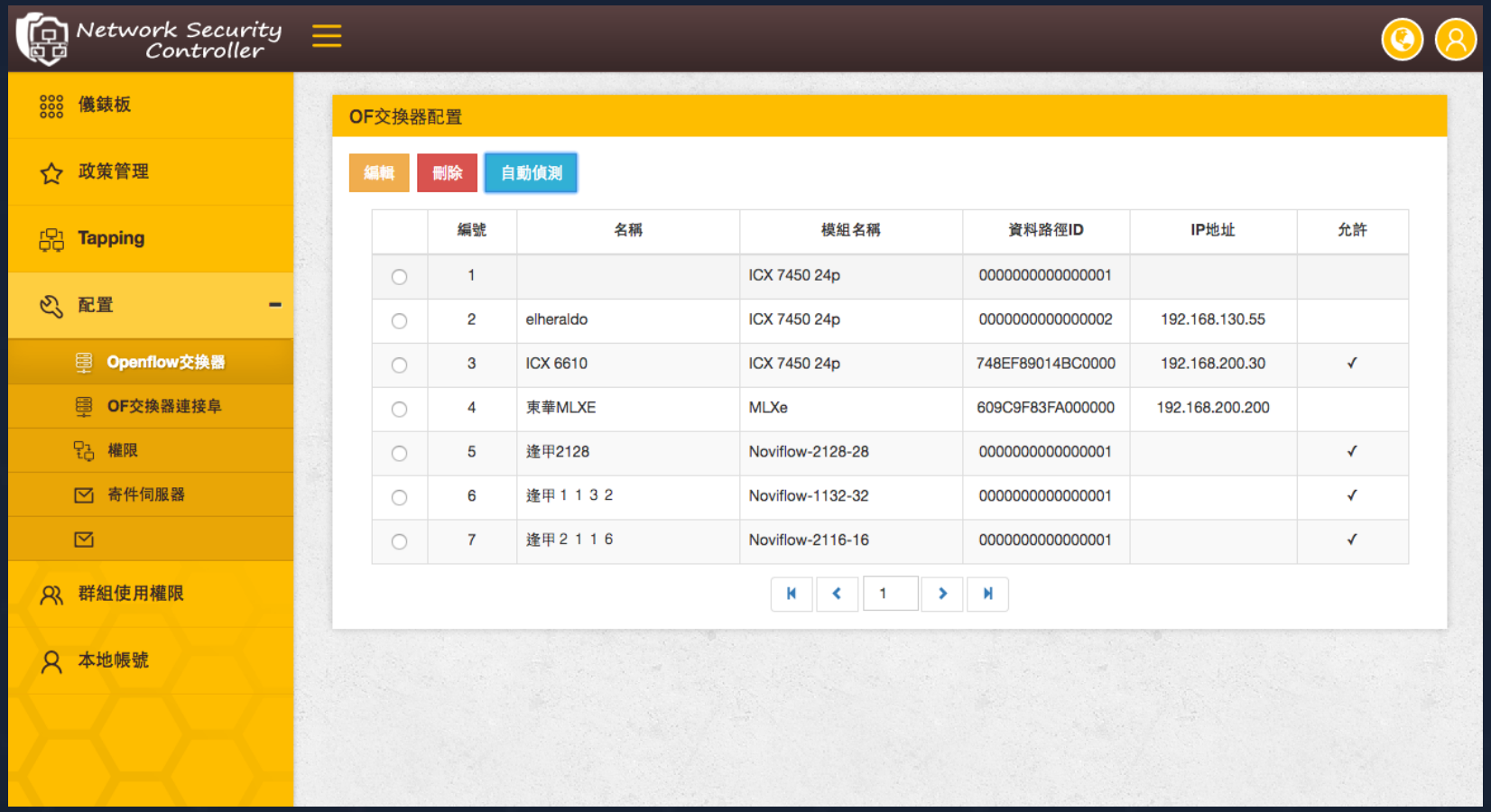
網路流量因不同需要必須增加額外條件

- 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

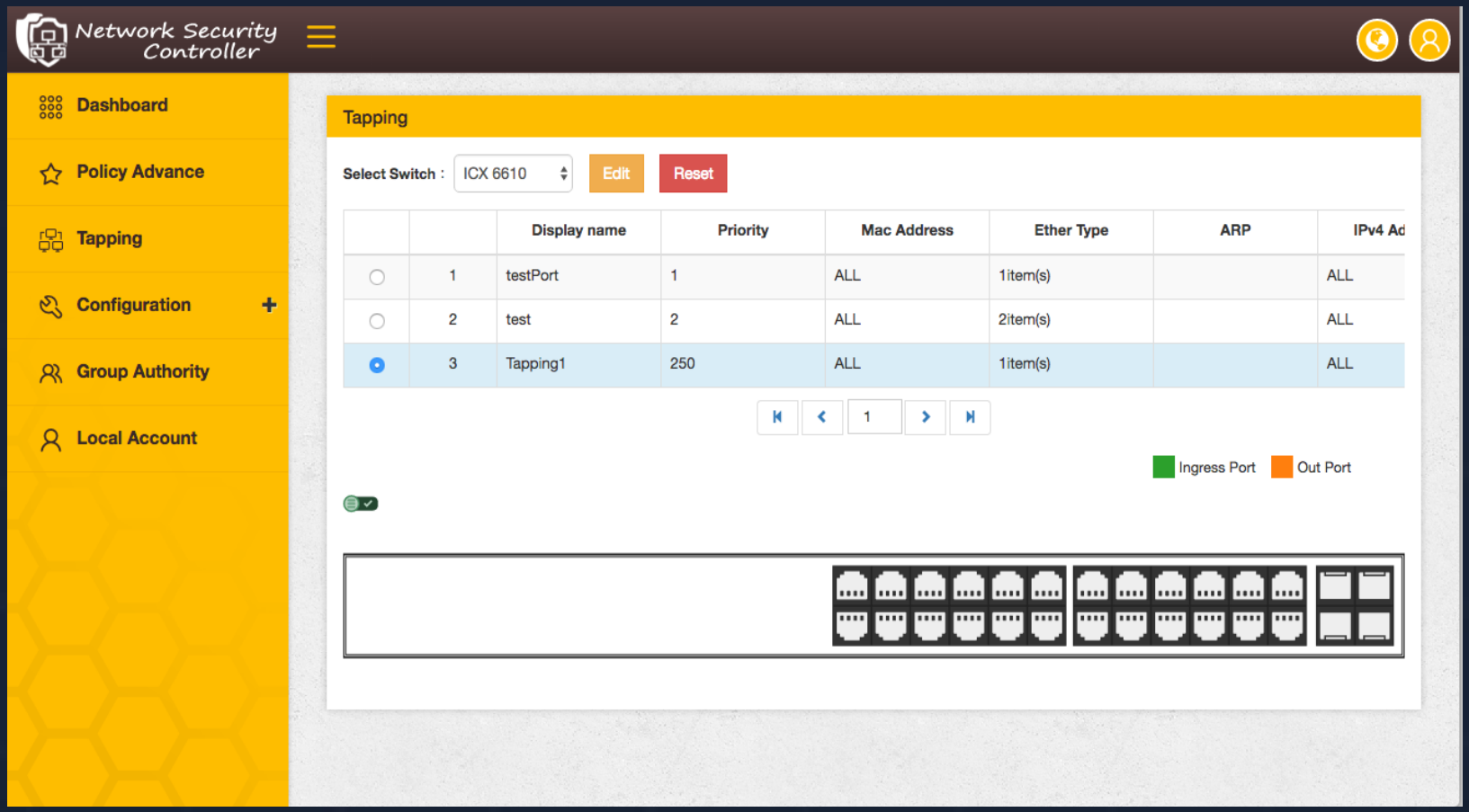
操作介面

SWITCH CONFIG



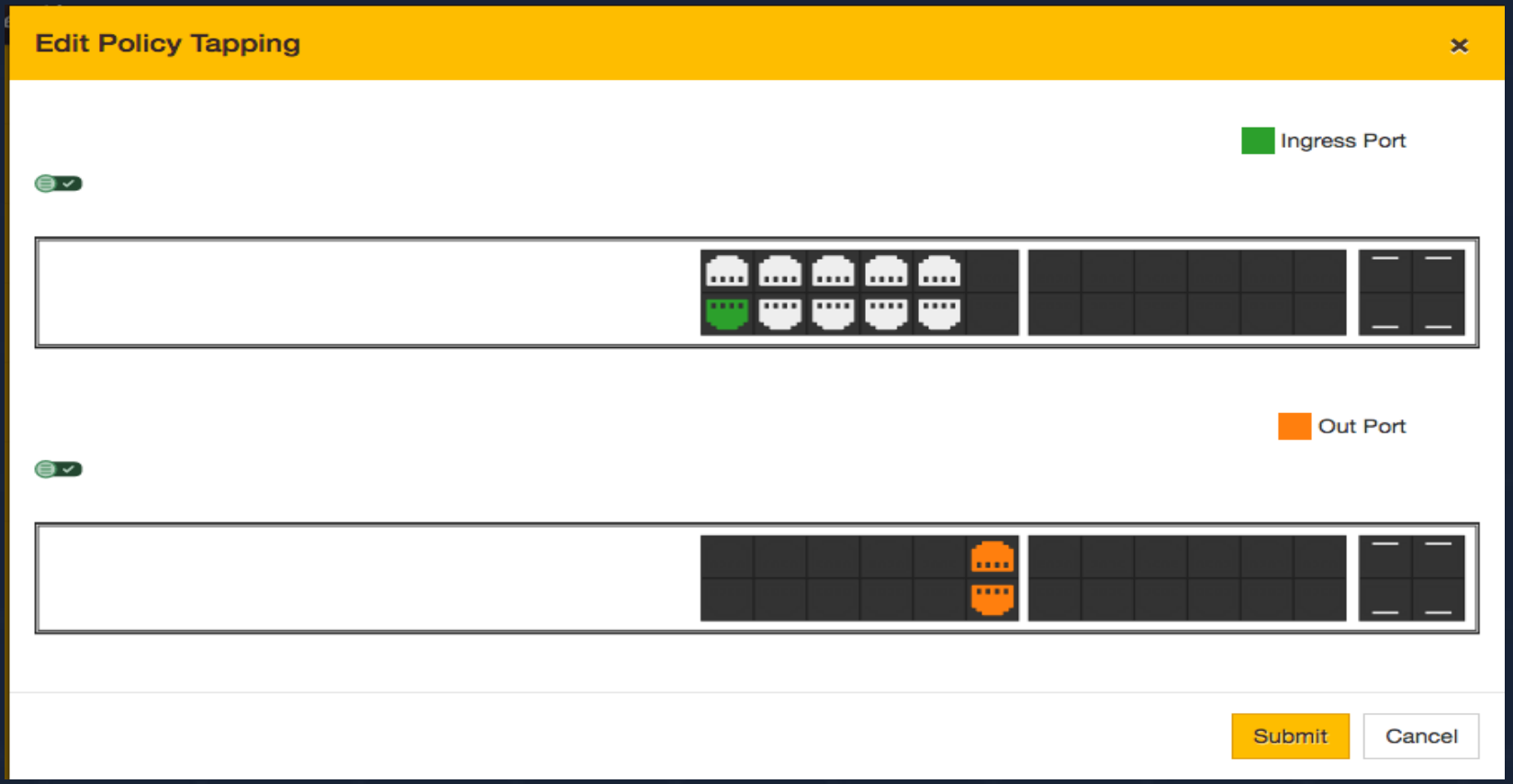
操作介面

TAPPING RULES CONFIG



操作介面

TAPPING RULES CONFIG



越世實業

Q & A

越世實業

THANK YOU