



# 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<sup>1</sup> cost saving compared to manual tapping tools
- No onsite technician for troubleshooting

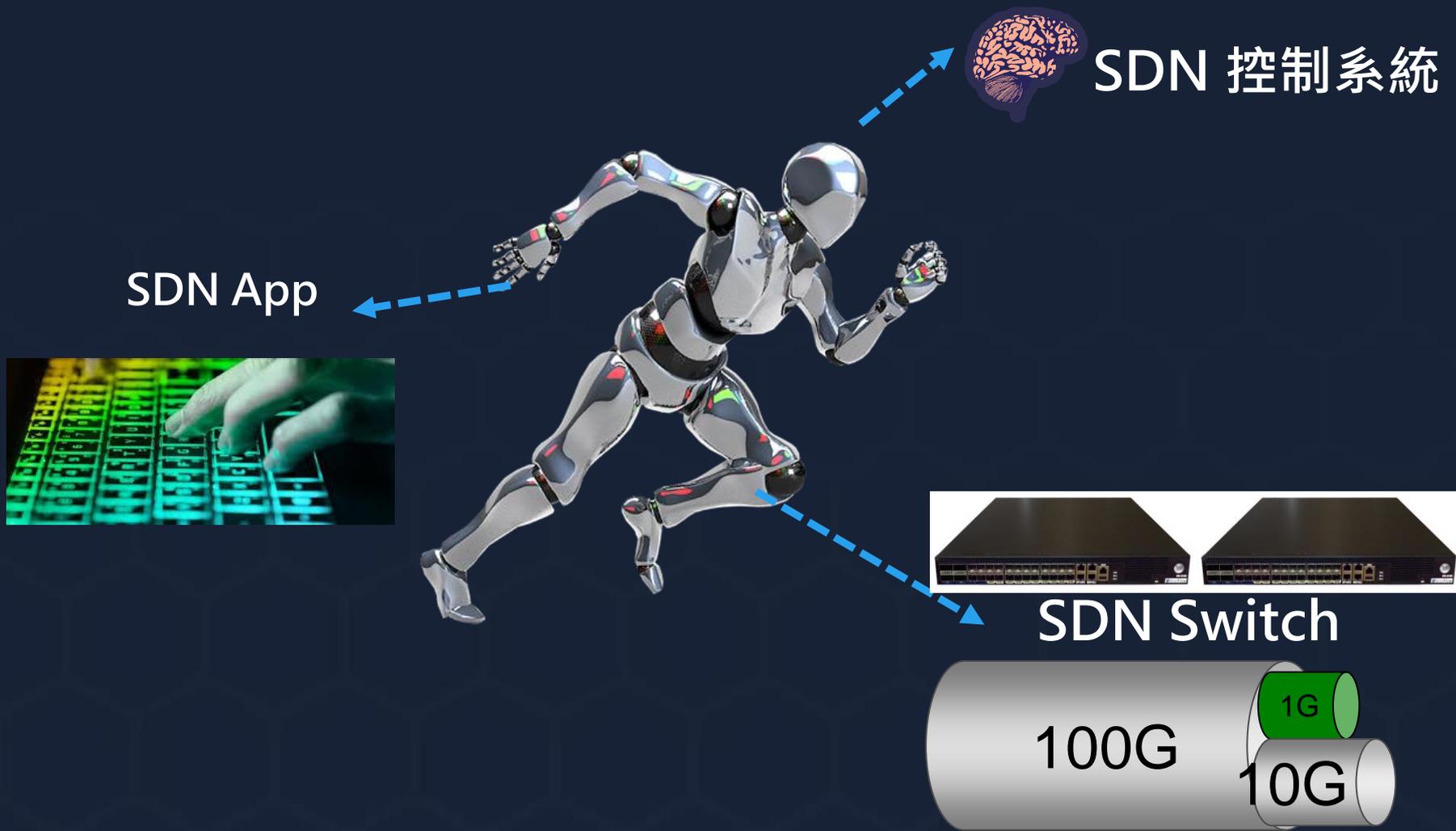
## SDN Network Defense Different

### 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



各種異常狀態的Log



### 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 I2-I4 / protocol / user id(must integrated with ad server) / application (must integrated with dpi devices).

### Smart load balance function

- Each I2-I4 / 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

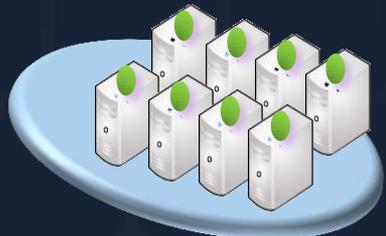


Service Chain 是分流系統  
也是完整 SDN Controller

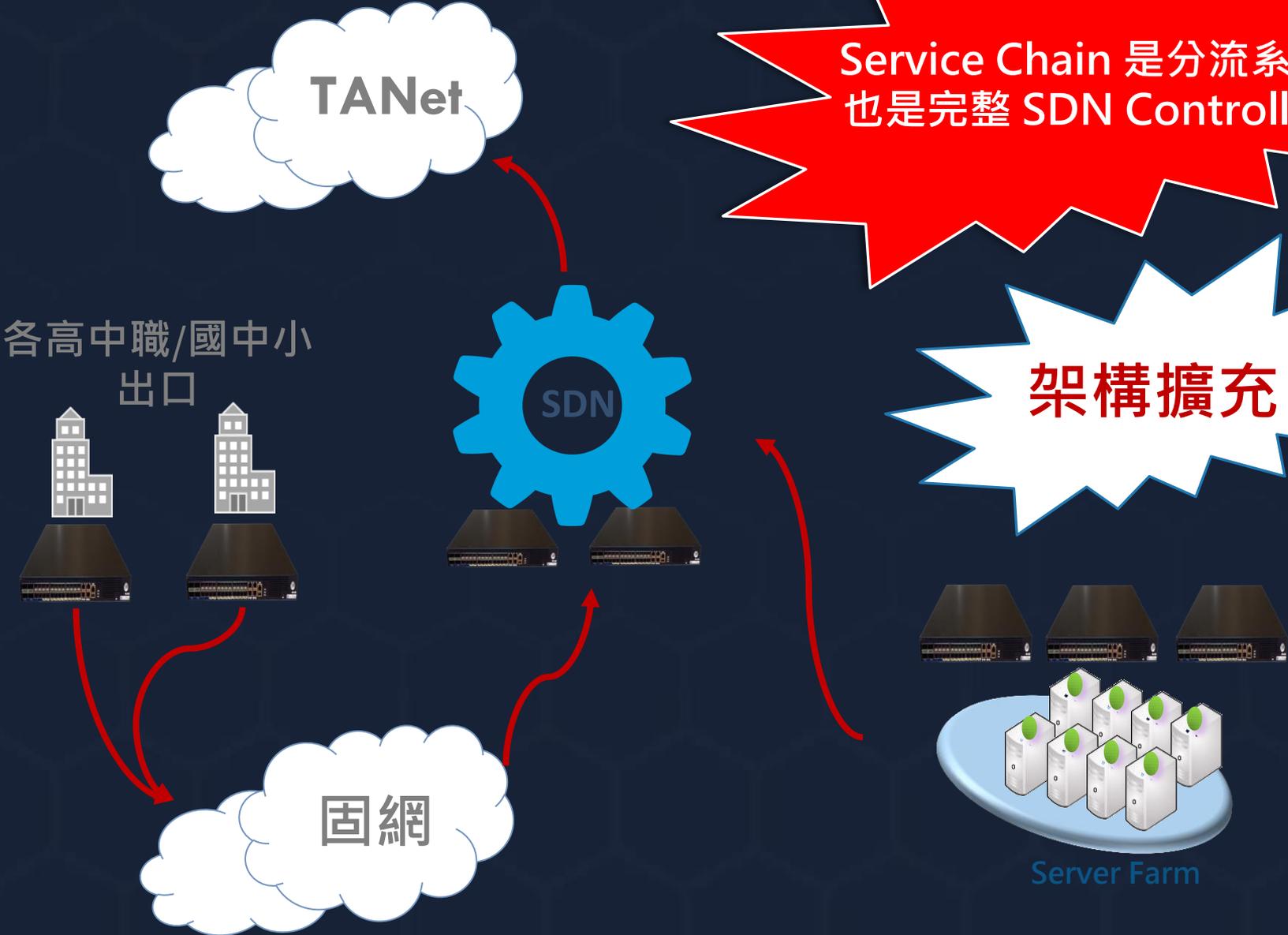
各高中職/國中小  
出口



架構擴充



Server Farm



# SDN 控制系統



## 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



智慧分流系統



功能擴充

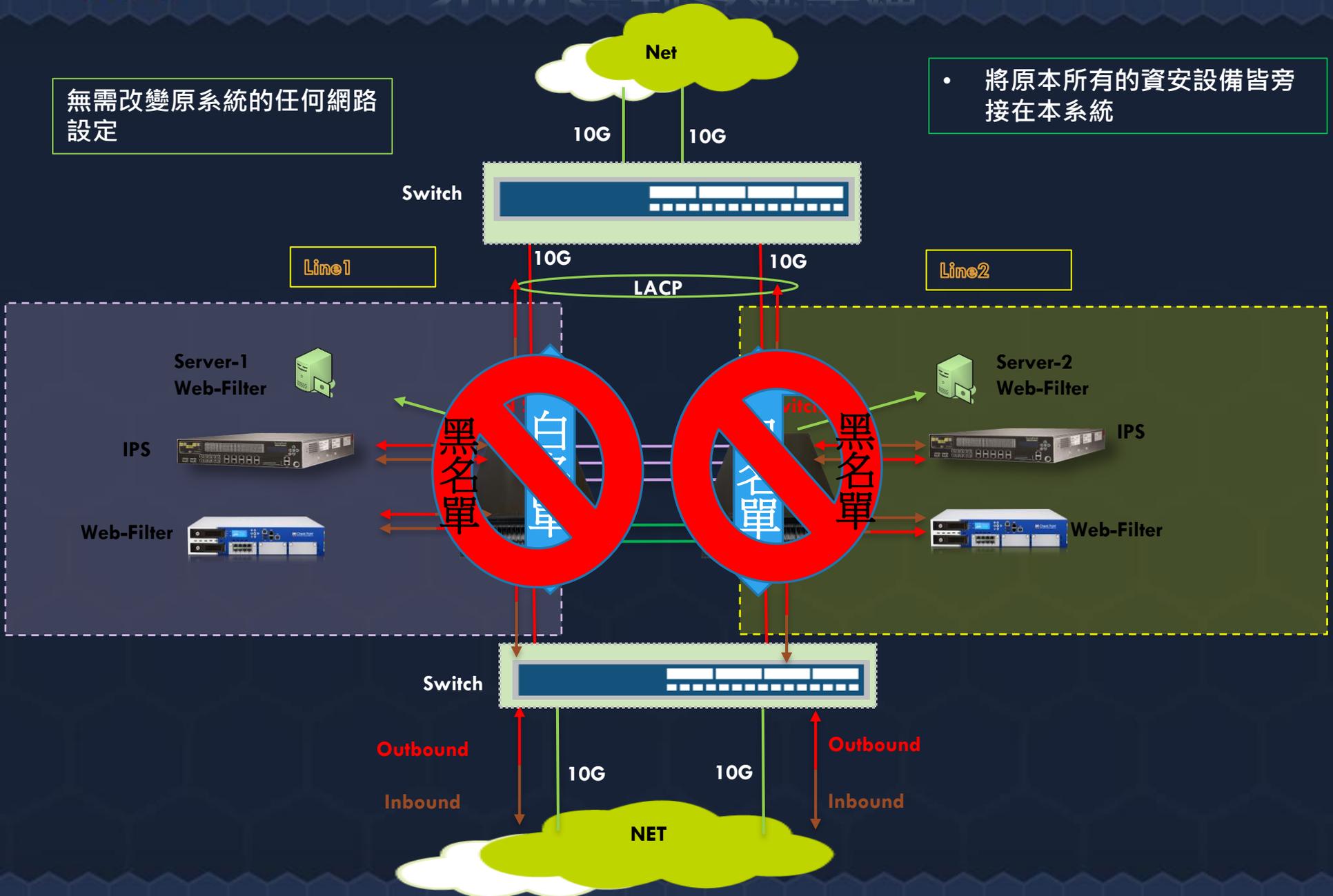
開放

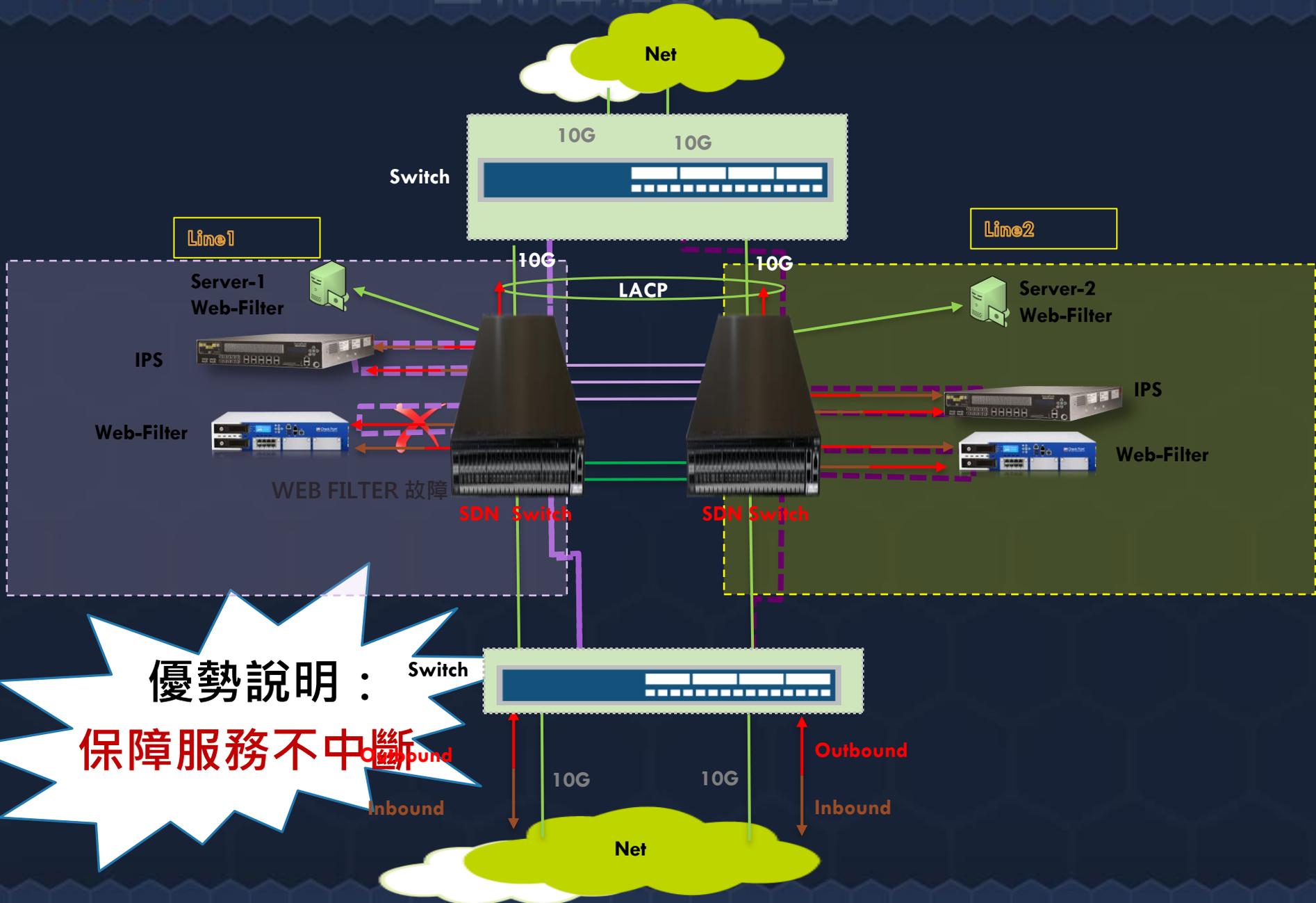
彈性

標準

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



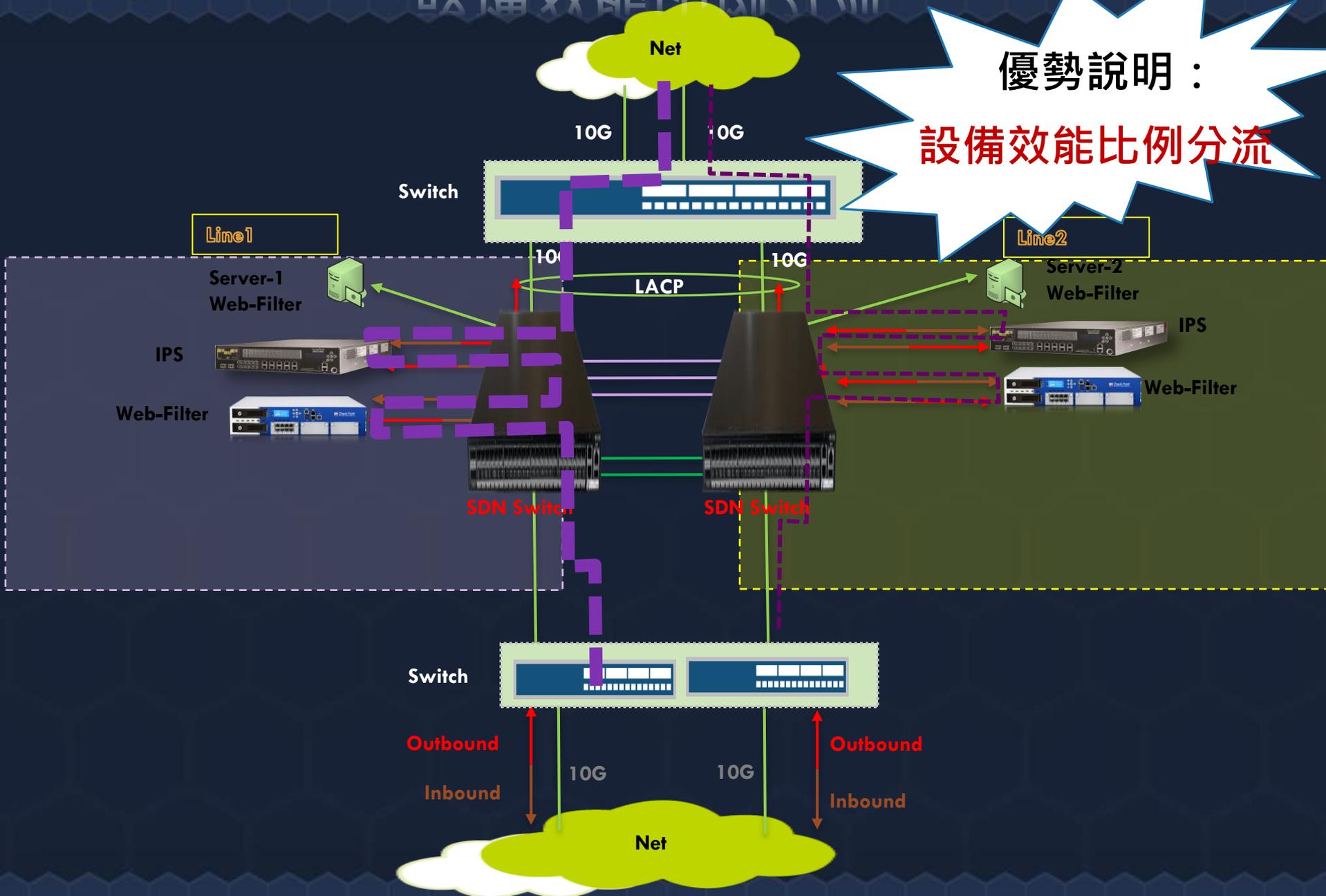


優勢說明：

保障服務不中斷

# 設備效能比例分流

優勢說明：  
設備效能比例分流



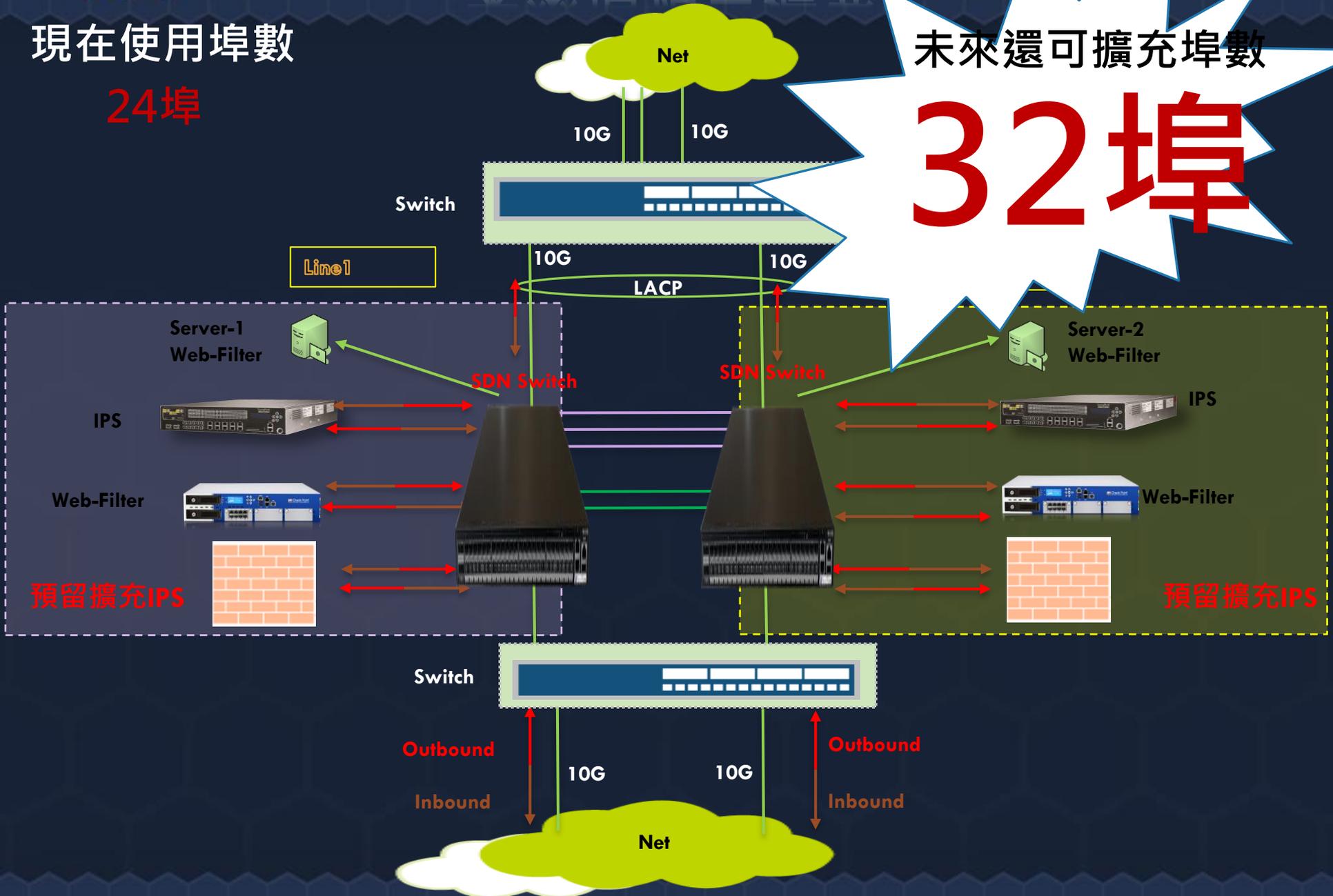
# 未來埠預留擴充

現在使用埠數

24埠

未來還可擴充埠數

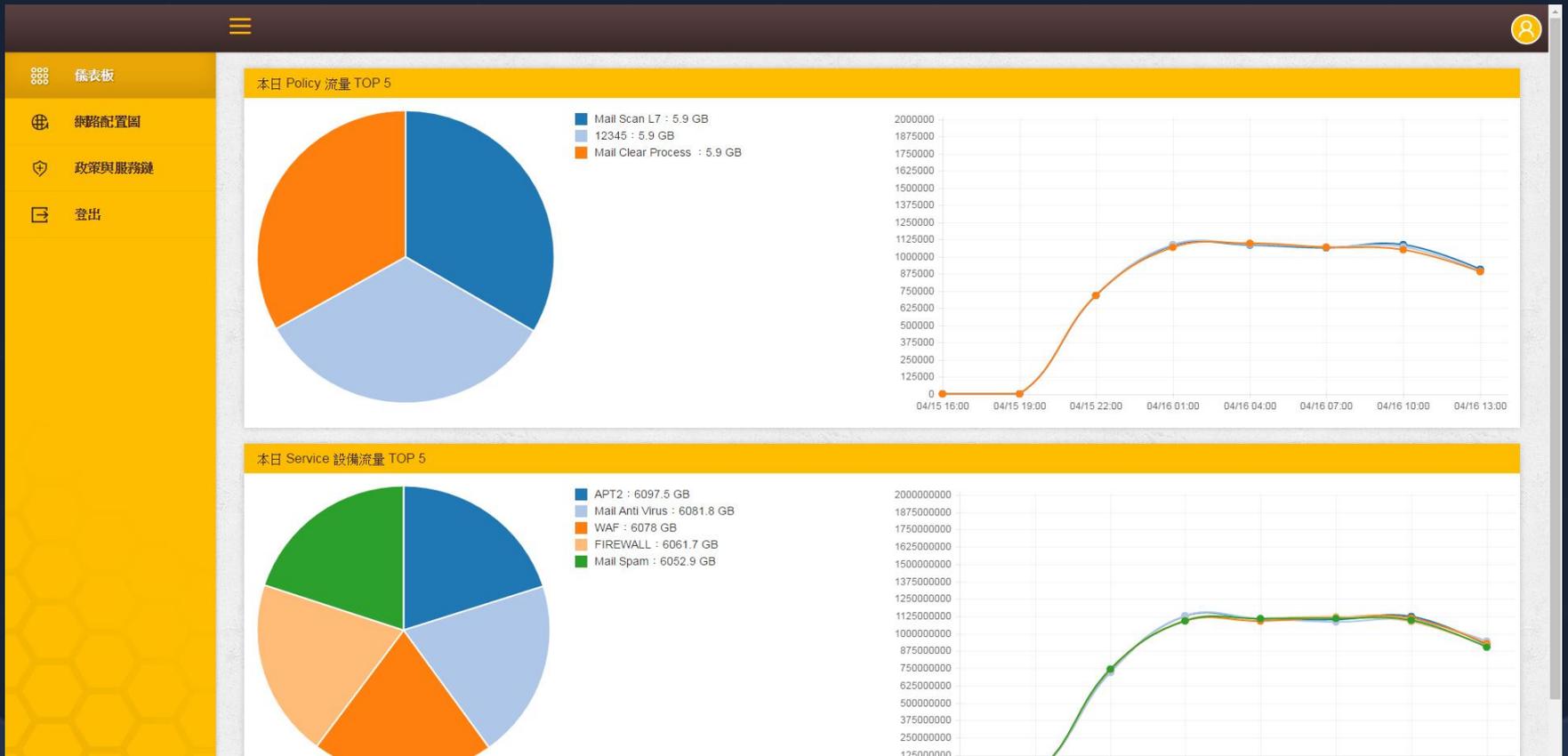
# 32埠



## 操作介面

### DASHBOARD 統計 ENVIRONMENT SETTING

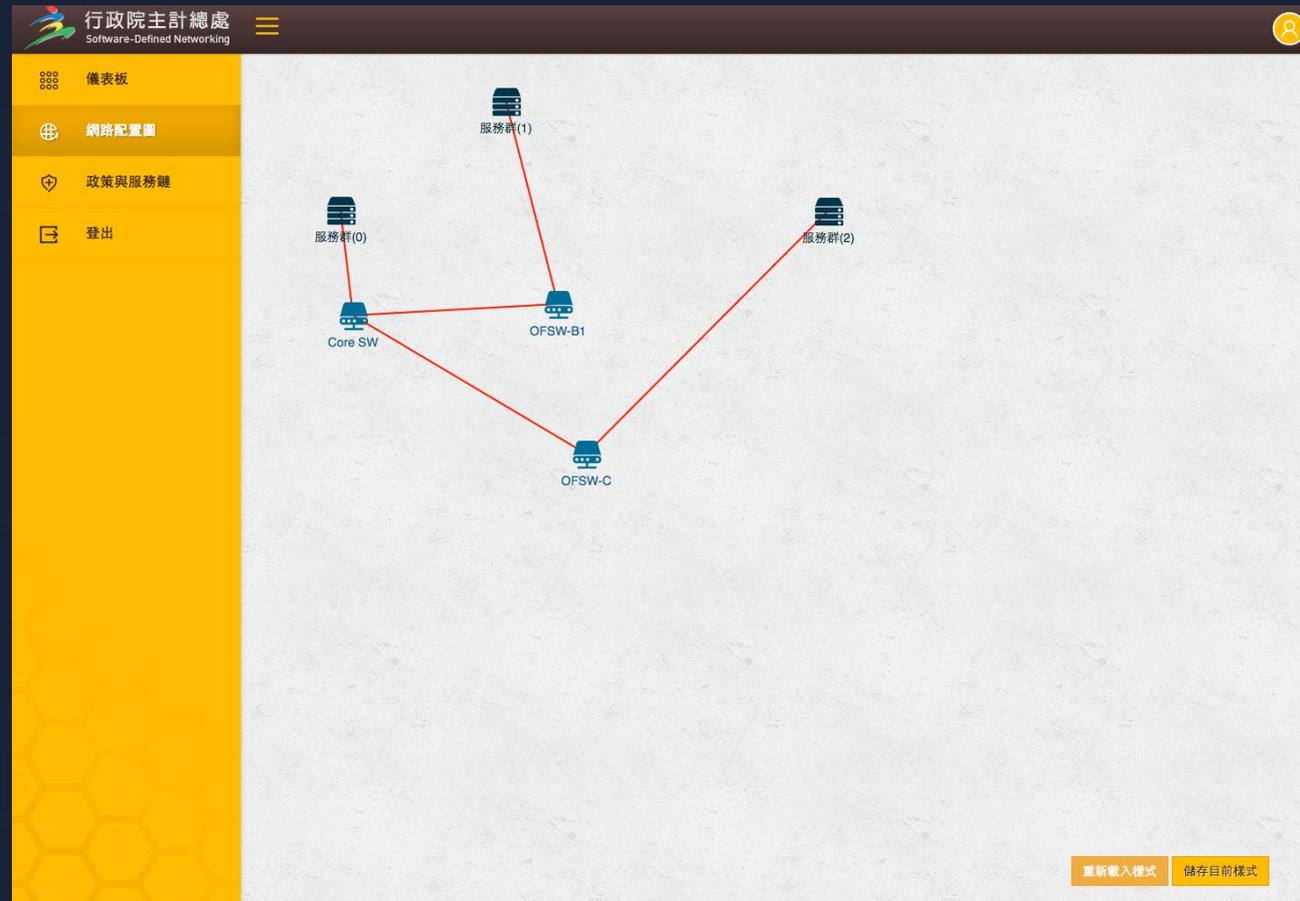
- 顯示 POLICY 流量 TOP 5
- 顯示 SERVICE 流量 TOP 5



# 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
<input type="checkbox"/>	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
<input checked="" type="checkbox"/>	Mail Scan	Mail Scan Servie Chain	Port 3	Port 24	不限定	不限定	不限定	不限定	100
<input type="checkbox"/>	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



## 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。

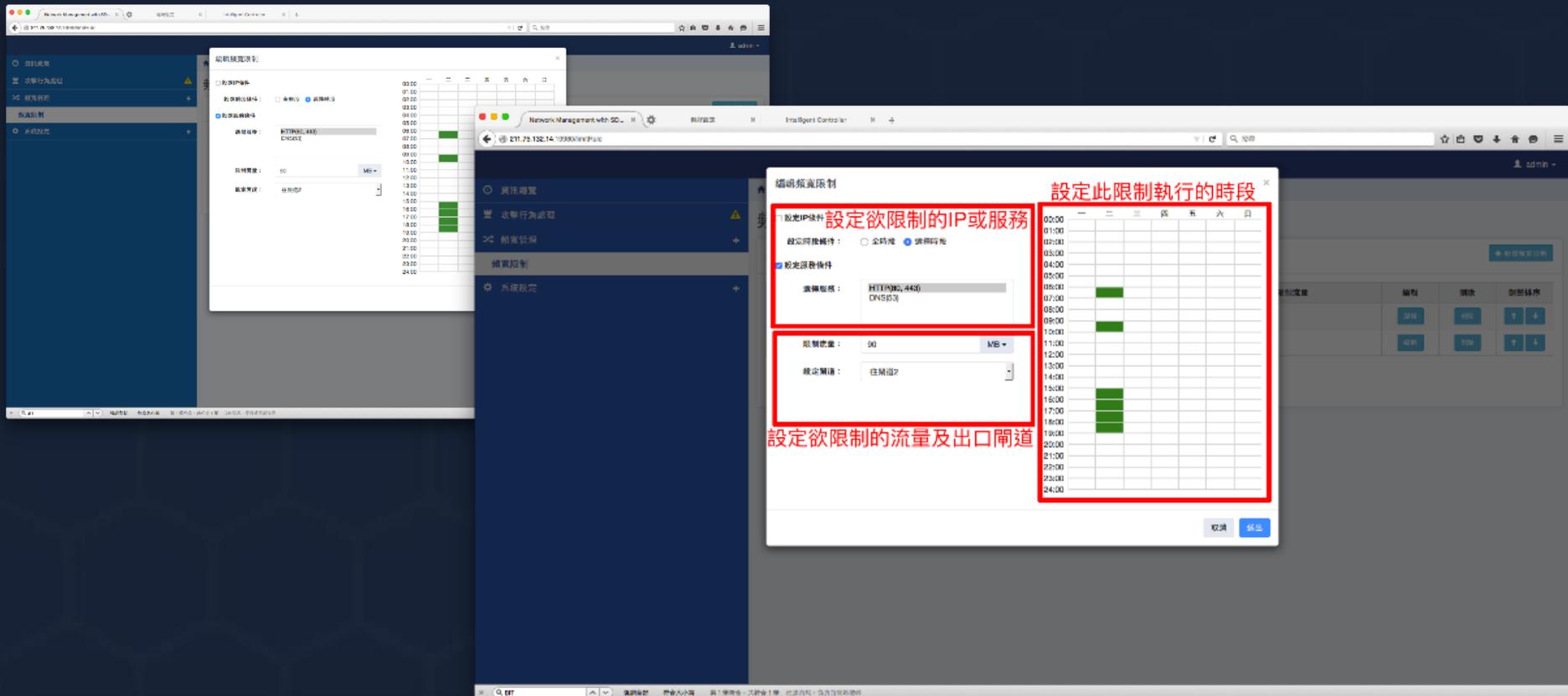
### 服務品質管理

- 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



The screenshot displays the 'Intelligent Controller' interface for Network Management v10.50.14. It shows a configuration window for '細則流量限制' (Detailed Traffic Limitation) with a calendar view. A red box highlights the '設定此限制執行的時段' (Set the time period for this restriction) section, which includes a calendar grid. Another red box highlights the '設定欲限制的IP或服務' (Set the IP or service to be restricted) section, which includes fields for '選擇條件' (Select conditions) and '限制數量' (Limit quantity). A third red box highlights the '設定欲限制的流量及出口閘道' (Set the traffic and egress gateway to be restricted) section, which includes fields for '限制數量' (Limit quantity) and '指定閘道' (Specify gateway).

細則流量限制

設定此限制執行的時段

設定欲限制的IP或服務

設定欲限制的流量及出口閘道

# ACCESS CONTROL存取控制

WITH SDN-OPENFLOW

## 適用場景

### 大量的員工使用網路

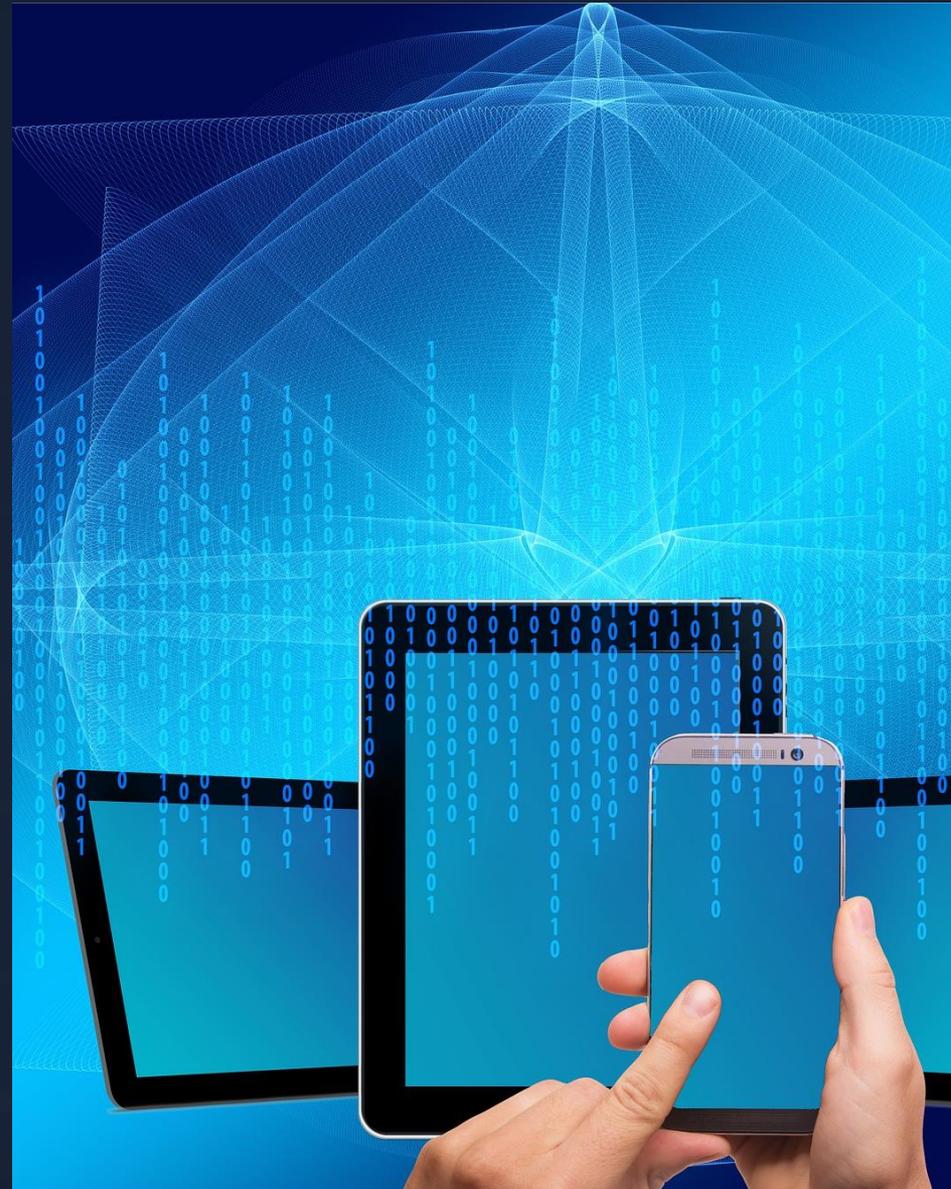
- 限制單日每個IP能夠使用的網路總流量，超過標準時則進行管理
- 限制每個網段的網路使用速率，避免小部分人員佔用大部分資源
- 檢測網路內的電腦是否疑似被殭屍網路所感染，讓該電腦的擁有者能夠在參與攻擊前進行電腦的清掃。

### 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

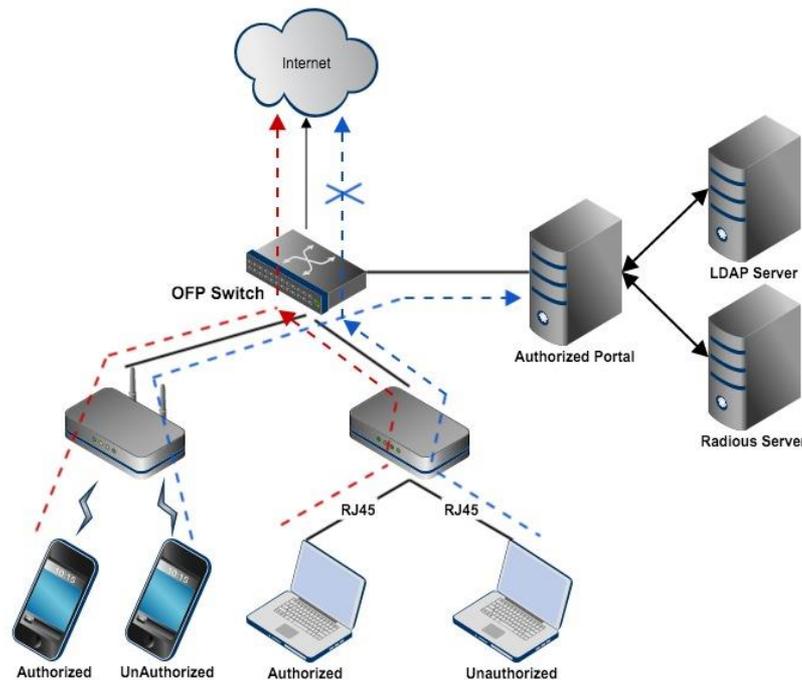
### 網路頻寬暴衝

### IP 相衝問題



## 系統架構概念

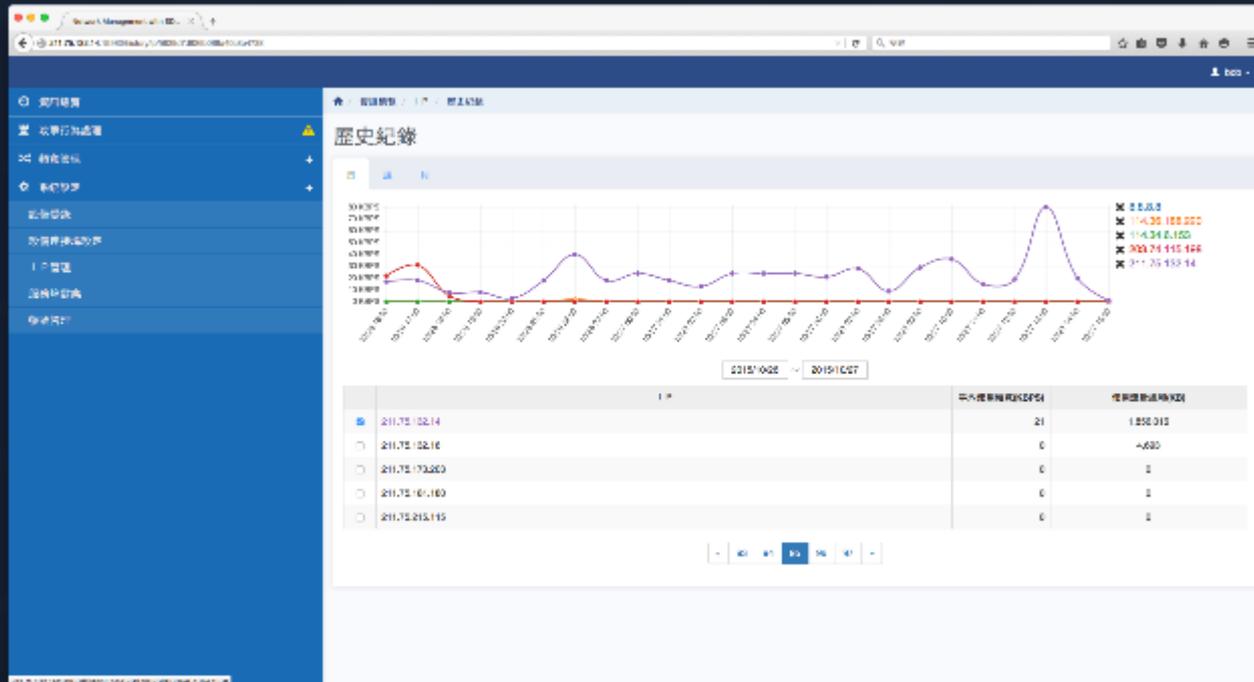
使用者分成授權(AUTHORIZED)與未授(UNAUTHORIZED)，授權者可通過OFP SWITCH連上INTERNET。而尚未通過授權之使用者則會被引導到授權頁面。



## 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**

將選取的项目依指定的顯示方式呈現

2015/10/25 - 2016/10/27

**跨頁選取欲查看的项目**

IP	平均使用數量(KBPS)	使用電量總和(KB)
<input checked="" type="checkbox"/> 211.75.132.14	21	1,856,016
<input type="checkbox"/> 211.75.132.16	0	4,693
<input type="checkbox"/> 211.75.173.203	0	0
<input type="checkbox"/> 211.75.101.100	0	0
<input type="checkbox"/> 211.75.215.115	0	0

Legend for chart:

- 8.8.8.8
- 114.36.188.220
- 114.34.8.153
- 203.74.115.198
- 211.75.132.14

# 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

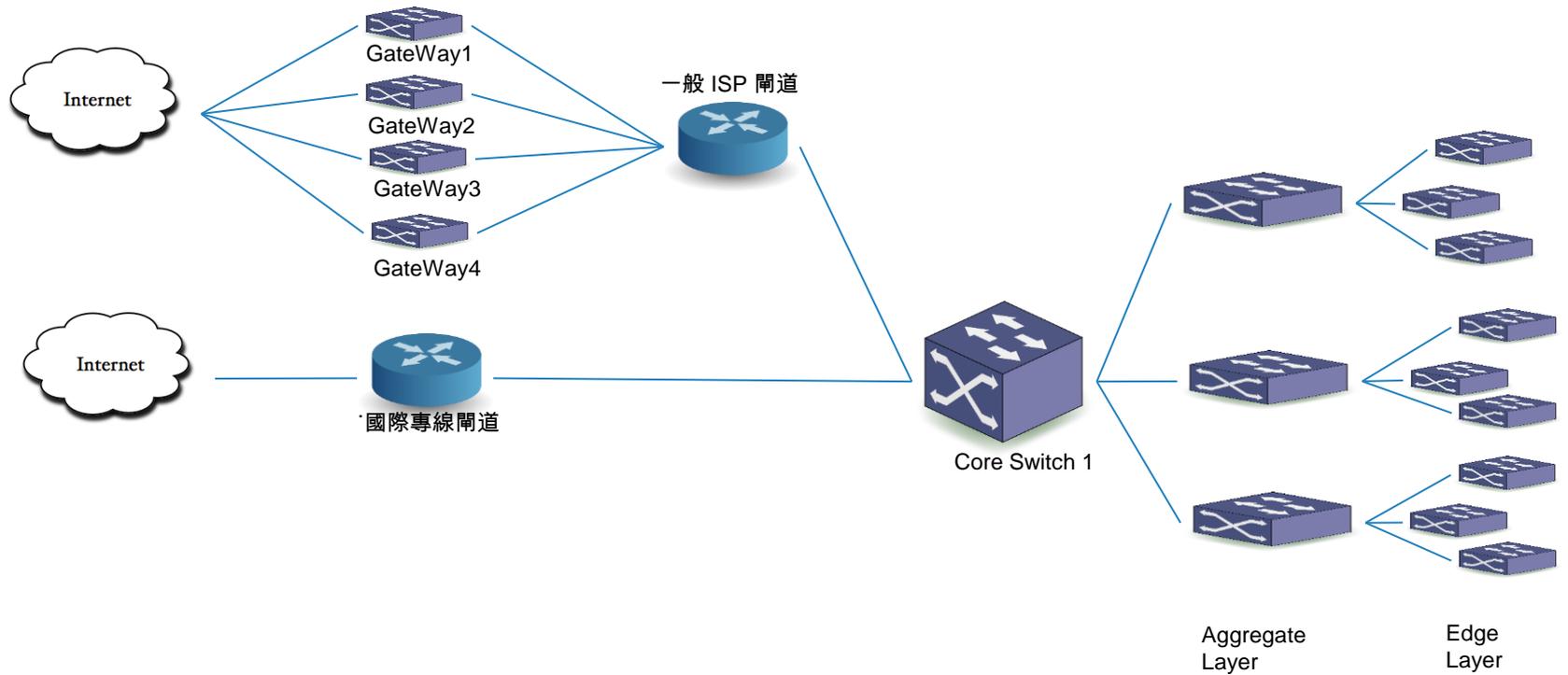
- 固定會有服務人員會一直在處理員工不同裝置要使用學校網路
- 限制每個IP的網路使用速率，避免公用電腦被不當使用、或佔用頻寬
- 可在特定時間將特定網段的流量導入不同的閘道，製造隔離的網路環境，供研發能夠切換成欲使用的開發環境

### 網路頻寬暴衝

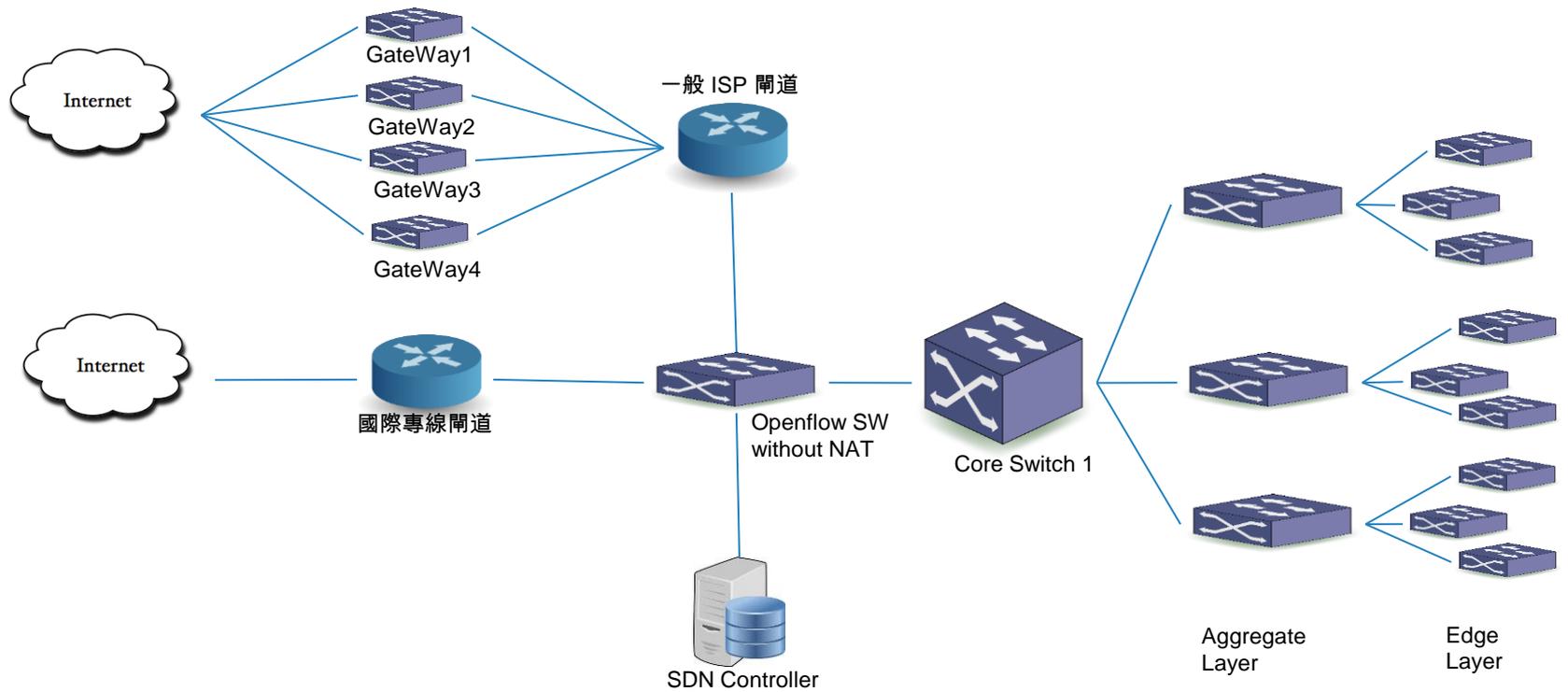
### IP 相衝問題



## 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。



The screenshot shows the 'WAN LOAD BALANCING' management interface. The left sidebar contains navigation options: 儀表板, 線路管理, Policy Group管理, 網路品質歷史紀錄, and App Group管理. The main content area is titled '線路管理' and includes a dropdown menu for '請選擇交換器: ICX7450 24p'. Below this is a visual representation of a switch port configuration with colored icons. At the bottom, there is a table titled '現有線路清單' (Existing Line List) with the following data:

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	✓	Blue	編輯	刪除
2	內部線路(POC測試網段)	00:0C:29:1C:80:...	internal	2		Yellow	編輯	刪除
3	一般ISP閘道	00:0C:29:1C:80:49	external	3		Green	編輯	刪除

## 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。

**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**

	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閘道	1	編輯	刪除
2	Google轉往一般ISP閘道	無	3個規則	一般ISP閘道	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

## 操作介面

### 導向規則設置 – APP GROUP管理

國立中興大學  
WAN LOAD BALANCING

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網道	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

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

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網道	設定	刪除
yahoo	限制流量： 5242880 BPS	設定	刪除

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

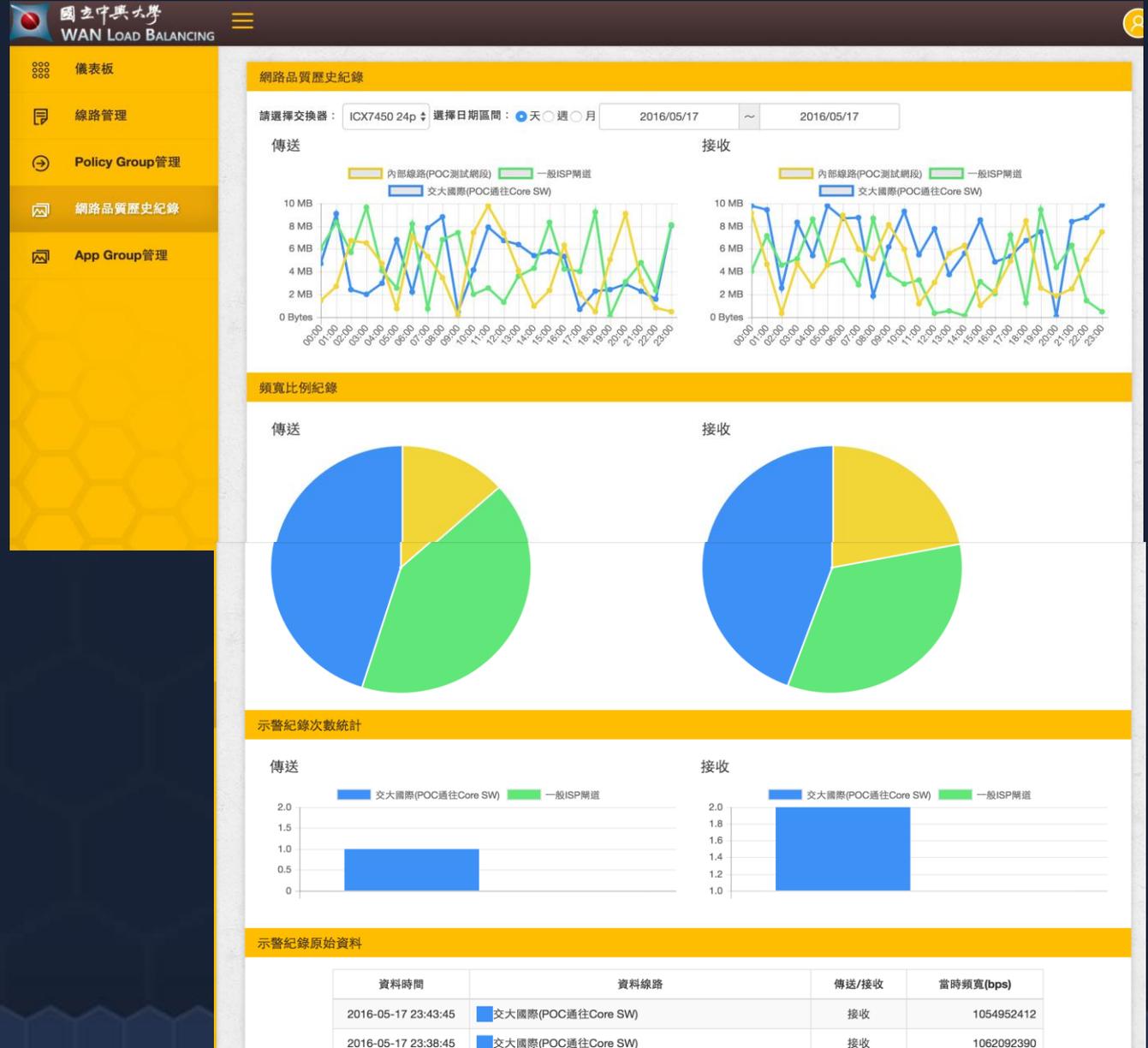
設備狀態異動紀錄

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

## 操作介面

## 歷史紀錄



# 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

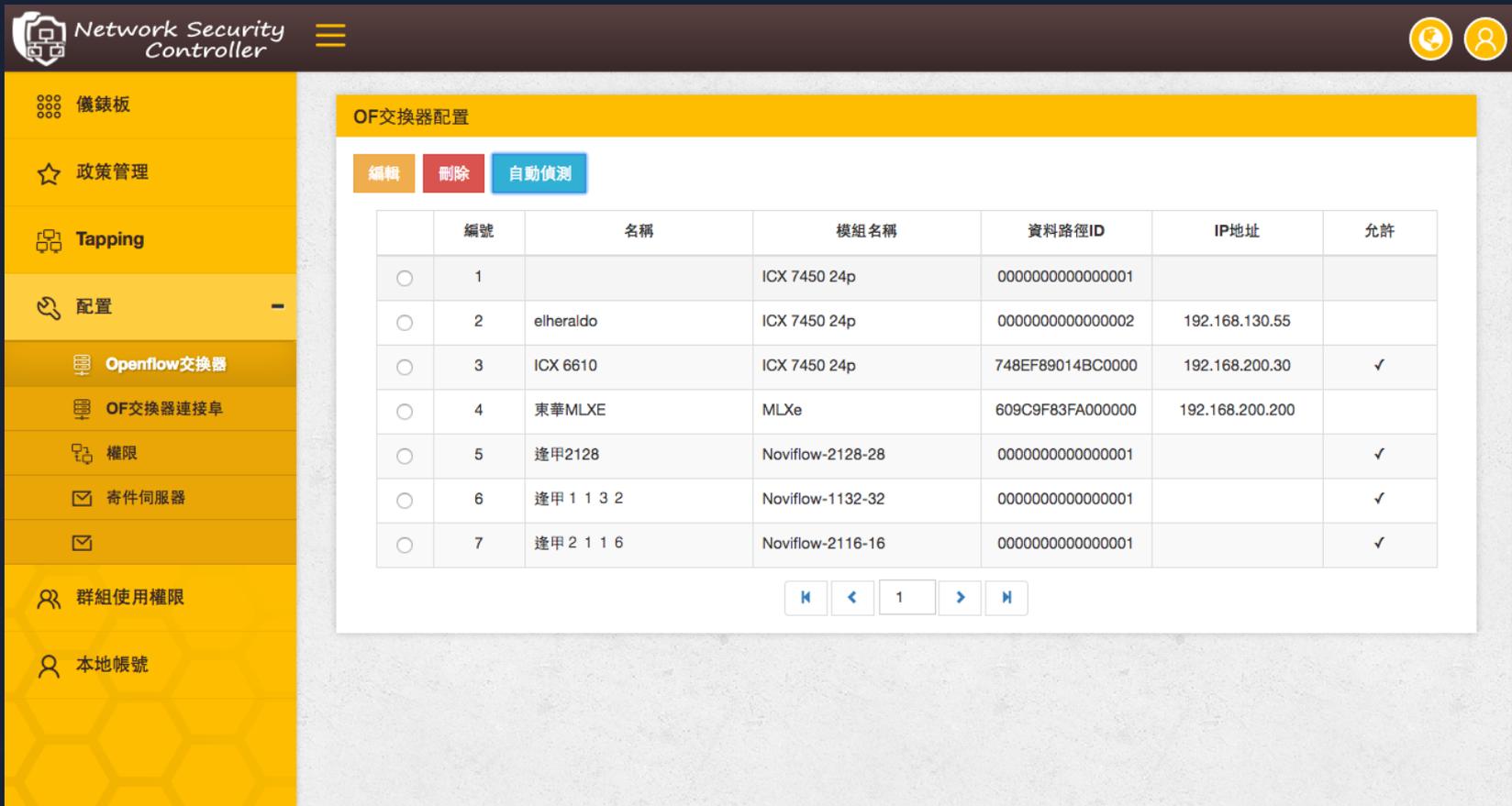
- 多個埠的流量需要匯總到同一個系統。
- 流量需加上網段，L2-L4，VLAN TAG 條件，符合後再進行複製。

### 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



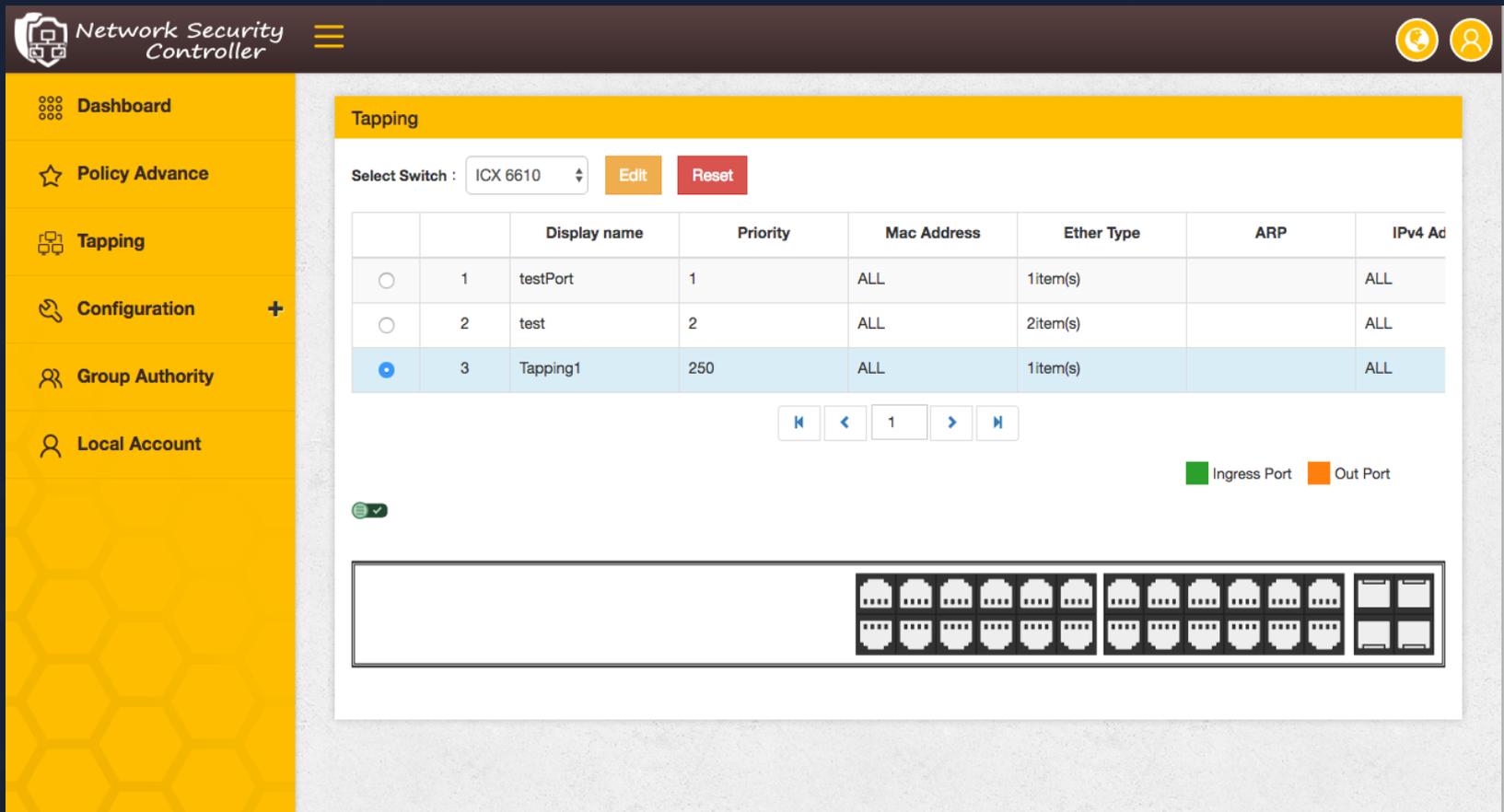
The screenshot displays the 'Network Security Controller' web interface. The left sidebar contains navigation options: 儀錶板, 政策管理, Tapping, 配置, Openflow交換器, OF交換器連接埠, 權限, 寄件伺服器, 群組使用權限, and 本地帳號. The main content area is titled 'OF交換器配置' and includes buttons for 編輯, 刪除, and 自動偵測. Below these buttons is a table listing switch configurations.

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

Navigation controls at the bottom of the table include:

## 操作介面

### TAPPING RULES CONFIG



The screenshot displays the 'Tapping' configuration page in the Network Security Controller. The interface includes a sidebar with navigation options: Dashboard, Policy Advance, Tapping, Configuration, Group Authority, and Local Account. The main content area shows a table of tapping rules for switch 'ICX 6610'.

**Network Security Controller**

Select Switch : ICX 6610 Edit Reset

		Display name	Priority	Mac Address	Ether Type	ARP	IPv4 Ad
<input type="radio"/>	1	testPort	1	ALL	1item(s)		ALL
<input type="radio"/>	2	test	2	ALL	2item(s)		ALL
<input checked="" type="radio"/>	3	Tapping1	250	ALL	1item(s)		ALL

Navigation: ⏪ ⏩ 1 ⏪ ⏩

Legend: ■ Ingress Port ■ Out Port

Switch Port Diagram: A schematic of a switch with 24 ports (12 on each side) and a console port on the right.





越世寰業

Q & A



**THANK  
YOU**