

2018大專校院資訊行政主管研討會

新一代校園網路管理

朱煜煌
電信研究院
107.09.27



大綱

- ➔ 校園網路現況
- ➔ 新一代校園網路管理
- ➔ EyeLAN網路解決方案
- ➔ EyeLAN應用案例
- ➔ EyeLAN管理介面
- ➔ 資料中心網路管理

校園網路現況

- 系統眾多，各有管理系統



網路印表機勒索威脅

- ➔ 2017年2月開始，全國至少46所大院校及國中小學遭駭客入侵，以網路印表機傳送恐嚇信，勒索3個比特幣、約10萬台幣，揚言不付款，將會癱瘓網路
- ➔ 事件觀察：
 - IoT設備多使用Public IP，易於從外網連入
 - 多數設備並無管控存取連線(Access Control)，任何IP皆可連入
 - 設備多為預設管理密碼，易遭駭客破解

校園比特幣勒索災情最新統計：全臺46校遭勒索，中小學占25%

教育部統計，全臺有46所學校受駭客勒索，半數以上為大專院校，並且，受侵入印表機裡面有73%印表機是HP。教育部認為，有些縣市學校收到威脅信後，網路沒受到影響，就不會主動通報，數量恐更多。

文/ 黃泓瑜 | 2017-02-23 發表

讚 5 按讚加入iThome粉絲團 讚 0 分享 G+



你以為印表機很安全嗎? 全臺46所學校印表機遭駭客入侵!

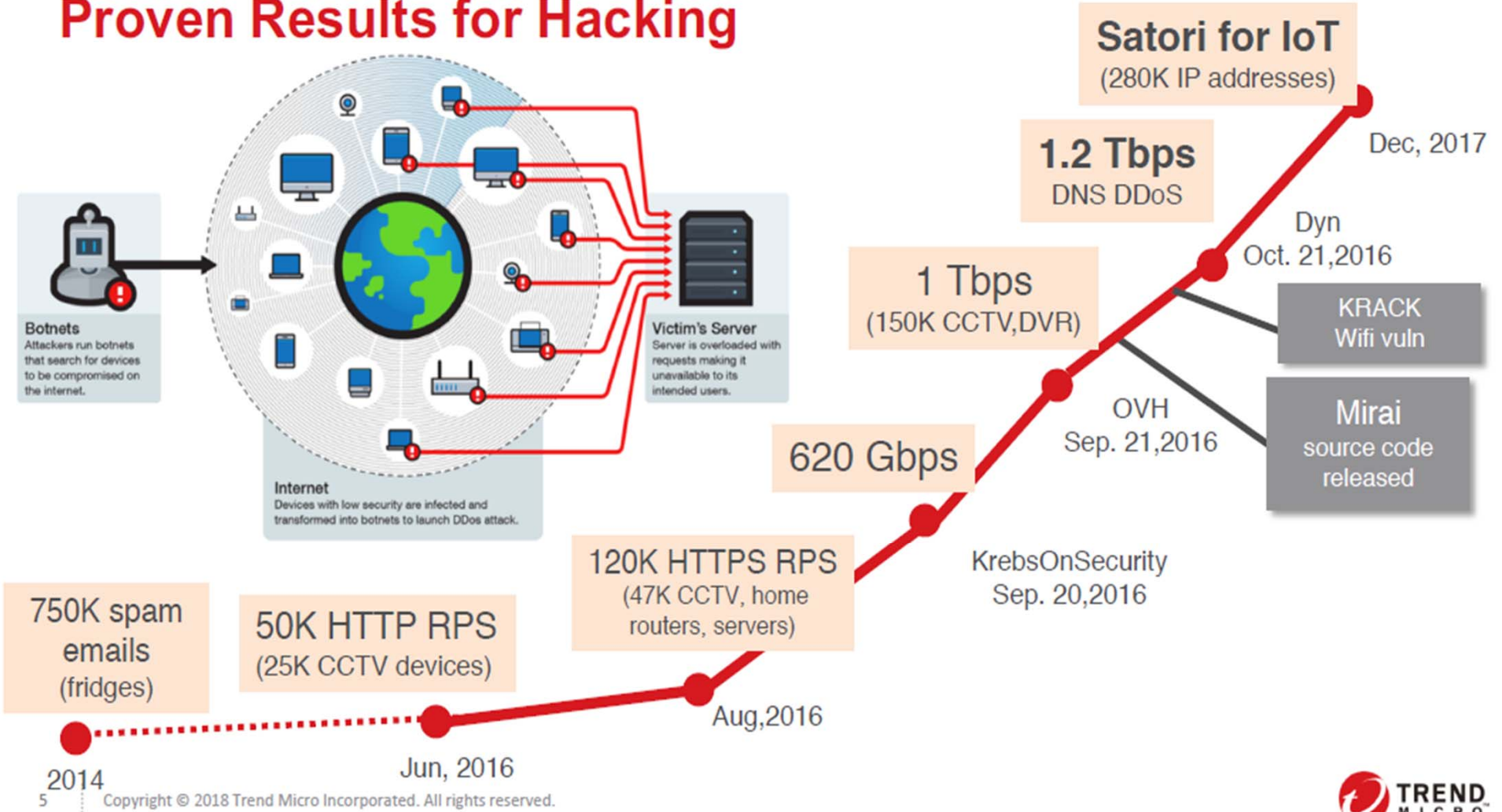
2017年03月10日 165反詐騙 165反詐騙專區

2017年資安風暴一波未平一波又起，上個月二月初臺灣證券市場才遭逢第一件大型駭客攻擊，二月底多所學校的網路印表機均收到自動列印署名為Emerson Rodrigues之恐嚇信件，要求校方指定時間前支付3個比特幣（約新臺幣10萬元），若未準時付款就會於3月1日發動網路攻擊以癱瘓學校網路。

IoT 攻擊逐年激增

誰的IoT設備?

Proven Results for Hacking



企業網路面對的資安威脅

2016年重大資料外洩事件年表

2016年2月9日

美國司法部：1萬名DHS與2萬名FBI員工個資遭竊

加州大學柏克萊分校：8萬名師生財務資料外洩

美國國稅局：70多萬納稅人資料遭竊

2016年3月10日

21st Century Oncology癌症醫療公司：坦言2015年遭竊220萬名患者資料

2016年4月11日

菲律賓選委會：匿名者組織侵入資料庫，5,500萬選民資料外洩

2016年5月11日

溫娣漢堡：美國300家連鎖店支付系統感染木馬，用戶支付卡資料遭竊

2016年5月17日

LinkedIn：發現2012年外洩1.17億筆資料

2016年9月22日

Yahoo：坦言2014年外洩5億筆帳戶資料

2016年10月20日

印度國家支付公司：POS機和ATM感染惡意程式，326萬張支付卡資料外洩

2016年11月13日

FriendFinder Networks成人網站：超過4.1億筆用戶資料外洩

2016年11月14日

Yahoo：揭露2013年還外洩10億用戶資料

2016年11月23日

美國海軍：外包公司員工筆電遭駭，13萬海軍個資外洩

資料來源：iThome整理，2017年1月

西班牙央行遭DoS攻擊，網站癱瘓近48小時

媒體報導，西班牙央行-西班牙銀行遭到DoS阻斷服務攻擊，外傳發動攻擊者是為抗議政治人物遭監禁，該銀行網站至今仍未恢復正常。

文/ 林妍潔 | 2018-08-28 發表

讚 5 高 按讚加入iThome粉絲團 讚 229 分享 G+



圖片來源: 維基百科/Luis Garcia



一銀ATM遭駭事件大剖析

這是臺灣金融史上第一次，與駭客集團暗中駭入臺灣大型銀行的41臺ATM，從倫敦一臺電話錄音伺服器，橫跨1萬公里，遠端遙控北中兩地22家一銀分行的41臺ATM，還派出十多名車手兵分多路，神不知鬼不覺地盜領8,327萬多元。但是，為何向來是資安優等生的第一銀行，事前一點跡象都沒有察覺？

資料來源: iThome 2016/07

攻擊手法：

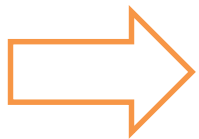
外對內 ⇒ DDoS攻擊 (購買防火牆無效)

內對內 ⇒ 外部遙控內對內攻擊

(透過Ethernet網路)

台積電抓出魔鬼：裝新機台未掃毒

- ➔ **蒸發78億！** 台積電抓出魔鬼：裝新機台未掃毒
- ➔ 消息人士透露，台積電是在上周五（二日）傍晚約**五、六時**遭電腦病毒入侵，並於**當晚十時許擴散至三大廠區**。依台積電昨天的公告推算，事件發生後約四十小時，已恢復八成機台生產作業，預計在關鍵的六十小時「排毒行動」後，可望全數排除電腦病毒；但比原先預期慢了約一天，受衝擊營收也比預期大
- ➔ 台積電昨天下午發布重大訊息指出，針對事件發生原因，主要是出於「新機台在安裝軟體的過程中操作失誤」，病毒在新機台連接到台積電**內部電腦網路時，發生病毒擴散**，但公司資料的完整性和機密資訊皆未受影響



電腦病毒會主動擴散

新一代校園網路管理



IoT設備管理

- ➔ 設備**實名制**: 門禁管理系統, 印表機, 多功能事務, 刷卡機
- ➔ 設備的**位置標示**: (例)A棟5F東側
- ➔ 流量監控: 即時、歷史
- ➔ 管理IoT設備**不會被駭入**: 網路隔離
- ➔ 管理每個設備**使用的範圍**: (例)印表機不能上Internet
- ➔ 管理每個設備**使用的時段**
- ➔ **集中管理畫面**

使用者設備 管理

- ➔ 使用者設備**實名制**: 使用者姓名、單位
- ➔ 使用者設備的**位置標示**: (例)A棟5F東側辦公室
- ➔ 流量監控: 即時、歷史
- ➔ 管理每個設備**使用的範圍**: (例)學生、教職員
- ➔ 管理每個使用者**使用的時段**: 宿舍上網(夜間)管理
- ➔ 管理網路**使用的內容**: 惡意網站、非法軟體
- ➔ **集中管理畫面**

目前常見商用解決方法

- ➔ 增購防火牆(FW)進行隔離
- ➔ 購買NAC設備，進行實名制管理


➔ 防火牆議題

- － 防火牆管理不易
- － 防火牆的漏洞: 靜態且長時間開通
- － 防火牆容量需不斷擴增

商用NAC管控設備限制

- 利用SNMP/Telnet進行蒐集資料
- 缺點: 只能看，發生障礙時無法作為 (且不即時)

議題	NetSecure
<u>1. 無法即時阻擋</u>	<ul style="list-style-type: none">• 因利用SNMP讀取Router ARP Table是週期性的(5分鐘或10分鐘)，會有<u>空窗期</u>，導致無法即時阻擋• <u>無法防治ARP偵測其他設備的IP/MAC資料</u>
<u>2. 有誤判情形及錯誤阻擋</u>	<ul style="list-style-type: none">• Router的ARP Table會被Spoofing(欺騙)，當Spoofing發生時，NetSecure會<u>誤判</u>認為諸多IP/MAC均有誤，而<u>封鎖大片交換器的Port</u>，導致錯誤阻擋• ARP Table及MAC均是學習來的，<u>容易被駭導致錯誤學習</u>
<u>3. 封鎖後的開通，會影響其他正常設備</u>	被封鎖的Ethernet Switch埠再次被開通時，被阻擋的設備若未被修正， <u>可能影響其他正常設備</u>

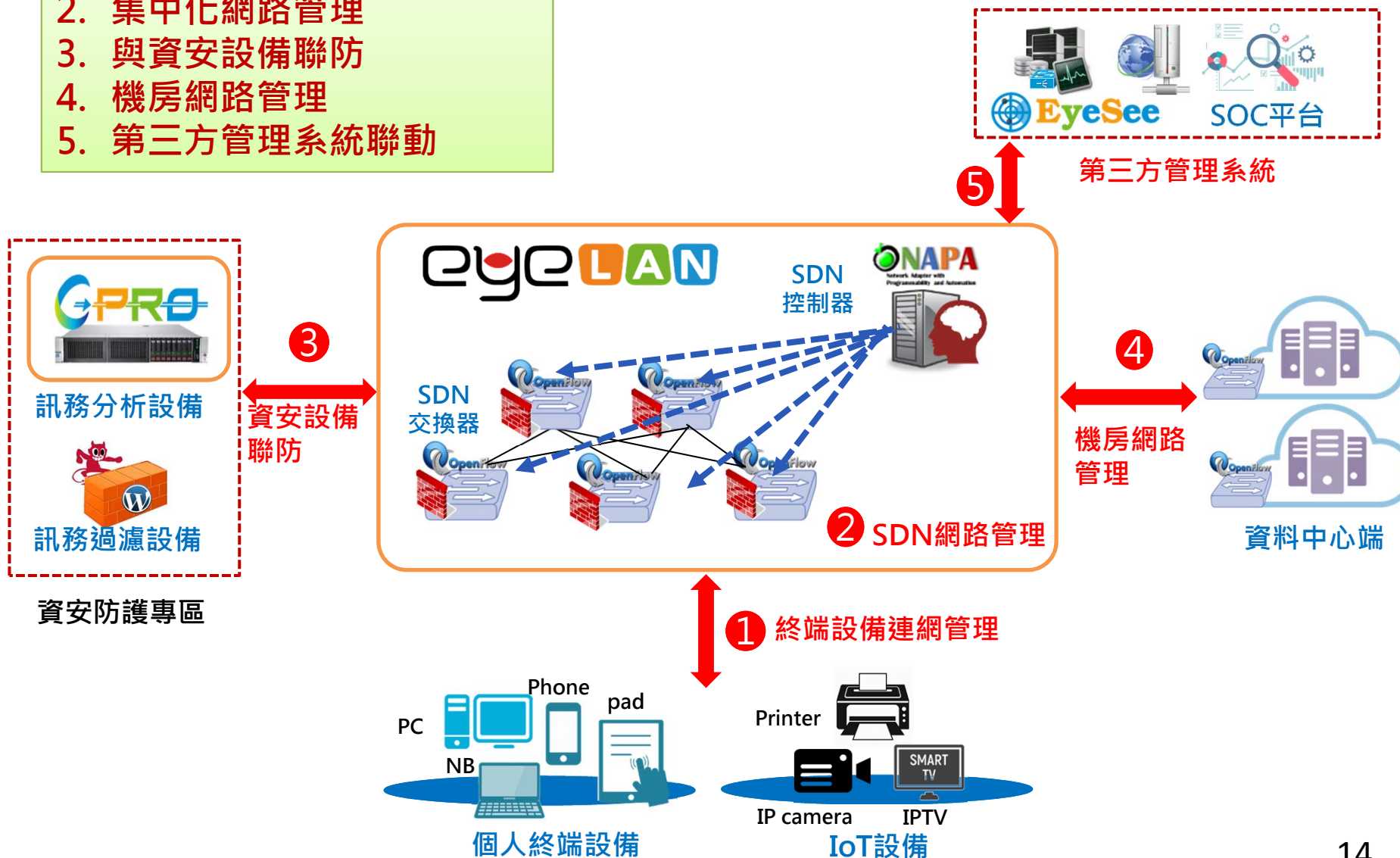


EyeLAN網路解決方案 (中華電信自主研發的新一代智慧網路管理系統)

EyeLAN 五大特點



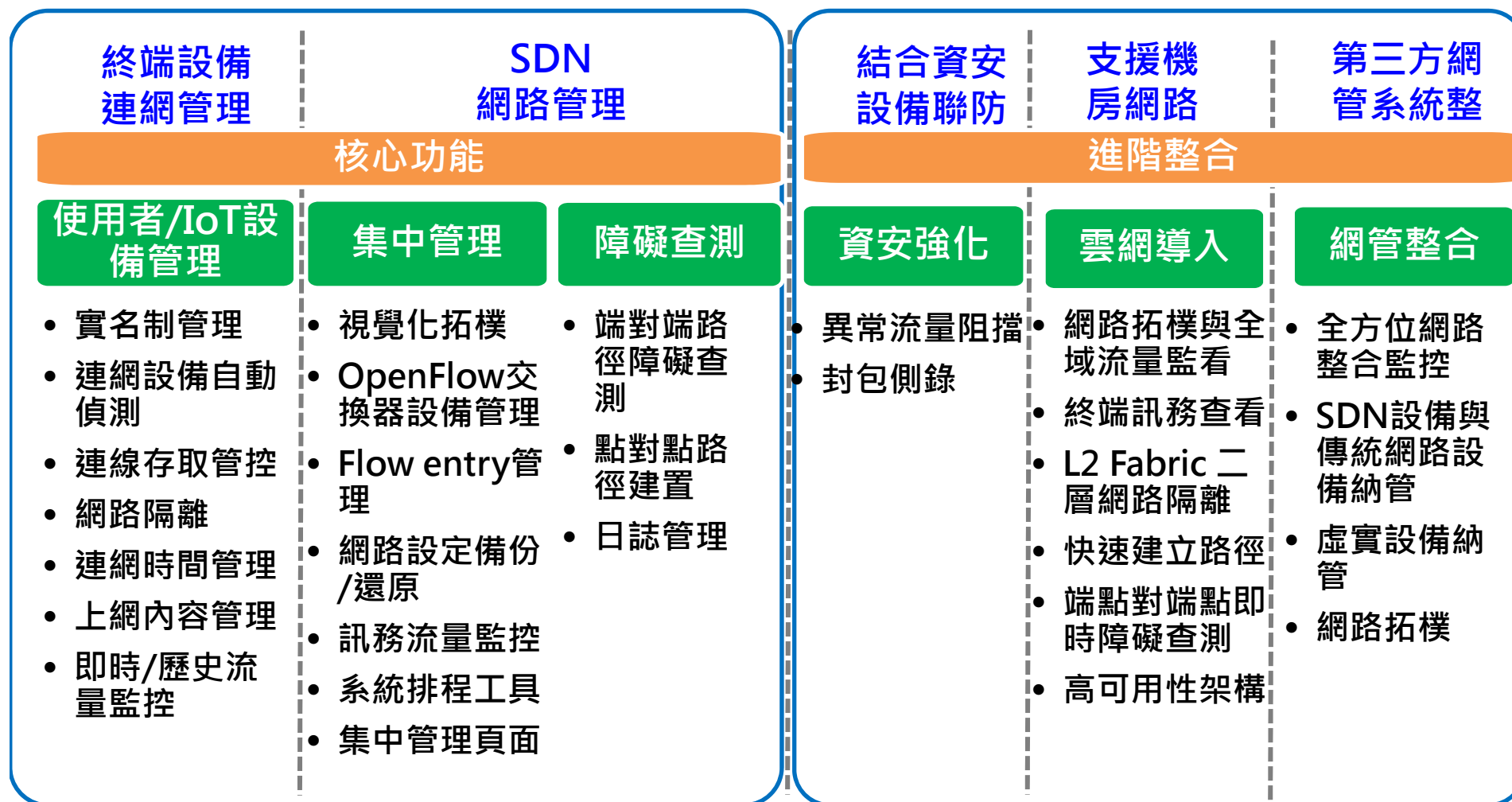
1. 終端設備連網管理
2. 集中化網路管理
3. 與資安設備聯防
4. 機房網路管理
5. 第三方管理系統聯動



EyeLAN功能總覽

基本版

進階版



EyeLAN 設備元件

➔ EyeLAN組成元件

- NAPA控制器 + OpenFlow 交換器
- (選配) SD-BOX, GPro, DPI.. 等

➔ 可與現有網路設備互運

EyeLAN產品基本組合



NAPA控制器



Open Flow交換器



增值應用(選配)

SD-BOX
L3 Routing、連線加密、安全功能)



GPro
訊務側錄分析



EyeSee
網管企業版

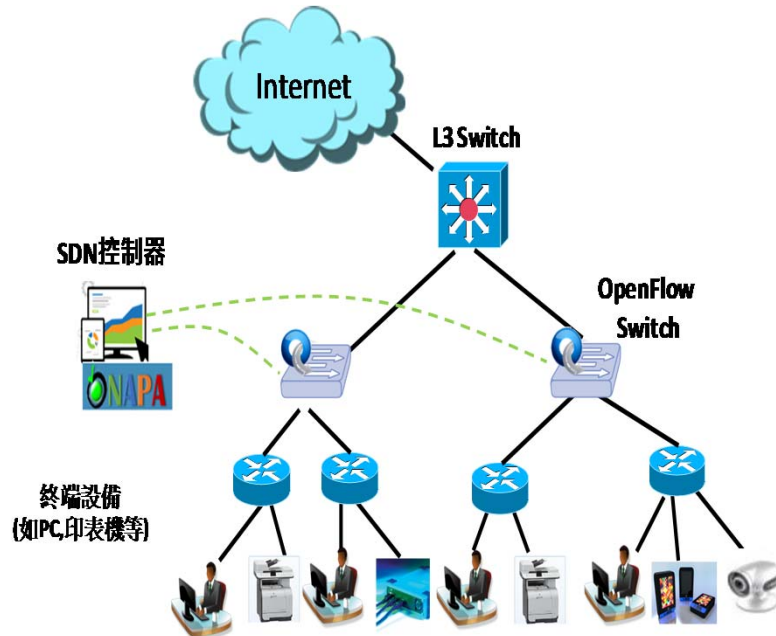


EyeQuila
APT潛伏威脅的偵測

EyeLAN網路架構建議

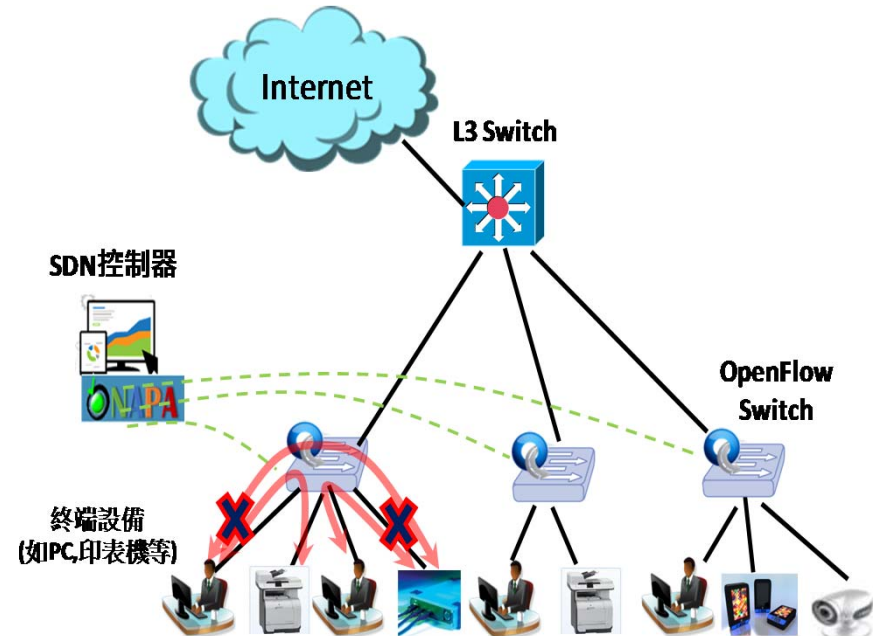
❖ 架構1

- 不改變原有網路架構
- 增加OpenFlow交換器
- 實名制可視化管理
- 無法防止ARP偵測其他設備的IP/MAC資料
- 無法防止東西向攻擊



❖ 架構2

- ✓ OpenFlow交換器取代L2交換器
- ✓ 實名制可視化管理
- ✓ 端對端隔離管理
- ✓ 可以防治ARP攻擊/偽造
- ✓ CHTNet 2.0 架構



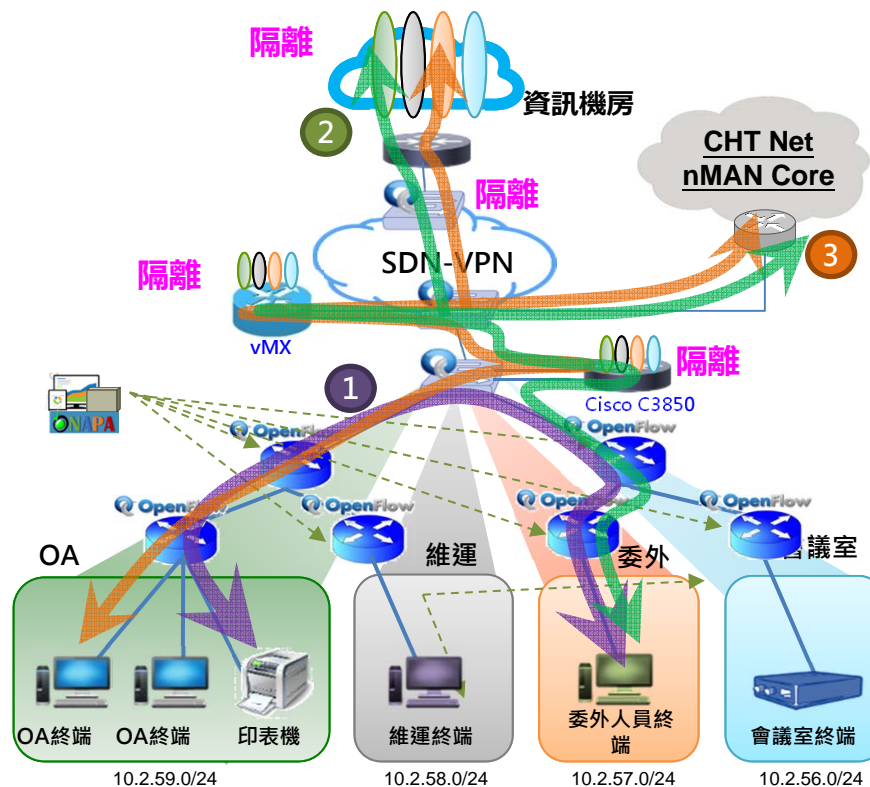
架構2範例

特色

- 由資訊系統(IPAM)管理網路的使用者
- 資訊系統可動態調整設備屬性，網路接收指令自動調整設定(無人工介入)
- NAPA依據屬性將設備導到不同路徑，彼此隔離
- 網管人員透過NAPA管理網路
- 骨幹網路確實隔離(各自有路由器)

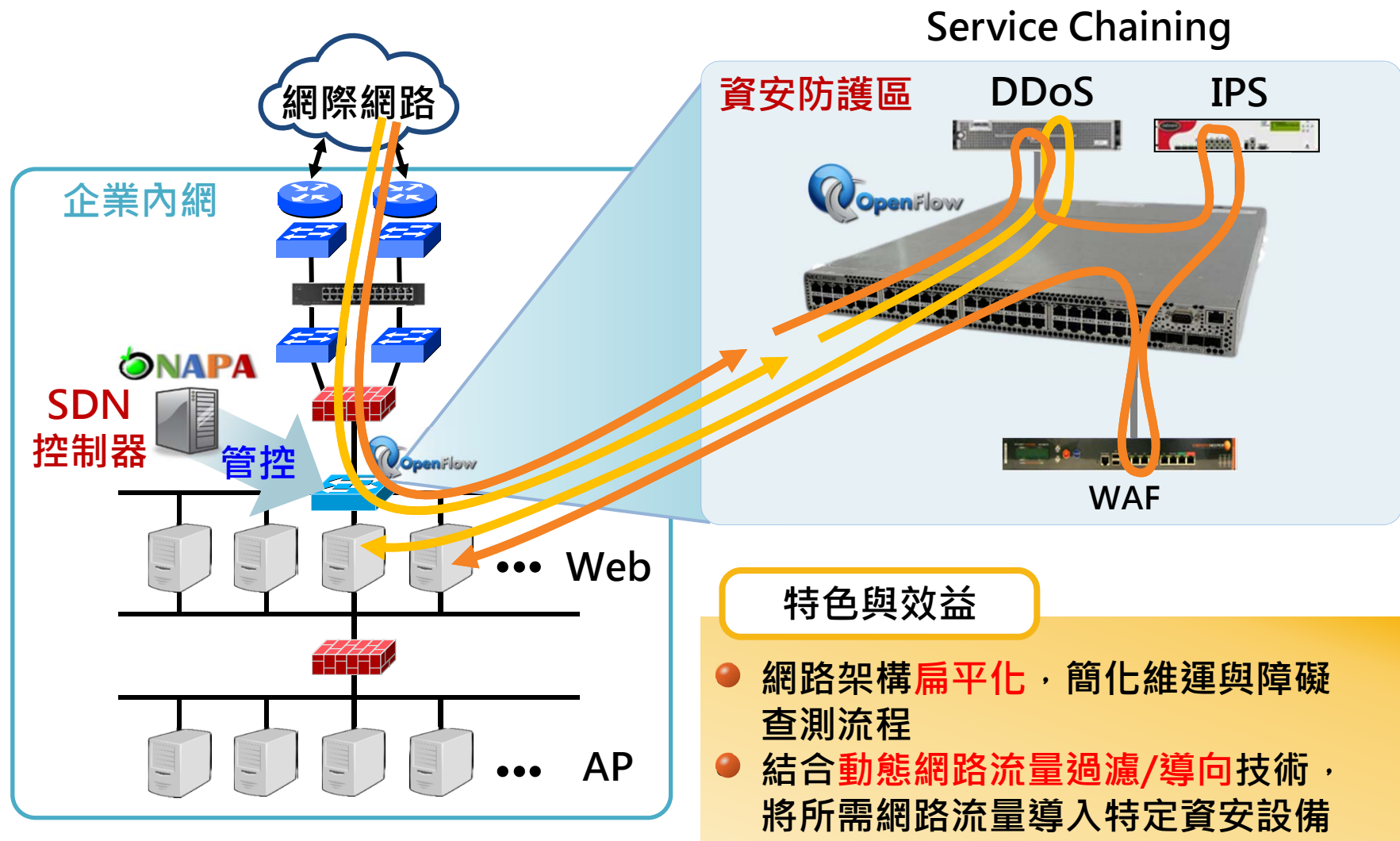


CHTNet 2.0

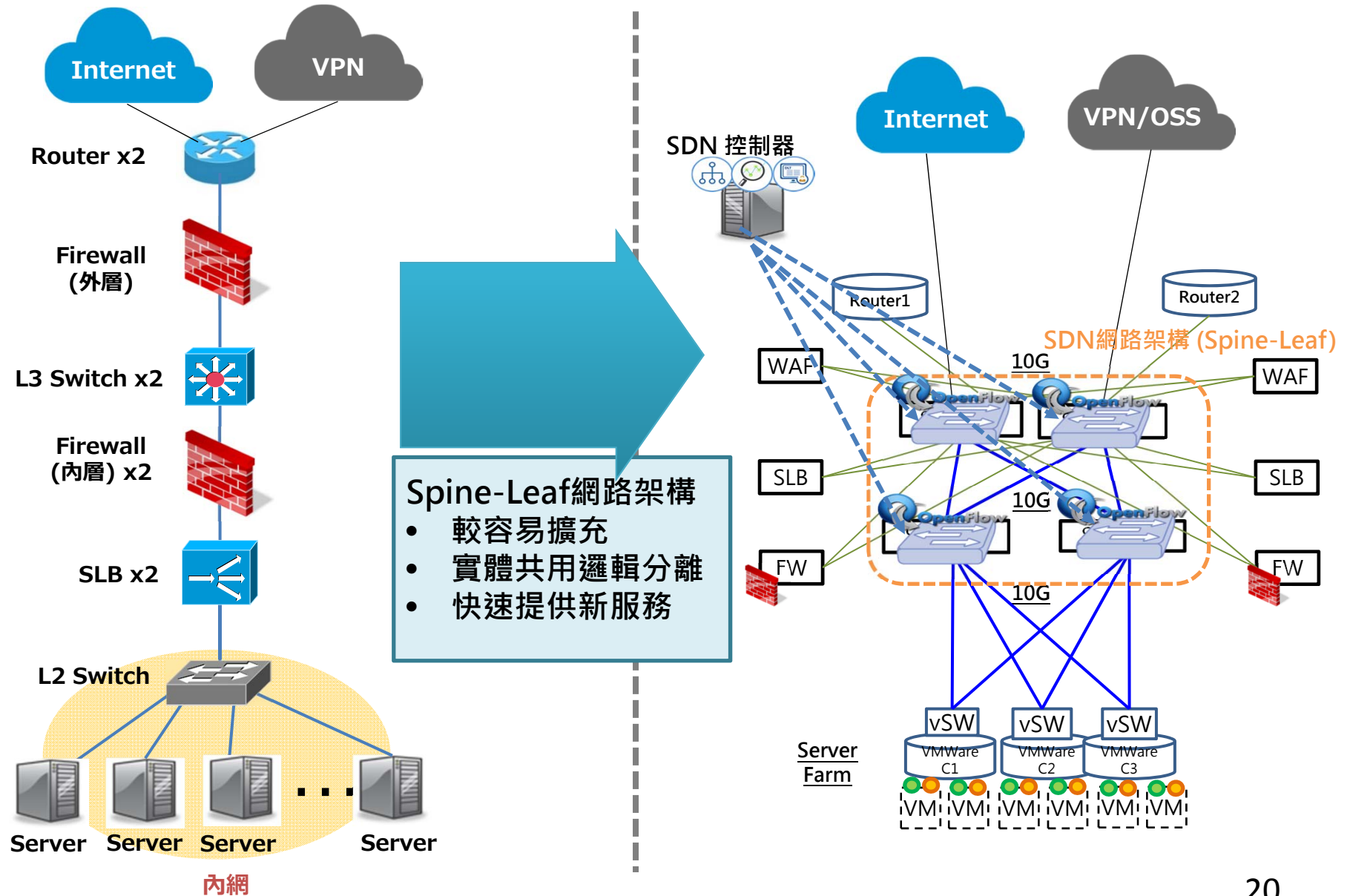


- 四個VPN
 - 正職
 - 專屬維運終端
 - 委外
 - 會議室終端

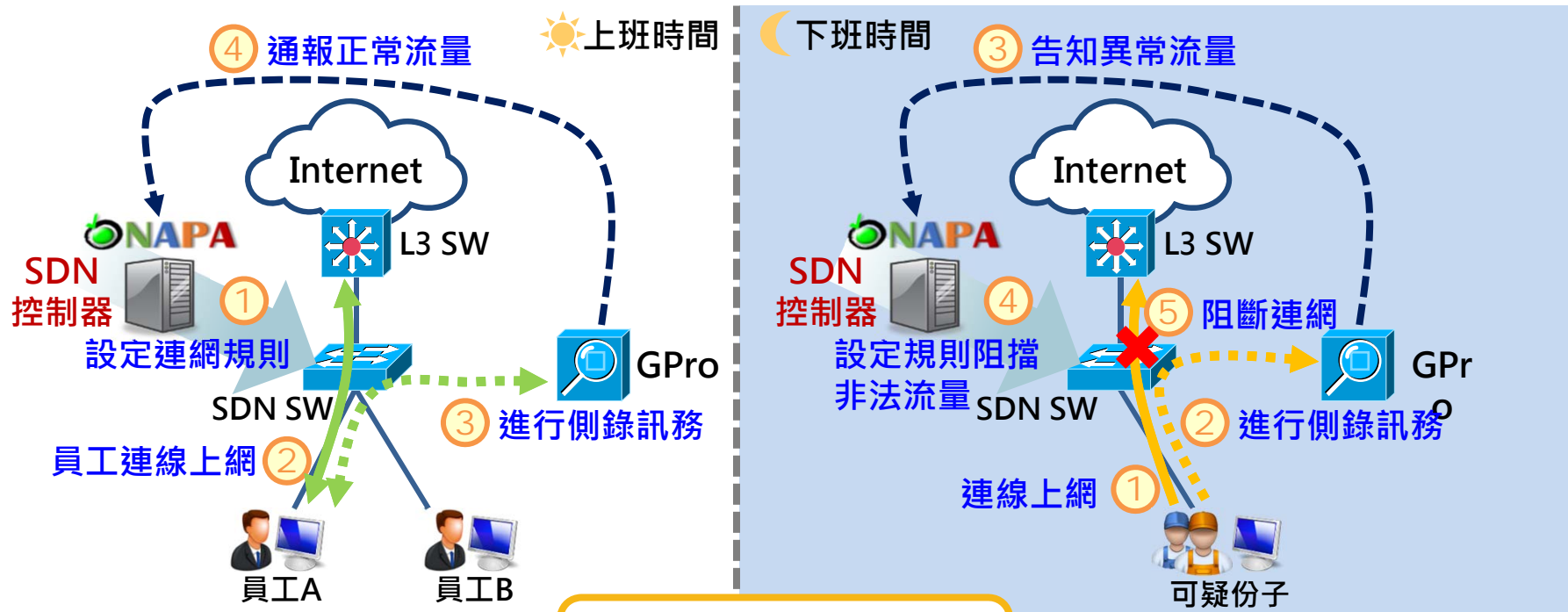
EyeLAN與資安設備架構建議



EyeLAN 導入資料中心網路架構



EyeLAN與封包側錄及異常阻擋



特色與效益

- 網路黑白名單(ACL)集中設定
- 非合法IP/MAC使用者禁止連網
- 依不同時間(如上/下班時間), 自動開啟或關閉網路
- 依實體埠/IP/MAC/應用服務, 側錄網路封包, 偵測異常可立即阻擋



網路流量側錄分析系統GPro - 網路威脅分析儀

資安防禦從被動轉為主動，快速掌握內網安全威脅，從點、線、面全面掌握內網可疑活動，完整歸納資安事件的來龍去脈。

自主研發

基礎數據完整收容

- 記錄**完整網路**開道活動軌跡
- 提供彈性調閱與檢索機制

◆惡意行為即時感知

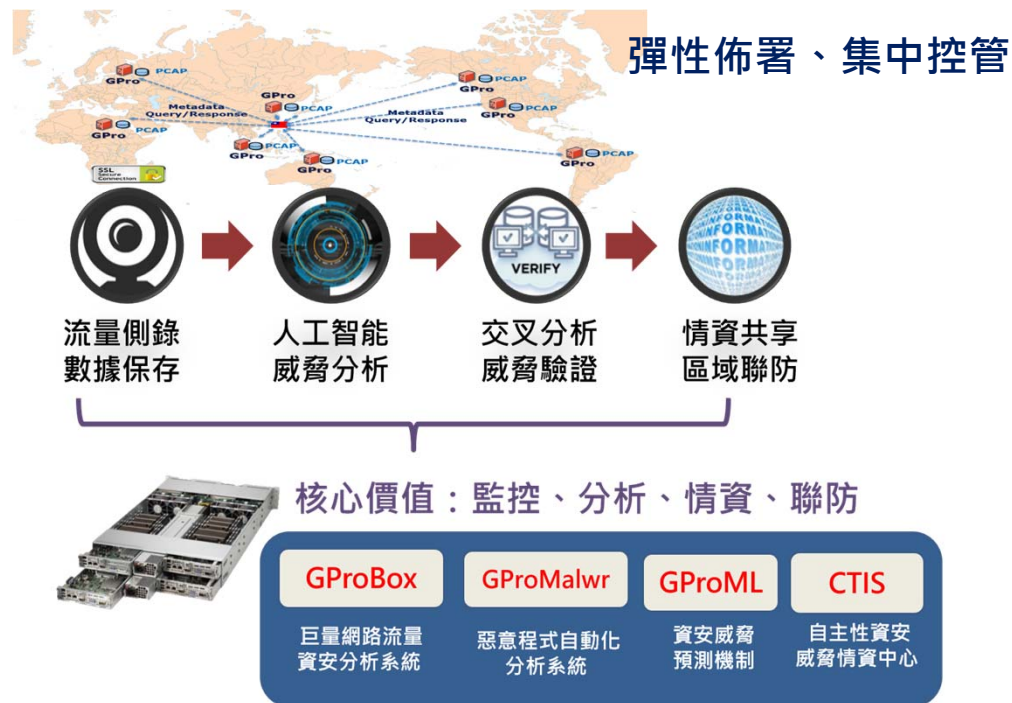
- 即時監控網路安全狀態
- **情資導向**設計理念，即時**標記惡意活動**

◆網路流量主動分析

- 自動化萃取與分析網路流量
- 數十項惡意檔案特徵比對模型，建構分群與分類機制

◆機器學習威脅預測

- 獨有惡意特徵數學模型
- 利用**機器學習**取得**未知威脅**與疑似受害電腦清單



已部署於**國安單位、政府機關與金融機構**等從事機敏業務單位

APT潛伏威脅的偵測系統 EyeQuila

- 中華電信自主研發的資安產品，專注在偵測進階持續威脅(APT)與未知威脅
- 透過網路與資安設備日誌分析可能的潛在風險
- 可提供軟硬體整合版本 或 軟體版本產品，可快速擴展的專屬硬體設計



長天期巨量資料機器學習 自動化回溯偵測機制 多面向威脅情資整合 視覺化整合分析統計

獨家開發的機器學習行為偵測引擎，分析長天期網路活動數據，補捉變化緩慢、難以察覺的攻擊行為

EyeQuila自動回溯分析保存的歷史軌跡能清查出曾經遺漏或是過去未曾發現的新型未知威脅

可自主擴增情資，介接外部黑名單(開源與商業資安情資來源)

視覺化整合，將可疑行為找出攻擊關聯性及範圍，掌握資安威脅的起源及受駭範圍

EyeLAN應用案例



案例一：校園網路應用

架構1

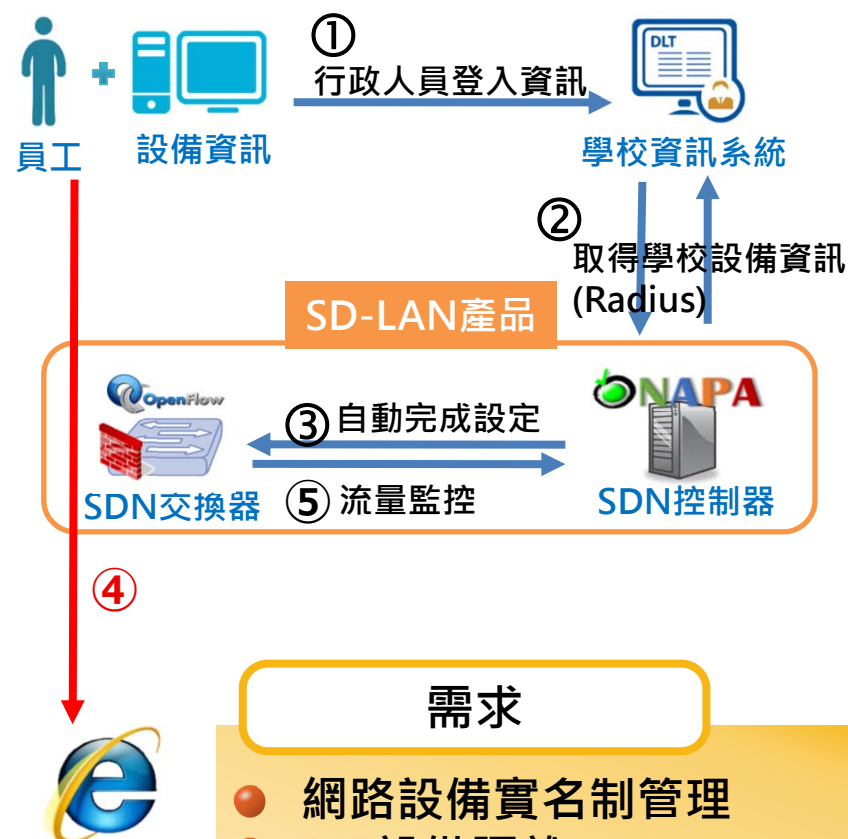
❖ 已執行

- 網路使用設備實名制管理
- 非註冊設備不可以使用網路
- 流量監控
- 管控IoT設備連網，避免被攻擊或操控 (6/4已裝機)

❖ 新需求

- 跨校園管理 (3個校區)
- 進出校園接口網路架構調整(導入SDN執行訊務工程)

情境說明



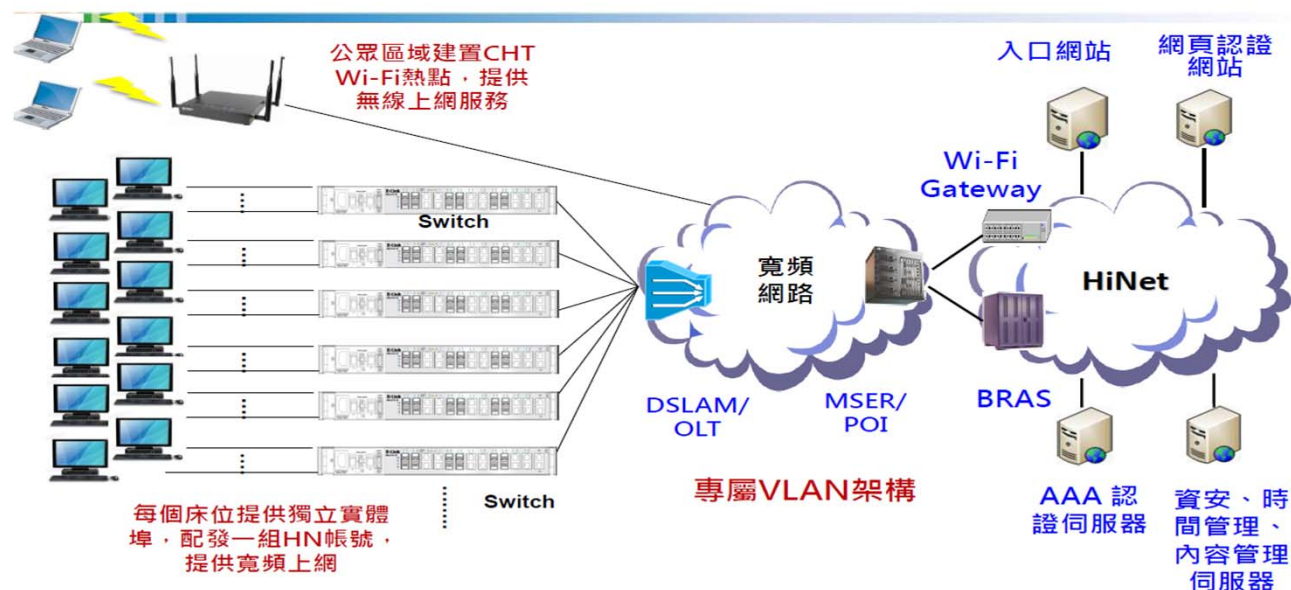
案例二：宿舍網路

架構1

- ➔ 可以綁定床位，可支援同學更換宿舍房間(有時幾週、有時每月)
- ➔ 可以提供使用者網路使用時數與網路流量的報表
- ➔ 可提供認證網頁，跟學校LDAP整合
- ➔ 可進行0-2點限制網速 (研究生例外)

需求

- 綁定位置
- 限時限頻寬管理
- 管理網頁Portal



案例三: xx大學SDN建設案

架構2

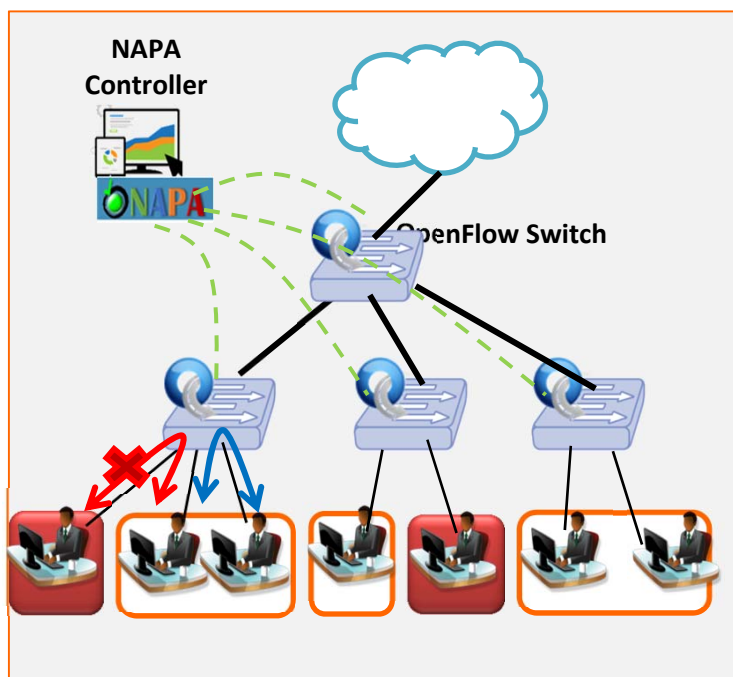
✦ 校園網路替換成SDN網路

✦ 主要需求

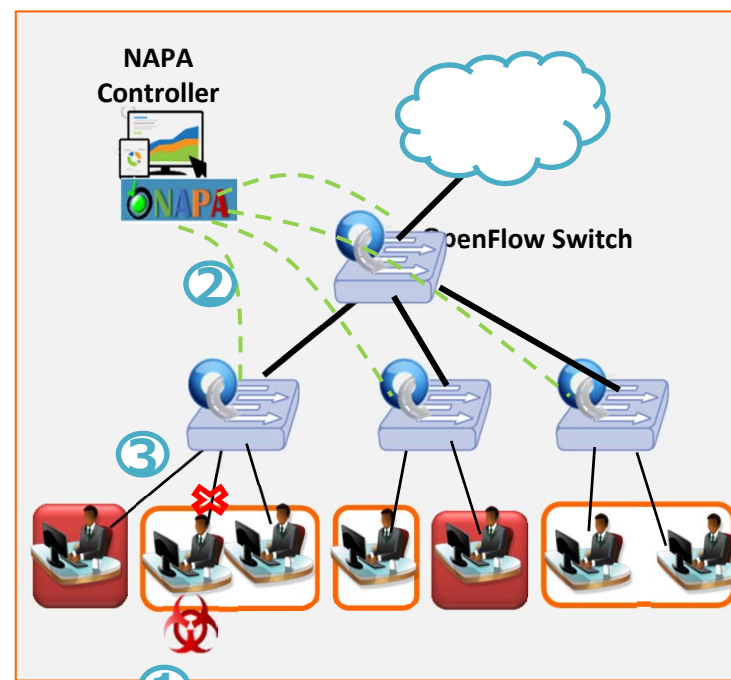
1. Micro-segmentation: Isolation upon infection
2. Autoconfig of switches: 換設備自動供裝、自動偵測設備、自動訊務蒐集、自動網路拓樸
3. Centralized management of 300+ switches

需求

- 網路隔離
- 自動化
- 集中管理



In normal situation



Host infected by virus

Segment 1

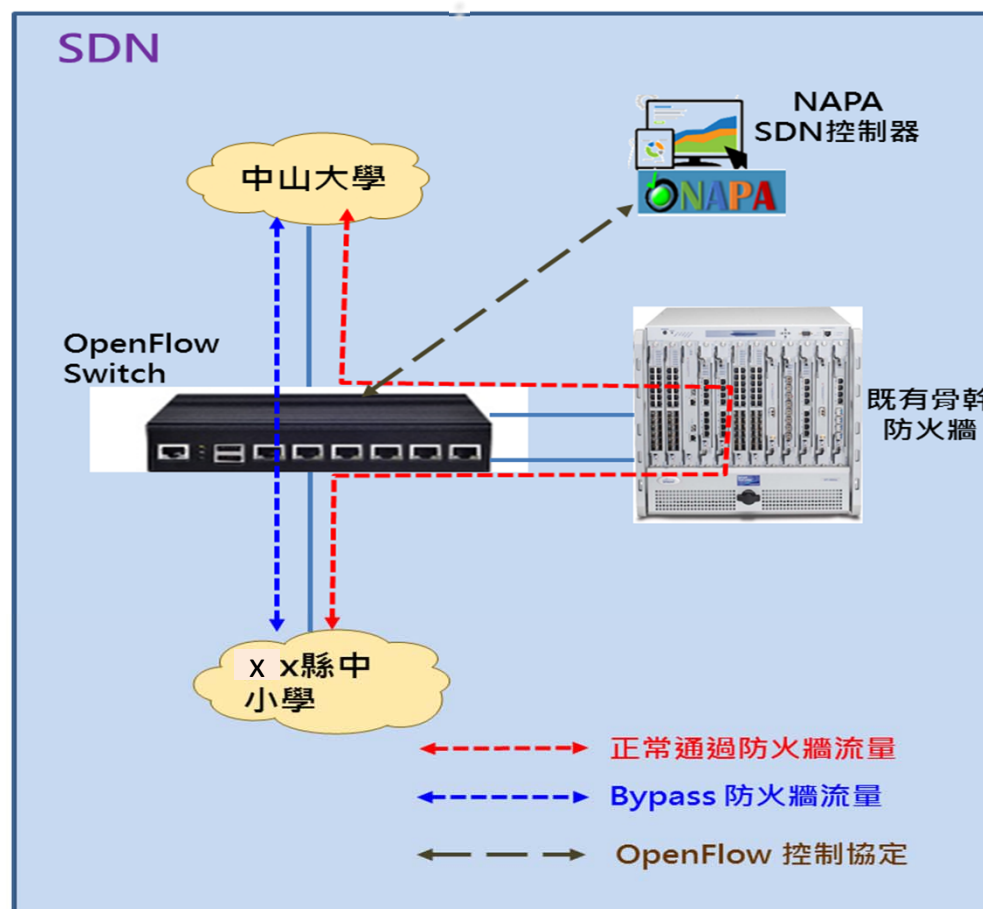
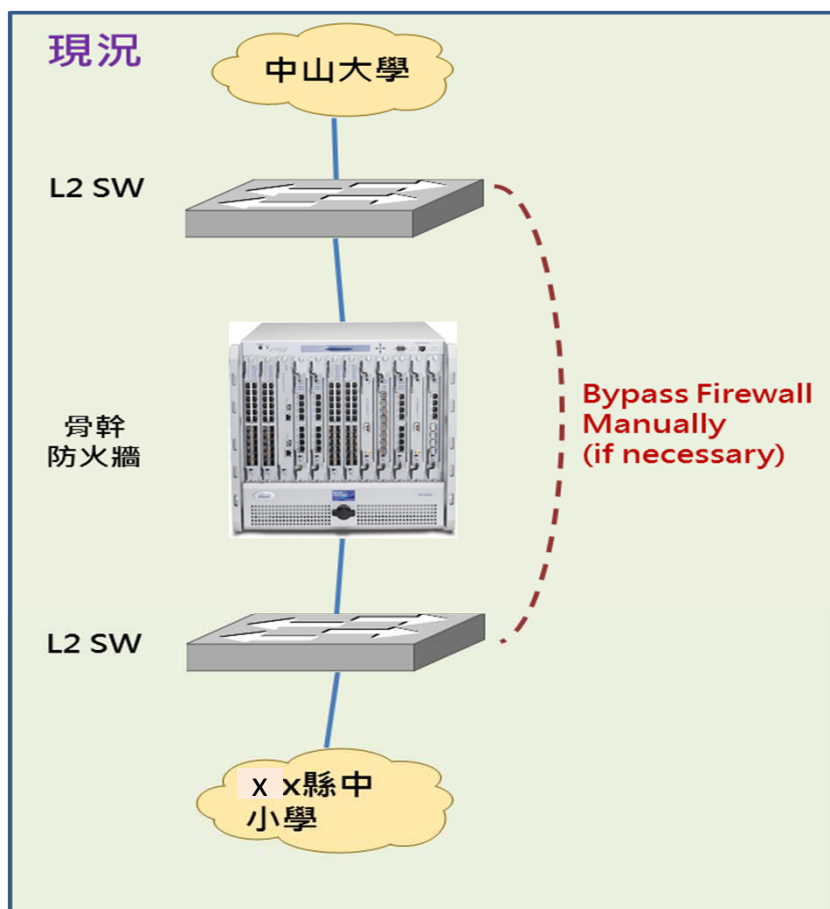
segment 2

案例四: SDN輔助骨幹防火牆 架構

- ➡ OpenFlow Switch旁掛防火牆
- ➡ 進行**防火牆流量offload**
- ➡ 防火牆障礙時，Bypass用途

需求

- 防火牆流量offload
- 降低防火牆負載



案例五: xx社區智慧路燈

架構2

- ➔ IoT設備可視化(實名制)管理
- ➔ 訊務監控 IoT設備設
- ➔ 主動偵測IoT設備是否存活
- ➔ QoS
- ➔ Multicasting

需求

- IoT設備實名制管理
- 主動偵測IoT設備狀況
- 點對多點傳送視訊
- 簡化維運負擔



網路拓樸圖 (網路架構)

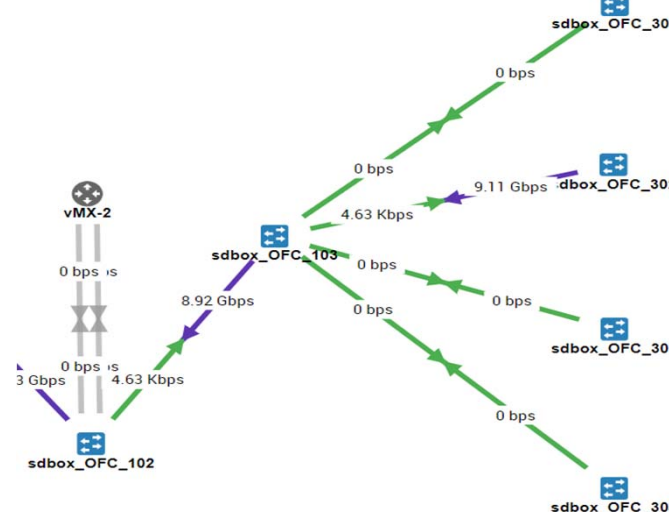


交換器設備集中管理

➔ OF交換器 設備 集中管理

- 提供鏈路流量監看,易於網路管理者掌握目前網路全貌
- 集中管理SDN OF交換器資訊與狀態

- 綠色: 0~25 %
- 黃色: 25~50 %
- 紅色: 50~75 %
- 紫色: 75~100 %

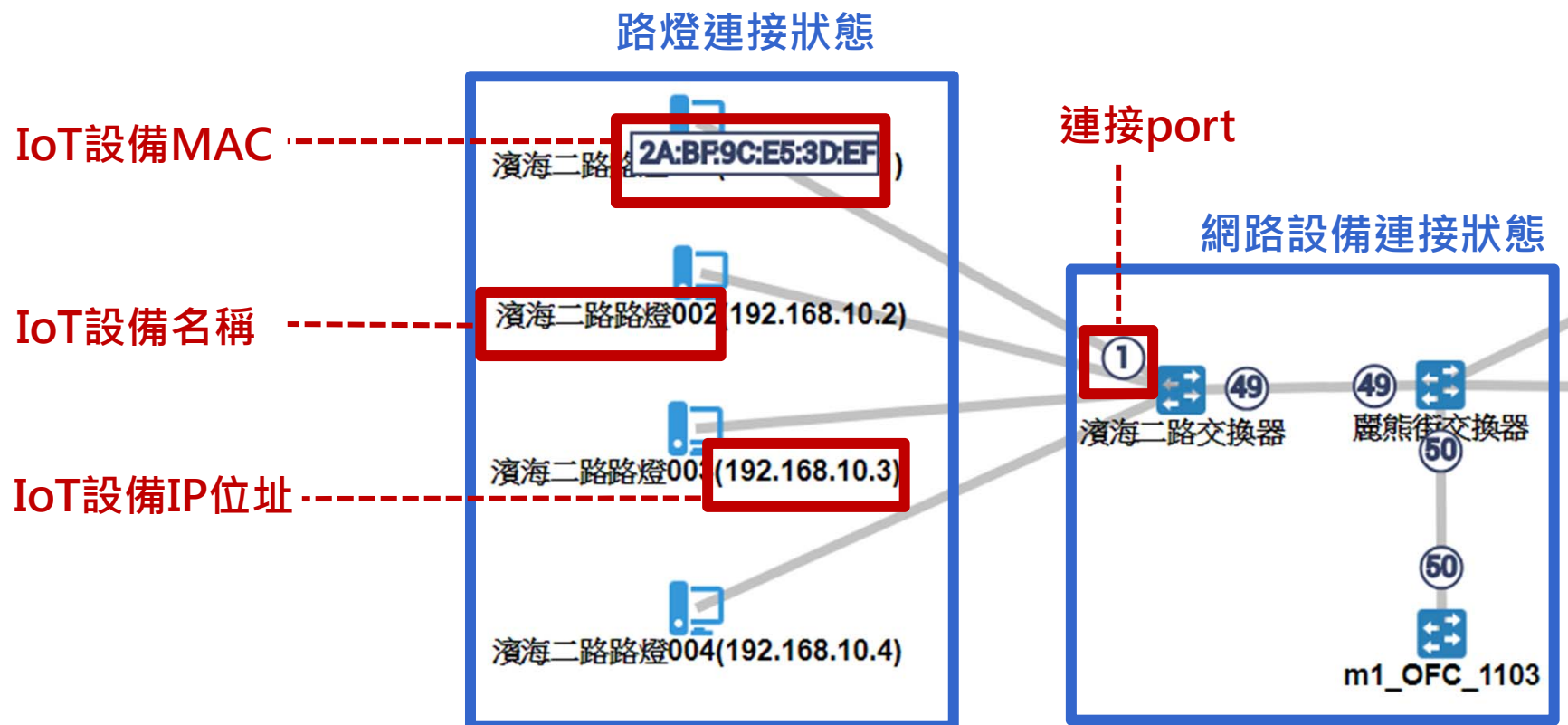


名稱↓	DPID -	IP -	硬體描述 -	軟體描述 -	製造商 -	OPENFLOW 版本 -	線上 -	指令 -
濱海二路交換器	1101	10.144.170.165	Open vSwitch	2.9.0	Nicira, Inc.	1.3	✓	👁️ ⚙️ 🗑️
麗熊街交換器	1102	10.144.170.165	Open vSwitch	2.9.0	Nicira, Inc.	1.3	✓	👁️ ⚙️ 🗑️

每個燈柱連接的網路設備 (IoT管理)

➔ IoT設備**可視化**管理

- 整體網路拓樸, 包括網路架構, 相連的實體埠(port)
- 顯示IoT設備**連接位置**、**連接port**、**名稱**、**IP位址**



IoT設備實名制管理

➔ IoT設備實名制管理

- 顯示所屬使用者以及IoT設備名稱、IP/MAC位址
- 顯示IP/MAC位址，並可加以管控
- 目前連網開通狀態

使用者與名稱

使用者 -	名稱 ↑	描述 -
	濱海二路路燈001	濱海二路路燈001
	濱海二路路燈002	濱海二路路燈002
	濱海二路路燈003	濱海二路路燈003
	濱海二路路燈004	濱海二路路燈004

IP/MAC資訊



IP -	MAC -
192.168.10.1	2A:BF:9C:E5:3D:EF
192.168.10.2	2A:BF:9C:7A:DF:3C
192.168.10.3	2A:BF:4D:F5:8C:72
192.168.10.4	2A:BF:9C:F5:8C:AF

連網開通狀態

狀態 -	指令 -
Enable	  
	  
Enable	  
	  

IoT設備流量檢視

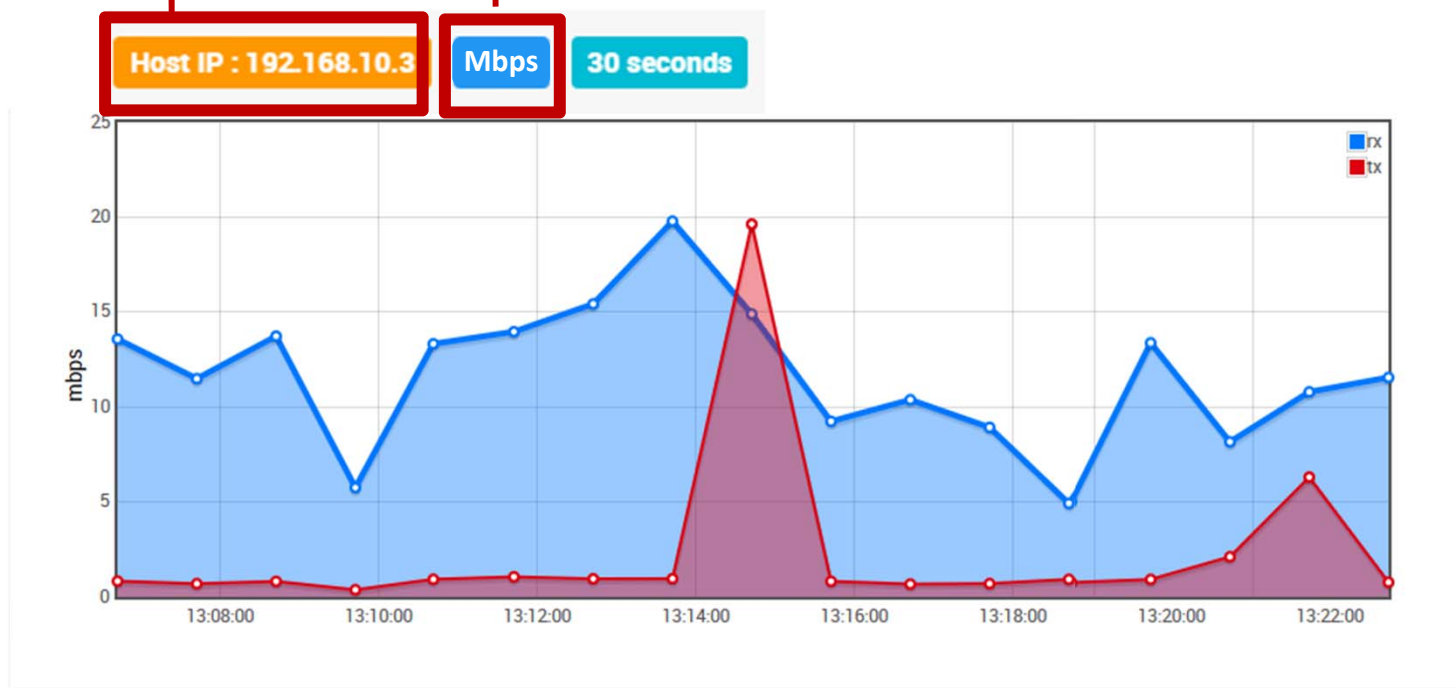
➔ 由設備管理頁面，檢視IoT設備即時流量

濱海二路路燈001 濱海二路路燈001 192.168.10.1 2A:BF:9C:E5:3D:EF Enable   

設備IP

顯示單位

檢視即時流量



案例六: 中華電信大樓

強化網路安全、易管理、自動化

	CHTNet 1.0	CHTNet 2.0
設計原則	<ul style="list-style-type: none">• 容易連線及使用(Default 開通) , 隨插隨用• 增購防火牆進行接管管理• 網路24小時全開通• 單一VPN網路	<ul style="list-style-type: none">• 網路嚴格管理(Default不通) , 沒有申請即無法使用• 進行設備管理(無須額外設備)• 上班時段網路開通 , 非上班時段需申請• 多個VPN網路
安全	<ul style="list-style-type: none">• 無內部防護機制• 可布建防火牆進行網段隔離• 可加購資安設備	<ul style="list-style-type: none">• 無法用ARP偵測其他設備的IP/MAC資料• 特定網段/特殊連線(業務會議)可進行隔離• 可加購資安設備
供裝維運	<ul style="list-style-type: none">• 人工操作• 個別設定• 人員異動須人工作業網路設定	<ul style="list-style-type: none">• 資訊系統自動供裝設定• 統一GUI集中設定/管理• 人員異動由資訊系統自動變更
費用		<ul style="list-style-type: none">• 整體費用低於CHTNet 1.0

EyeLAN管理介面



1 EyeLAN 使用者管理 (1/3)

Who

Where

阻擋私設IP

- **實名制管理**: 以使用者與身份特性管理誰可以使用網路
- **IP+MAC管控**: 僅允許合法IP/MAC使用網路,
- **自動偵測終端**: 自動偵測使用網路的主機，提供包含IP位址、MAC位址，及連入交換器(Switch/Port)等資訊

實名制管理

使用者 ↓	名稱 -	描述 -
黃奕欽	黃奕欽6樓辦公室PC	委外員工
謝靖慈	謝靖慈6樓辦公室PC	正職員工
謝靖慈	實驗室F201伺服器	

IP+MAC管控

IP -	MAC -	狀態 -
192.168.59.1	5E:16:71:AH:D9:F5	Enable
192.168.58.1	9B:16:A8:C5:D9:F7	Enable
192.168.57.1	BE:D9:F4:AF:16:71	Disable

自動偵測未知終端

Hosts List sdbox_OFC sdbox_OFC_3 All All

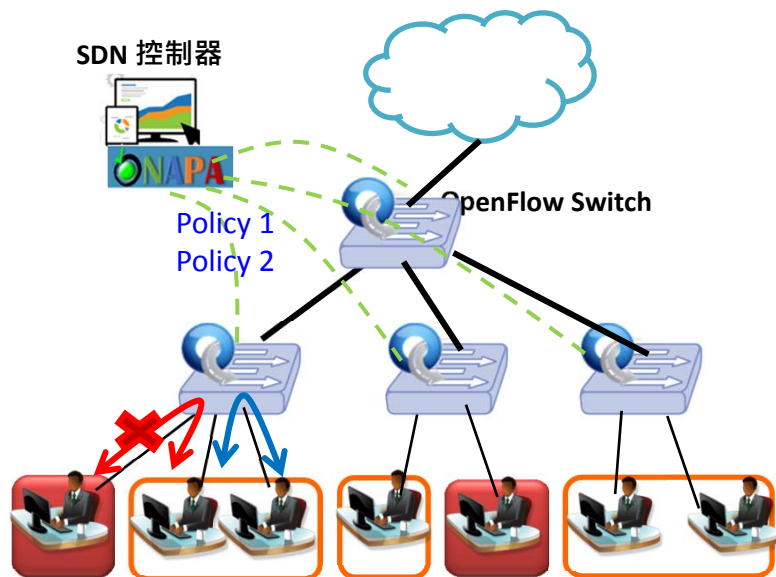
USER -	HOSTNAME -	DESC -	IP -	MAC -	STATUS -	Mac	* Network	* Switch	* Port
						86:26:5d:ba:7f:a4	NOTHING SELECTED	SDBOX_OFC_3	S3-ETH1

1 EyeLAN 使用者管理 (2/3)

Who

- ➔ 網路安全隔離 (不同群組隔離)
 - 透過連網策略管理建立內部主機適當隔離的資安政策

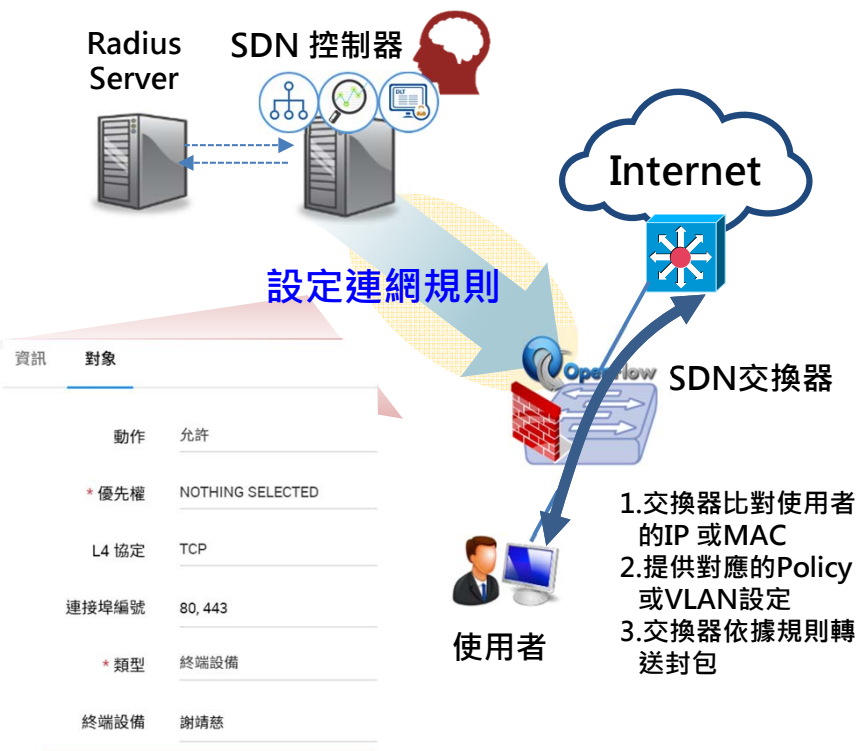
網路安全隔離



不同群組間主機不互通

- ➔ L1~L4網路存取控管 (ACL): 黑名單/白名單設計, 管控主機連網範圍

L1~L4網路存取控管



Policy設定可以終端設備、群組為目的端

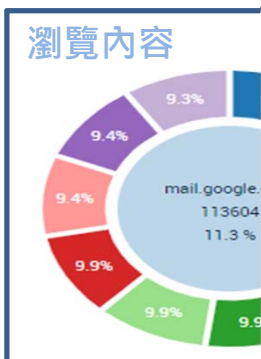
1 EyeLAN 使用者管理 (3/3)

➔ 使用者流量監看

What

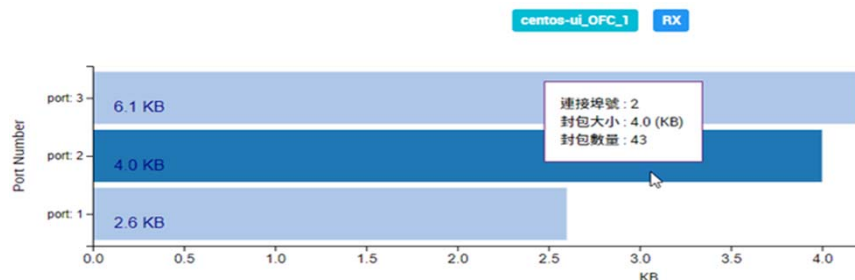
- 上網瀏覽內容與使用者流量統計(By Port/VLAN/IP)，異常時告警

TopN流量排名統計



- 1 mail.google.com
- 2 nchu.edu.tw
- 3 www.messenger.com
- 4 gamer.com.tw
- 5 datatables.net
- 6 stackoverflow.com
- 7 www.google.com.tw
- 8 www.w3cplus.com
- 9 google.com.tw
- 10 www.facebook.com

使用流量排名 (Port, VLAN, IP)



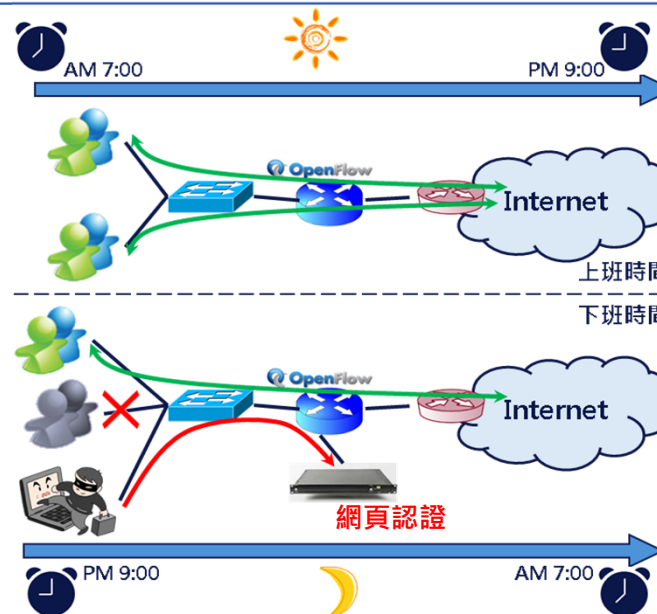
➔ 管控網路使用時間

When

- 下班時間上網，須經網頁認證，留存紀錄，email通知主管

管控網路使用時間

名稱 ↑	描述 -	時間 -
上班時間連網政策	IPAM開通	每日 08:00 - 18:00
下班連網政策	網頁認證	每日 18:01 - 23:00



2 EyeLAN網路管理(1/2)

How

➔ 集中管理

- 提供統一GUI操作畫面, 視覺化儀表及自定義介面

The screenshot displays the EyeLAN network management dashboard. On the left is a sidebar menu with the following items: Dashboard, 服務 (Services), 拓樸管理 (Topology Management), Log 管理 (Log Management), and 資源 (Resources). The main dashboard area is divided into several sections:

- 快速開通捷徑 (Quick Start Shortcut):** A blue card showing '未知終端設備' (Unknown terminal devices) with a count of 0 and a checkmark icon.
- 事件記錄 (Event Log):** A red card showing '事件 Log' (Event Log) with a count of 0 and a warning icon.
- 伺服器使用率 (Server Usage):** A section with four circular gauges: '平均負載' (Average Load) at 0%, 'CPU 使用率' (CPU Usage) at 1%, '記憶體使用率' (Memory Usage) at 93%, and '磁碟使用率' (Disk Usage) at 9%.
- 操作人員登入資訊 (Operator Login Information):** A table titled '最後登入' (Last Login) showing a list of login attempts.

A green box highlights the sidebar menu, labeled '功能選單' (Function Menu).

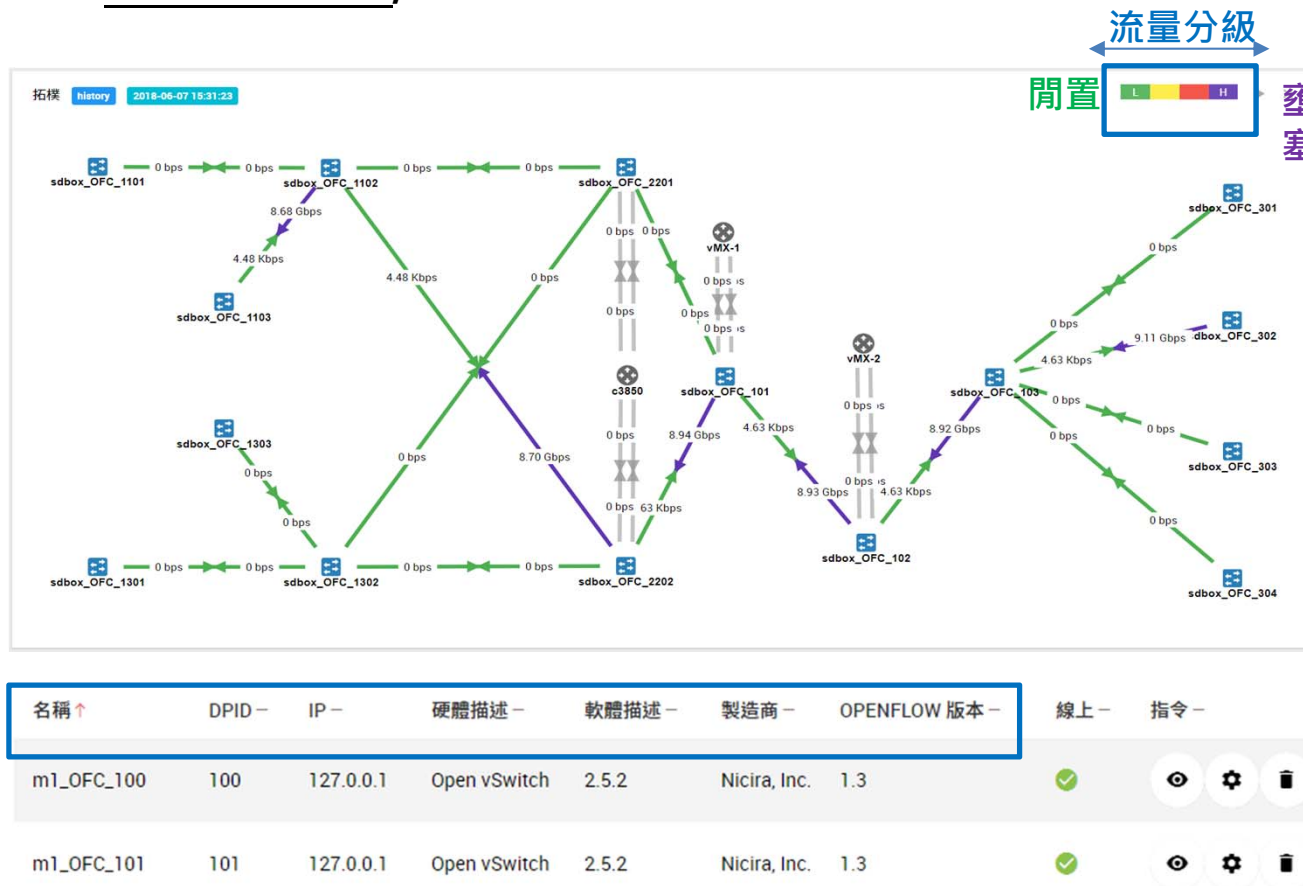
時間	訊息
2018-07-18 13:23:28	User [None] LOGIN_FAIL
2018-07-18 13:22:12	User [None] LOGIN_FAIL
2018-07-18 13:16:41	User [None] LOGIN_FAIL
2018-07-18 13:15:27	User [None] LOGIN_FAIL
2018-07-18 13:14:35	User [sdbox] LOGIN from 10.144.169.41
2018-07-18 13:13:41	User [None] LOGIN_FAIL
2018-07-18 13:10:32	User [None] LOGIN_FAIL

2 EyeLAN網路管理(2/2)

How

SDN網路拓樸

- 顯示整體網路拓樸, 包括OpenFlow交換器資訊, 相連的實體埠(port)及相關Flow設定等
- 提供鏈路流量監看, 易於網路管理者掌握目前網路全貌

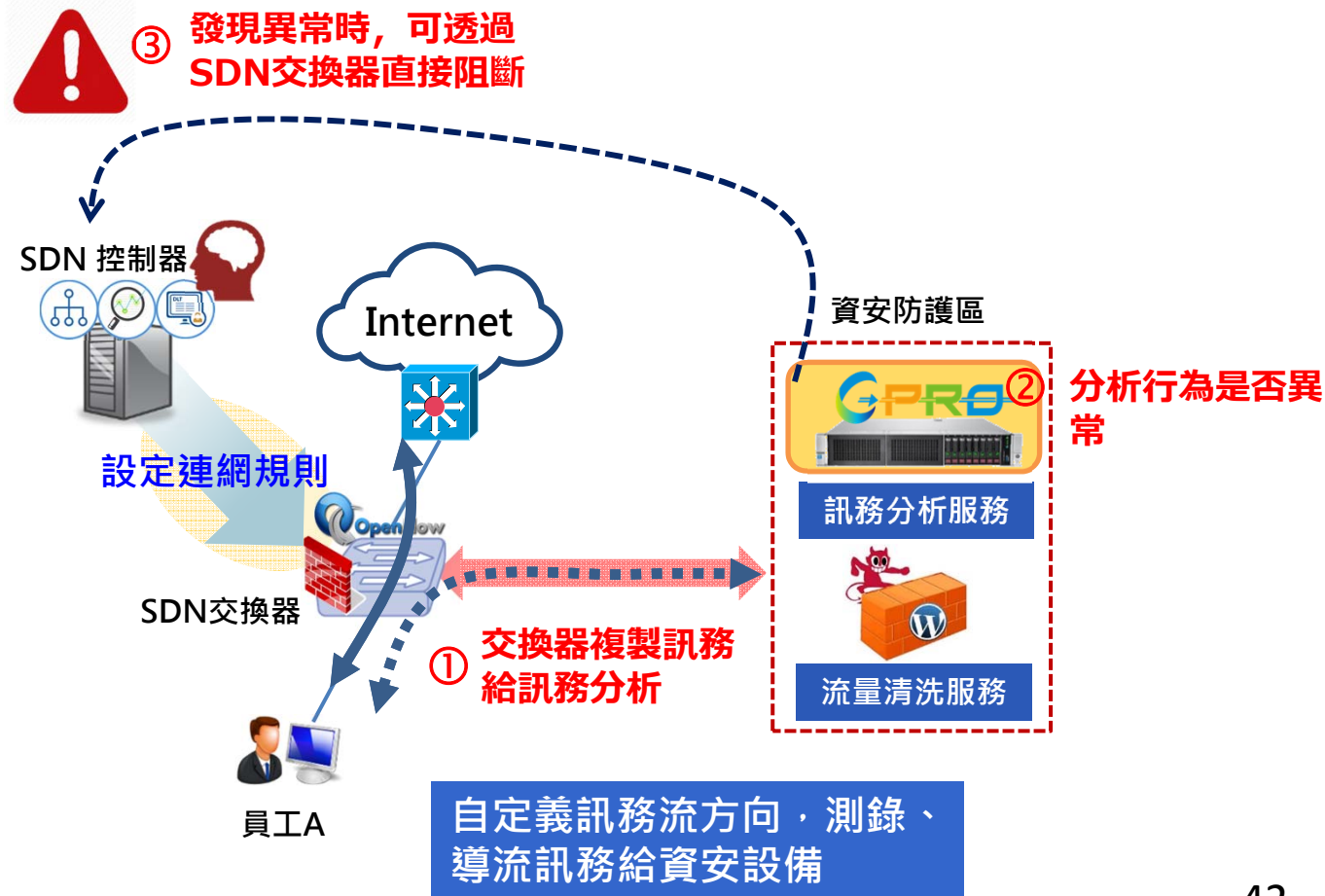


3 EyeLAN 整合資安設備

How

結合資安設備與SDN設備，進行資安聯防

異常流量管理：導流訊務給資安設備測錄，當發現有異常流量則可以由網管人員決定是否阻擋





中華電信
Chunghwa Telecom

感謝聆聽 敬請指教