旁路交換器助陣，利用網路可視性 (Network Visibility) 平台打造多層資安防禦機制

Silicom Ltd.
Connectivity Solutions

PacketX
Software Defines Monitoring

辰亞科技
Zenya Technology

March 2018

Prepared by
Bryan Huang

概說

- 過去，企業投資了很多資安防禦與效能分析工具，因為：
  1. 頻傳的網路攻擊，或駭客事件讓人擔心。。。
  2. 網路效能，影響企業營運績效更深。。。

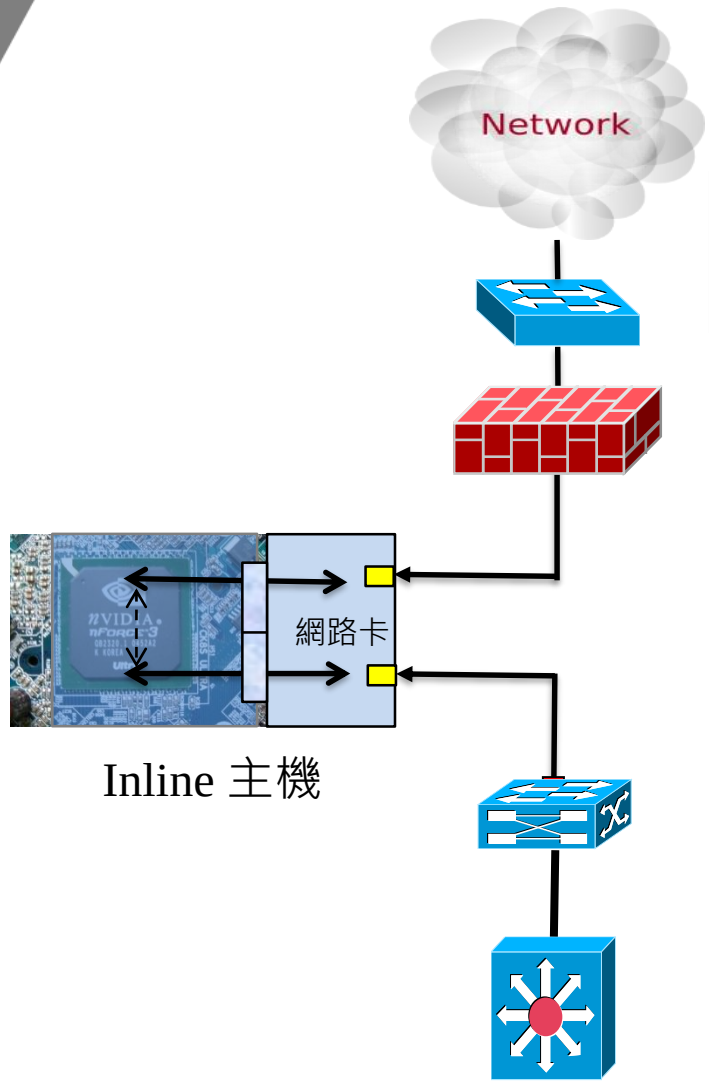
但是...是否想過...

- 部署資安防禦工具的隱憂
- 是否讓防禦與分析工具效率最大化

Objective

- 概說
- 佈署資安設備的隱憂
- 如何利用網路可視性打造多層架構防禦
- 為何需要**Silicom**智慧型**Bypass Switch**
- **Silicom**原廠簡介
- **PacketX**原廠簡介**(PacketX**技術長**)**
- 以網路可視化平台**(Network Visibility Platform)**為樞紐之網路安全設備佈署策略**(PacketX**技術長**)**
- **Question?**

透通模式的監控設備，有效阻隔攻擊或監控



IPS
DDoS

WAF
NG
Firewall

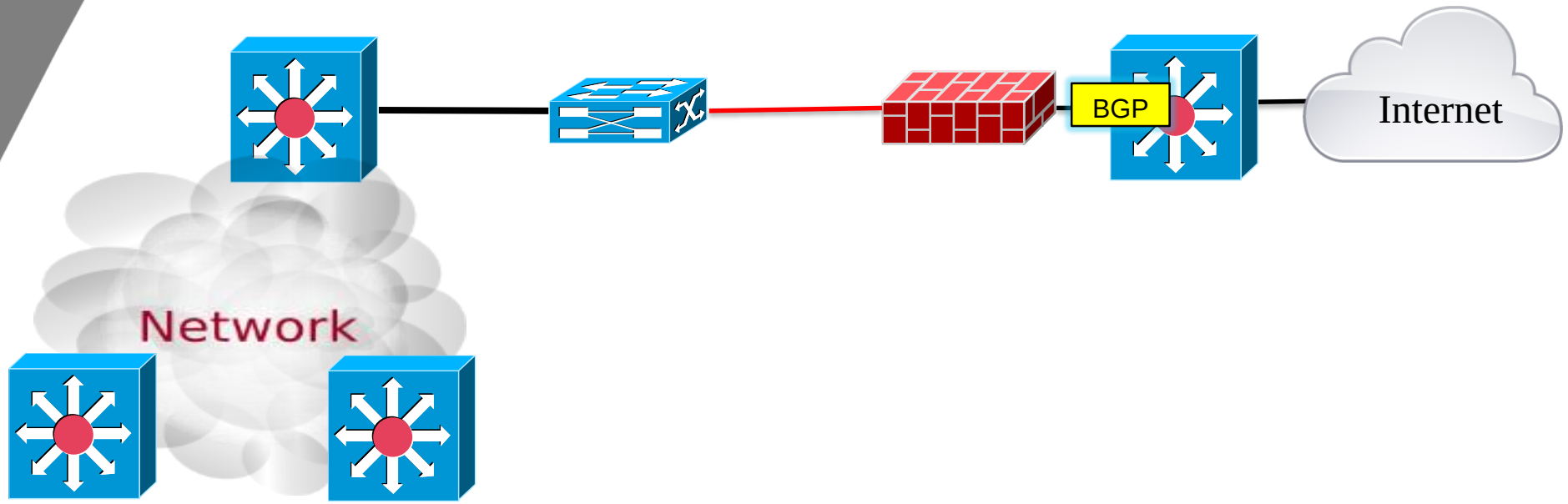
DAM
SSL Proxy

PCEF
DPI網路
行為分析

cisco
SOURCEfire
paloalto networks
the enterprise security company
McAfee
Together is power.
TREND MICRO
WatchGuard
f5
CITRIX
radware
ARBOR NETWORKS
The Security Division of NETSCOUT
IMPERVA
FORCEPOINT
A10
BLUE COAT
IMPERVA
IPOQUE
Networks
Secure Networks at Layer-7
AllOt
communications
sandvine
PROCERA

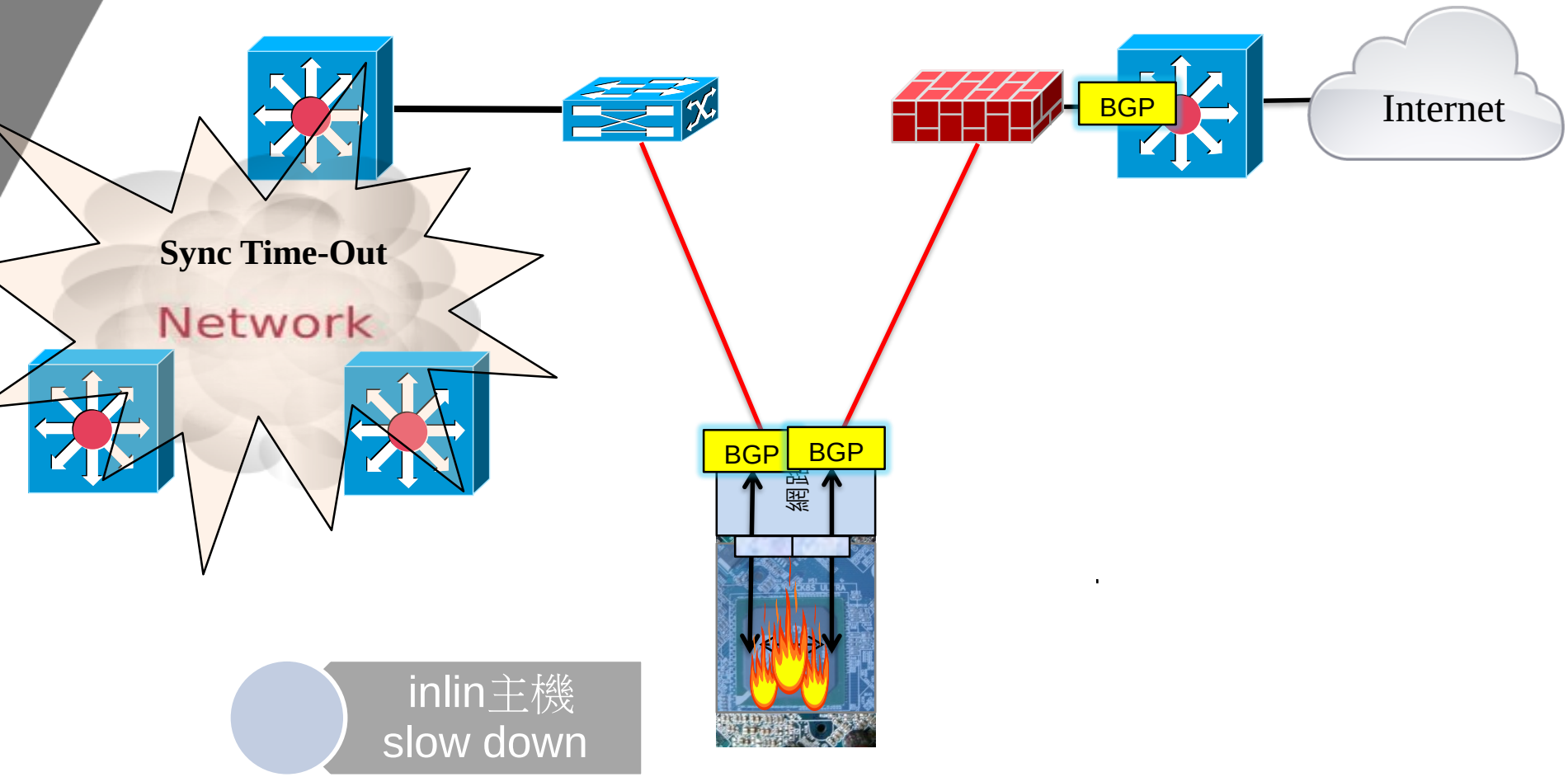
隱憂一：透通設備Bypass 網路卡防護盲點

隱憂二： BGP/OSPF – Synchronization



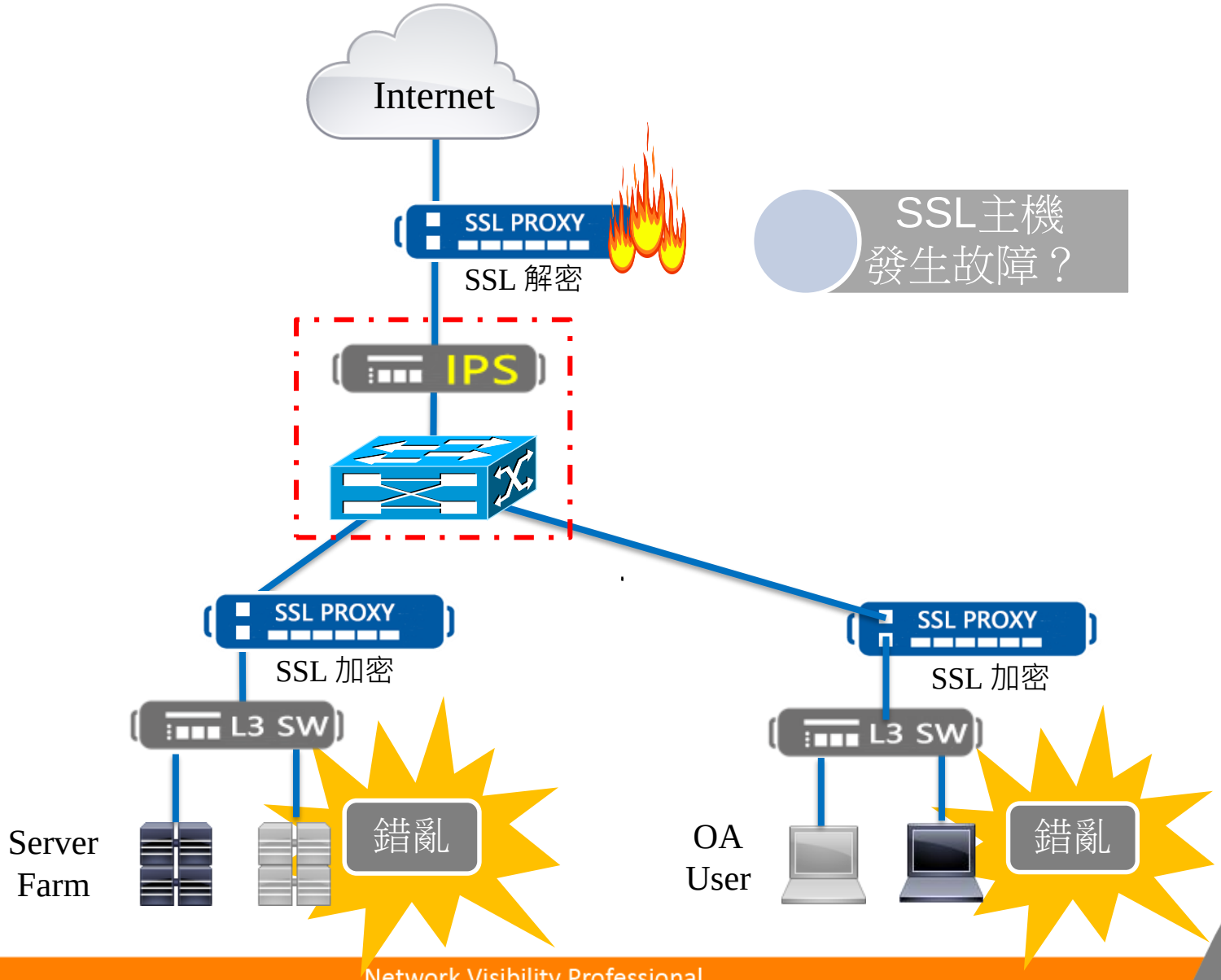
Inline 主機

隱憂二： BGP/OSPF – 同步失敗

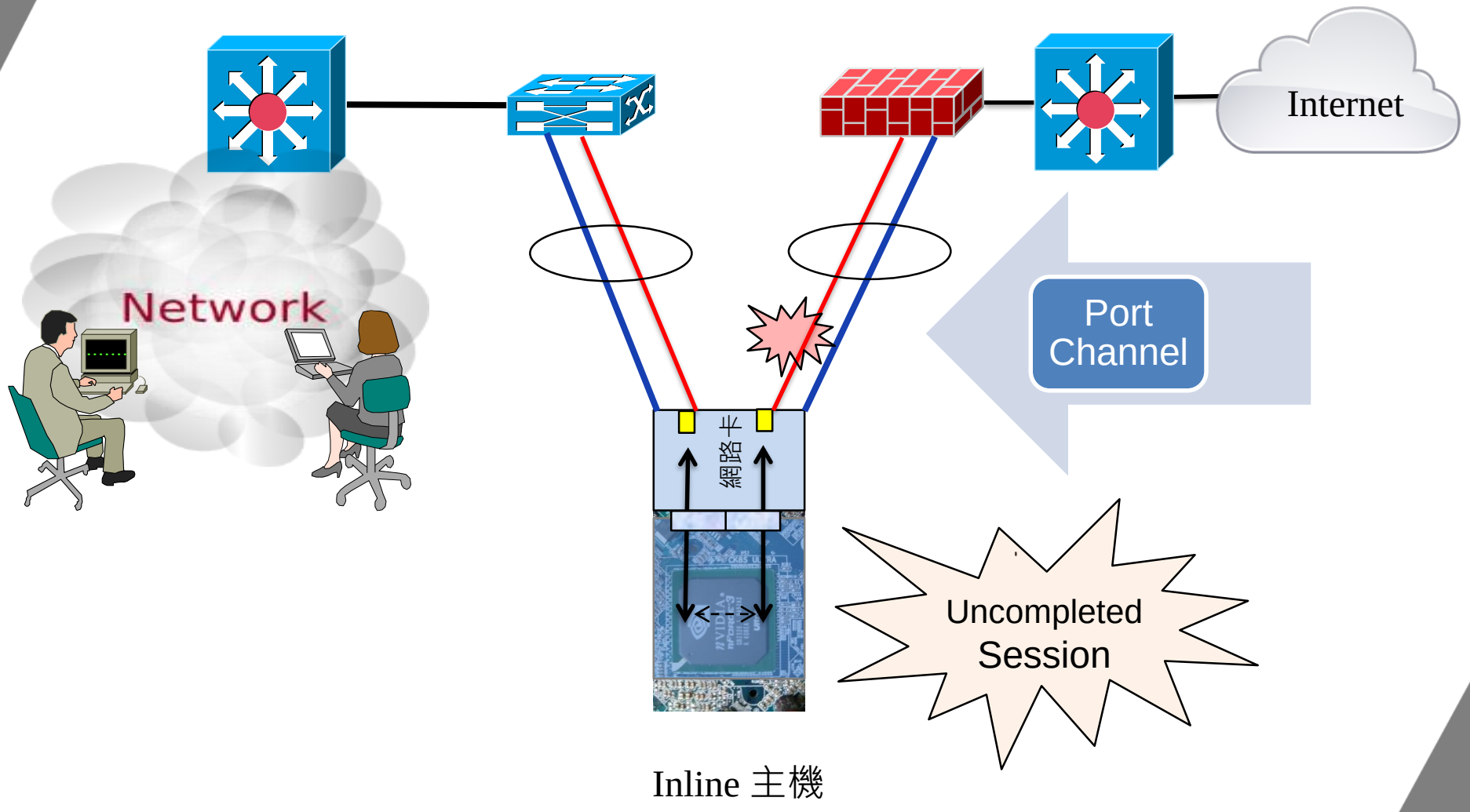


Inline 主機

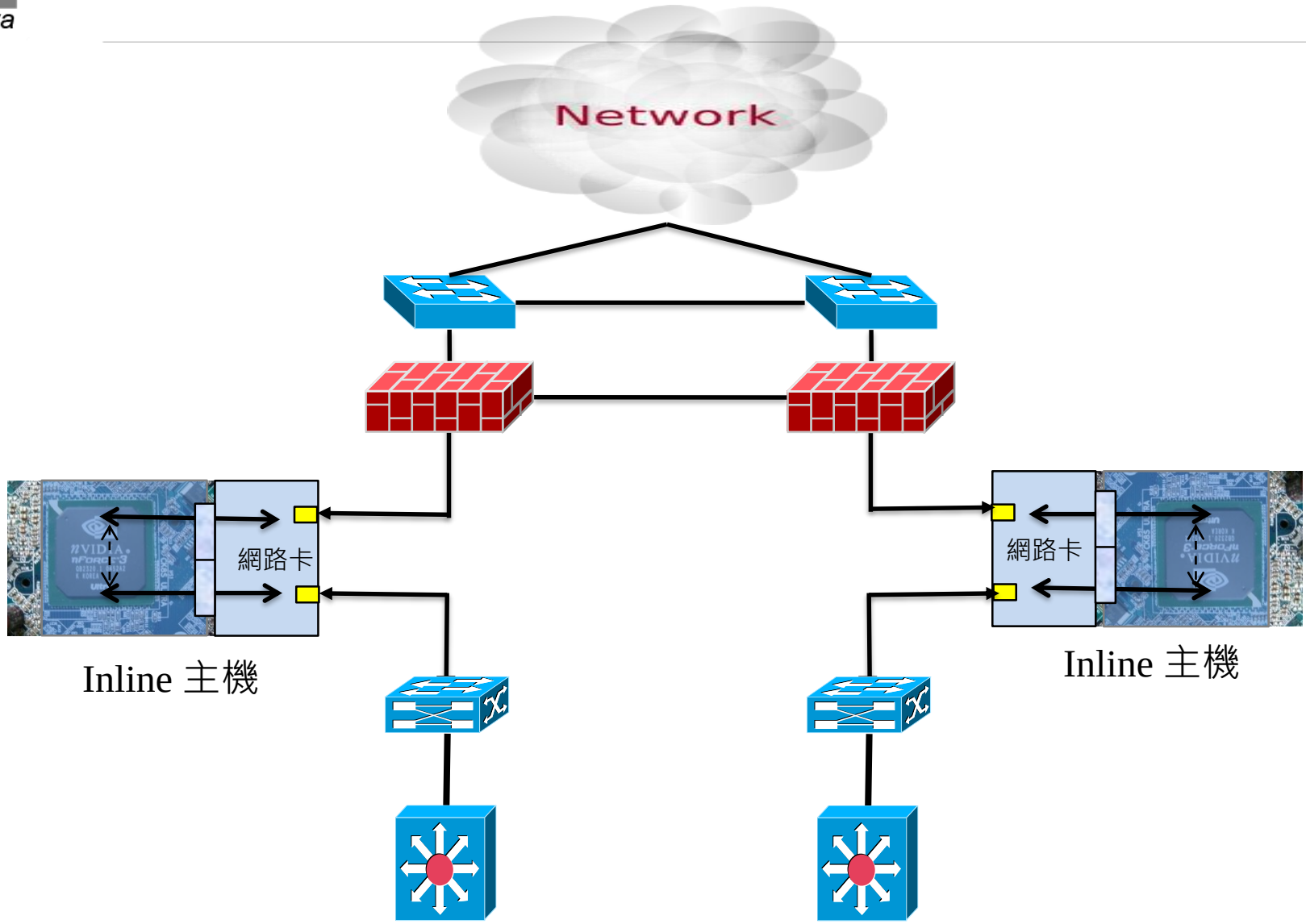
隱憂三：佈署多套 SSL 解密設備



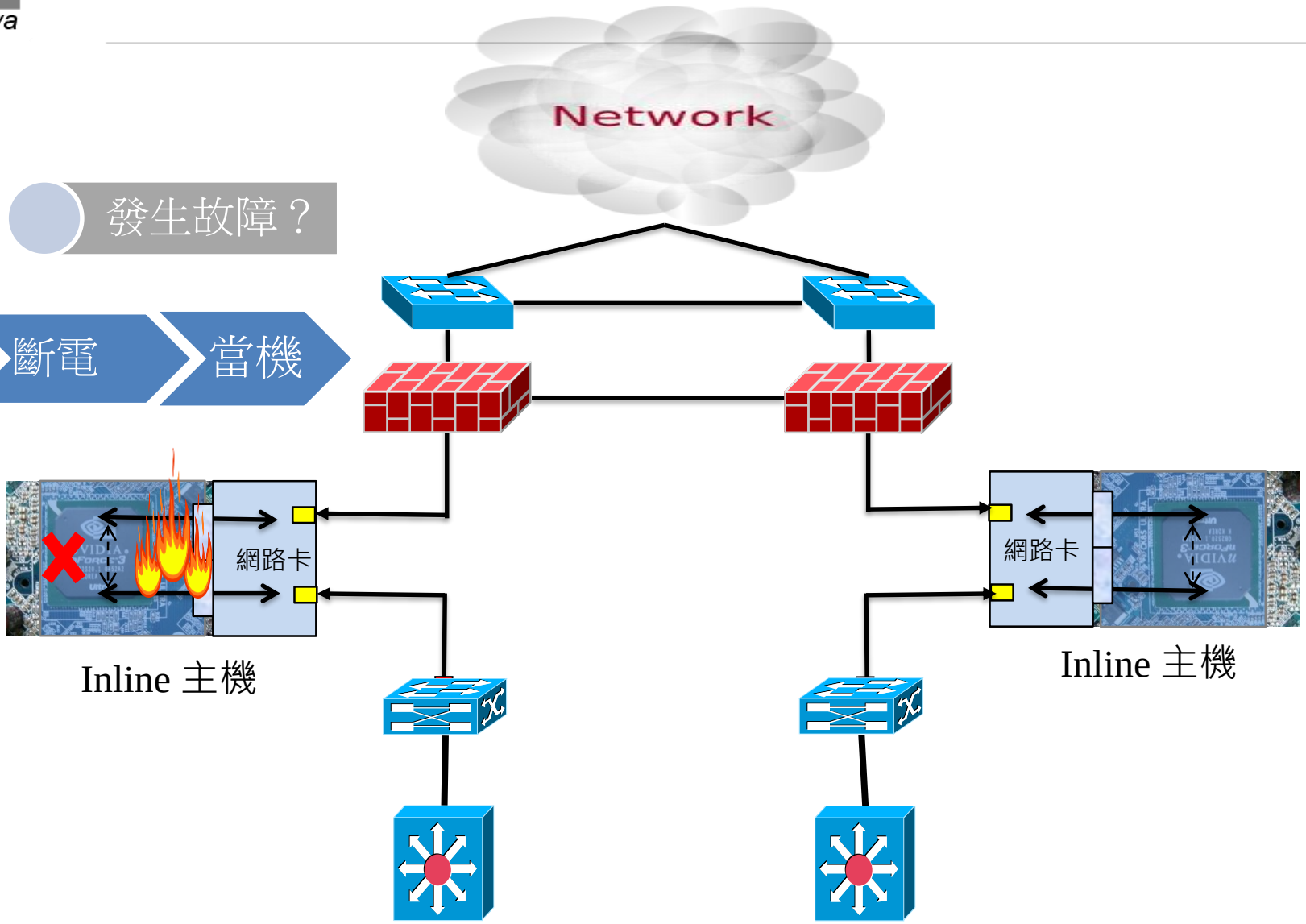
隱憂四：Port Channel下的inline裝置斷線防護機制？



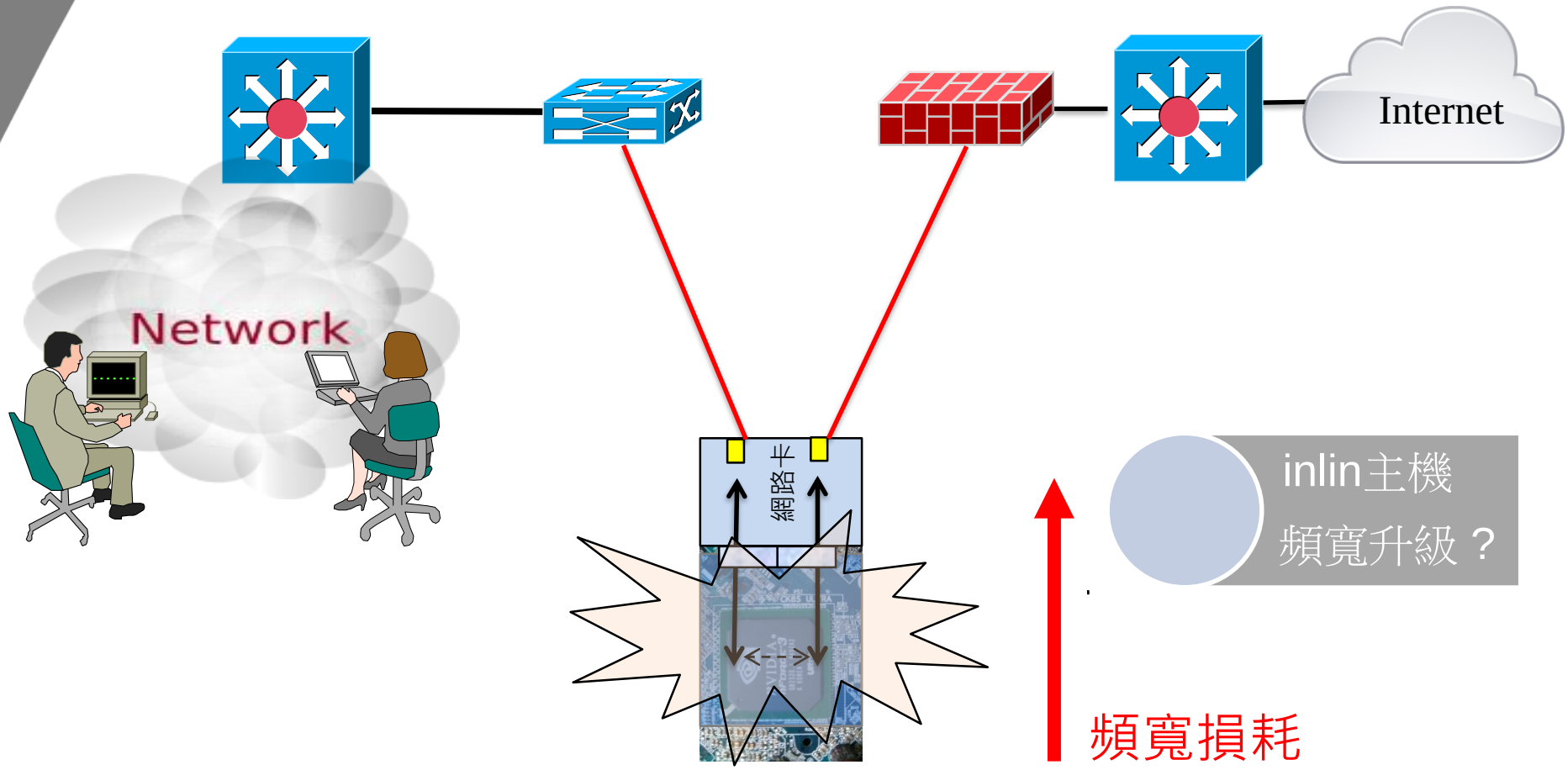
隱憂五：HA架構的盲點



隱憂五：HA架構的盲點 單邊失效路由卻未切換



隱憂六：浪費資源 - 不須檢查的封包佔據頻寬



Inline 主機

如何利用網路可視性打造多層架構防禦

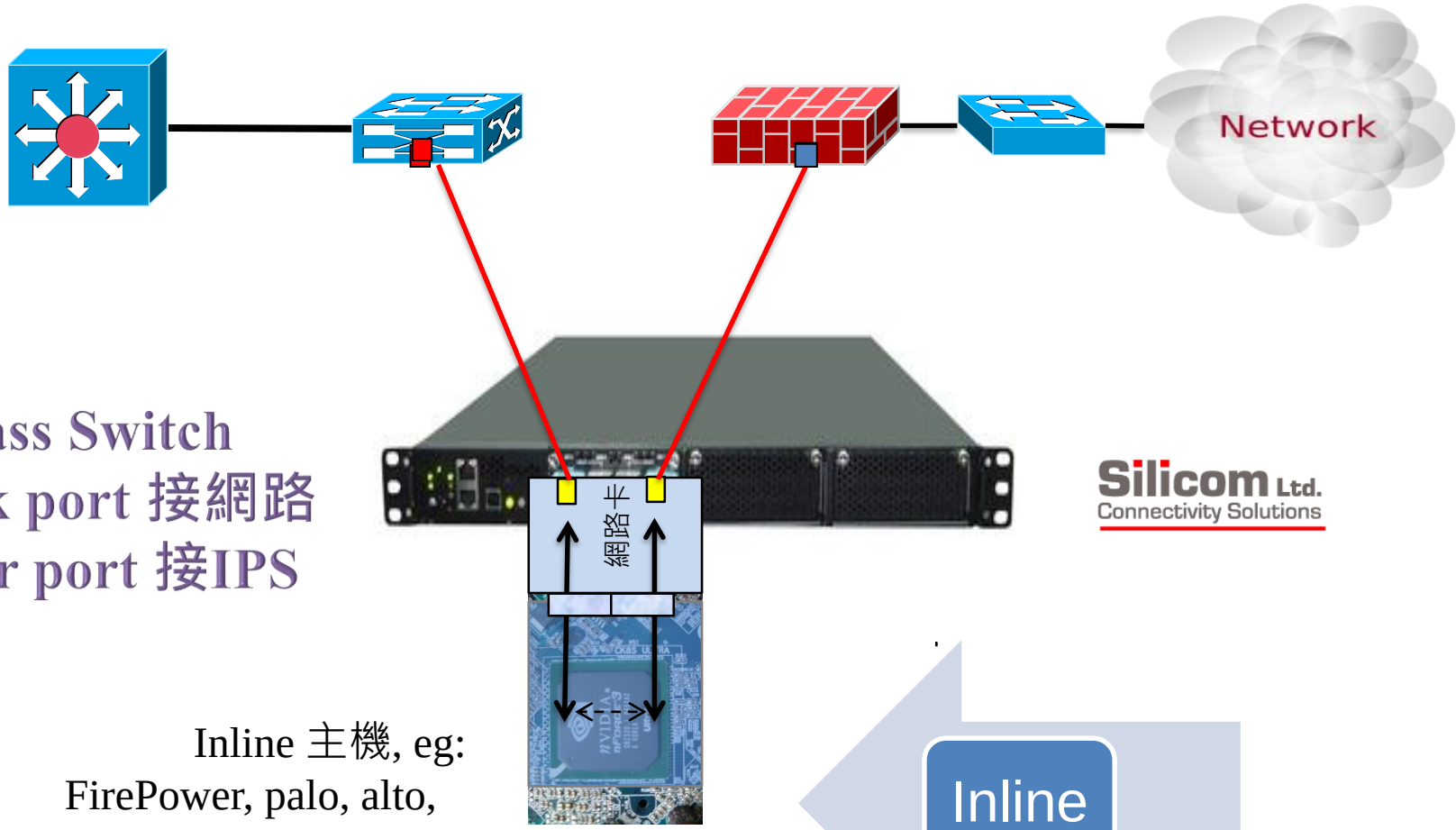
Bypass Switch與Network Packet Broker

Silicom Ltd.
Connectivity Solutions

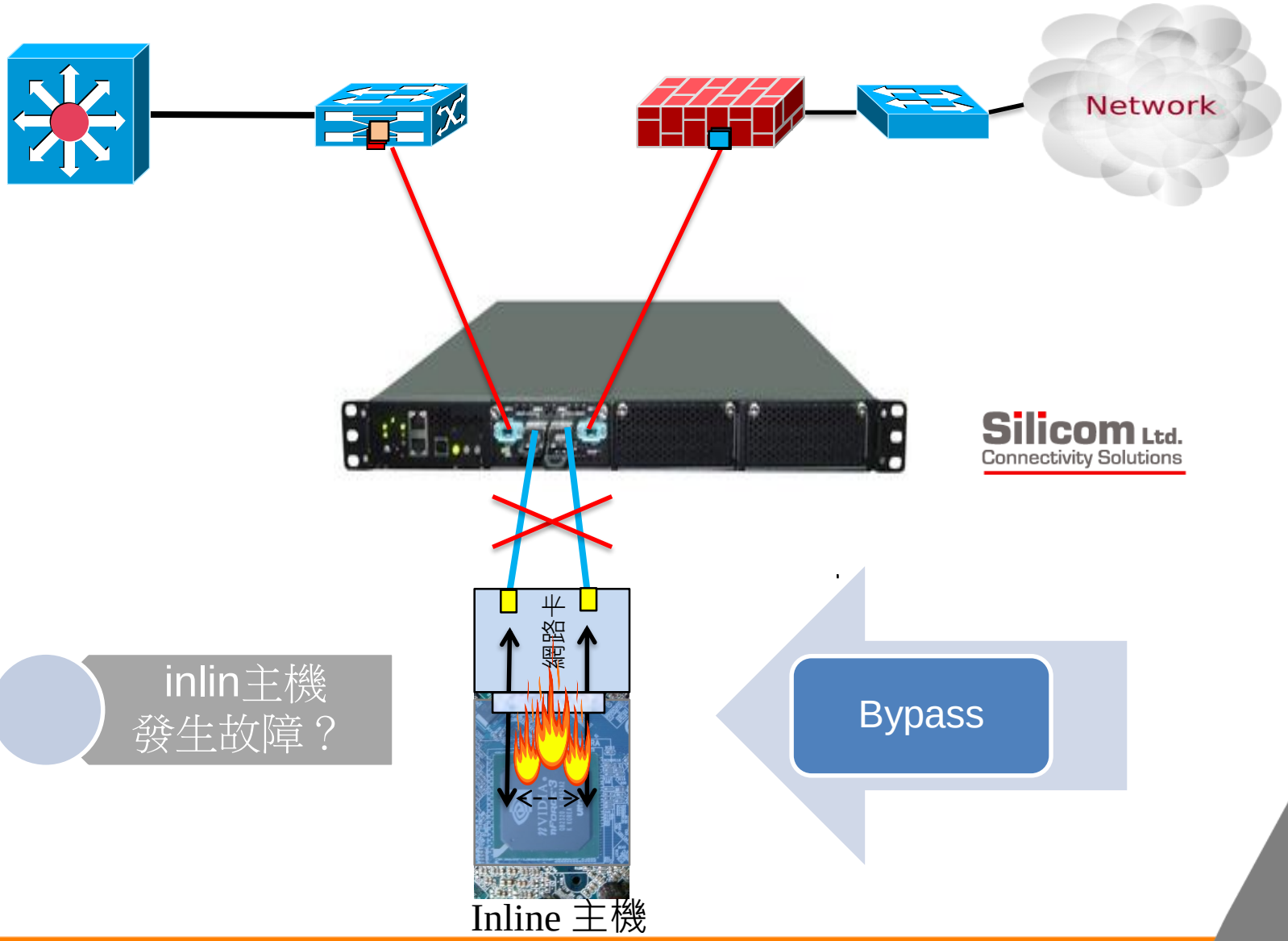
PacketX
Software Defines Monitoring

辰亞科技
Zenya Technology

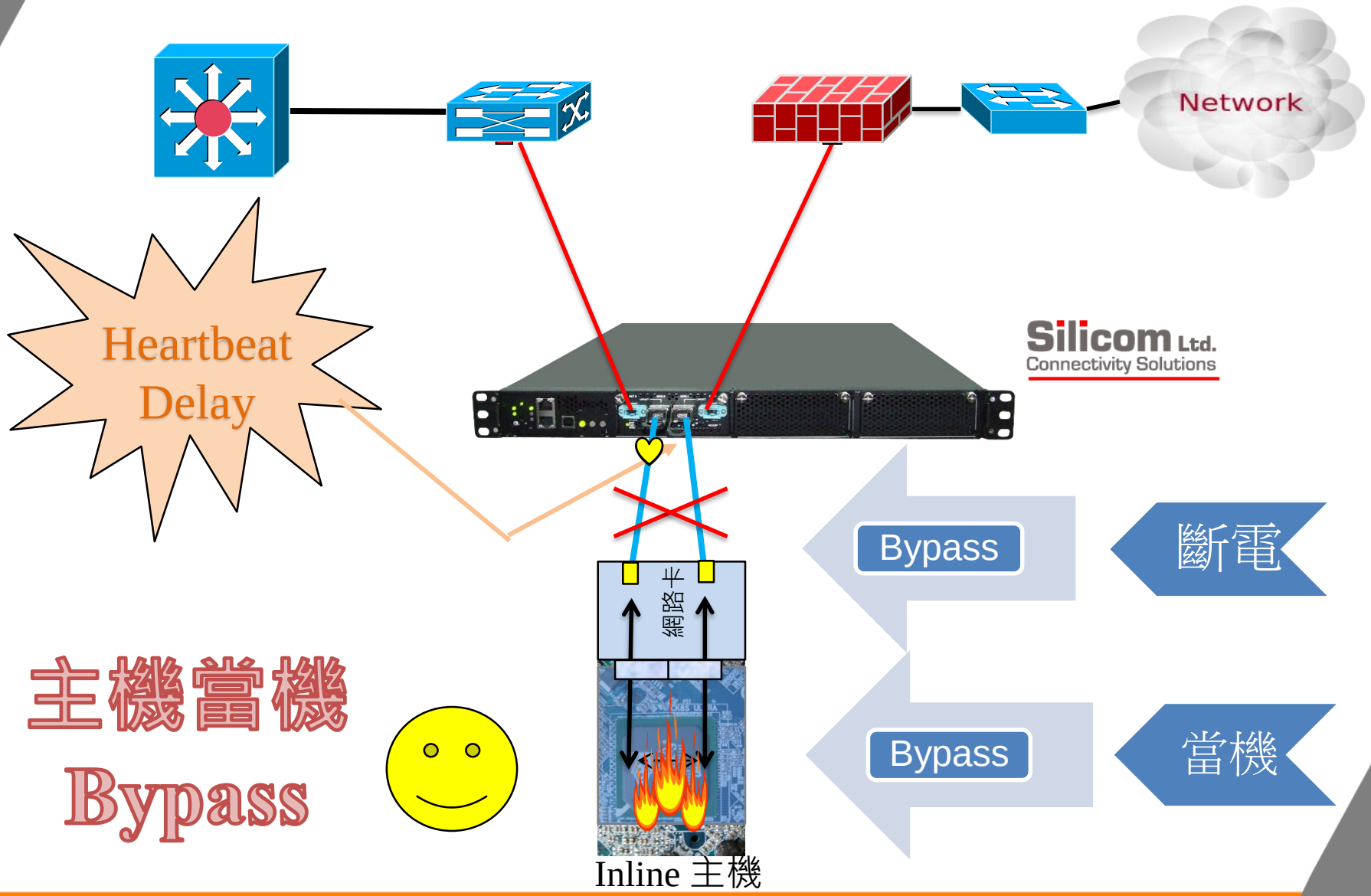
Silicom Bypass Switch連接架構圖 – Inline mode



Bypass Switch連接架構圖 – Bypass Mode



Silicom 智慧型旁路 – Healthy Check

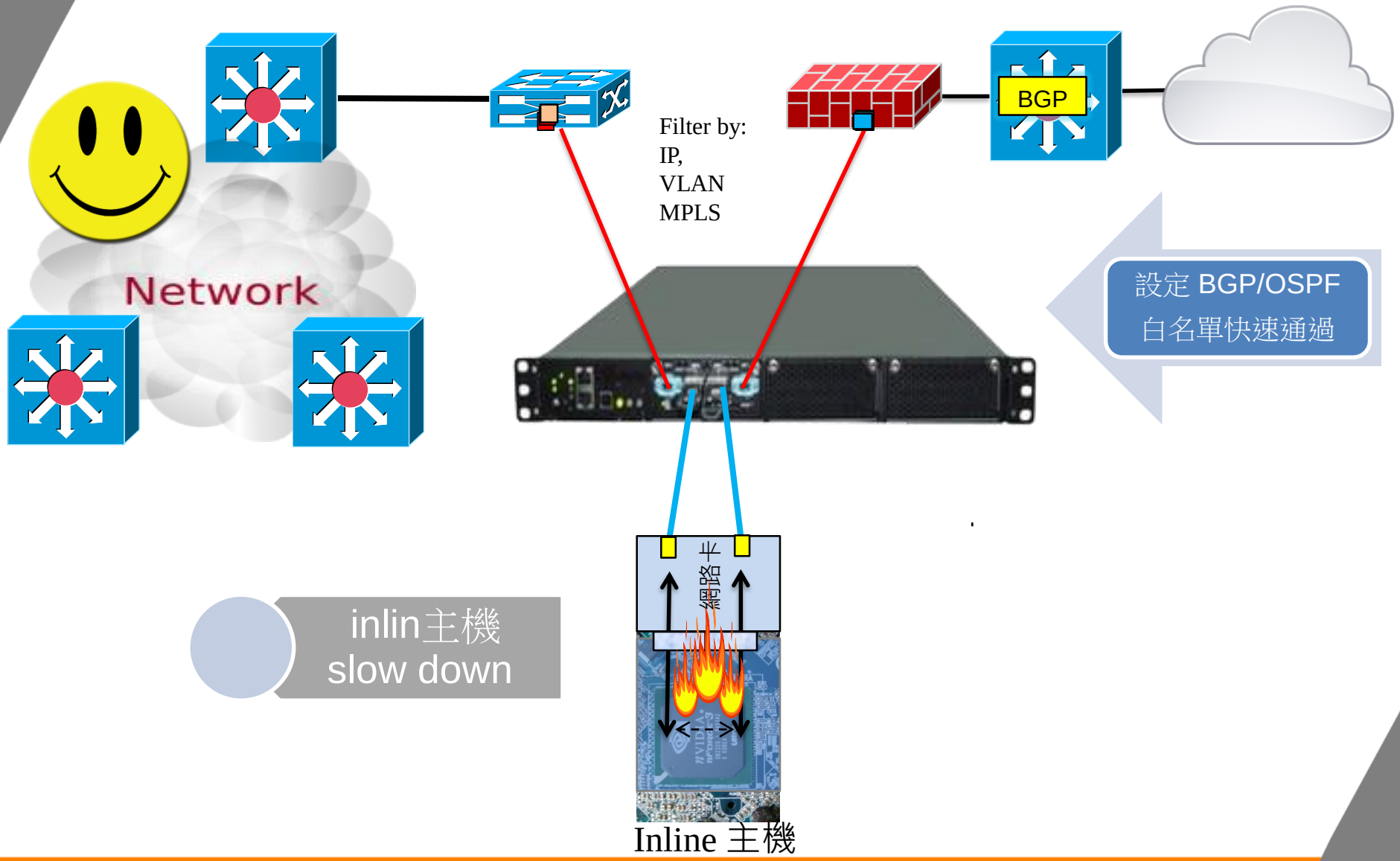


目前主流的Bypass方式 - 智慧型

- **獨立於In-Line設備之智慧型旁路交換機 (Intelligent Bypass Switch)**
  - 優點：同時具備硬體/軟體bypass，不管是設備斷電、系統/軟體當機，都能有效啟動Bypass機制，且獨立地由外部Heartbeat封包跟隨流量進行healthy check，無In-Line設備廠牌匹配問題。
  - 缺點：？？

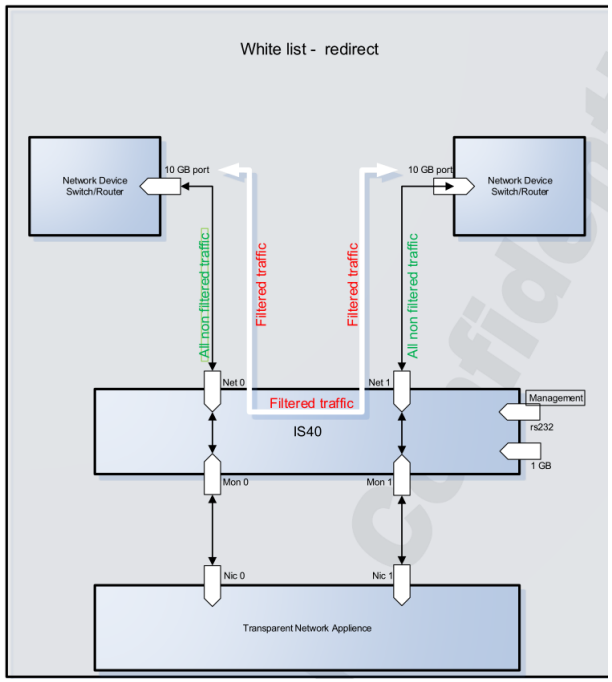
Silicom Ltd.
Connectivity Solutions

BGP/OSPF – Selective Bypass Filter

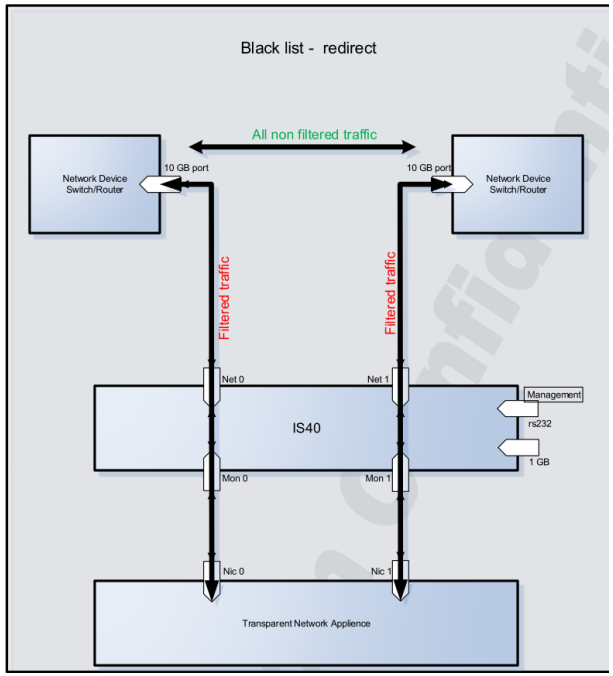


Silicom – Selective Bypass Filter

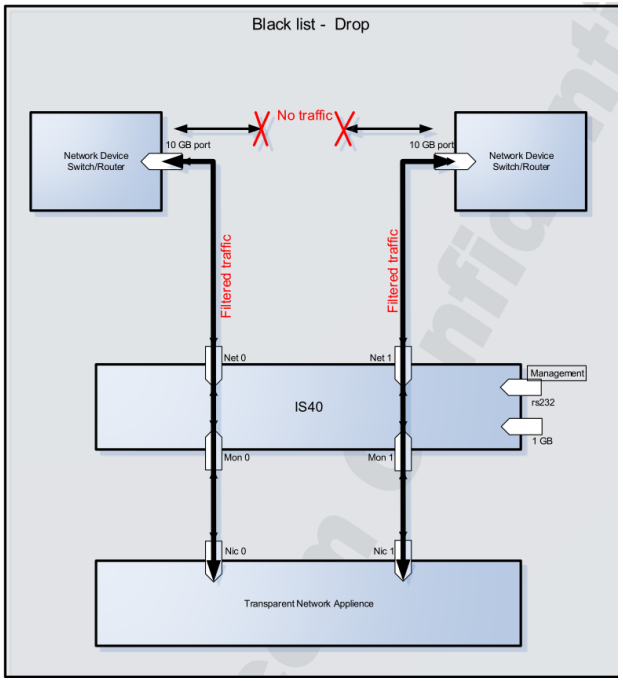
白名單放行



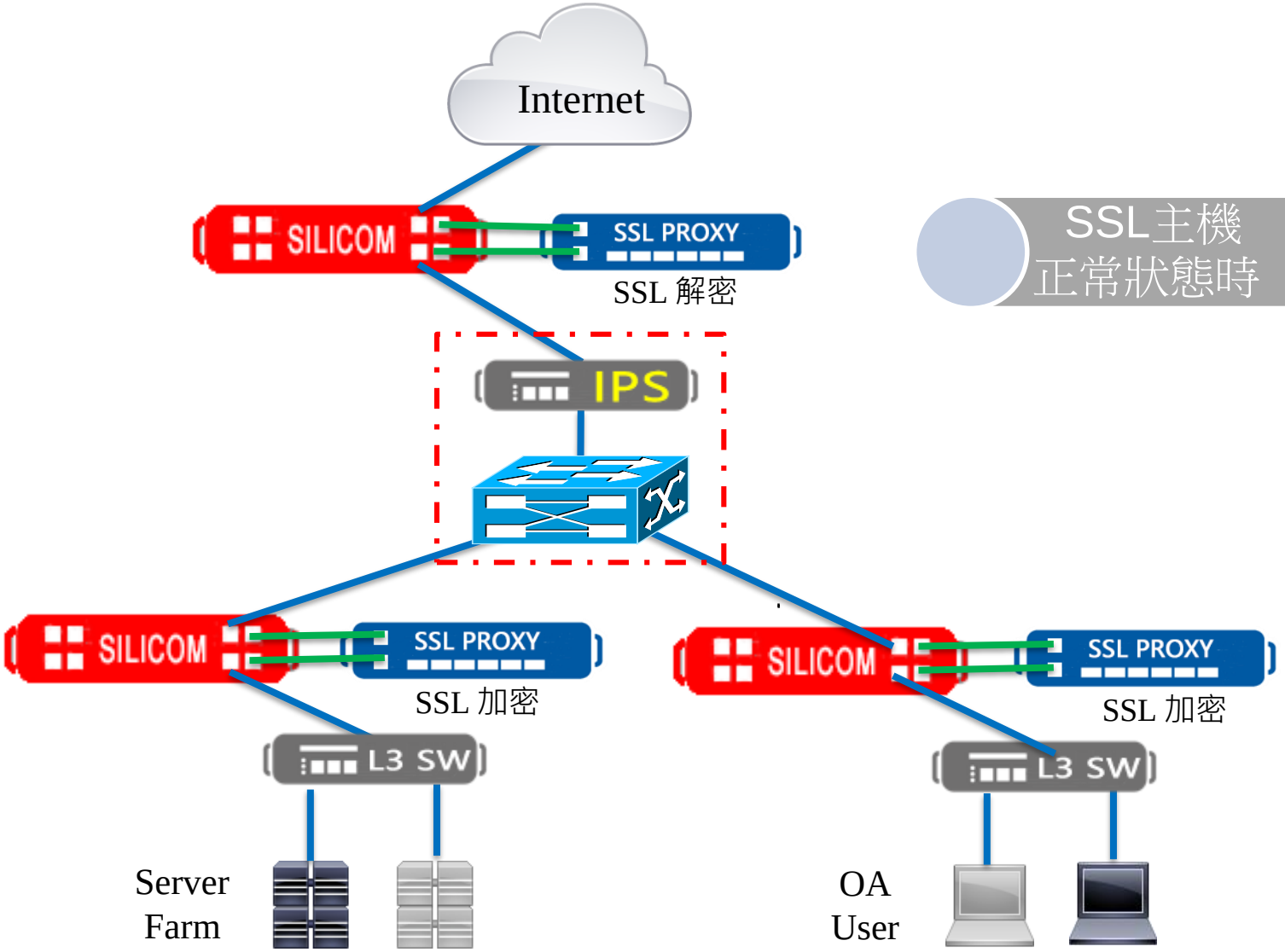
黑名單檢測
其餘放行



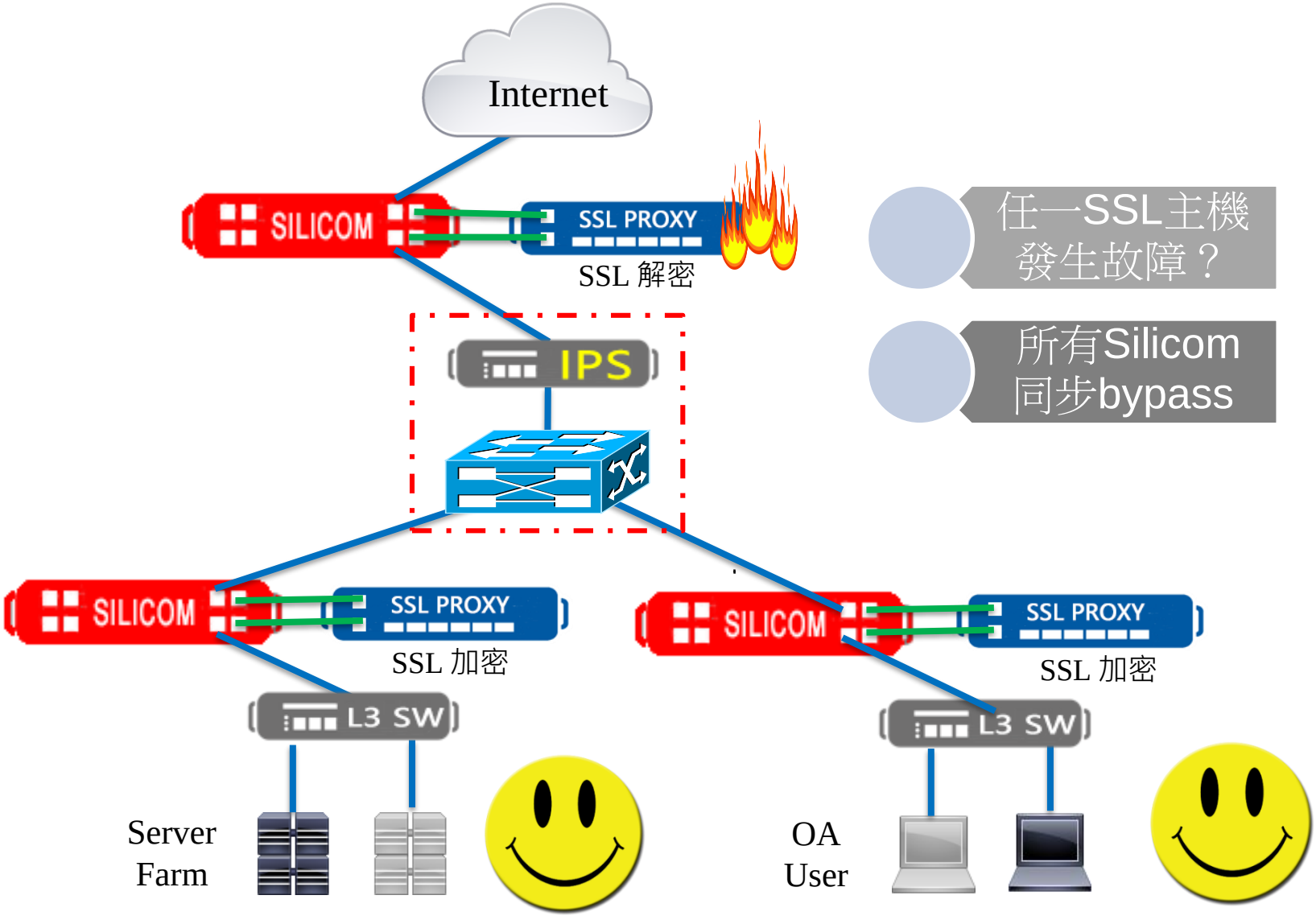
黑名單檢測
其餘丟棄



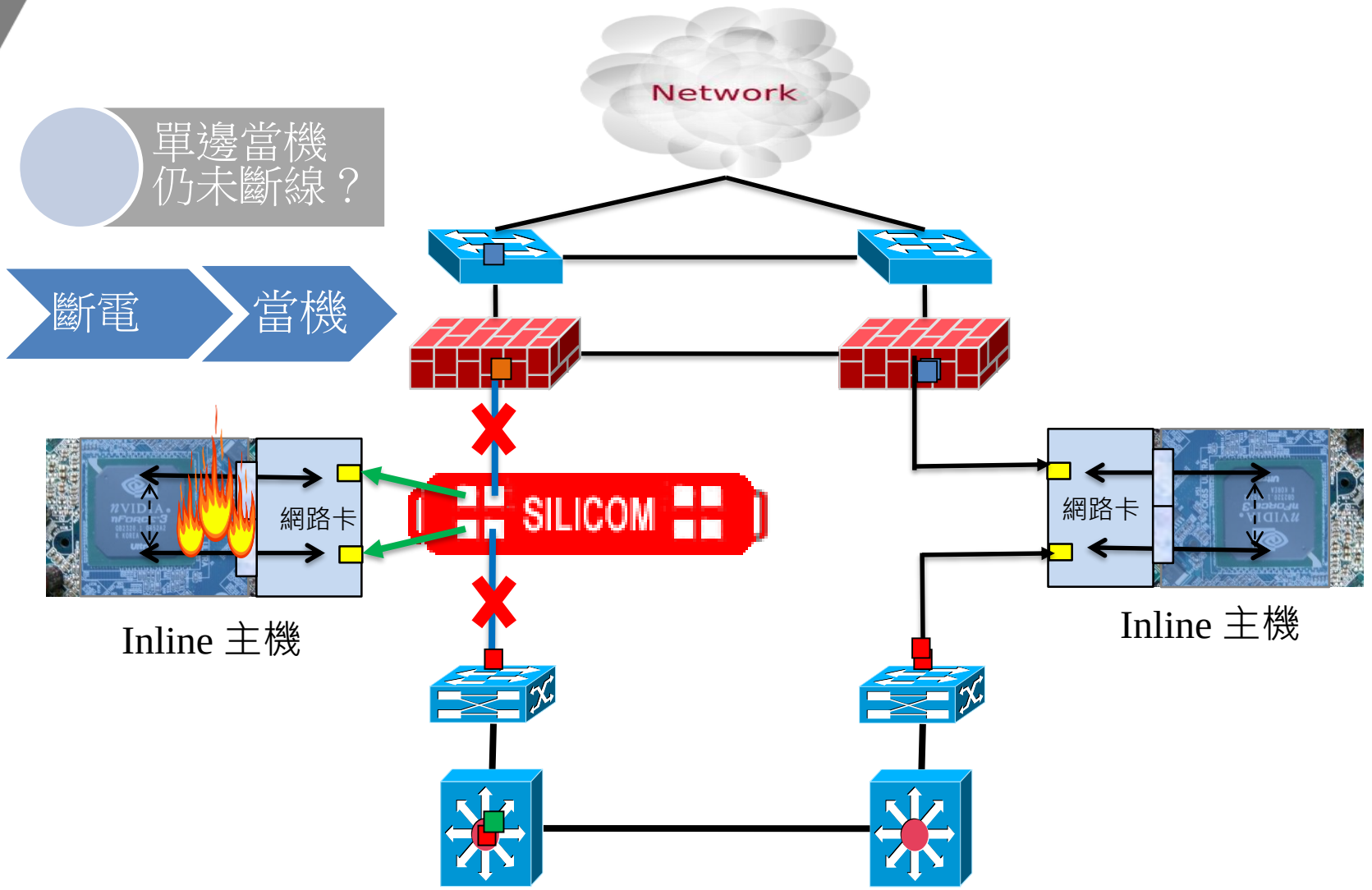
同步inline/bypass：佈署多套 SSL 解密設備 (一)



同步inline/bypass：佈署多套 SSL 解密設備(二)



HA架構的盲點：單邊當機，自動強迫故障主機離線



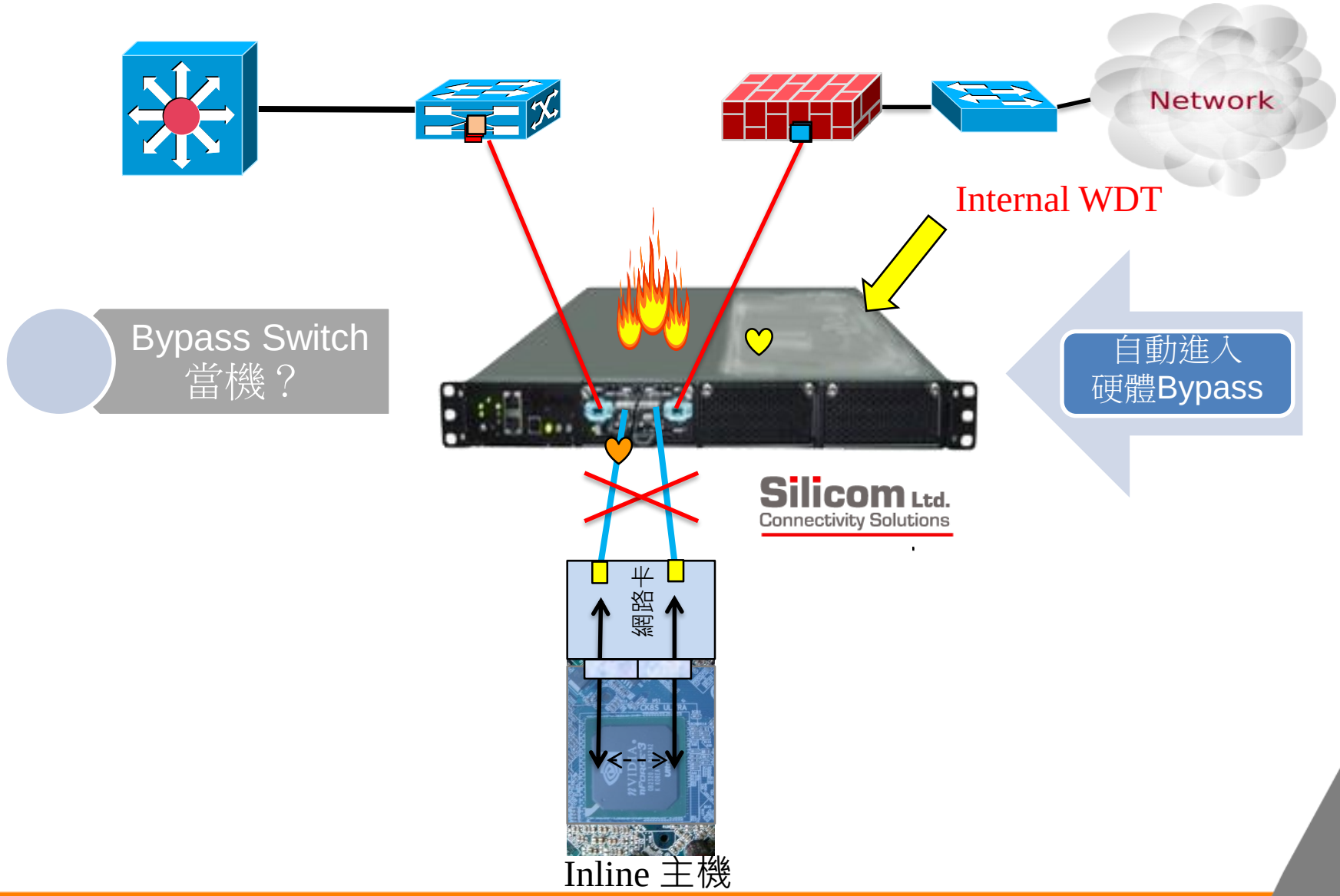
主動式 Active Bypass 時機 (智慧型)

- **Inline 主機 Link Loss**
  - 斷電
  - 拔線
- **Heartbeat Packet Hold Time Expired**
  - 主機應用程式軟體故障
  - 主機當機

Passive Bypass 時機

- **Bypass Switch 斷電**
- **Internal Watch Dog Timer expired.**

Internal WDT內部看門狗 – Double Safe / Double Bypass 使Silicom不可能是故障點



原廠簡介

Silicom Ltd.
Connectivity Solutions

PacketX
Software Defines Monitoring

Silicom

- 高效能伺服器介面卡、**Bypass**技術、網路設備業界領導廠商
- 成立於**1987**年.
- 總公司、研發中心、設備製造工廠位於以色列，美國分公司位於**New Jersey.**
- **RAD**控股集團成員之一
- **1994**於**NASDAQ**股票公開發行上市，**Dual Listing in Israel since 2005.**
- **21** 年以上網路產品製造經驗。
- 許多世界級網路設備領導廠牌，是策略性夥伴

Our Sales Model

- **Trusted OEM supplier to 90+ customers,**
- **including many market leaders**

Network Appliances	WAN Optimization	Internet Security	Application Delivery	Network Monitoring
Market Leaders	▪ Riverbed ▪ Citrix ▪ Blue Coat ▪ Silver Peak ▪ Cisco	▪ Checkpoint ▪ Cisco ▪ Juniper ▪ McAfee ▪ Symantec ▪ Trend Micro	▪ F5 Networks ▪ Citrix ▪ Radware	▪ Netscout ▪ Riverbed ▪ Opnet (Riverbed) ▪ Niksun

Exploding data and Internet traffic dramatically increase the need for connectivity & bandwidth - and the use of Network Appliances.

代表客戶

- 教育
  - 台灣大學
  - 國家高速網路中心
  - 政治大學
  - 交通大學
  - 中央大學
  - 暨南大學
  - 逢甲大學
  - 靜宜大學
  - 台灣藝術大學
  - 台北商業大學
  - 陽明大學
  - 新竹縣網
  - 台北大學
- 電信
  - 中華電信行動通信分公司
  - **Hinet**
  - 遠傳電信IDC
  - 台灣大哥大行通
  - 台灣之星
- 政府
  - **Taipei Free WiFi**
  - 世大運
  - 財政部資訊中心
  - 移民署
  - 中科院資管中心
  - 南投縣政府
  - 疾病管制局
  - 兩廳院
  - 經濟部
  - 台灣郵政公司
- 企業
  - 華碩電腦
  - 華亞科技
  - 南訊科技
  - 台灣電訊
  - 中佑資訊
  - 向上科技
  - 元大銀行
  - 台銀證券
  - 合作金庫
  - 森森購物
  - 國泰人壽
  - 中國信託

PacketX

- 成立於 **2013**，總部研發中心位於新北市中和區
- 主要成員**10**年以上**DPI**封包辨識、通訊監察相關領域。
- 客戶遍及電信商、國安領域、一般企業。
- 使用**Appliance**、**ATCA**平台
- **CAVIUM@ATCA**的電信網路應用

重要客戶列表

中華民國國家安全局
National Security Bureau, R.O.C.

中華民國外交部
Ministry of Foreign Affairs
Republic of China (Taiwan)

中華民國
財政部
Ministry of Finance, R.O.C.

新北市政府警察局
NEW TAIPEI CITY POLICE DEPARTMENT

中華電信
Chunghwa Telecom

NATIONAL KAOHSIUNG UNIVERSITY
OF HOSPITALITY AND TOURISM
國立高雄餐旅大學

國泰人壽
Cathay Life Insurance

NARLabs 國家實驗研究院
國家高速網路與計算中心

暨南大學
JINAN UNIVERSITY

國立宜蘭大學
National Ilan University

中國信託銀行
CTBC BANK

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

GIGABYTE

ADLINK
TECHNOLOGY INC.
凌華科技

T STAR
台灣之星

Taifo
Taiwan Intelligent Fiber Optic Network
台灣智慧光網

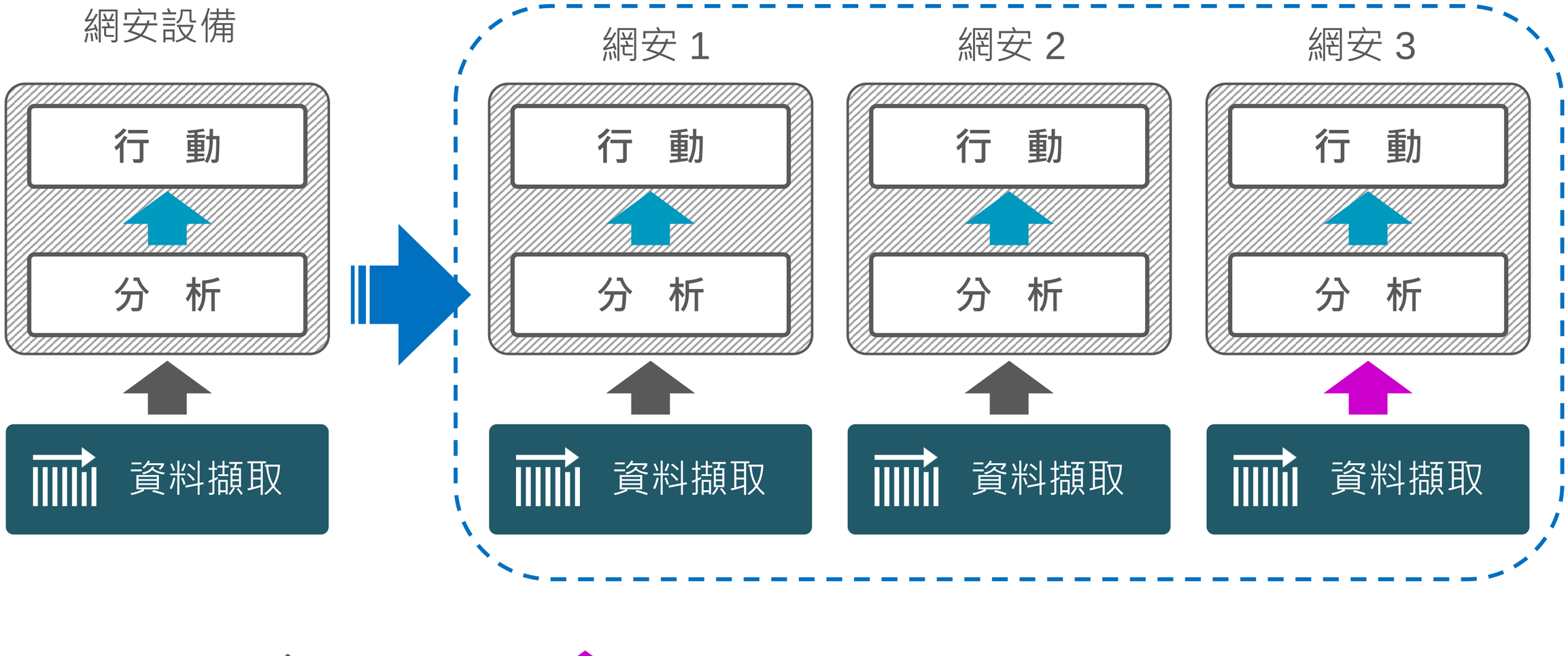
questions

Thanks

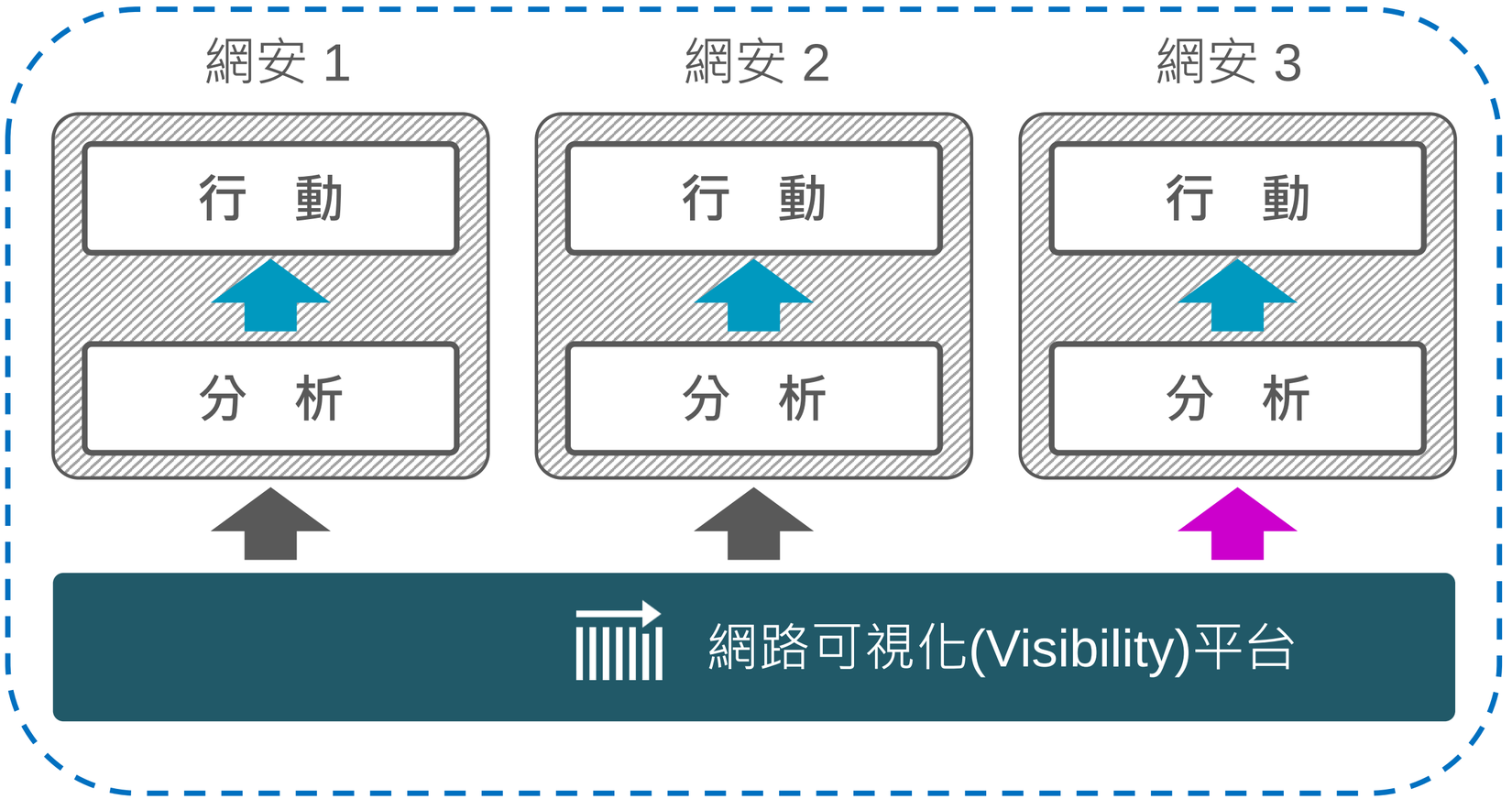
以Network Visibility Platform為樞紐之網路安全設備佈署方針

Speaker: Tony Wang
PacketX CTO

網路安全機制三部曲


網安設備
行　動
分　析
資料擷取
網安 1
行　動
分　析
資料擷取
網安 2
行　動
分　析
資料擷取
網安 3
行　動
分　析
資料擷取
原始資料(流量)
Metadata

進化後的資料擷取機制
Network Visibility Platform



Network Visibility的挑戰

1.流量持續成長
2.傳輸技術的創新: ex. SDN, VxLAN..
3.多種安全設備要同時運作

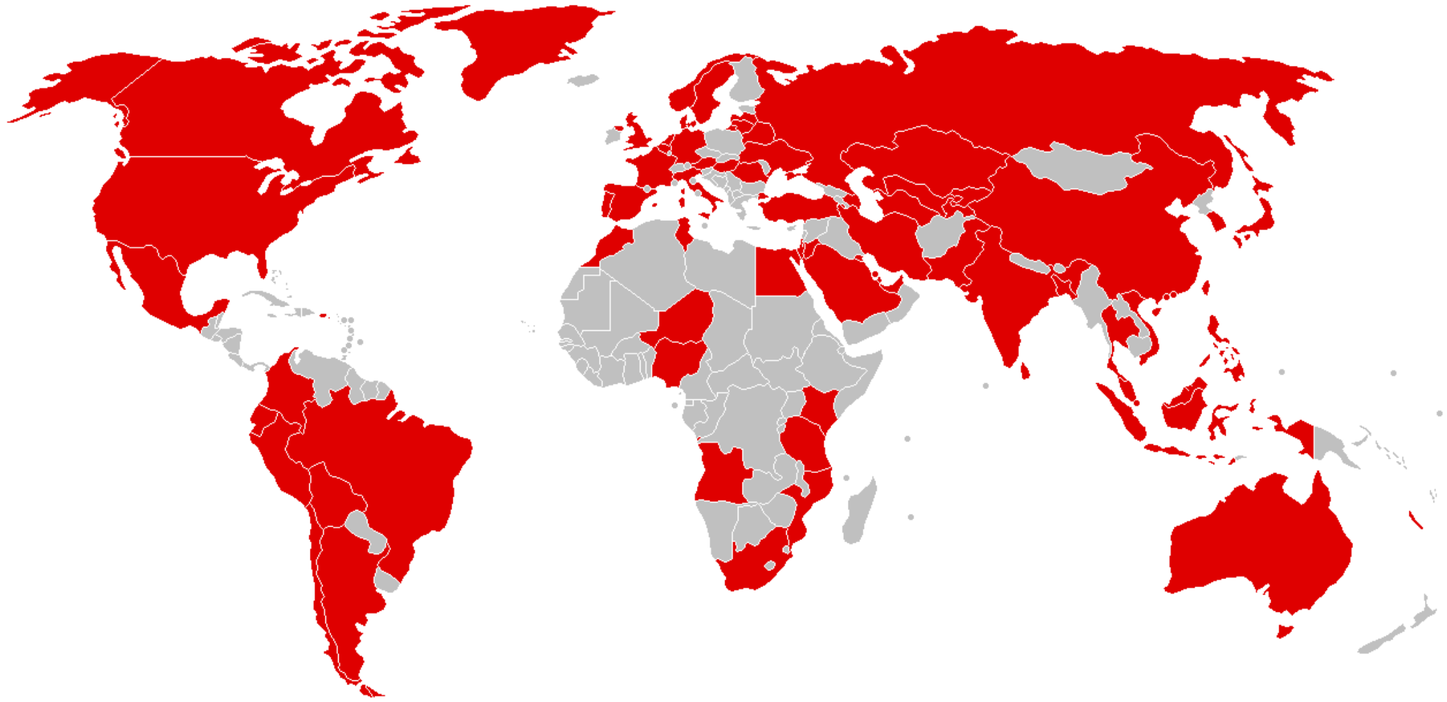
網路可視化(資料擷取)之複雜度遽昇
疏忽於此的企業，安全機制之可靠性與
效能恐將雙雙降級。

資安設備太弱 vs. 可視化不足

WannaCry 的啟示

公司員工中了WannaCry
難道他們的公司沒有Firewall/IPS
難道電腦上沒有防毒軟體

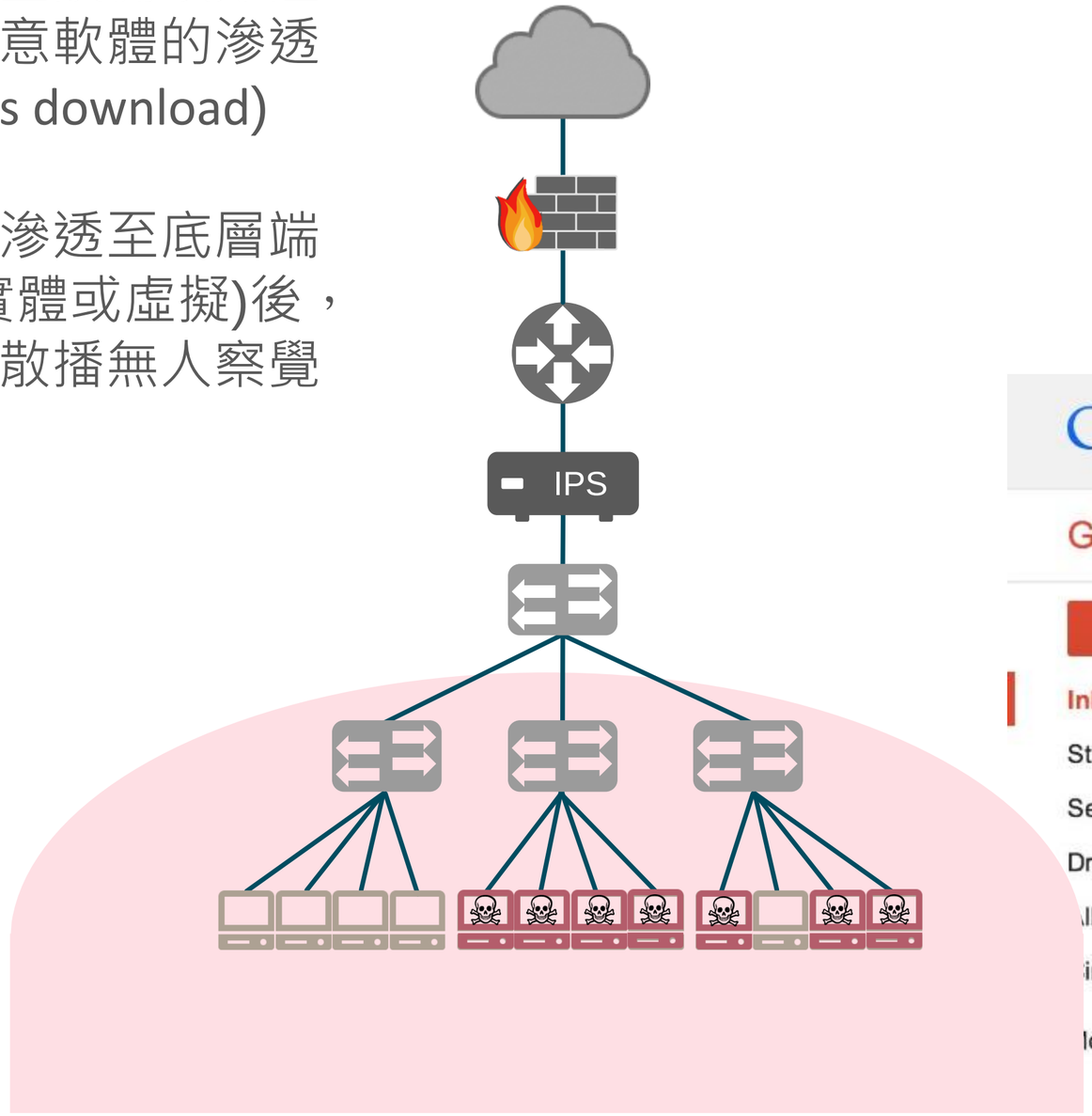
IT人員在惡意程式散播期間
竟沒有嗅到任何一絲不對勁?!

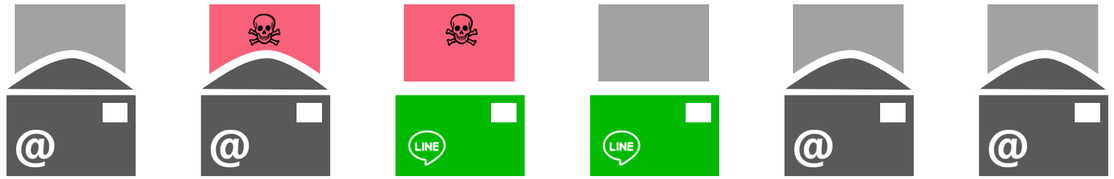


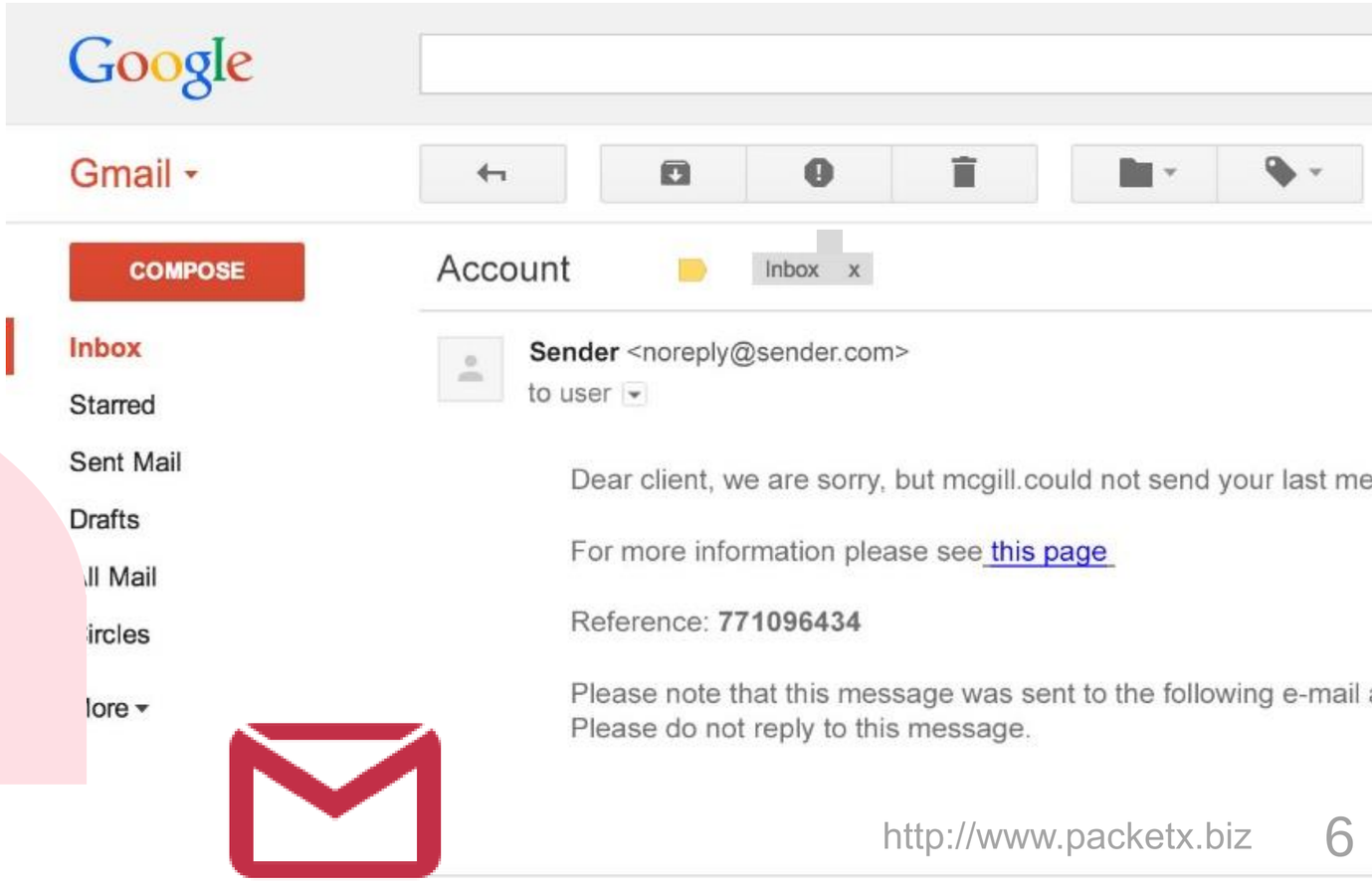
Source : Wikipedia

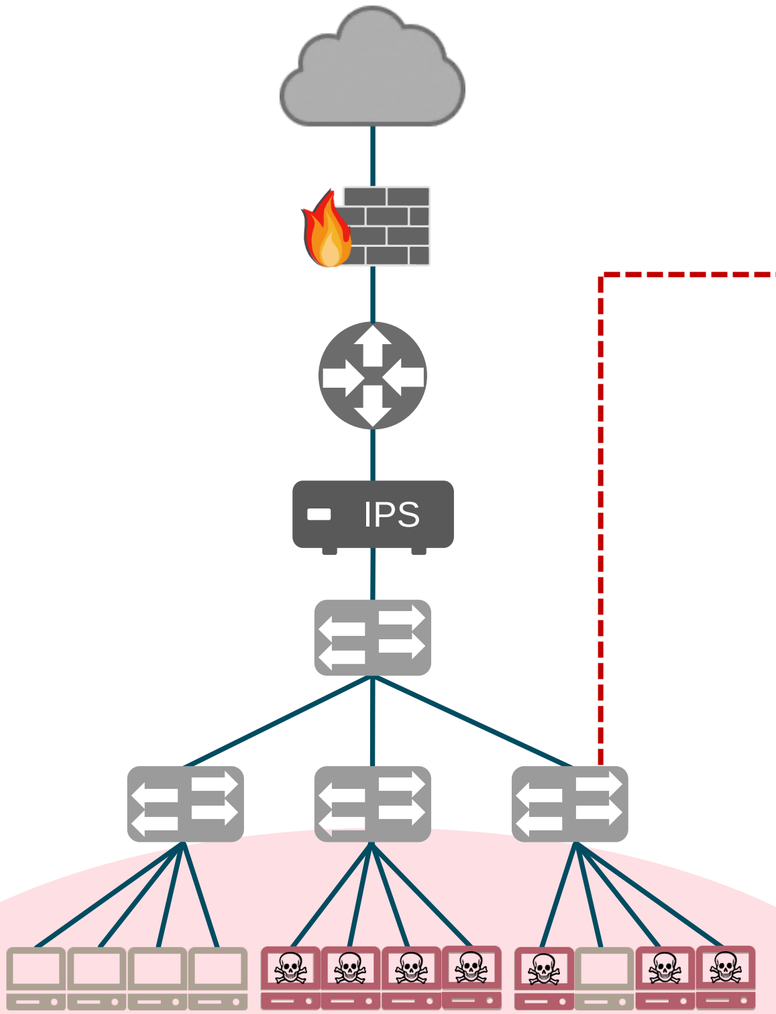
建置於入口端的網路安全設備很難阻擋惡意軟體的滲透(https download)

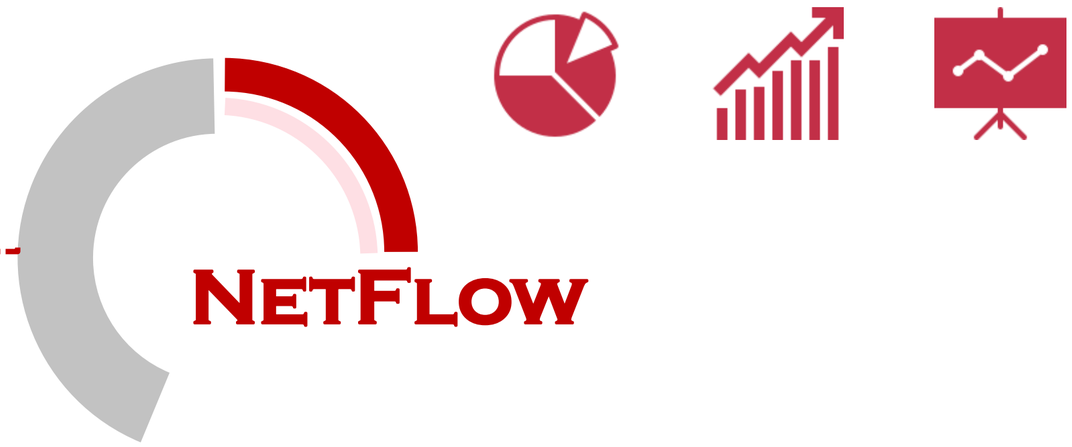
成功滲透至底層端點(實體或虛擬)後，橫向散播無人察覺









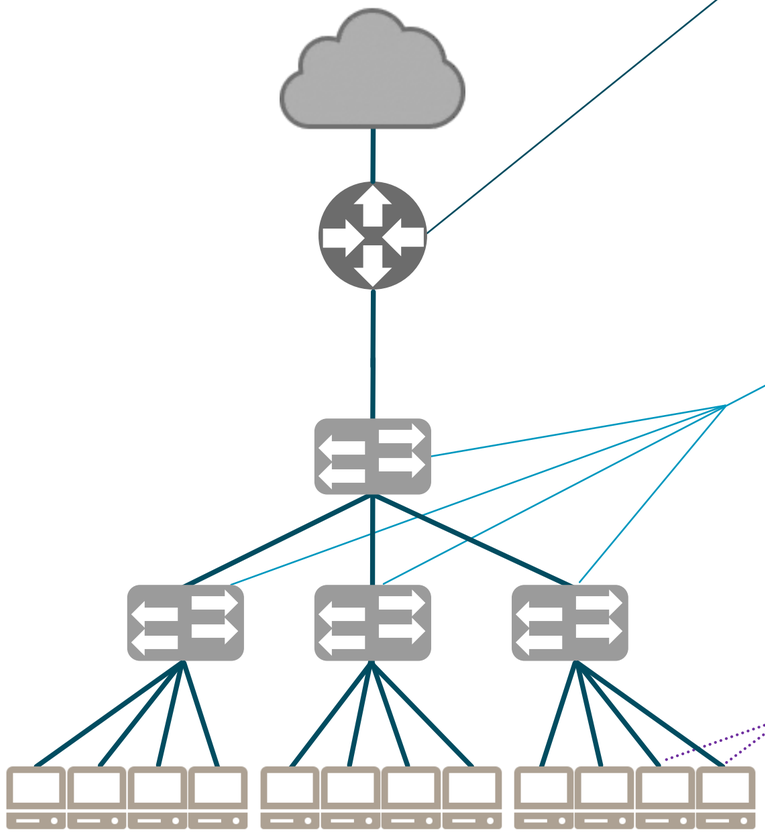


如果access switch能送出NetFlow...(或是有設備能幫access switch產生NetFlow)
IT人員有機會提早發現異狀!!

偵測對外連線

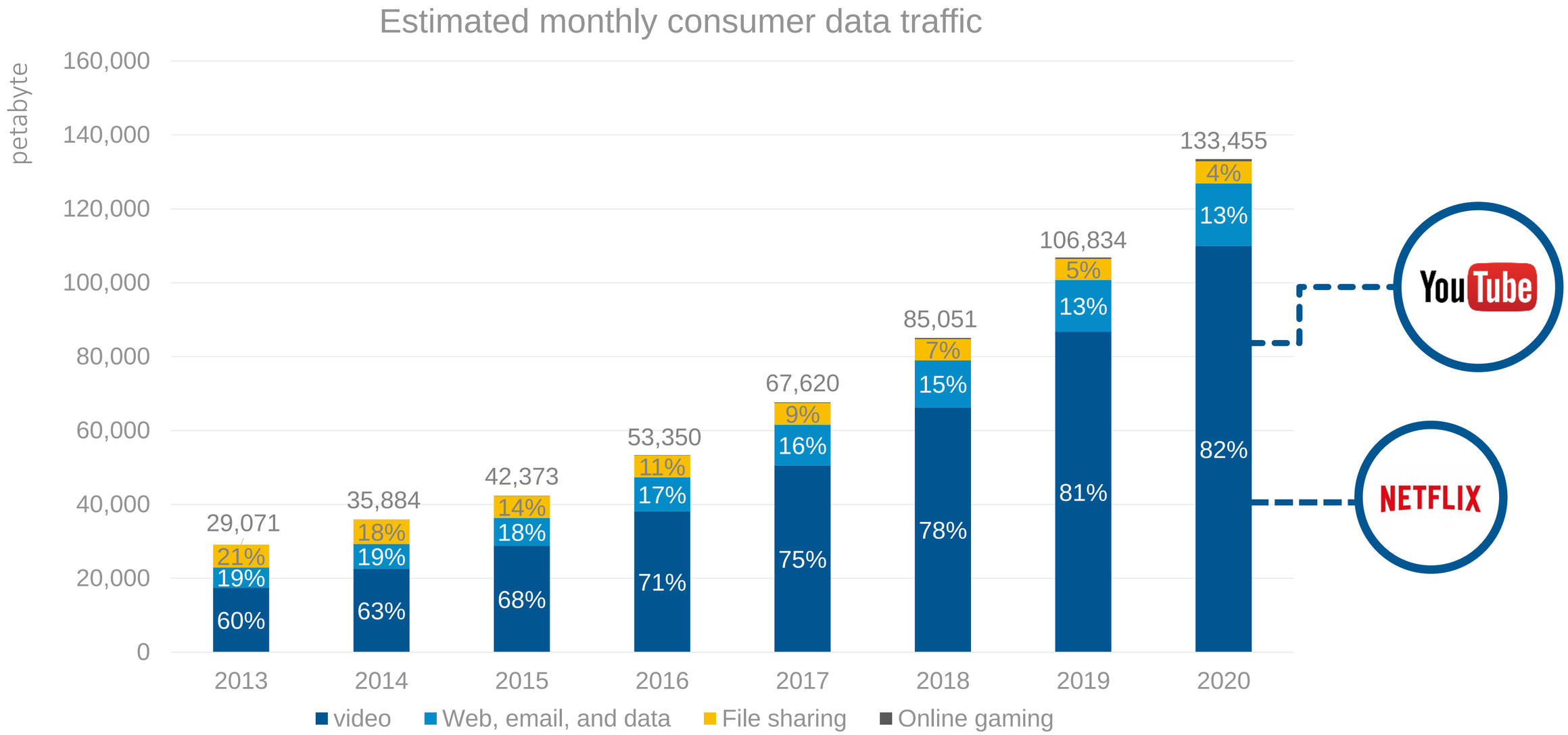
偵測底層活動

偵測終端與VM



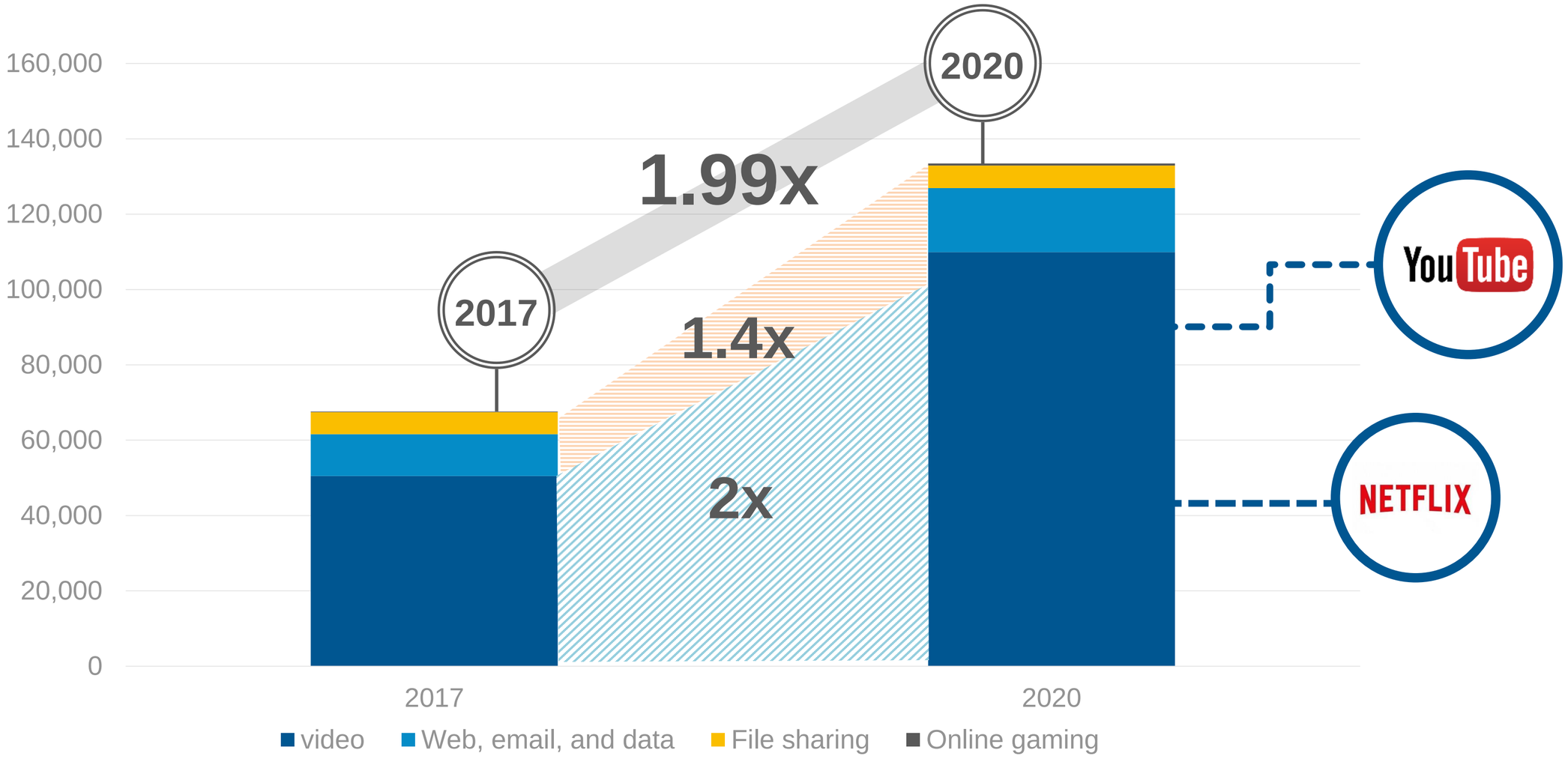
全面可視化

網路流量成長趨勢



Source : Cisco

多媒體流量是成長主力


160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
2017
2020
1.99x
1.4x
2x
2017
2020
video
Web, email, and data
File sharing
Online gaming
YouTube
NETFLIX

網路安全支出

網路安全設備支出=K *威脅特徵數量* 網路流量

K為一常數

網路安全支出估算

網路安全支出=K *威脅特徵數量* 網路流量

K為一常數

網路安全設備佈署的策略性原則

0. 網路安全設備僅需取得與其**任務相關**的流量

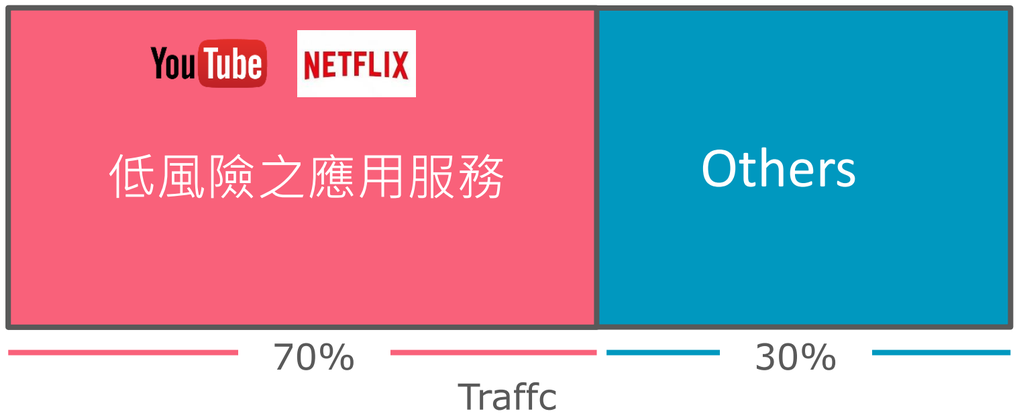
1.低風險流量豁免進入網路安全設備
YouTube/NetFlix/企業VoIP….列白名單

2. 已知威脅(聯防情資 & 成熟攻擊型態)阻斷
擔任第一線防禦
讓網路安全設備專心處理最複雜最隱晦的攻擊

3. 全網可視化
從WAN到LAN，含括實體與虛擬

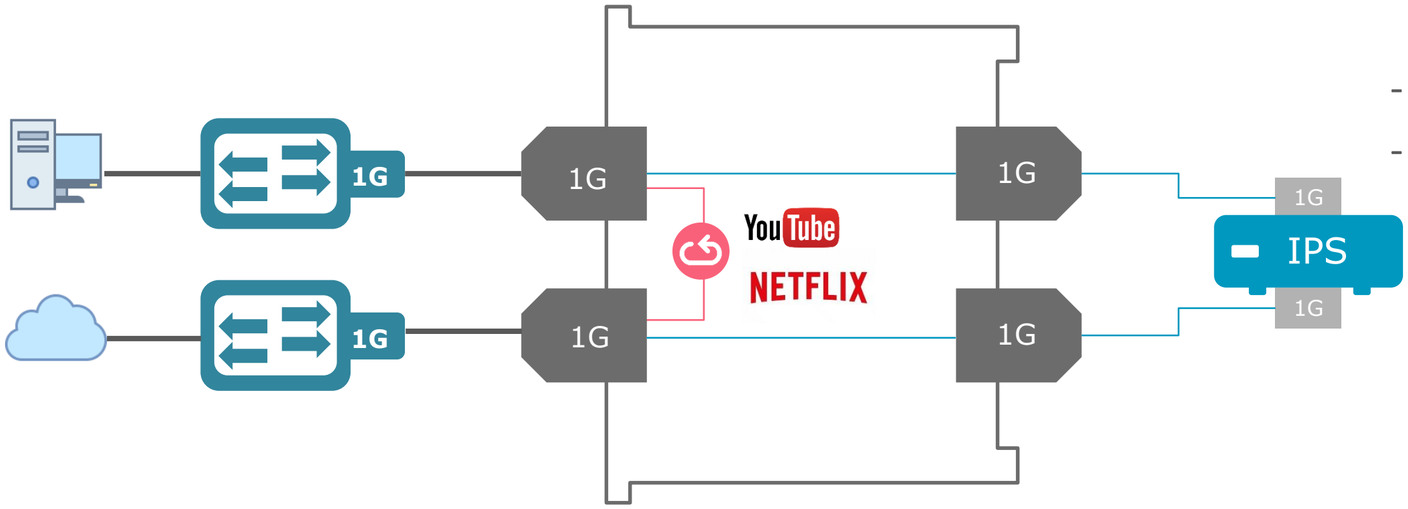
4. 經濟原則

應用服務流量旁路

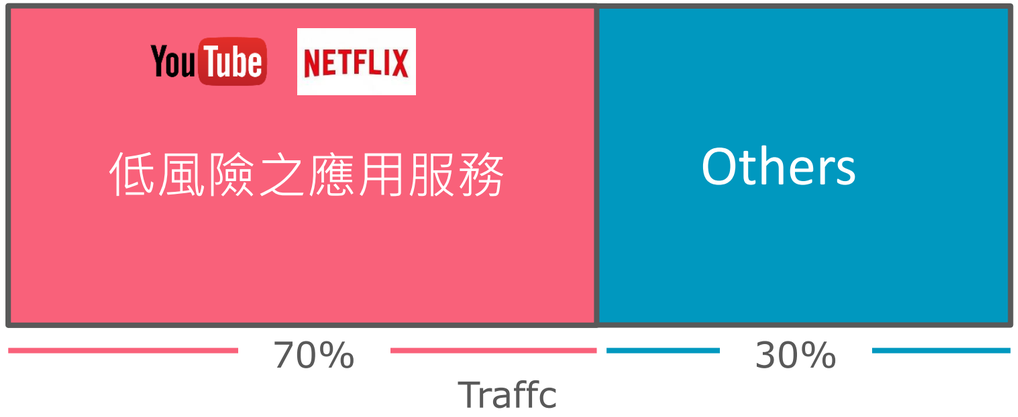


In-line 流量辨識與選擇性旁路

- 部分應用服務流量(如YouTube、Google Search、Facebook)不具安全威脅, 可豁免其進入IPS(或其他In-line資安設備)
- 使用者可自訂豁免條件: L2-L7
- 保留分析資源對付真正有威脅性的流量

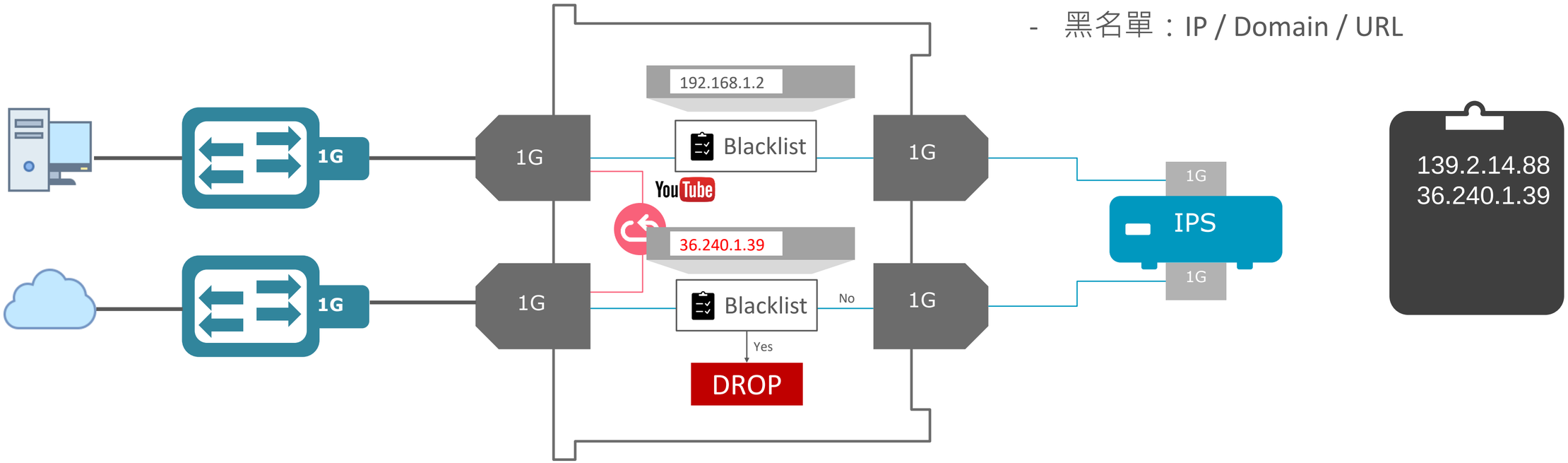


黑名單(已知威脅)阻斷



In-line 流量辨識及時阻斷

- 黑名單：IP / Domain / URL



虛擬化環境監測

1 跨主機VM連接 B C

- 兩台實體機器間有VxLAN通道，一般IDS無法正確處理

2 物理機內VM連接 A B

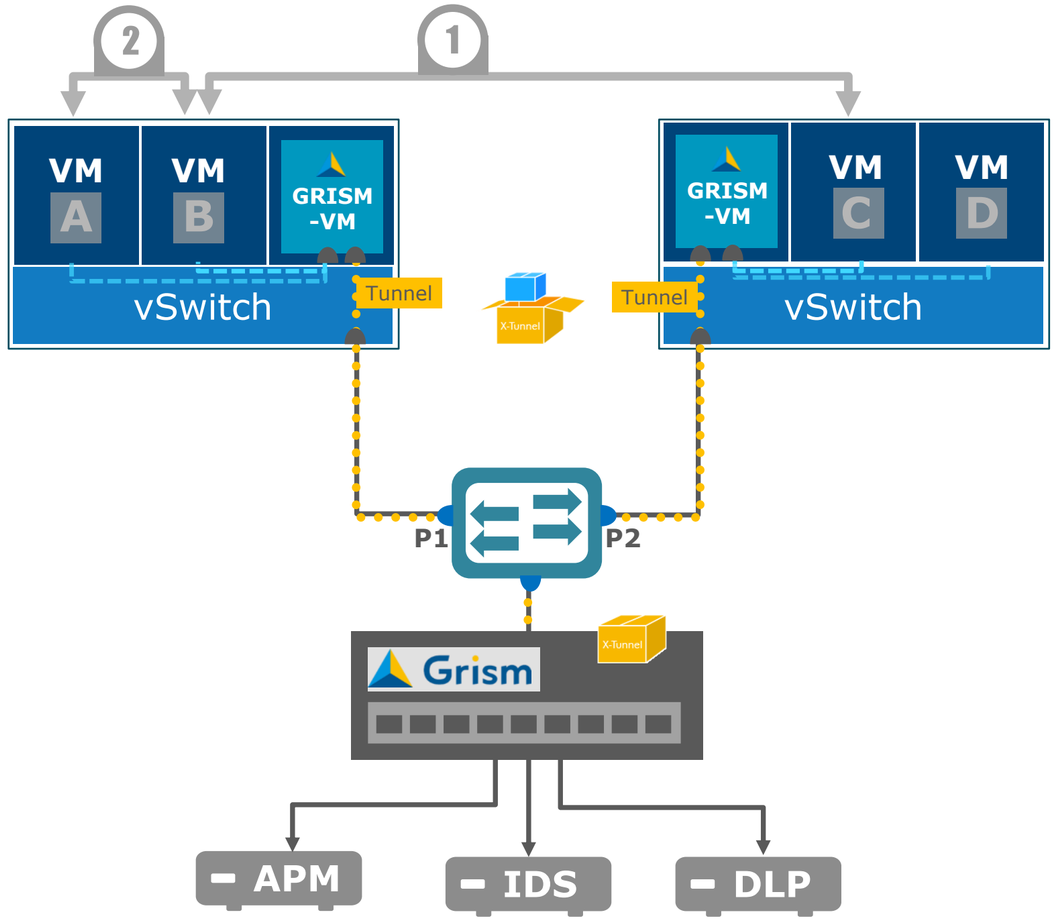
- 流量無法監控與分析

解決方法

GRISM -VM

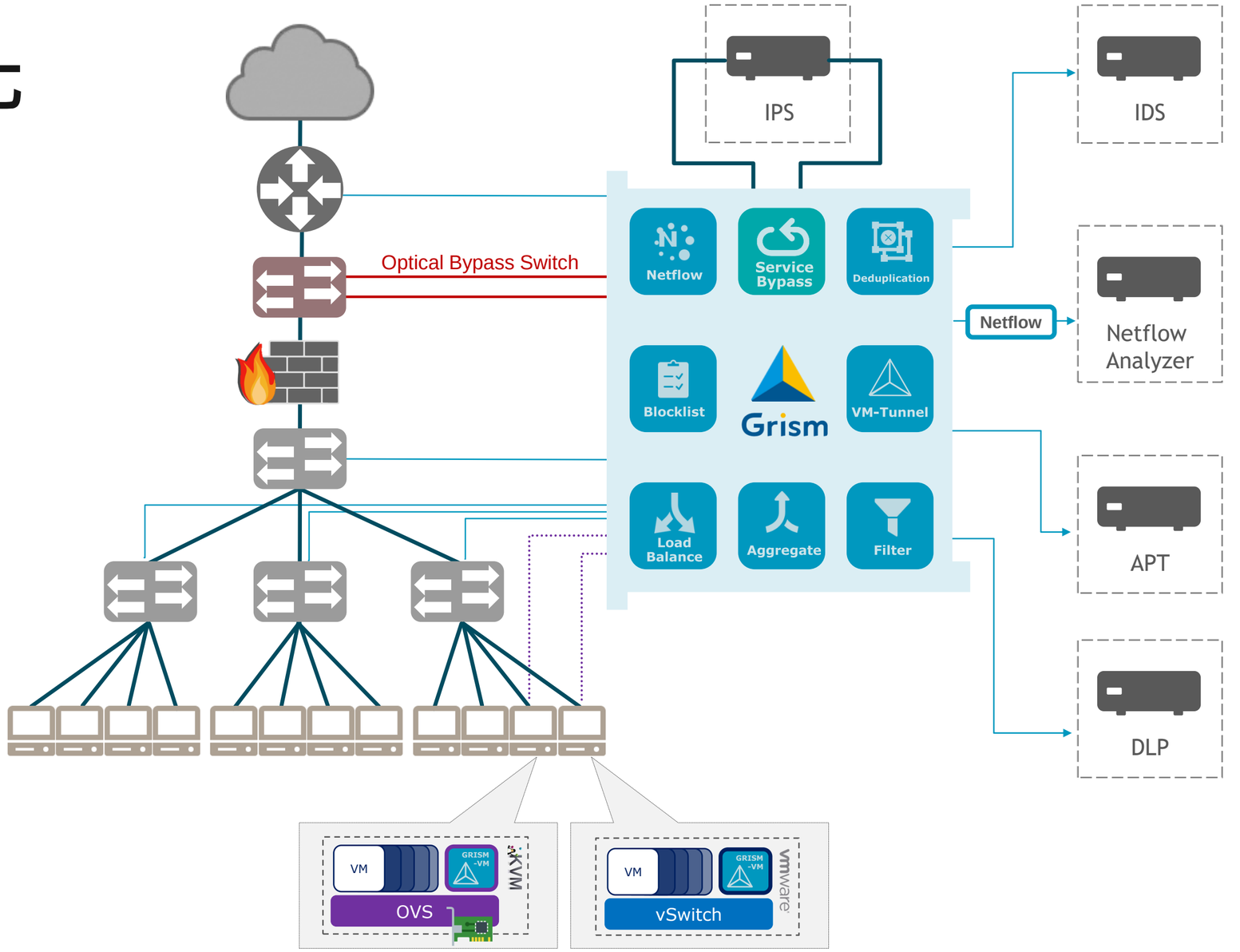
接收內部mirror流量

X-tunnel 封裝送出

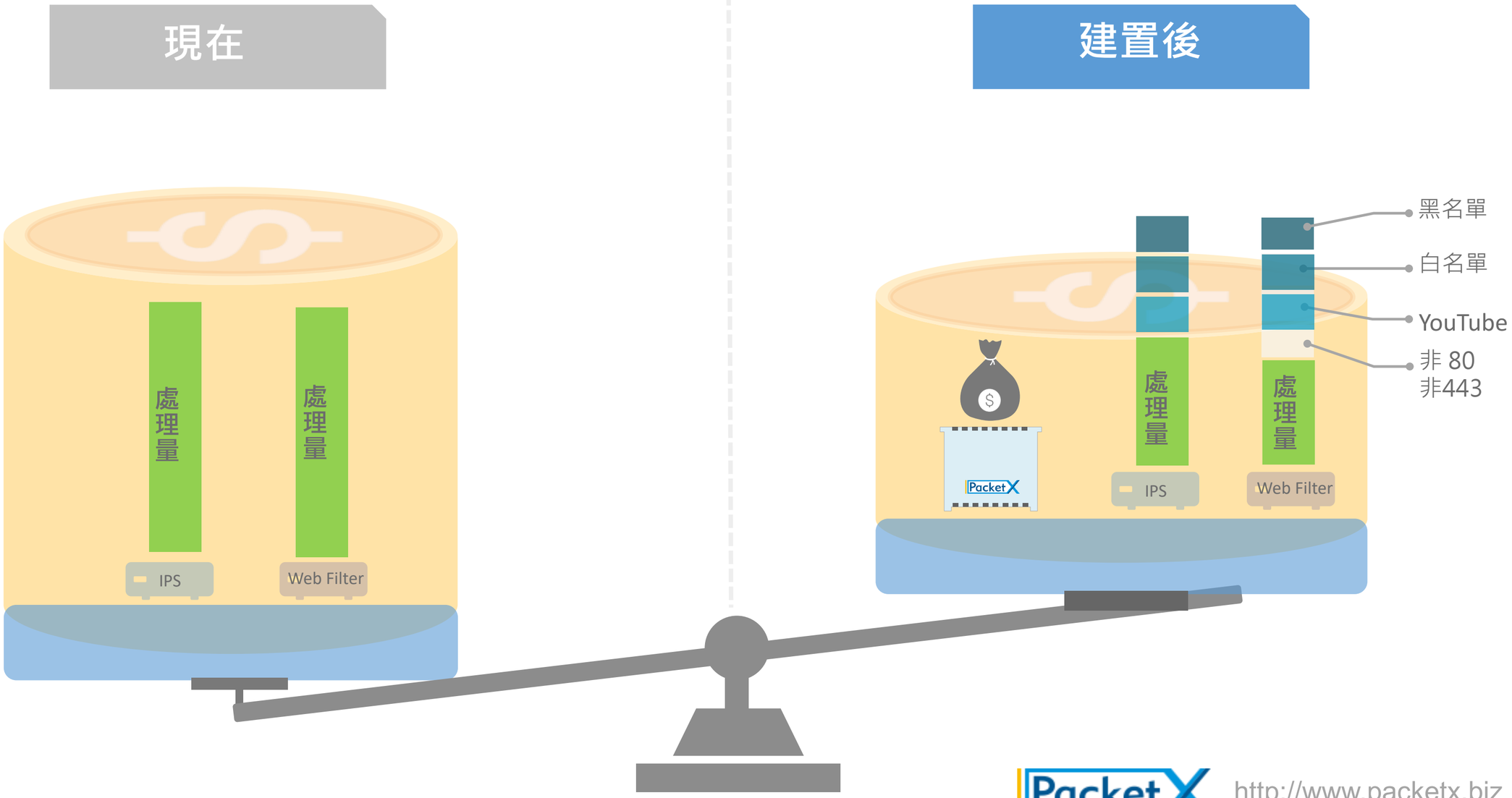


Grism

全網可視化


IPS
IDS
Optical Bypass Switch
Netflow
Service Bypass
Deduplication
Netflow
Netflow Analyzer
Blocklist
Grism
VM-Tunnel
Load Balance
Aggregate
Filter
APT
DLP
VM
GRISM -VM
KVM
OVS
VM
GRISM -VM
vmware
vSwitch

整體資安建置費用下降


現在
建置後
處理量
處理量
IPS
Web Filter
PacketX
處理量
處理量
IPS
Web Filter
黑名單
白名單
YouTube
非 80
非443

[以NPB先行篩選配送封包 提升網管資安設備效率]

[虛擬平台流量可視化 電信級網路補足最後一哩]

[2017臺灣資安大會 新聞台專訪 – PacketX / 王騰嶽]

[APNIC44 - SDN-based Security Mechanisms – Tony Wang]

[旁路交換器助陣，利用網路可視性 (Network Visibility) 平台打造多層資安防禦機制]

[貿協帶13家新創廠商組台灣隊到MWC拼場]

Thank You. It is Q&A time now.