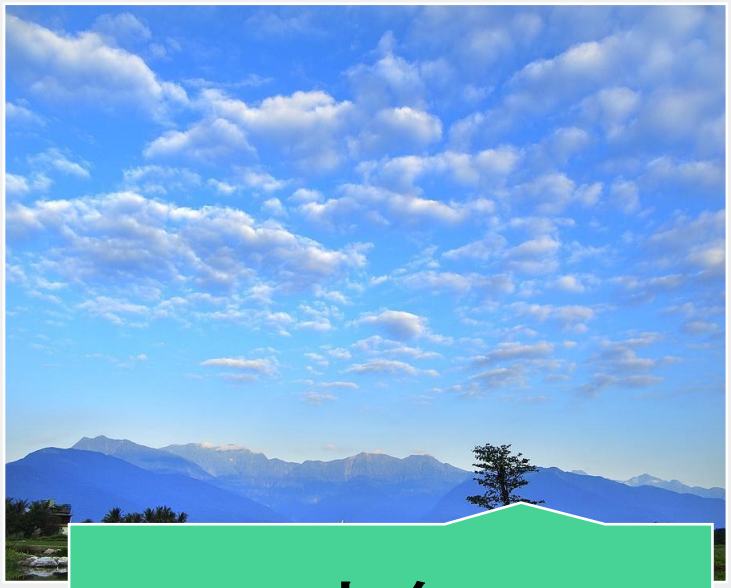
正面迎戰!加密流量這場戰役你我都不缺席
FortiProxy+FortiIsolator

Josh Lin
Technical Consultant Taiwan

人類世界不可缺少的三要素

陽光



空氣

水

資安世界不可缺少的三要素

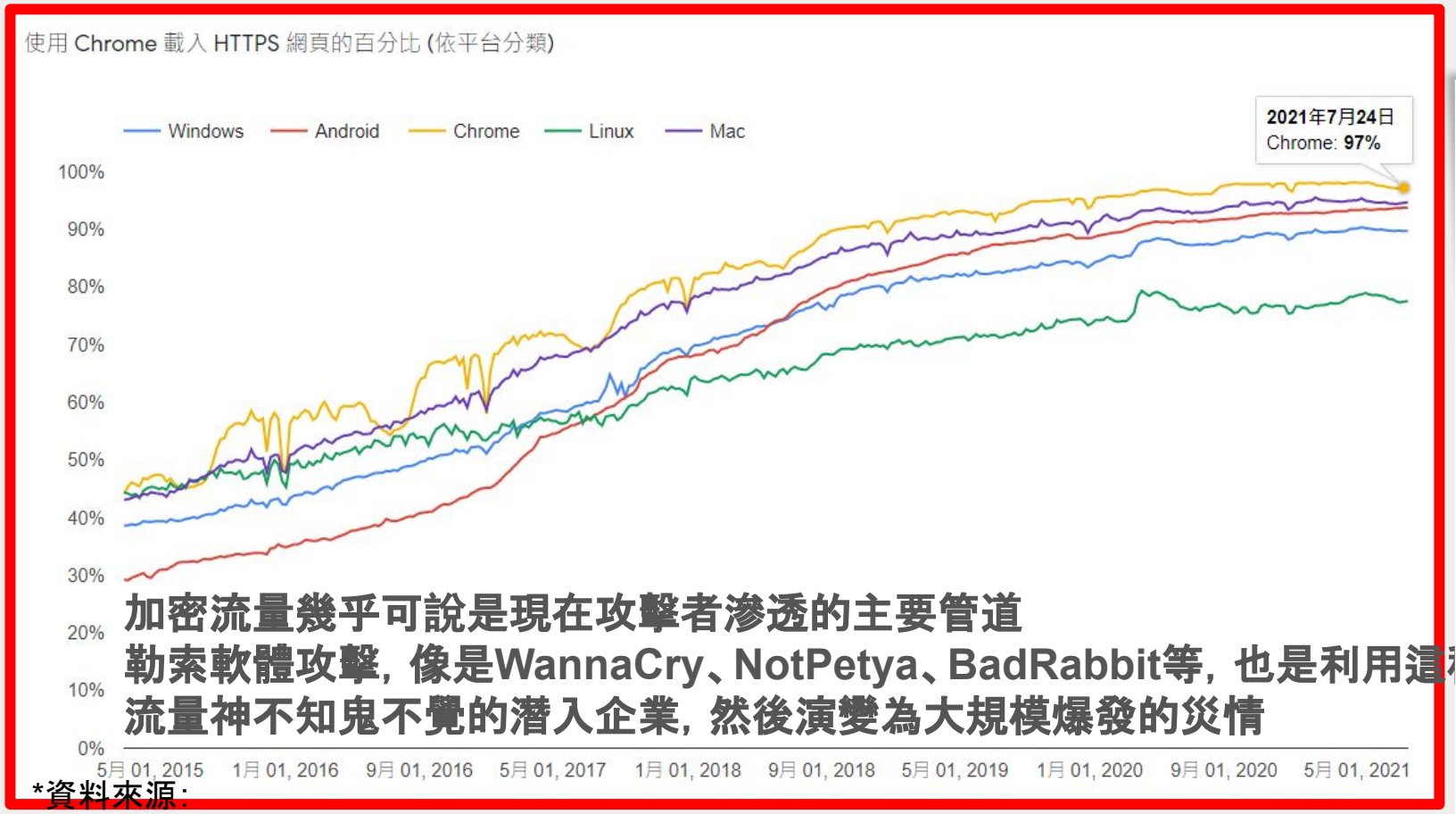
可視性

即時回應

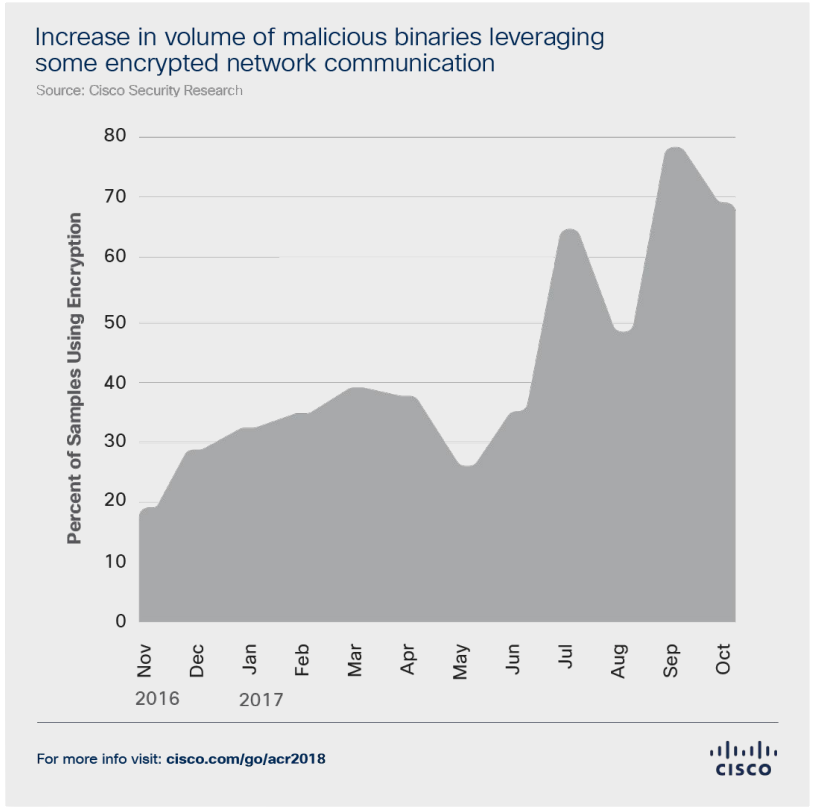
加密流量

加密流量已成主流

水能載舟亦能覆舟，加密流量已遭攻擊者濫用



加密流量幾乎可說是現在攻擊者滲透的主要管道
勒索軟體攻擊，像是WannaCry、NotPetya、BadRabbit等，也是利用這種
流量神不知鬼不覺的潛入企業，然後演變為大規模爆發的災情

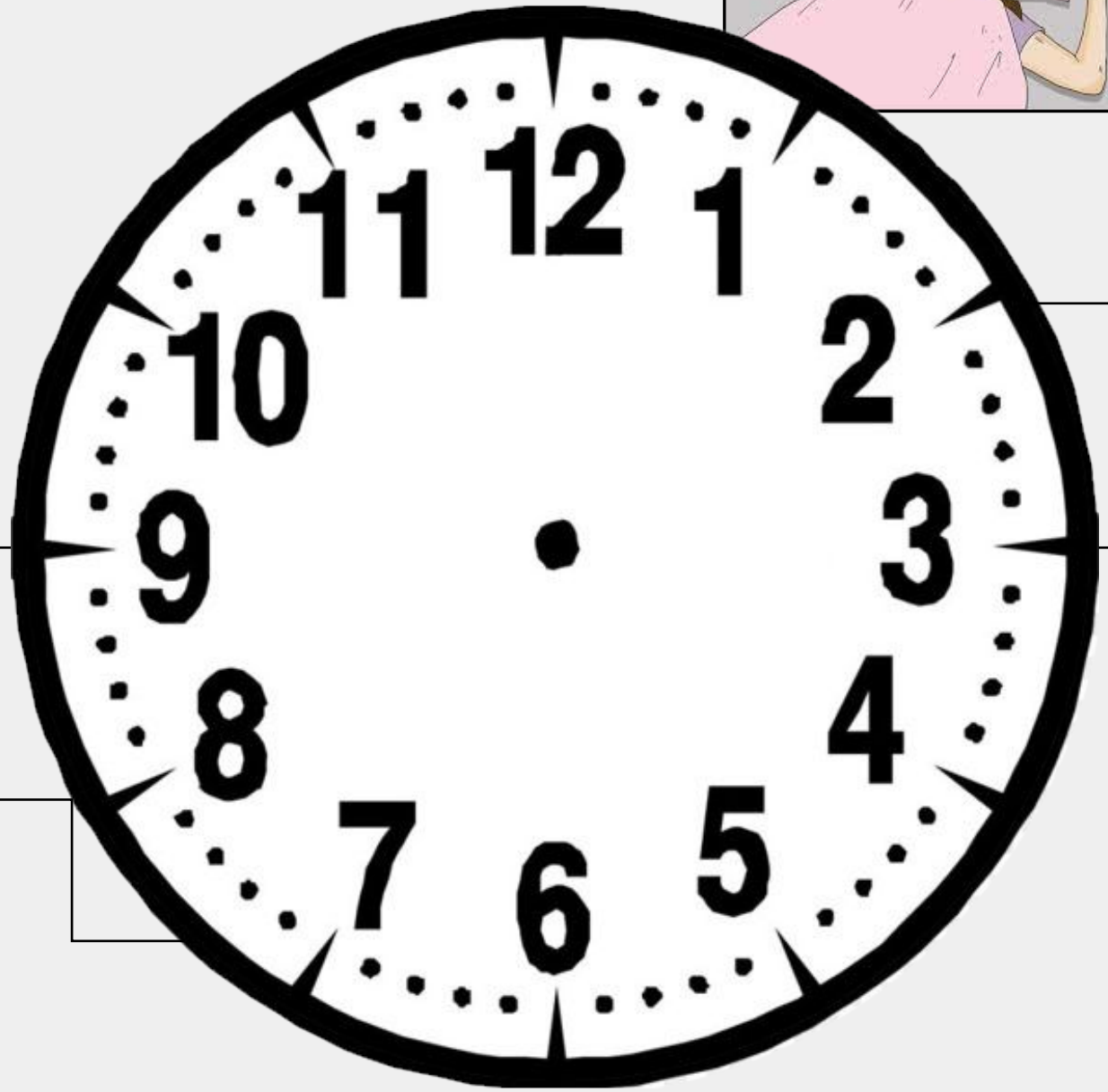


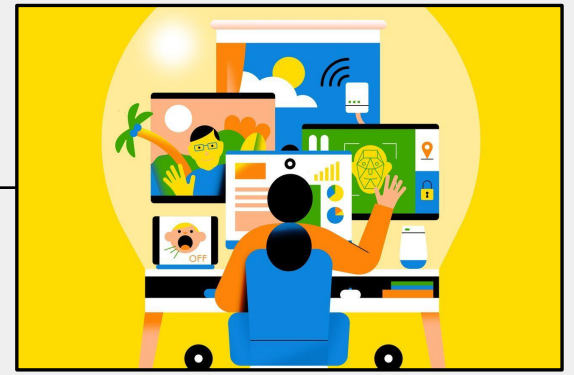
*資料來源：

https://transparencyreport.google.com/https/overview

https://blogs.cisco.com/security/as-encrypted-malicious-web-traffic-increases-defenders-need-advanced-tools-that-provide-visibility

網路和生活已密不可分

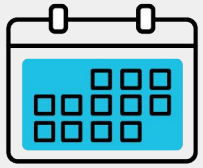




90% 的網路攻擊來自於網頁瀏覽和郵件

網頁瀏覽威脅

1,400+
每年有新的瀏覽器外掛程式, 含有惡意威脅



78% 的網站可被用於惡意軟體下載

每秒 **4** 一個未知的惡意軟體被下載

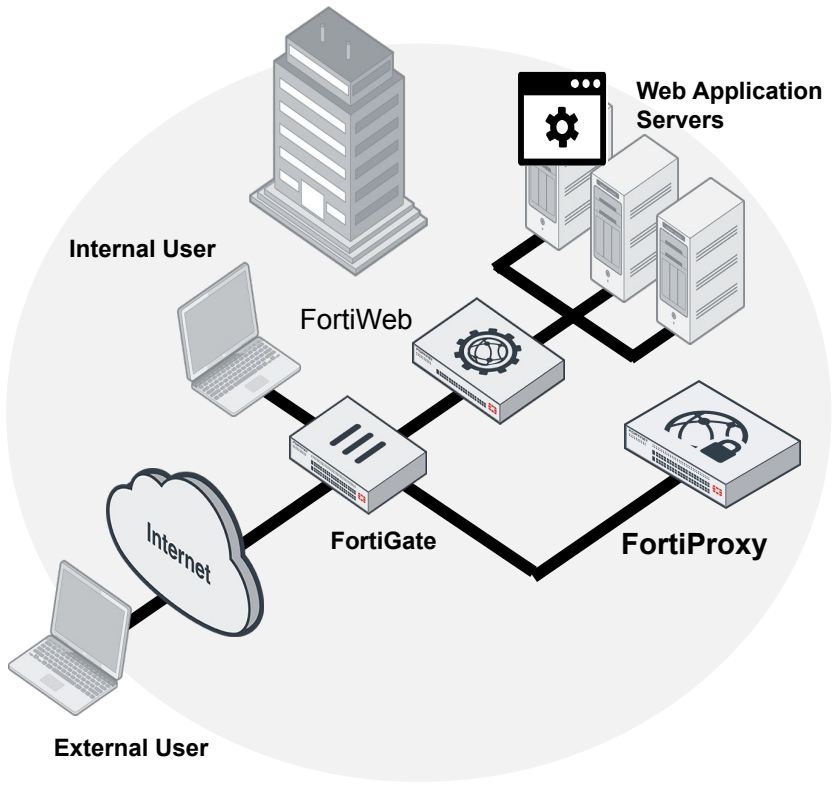
郵件和釣魚威脅

83% 的增長是由釣魚郵件啟動

55% 的大企業是釣叉式釣魚攻擊的目標

12% 使用者點擊了不被信任的連結或附件

上網安全閘道 - Gartner怎麼說?



Gartner

上網安全閘道(SWG)利用URL過濾，進階威脅和傳統惡意軟件防禦，保護用戶免受**網際網路的威脅**，並**幫助企業實施合規公司策略的上網政策**

今日上網安全閘道(SWG)的部署，主要是因為它們的安全功能。專注於**提供強大的阻擋惡意軟體和進階威脅檢測功能**的供應商最有能力在這個市場中獲得領先優勢地位

*資料來源: https://www.gartner.com/en/information-technology/glossary/secure-web-gateway

為什麼要專屬的加解密設備

NSS Labs Findings

- The average proportion of SSL traffic within a typical enterprise is 25% – 35%.
- The NSS threat database[1] has uncovered a small percentage (~1%) of malware using SSL.
- NSS research indicates that the majority of threats that are using SSL as a transport fall under the targeted persistent attack (TPA) category.
- The mean average of performance loss across 7 NGFW's:
  ~74% with 512b and 1024b ciphers
  ~81% with 2048b ciphers.
- The mean average of transactions per second (TPS) loss across 7 NGFW's:
  ~86.80% with a 512b cipher
  ~87.79% with a 1024 cipher
  ~92.28% with a 2048 cipher
- The Sourcefire NGFW had the highest rated TPS performance. However, Sourcefire was the only vendor that used a dedicated SSL appliance.
- The Dell SonicWALL SuperMassive E10800 NGFW had the highest rated TPS performance with onboard SSL decryption.
- Juniper was rated the best with regards to performance loss and reduction in TPS.
- All vendors had significant performance issues and TPS loss with 2048b ciphers.
- NSS has concerns for the viability of SSL inspection in enterprise networks without the use of dedicated SSL decryption devices.

加密流量管理的最佳工具

- 高效能與可擴充的**代理 (Proxy) 設備**
- **專屬上網防護及加密流量管理解決方案**
- **按需購買**的授權方案(Pay As You Grow)
- 多層次**偵測與預防**威脅機制
- 使用認證授權的 **WEB 應用程式控管**
- 網路**頻寬優化**與進階網頁**內容快取**機制

SSL 加密流量解析

- 硬體加速專用晶片
- 加密流量的可視化
- 多種威脅檢測保護

多層次防禦策略

- 整合世界級 FortiGuard 威脅情資
- 支援整合地端/雲端 FortiSandbox

認證存取機制

- 精細的應用程式控管政策
- 即時主動式的活動監控
- 基於用戶或群組的社群網站限制存取

多層安全防護及強大的效能

安全防護

- Intrusion Prevention System
- Application Control
- Antivirus
- Web Filtering
- DNS Filtering
- Web Rating Overrides
- Data Leak Prevention
- SSL-VPN
- SSL IPsec
- External threat inspection list
- SSL/SSH Inspection
- Content Analysis (3rd party solution)
- User Authentication
- Sandbox Inspection Integration (On-Premises and Cloud)

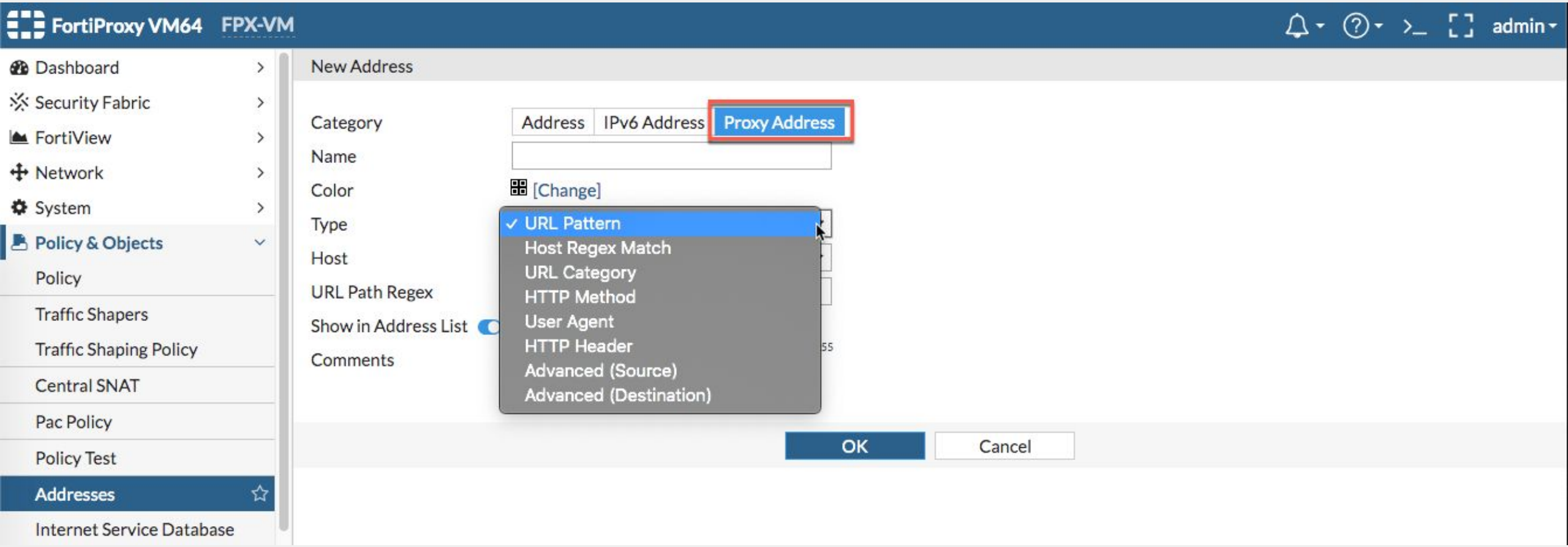
效能

- Full Proxy Application
- Content Caching
- WAN Optimization
- Video Caching & Stream Splitting

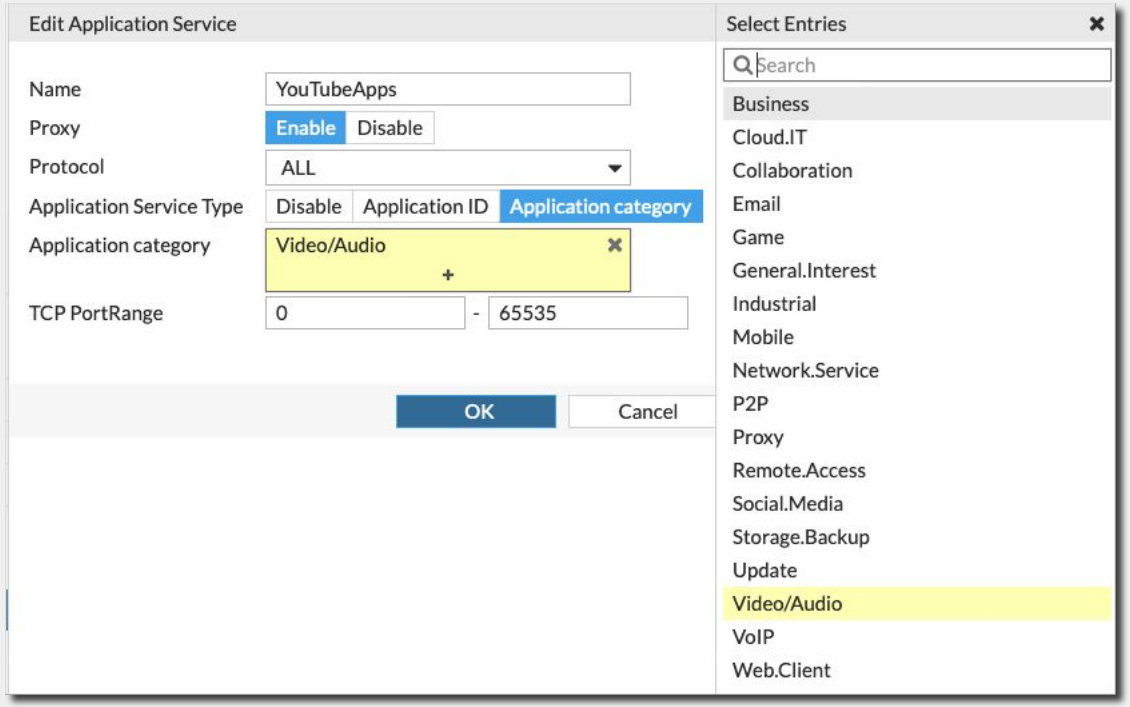
行為可視性

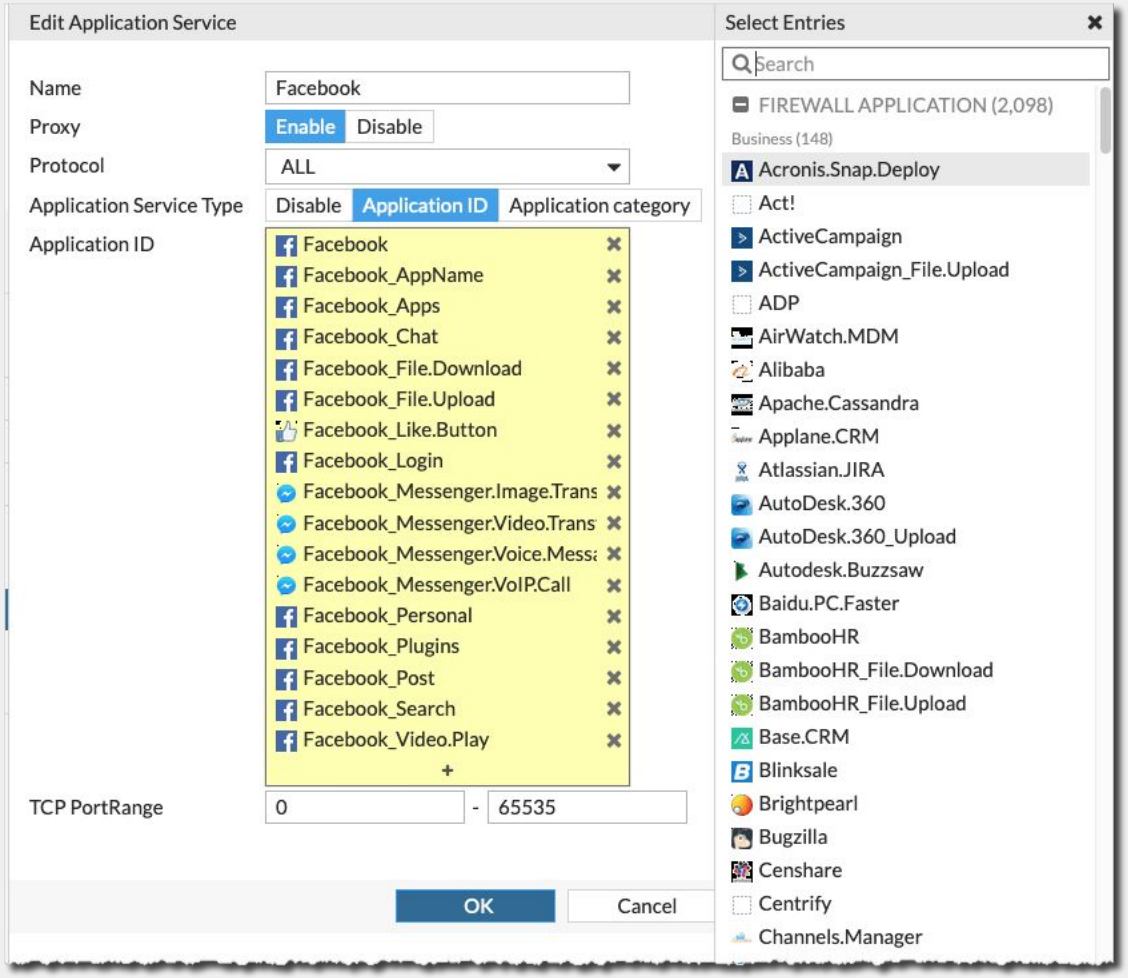
- Monitor and Logging
- FortiAnalyzer Integration
- FortiView Integration
- FortiCloud Intergation

彈性且細緻的控管能力



應用程式識別

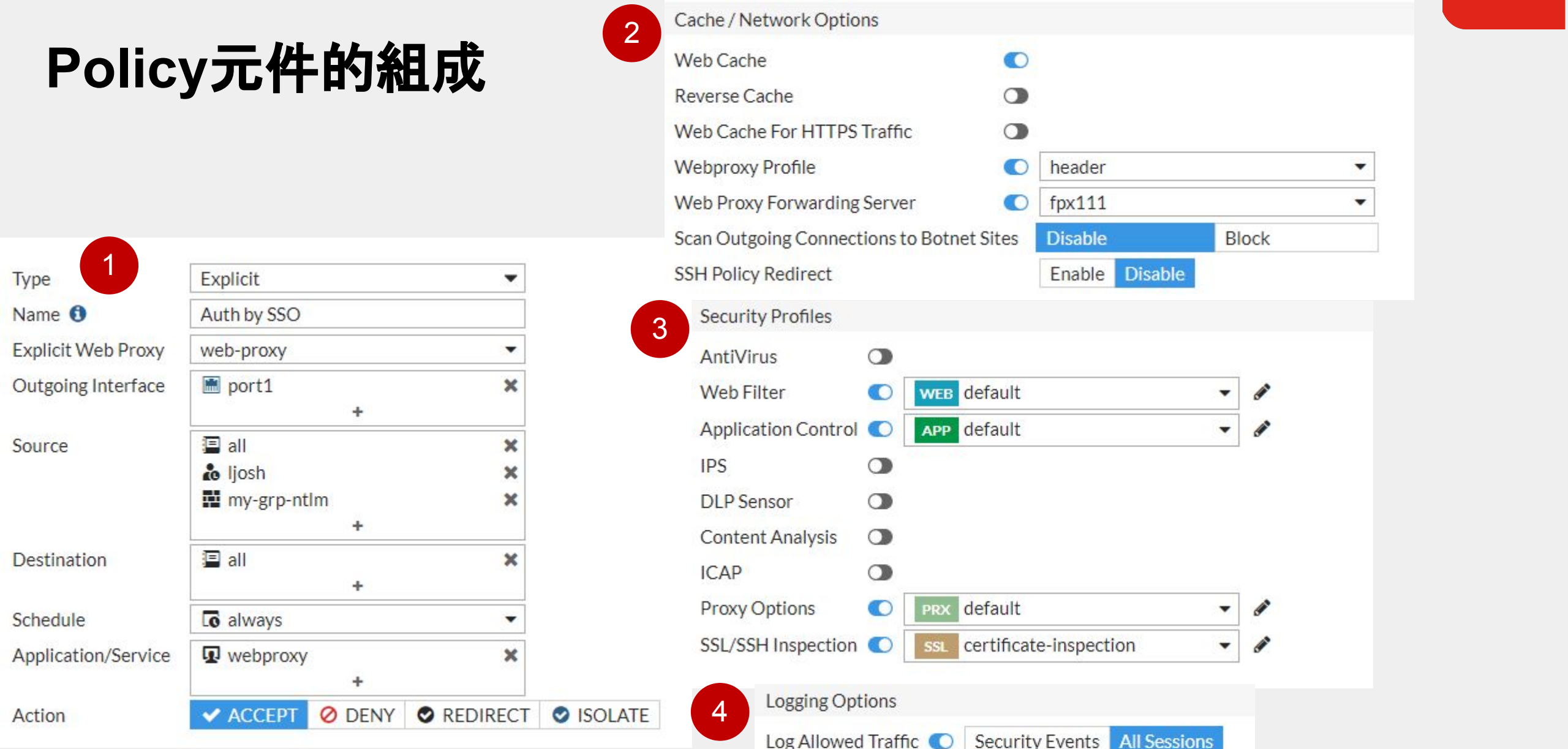




Policy設定&検査順序

Name	Source	Destination	Schedule	Service	Action	Security Profiles	Log
web-proxy → port1 15							
	r/https-post/ r/proxy-connection	all	always	webproxy	DENY	PRX default SSL certificate-inspection	All
	all my-grp-ntlm ljosh	all	always	webproxy	ACCEPT	WEB default PRX default SSL deep-inspection	All
Auth by SSO	all my-grp-ntlm ljosh	all	always	webproxy	ACCEPT	WEB default APP default PRX default SSL certificate-inspection	All
hd/referrer test	all	4xion-preload	always	webproxy	ACCEPT	PRX default SSL deep-inspection	All
	all	*.cnn.com *.ruten.com.tw	always	webproxy	DENY	PRX default SSL certificate-inspection	Disabled

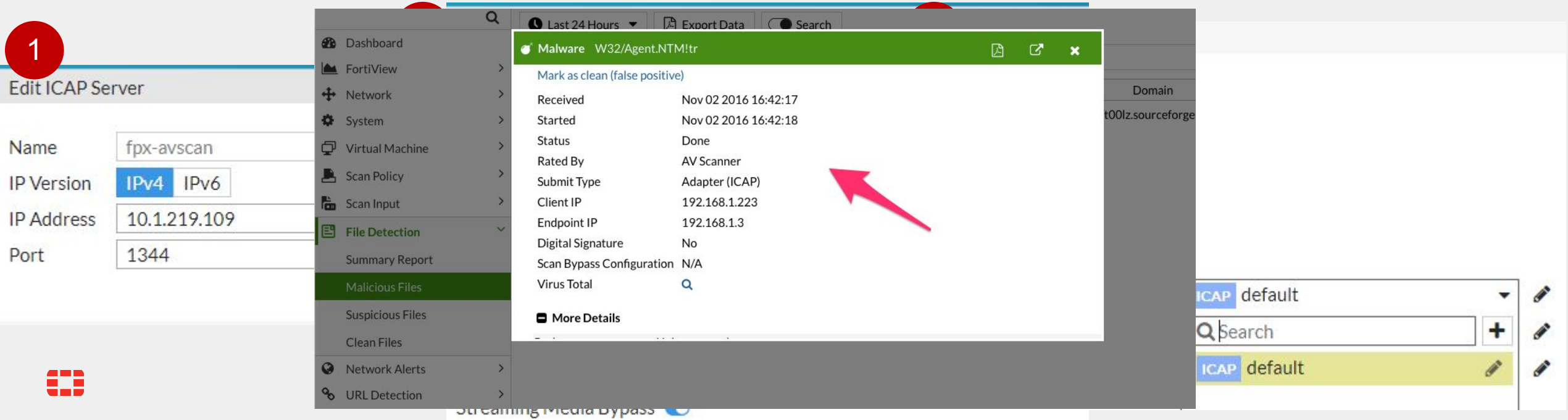
Policy元件的組成



聯防他牌資安設備

Internet Content Adaptation Protocol (ICAP)

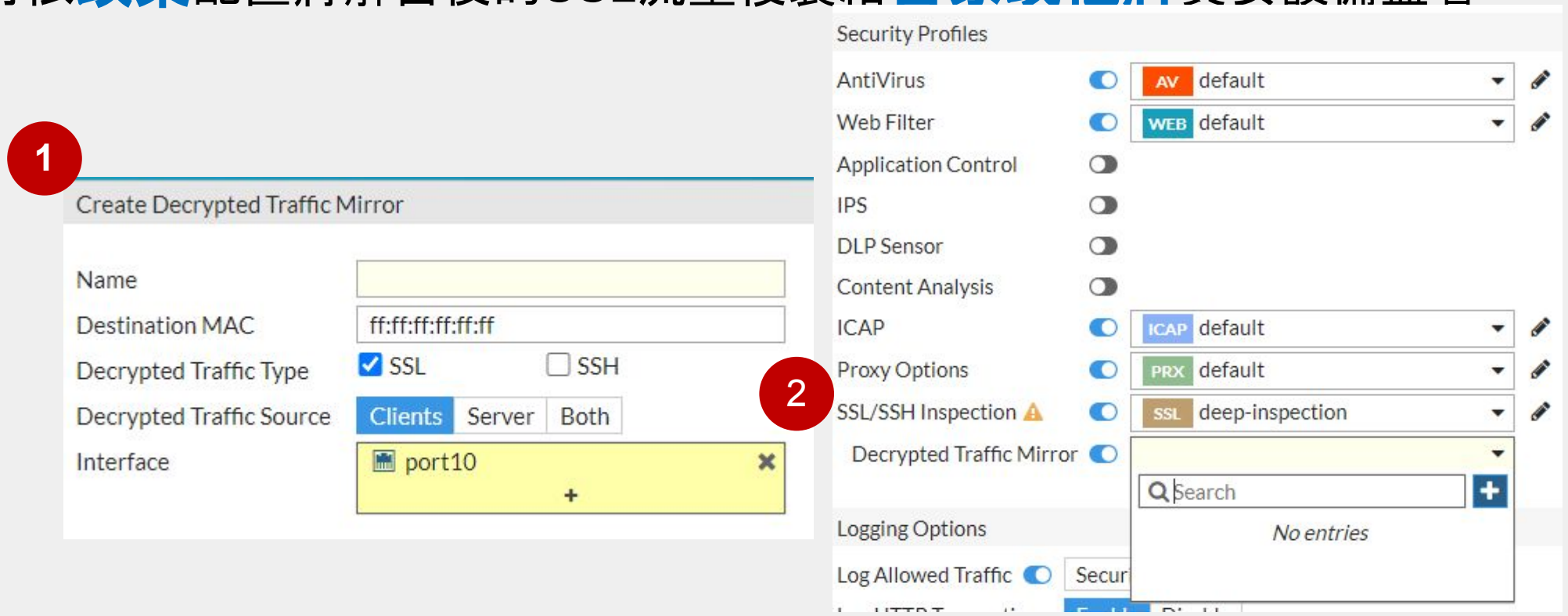
- ICAP一種應用層協議，用於將**掃描或清洗任務**導向至他牌專用的資安設備，如:防毒牆、DLP
  - ICAP Request Mode: 當收到新請求時，將請求發送到掃描設備以確保它是一個有效的訪問請求
  - ICAP Response Mode:當新請求有效時，將掃描任何返回的內容



聯防他牌資安設備 (cont'd)

Decrypted Traffic Mirror

- 解密並將流量複製(mirror)到指定端口
- 可依**政策**配置將解密後的SSL流量複製給**自家或他牌**資安設備監看



Log & 報表

Source	Group	Destination
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	139.175.87.67 (139-175-87-67.dialup.dynam
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	23.11.183.207 (a23-11-183-207.deploy.static
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	13.107.6.171
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	13.107.6.171
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	13.107.42.11
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.139.155.175
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	40.90.23.206
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	139.175.107.80 (139-175-107-80.dialup.dyn
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	13.105.74.49
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	52.114.77.34
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	23.11.183.207 (a23-11-183-207.deploy.static
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	23.11.183.207 (a23-11-183-207.deploy.static

Top 20 Most Active Users

#	User (or IP)	Requests
1	ljosh@ftnttw.net	6,694

Top Categories by Request

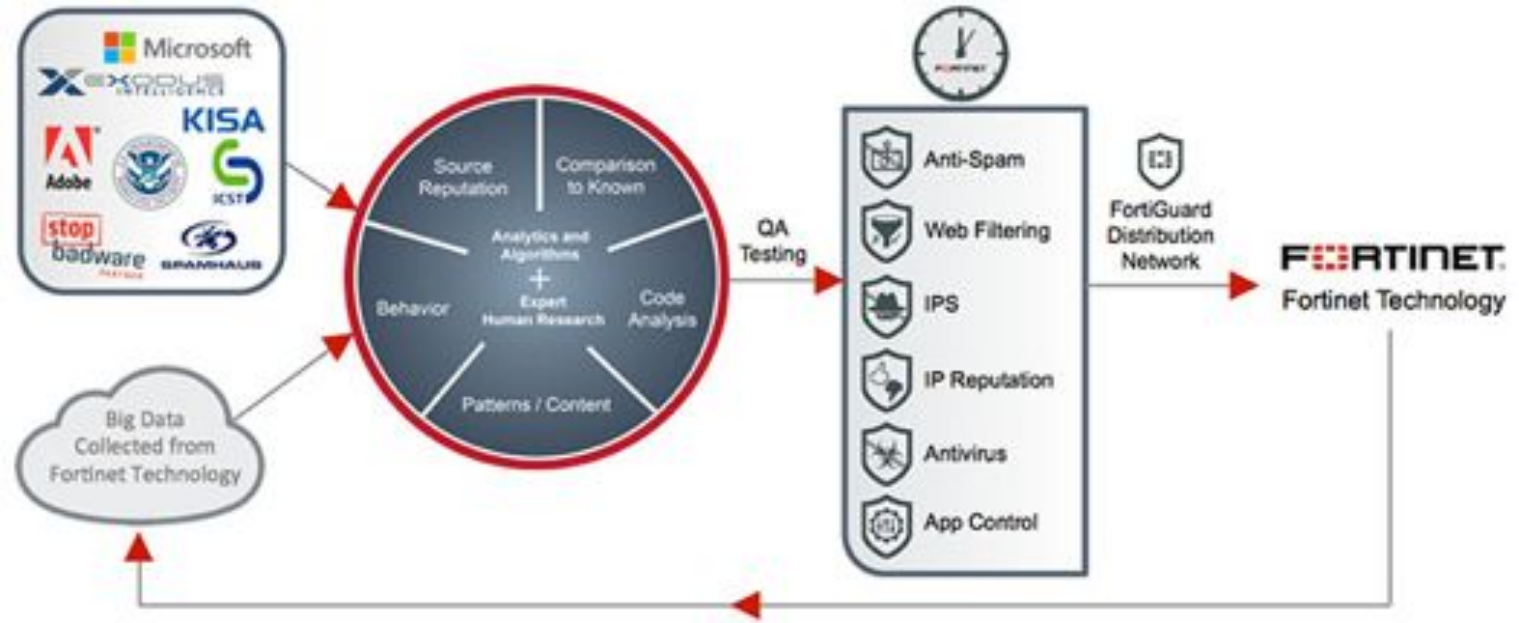
Search Engines and Portals	29.80%
Information Technology	25.56%
Advertising	12.49%
Social Networking	6.53%
Content Servers	6.02%
Business	5.89%
News and Media	4.09%
Web-based Applications	3.02%
Web Analytics	2.36%
Finance and Banking	1.09%
Others	3.15%

Top 20 Allowed Web Categories

#	Category	Requests
1	Search Engines and Portals	1,995
2	Information Technology	1,711
3	Advertising	836
4	Social Networking	437
5	Content Servers	403
6	Business	394
7	News and Media	274
8	Web-based Applications	202
9	Web Analytics	158
10	Finance and Banking	73
11	Streaming Media and Download	56
12	File Sharing and Storage	56
13	Shopping	29
14	Web-based Email	20
15	Meaningless Content	13
16	Instant Messaging	13
17	Newsgroups and Message Boards	8
18	Internet Radio and TV	6
19	Reference	5
20	Arts and Culture	3

豐富即時的威脅情資和保護- FortiGuard

全球最大的資安雲



- 結合了領先業界的資安廠商和Fortinet的威脅情報，以提供最大程度的保護
- 大數據、機器學習、自動化以及Fortinet專利的分析和研究
- 已出貨超過 220 萬台設備，擁有超過 250,000 名客戶，提供世界一流的威脅情報
- 針對已知和未知威脅的最佳保護

FortiProxy產品線

FPX-400E

- **500** – 4,000 users
- **3 Gbps** Proxy Mode
- **1.5 Gbps** AV, WF, App
- **1 Gbps** AV,WF, App.Ctrl, IPS, SSL Full Inspection

FPX-2000E

- 2,500 – 15,000 users
- **9 Gbps** Proxy Mode
- **4 Gbps** AV, WF, App
- **3 Gbps** – AV,WF, App.Ctrl, IPS, SSL Full Inspection

FPX-4000E

- 10,000 – 50,000 users
- **18 Gbps** Proxy Mode
- **9 Gbps** AV, WF, App
- **6 Gbps** – AV,WF, App.Ctrl, IPS, SSL Full Inspection

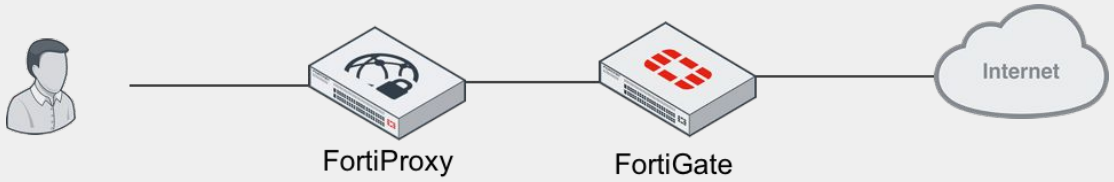
FPX-VM

- 100 – 50,000 users
- Performance HW dependent

Web/DNS Filtering | Application Control | Anti-Virus | Intrusion Prevention | Content Analysis | Traffic Shaping | Advanced Caching and WAN Opt. + DNS Protection

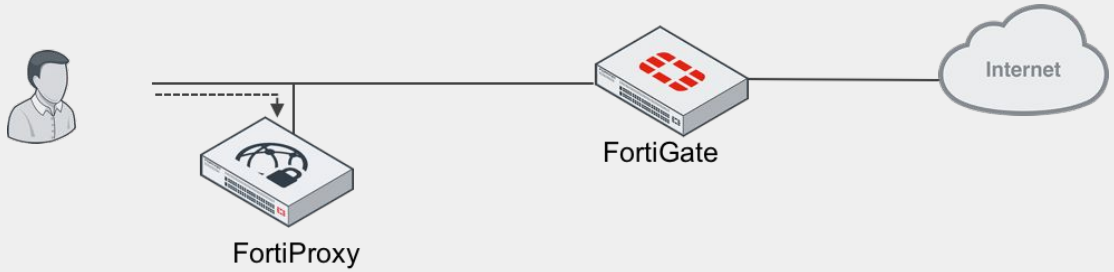
彈性的部署模式

Inline (L2/L3) Deployment



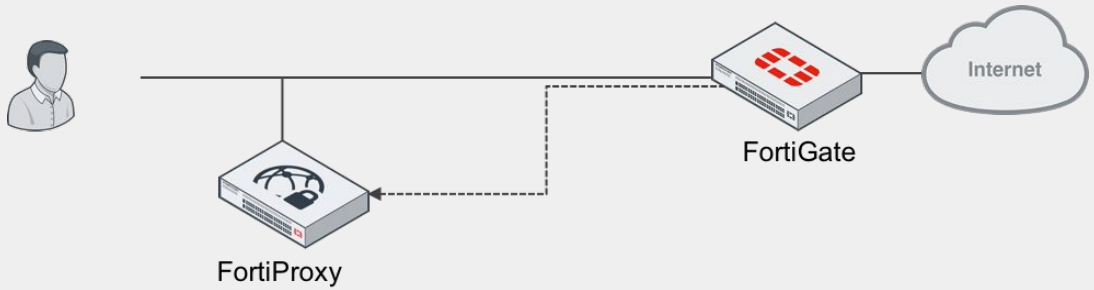
- 設備在網路環境扮演橋接設備(inline)，監控解析通過設備本身的使用者連線內容

Explicit Deployment



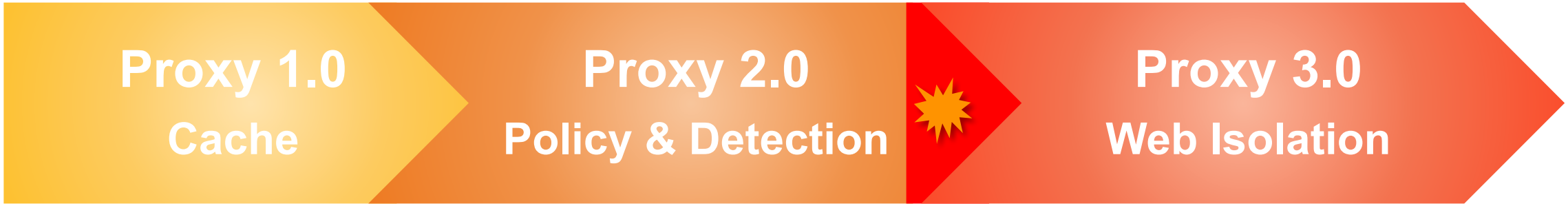
- Explicit模式代理使用者發起的所有web連線
- 客戶端瀏覽器必須指向代理伺服器，支援PAC files；同時也可以扮演PAC server

Transparent/WCCP Deployment



- 設備在網路環境透明代理(transparent)使用者連線請求，監控解析通過設備本身的使用者連線內容
- PBR(Policy-Based Route)/WCCP 可與現有網絡架構集成並提供可擴展性和負載平衡

上網控管的演變歷程



- 昂貴的線路頻寬
- 連接速度慢
- 代理1.0主要是一個快取解決方案 (Gen1 Cache)

- Web訪問控制和合規性
- URL過濾和風險級別
- SSL可見性和內容檢查
- 沙箱和反惡意軟件
- 代理2.0是Block or Allow 解決方案
- Web 2.0 內容快取 (Gen2 Cache)

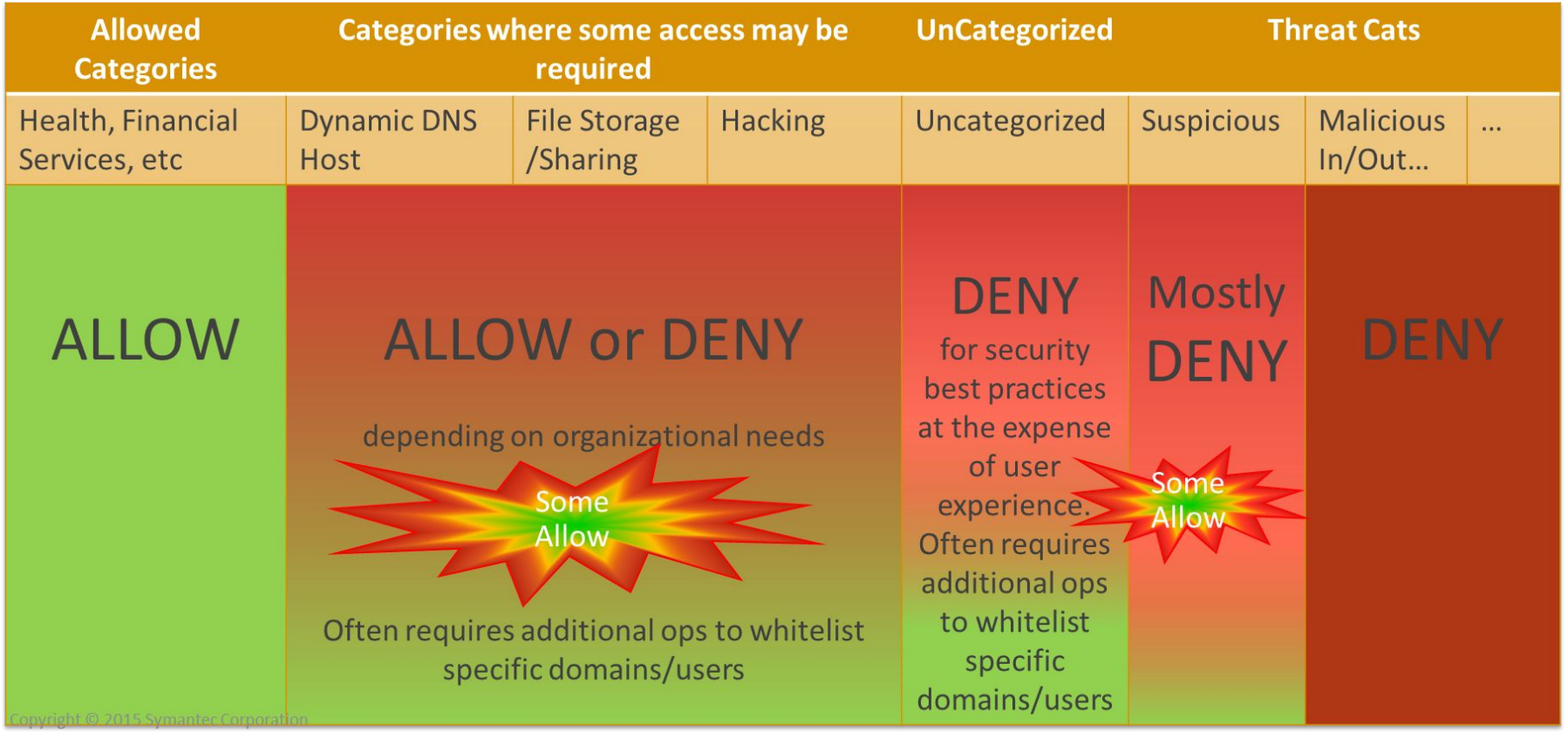
- Block 或 Allow 對於現在…未來的各種用趨勢，但無法滿足要求
- 惡意程式和網絡釣魚迴避傳統解決方案

- 消除感染的威脅
- 遠程執行網頁內容
- 解決未分類網站的挑戰
- 降低access policy 管理成本和錯誤警報的開銷和復雜性
- 有效避免了 over-blocking

問題: 過度阻擋”灰色地帶”網站

Web 控管策略

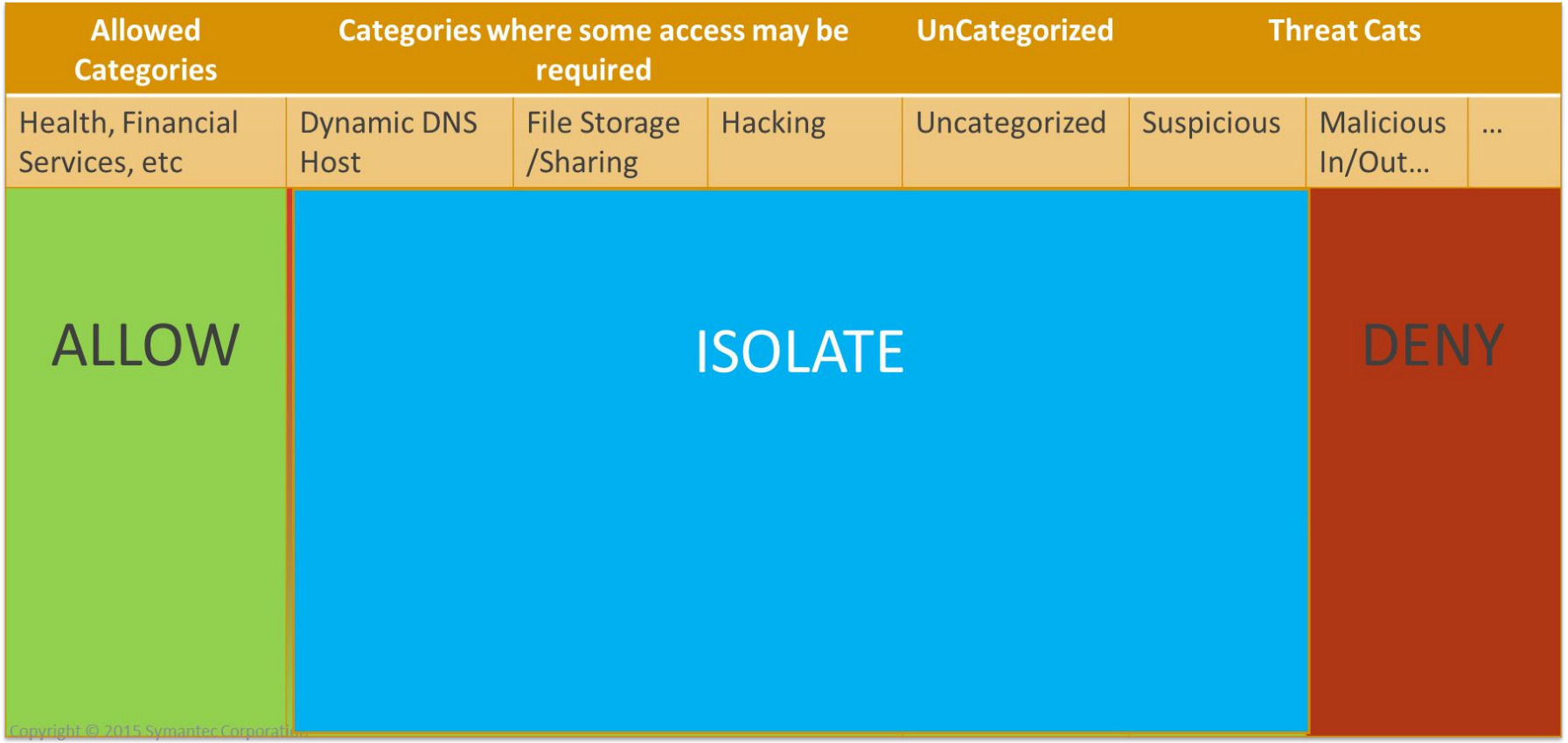
- ***VIP用戶*** **特權瀏覽**
- ***總是允許*** **特定URL類別及網站**
- ***總是阻擋*** **特定URL類別及網站**
- ***關鍵問題*** **– 灰色地帶**
  - **過度阻擋 – 造成用戶問題，體驗不佳**
  - **寬鬆政策 – 惡意軟體風險增加**



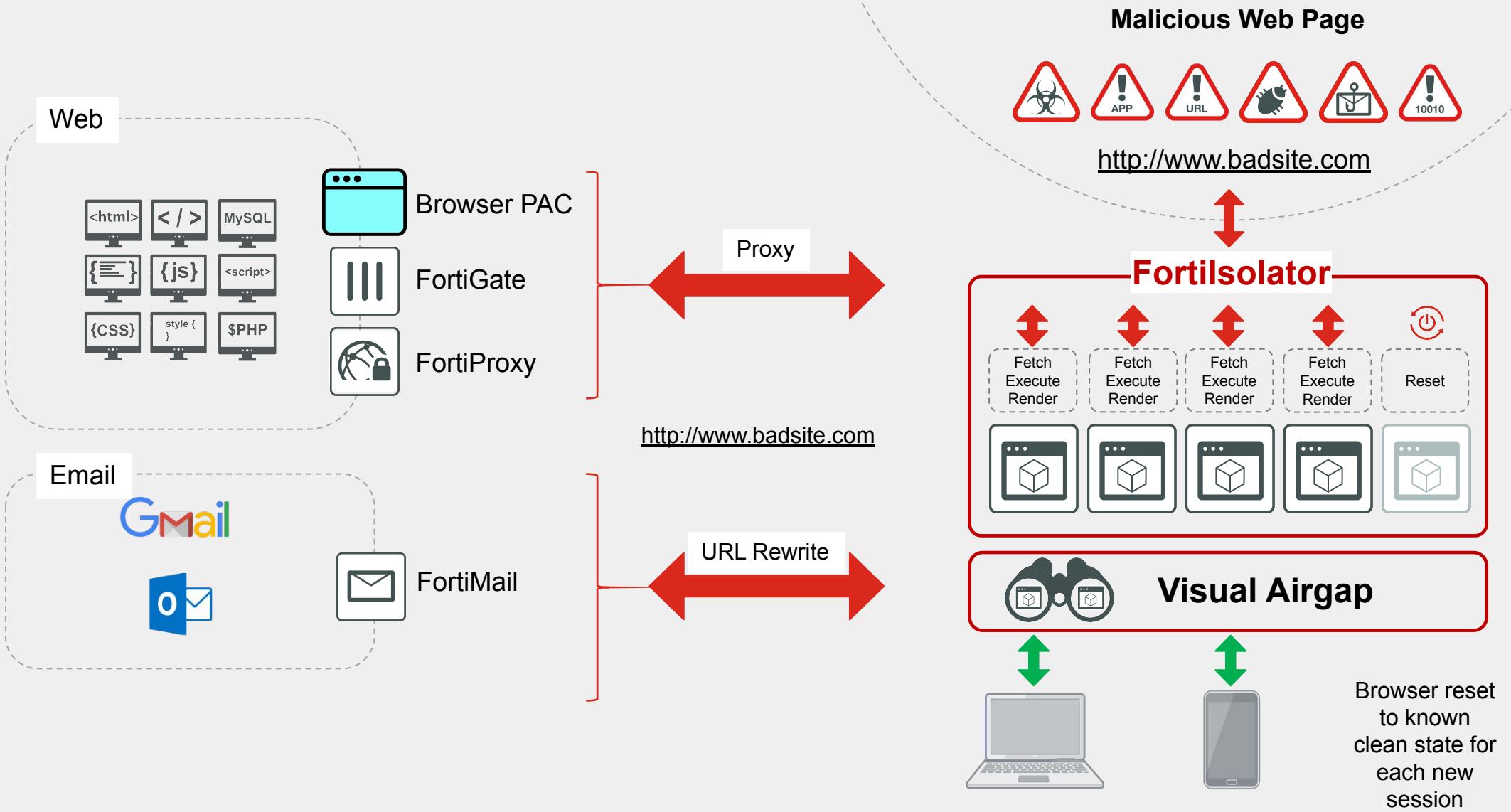
解決過度阻擋的問題

Web 控管策略

- ***VIP用戶*** **特權瀏覽**
- ***總是允許*** **特定URL類別及網站**
- ***總是阻擋*** **特定URL類別及網站**
- ***關鍵問題*** **– 灰色地帶**
  - **過度阻擋 – 造成用戶問題，體驗不佳**
  - **寬鬆政策 – 惡意軟體風險增加**

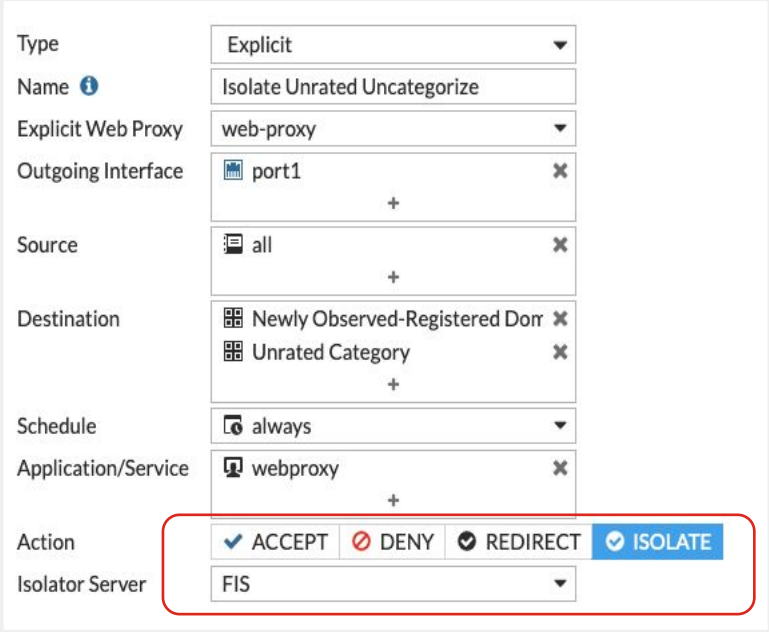


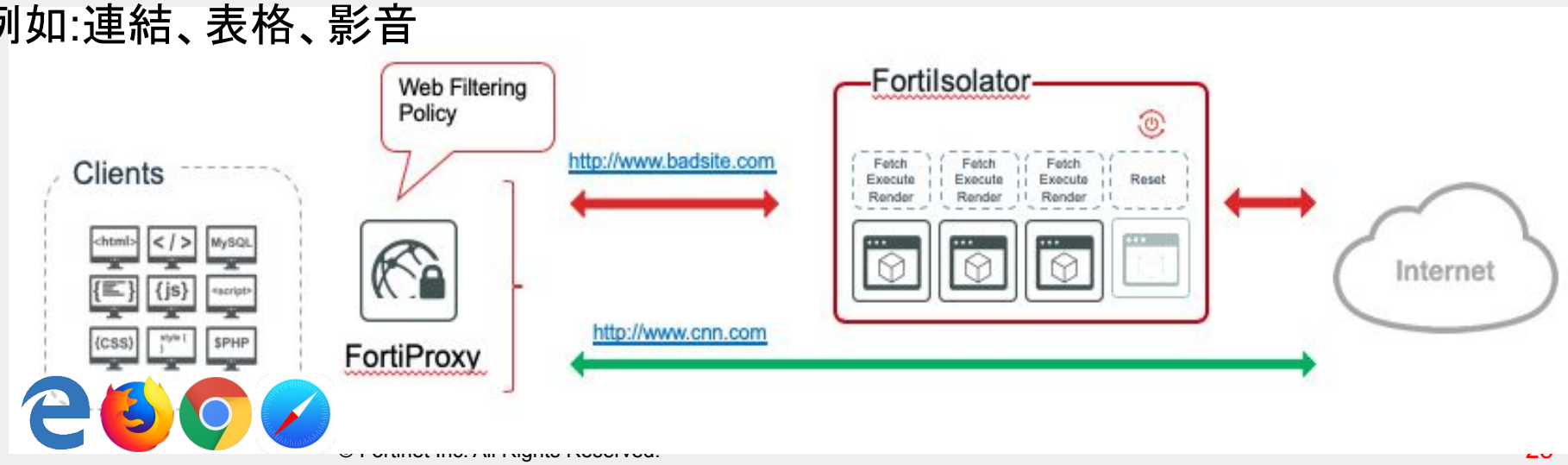
上網隔離(FIS)怎麼運作



隔離瀏覽- 零信任Web存取

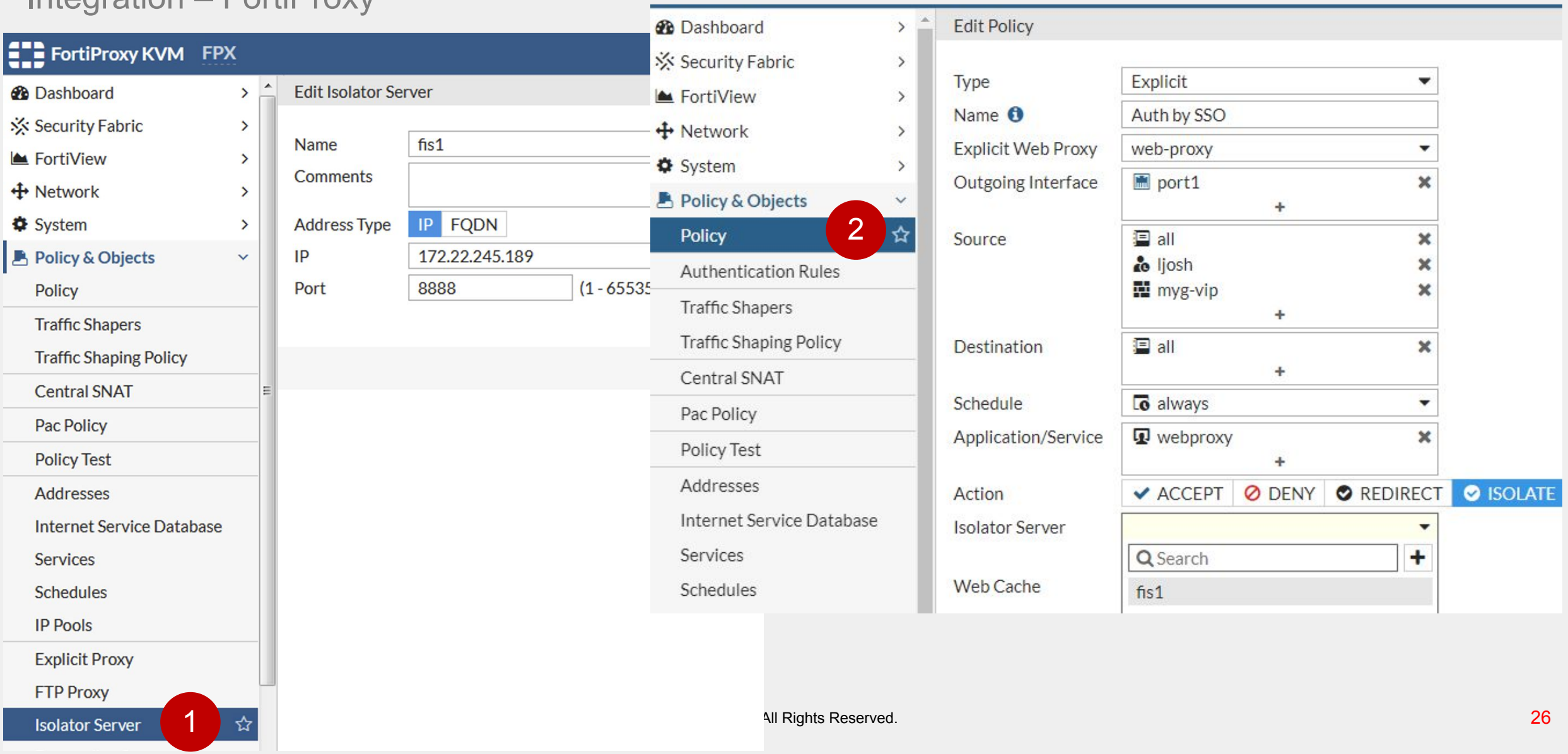
- 毋須安裝用戶端程式在本機電腦
  - 相容支援HTML5的瀏覽器
  - 使用原來慣用的瀏覽器軟體，就能得到上網防護
- 消除上網產生的惡意威脅，同時保持生產力
  - 沒有第三方程式碼在本地電腦上運行
  - 瀏覽連線在乾淨的容器(Container)中運行
  - 安全的網頁內容呈現給用戶端
  - 支援互動式網頁，例如:連結、表格、影音





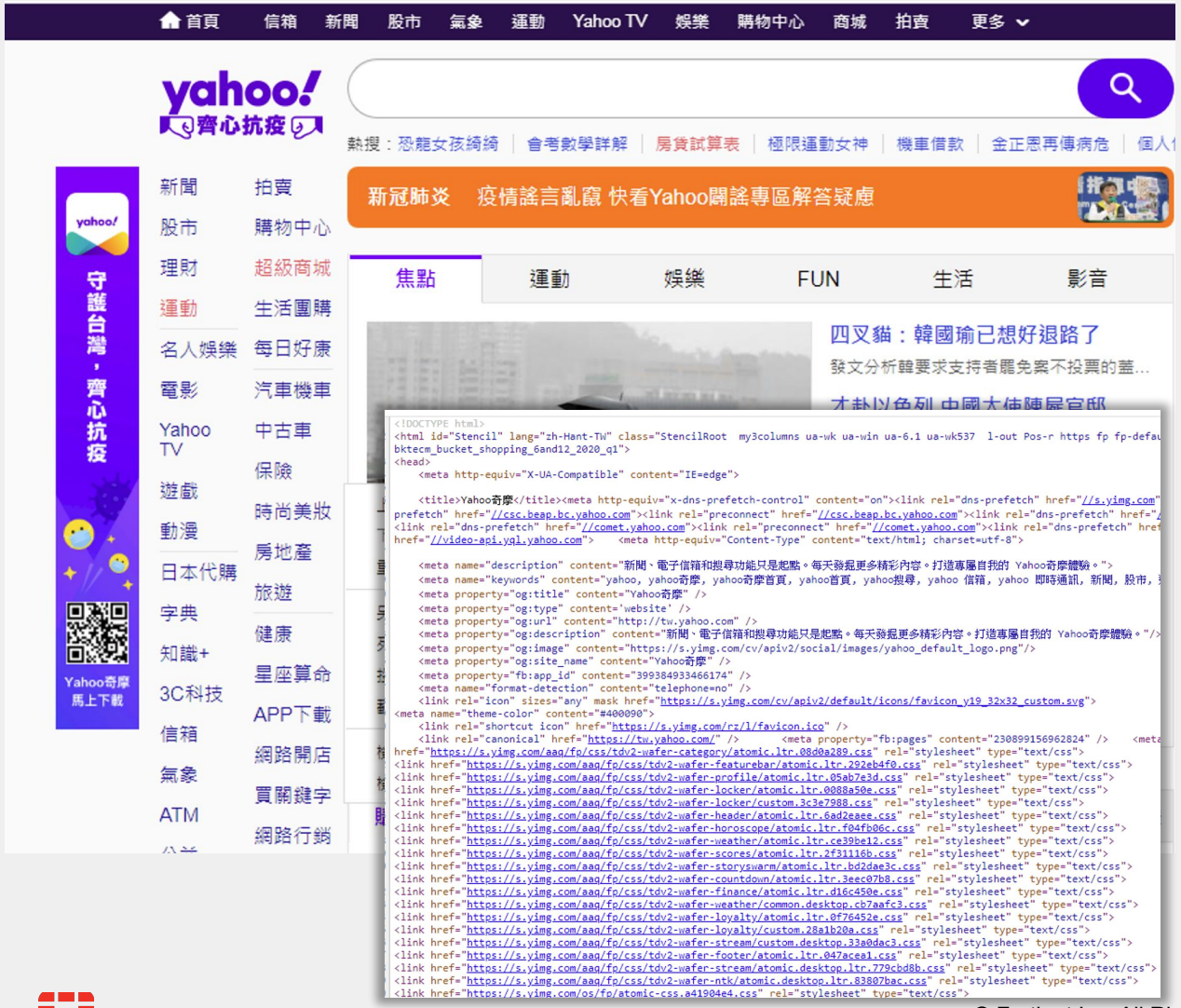
簡易的設定，讓你幾乎忘了曾設定過

Integration – FortiProxy

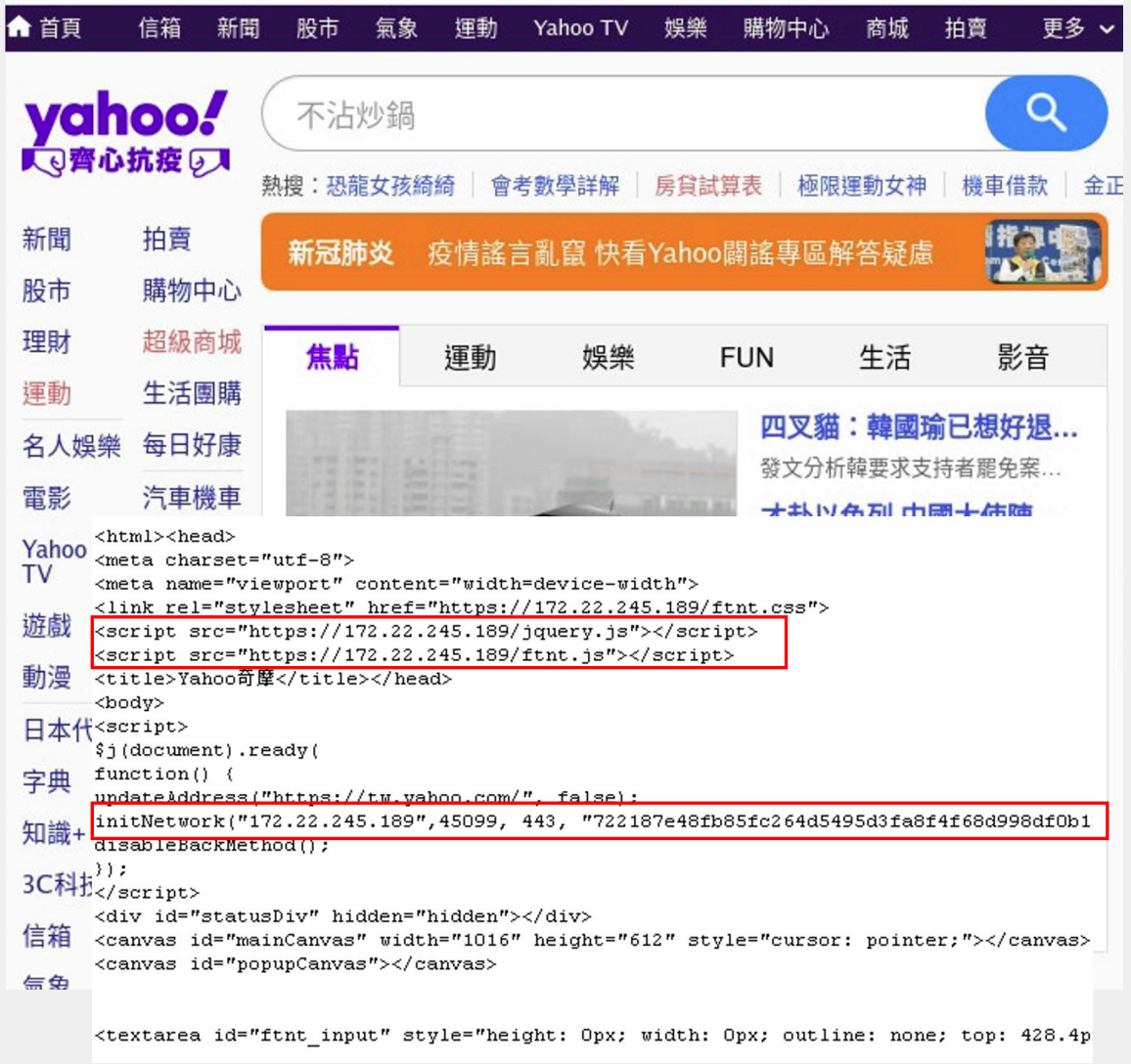


隔離前後差異

Before Isolation



After Isolation



加密流量管理工具怎麼選

3加1口訣

好的加密流量管理解決方案:

- **加值**現有的安全基礎設施防護能力
- **加強**可視性，打擊隱藏在加密流量的安全威脅
- 確保機密數據，如針對醫療保健和銀行網站間溝通的訊息，仍可保持**加密**狀態
- 專屬**一台**為應付 SSL 流量所開發的高效能高安全性解決方案


FORTINET