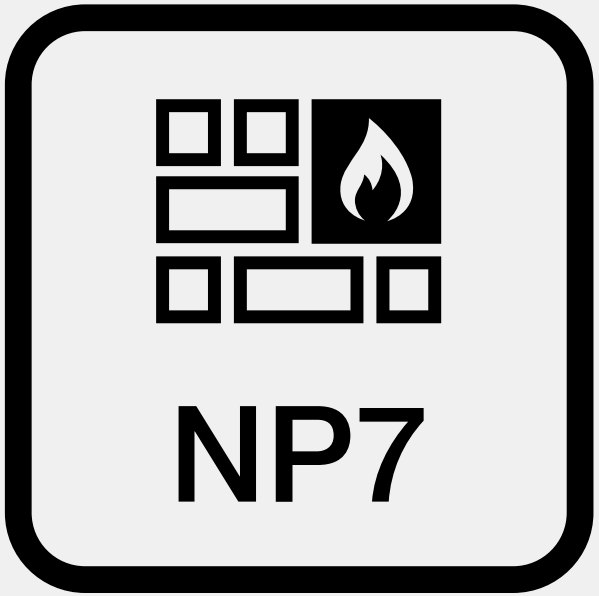
Lucky Number
引領資安防禦全面升級

Paul Li

Technical Consultant Taiwan



What's New in Version 7

軟硬整合
資安防護全面升級

NP7 整合 FortiOS 7.0

Ultra Scalable Chassis
FG7121F

資安無死角
防護鋪天蓋地

SOC Services:
SOC as a Service Offering
FortiGuard Outbreak Alert Subscription

ZTNA
Expanded DNS Security
FortiGuard Video Filtering Service

AI 智能
高效營運

Simplify and Automate
Support for Security Fabric in Multi-VDOM mode

Automate
Automation Workflow Improvements

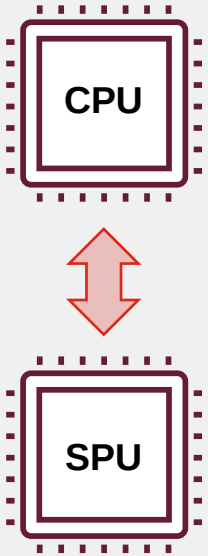
NP7

Security
Processing
Unit

Fortinet 專屬資安處理晶片 Security Processing Unit (SPU)

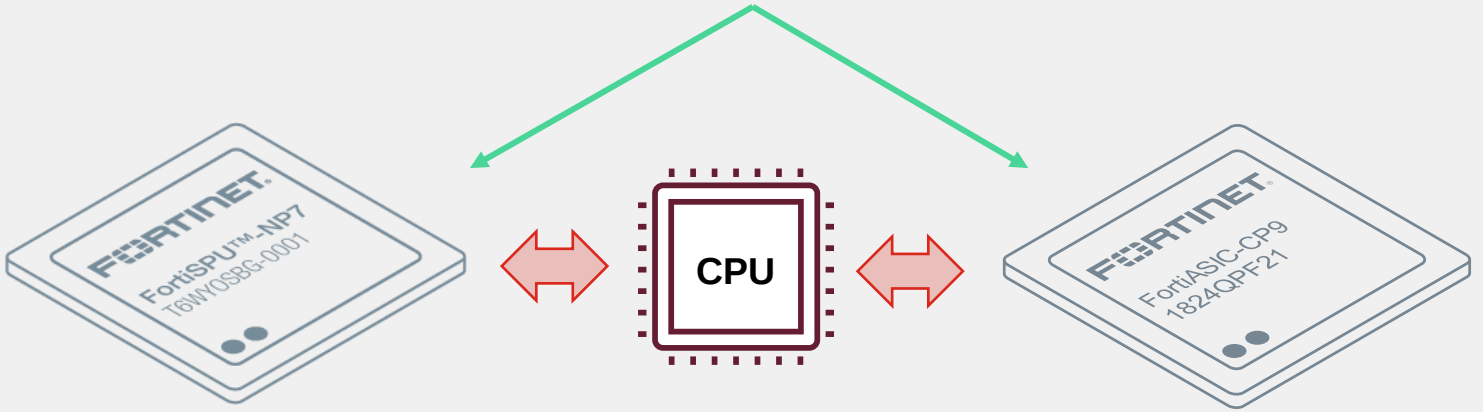
NP7 跨世代安全流量處理晶片掀起資安效能變革

FortiGate Systems



Security Processing Unit (SPU)

Security Processing Unit (SPU)



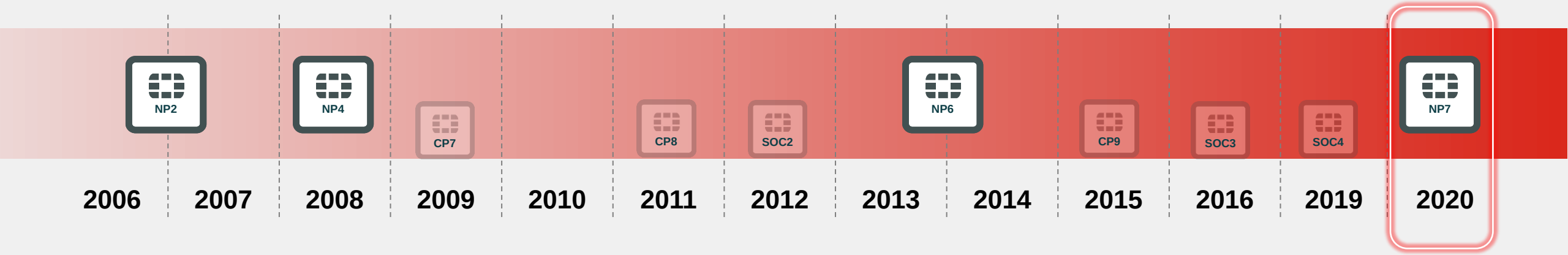
Network Processor (NP)

Off-Loads Networking Functions

Content Processor (CP)

Off-Loads Security Functions

重新定義大數據中心資訊安全效能輸出



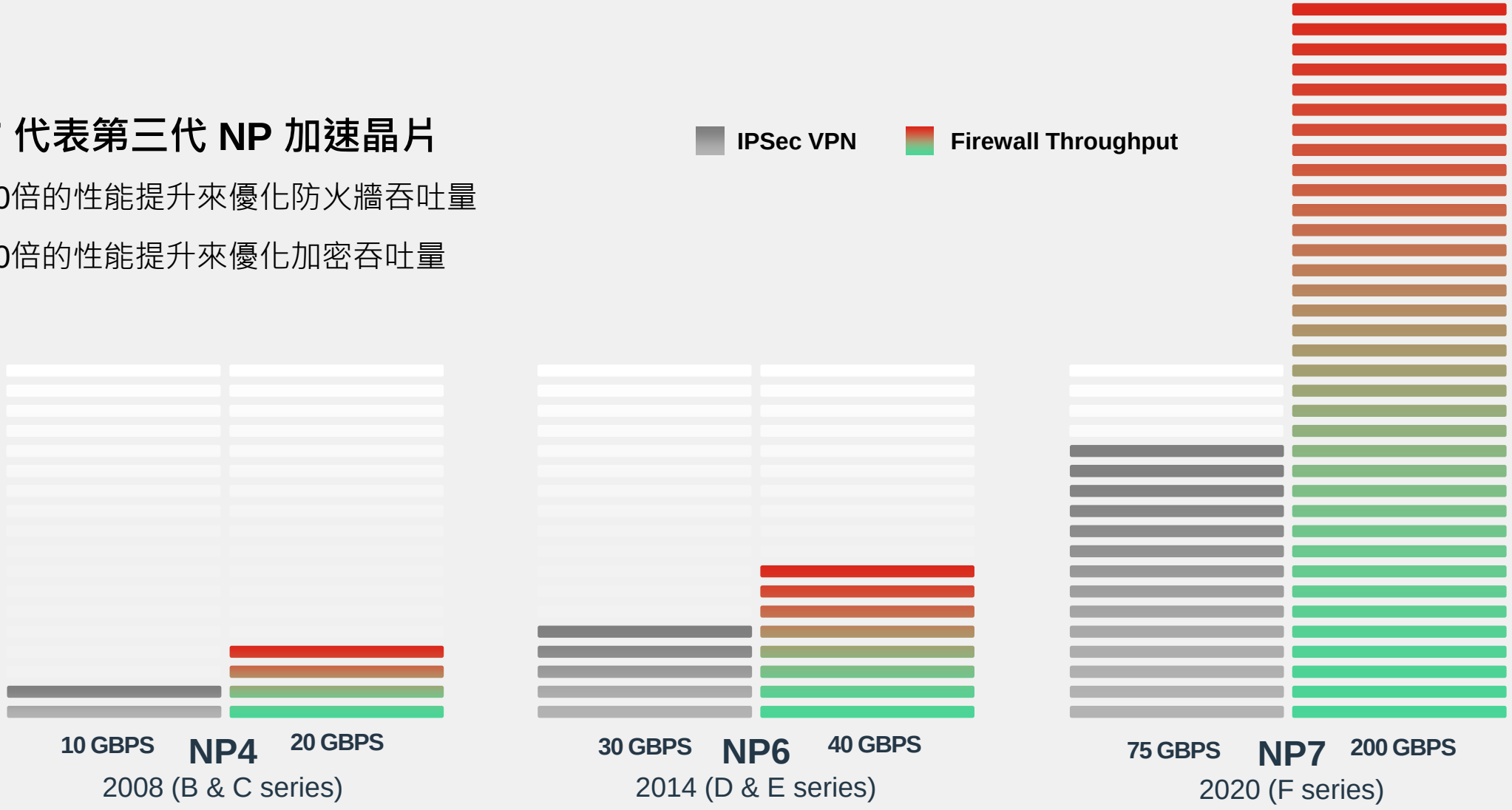
NP7 安全流量處理晶片超越競爭對手，以次世代的效能輸出提升資安防護等級

2 X 100 G	100 M		2 M/SEC	200GBPS	75 GBPS	VXLAN	20 W
NETWORK PORTS	CONCURRENT SESSIONS	HARDWARE LOGGING	SESSION SETUP RATE	FORWARDING THROUGHPUT	IPSEC THROUGHPUT	NVGRE	POWER ESTIMATION

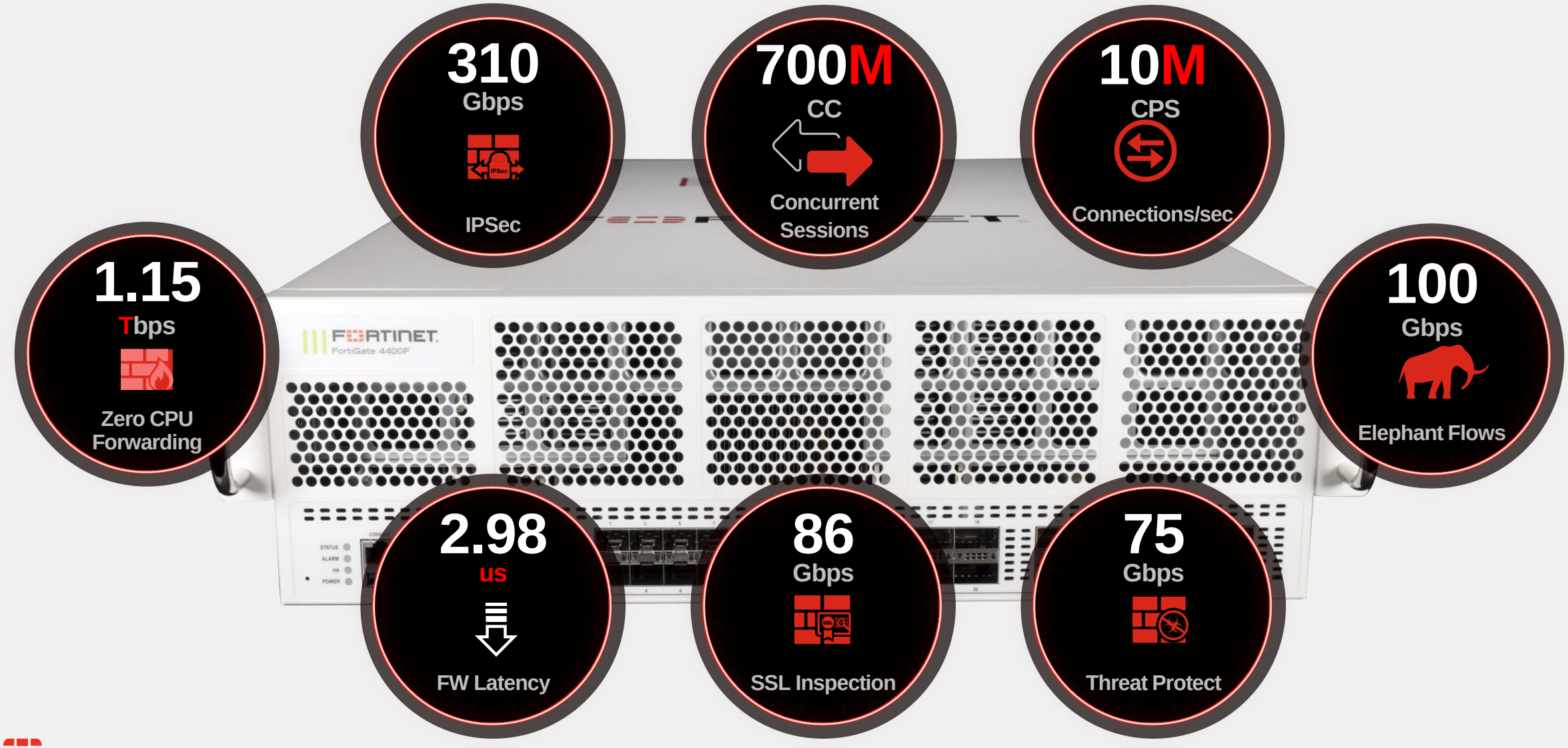
High Performance DNA

NP7 代表第三代 NP 加速晶片

- 以10倍的性能提升來優化防火牆吞吐量
- 以10倍的性能提升來優化加密吞吐量

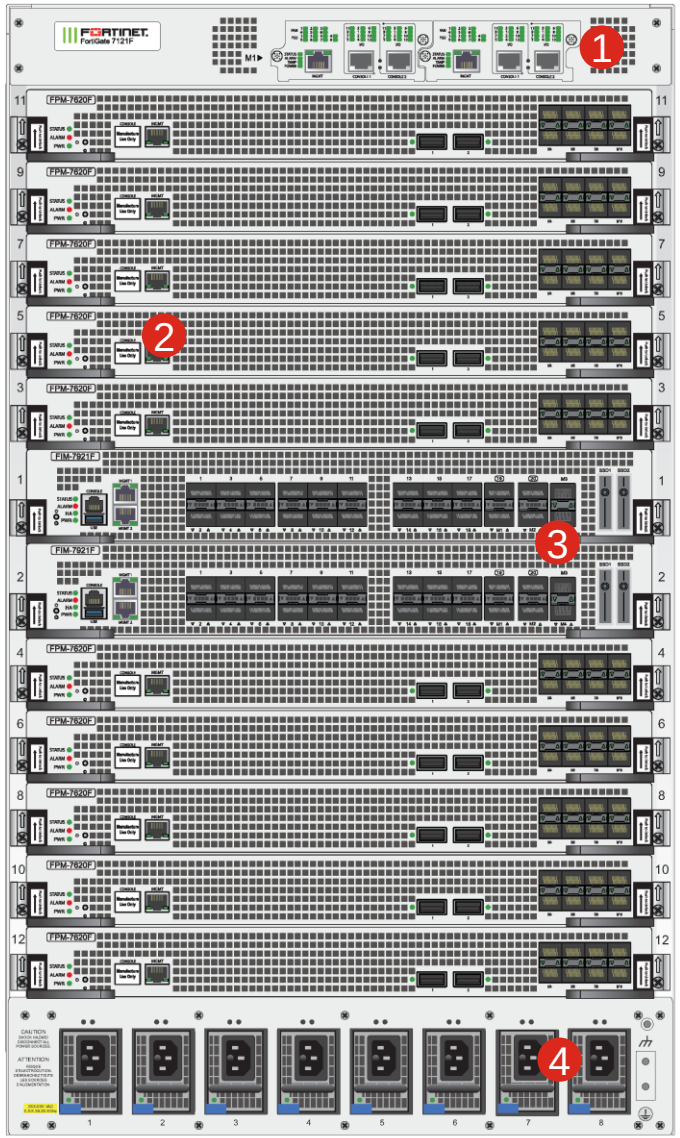


FortiGate 4400F 高效能硬體規格



FortiGate 7121F

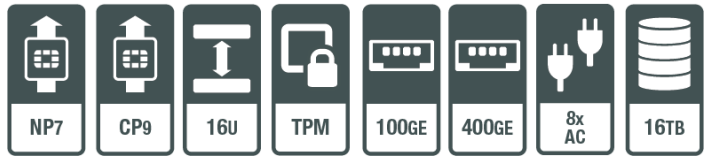
次世代資料中心高等級機箱防護演進



1. SMM: System management Modules
2. FPM: processing Modules
3. FIM: Interfaces Modules
4. 4+4 Hot Swappable Redundant PS

① 2 x Management Modules
② 10 x FPM-7620F Processing Modules
③ 2 x FIM-7921F I/O Modules
④ 8 x Hot Swappable Redundant PS

FG7121F Base Hardware Bundle
→ 2x FPM-7620F + 2x FIM-7921F
FG7121F Full Hardware Bundle
→ 10x FPM-7620F + 2x FIM-7921F



1.89 Tbps
Firewall throughput

9 Mil
New Sessions/Sec

1 Billion
Concurrent Sessions

675 Gbps
SSL Inspection Throughput

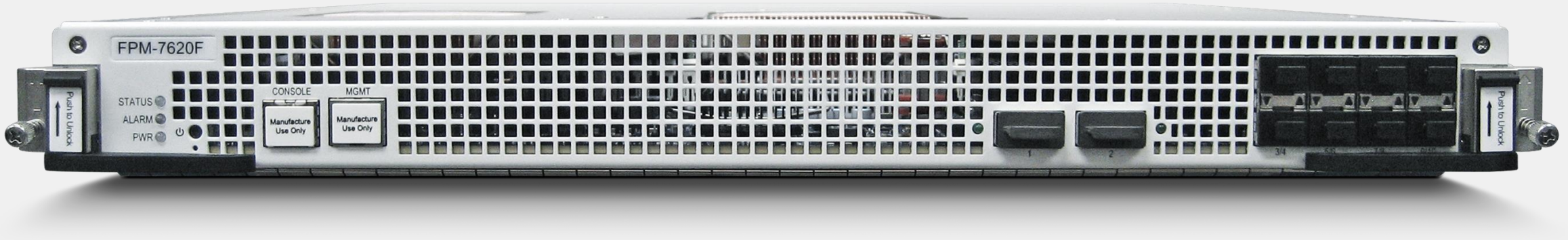
675 Gbps
IPS Throughput

550 Gbps
NGFW Throughput

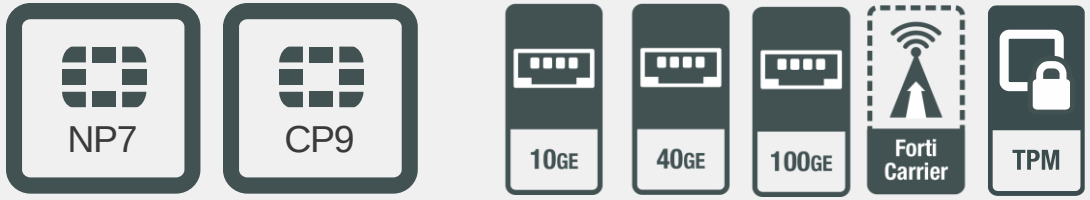
520 Gbps
Threat Protection Throughput

** Specs with fully populated FPMs*

FortiGate Processor Module FPM-7620F (效能模組)



Interface	8x 10GE/ 25GE SFP28 Support 2x 100GE QSFP28 Support
SPU	▪ 2x NP7 ▪ 8x CP9
Flexibility	▪ FPM includes front interface traffic ports ▪ 2x QSFP28 100G ▪ 8x SFP28 10/25G Support
Performance	**67.5G IPS Performance*** **52G Threat Protection***



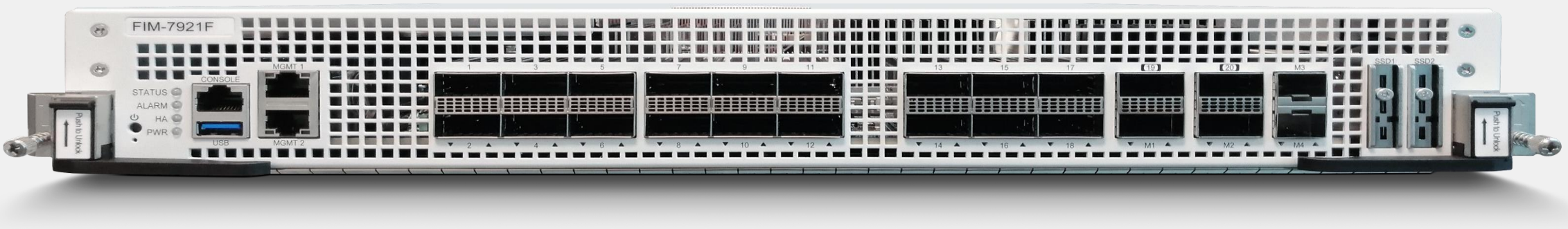
Large Enterprise / Data Center / Service Provider

NGFW / ISFW / DCFW /CCFW

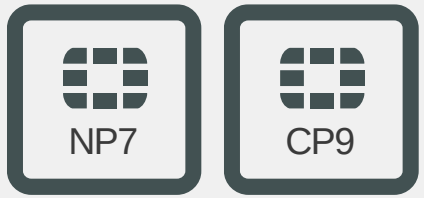
Flexible Deployment Options

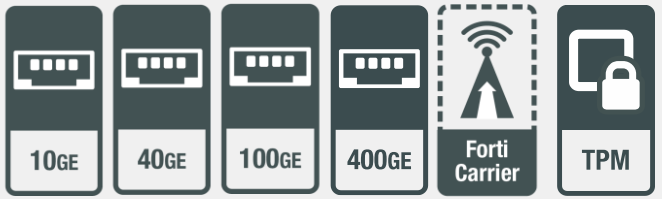
** Target specification subject to change*

FortiGate Interface Module FIM-7921F (介面模組)



Interface	▪ FIM-7921F: ▪ **18x QSFP28 100G Support** ▪ **2x QSFPDD 400G Support** (Max combination 2x FIM per chassis) ▪ Includes Disk Support
SPU	▪ 5x NP7
Performance	**12.8 Tbps Switch Fabric performance** **1 Tbps between FIMs**



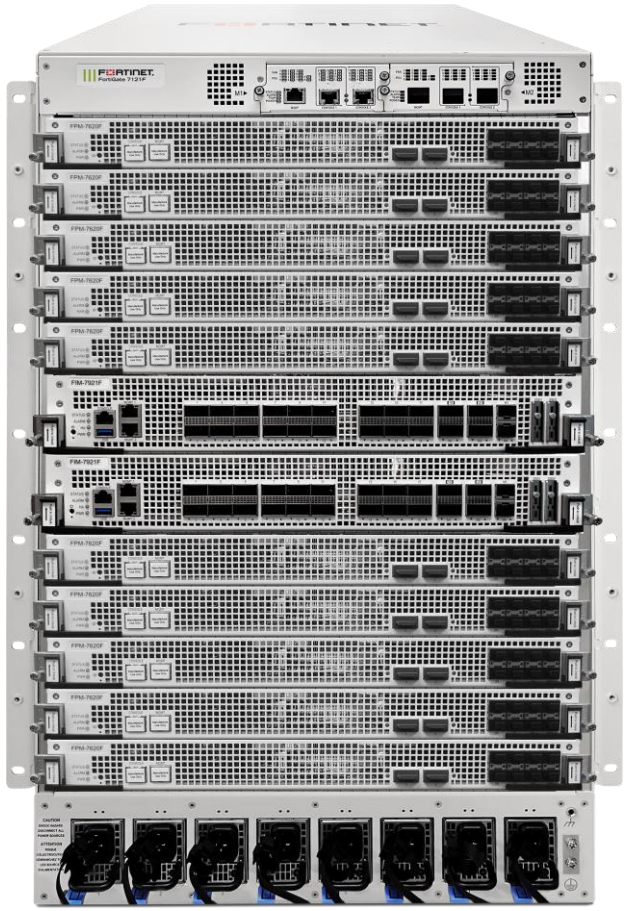


Large Enterprise / Data Center / Service Provider

NGFW / ISFW / DCFW /CCFW

Flexible Deployment Options

FG7121F 定價結構 (加量不加價)



- **FG7121F 基本硬體套件組 (Base Hardware Bundle)**
  is with **2x** FPM-7620F (效能模組) + 2x FIM-7921F (介面模組)
- **FG7121F 高效能硬體套件組 (Full Hardware Bundle)**
  is with **10x** FPM-7620F (效能模組) + 2x FIM-7921F (介面模組)
- **FortiGuard 服務訂閱成本以及 FortiCare 訂閱費用以基本硬體套件組 (Base Hardware Bundle) 為計價單位**
- **新增的 FPM 效能模組除提升防護效能外，不會有任何額外的訂閱費用或效能級距費用 (加量不加價)**

Overview

What’s New in FortiOS 7.0

FOS 7 – 新增 300 項功能，資安防禦全面升級

Security Driven Networking (**SASE Edge -** SASE)

- Securing remote workforce with orchestration portal for SASE capabilities
- Securing thin branch with FEX 200F + 25Mbps subscription
- New Thin Edge line us (LTE/5G)
- Journey to Zero Trust with extended risk posture checking

Security Driven Networking (**WAN Edge:** SD-WAN)

- Increased Resiliency (FEC/DUP)
- Enhanced packet duplication
- Accelerated Convergence (FWF 80F)
- Efficient Operations (scalable ZTP, Analytics, Passive WAN Measurement)
- Accelerated convergence for Thin & WAN edge

Security Driven Networking (**DC Edge:** NGFW)

- Ultra-Scalability with pay as you grow model (FGT 7121F, 400G)
- Attack surface Reduction (Video filtering , DNS)
- Efficient Operations with network automation (Policy Learn mode, automated upgrades)

Security Driven Networking (**LAN Edge:** WiFi/Switch)

- Unified code base (L3 FortiLink, NAC Visibility and Zero trust response)
- Convergence (WLM and AIOps on FMG, FortiLAN cloud)
- Simplified Operation AI/ML driven wireless easy classification and remediation)

Security Driven Networking (**LTE Edge:** 5G)

- 5G backup (+SD-WAN for WWAN with new dual modem)
- LTE portfolio expansion (+WWAN application release, 101F/201F)
- SASE bundle for Thin edge and remote workers

Zero Trust Access (ZTNA)

- single policy for on-net / off-net behavior
- Better & easier VPN with automated setup for HW/VM//SASE & cloud
- Granular access with role based application access
- Leverage existing products

Adaptive Cloud Security (VM, CWP, CASB)

- Centrally managed hybrid cloud (expended support & multi tenant policies)
- Effective usage of resources with autoscaling
- Extended application support for CASB
- Container guardian

Adaptive Cloud Security (WAF & Email)

- Email continuity switch to FortiMail cloud when service go down
- FortiWeb enhanced with ML-based API discovery, deeplearining and more.
- FortiADC/FortiGSLB user experience visibility and Auto-Scaling capabilities

FortiGuard Thre*at Intelligence* (Security Services)

- Increased Attack Surface Coverage – Video Filtering enhancement to our web filtering offering
- Security Rating expended to **Fabric Rating**
- **IoT real-time query service**

Fabric Management Center (SOC)

- MITRE attack analysis with expansion in cover and automated protection across the fabric and ecosystem
- SOAR enhanced AI/ML & out-of-the-box content packs. Intergrations. FSR cloud. mobile app.
- IR unified console, FORTISOAR container, FortiCASB connector

Fabric Management Center (NOC)

- Insider threat analysis with EUBA support
- Enhanced visibility with extended product support across the Fabric & SD-Branch
- Efficient and scalable operation with SIEM
- SaaS management with Unified GUI, easy on boarding with ZTP templet and more & efficient full branch operations

Advance Services

- SOC as a Service to augment organization and MSSP's SOC
- Best Practice Evaluation
- FortiGuard Consultant

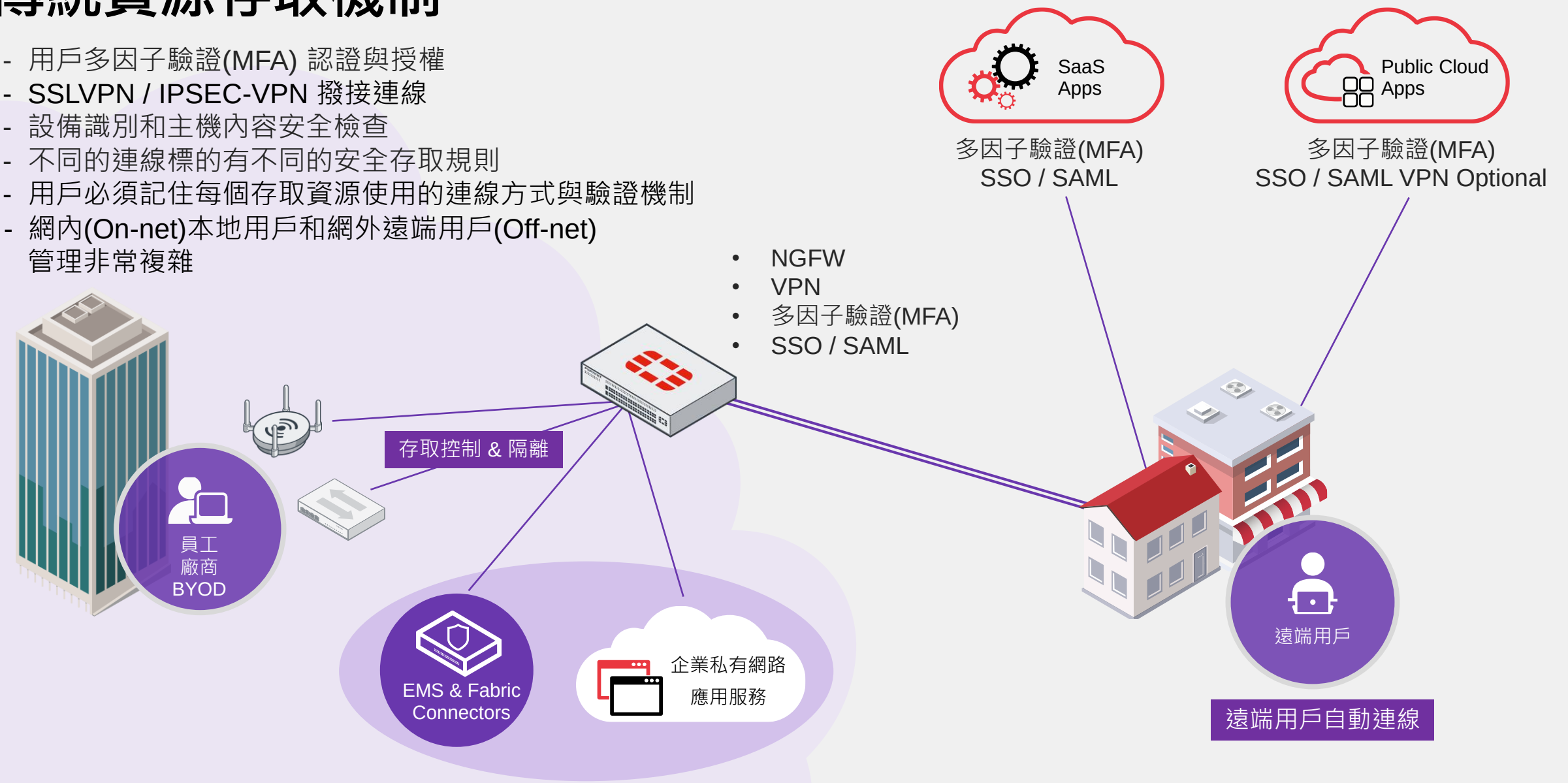
有效管理公司內、公司外的連線人員與連線設備識別、驗證與授權

Users and Device Security

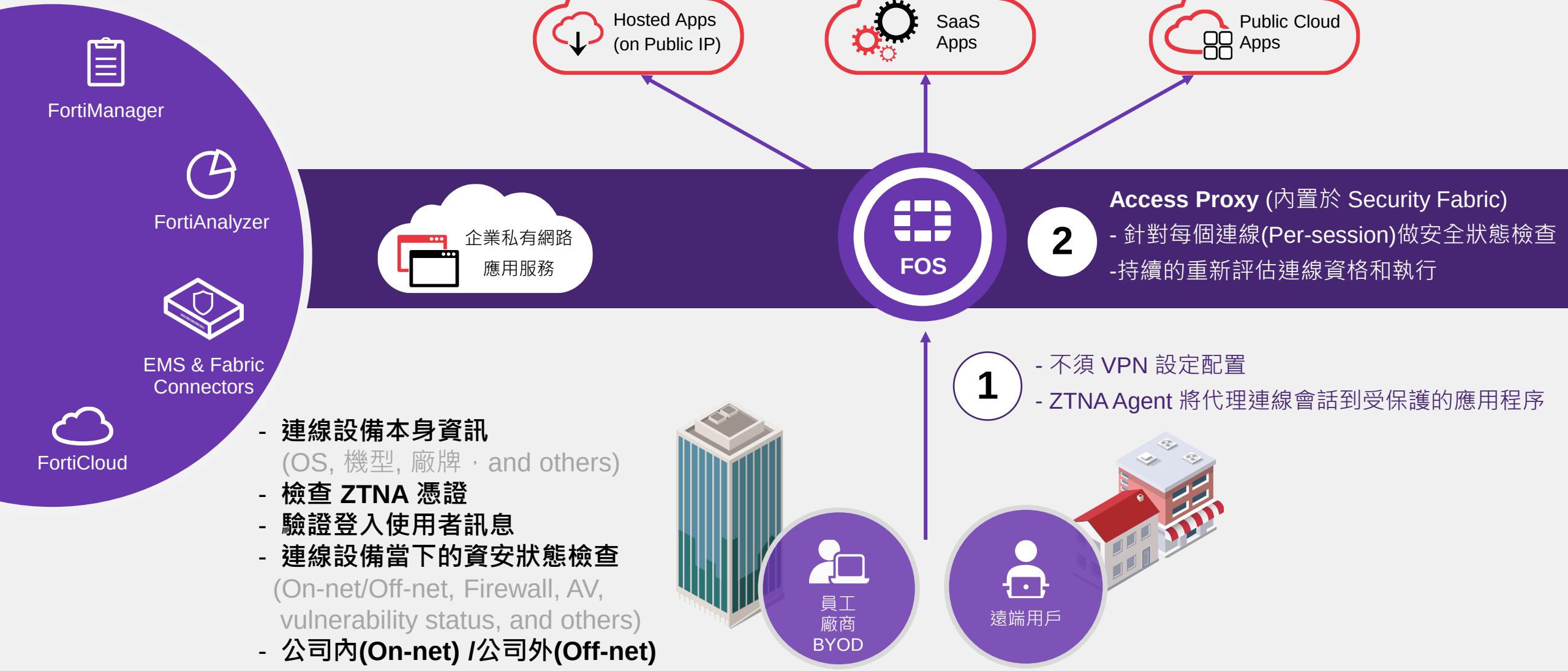
Zero Trust Access
零信任存取

傳統資源存取機制

- 用戶多因子驗證(MFA) 認證與授權
- SSLVPN / IPSEC-VPN 撥接連線
- 設備識別和主機內容安全檢查
- 不同的連線標的有不同的安全存取規則
- 用戶必須記住每個存取資源使用的連線方式與驗證機制
- 網內(On-net)本地用戶和網外遠端用戶(Off-net)
  管理非常複雜



遠端存取變革 (ZTNA)



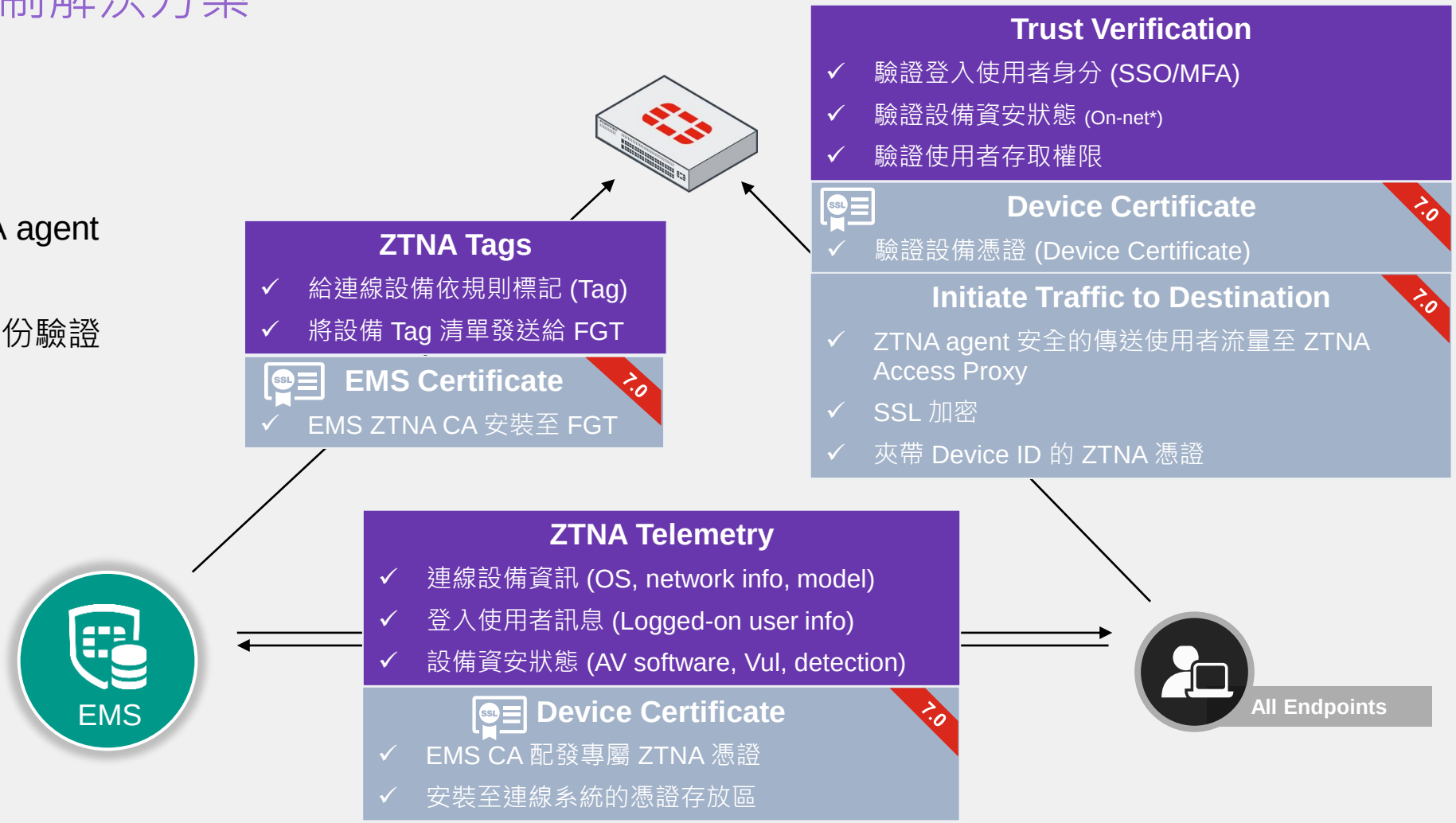
- **連線設備本身資訊**
  (OS, 機型, 廠牌，and others)
- **檢查 ZTNA 憑證**
- **驗證登入使用者訊息**
- **連線設備當下的資安狀態檢查**
  (On-net/Off-net, Firewall, AV, vulnerability status, and others)
- **公司內(On-net) /公司外(Off-net)**

零信任存取機制 Zero-Trust Network Access

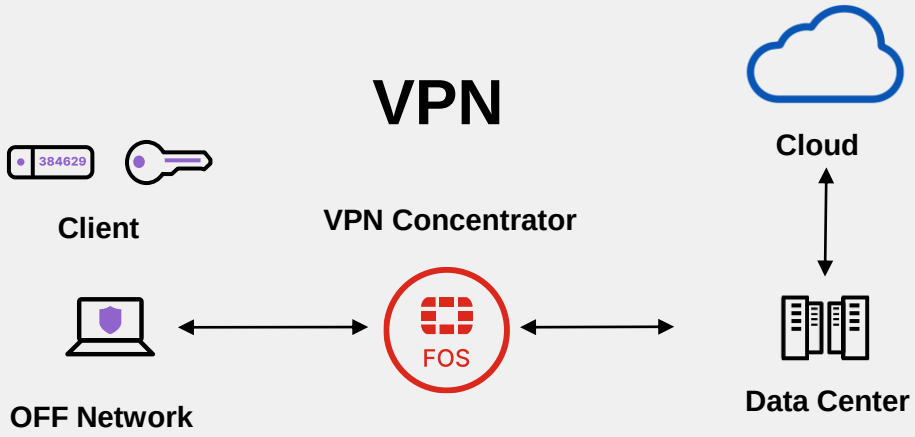
全新零信任存取機制解決方案

增加了新功能來支援新的零信任解決方案

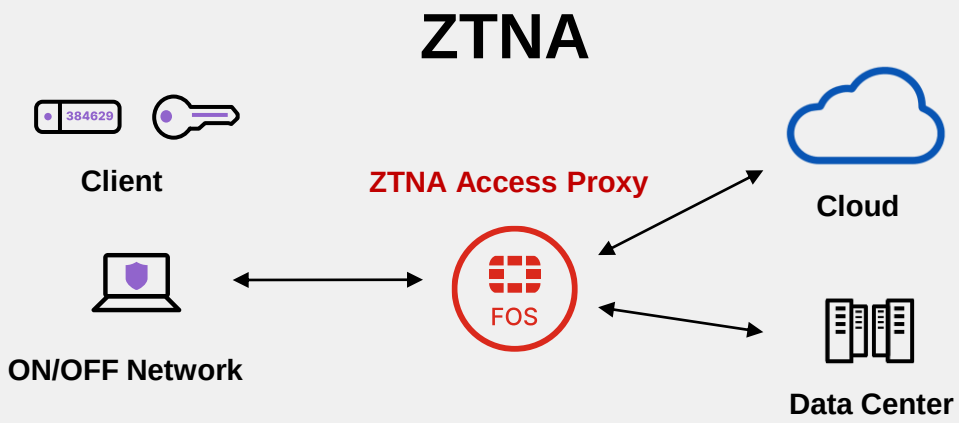
- 使用 FortiClient 作為 ZTNA agent 的 HTTPS 存取代理服務
- 證書(ZTNA certificate)的身份驗證強化存取信任驗證



從 A 到 A+，傳統 VPN 到 ZTNA 的變革



- 登入時一次性的檢查
- 基於網段的存取
- 傳統的防火牆控制策略



- 持續性的資安狀態檢核
- 針對指定應用服務提供存取
- 使用者狀態上下文規則控制策略

Fortinet ZTNA 優勢

資安完整覆蓋 vs. 其他 ZTNA 解決方案

利用既有已投資的公司資產(次世代防火牆)

- 大多數的 ZTNA 解決方案是 SASE 服務商其中一項資安功能選項，伴隨著昂貴的訂閱費用
- 透過 FGT 可更快速的存取本地資料中心內的服務與資源
- 可運用 Fortinet SD-WAN, SD-Branch, Security Fabric 整合方案

專注於安全提升的 (“Secure ZTNA”)

- 延展 FGT 防護至企業提供服務的任何地方
- 存取流量穿越業界領導品牌 FortiGate 資安防護技術
- 提供 FortiGuard Labs services

無須添購額外的 License

- 只需啟用 FortiGate 和 FortiClient 中的 ZTNA 功能即可！
- 輕鬆的從 VPN Access 數位轉型至 ZTNA

在任何存取邊界提供企業資安防護和提升用戶使用體驗

Network Security

Security-driven Networking
安全驅動型網路

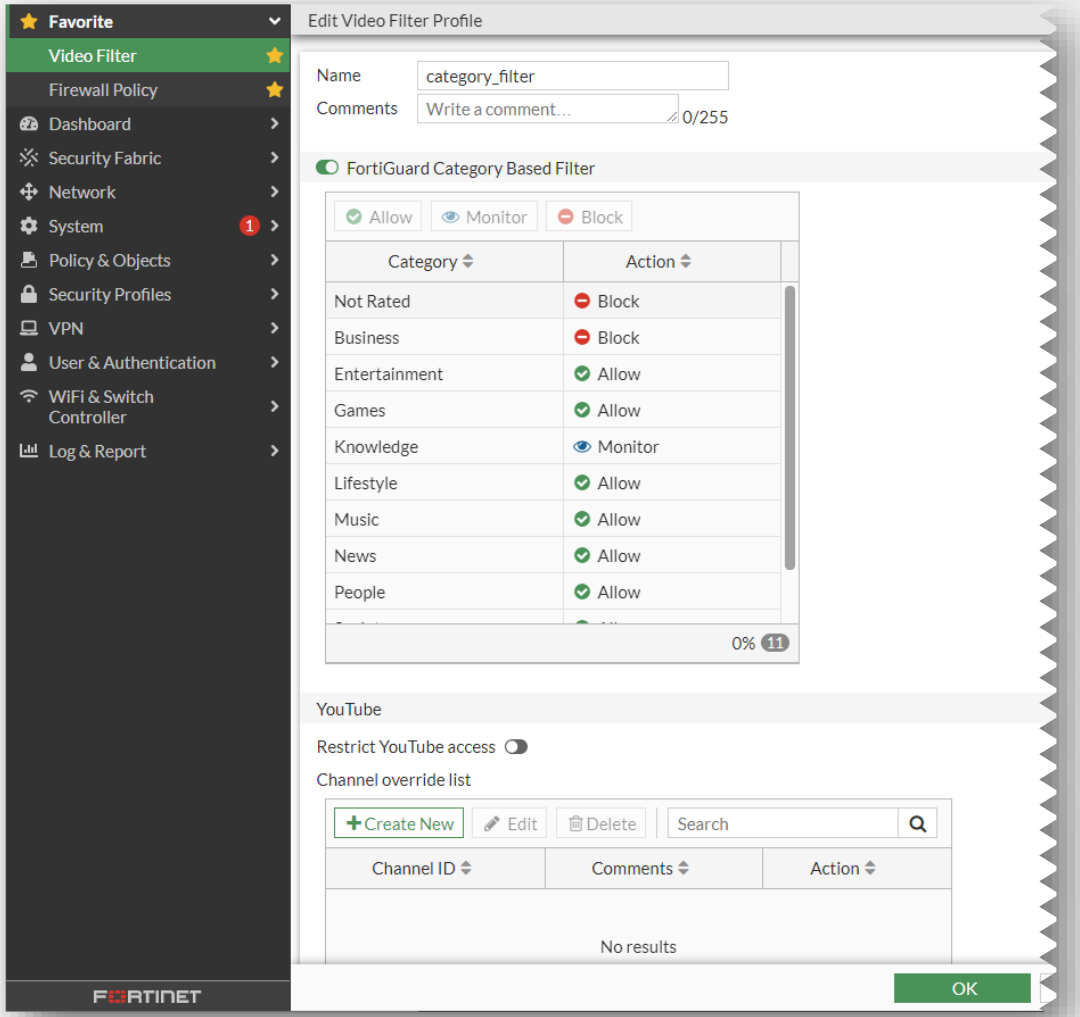
Security-driven Networking

FortiGuard Video Filtering Service (視頻過濾服務)

- **新增可對 YouTube、Vimeo、Daily Motion，依category rating (類別評級) 做視頻過濾**
- **可對 YouTube 的 channel ID 做 static filter (頻道覆蓋清單)**
  - 使用 video filter 配置設定，可以依 FortiGuard 類別評級分類挑選適合用戶觀賞的頻道.
  - 使用 video filter 配置設定，可以依個別 YouTube channel ID, 細緻的管理用戶可瀏覽的 YouTube 指定頻道或指定視頻.
  - Video filter 配置設定目前支援在 proxy-based policies 並且需要開啟 SSL deep inspection.

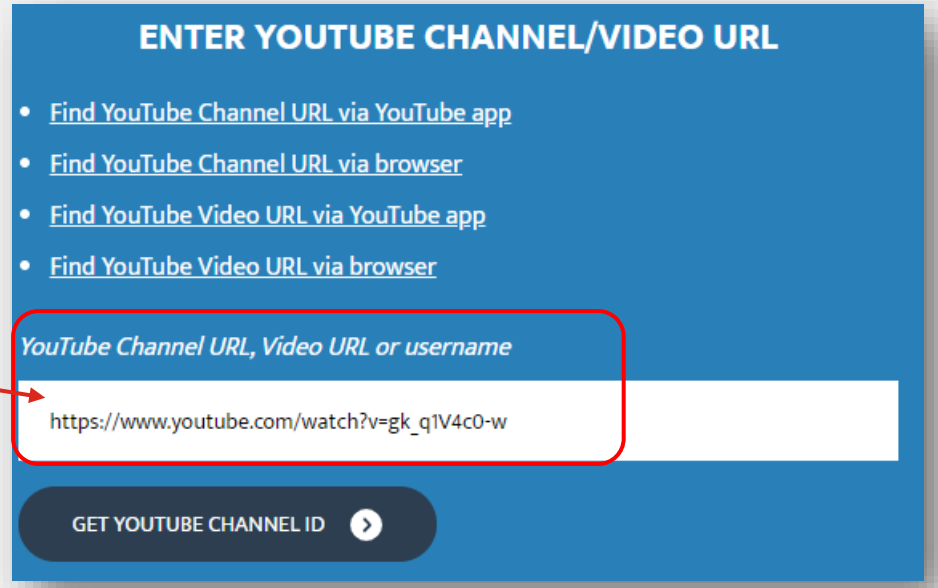
The following identifiers are used for YouTube channels:

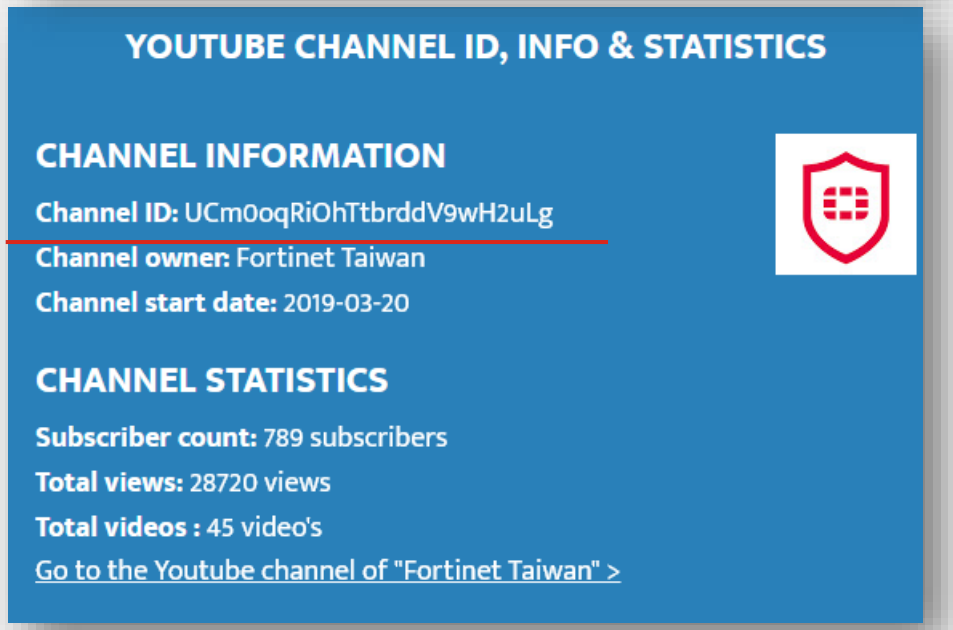
```
www.youtube.com/channel/<channel-id>
www.youtube.com/user/<user-id>
www.youtube.com/watch?v=<string>
```



Security-driven Networking

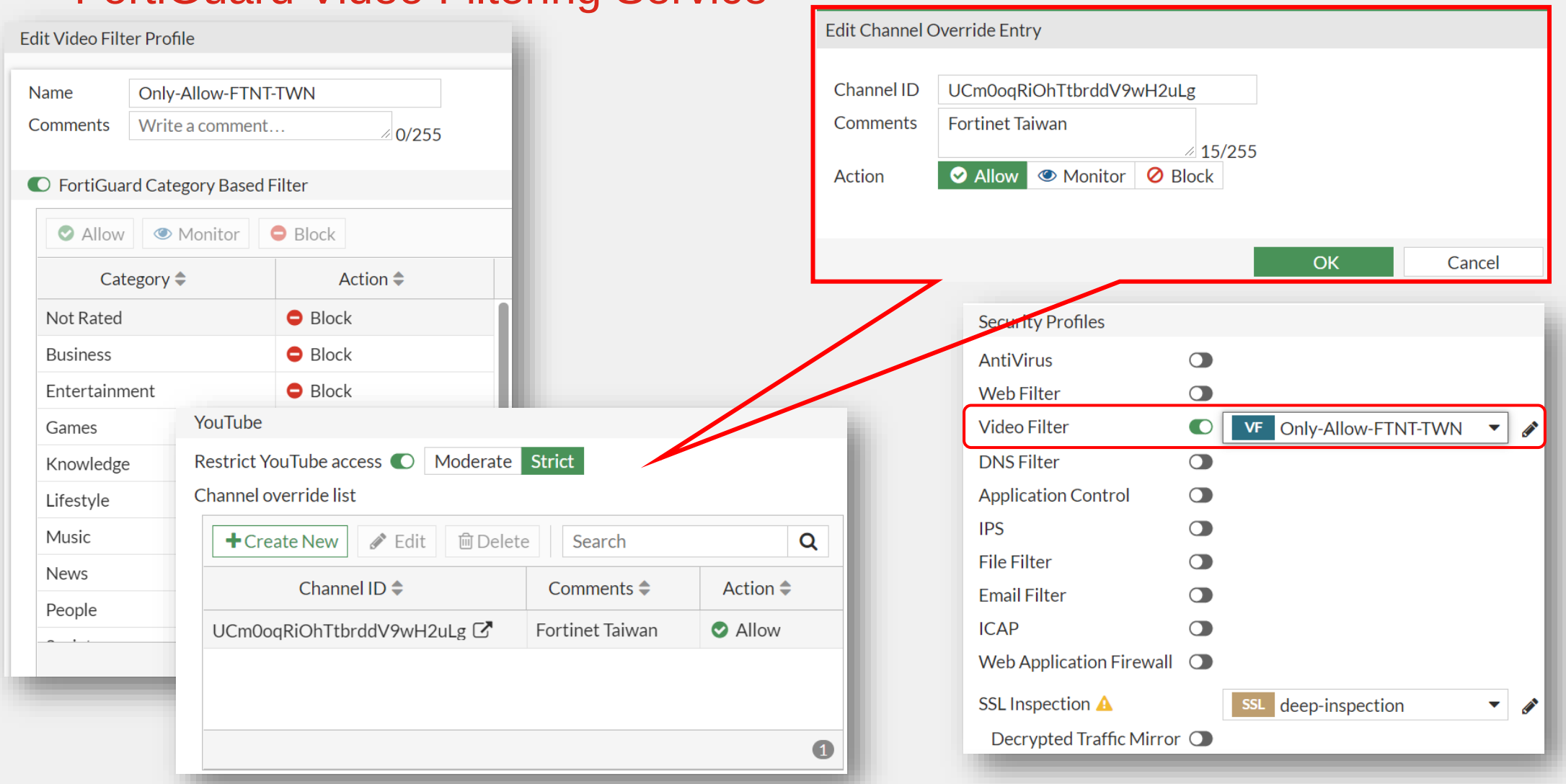
FortiGuard Video Filtering Service





Security-driven Networking

FortiGuard Video Filtering Service



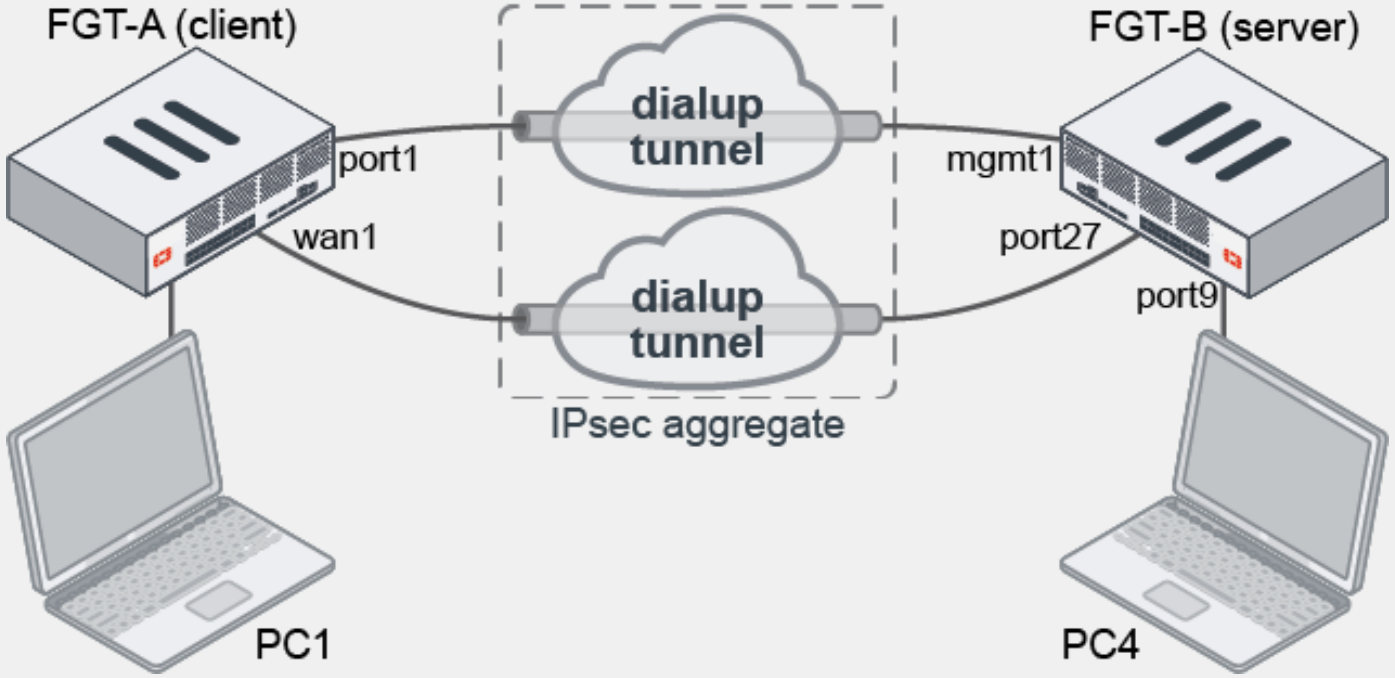
Security-driven Networking

Packet duplication Improvement (封包複製傳遞)

Packet duplication for dial-up IPsec tunnels

- 支援封包複製傳遞功能於站點與站點之間的 dial-up IPsec tunnels，每個 spoke 必須配置一個 location ID.
- 在 Hub 端，對 IPsec 聚合通道 (IPsec aggregate Tunnel)中具有相同 location ID 的 Tunnel 進行封包複製傳遞
- 在 Hub 端，可以聚合(aggregated) 具有相同 location ID 的多路 dial-up VPN 通道，並依據負載平衡演算法結果進行封包負載平衡

在以下範例中，將兩路 dial-up IPsec tunnels 配置為 IPsec 聚合通道 (IPsec aggregate Tunnel) 即可支援封包複製傳遞效果



Security-driven Networking

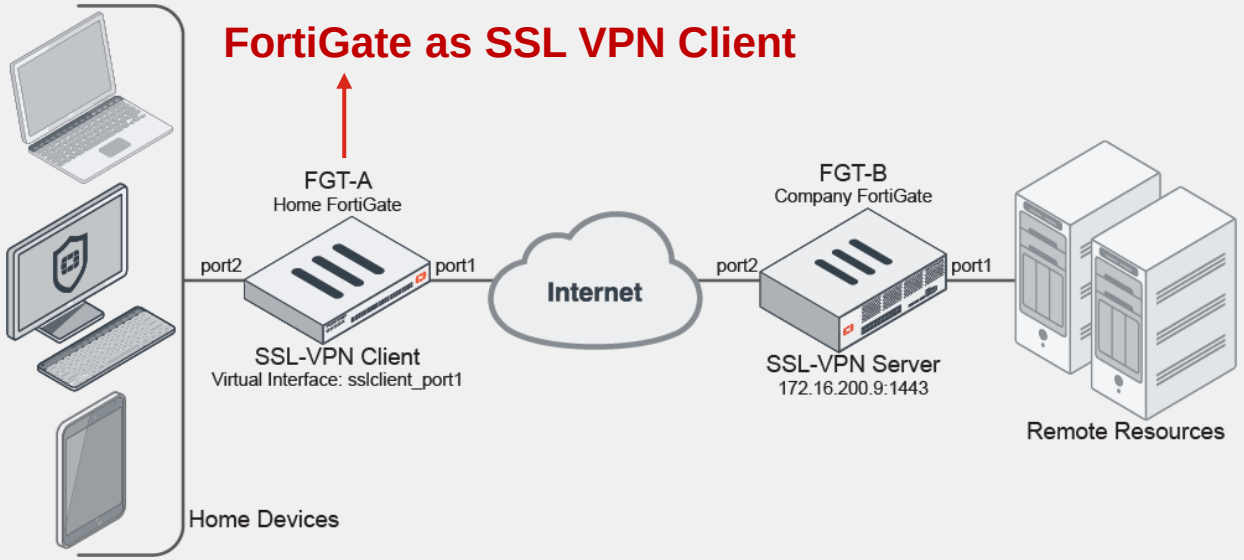
SSL VPN Client on FortiGate (FortiGate 也可做為 SSL VPN Client)

FortiGate as SSL VPN Client

- FortiGate 可以設定扮演 SSL VPN Client，透過 *SSL-VPN Tunnel* 介面型態連接
- 當 SSL VPN Client 連線建立完成後，client 端會動態的將 SSLVPN Server 端返回的網段資訊加入自身的路由表中
- FortiOS 7.0 可以設定扮演 SSL VPN Server，也可以扮演 SSL VPN Client，透過 SSL VPN Tunnel 連接
- 可規劃 SSL VPN hub and spokes 架構

這有助於避免因 ISP 或連線提供者**中間設備**引發的問題非常有用，例如：

- ESP packets (IP protocol 50) 被封鎖.
- UDP ports 500 (IKE) 或 4500 (IPSEC NAT-T) 被封鎖.
- Fragments 被丟棄, 如果對端設備不支援 IKE fragmentation，則會導致使用大size憑證的IKE 協商失敗

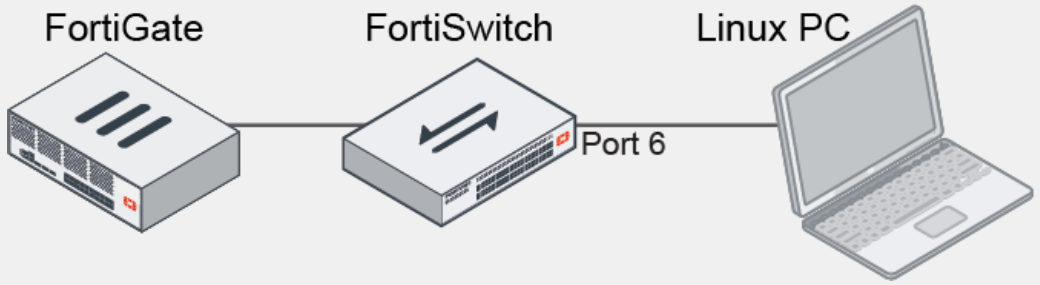


Security-driven Networking

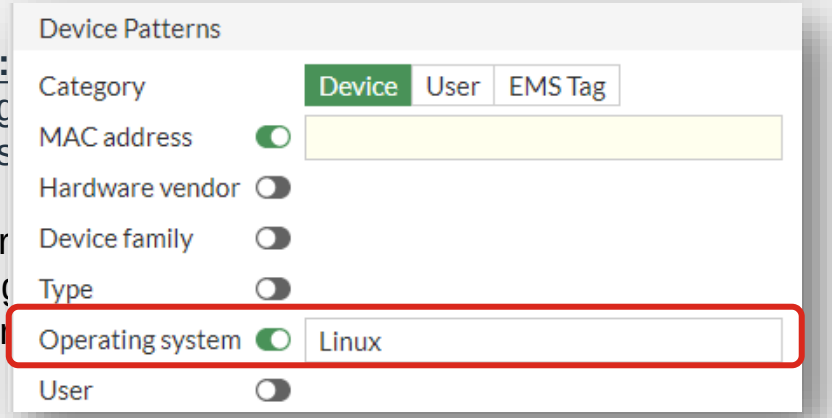
Integrated NAC feature on FortiSwitch (搭配 FortiSwitch 實現 NAC 功能)

- 可以在 FortiOS 中配置設定 FortiSwitch 網路存取控制政策(NAC policy)，僅允許符合指定條件的設備、屬於指定 User Group 的設備，或指定有安裝 FortiClient 並具備 EMS tag 的設備存取網路
- 可依設備識別後的狀態自動分配到專屬的特定 VLAN 或套用專屬介面參數

在以下範例中，
啟用並配置 NAC 設定，將 Linux PC 在接入網路並被辨識後，自動配置到 Linux 平台使用的 VLAN

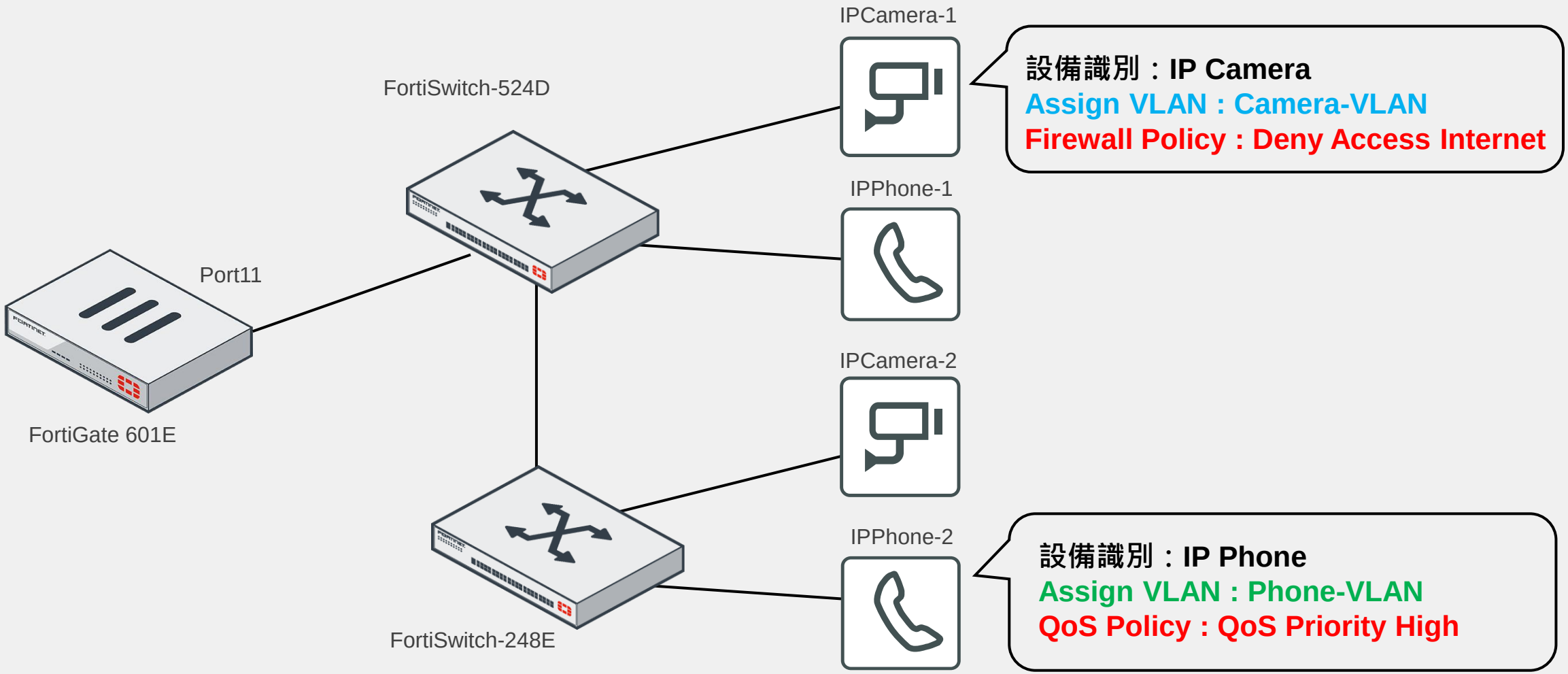



```
# diagnose user device get 00:
   vd root/0  00:11:32:24:91:90
created 6214173s  gen 1393
ip 10.1.200.151  src mac
hardware vendor 'Synology'
os 'Linux'  src tcp  id 163
host 'SYNOLOGY_DS213J'
```



Security-driven Networking

Integrated NAC feature on FortiSwitch



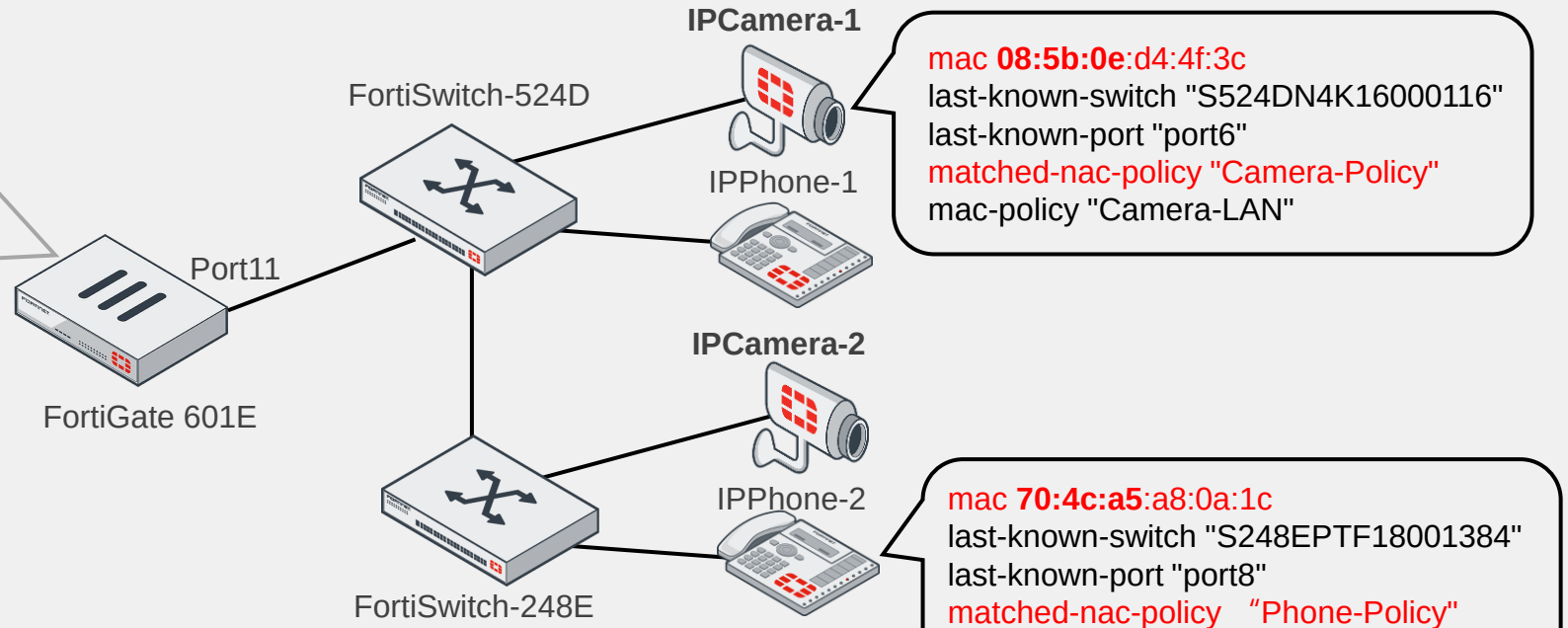
Security-driven Networking

Use wildcards in a MAC address in a NAC policy

在設定 NAC policy 時，可以在 MAC 地址使用 wildcard * 字元來套用指定製造商設備群

- 在以下範例中, IPCamera-1 與 IPCamera-2 的 MAC 地址都是以 08:5b:0e 開頭
- 在 FortiGate 601E 上建立 NAC policy 用以套用 08:5b:0e 開頭的 IP Camera 設備
- IP-Cameras 連接到 FortiSwitch 後，它們會被 NAC policy 識別出來並自動分配至 Camera_VLAN.

```
config user nac-policy
    edit "Camera-Policy"
        set mac "08:5b:0e:**:**:**"
        set switch-fortilink "port11"
        set switch-mac-policy "Camera-LAN"
    next
!
edit “Phone-Policy"
        set mac "70:4c:a5:**:**:**"
        set switch-fortilink "port11"
        set switch-mac-policy “Phone-LAN"
    next
```

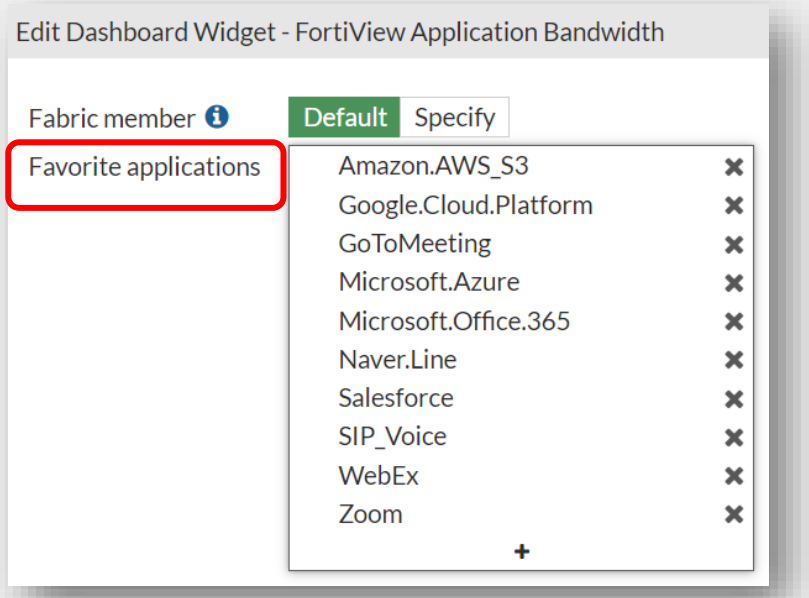


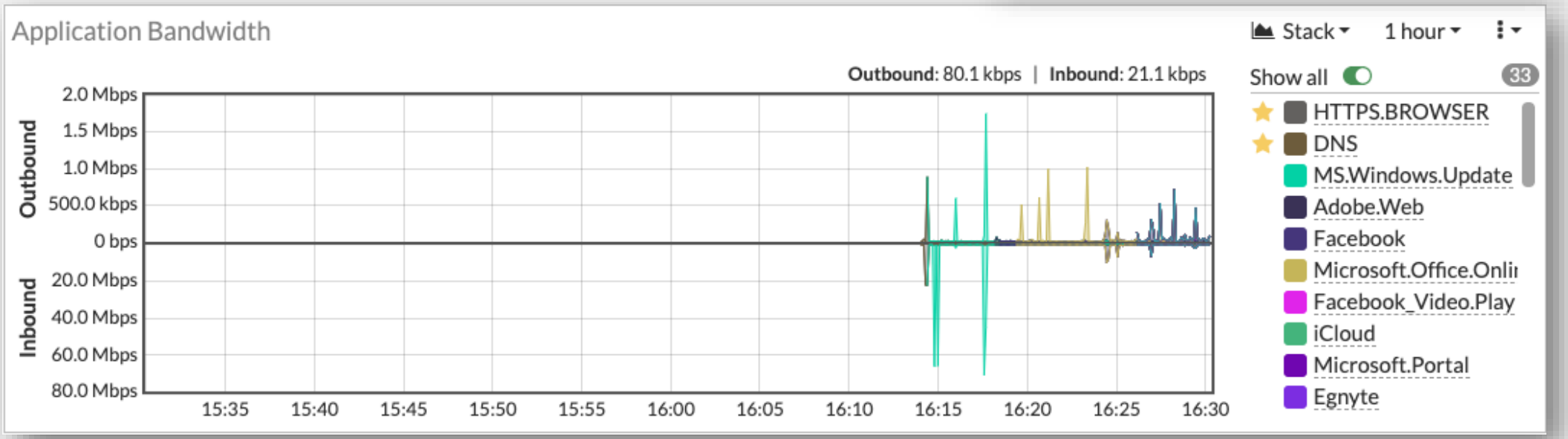
Security-driven Networking

Application Bandwidth Utilization Graph

新widget (小工具), 可監看**即時應用程式頻寬使用流量圖**

- 使用者可依喜好來設定過濾器條件，只呈現欲監看的應用程式
- 預設會顯示 **top X** 頻寬使用量的應用程式



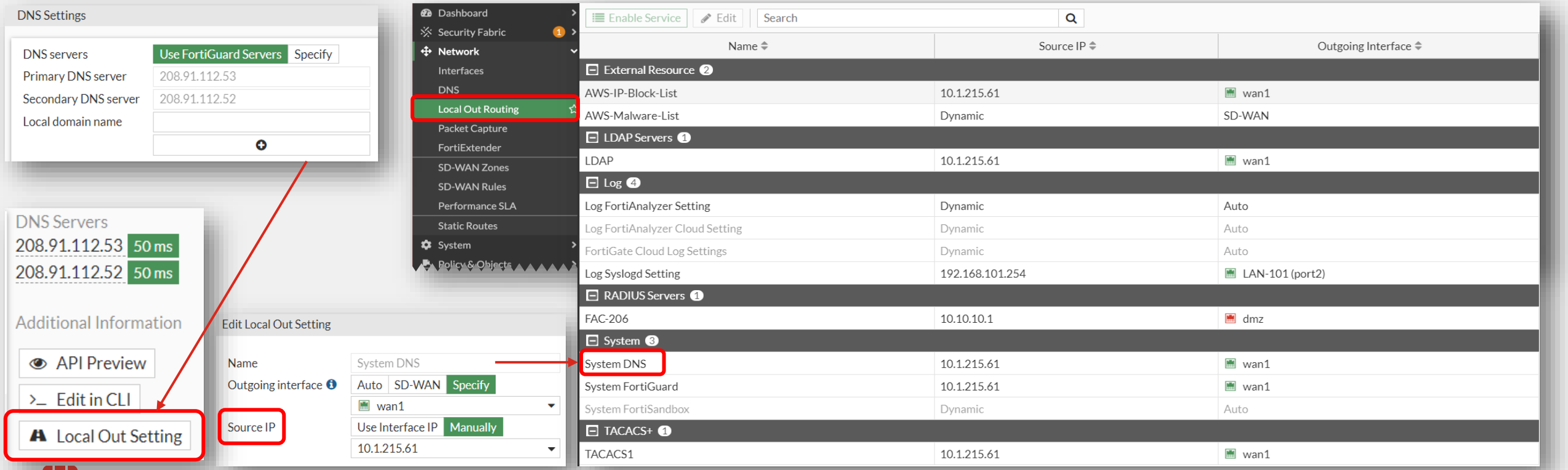


Security-driven Networking

Local Out Routing Page (本地輸出介面與IP集中管理)

將各類本地輸出配置設定 (Local Out settings) 合併到單一介面，方便設定與管理

- 集中管理本地輸出配置設定 – 例如：系統、日誌記錄和外部身份驗證服務等相關的設置
- 可運用在 Global 或 Per-VDOM Level
- 範例: FortiGuard, System DNS , FortiSandbox, FortiAnalyzer, Syslog, LDAP, RADIUS, TACACS, External Resource …..



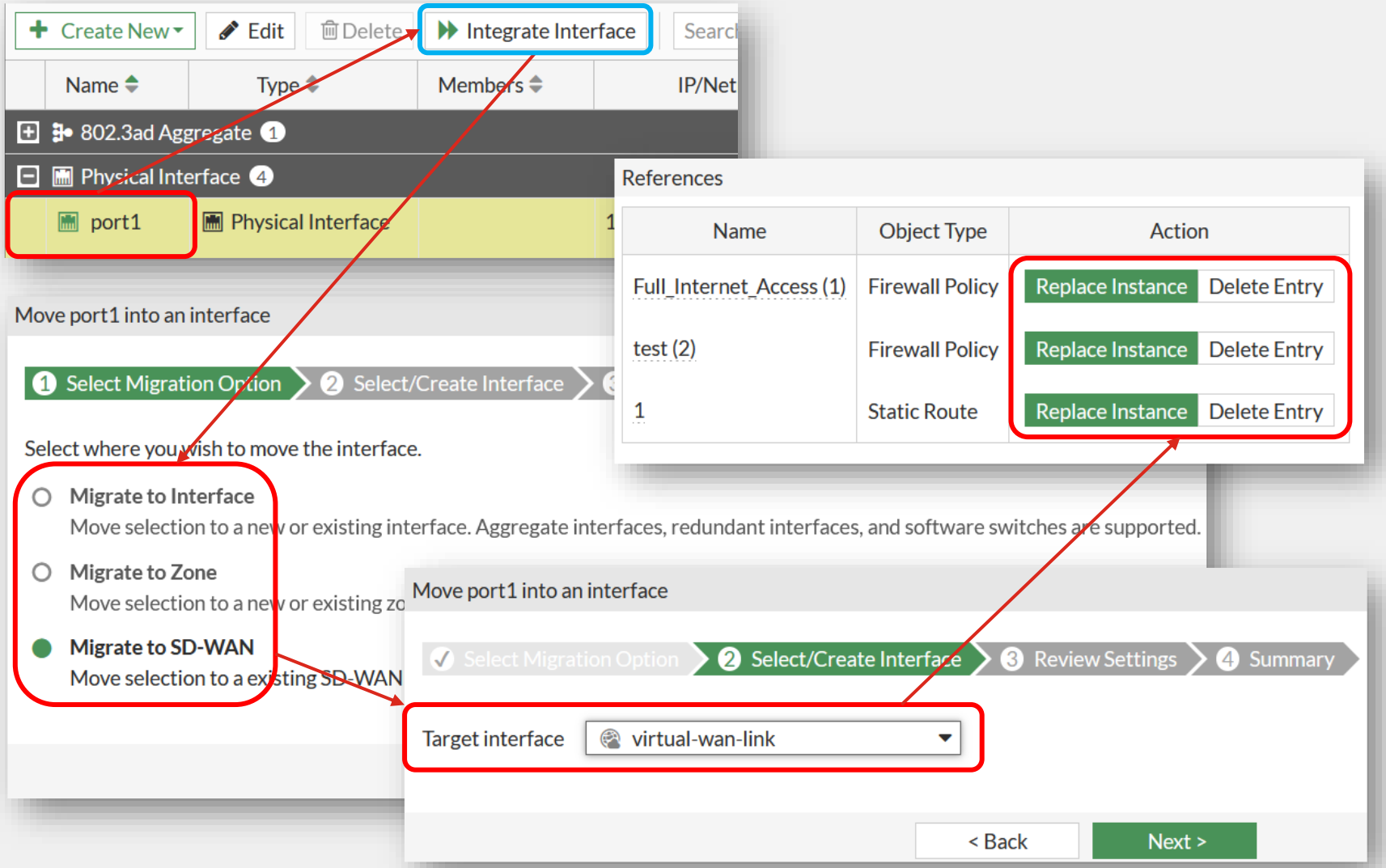
Security-driven Networking

Interface Migration Wizard (介面移轉精靈)

提供**移動**現有物件的能力，即使它們已被**引用** (references)

範例:

- 改變 VLAN 介面的 VLAN ID
- 移動已被引用的介面到 SD-WAN
- 新增已被引用的介面到 Zone



AI-driven Security Operations

(人工智慧驅動的安全營運)

FortiGuard Threat Intelligence
FortiGuard 威脅情資

AI-driven Security Operations

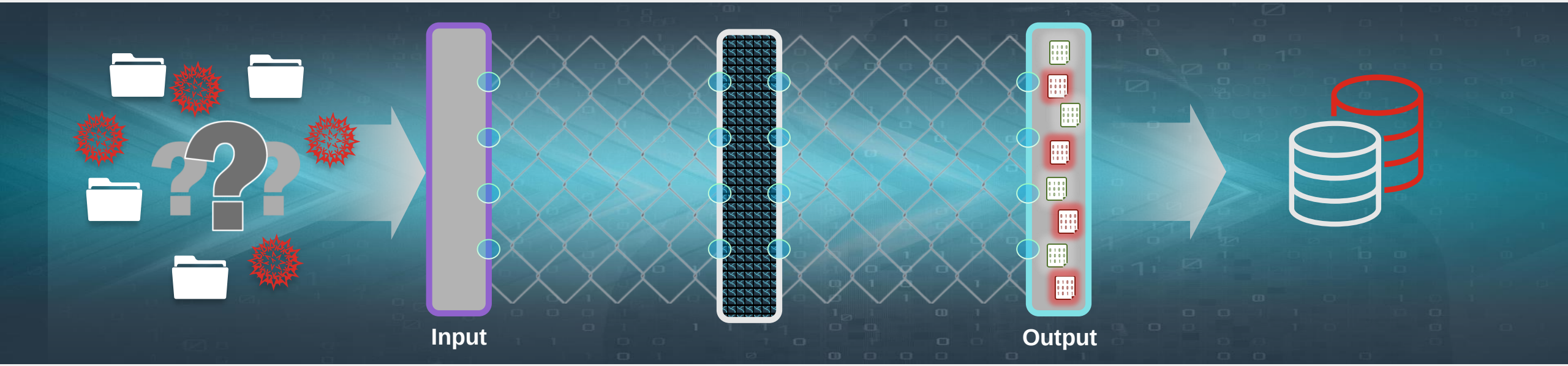
AI based Malware Detection (基於AI的惡意軟體檢測)

導入 AI 與機器學習，加速進階威脅偵測

- 由防毒/ 沙箱引擎的專業團隊所研發出來
- 整合至常規防毒掃描中，協助檢測潛藏在 Windows 可執行文件(PE)中的可疑行為，減輕**零日攻擊(zero-day attacks)**威脅

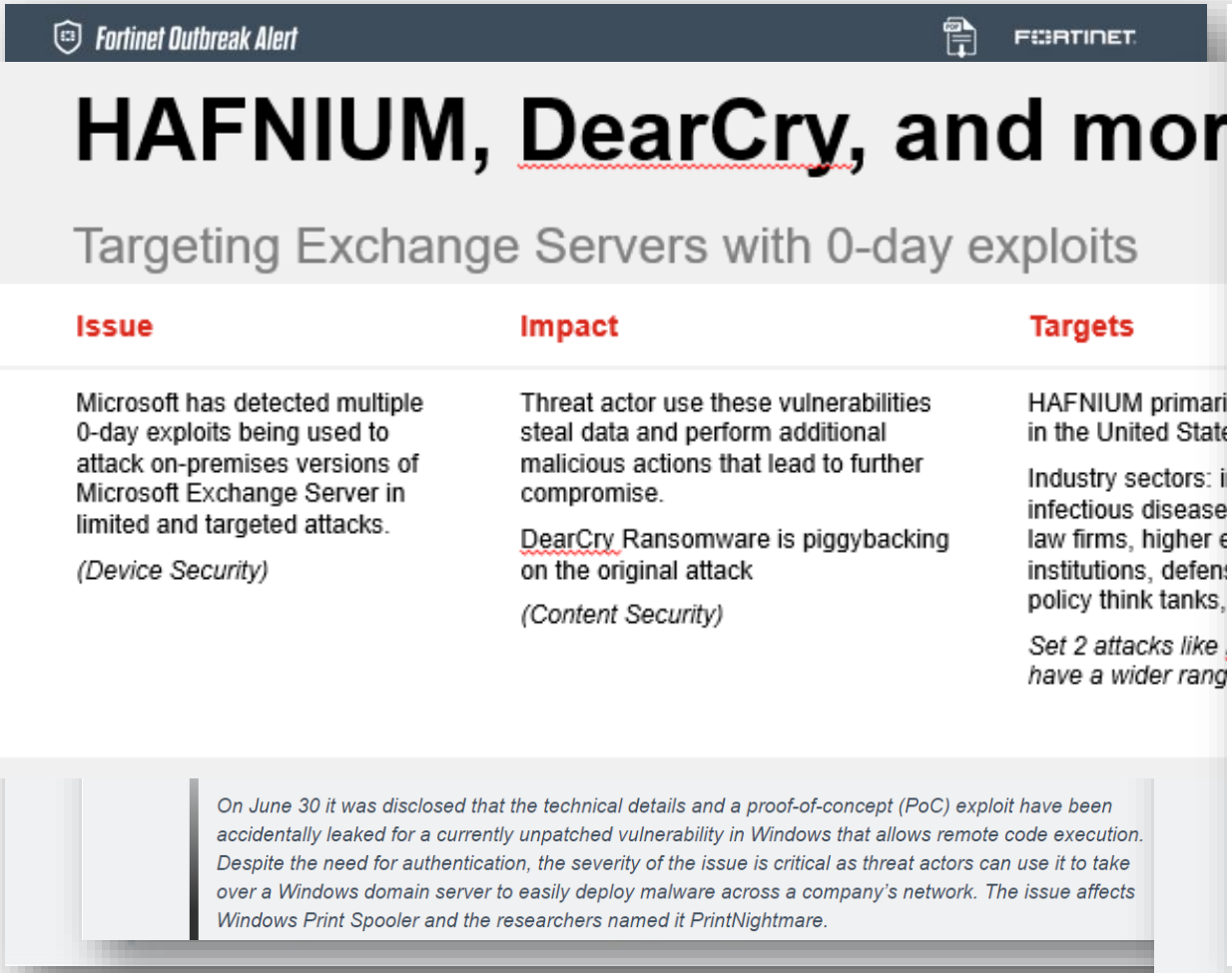
 # config antivirus settings

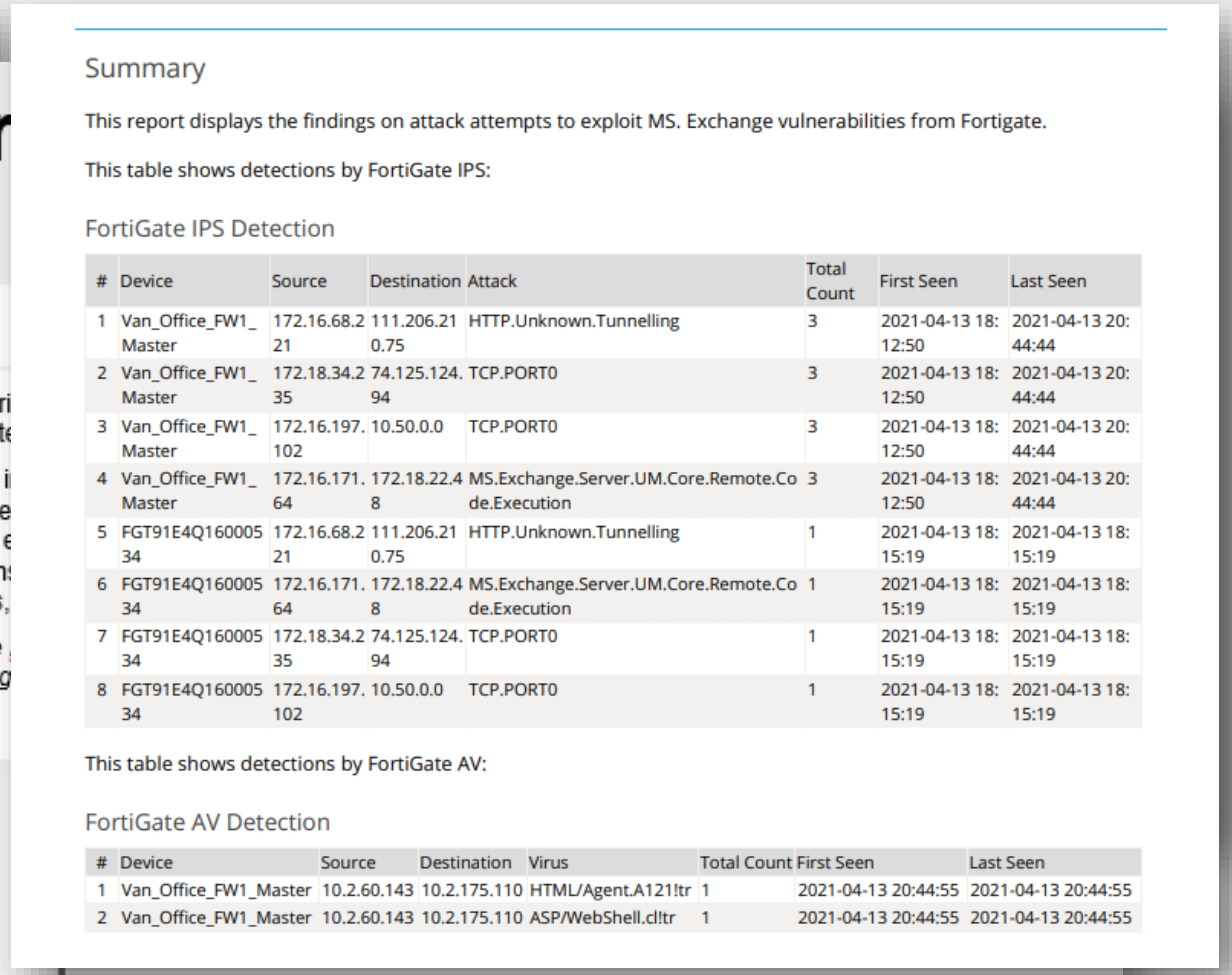
set machine-learning-detection {**enable**| monitor | disable}



New: Outbreak Alert (資安事件爆發告警)

- FortiGuard 資安事件爆發警報將成為向客戶和合作夥伴傳達重要信息的機制。
- 當發生對網路安全產生重大影響並影響眾多組織的資安事件與攻擊時，即時更新 FortiGuard 爆發警報的鏈接
- 可以產出 HTML、PDF、XML 和 CSV 格式的報告





Summary

This report displays the findings on attack attempts to exploit MS. Exchange vulnerabilities from Fortigate.

This table shows detections by FortiGate IPS:

FortiGate IPS Detection

#	Device	Source	Destination	Attack	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	172.16.68.221	111.206.210.75	HTTP.Unknown.Tunnelling	3	2021-04-13 18:12:50	2021-04-13 20:44:44
2	Van_Office_FW1_Master	172.18.34.235	74.125.124.94	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
3	Van_Office_FW1_Master	172.16.197.102	10.50.0.0	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
4	Van_Office_FW1_Master	172.16.171.64	172.18.22.48	MS.Exchange.Server.UM.Core.Remote.Code.Execution	3	2021-04-13 18:12:50	2021-04-13 20:44:44
5	FGT91E4Q16000534	172.16.68.221	111.206.210.75	HTTP.Unknown.Tunnelling	1	2021-04-13 18:15:19	2021-04-13 18:15:19
6	FGT91E4Q16000534	172.16.171.64	172.18.22.48	MS.Exchange.Server.UM.Core.Remote.Code.Execution	1	2021-04-13 18:15:19	2021-04-13 18:15:19
7	FGT91E4Q16000534	172.18.34.235	74.125.124.94	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19
8	FGT91E4Q16000534	172.16.197.102	10.50.0.0	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19

This table shows detections by FortiGate AV:

FortiGate AV Detection

#	Device	Source	Destination	Virus	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	HTML/Agent.A121!tr	1	2021-04-13 20:44:55	2021-04-13 20:44:55
2	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	ASP/WebShell.cl!tr	1	2021-04-13 20:44:55	2021-04-13 20:44:55

安全織網防護下的自動化資安管理維運中心

Security Operations

Security
Operations Center
(SOC)

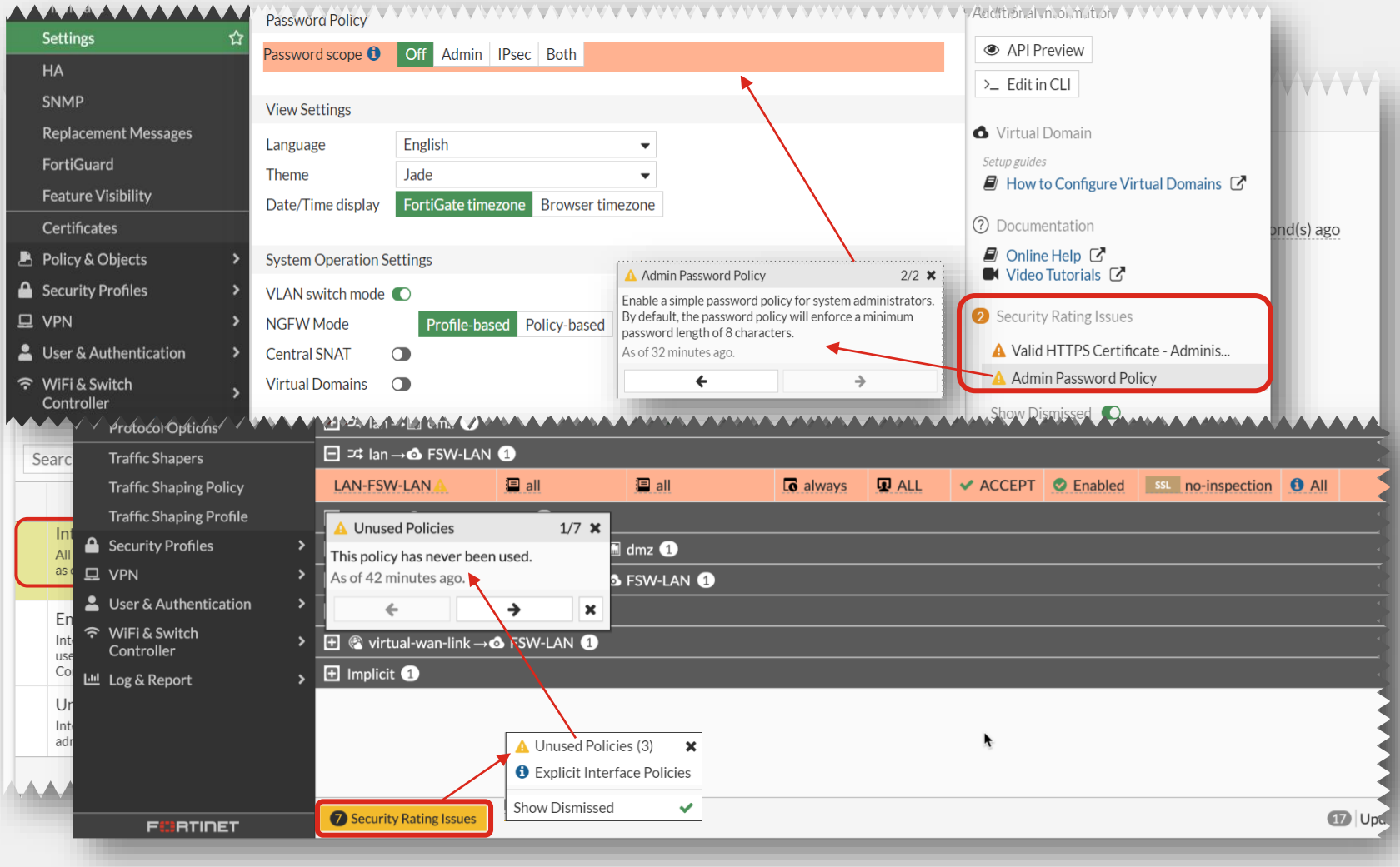
Fabric Management Center
Fabric 管理中心

Fabric Management Center

Security Rating Overlays (資安評級量化)

資安評級通報

- 安全等級配置問題直接顯示在設定頁面，很清楚地點出並建議管理者相關設定之安全配置建議
- PCI-DSS 支付卡產業資料安全標準
- 點選安全注意圖示，查看建議修復配置，單鍵點選設定修復，並匯出報表呈報與追蹤
- 可應用於金管會要求金融機構進行資安自理成熟度規範，協助金融機構資安自評項目量化

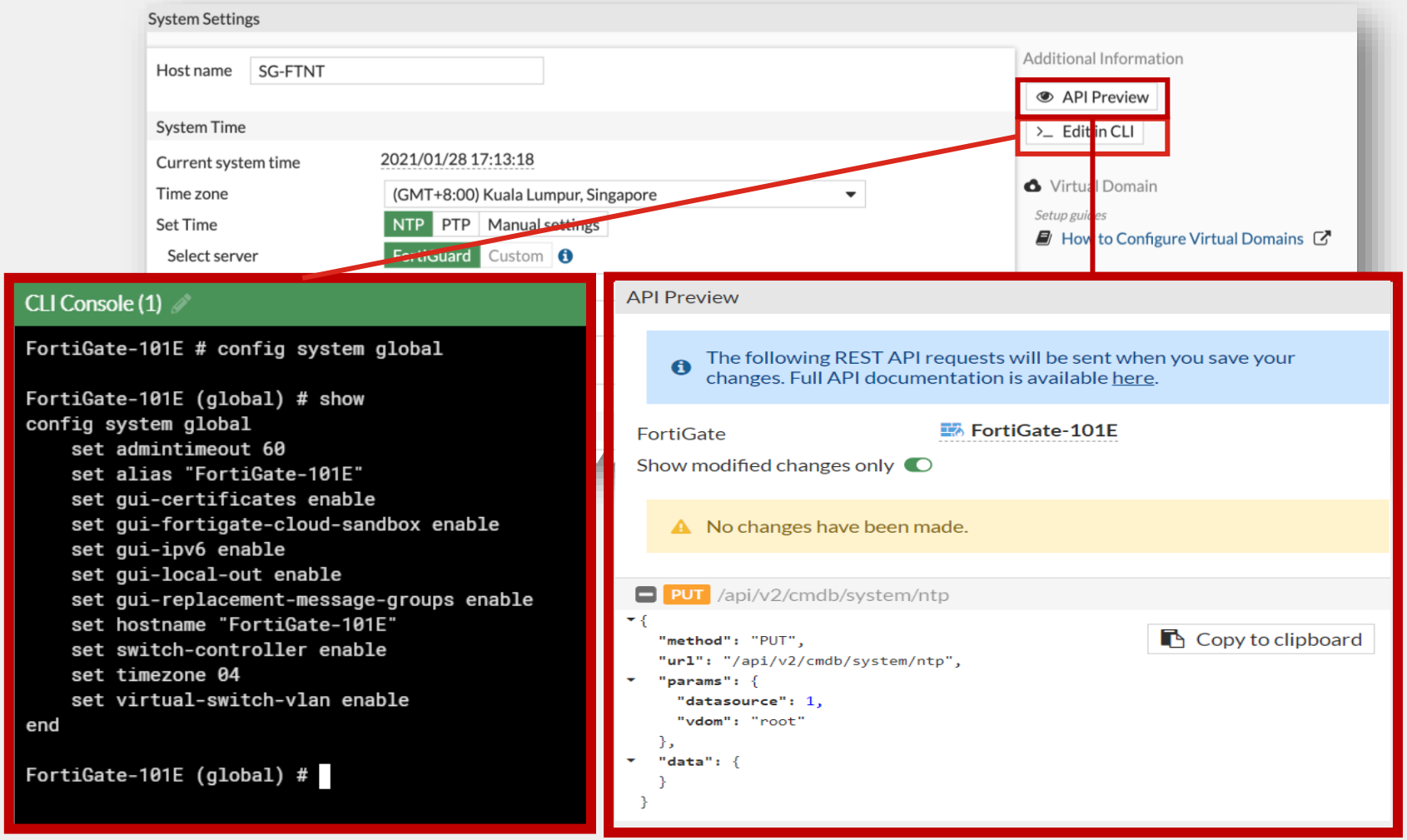


Fabric Management Center

直接顯示 GUI 操作等效的 REST API 與 CLI 命令模式

直接顯示 GUI 頁面上的 REST API 編寫語法與 CLI 命令模式

- 點選 “Edit in CLI” 查看目前 GUI 頁面上的 CLI 命令，透過 CLI 可配置 Advanced 進階設定
- 點選 “API Preview” 查看目前 GUI 頁面上的 API 命令，調整 GUI 設定後，可直接查看有哪些 API 調動

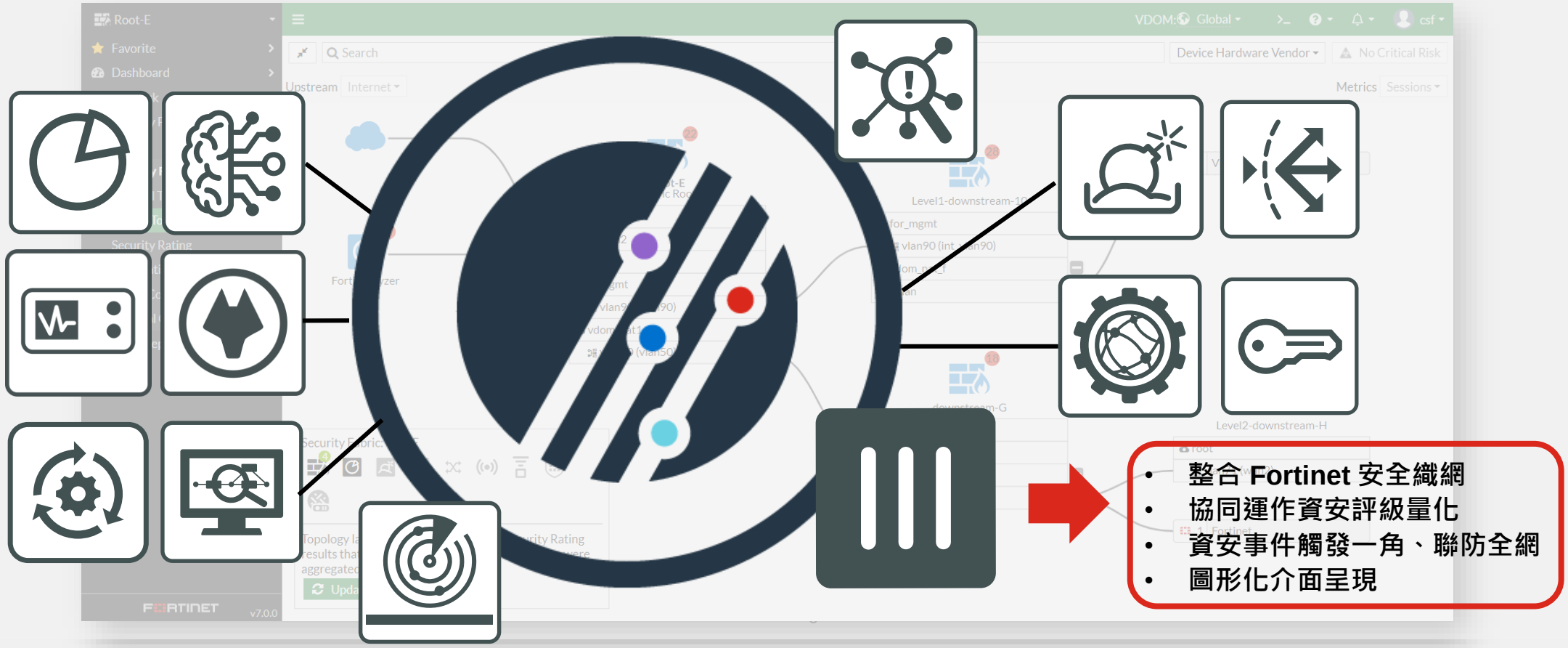


Fabric Management Center

安全織網 (Security Fabric) 可支援在 Multi-VDOM mode

FortiOS 7.0 支援在 Multi-VDOM 的環境下，享受安全織網 (Security Fabric) 帶來的全面防護

- 功能涵蓋包含**圖型拓樸架構**、**資安評級量化**以及**自動化維運**...等等

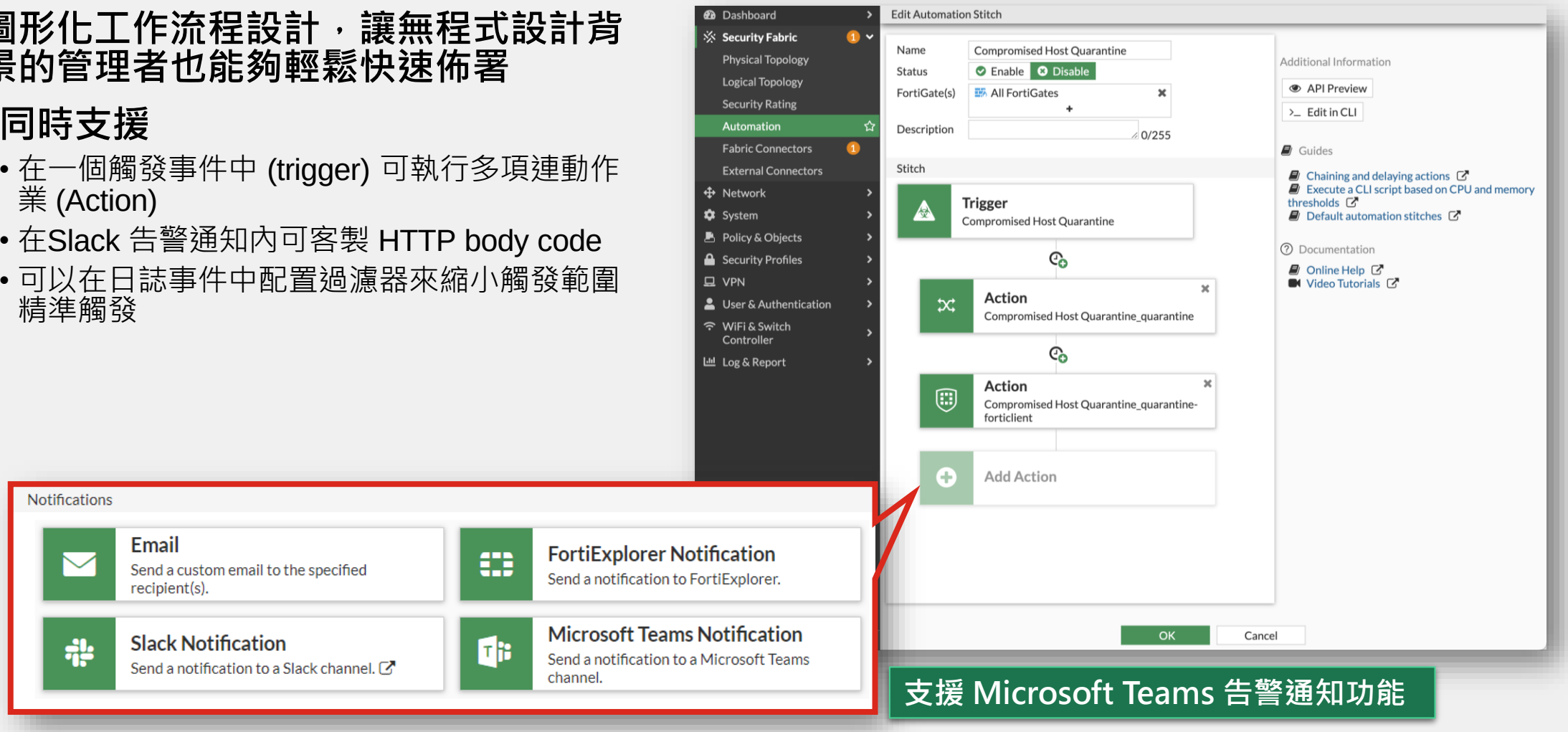


Fabric Management Center

Automation Workflow Improvements (自動化流程精進)

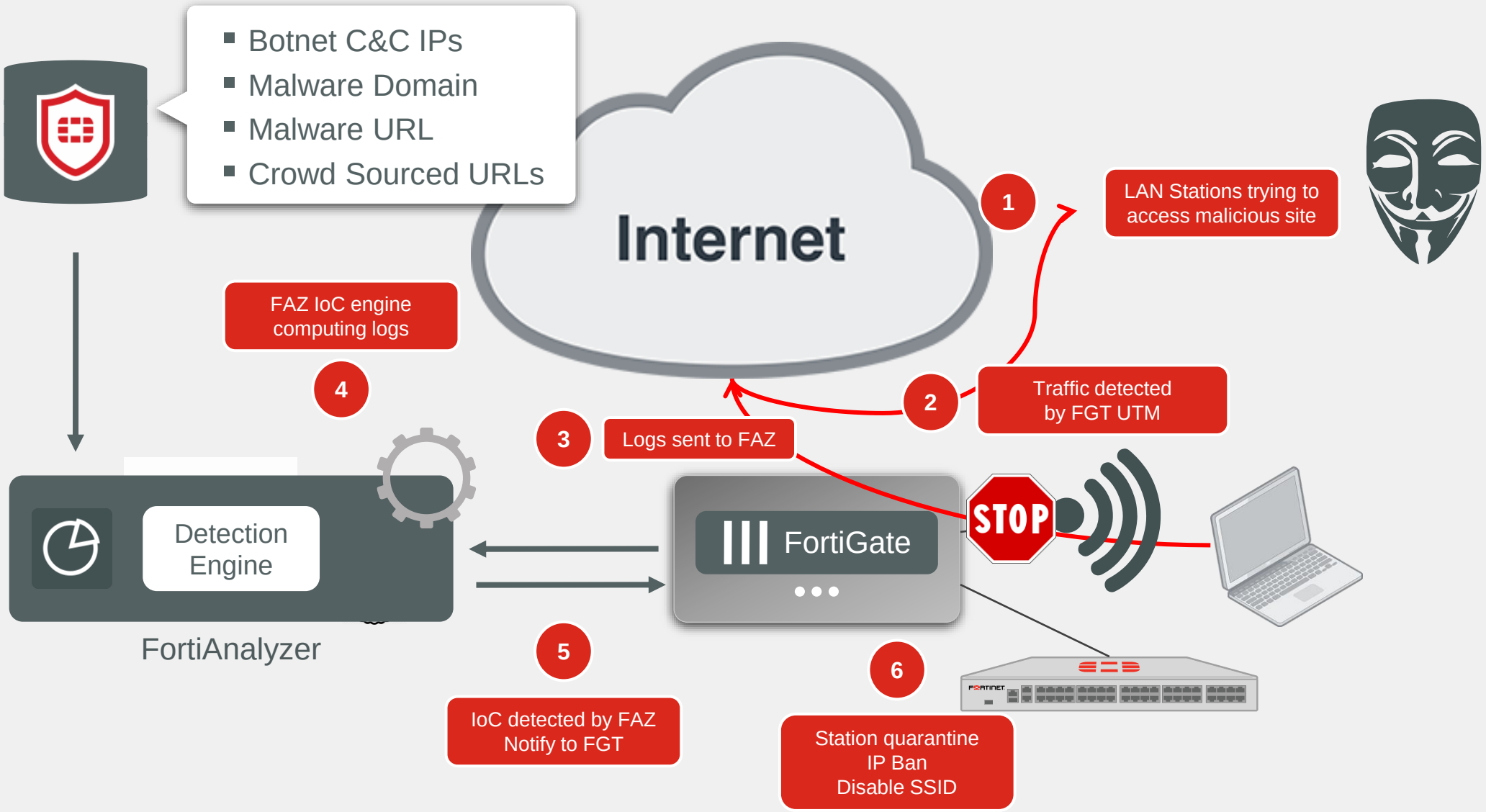
圖形化工作流程設計，讓無程式設計背景的管理者也能夠輕鬆快速佈署

- **同時支援**
  - 在一個觸發事件中 (trigger) 可執行多項連動作業 (Action)
  - 在Slack 告警通知內可客製 HTTP body code
  - 可以在日誌事件中配置過濾器來縮小觸發範圍精準觸發



支援 Microsoft Teams 告警通知功能

Automation Workflow



FortiOS 7.0 新增 300 項功能，資安防禦全面升級

- Fortinet Zero Trust Network Access (ZTNA)
- FortiGuard Video Filtering and IoT Real-time Query
- Over 300 New Features and Updates Deliver Even More Reasons to Choose Fortinet


FORTINET