Fortinet ZTNA & FortiSASE
零信任存取與SASE解決方案

Michael Shiah

mshiah@fortinet.com

Agenda

1 何謂”零信任存取” ZTNA(Zero Trust Network Access)

2 Fortinet ZTNA架構

3 ZTNA Dynamic Tagging範例

4 FortiSASE(安全存取服務邊緣)

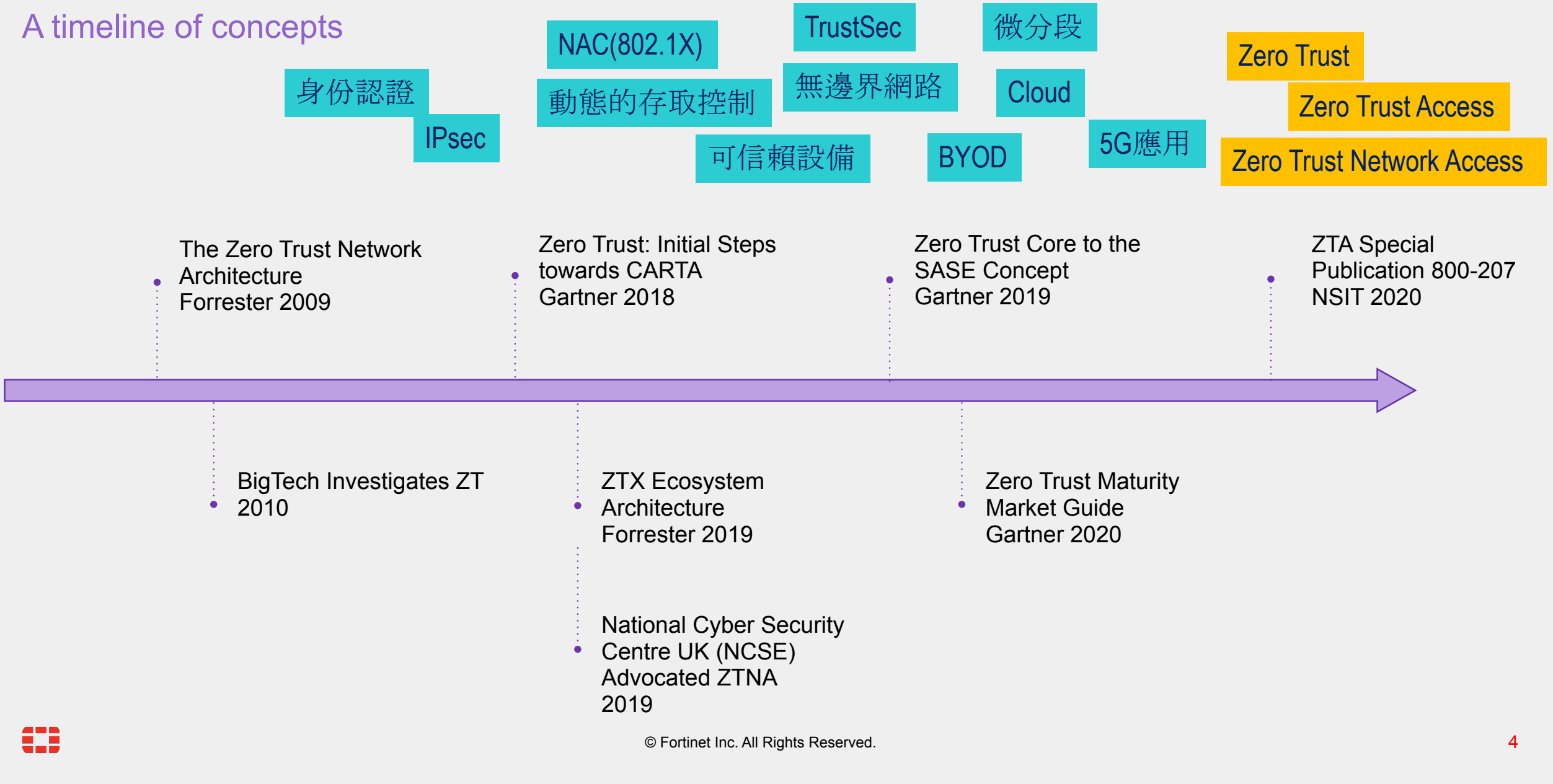
5 Q&A

何謂”零信任存取” ZTNA (Zero Trust Network Access)

Section Subhead

零信任概念的歷史

A timeline of concepts



零信任ABCDE原則

For users and devices

- Verify(確認)
  - 認證與確認 – 必須持續進行
- Give minimal access (最小權限)
  - 網路分段, 劃分幾個小區域進行控制
  - 對應用, 資料與資源的存取進行控管
  - 基於需要或角色賦予可執行任何的最小權限
- Assume Breach(假定會被入侵)
  - 假定駭客攻擊存在內網與外部網路
  - 不再以網路Location定義所謂“trusted zone”的概念, 比如, ‘in the office’

ABCDE Principles: Assume nothing(不做任何假定), Believe nobody(不相信任何人), Check everything(隨時檢查一切), Defeat dynamic risks(防範動態威脅), Expect for the worst(做最壞打算)

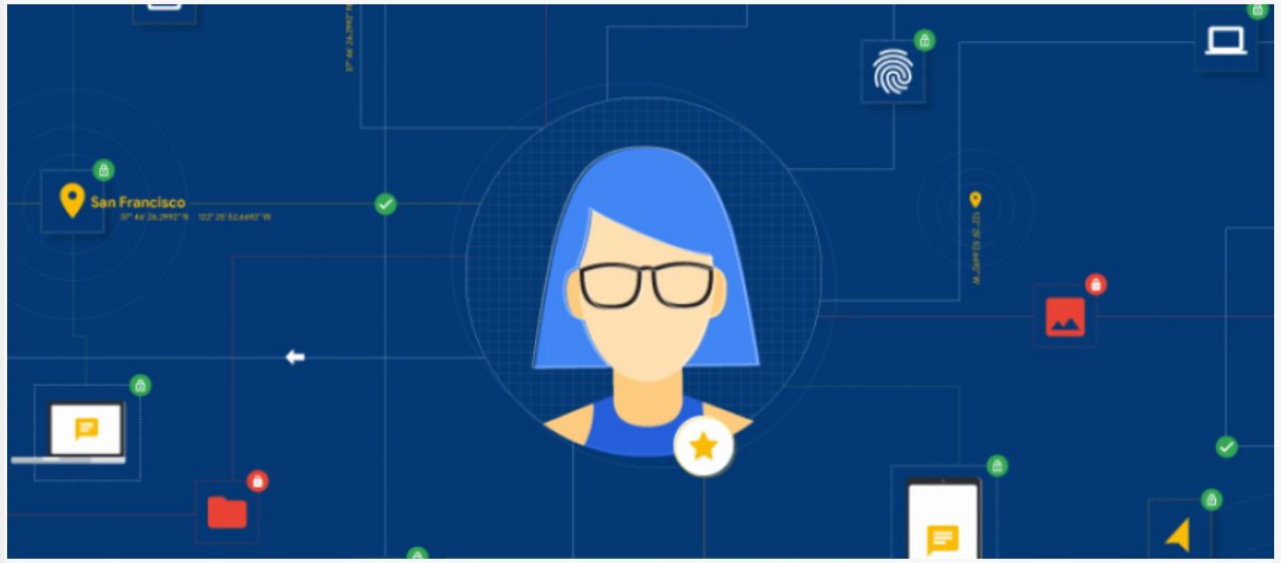
What is ZTNA?

如何處理零信任網路的資料存取需求? Google 這麼做

Google內部採用零信任網路（Zero Trust Network），讓員工可以不需要透過以VPN為核心的特權企業網路，進行遠端連線作業，Google技術長辦公室技術總監Max Saltonstall表示，為此需要把存取權控制從網路轉移到使用者與其使用的裝置上。

文/ 李建興 | 2018-07-04 發表

讚 6.5 萬 按讚加入iThome粉絲團 讚 31 分享



Google根據設備安裝的軟體、補丁更新的情況以及其他特徵進行信任評估。

Max Saltonstall提到，企業要從以VPN為核心的特權企業網路，轉移至零信任網路的第一步，便是了解員工以及設備。當網路不再提供存取關鍵服務需要的信任時，Google轉而使用個別員工以及裝置上的資訊，透過兩者最新的資料集設置存取最佳策略。

裝置與人員在零信任網路中一樣重要，因此追蹤系統還要掌握員工使用的裝置精確且即時的資訊，Max Saltonstall表示，他們不希望受信任的人員，卻因為使用了受感染的裝置，而無意間與攻擊者分享了他們有權存取的敏感資訊

What is ZTNA?

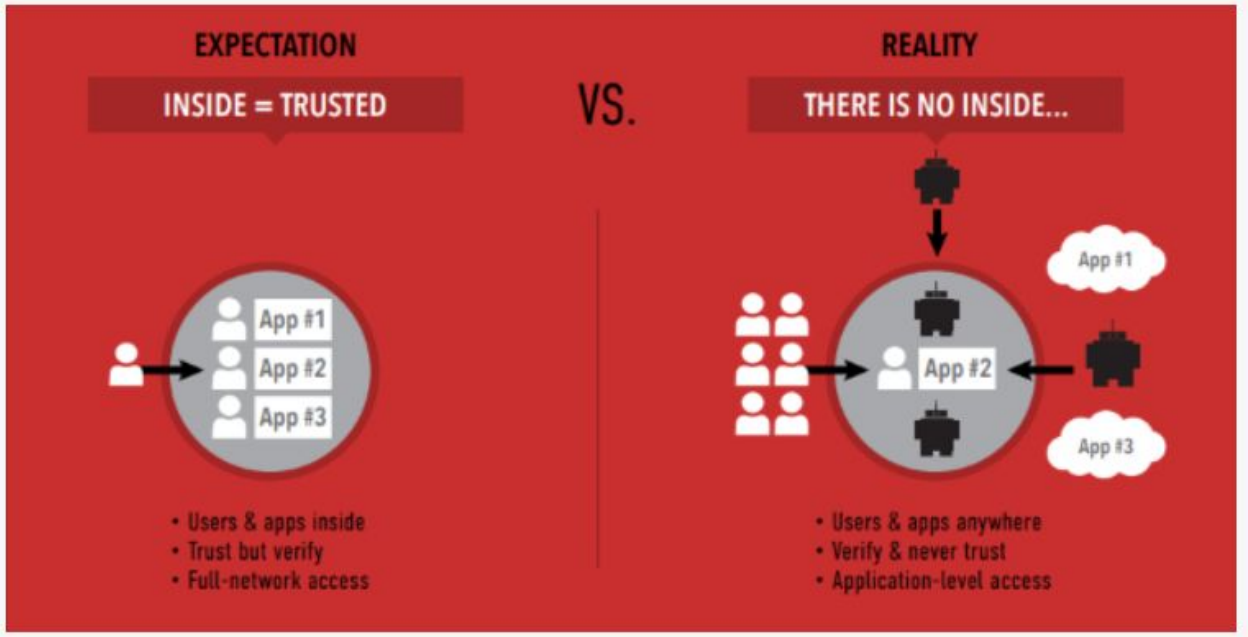
【網路世界徹底提升資安的自保之道】防護無邊界，零信任才能夠真安全

面臨各種資安威脅橫行的局勢，內部網路環境、公司管理的個人電腦都有可能受到攻擊而癱瘓、遭駭，甚至反過頭來成為加害者，早已沒有內外之分，因此，零信任的管理模式已勢在必行

文/ 李宗翰 | 2018-07-28 發表

讚 6.6 萬 按讚加入iThome粉絲團 讚 289 分享

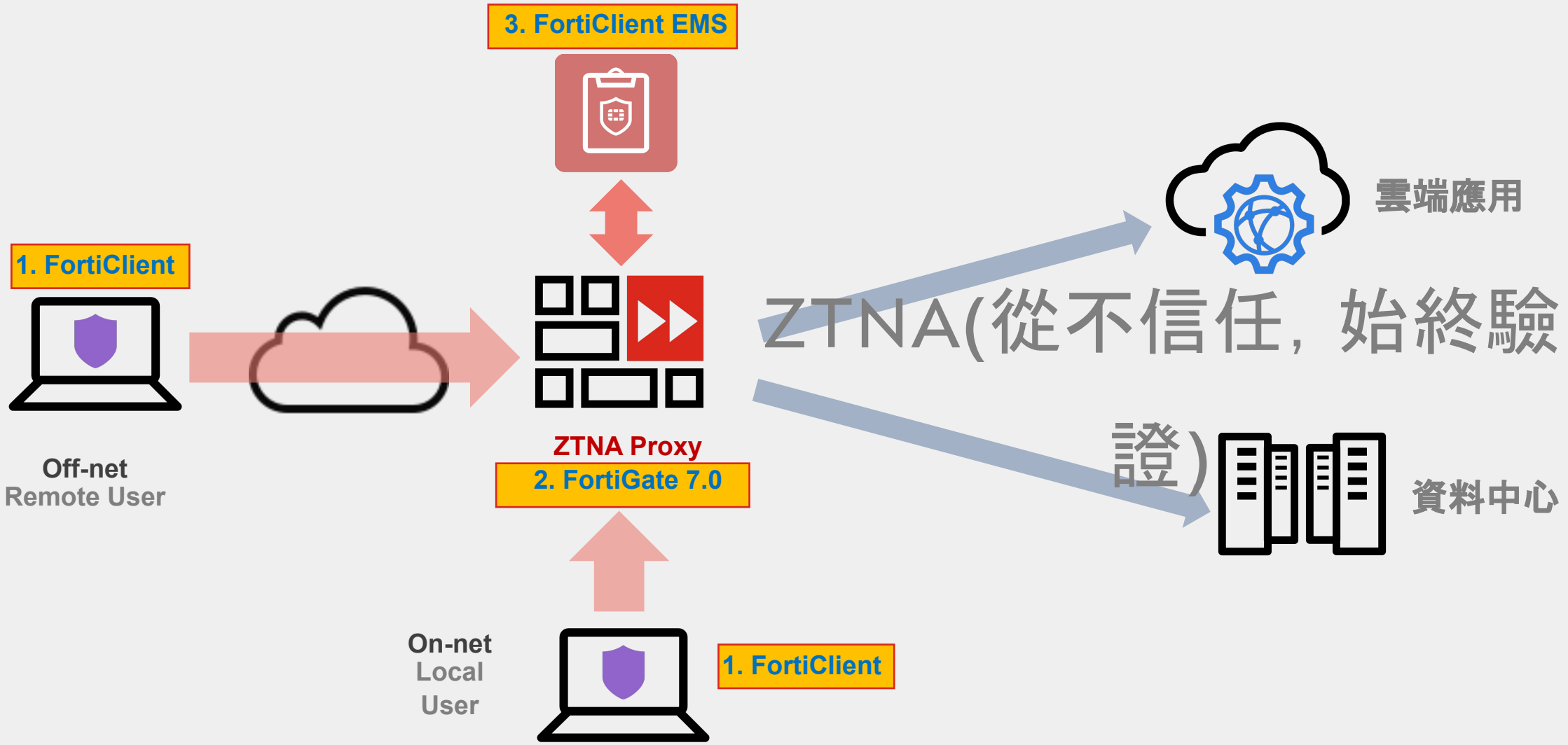
除了Google, 最近, 我們還看到另一家建置零信任架構的網路公司, 那就是知名的線上影音業者Netflix。
在今年初的Usenix Enigma大會, 該公司資深安全工程師Bryan Zimmer公開介紹他們的零信任架構, 稱為無關位置的安全途徑(Location Independent Security Approach, LISA)當中包含三大基本原則:(一)是否信任的關鍵, 在於使用者身分與端點健康狀態, 而不是所在位置;(二)對於辦公室網路, 不能信任;(三)設備要隔離。



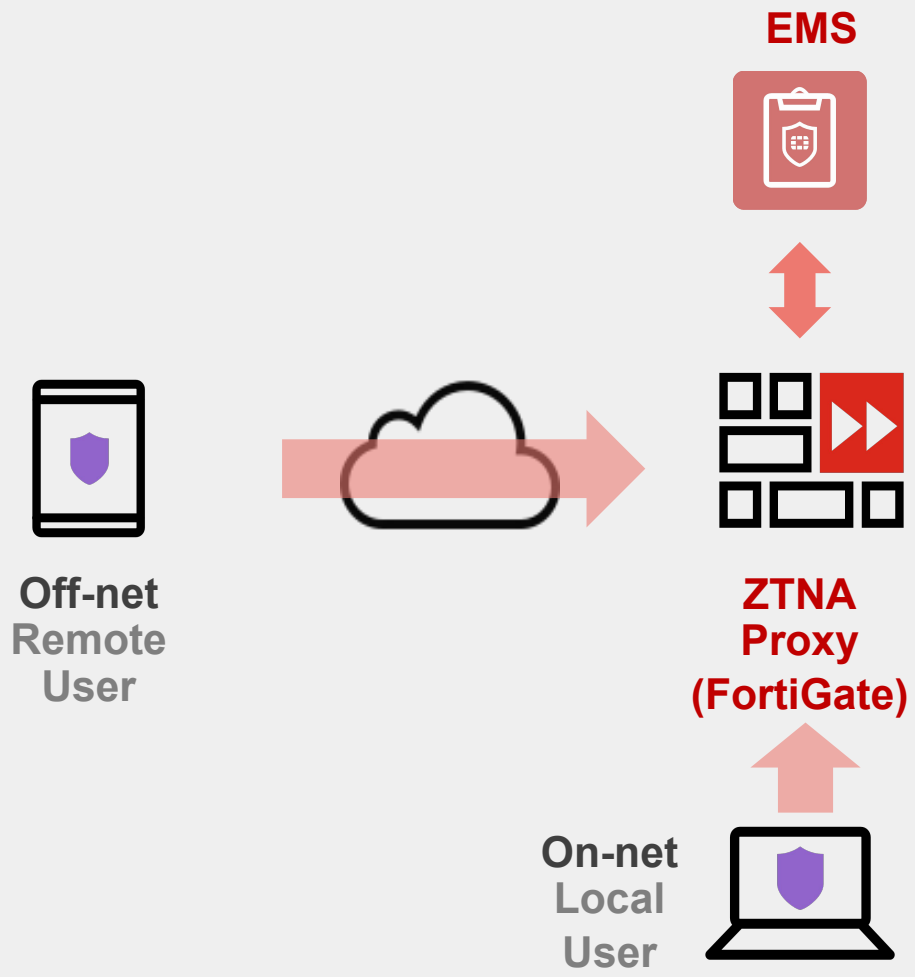
Fortinet ZTNA架構

Section Subhead

Fortinet ZTNA 架構及元素



ZTNA - On-net & Off-net(網內&網外控管)



ZTNA(從不信任，始終驗證)

不再只是能控管 Remote User

也可針對 Local User 做控管

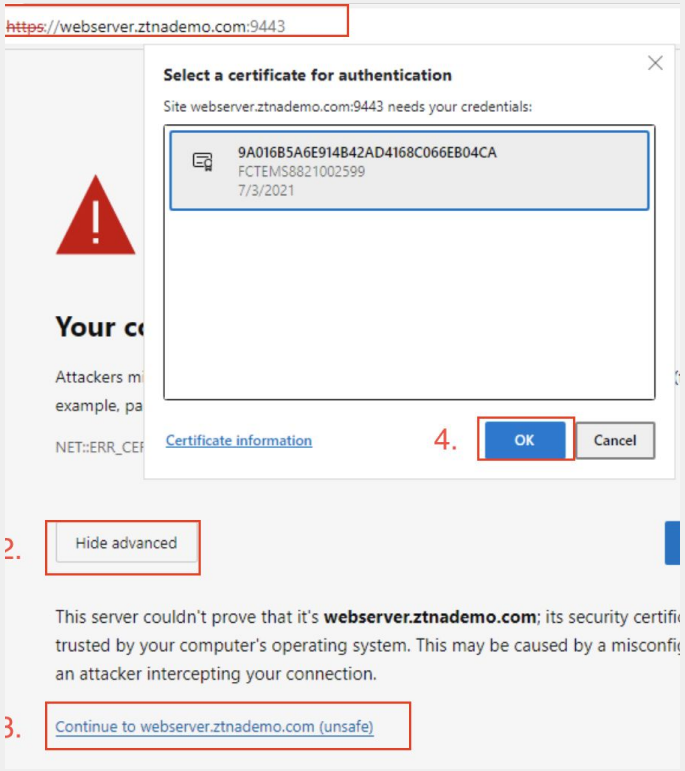
當你有 ZTNA 時

簡單快速使用

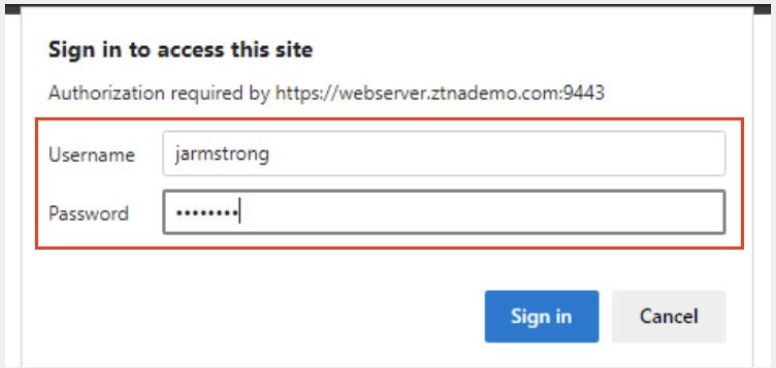
On-net / Off-net
辨識

多層次
細部控管

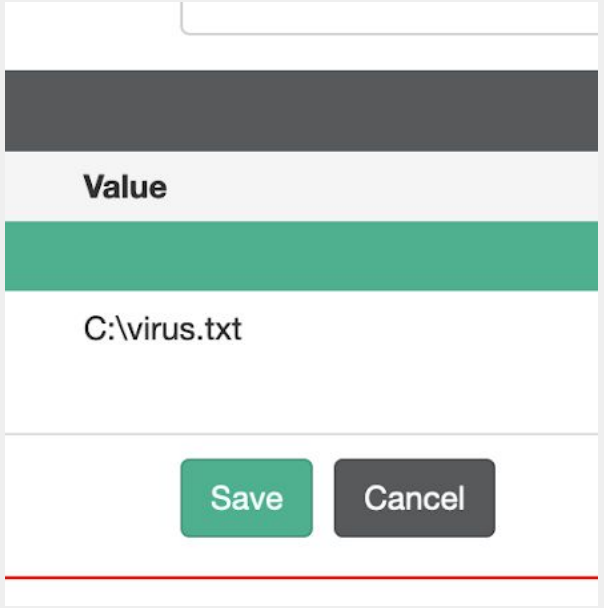
ZTNA 多層次且細部控管



憑證認證

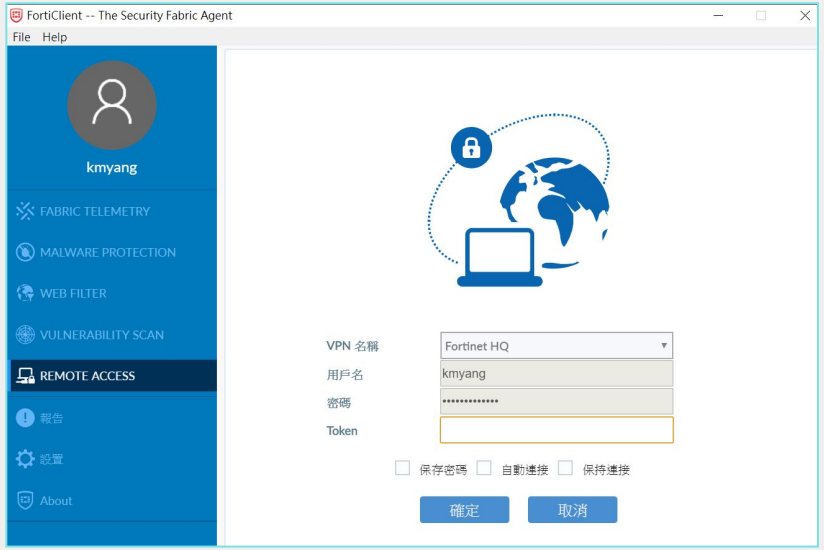


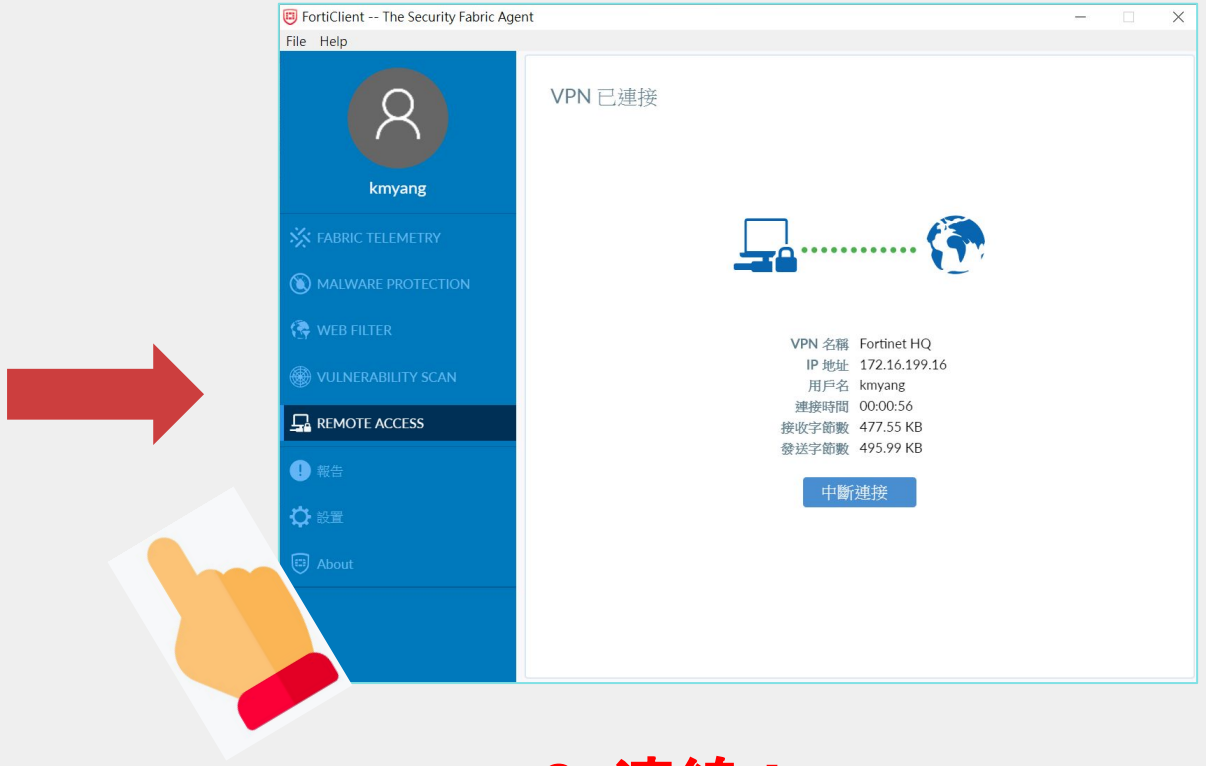
整合外部認證或
SAML或OTP



可針對
file/Registry/Process
等做控管

傳統SSLVPN (Fortinet WFH方案)

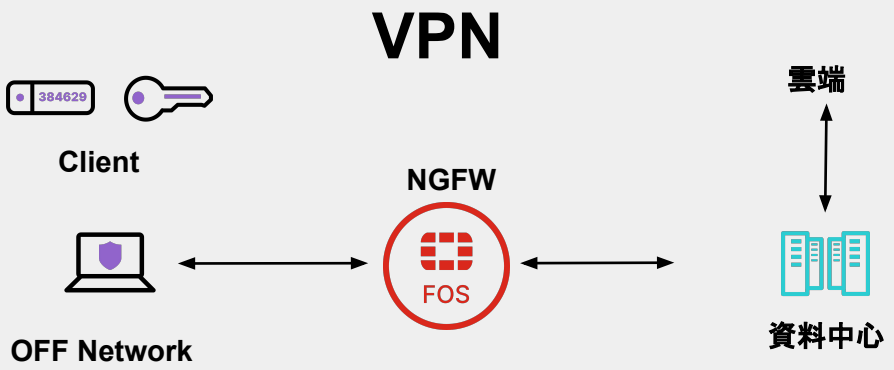


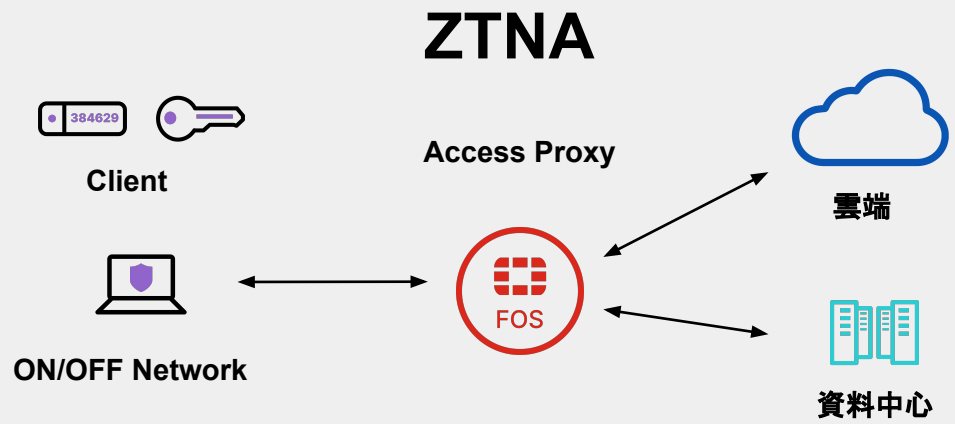


1. 用戶登入

2. 連線！

從 VPN 跳耀至 ZTNA



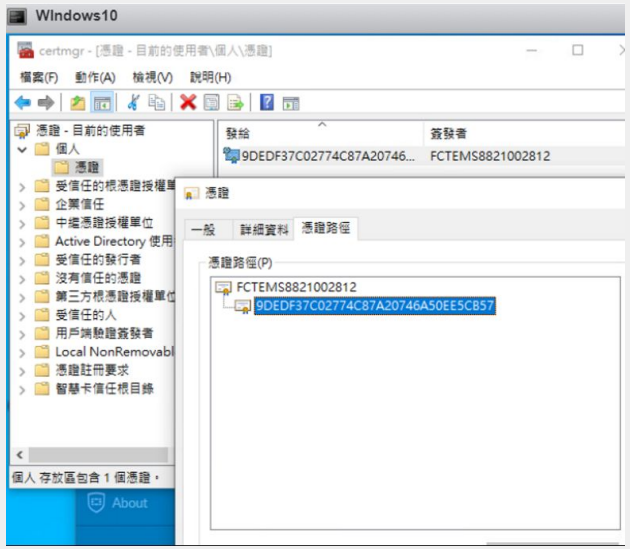


- 每次需要”撥”SSLVPN
- 大部份是基於網段的存取
- 傳統的防火牆IP/App控制策略
- 登入SSLVPN一次性的檢查

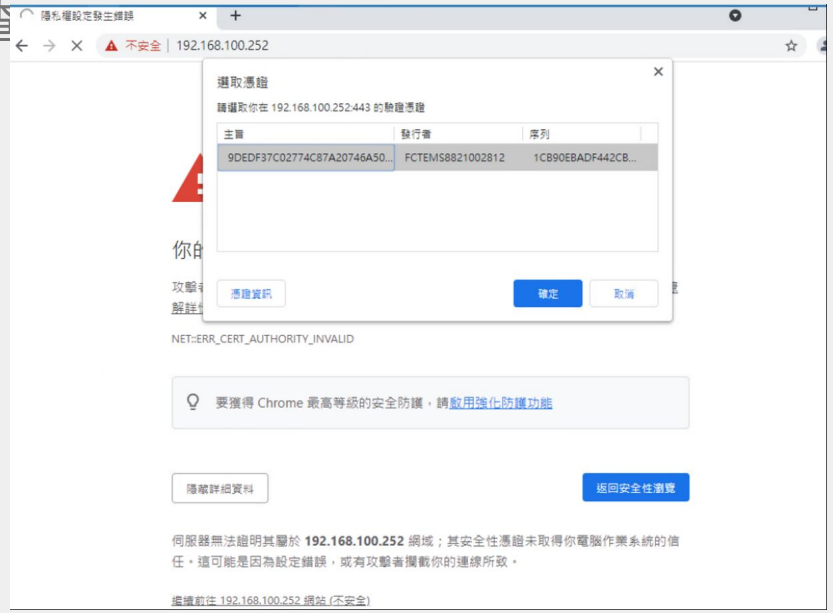
- 使用Access Proxy自動隧道技術(使用者無感)
- 針對特定應用提供透通存取
- User與Device狀態相關的控制策略
- Per-Session持續性可信任的Context檢查(包括裝置憑證)

ZTNA – HTTPS Access Proxy(取代傳統SSLVPN)

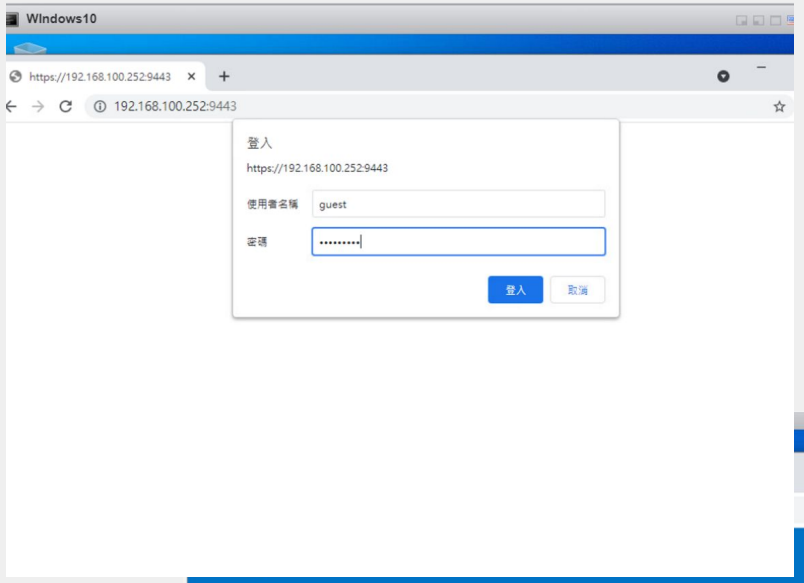
1. Client 端會安裝裝置憑證且
   需要與EMS連線

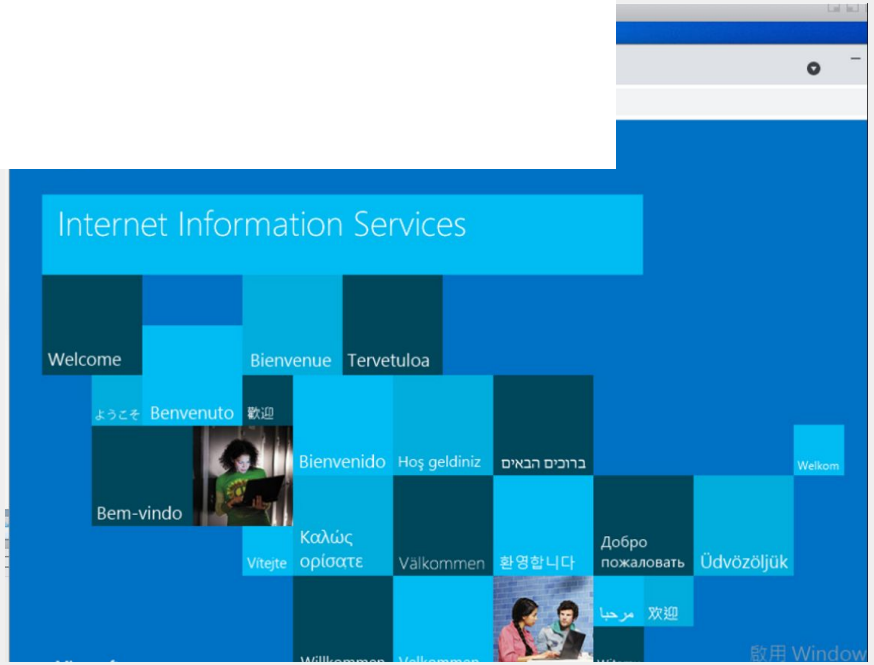


2. 輸入外部VIP IP，瀏覽器會跳出憑證認證的檢查



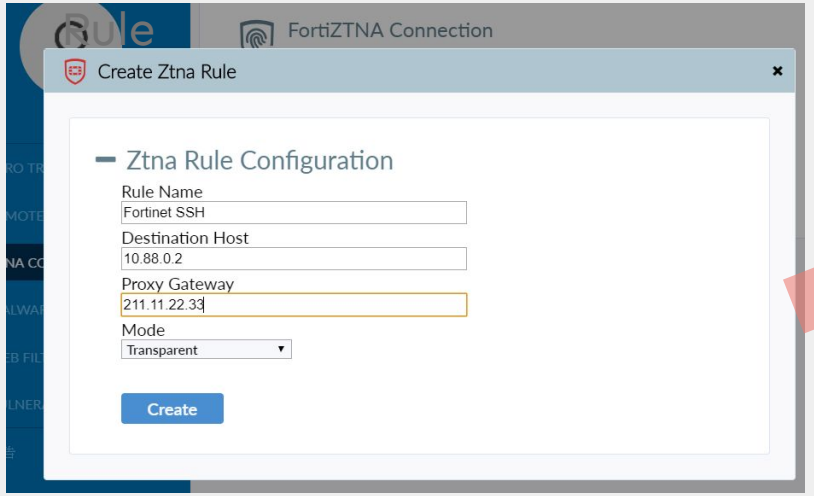
3. 認證成功後，就可以存取內網網頁



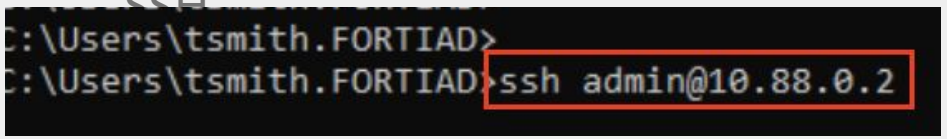


ZTNA – TCP Access Proxy for SSH(取代傳統SSLVPN)

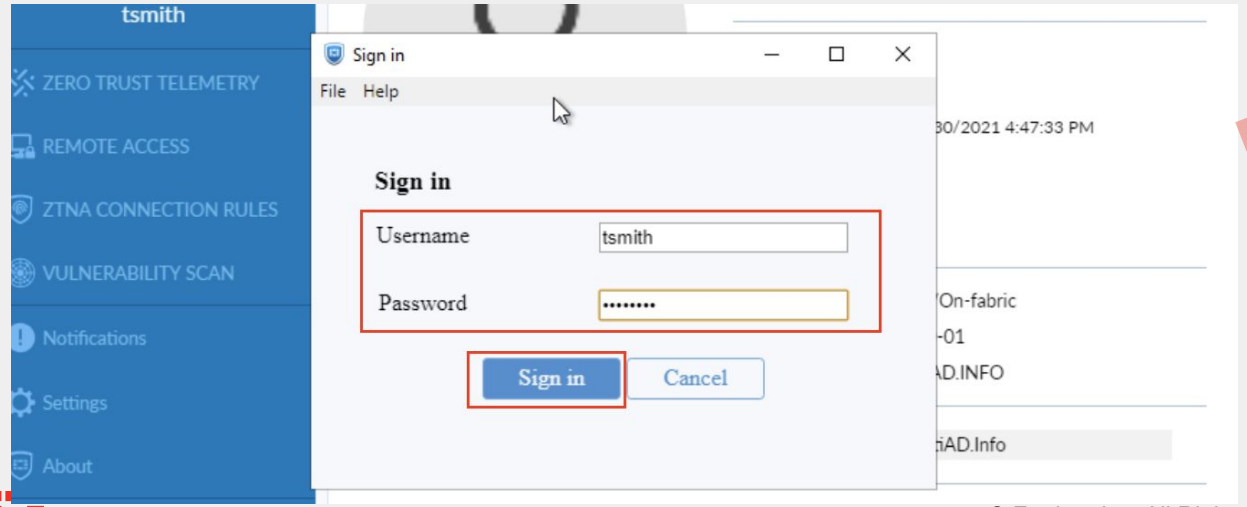
0. FortiClient設定ZTNA



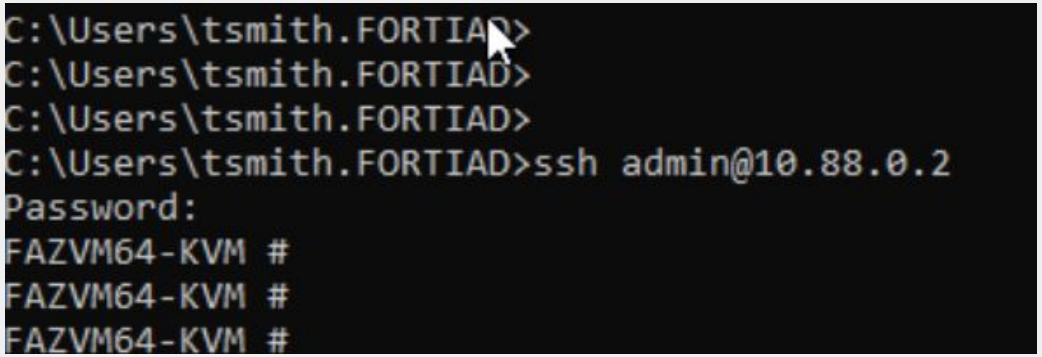
1. Client 端連內部 SSH



2. FortiClient 會跳出帳密認證頁面，輸入 LDAP 帳密



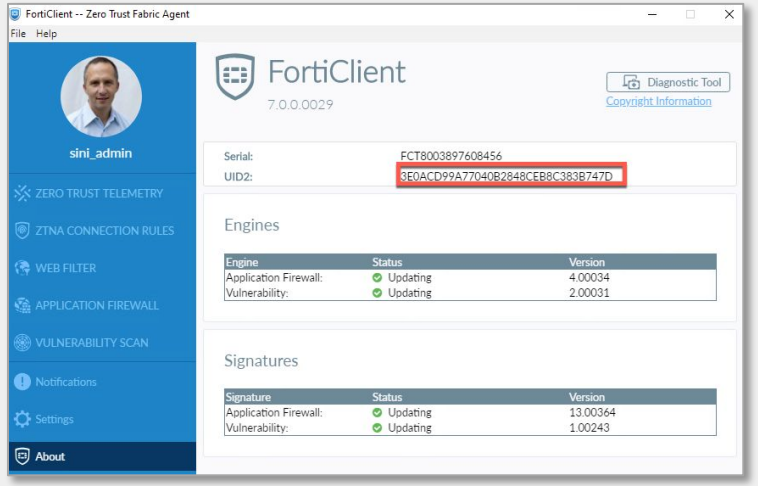
3. 認證成功後，就可以再做 SSH 登入

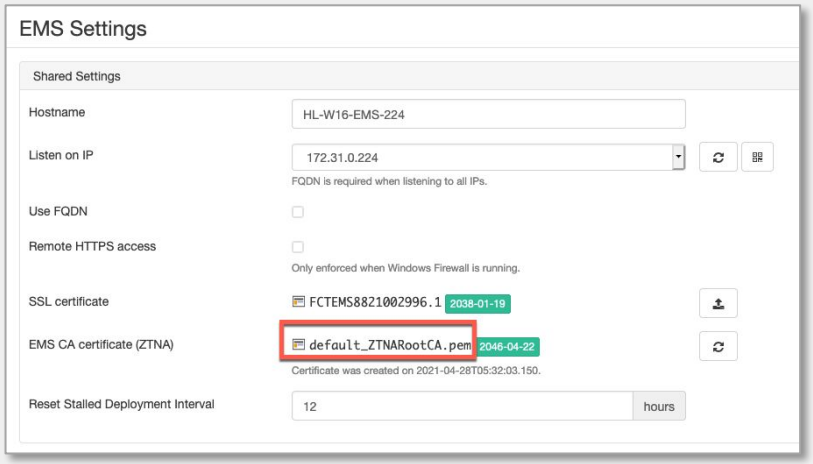


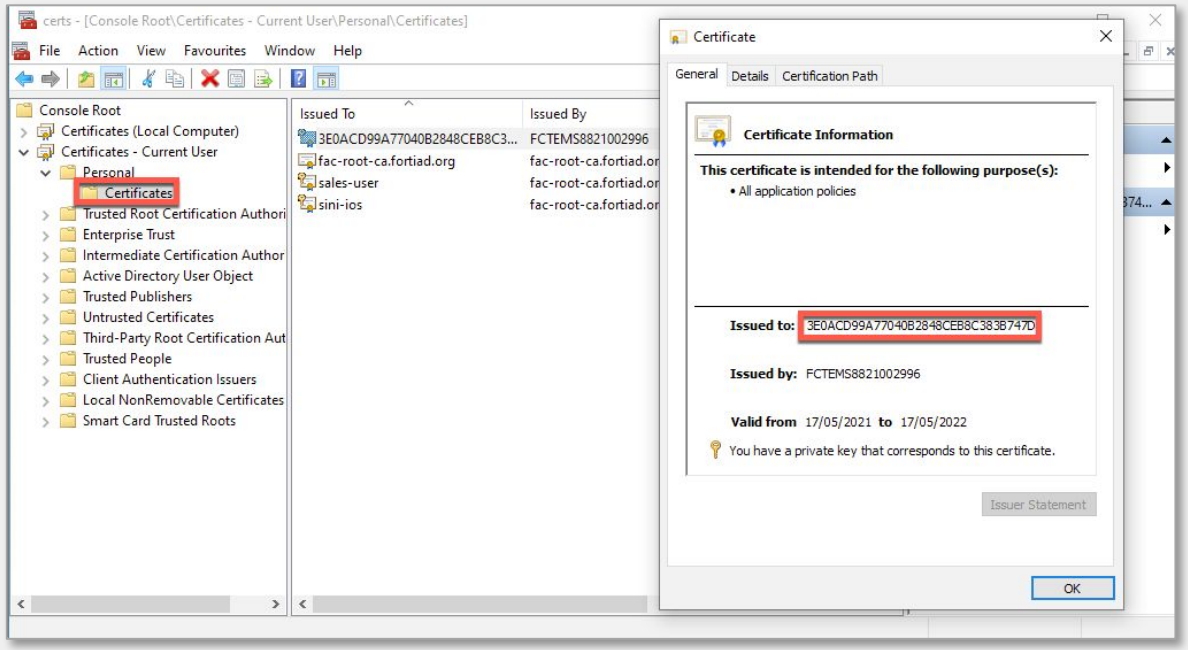
ZTNA Client憑證

ZTNA Certificate

1. FortiClient成功註冊到EMS後會送CSR to EMS
2. EMS會回傳signed FortiClient certificate給Client，FortiClient會安裝此憑證到User Certificate Store
   - Certificate CN = FCT UID



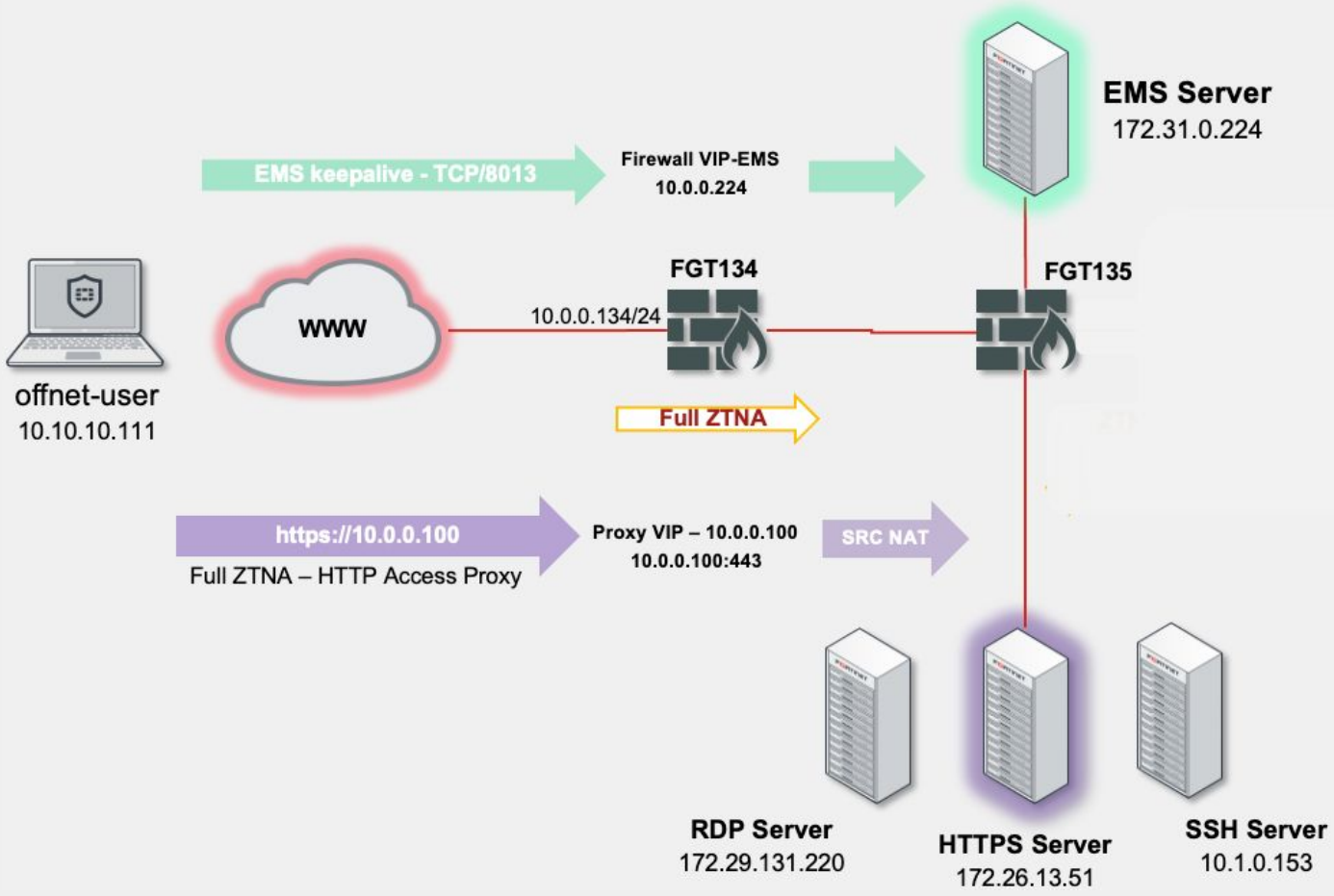




ZTNA模式 – Full ZTNA for HTTPS

ZTNA Modes – Full ZTNA - HTTPS Access Proxy

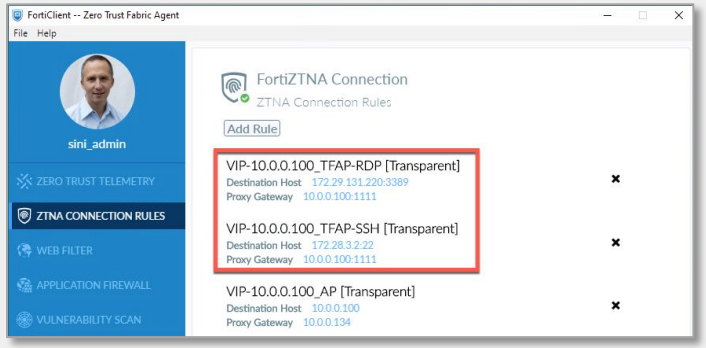
- FGT以Reverse Proxy方式運作運作，代理到後端HTTP Server的連線(Proxy VIP)。瀏覽器與FGT間建HTTPS Tunnel，不需FortiClient介入。
  - Browser support
    - **IE and Google Chrome** are currently supported due to certificate onboarding restriction
    - Note: ZTNA Certificate installed in OS Certificate Store doesn't provide an option to export Private Key
- FortiGate負責連線代理並做使用者認證。Certificate on the browser (match against ZTNA endpoint record from EMS = certificate serial number)
- Optional authentication (local, LDAP, Radius or SAML) is available (Captive Portal)
- ZTNA rules evaluation
- Destination is the **VIP address**



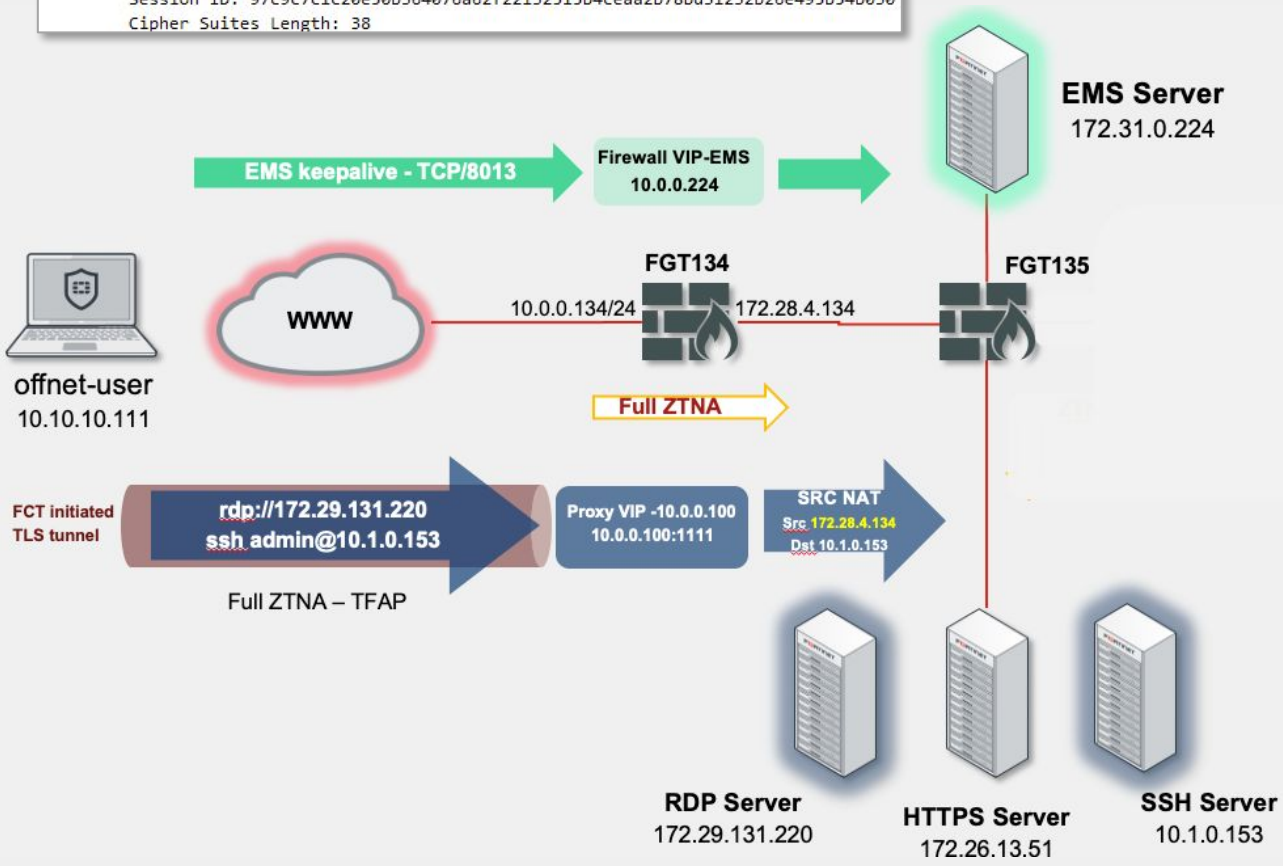
ZTNA模式 – Full ZTNA for TCP

ZTNA Modes – Full ZTNA - TCP Forwarding Access Proxy (TFAP)

- FortiClient負責跟FGT建Tunnel，FGT再跟後端Server進行TCP流量連線。FGT的角色也是Reverse Proxy角色，會在Client端與FGT之間建TLS Tunnel。
  - TLS v1.3 for record layer
  - TLS v1.2 for handshake
- 也是基於Client端憑證的認證, same as HTTPS Access Proxy method
- ZTNA rules evaluation
- Optional SAML authentication is available
- Acts like Transparent proxy □ destination is the **real IP** of the server



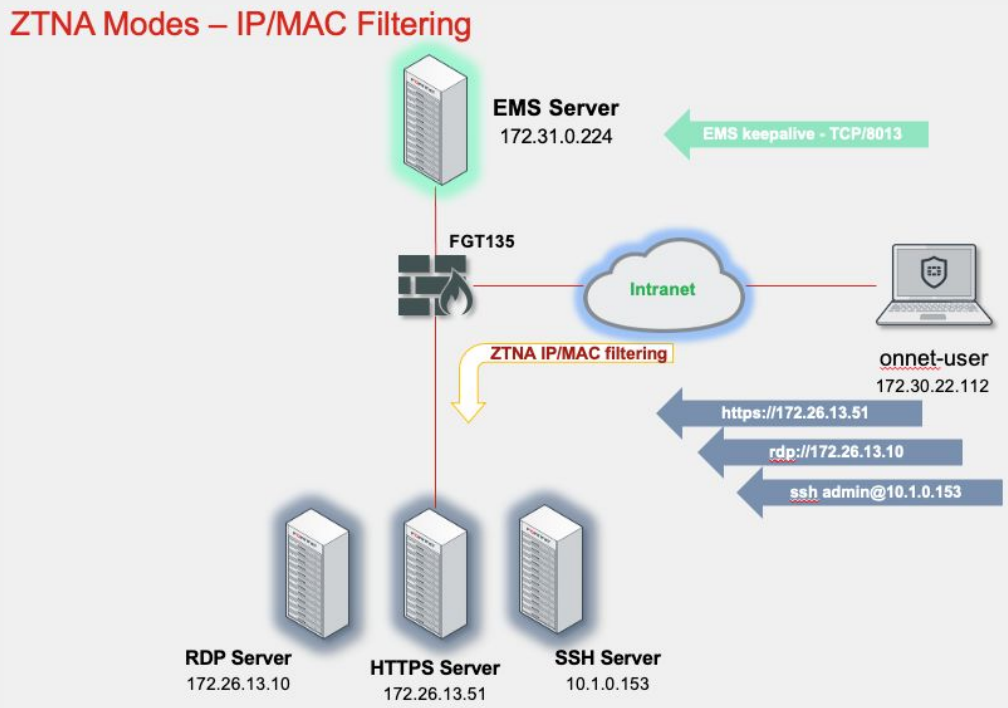

```
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 238
  Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 234
      Version: TLS 1.2 (0x0303)
      Random: 7d738b352164329849491ad362fff2de6ba2bee7015fdea9920c817927a61dc0
      Session ID Length: 32
      Session ID: 97c9c7c1c20e50b364076a62f22132515b4ceaa2b78bd31232b26e495b54b030
      Cipher Suites Length: 38
```



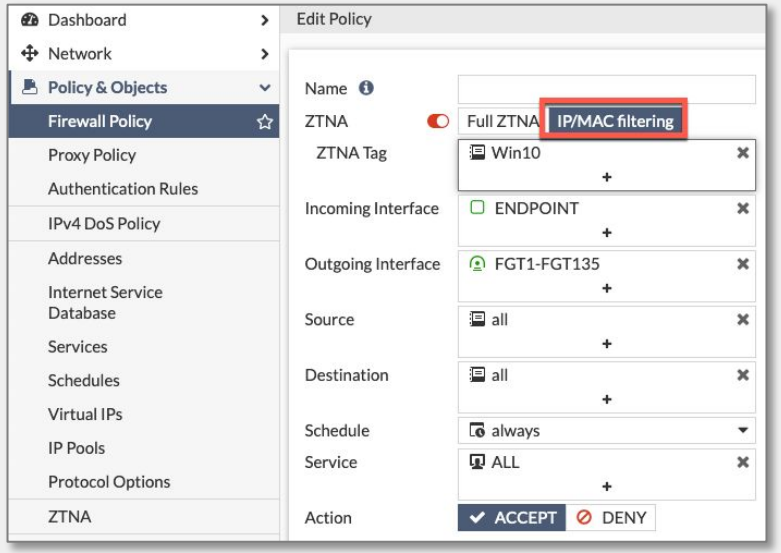
ZTNA模式 – IP/MAC Filtering

ZTNA Modes – **IP/MAC Filtering**

- EMS 6.4版前就有所謂的Tag可以用來控制存取
- “Tags”會同步到FortiGate的dynamic address list objects
- On FortiGate, tags are processed (matched) as an IP or MAC address group within Security Policy

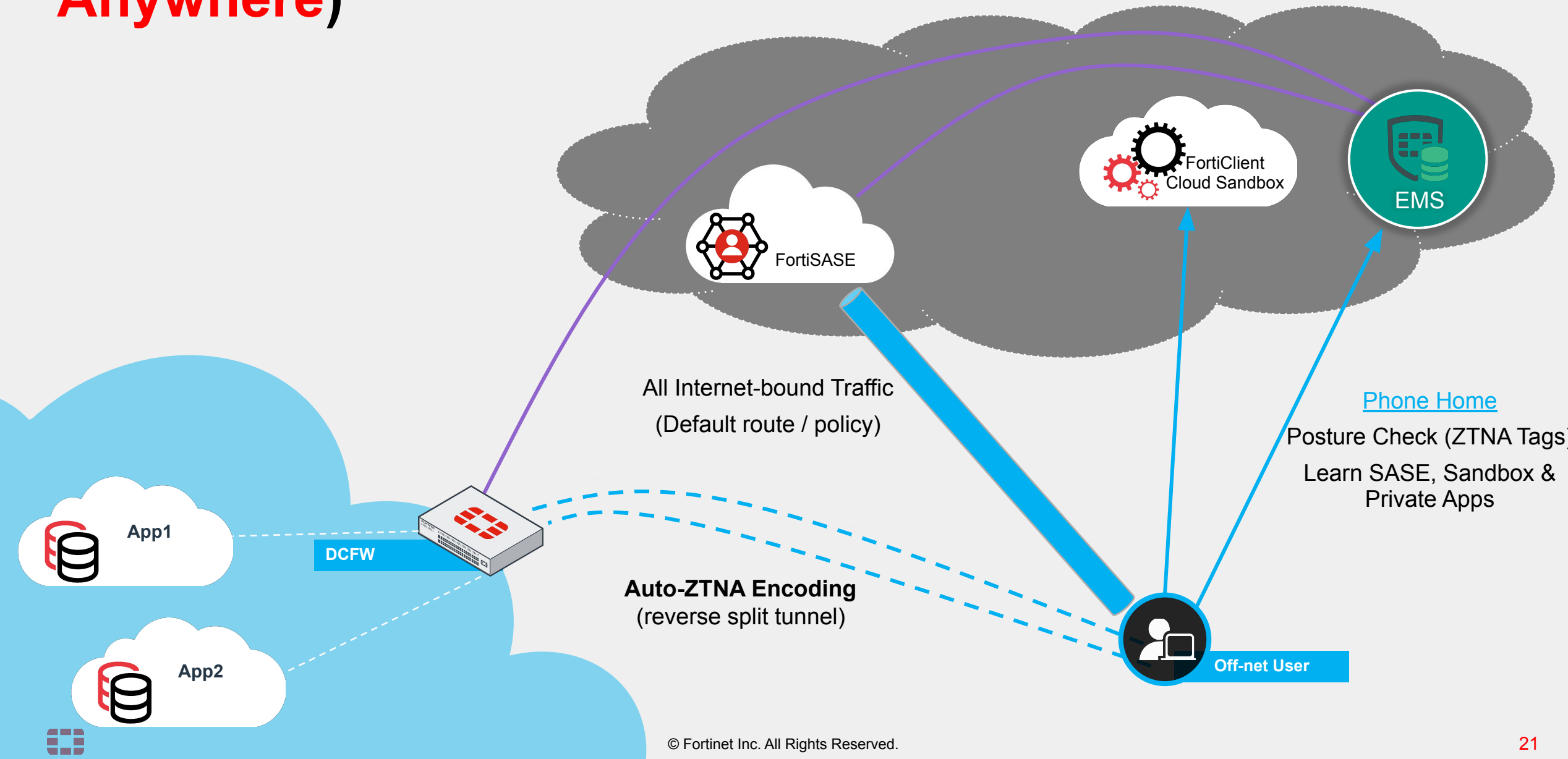


IP-based processing in the Firewall Policy rule (looking at ‘diagnose firewall dynamic list’ output)



Note: Use CLI to assign TAG to the policy

Fortinet零信任架構應用(WFH到WFA, Work From Anywhere)



FortiClient功能

3 **ENDPOINT PROTECTION (EPP)(端點防護)**

App FW, Anti-malware, Anti-exploit, Web Filtering

ADVANCED THREAT PROTECTION(威脅防護)

Sandbox Integration

2 **SECURE REMOTE ACCESS(遠端存取)**

SSL & IPSec VPN, SSO

1 **FABRIC AGENT(織網代理程式)**

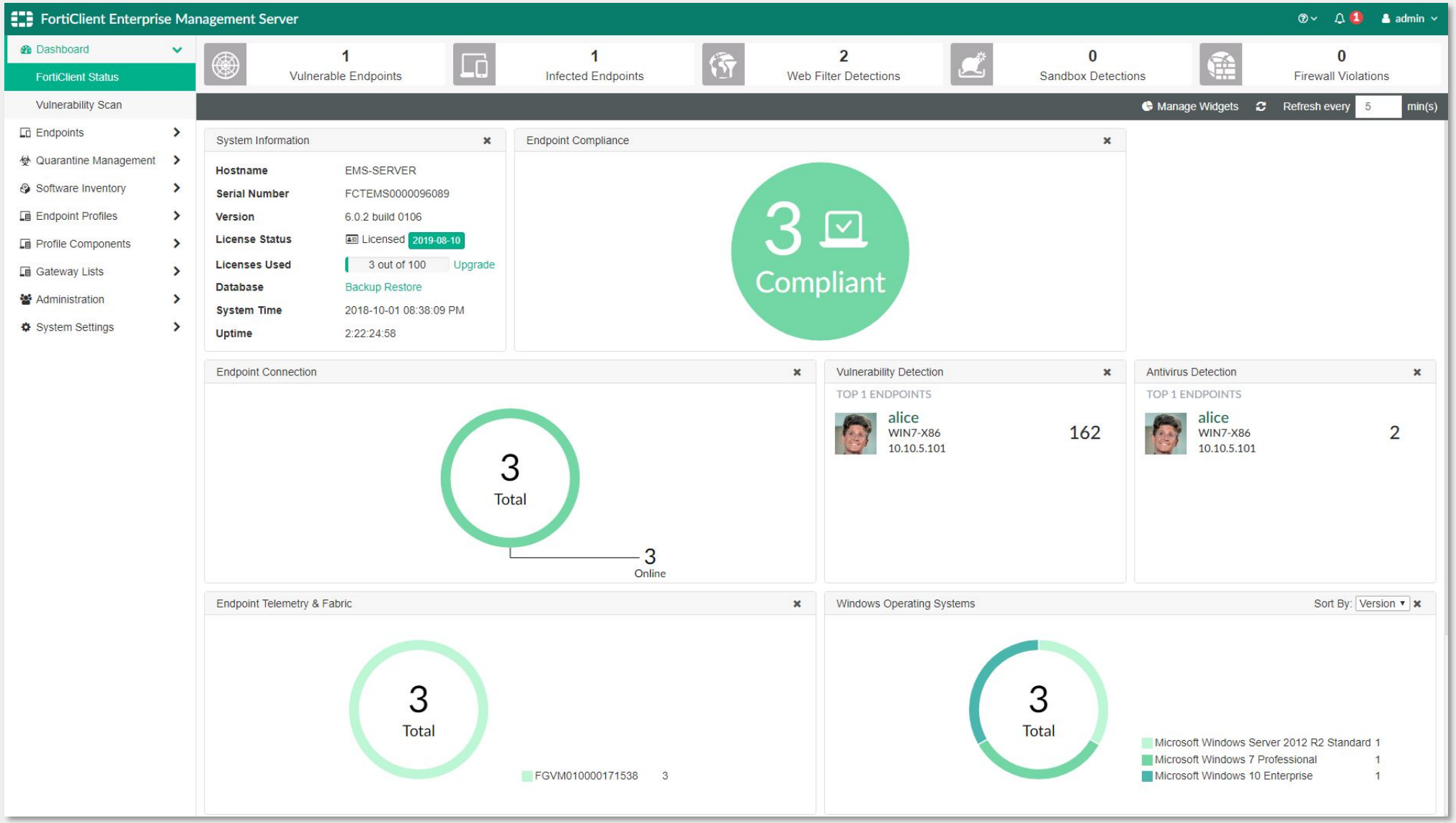
Telemetry, Quarantine, Vulnerability, App Inventory

整合Fortinet安全織網
FortiGate, FortiSandbox, FortiAnalyzer, FortiAuthenticator

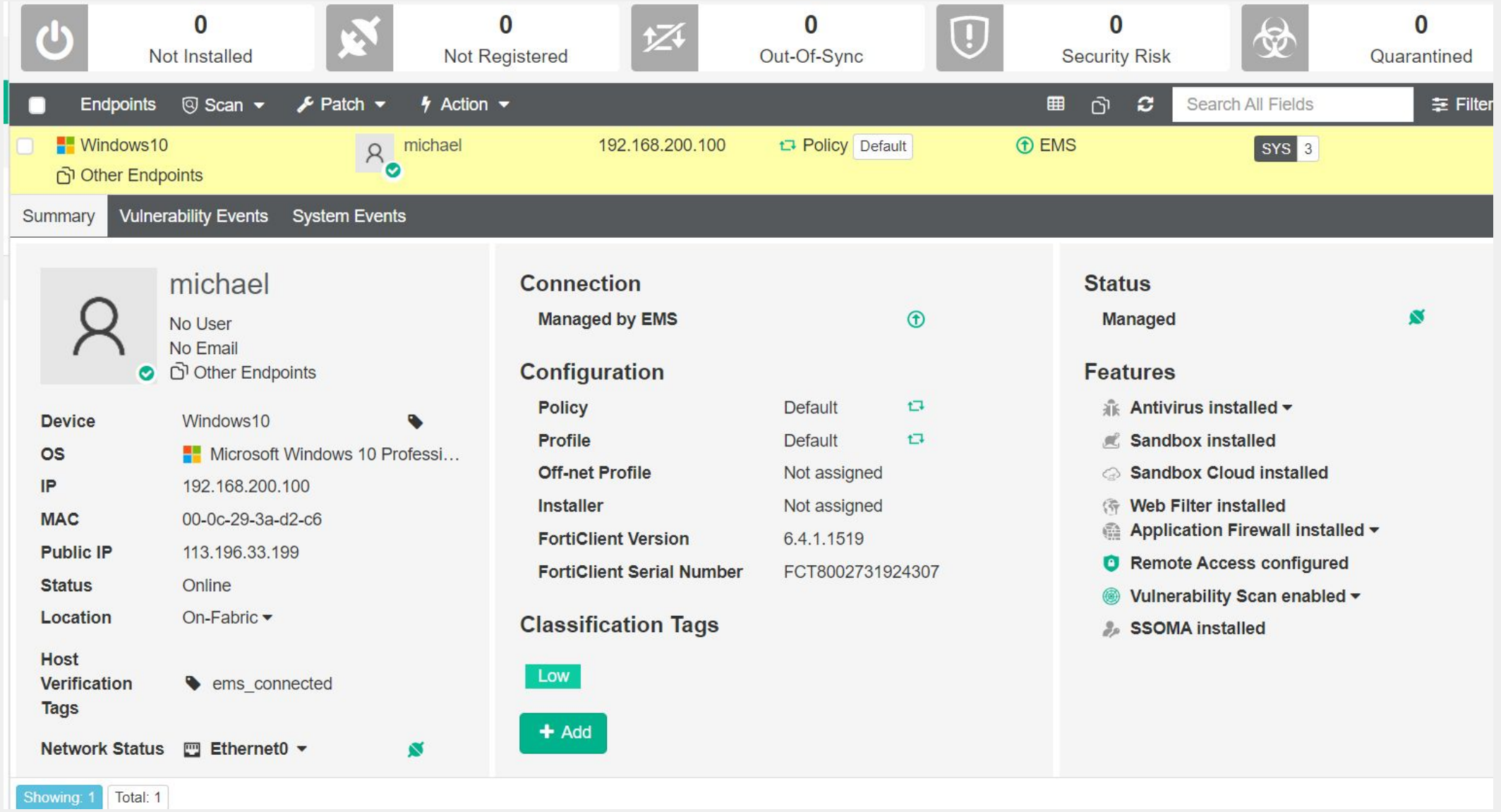
FortiGuard Services
CPRL AV, Web Filtering, App Firewall, Vulnerability Management

1	2	3
Endpoint/IoT Visibility and Control, and Compliance	**Secure Remote Access**	**Advanced Endpoint Protection**
FortiClient FortiGate Fabric Partners	**FortiClient FortiGate, FortiAuthenticator**	**FortiClient FortiSandbox FortiGuard**

FortiClient中央管理平台 – FortiClient EMS



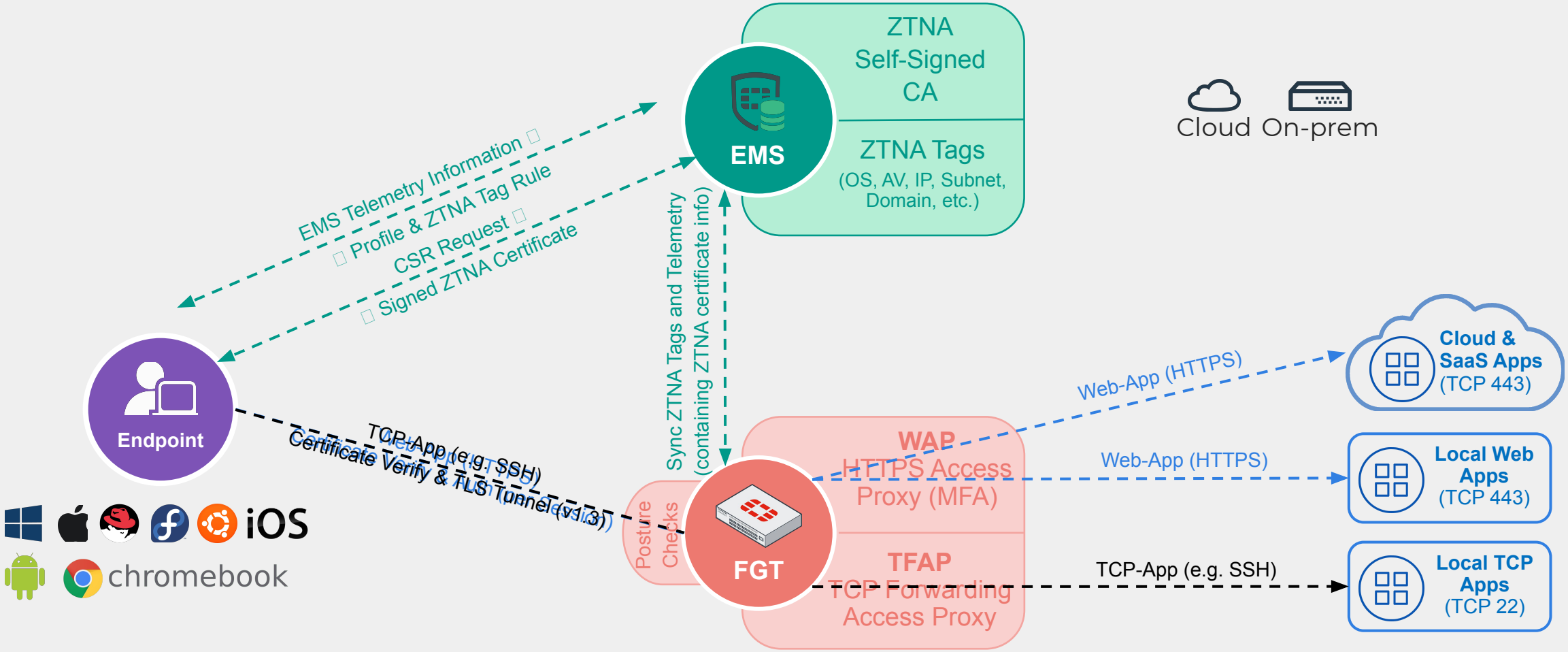
FortiClient中央管理平台 – FortiClient EMS



ZTNA Dynamic Tagging範例

Section Subhead

FortiClient EMS會同步Telemetry資訊給FGT



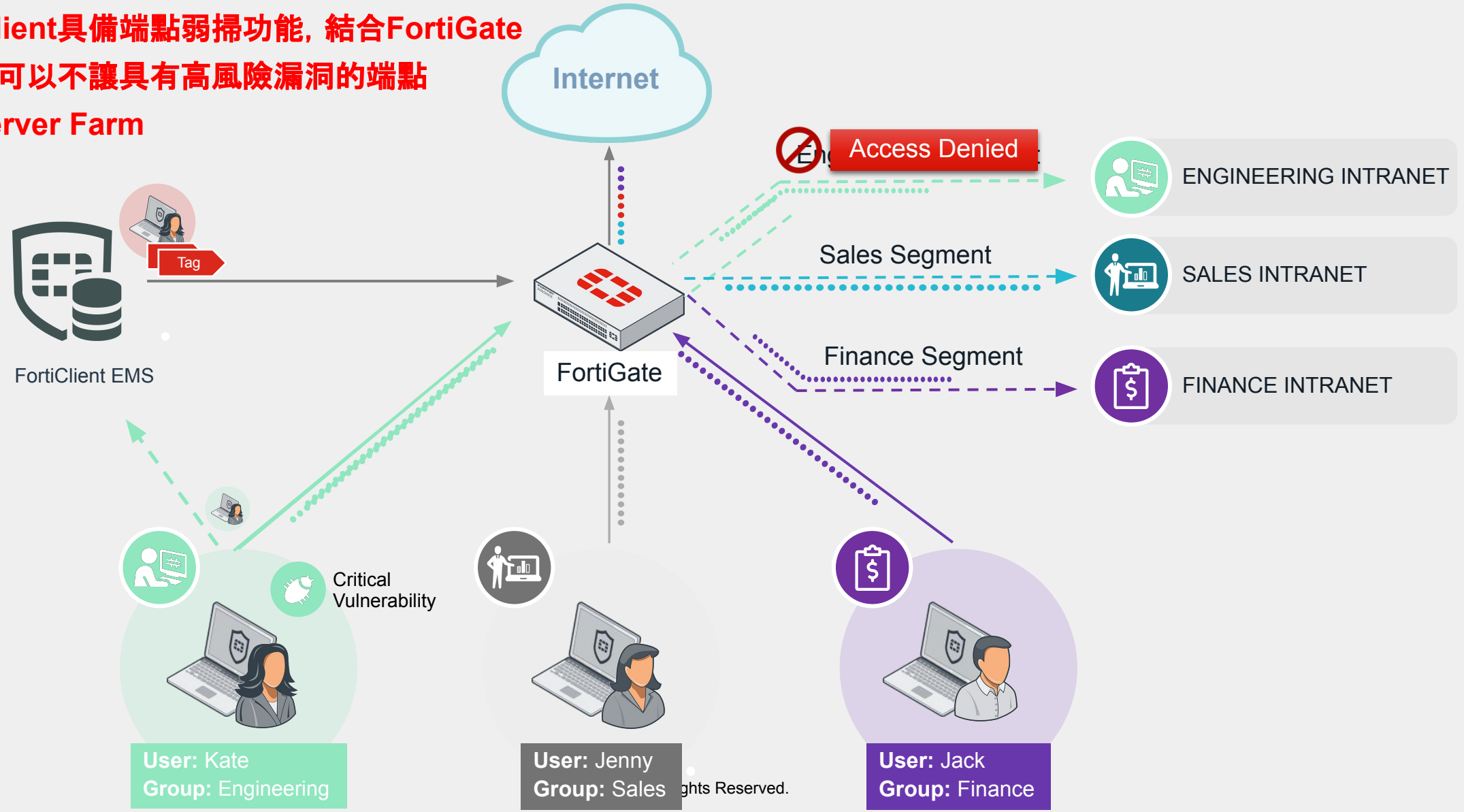
Dynamic Access Control (Intent Based Segmentation基於意圖的內網隔離)

Use Case: Block Access for Security Risk Endpoints

FortiClient具備端點弱掃功能，結合FortiGate

防火牆可以不讓具有高風險漏洞的端點

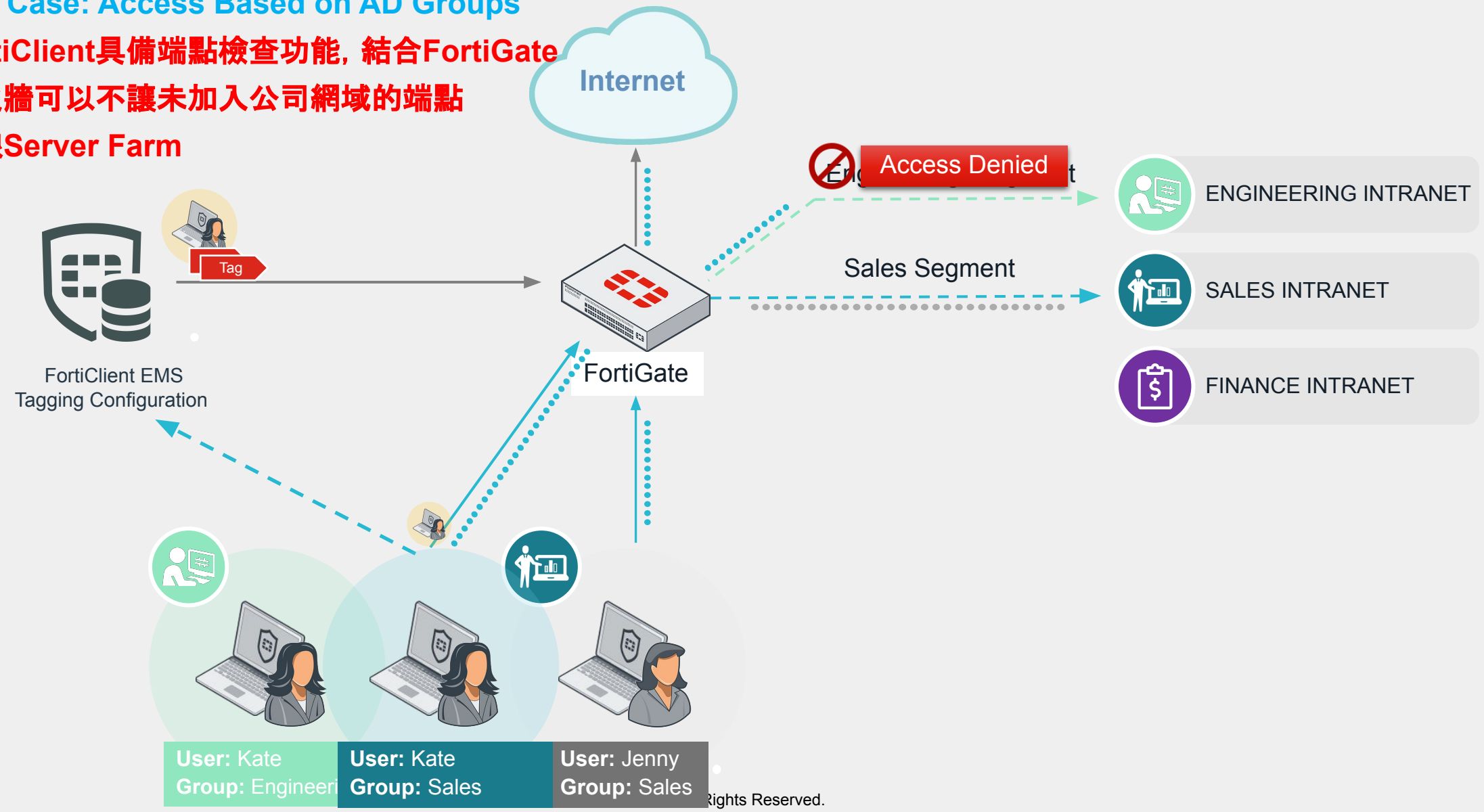
連線Server Farm



Dynamic Access Control (Intent Based Segmentation基於意圖的內網隔離)

Use Case: Access Based on AD Groups

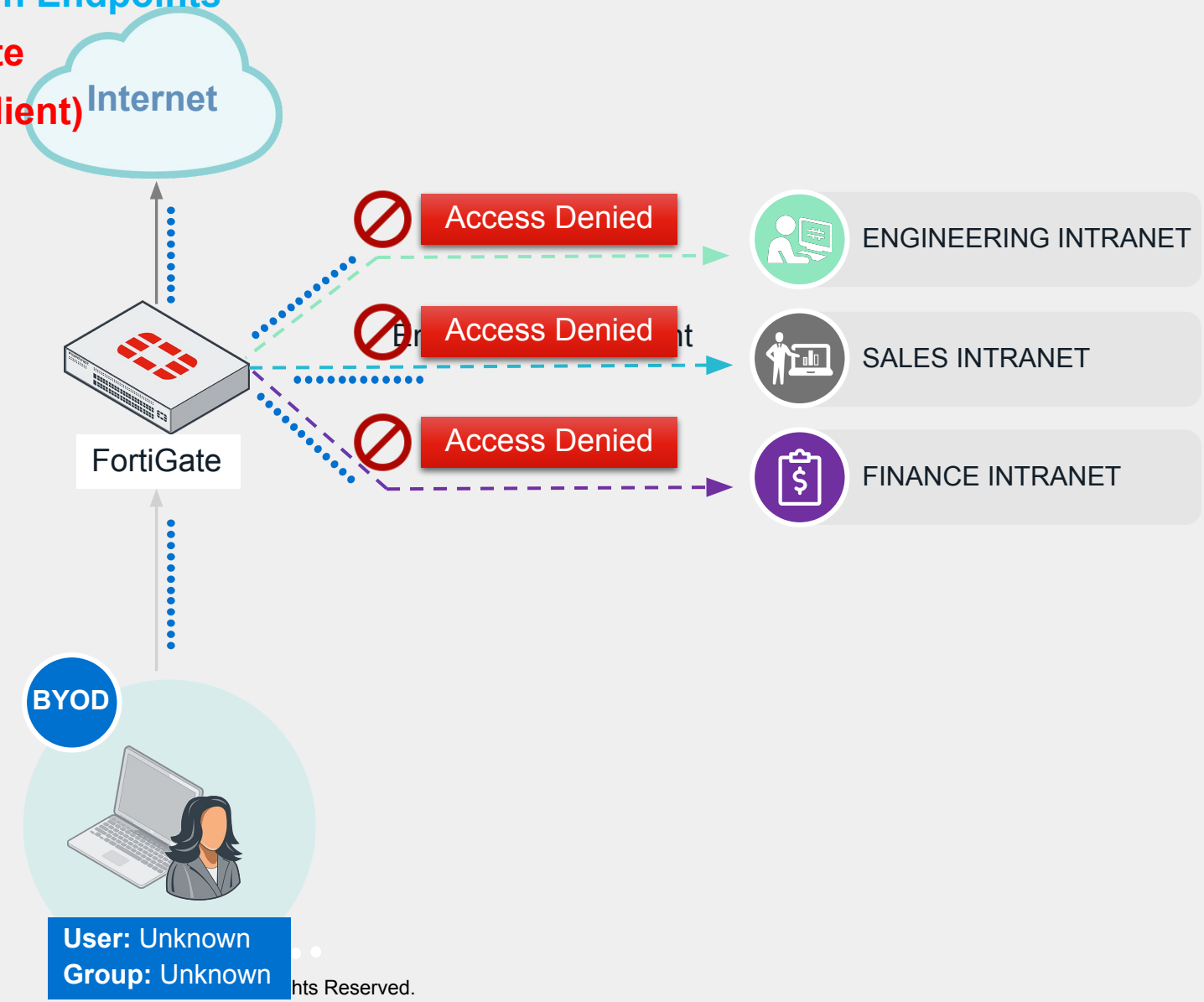
FortiClient具備端點檢查功能，結合FortiGate防火牆可以不讓未加入公司網域的端點連線Server Farm



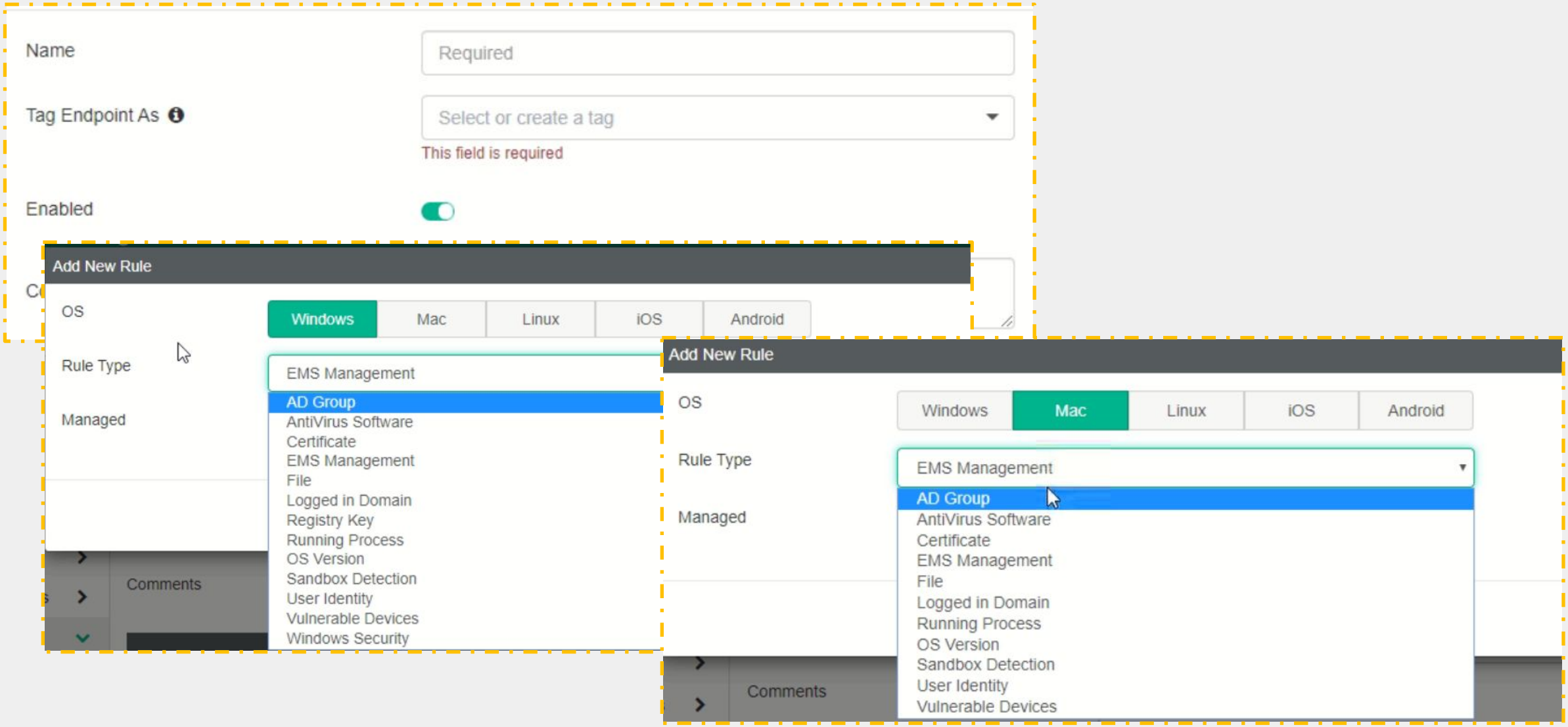
Dynamic Access Control (Intent Based Segmentation基於意圖的內網隔離)

Use Case: Restricted Access for Unknown Endpoints

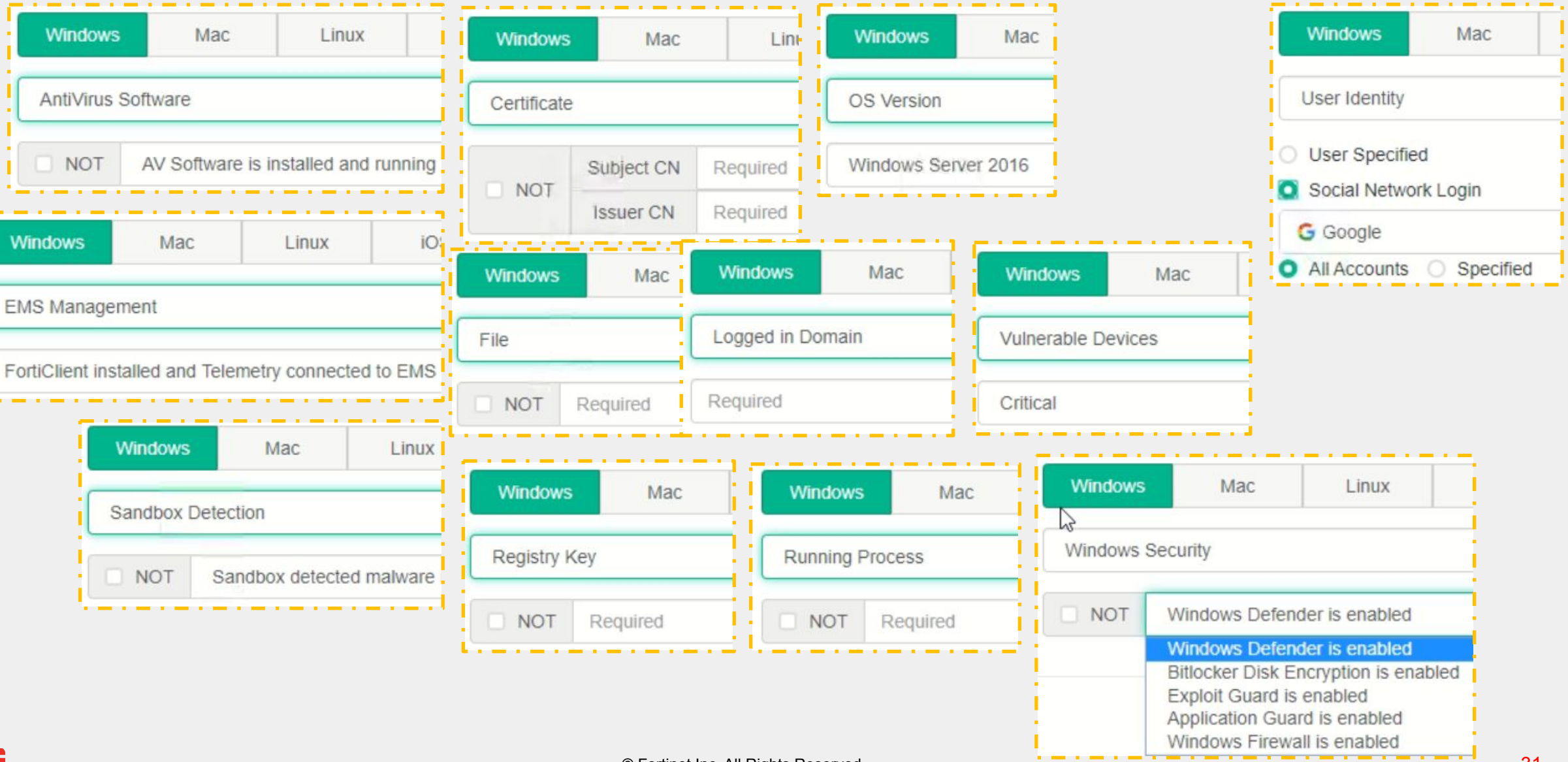
FortiClient具備端點檢查功能, 結合FortiGate
防火牆可以不讓未知使用者(或未安裝FortiClient)
的端點連線內網其他網段或出外網



FortiClient EMS上可以設定不同條件的 Rule



Rule中可以用多種屬性組合當Tagging條件



Fortinet Zero Trust Vision(一次或階段建置)

Zero Trust Networking

Users & Devices, Access & Segmentation

Phase 1

Zero Trust Access

Users & Device Access

FortiClient

Identity & Access Management (IAM)

384629

User Authentication/FortiToken

VPN Tunnel

Remote Access

Access Control (VPN+EMS)

FortiOS 7.0

Phase 2

Zero Trust Segmentation

Network Security

Segmentation (North-South)

Segmentation (East-West)

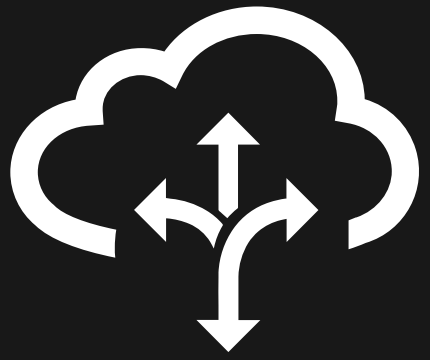
Micro Segmentation

FortiSASE(Security Access Service Edge)
安全存取服務邊緣

數位創新提供新服務

無處不在的業務需要無處不在的安全性

多雲服務的採用



93% 的企業採用多雲策略

2020 State of the Cloud Report, Flexra

遠端/行動用戶

70% 的用戶更喜歡遠程工作，但需要更好的用戶體驗

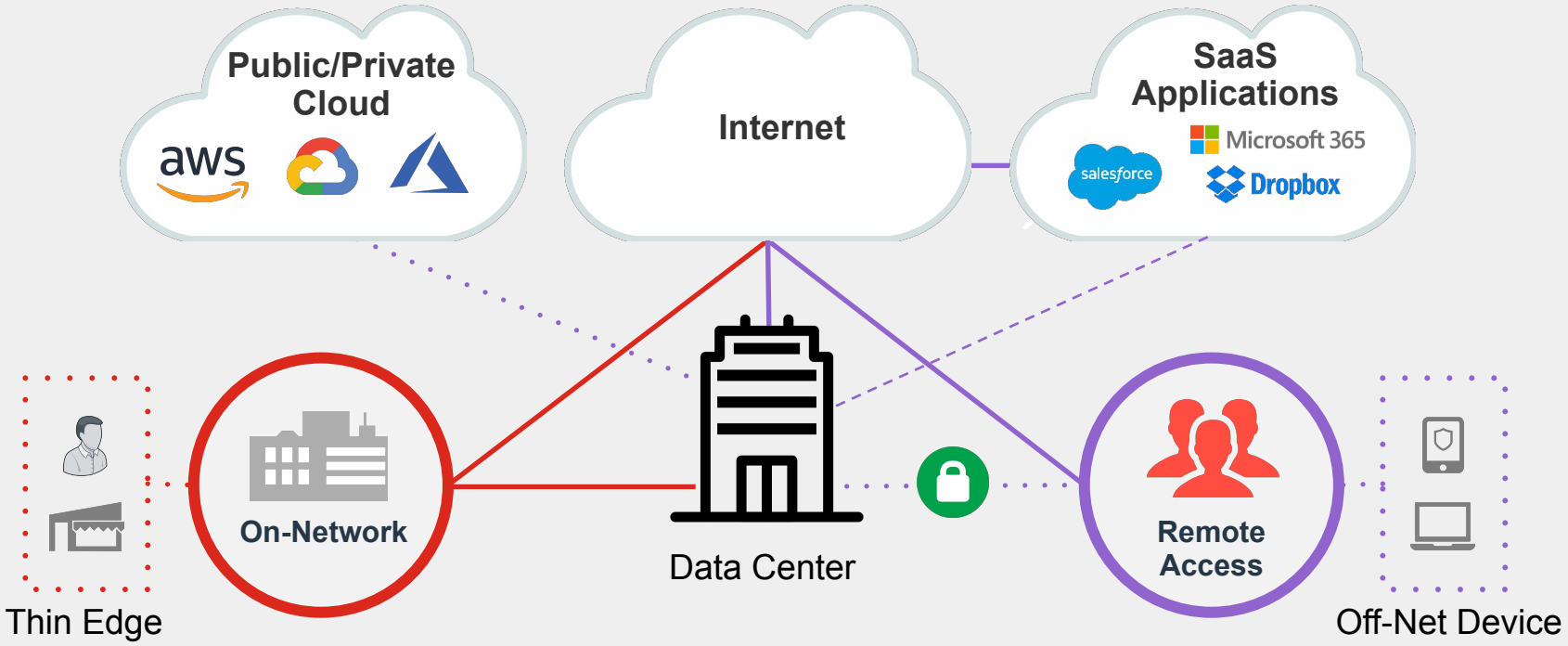
2020 State of Remote Work, Buffer

無處不在的安全

企業內和網路外的安全性必須保持一致

2020 FortiGuard Threat Report, Fortinet

企業擴展的新挑戰



主要挑戰

1. 多雲環境使用者體驗不佳
2. 行動辦公資安問題
3. 缺乏一致性的安全防護在所有的edge邊緣端

COVID-19疫情轉變了工作型態

Before COVID

17%

of workers did most of their work remotely[iii]

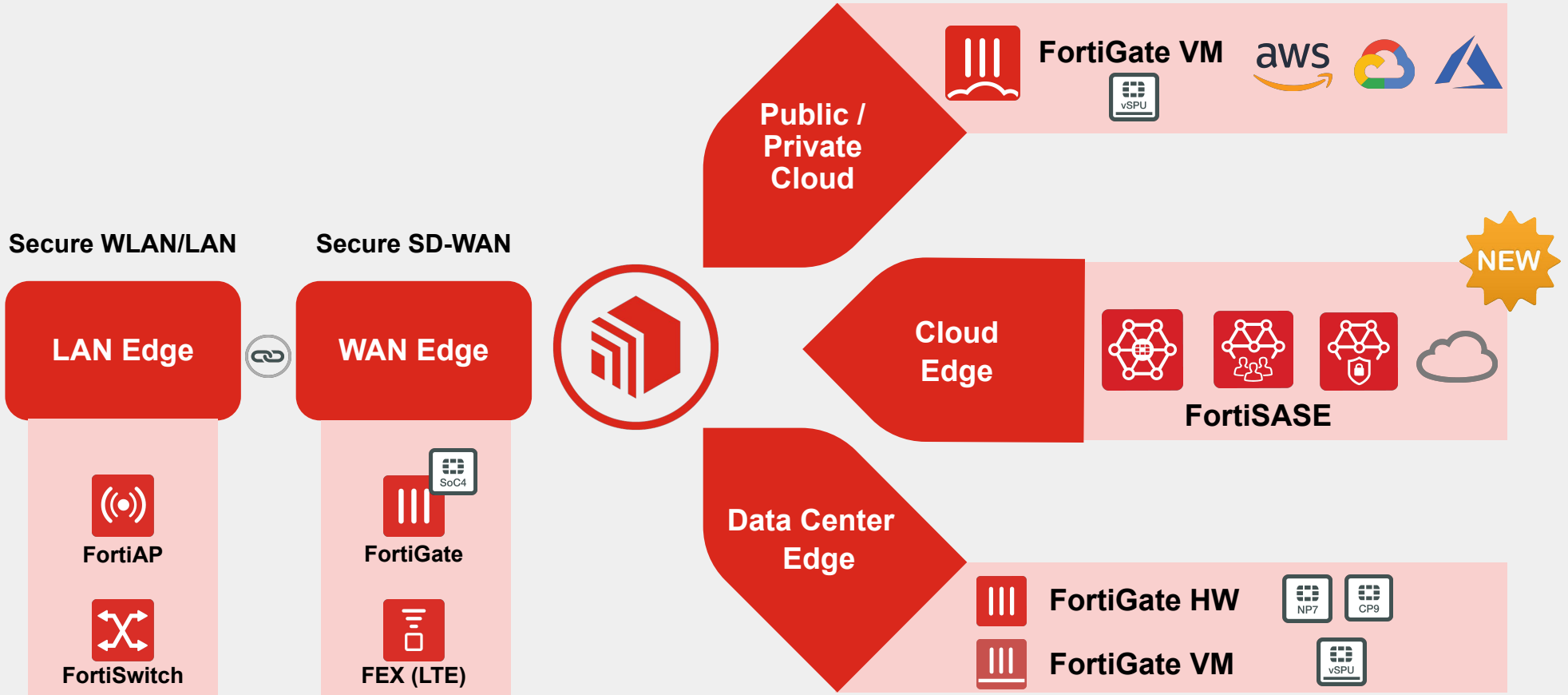
Since COVID

78%

of workers do most of their work remotely[iv]

安全驅動的網路願景

彈性，無處不在的安全性



什麼是SASE?!

到2024年，至少40%的企業有明確的策略來採用SASE

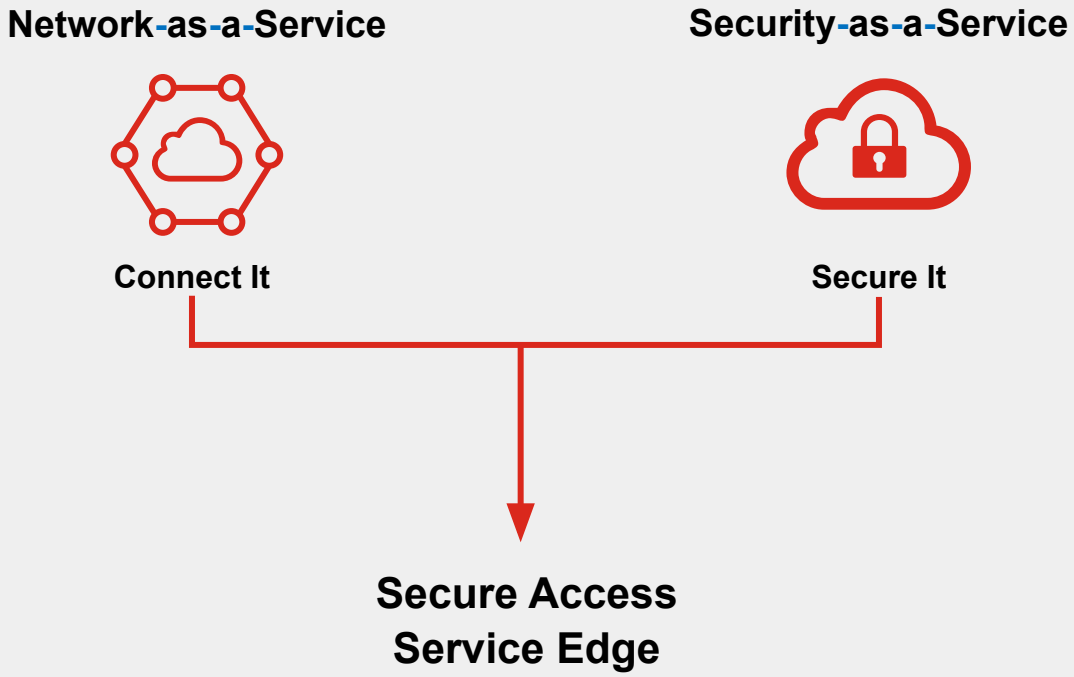
客戶對簡單性，可伸縮性，靈活性，低延遲和普遍安全性的需求迫使WAN邊緣和網絡安全市場融合

Customer demands for simplicity, scalability, flexibility, low latency and pervasive security force convergence of the WAN edge and network security markets

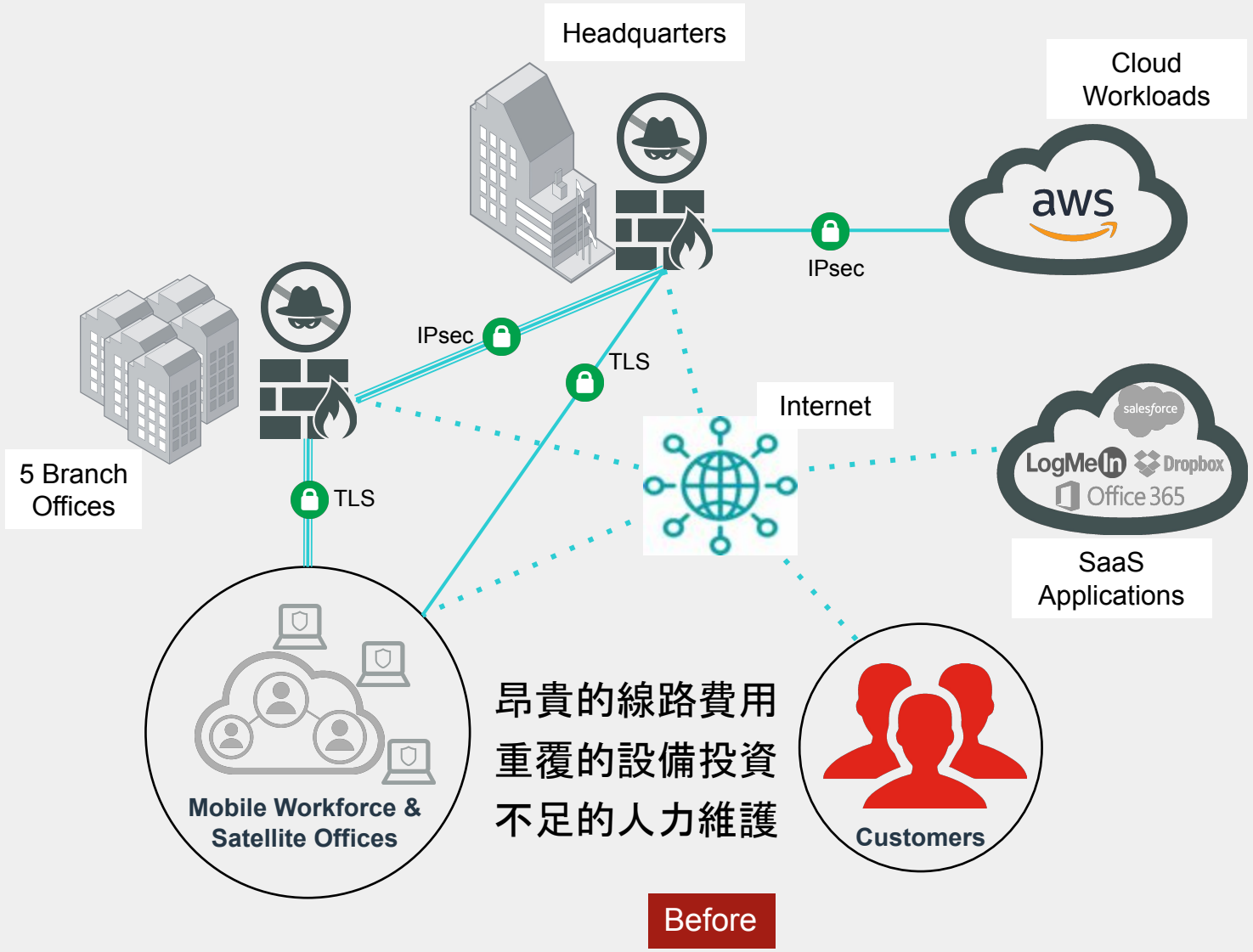
Gartner

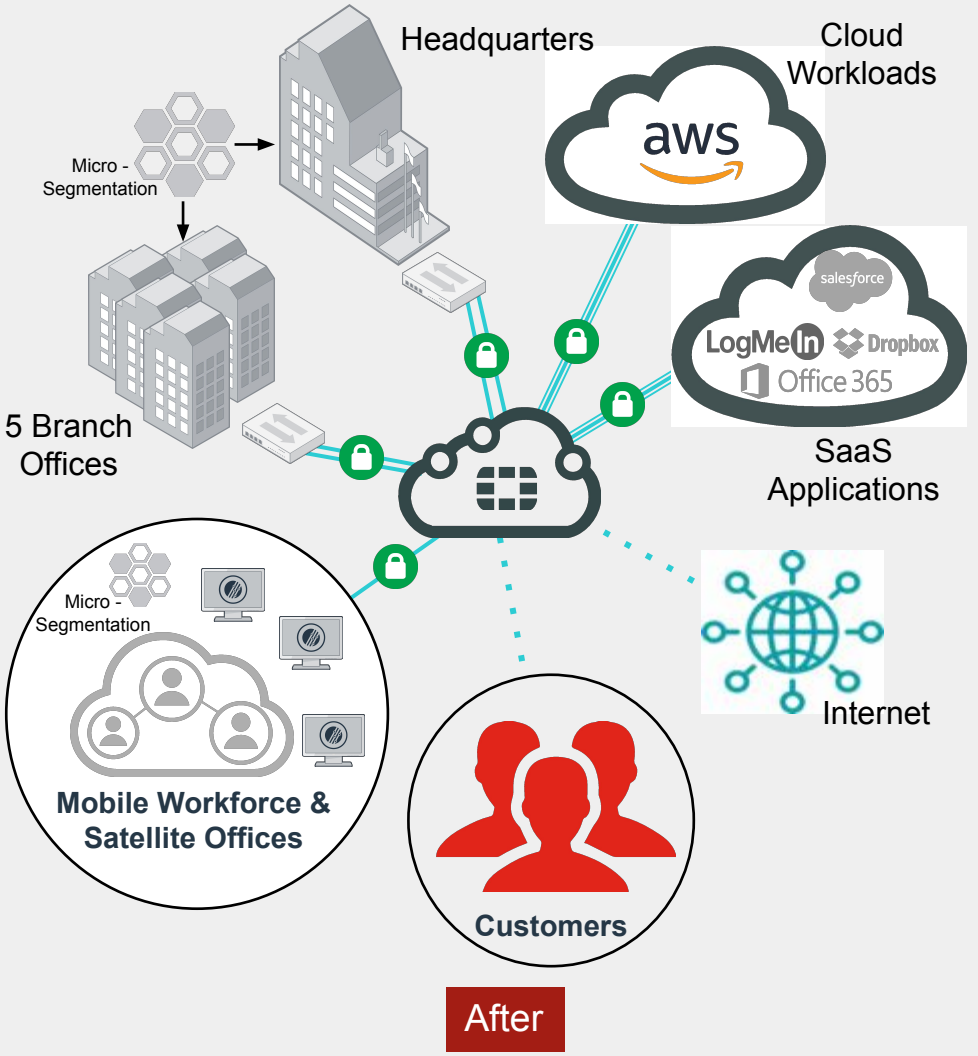
Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge – 29 July 2019

Source: Gartner



架構要簡單，端點更要安全

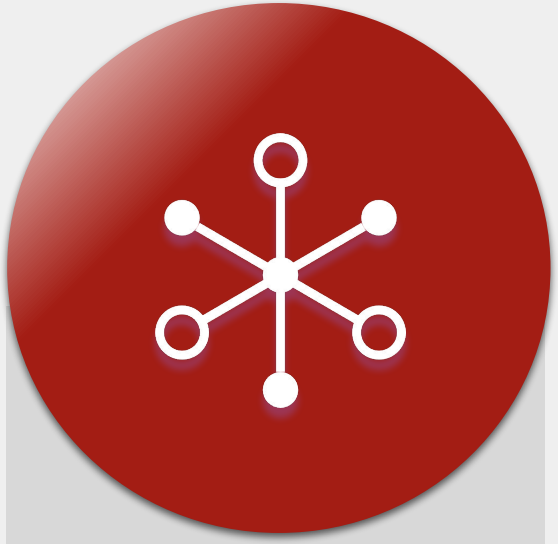




FortiSASE的創新性改革

高性能網路優化應用程序和用戶體驗

性能



雲端架構服務，可按需求彈性擴展

敏捷

一致性的存取政策

存取安全

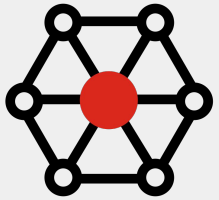
輕鬆設定，一鍵部署，服務不間斷，始終安全

管理

FortiSASE核心安全服務元件

Desired SASE Components per Gartner

ZTNA as a Service	ZTNA standalone	SWG	CASB	FW(aaS)	WAF/WAAP	VPN	CDN
RBI	VDI	Sanitized DNS	Network Sandbox	Network Obfuscation	Edge Compute Protection	SD-WAN	

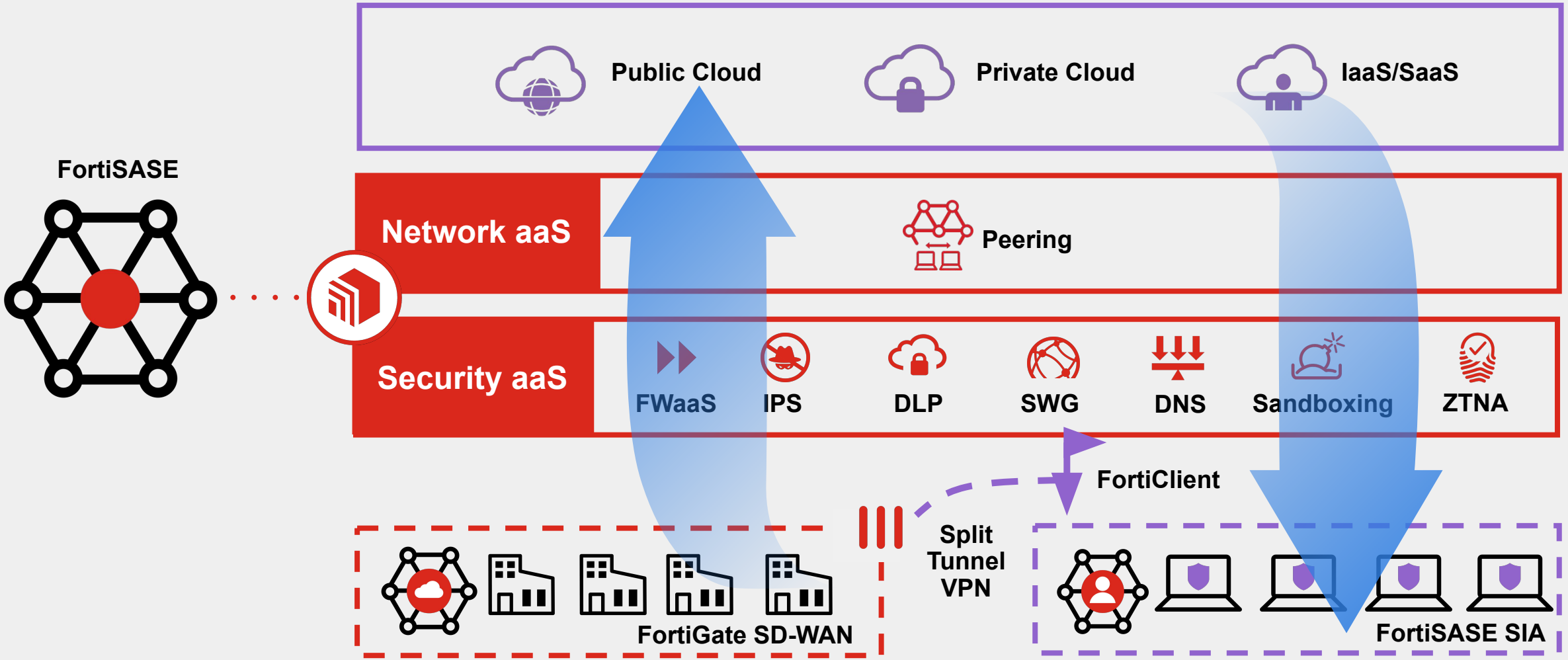


FortiSASE提供業界支援最廣泛的SASE服務

Gartner: SASE Will Improve Your Distributed Security Everywhere - Published 8 December 2020

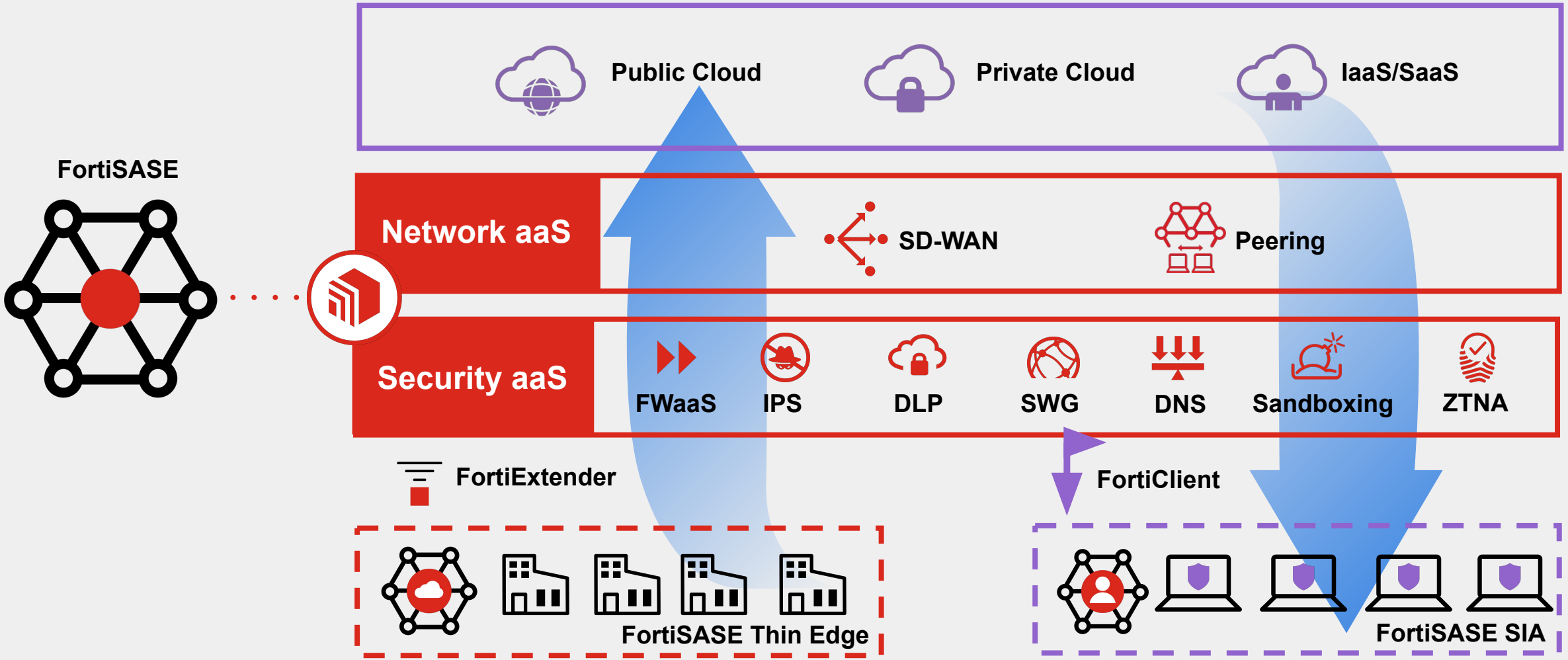
FortiSASE SIA

快速，安全與可擴充的VPN替代方案

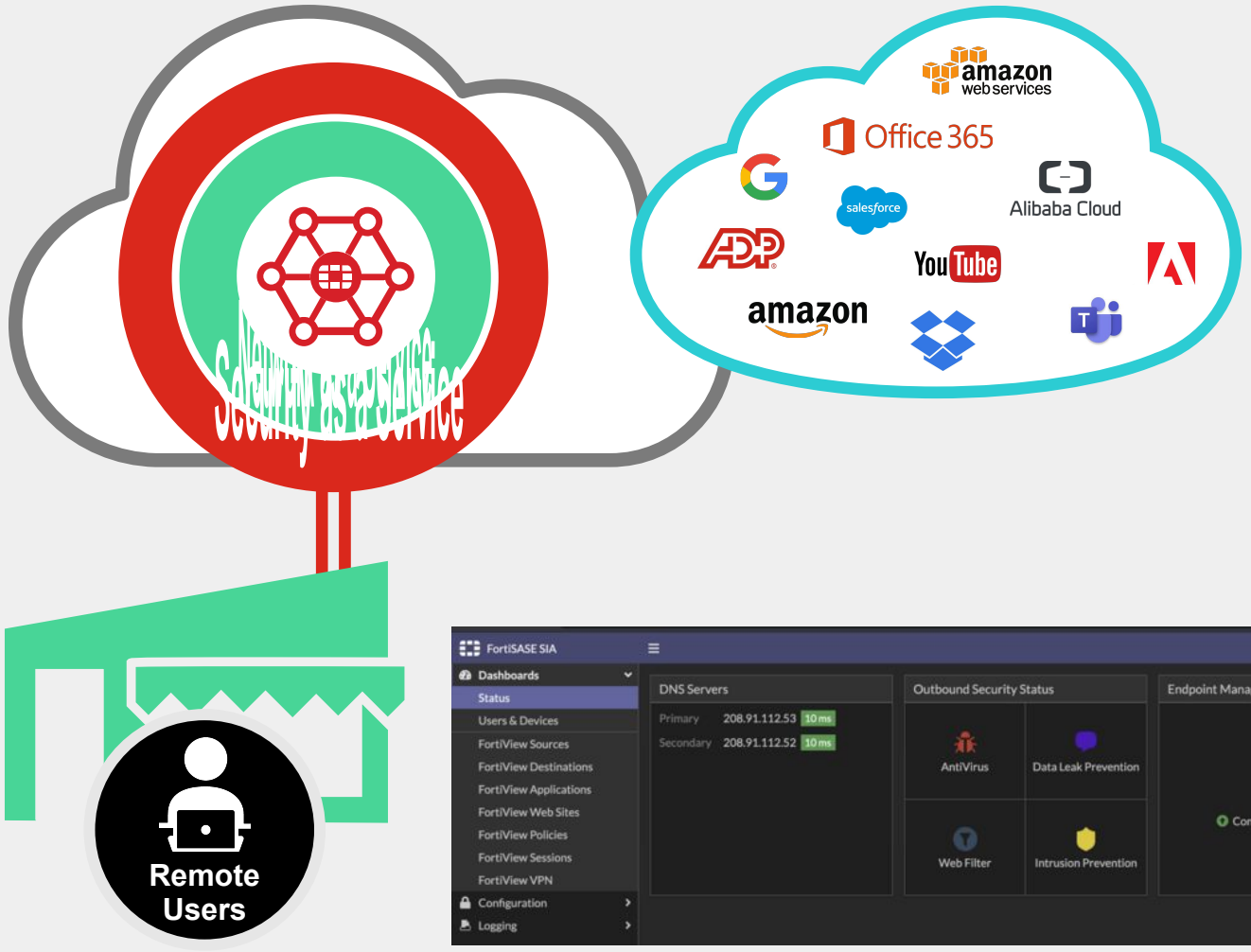


FortiSASE Thin Edge + SIA

擴展資安橫跨light and heavy branch locations



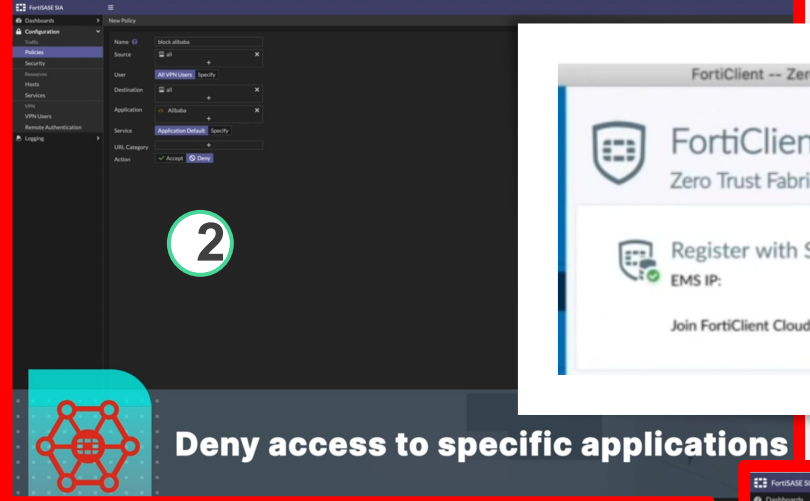
FortiSASE Secure Internet Access (SIA)

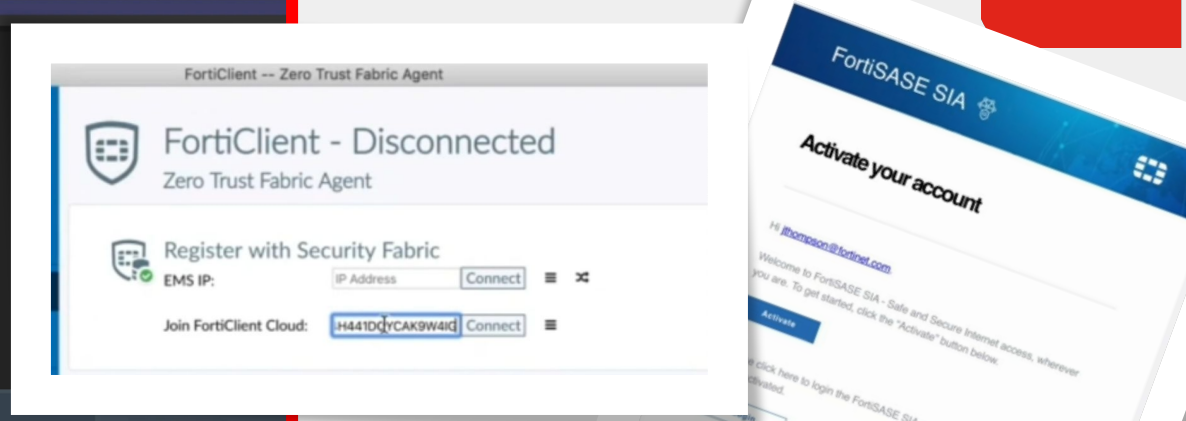


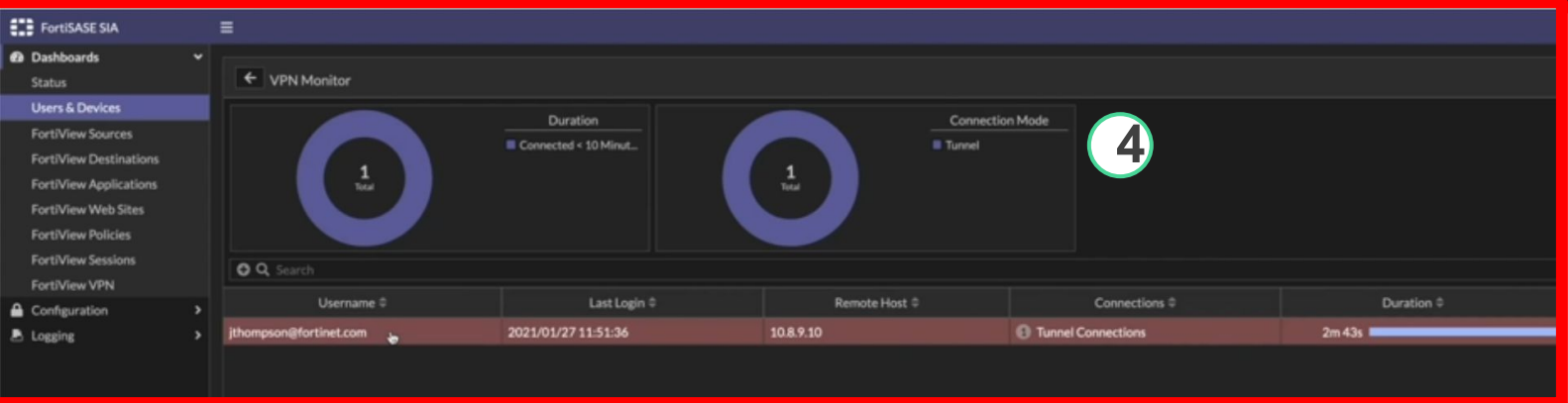
	SASE Edition
Zero Trust Security	Windows, MAC, Linux
Zero Trust Agent	·
Dynamic Security Fabric Connector	·
Vulnerability Agent & Remediation	·
SSL / IPSEC VPN with MFA	·
USB Device Control	·
Automated Endpoint Quarantine	·
Application Inventory	·
Cloud Based Endpoint Security (SASE)	
SSL Inspection	·
Inline AV & Anti-Malware	·
Intrusion Prevention (IPS)	·
FortiGuard Web Filtering	·
Application Firewall	·
Data Leak Prevention	·
Additional Services	
24 x 7 Support	Included
SASE Cloud Management	Included
SASE Cloud Logging	Included
Best Practice Onboarding Service	Included in 1st Year

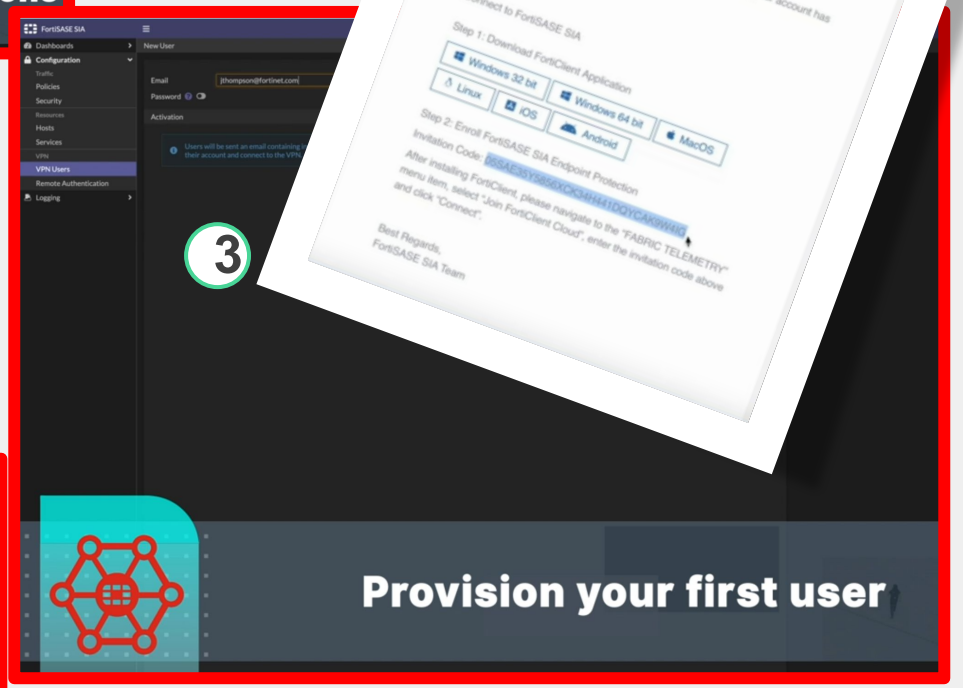
Available in Packs of 25, 500, 2000 and 10,000

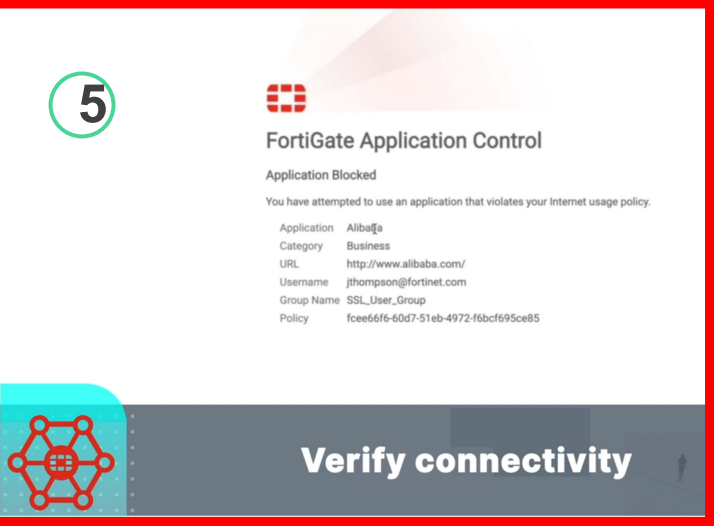

1
Configure Security Inspection rule

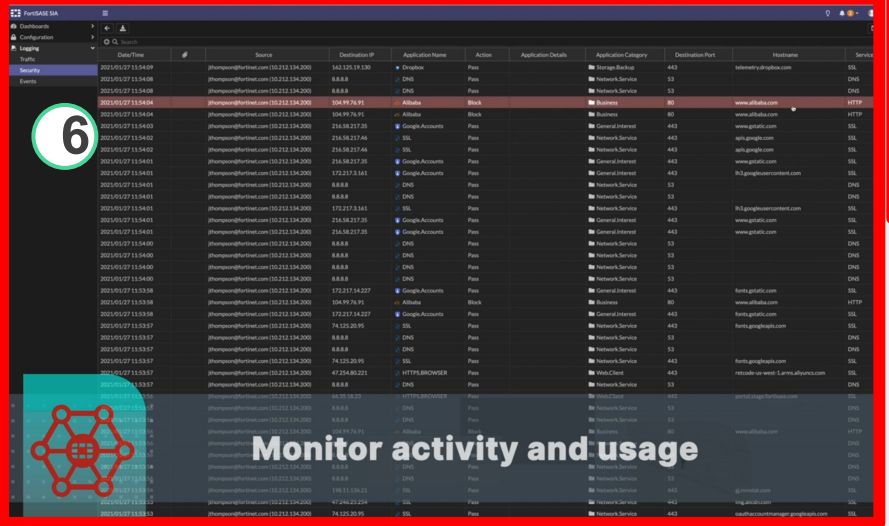

2
Deny access to specific applications


FortiClient -- Zero Trust Fabric Agent
FortiClient - Disconnected
Zero Trust Fabric Agent
Register with Security Fabric
EMS IP:
IP Address
Connect
Join FortiClient Cloud:
Connect


FortiSASE SIA
Dashboards
Status
Users & Devices
FortiView Sources
FortiView Destinations
FortiView Applications
FortiView Web Sites
FortiView Policies
FortiView Sessions
FortiView VPN
Configuration
Logging
VPN Monitor
Duration
Connected < 10 Minut...
Connection Mode
Tunnel
4
Search
Username
Last Login
Remote Host
Connections
Duration
jthompson@fortinet.com
2021/01/27 11:51:36
10.8.9.10
Tunnel Connections
2m 43s


3
Activate your account
FortiSASE SIA
Provision your first user


5
FortiGate Application Control
Application Blocked
You have attempted to use an application that violates your Internet usage policy.
Application Alibaba
Category Business
URL http://www.alibaba.com/
Username jthompson@fortinet.com
Group Name SSL_User_Group
Policy fcee66f6-60d7-51eb-4972-f6bcf695ce85
Verify connectivity


6
Monitor activity and usage

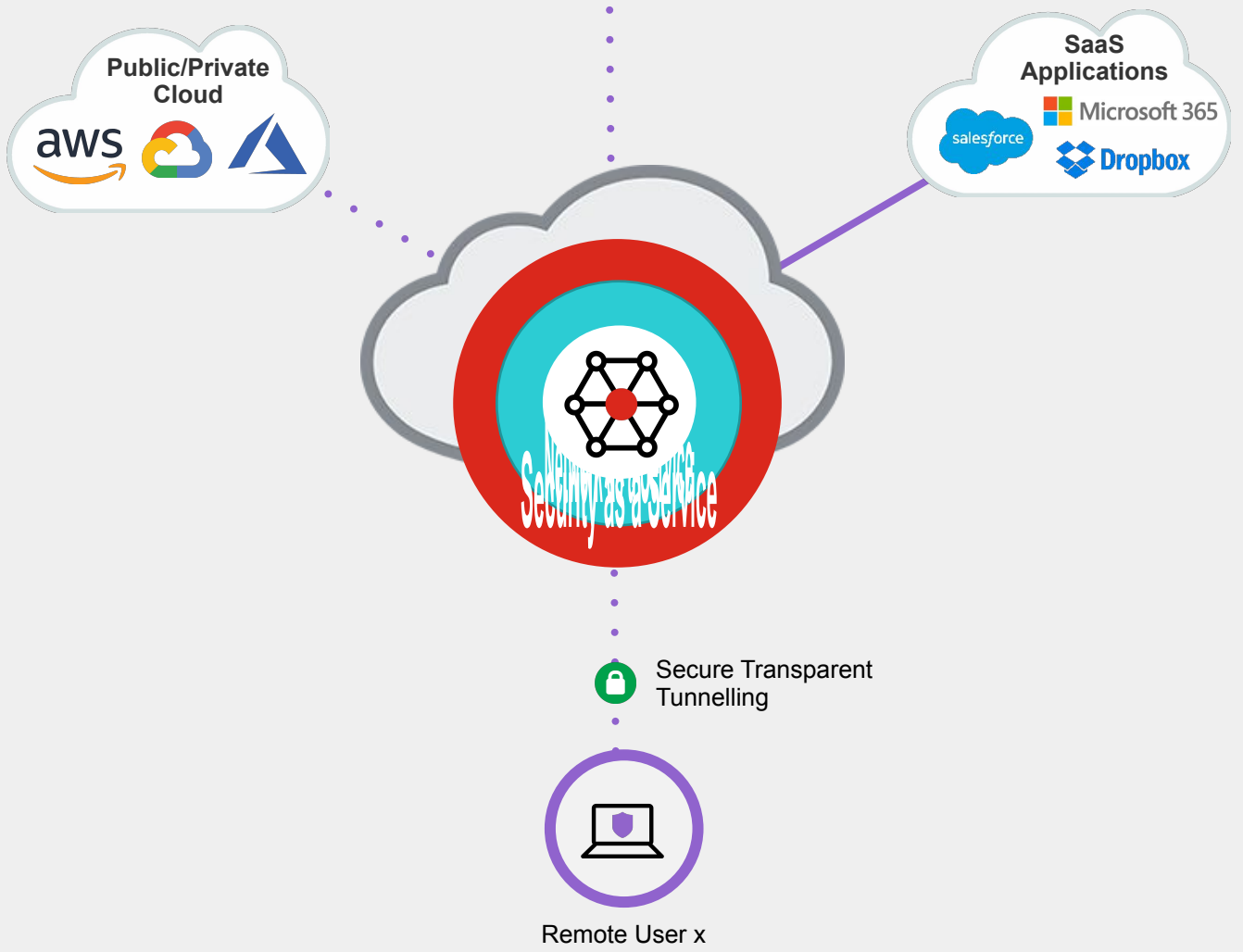

FORTINET

保護行動/遠端用戶

透過雲端為行動用戶提供安全

Outcomes

- 輕量級 (lightweight)代理程式，提供多種功能
- 直接存取SaaS，以獲得更好的用戶體驗和優化
- 深層過濾檢查，提供進階威脅防護(ATP)
- 一致性，擴展的防火牆功能和控制即服務交付



保護分公司

不間斷，永遠可用的安全訪問

Outcomes

- 減少對昂貴線路(MPLS or DSL)的依賴
- 從一致性的安全政策從總公司、外點到行動用戶
- 透過3G/4G、5G等低成本連網方式即可達到安全保護