Fortinet Security-Driven Networking – 輕鬆部署安全的網路環境

Jarvis Lee

ljarvis@fortinet.com

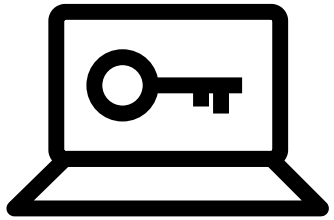
IT以及網路安全的趨勢

隨時隨地

都能工作

COVID-19之後，遠程工作的轉變仍將持續。
52% 的 CIO 預計 2021 年在家工作將增加。

Gartner – Top Priorities for IT Leadership 2021

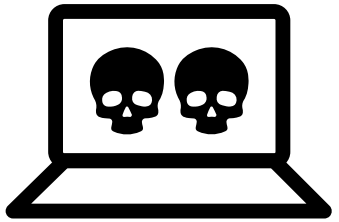


安全的

數位轉型

69% 的企業通過數位轉型加速響應 COVID-19，
而 60% 的企業選擇通過數位轉型提高運營卓越性。

Gartner – Top Priorities for IT Leadership 2021



防止

網路攻擊

36% 的企業表示，威脅環境日益複雜是防止勒索軟件攻擊的最大挑戰。

Fortinet – Ransomware survey 2021

網路/資安

人才短缺

73% 的企業在過去一年中至少發生過一次入侵/違規事件，部分原因是網絡安全技能方面的差距。

Fortinet – Cybersecurity Skills Survey 2,500 US and Canadian companies 2021

保護所有網路邊界

每個邊界都必須要做到網路以及安全融合

- 傳統的Hub以及Spoke架構對於新的工作型態WFA以及多雲應用來說效率以及可擴展性不高
- 單純透過互聯網直接訪問Internet並透過4G/5G當作備援，缺乏安全性與有效的線路利用無法實現完美的數位轉型。
- 透過各別的Wan Loadblance + Firewall解決方案，缺乏統一系統管理造成維運負擔。
- 異常發生時透過只透過手動方式操作，影響用戶體驗。網路問題極難解決。

有效的安全營運

在擴展的攻擊面中跟上複雜的威脅攻擊

- 有組織且複雜的威脅行為 (犯罪組織、國家資助) 正在開發規避傳統保護技術的策略。
- 隨著 WFA, Cloud, 等應用的出現，擴展了攻擊面引發網路攻擊的激增。
- 獨立運行的安全產品增加，會減緩響應速度並且較難達到自動化維運。
- 大量的安全事件無法識別、事後調查、補救。
- 缺乏熟練的網路安全專業人員，也因設備增加環境複雜使得招娉以及留住員工變得困難。

Fortinet Security Fabric 安全織網

全面性 (Broad)

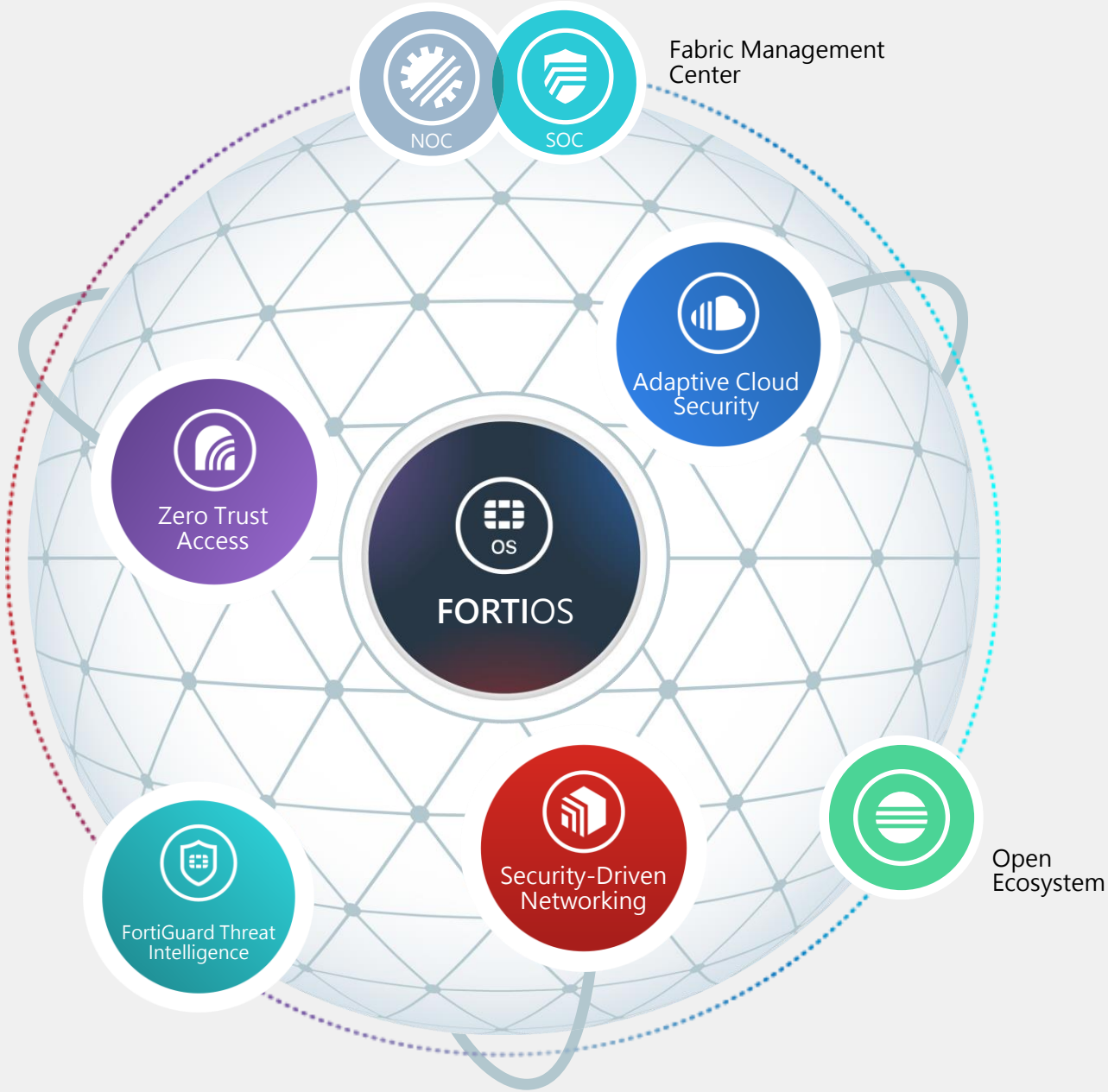
對全部數位化攻擊面提供更佳可視性與防護，以利更好的風險管理

整合性 (Integrated)

整合多樣化產品解決方案，降低管理複雜度，並能共享威脅情資

自動化 (Automated)

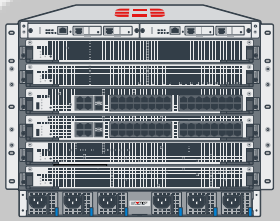
導入AI與機器學習，帶動資安聯防自動化，提升營運效率和威脅回應速度



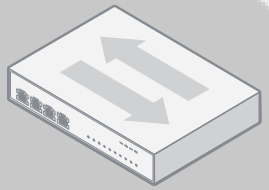
在任何邊界提供企業保護和用戶體驗，藉以協助企業提高生產力。

Network Security

Security-driven Networking

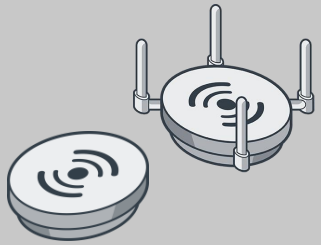


FortiGate



FortiSwitch

Fortinet
Secure SD-WAN
Secure SD-Branch



FortiAP

FortiAnalyzr
FortiManager

Secure SD-WAN Solution

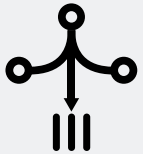
一流的安全 SD-WAN 解決方案

善用WAN線路，透過單一的操作系統提供安全的WAN環境。

01 卓越的用戶體驗

Accurate application steering with advanced WAN remediation and better user experience

02 有效的善用資源



Powered by One OS with advanced routing, SD-WAN and NGFW with best performance

03 效率的安全營運

Scalable Centralized Management and analytics for SD-WAN & SD-Branch to provide NOC and SOC

Fortinet Secure SD-WAN 解決方案和優勢

10X
任何規模的體驗改進

通過 Advanced WAN 實現準確的應用程序控制，以提供更好的用戶體驗

65%
有效降低人力成本

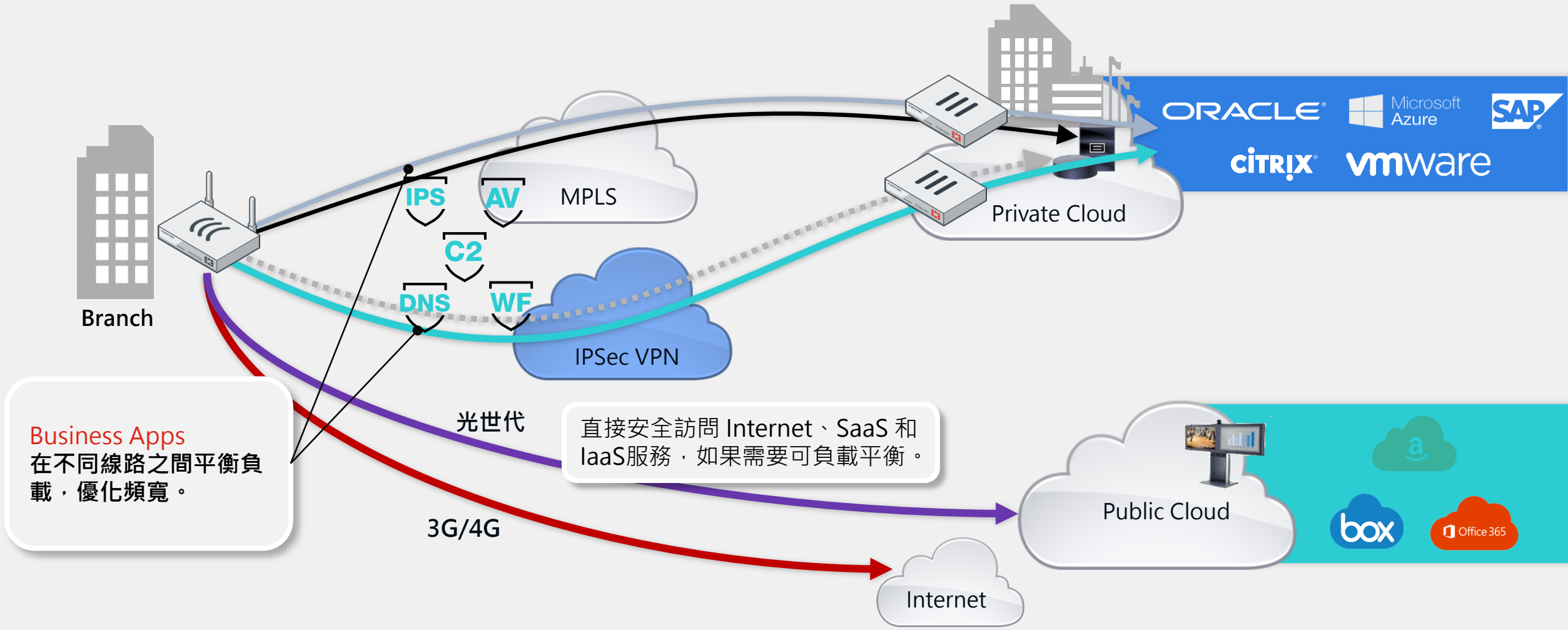
無處不在的自動化；結合NOC 和 SOC 的 SD-WAN SD-Branch 集中管理分析

99%
增加正常運行時間 降低風險

一致的安全性；架構簡化和靈活部署；面向 SASE 和 SD-Branch 的未來

2022 年 SD-WAN魔力像限中的領導者和最高執行能力

支援多樣化的線路整合



使用Mean Opinion Score (MOS)來評價語音品質

Mean Opinion Score (MOS) 質量評估並應用於 SLA 紀錄

MOS	Quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Sightly annoying
2	Poor	Annoying
1	Bad	Very annoying

(MOS) 是一種測量語音品質質量的方法，給予 0~5 的評估等級

```
config health-check
    edit "Test_MOS"
        set server "2.2.2.2"
        set sla-fail-log-period 30
        set sla-pass-log-period 30
        set members 0
        set mos-codec {g711 | g729 | g722}
        config sla
            edit 1
                set link-cost-factor mos
                set mos-threshold "4.0"
            next
        end
```

Verify the MOS calculation results (正常狀況下的測量值)

```
# diagnose sys sdwan health-check
Health Check(Test_MOS):
Seq(1 dmz): state(alive), packet-loss(0.000%) latency(0.114), jitter(0.026), mos(4.123) ...
Seq(2 port15): state(alive), packet-loss(0.000%) latency(0.100), jitter(0.008), mos(4.123) ...
```

使用Mean Opinion Score (MOS)來評價語音品質

Mean Opinion Score (MOS) 質量評估並應用於 SLA 紀錄

MOS	Quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Sightly annoying
2	Poor	Annoying
1	Bad	Very annoying

(MOS) 是一種測量語音品質質量的方法，給予 0~5 的評估等級

Increase the latency on the link in port15. port15 is out of SLA since its MOS value is now less than the 4.0. (增加 Port15 latency 導致 MOS 質量低於 4)

```
# diagnose sys sdwan health-check
Health Check(Test_MOS):
Seq(1 dmz): state(alive), packet-loss(0.000%) latency(0.106), jitter(0.022), mos(4.453) ...
Seq(2 port15): state(alive), packet-loss(0.000%) latency(300.119), jitter(0.012),
mos(3.905) ...
```

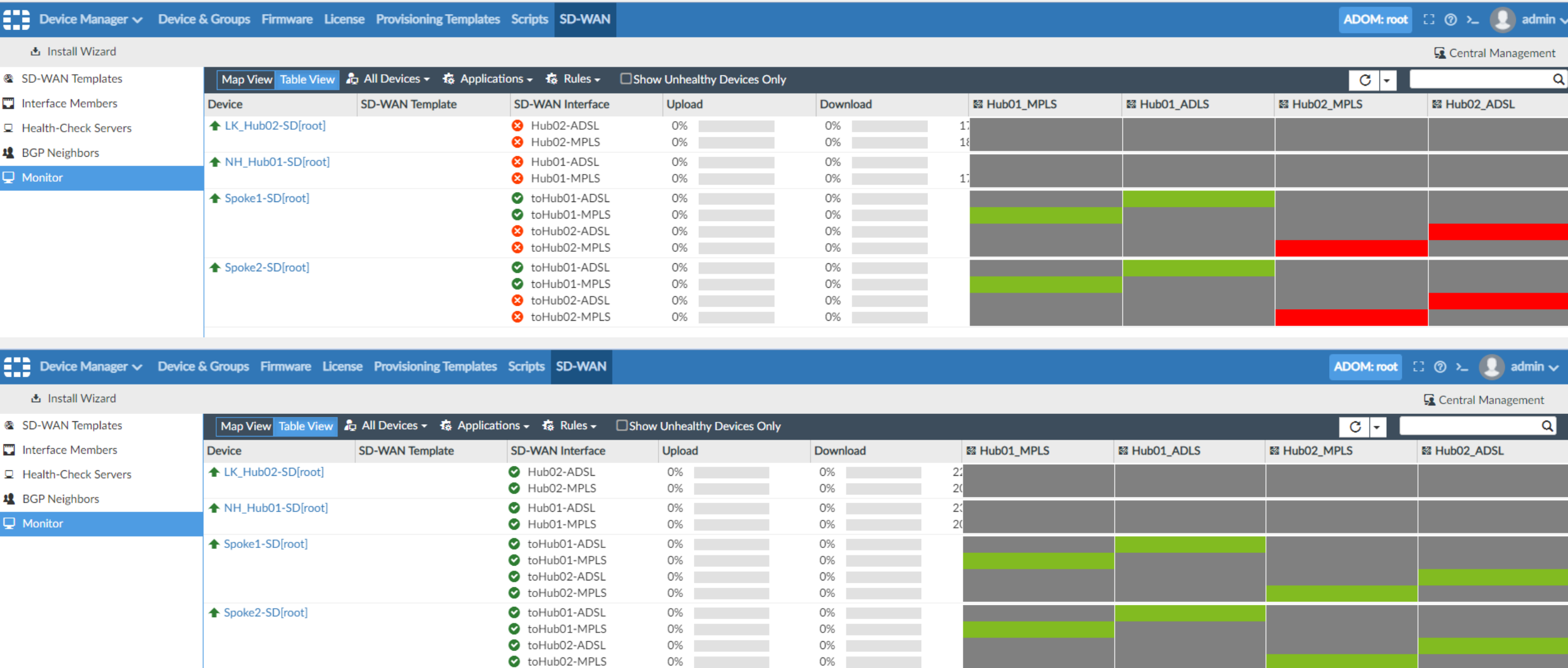
MOS value is now less than the mos-threshold (4.0) Sample logs

```
logdesc="SDWAN SLA notification" eventtype="SLA" healthcheck="Test_MOS"
slatargetid=1 interface="port15" status="up"
latency="300.118" jitter="0.013" packetloss="0.000" mos="3.905" slamap="0x0" ...
metric="mos" msg="Health Check SLA status.
SLA failed due to being over the performance metric threshold."
```

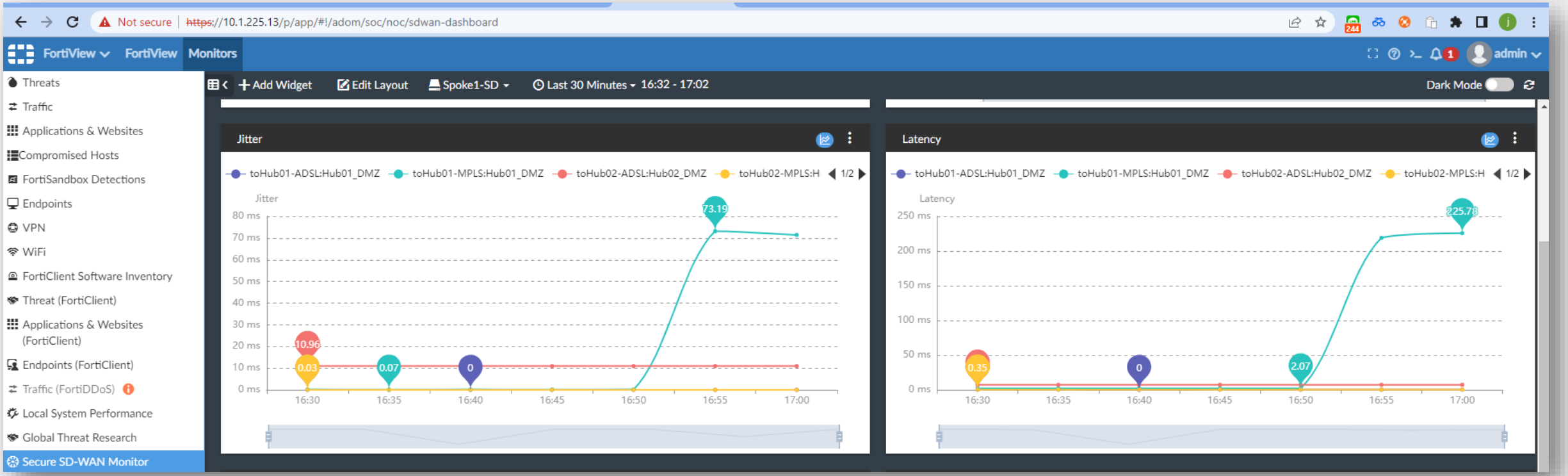
MOS value is now over the mos-threshold (4.0) Sample logs

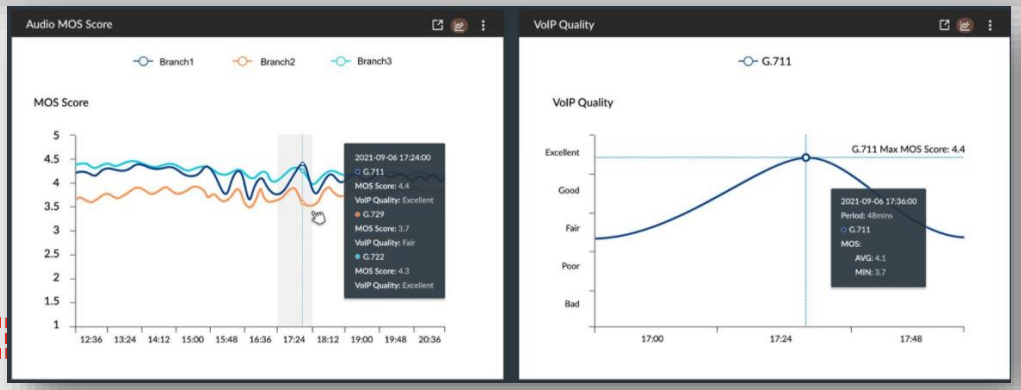
```
logdesc="SDWAN SLA notification" eventtype="SLA" healthcheck="Test_MOS"
slatargetid=1 interface="port15" status="up"
latency="0.106" jitter="0.007" packetloss="0.000" mos="4.453" slamap="0x1"  ...
Metric="mos" msg="Health Check SLA status.
```

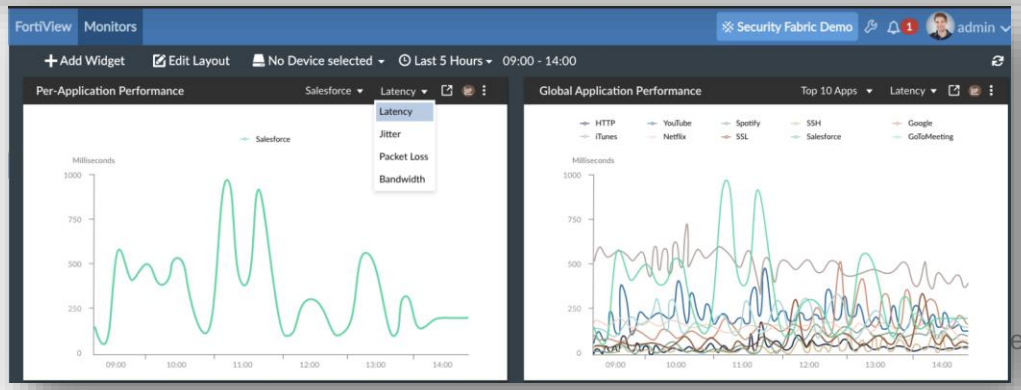
統一監看各點線路狀況


Device Manager
Device & Groups
Firmware
License
Provisioning Templates
Scripts
SD-WAN
ADOM: root
admin
Install Wizard
Central Management
SD-WAN Templates
Interface Members
Health-Check Servers
BGP Neighbors
Monitor
Map View
Table View
All Devices
Applications
Rules
Show Unhealthy Devices Only
Device
SD-WAN Template
SD-WAN Interface
Upload
Download
Hub01_MPLS
Hub01_ADLS
Hub02_MPLS
Hub02_ADSL
LK_Hub02-SD[root]
Hub02-ADSL
Hub02-MPLS
NH_Hub01-SD[root]
Hub01-ADSL
Hub01-MPLS
Spoke1-SD[root]
toHub01-ADSL
toHub01-MPLS
toHub02-ADSL
toHub02-MPLS
Spoke2-SD[root]
toHub01-ADSL
toHub01-MPLS
toHub02-ADSL
toHub02-MPLS
0%

統一監看各點線路品質

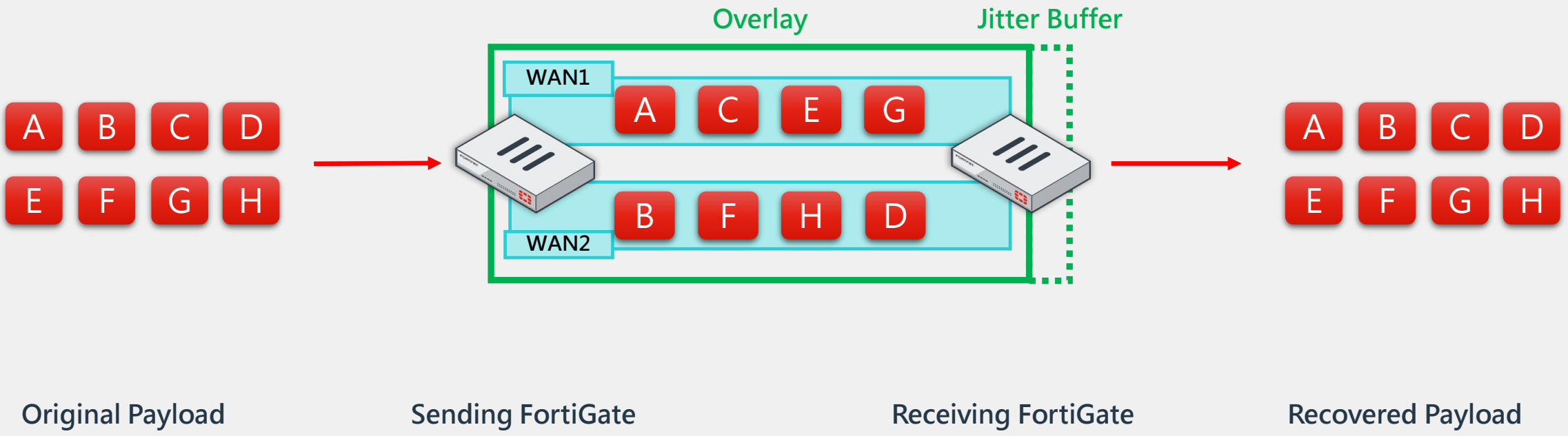

Not secure https://10.1.225.13/p/app/#!/adom/soc/noc/sdwan-dashboard
FortiView
FortiView
Monitors
admin
Threats
Traffic
Applications & Websites
Compromised Hosts
FortiSandbox Detections
Endpoints
VPN
WiFi
FortiClient Software Inventory
Threat (FortiClient)
Applications & Websites (FortiClient)
Endpoints (FortiClient)
Traffic (FortiDDoS)
Local System Performance
Global Threat Research
Secure SD-WAN Monitor
Add Widget
Edit Layout
Spoke1-SD
Last 30 Minutes 16:32 - 17:02
Dark Mode
Jitter
toHub01-ADSL:Hub01_DMZ
toHub01-MPLS:Hub01_DMZ
toHub02-ADSL:Hub02_DMZ
toHub02-MPLS:H
1/2
80 ms
70 ms
60 ms
50 ms
40 ms
30 ms
20 ms
10 ms
0 ms
10.96
0.03
0.07
0
73.19
16:30
16:35
16:40
16:45
16:50
16:55
17:00
Latency
250 ms
200 ms
150 ms
100 ms
50 ms
0 ms
0.35
0
2.07
225.78

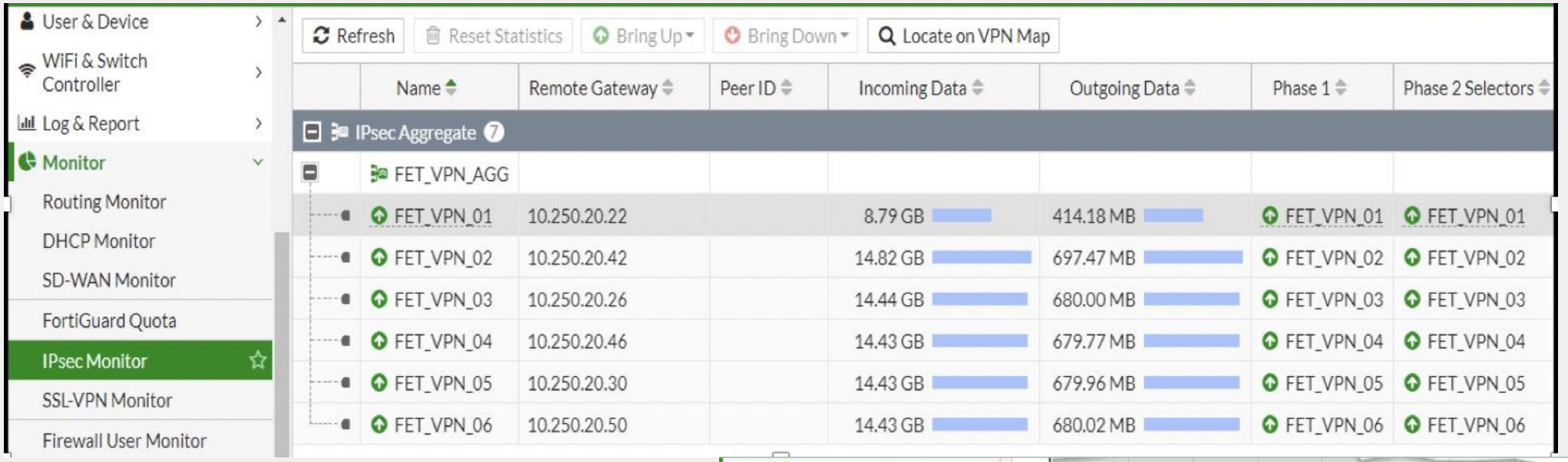

Audio MOS Score
Branch1
Branch2
Branch3
MOS Score
VoIP Quality
G.711
Excellent
Good
Fair
Poor
Bad
G.711 Max MOS Score: 4.4

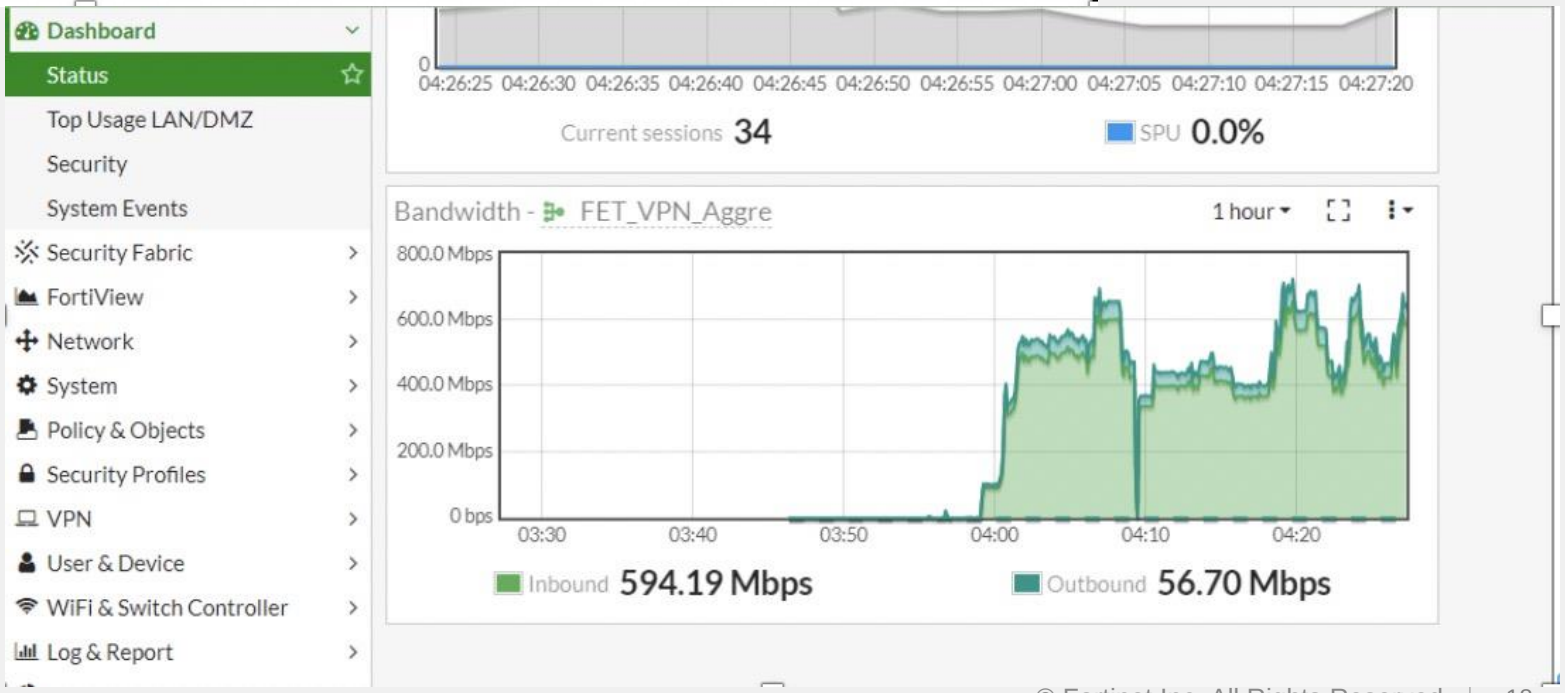

FortiView
Monitors
Security Fabric Demo
admin
Add Widget
Edit Layout
No Device selected
Last 5 Hours 09:00 - 14:00
Per-Application Performance
Salesforce
Latency
Jitter
Packet Loss
Bandwidth
Global Application Performance
Top 10 Apps
HTTP
YouTube
Spotify
SSH
Google
iTunes
Netflix
SSL
Salesforce
GoToMeeting
Milliseconds

頻寬倍增技術

Per packet WAN Path Steering







Secure SD-Branch Simplified

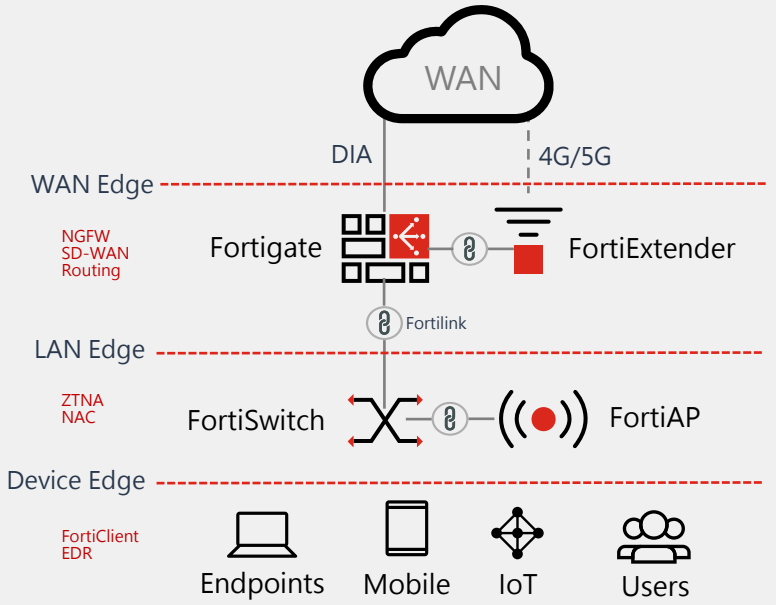
Secure SD-Branch

結合Security的簡化分佈式企業邊緣部署

SD-WAN 善用所有WAN (ADSL / 4G 5G / MPLS / IPSEC VPN) 資源，降低服務斷線風險增加正常運作時間，無需而外成本。

LAN Edge 保護邊緣設備包含有線網路無線網路，確保所有接入設備的安全性。

Secure SD-Branch Solution



Fortinet SD-Branch 解決方案和優勢

統一
單一平台、單一介面、
簡化操作

安全
NGFW檢視、NGFW可視性、
NGFW控制

自動化
加快響應速度、更主動的IT

FortiOS

Security Fabric

FortiAIOPs

輕鬆建置 Branch Office 網路環境

FortiGate ZTP (Zero touch provisioning)

設備被運送到現場並接上線。

設備通過 ZTP 或手動連接到 FMG。

FortiManager 接受設備並推送配置。

設備上線，設定和策略包同步成功。

```
========== #1, 2021-08-18 21:57:51 ==========
DC1_FGT $  exec central-mgmt register-device FMG-VMTM20009651 DC1_FG
Start Registering ...
Registering device to FMG fail
========== #2, 2021-08-18 22:02:53 ==========
DC1_FGT $  exec central-mgmt register-device FMG-VMTM20009651 DC1_FG
Start Registering ...
Registering request sent
```

Group Error Devices | Delete | View Details | Show Status | Column Settings

ID	Source	Description	User	Status	Time Used
3370	Install Configuration	Push config to device.	admin	(90%)	20s
3369	Device Manager	Add/delete Unauthorized Devices	Auto link	(60%)	30s

Edit | Delete | Import Policy | Install | More | Column Settings

Device Name	Config Status	Policy Package Status	CLI Template Status	Firmware Version	Host Name
BR1_FG	Unknown	Branch_Policy-Package		FortiGate 6.4,build1878	BR1_FG
BR2_FG	Unknown	Branch_Policy-Package		FortiGate 6.4,build1878	BR2_FG
DC1_FG	Synchronized	DCs_Policy-Package		FortiGate 6.4.6,build1879 (GA)	DC1_FG
DC2_FG	Auto-update	DCs_Policy-Package		FortiGate 6.4.6,build1879 (GA)	DC2_FG

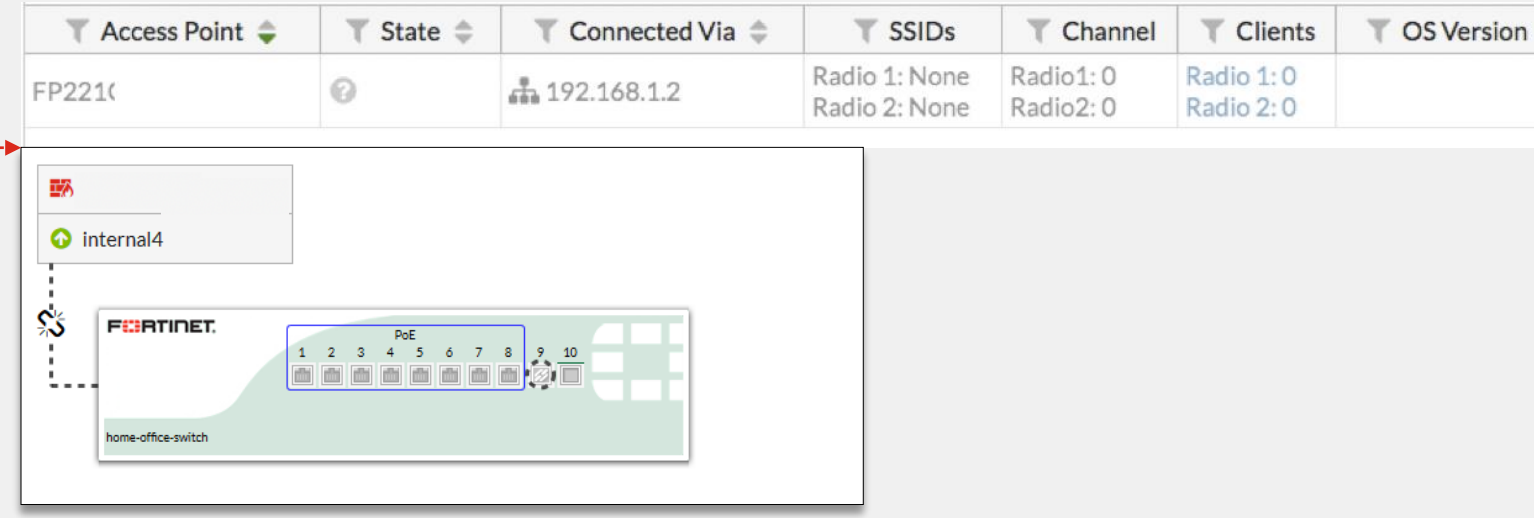
輕鬆建置 Branch Office 網路環境

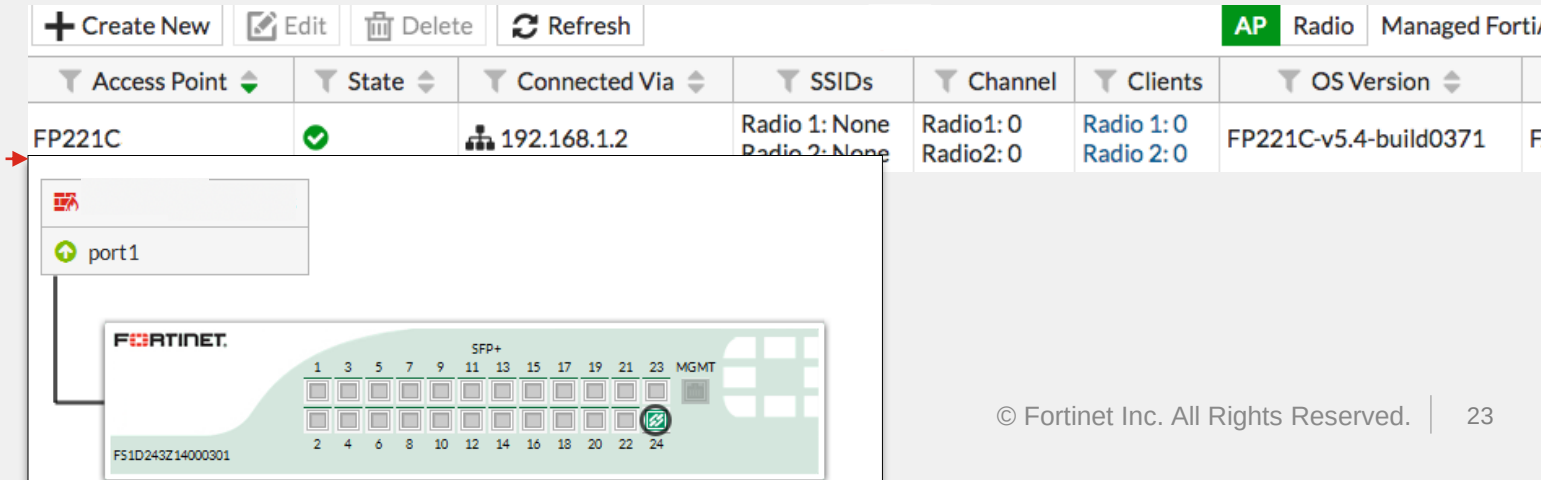
FortiSwitch FortiAP ZTP (Zero touch provisioning)

設備被運送到現場並接上線。

FortiGate偵測到設備並手動或自動註冊。

確認設備上線配置Config。

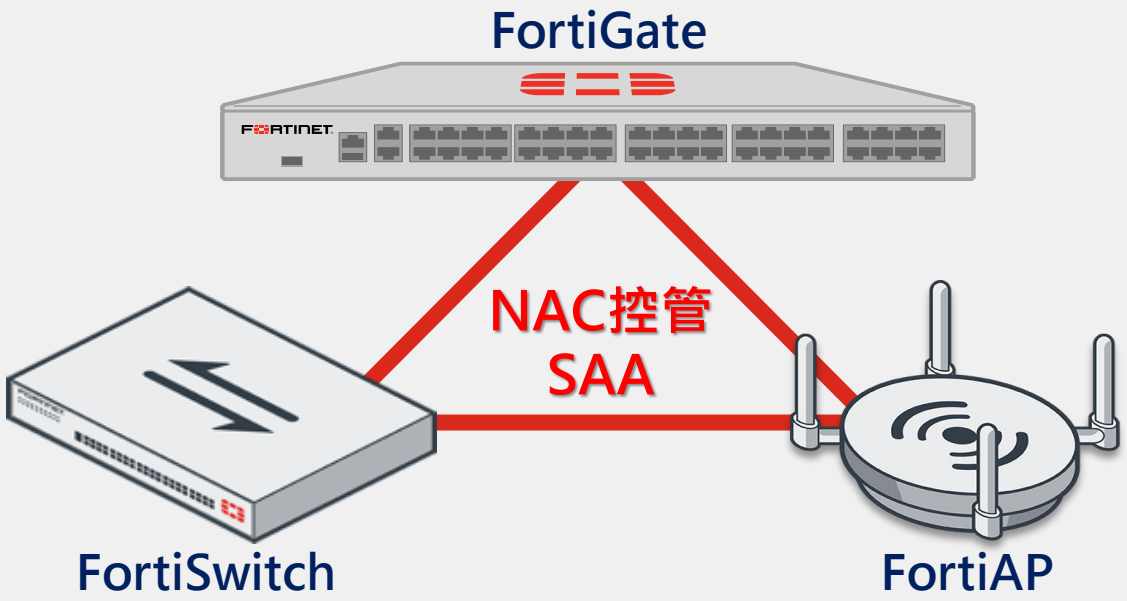




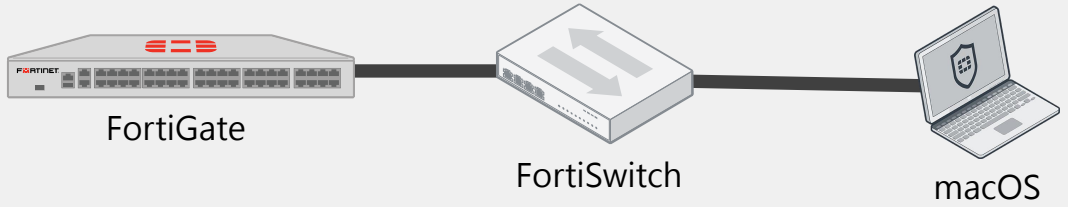
安全存取架構（Secure Access Architecture，SAA）

Fortinet推出的有線無線安全統一控管解決方案-輕鬆部署嚴謹的網路環境。

設備識別功能(NAC)，當識別到設備將給予對應的安全政策。(IOT License + FSW 可以辦識千種設備)



範例：
FortiGate中配置FortiSwitch使用NAC策略(MAC OS)，
偵測到MAC OS上線將分配符合MAC OS的安全政策至該介面



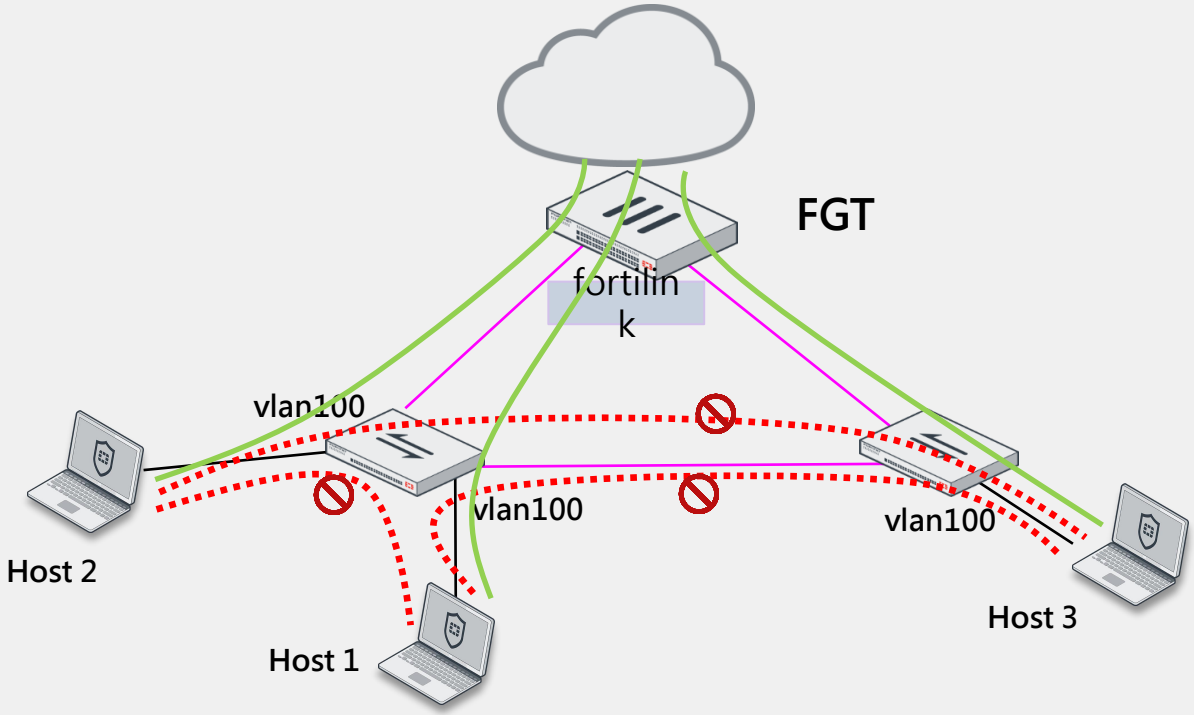
其餘功能：

- 全面性的內外網防護
- 智能單一管理系統
- 容易部署、彈性擴充
- 網路資安等資訊高可視性
- 自動產生拓撲圖/自動修正錯誤連接

阻隔同網段的流量

可讓同網段使用者不能互通,防止橫向感染

- 一鍵開啟 " block intra-vlan traffic " 阻隔同網段的流量
- 同網段PC無法看到彼此
- PC流量只能送到FortiGate
- 若PC間有特殊需求要能互相傳送資料,
  可以在FortiGate上設定防火牆政策允許



FortiSwitch Port-to-Port Policy

在FortiGate上設定防火牆政策允許同網段流量

C:\Users\Jarvis>arp -a

介面: 192.168.228.1 --- 0x8

網際網路網址	實體位址	類型
192.168.228.255	ff-ff-ff-ff-ff-ff	靜態
224.0.0.2	01-00-5e-00-00-02	靜態
224.0.0.22	01-00-5e-00-00-16	靜態
224.0.0.251	01-00-5e-00-00-fb	靜態
224.0.0.252	01-00-5e-00-00-fc	靜態
239.255.255.250	01-00-5e-7f-ff-fa	靜態
255.255.255.255	ff-ff-ff-ff-ff-ff	靜態

介面: 192.168.100.2 --- 0xa

網際網路網址	實體位址	類型
192.168.100.1	90-6c-ac-16-24-b6	動態
192.168.100.254	90-6c-ac-16-24-b6	動態
192.168.100.255	ff-ff-ff-ff-ff-ff	靜態
224.0.0.2	01-00-5e-00-00-02	靜態
224.0.0.22	01-00-5e-00-00-16	靜態
224.0.0.251	01-00-5e-00-00-fb	靜態
224.0.0.252	01-00-5e-00-00-fc	靜態
239.255.255.250	01-00-5e-7f-ff-fa	靜態
255.255.255.255	ff-ff-ff-ff-ff-ff	靜態

C:\WINDOWS\system32>arp -a

介面: 192.168.228.1 --- 0x8

網際網路網址	實體位址	類型
192.168.228.255	ff-ff-ff-ff-ff-ff	靜態
224.0.0.22	01-00-5e-00-00-16	靜態

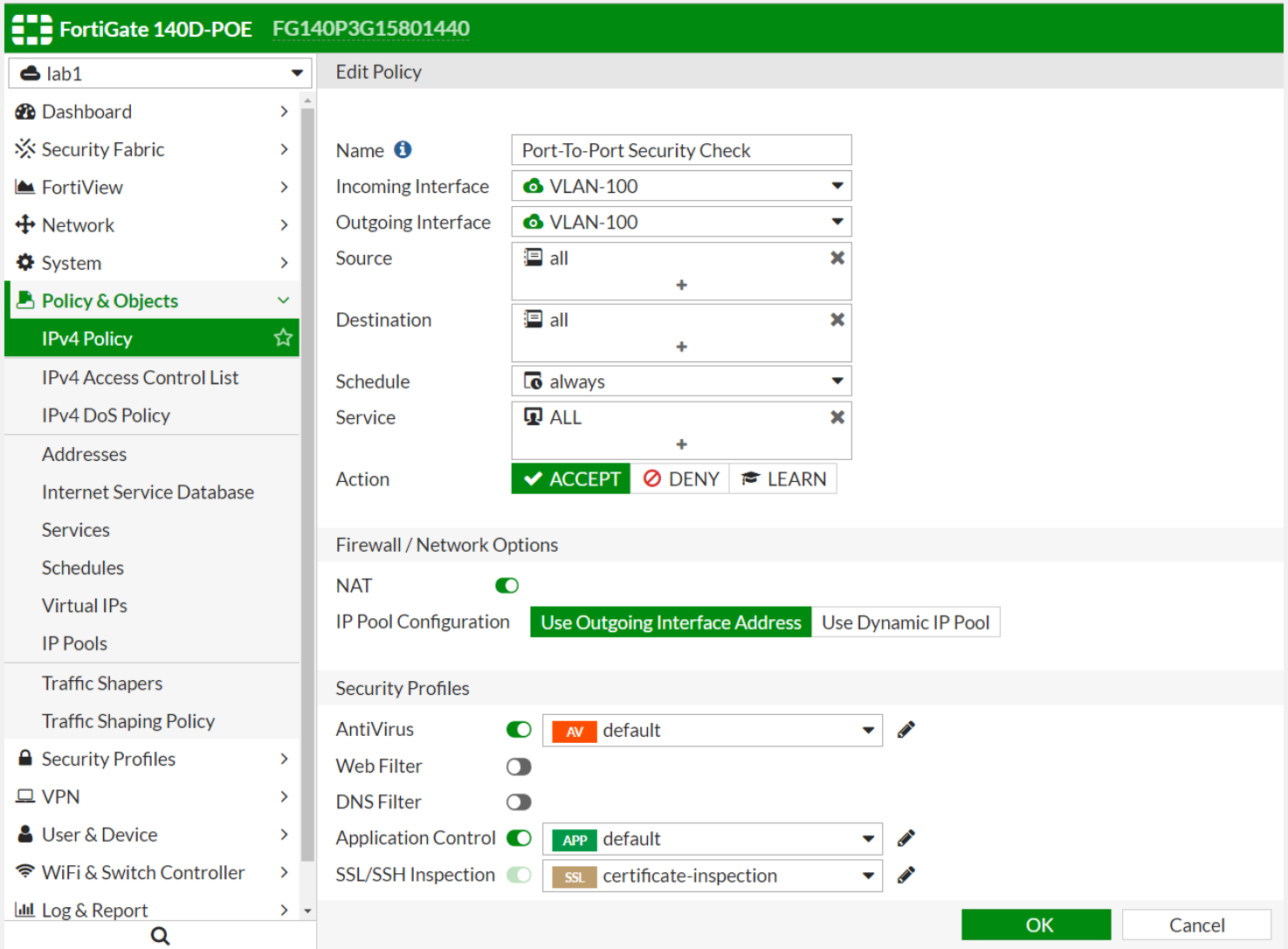
介面: 192.168.100.2 --- 0xa

網際網路網址	實體位址	類型
192.168.100.1	00-26-22-98-a0-9e	動態
192.168.100.254	90-6c-ac-16-24-b6	動態
192.168.100.255	ff-ff-ff-ff-ff-ff	靜態
224.0.0.22	01-00-5e-00-00-16	靜態

C:\WINDOWS\system32>

FortiSwitch Port-to-Port Policy

在FortiGate上設定防火牆政策允許同網段流量

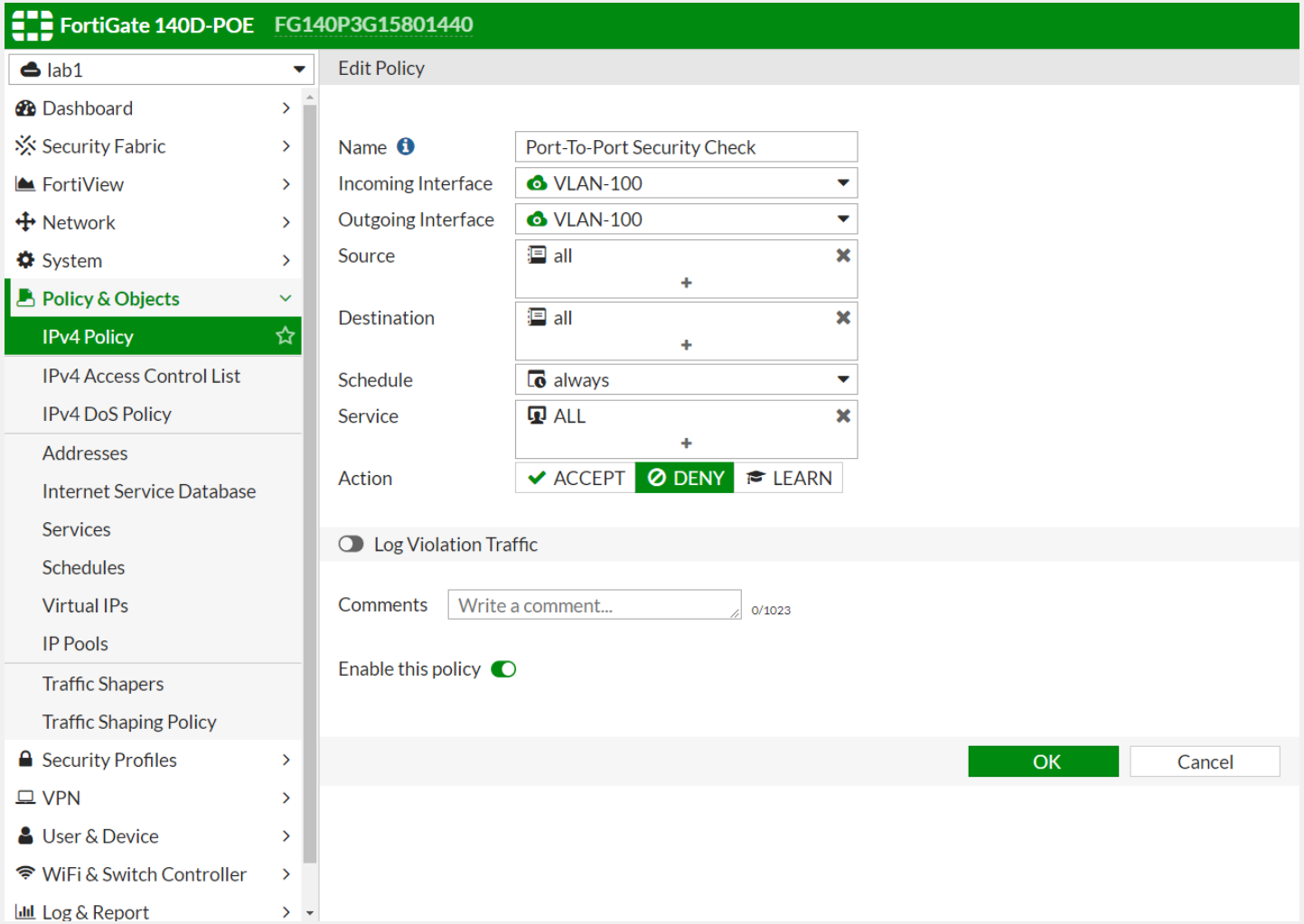



```
C:\Users\Jarvis>ping 192.168.100.1 -t

Ping 192.168.100.1 (使用 32 位元組的資料):
回覆自 192.168.100.1: 位元組=32 時間<1ms TTL=127
回覆自 192.168.100.1: 位元組=32 時間<1ms TTL=127
回覆自 192.168.100.1: 位元組=32 時間<1ms TTL=127
回覆自 192.168.100.1: 位元組=32 時間<1ms TTL=127
回覆自 192.168.100.1: 位元組=32 時間<1ms TTL=127
回覆自 192.168.100.1: 位元組=32 時間<1ms TTL=127
回覆自 192.168.100.1: 位元組=32 時間<1ms TTL=127
回覆自 192.168.100.1: 位元組=32 時間<1ms TTL=127
回覆自 192.168.100.1: 位元組=32 時間<1ms TTL=127
```

FortiSwitch Port-to-Port Policy

在FortiGate上設定防火牆政策允許同網段流量



192.168.100.1 的 Ping 統計資料:
　封包: 已傳送 = 312，已收到 = 296, 已遺失 = 16 (5% 遺失)，
大約的來回時間 (毫秒):
　最小值 = 0ms，最大值 = 166ms，平均 = 0ms
Control-C
^C
C:\Users\Jarvis>ping 192.168.100.1 -t

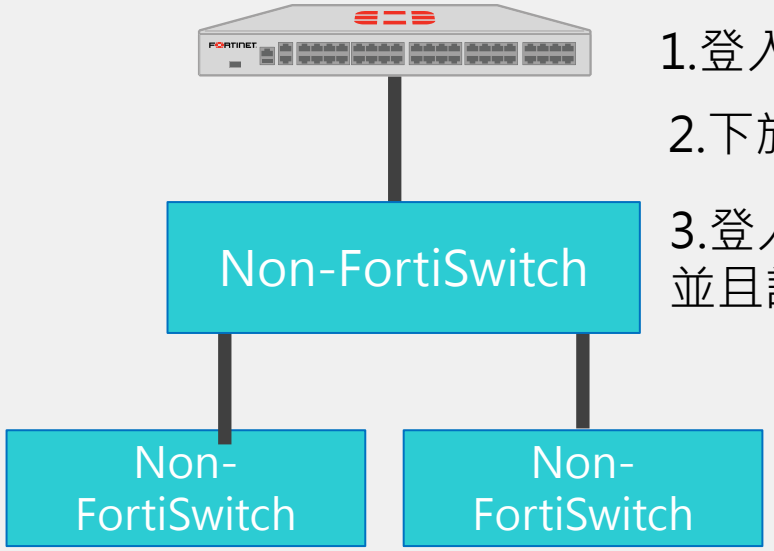
Ping 192.168.100.1 (使用 32 位元組的資料):
要求等候逾時。
要求等候逾時。
要求等候逾時。
要求等候逾時。

關於新增VLAN那件事

Switch Controller – 防火牆就是你的控制器

傳統方式

4.登入Firewall新增Policy



1.登入Edge Switch新增VLAN

2.下放VLAN到指定的介面

3.登入Core Switch新增VLAN
並且設定UPLINK允許VLAN通過

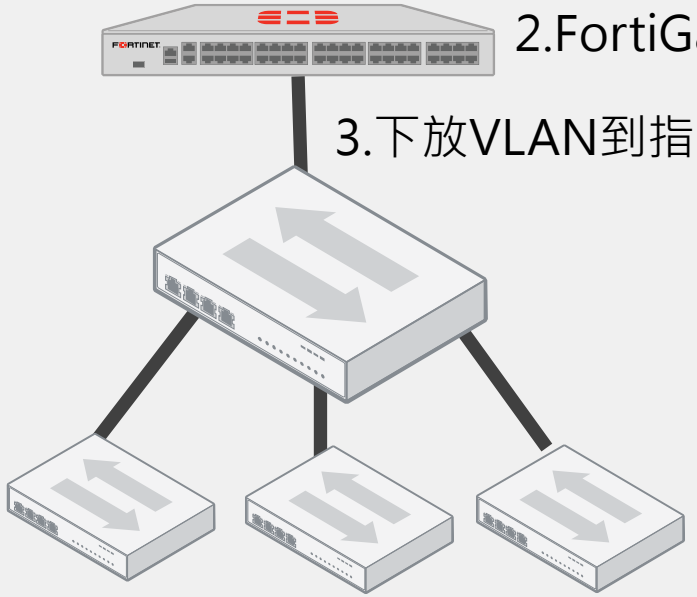
要設定的設備多步驟繁雜

Fortinet資安鐵三角

1.登入FortiGate新增VLAN

2.FortiGate新增Policy

3.下放VLAN到指定的FSW介面



三步驟統一在FortiGate操作

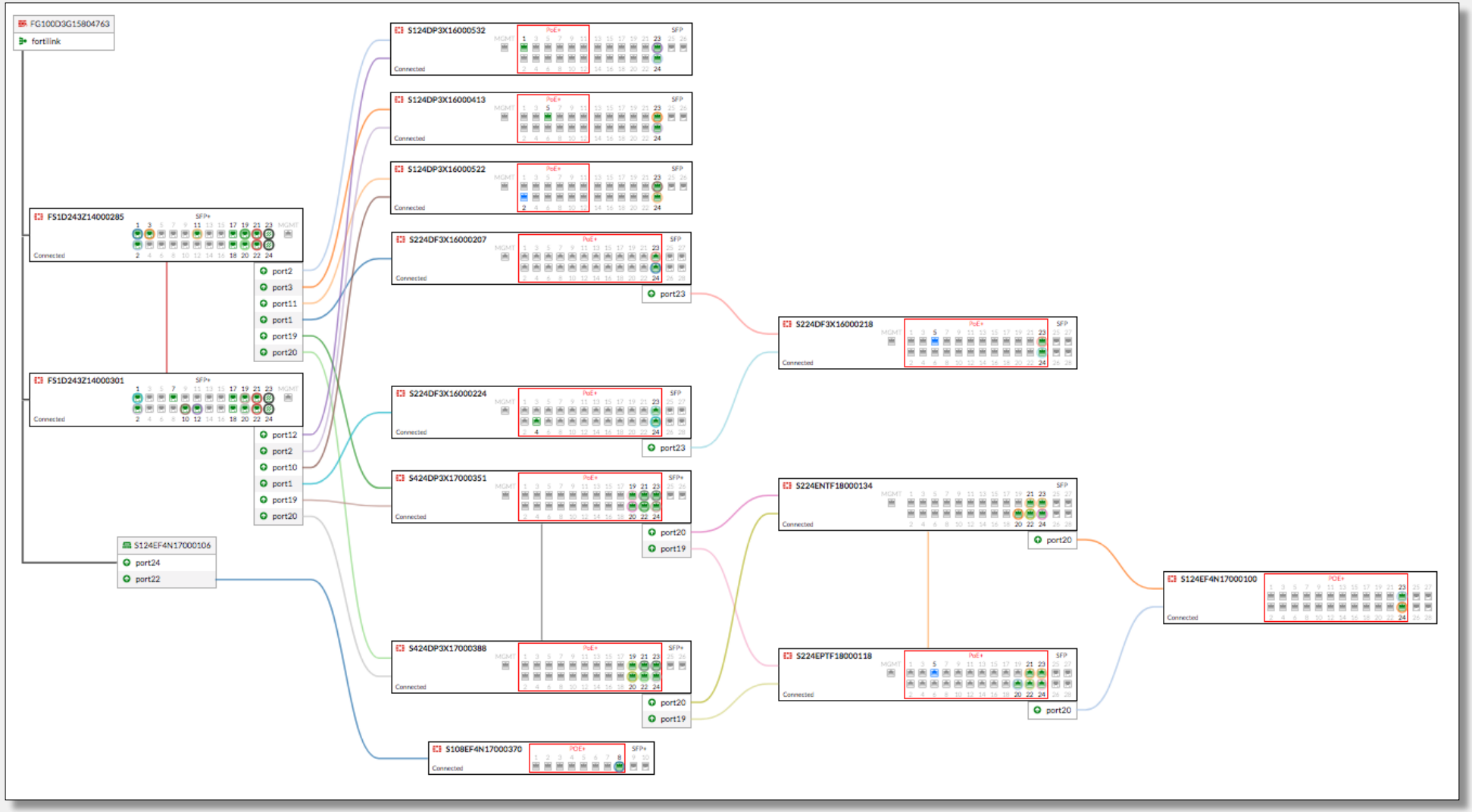
關於新增SSID那件事

AP Controller – 防火牆就是你的控制器

輕鬆建置無線環境 - FAP 五部曲

自動產生拓撲圖

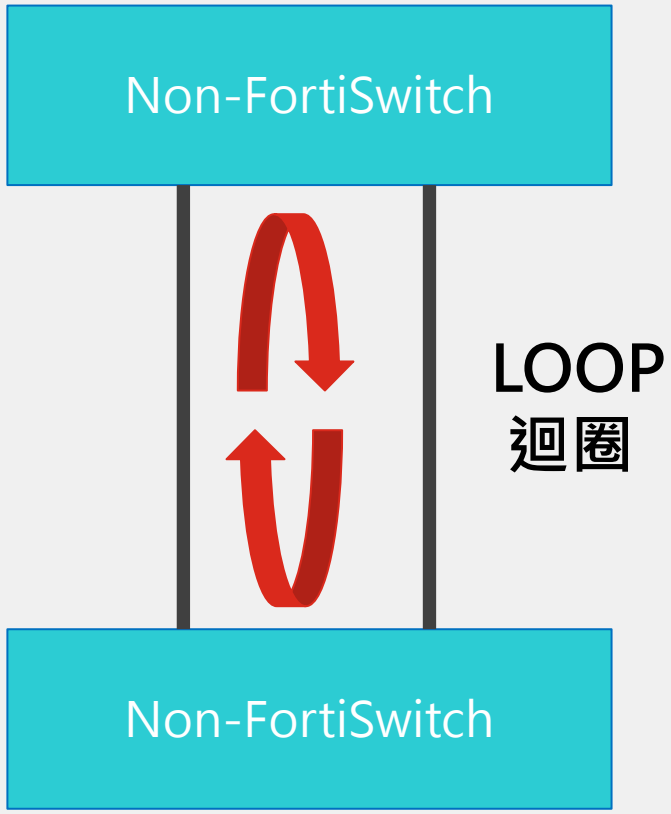
一個畫面看清所有FSW介接狀況 (自動產生)



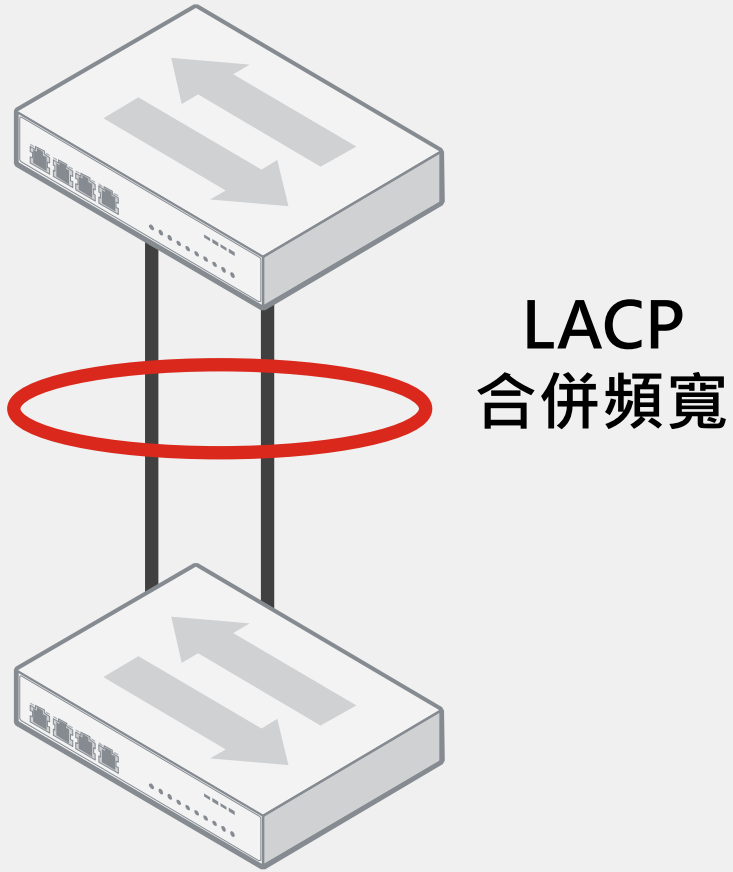
自動修正錯誤連接

再也不用擔心接錯線路導致服務異常

傳統架構

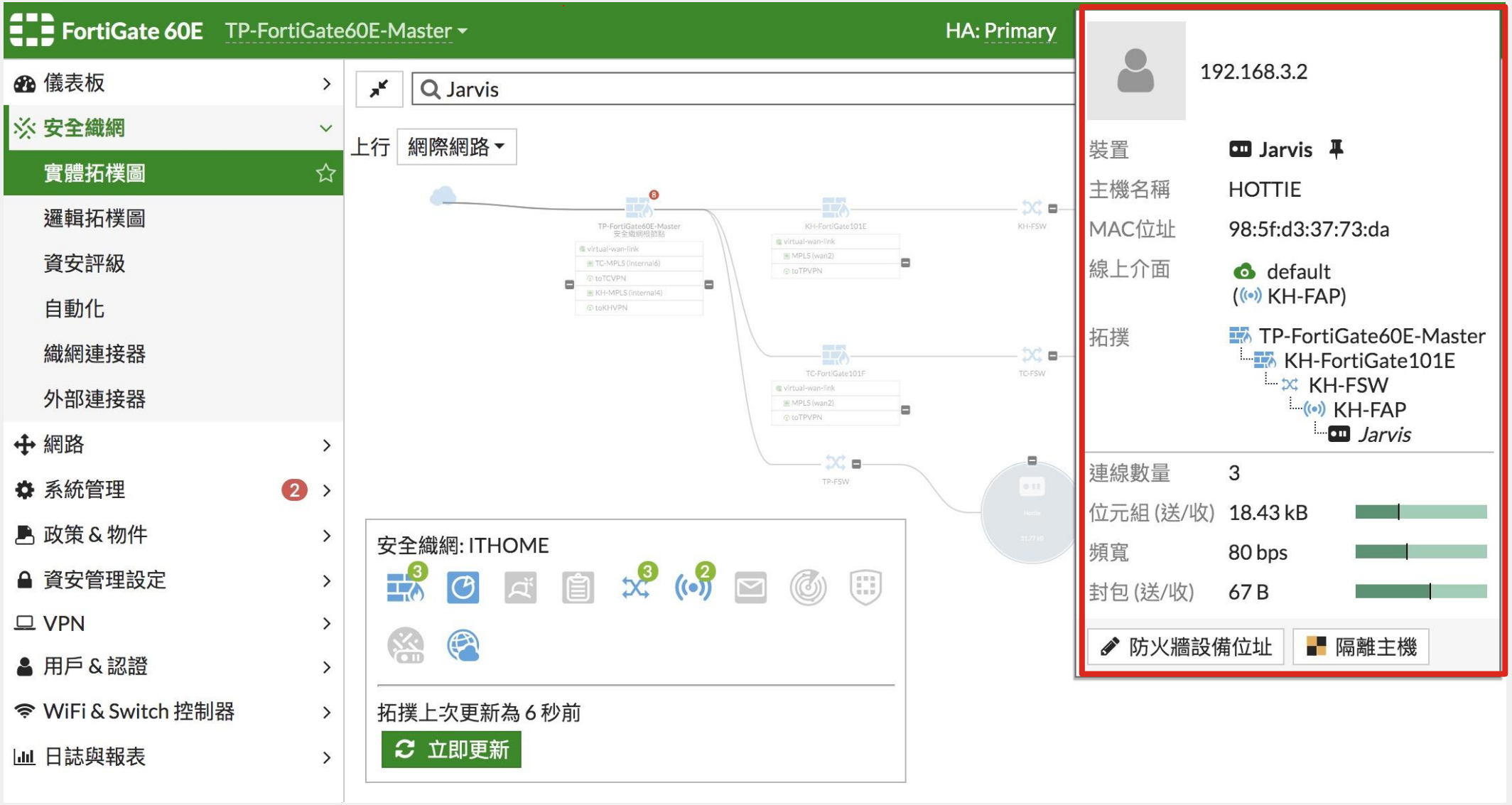


Fortinet資安鐵三角



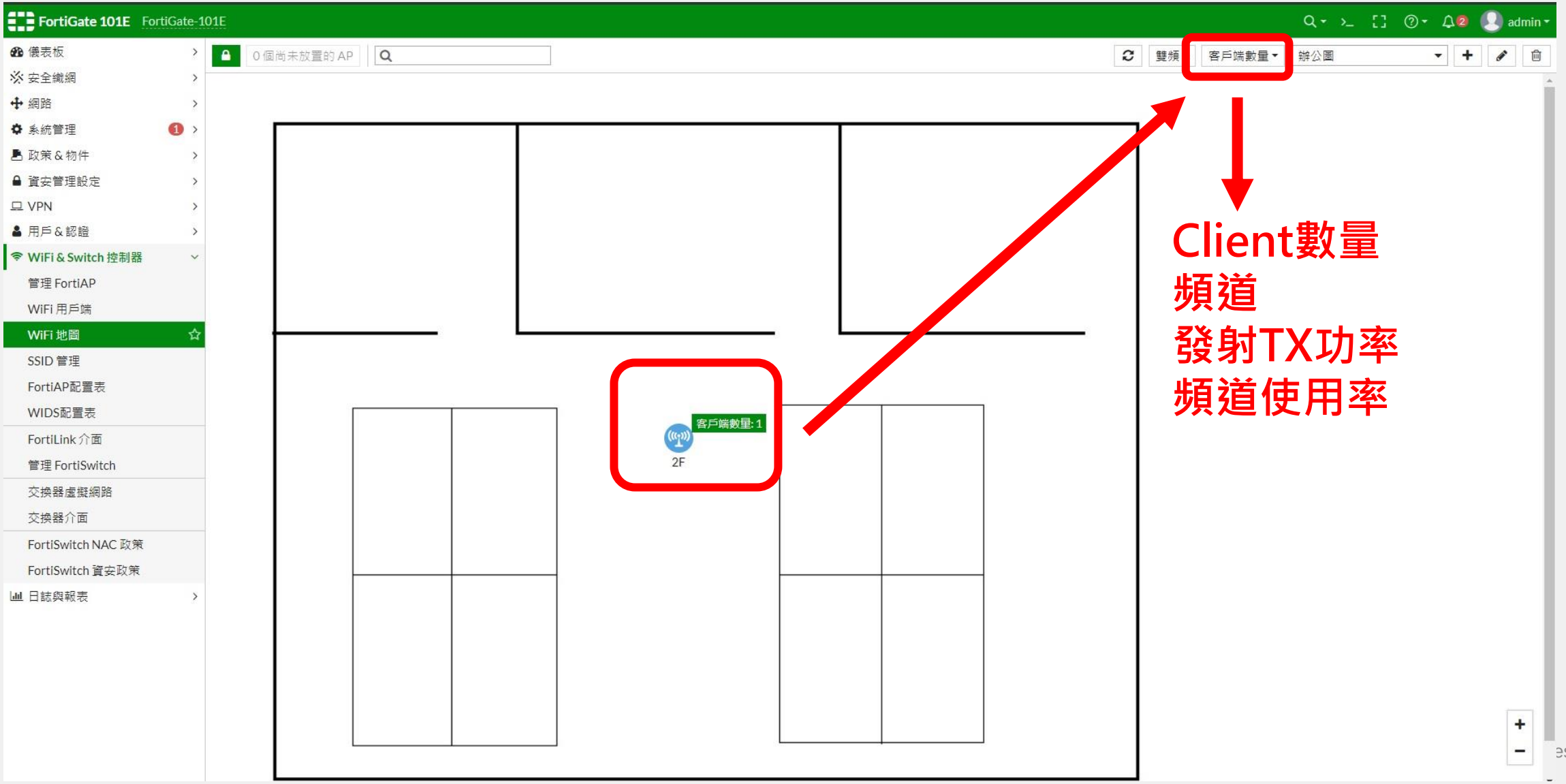
Network Topography

實體拓撲圖 - 輕鬆檢視網路狀態　包含查看使用者狀態 (例：輸入使用者名稱 Jarvis)



FortiAP - WIFI地圖

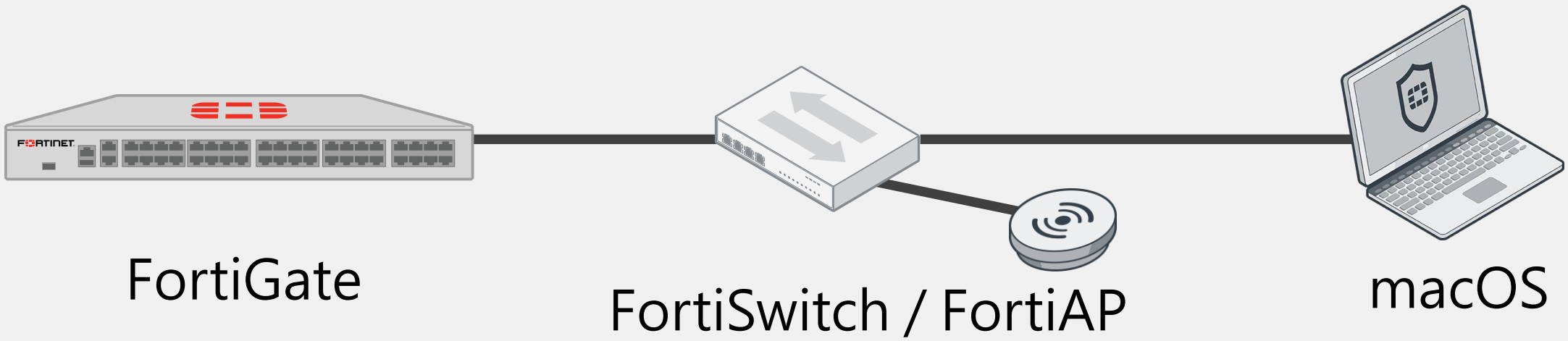
再也不用擔心忘記AP身在何處



FortiSwitch / FortiAP - 關於NAC那件事

支援設備識別功能，當識別到設備將給予對應的安全政策。
可額外購買FortiGuard License擴增設備辨識度。

範例：
FortiGate中配置FortiSwitch使用NAC策略(MAC OS)，
偵測到MAC OS上線將分配符合MAC OS的安全政策至該介面。



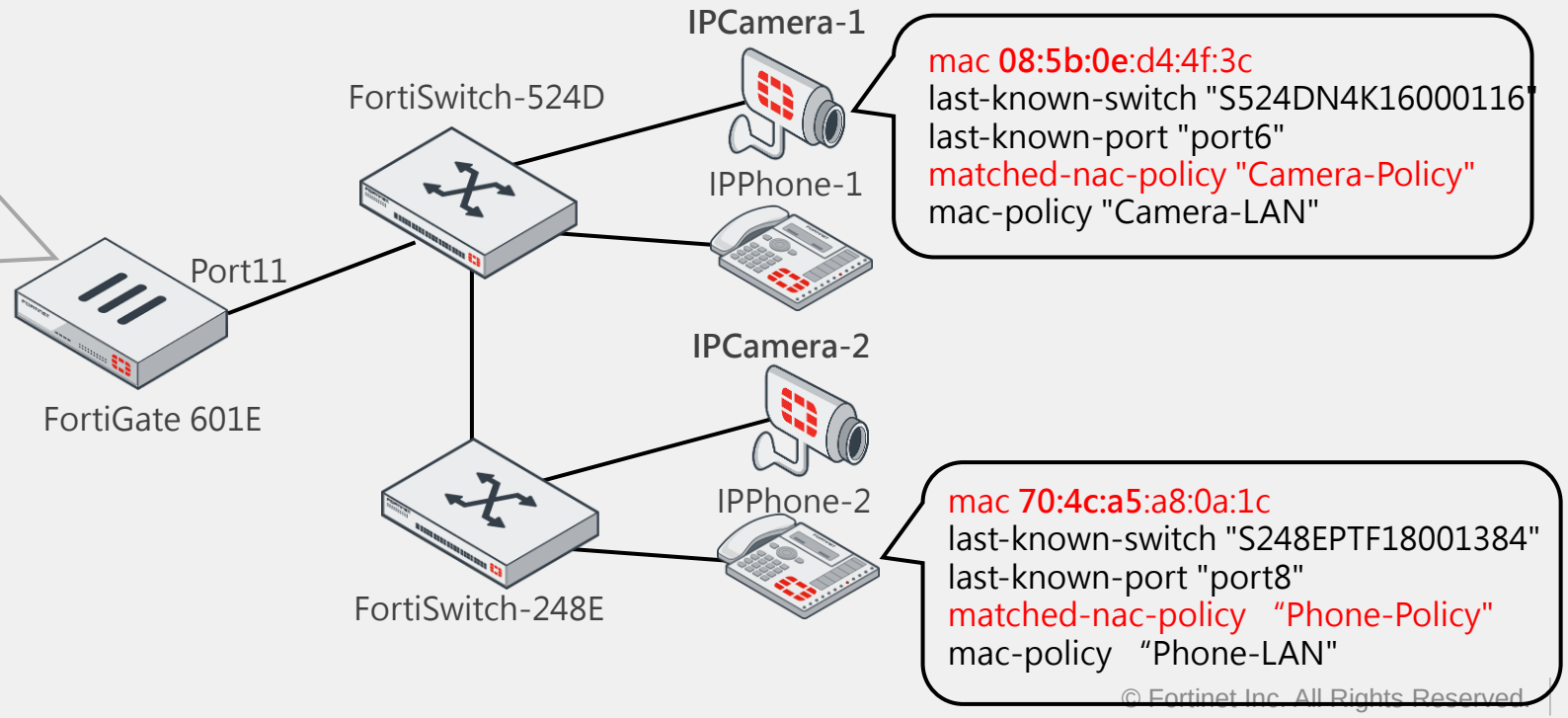
FortiSwitch / FortiAP - 關於NAC那件事

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
```



FortiSwitch / FortiAP - 關於設備壞掉那件事

更換設備三部曲

1.取消舊有設備在FortiGate上的授權

2.下達指令將新設備取代舊有設備。

execute replace-device fortiswitch <Old-Switch-S/N> <New-Switch-S/N>

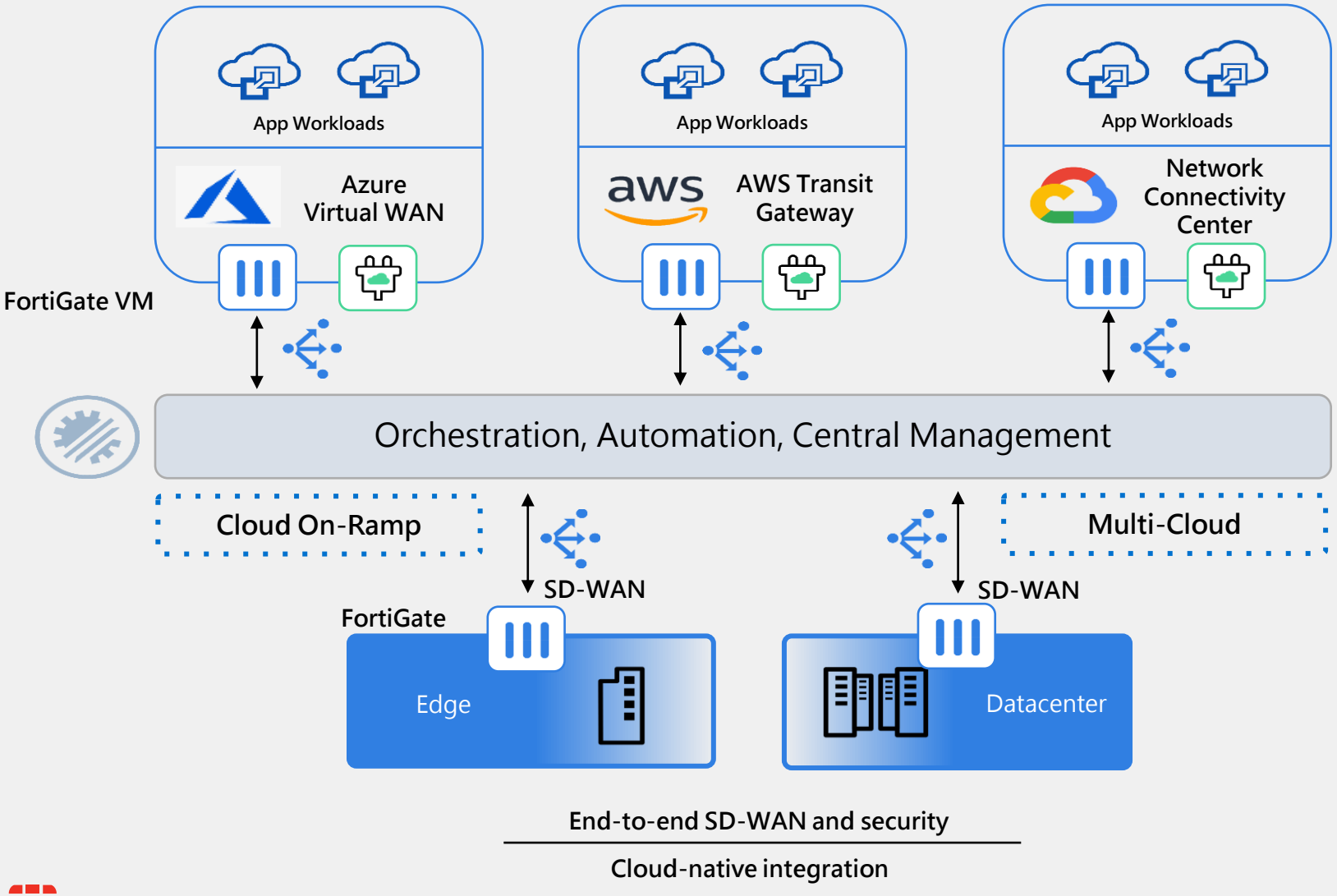
成功後會出現以下訊息：

Existing switch <Old-FortiSwitch-S/N> is replaced by new switch <New-FortiSwitch-S/N>

3.將新來的設備接上可以通往FortiGate的網路線。(光纖Port or 最後兩個UDP Port)

Multi-cloud SD-WAN

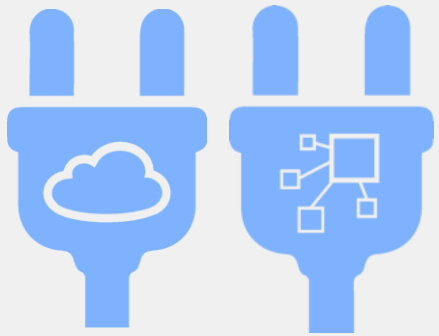
適用於混合雲和多雲的 Fortinet 安全 SD-WAN

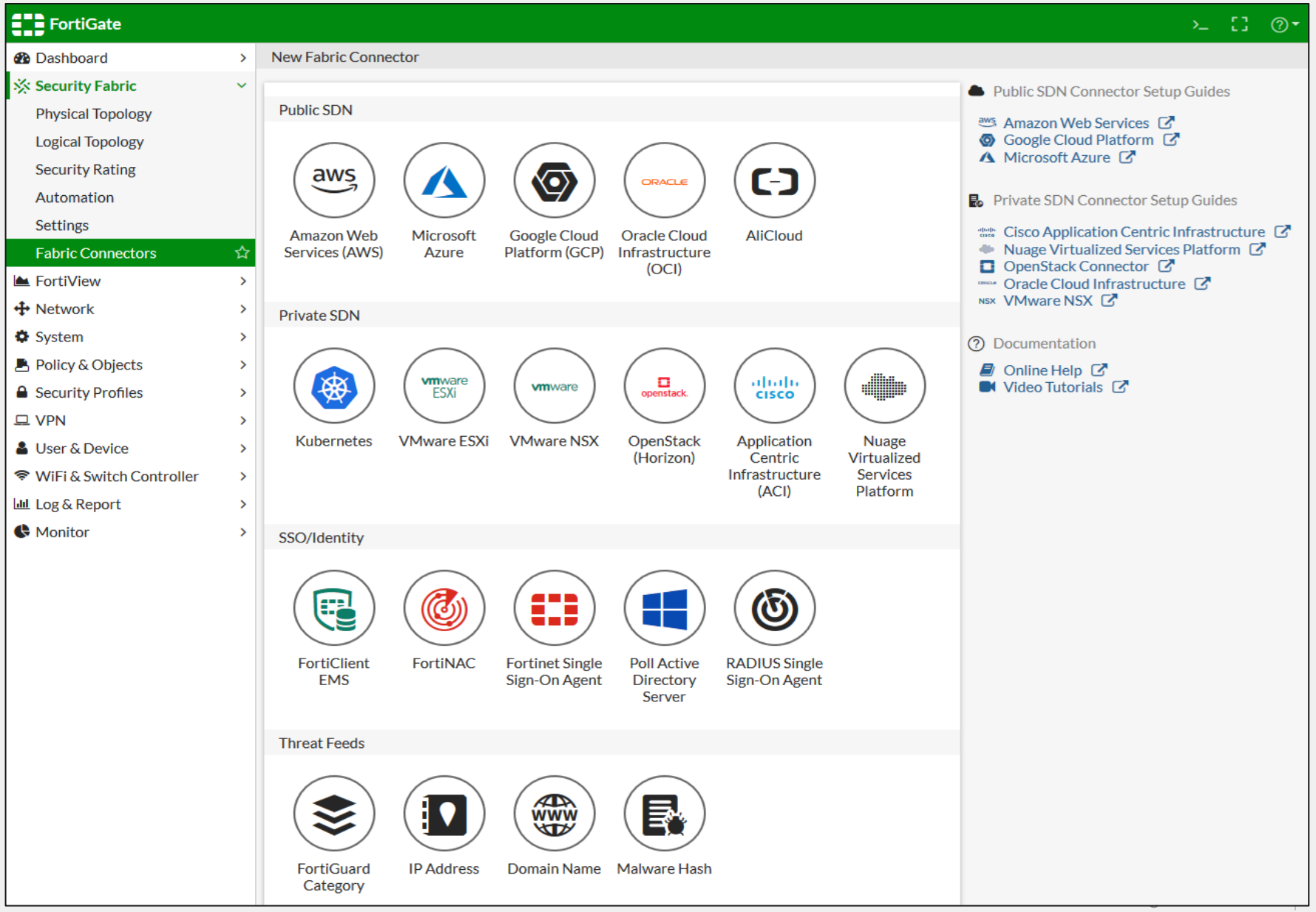


- 單一的網路以及安全操作系統
- 一致的UI,用於創建/驗證/控管應用程序以及用戶流量過濾
- 詳細的日誌紀錄
- 整體Security fabric精細的可視性

Fabric Connectors

- 雲環境屬性的更改在 Security Fabric 中自動更新。
- 使用 SDN 連接器來創建基於雲環境，提供動態訪問控制的策略。
- 每當雲環境發生變化時，無需手動重新配置地址和策略。





How Fortinet's ZTNA benefits from SD-WAN

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)

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)

- 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

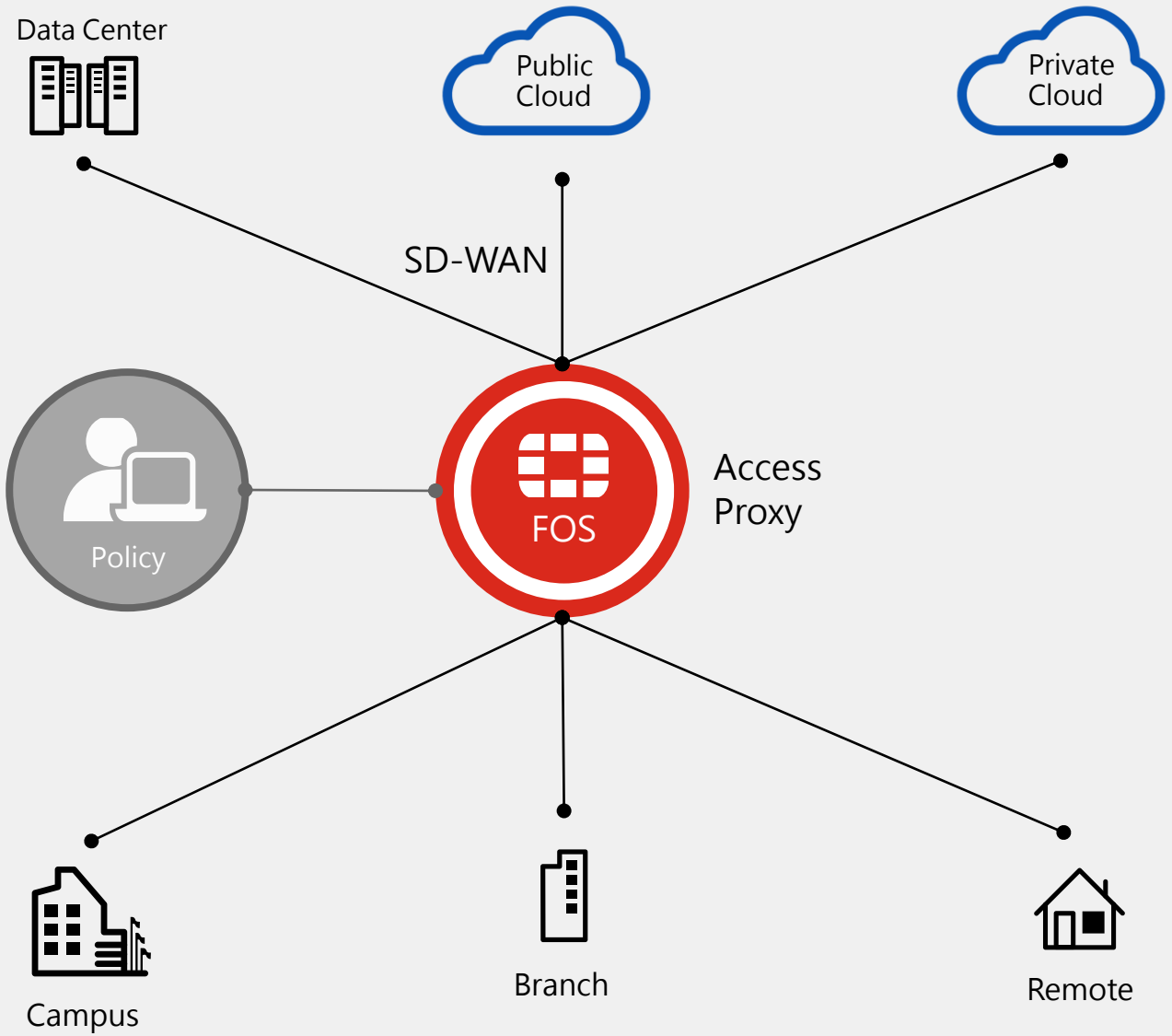
專注於安全提升的（“Secure ZTNA”）

- 完整的WFA，延展 FGT 防護至任何地方
- 存取流量穿越業界領導品牌 FortiGate 資安防護技術
- 提供 FortiGuard Labs services

資安完整覆蓋

- 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

ZTNA 架構

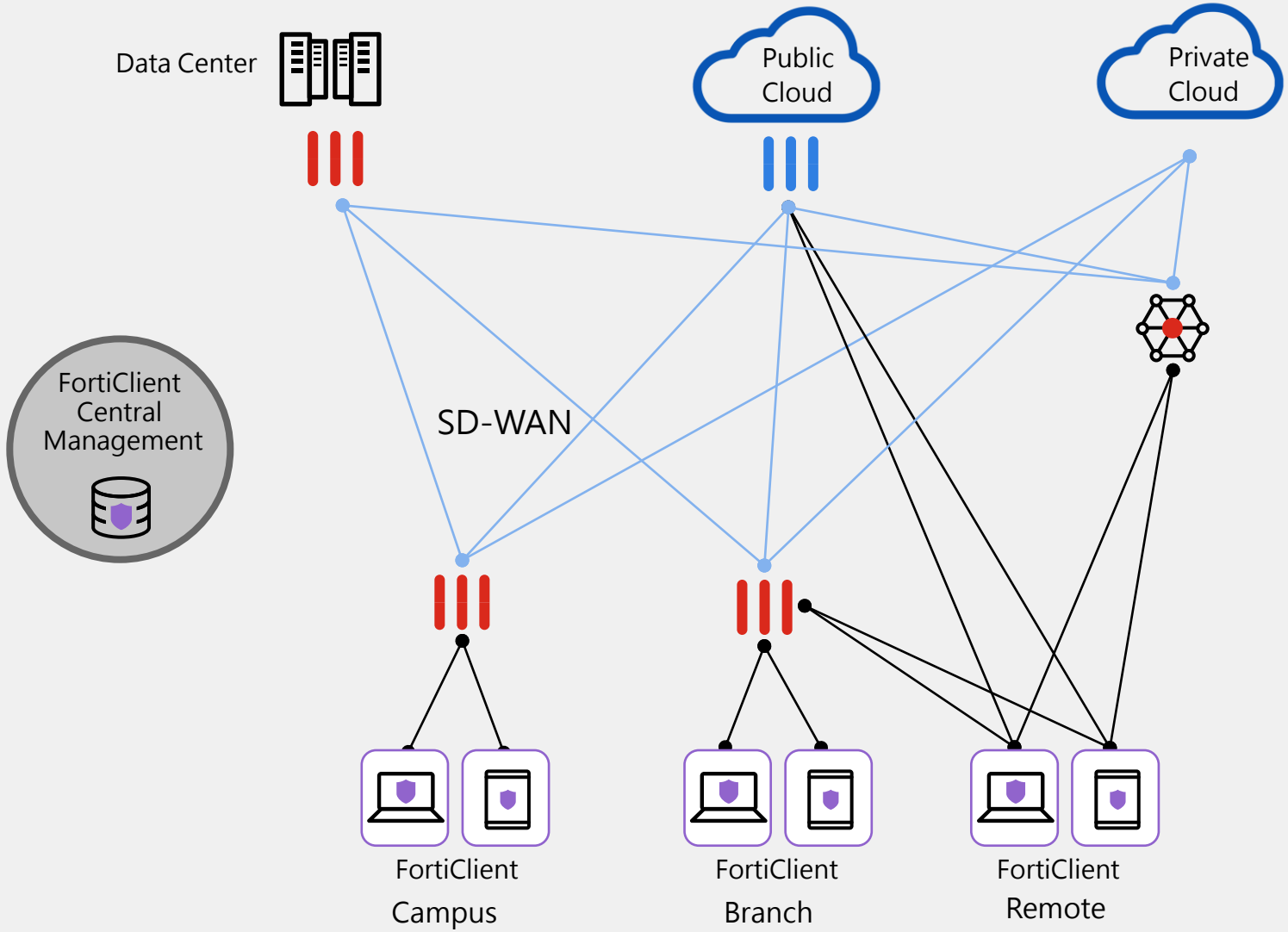


無論應用程式在哪裡

在訪問之前驗證用戶身份以及設備狀態

無論你身在何處

ZTNA + SDWAN 架構

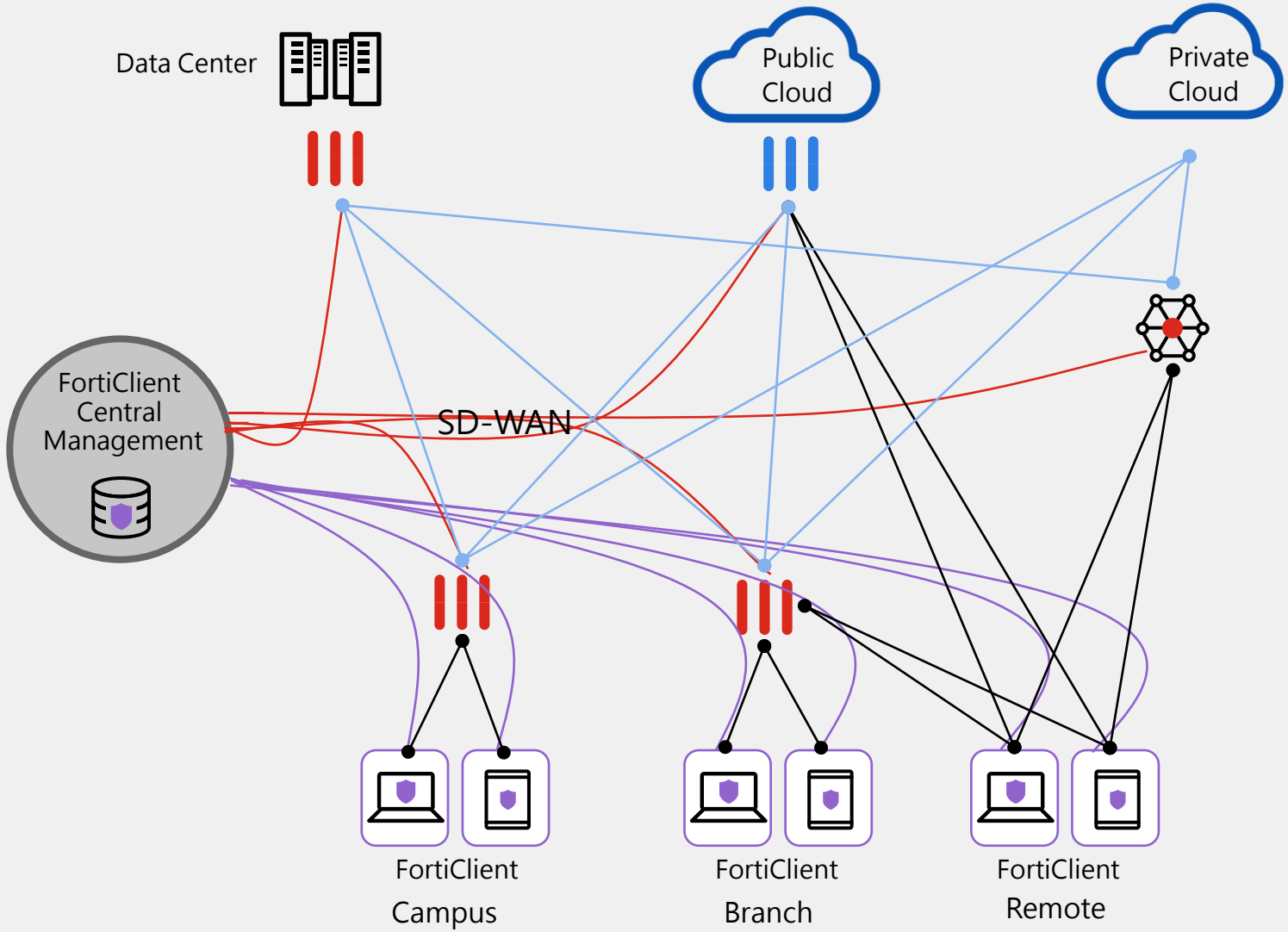


利用現有的設備(FortiGate)做基礎的設施

持續驗證永不信任

開啟ZTNA安全隧道(HTTPS / SSH) 等

ZTNA + SDWAN 運作過程



ZTNA Telemetry

Fabric Sync

Tunnel & Posture Check

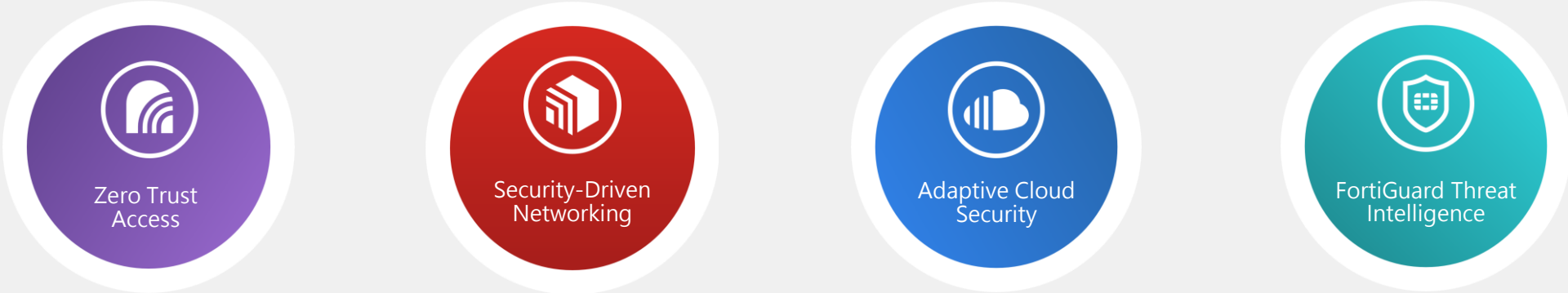
Access

關鍵要點

安全性 – 從核心企業網路到分支機構，再到雲端或家裡辦公，你的整個環境都是安全的。

簡單 – 簡單的部署/管理/License確保服務的最大效率。

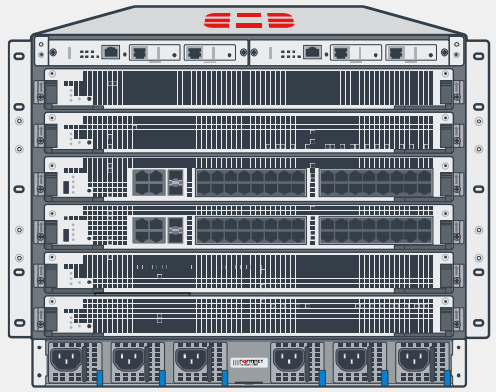
低成本 – 一個好的解決方案不應該有過高的成本。Security SD-WAN / Security SD-Branch / ZTNA 以FortiGate的核心功能為基礎保護整個數位轉型環境，為你提供最佳的投資回報率。



你的FortiGate不再只是一台NGFW

Security Fabric Brain

ZTNA Access Proxy



Switch Controller

應用程式導向的 SD-WAN分流

AP Controller


FORTINET