FORTINET

資安新境遇 –
Fortinet讓校園擁有毫不妥協的安全防護

Jarvis Lee 李尚峰

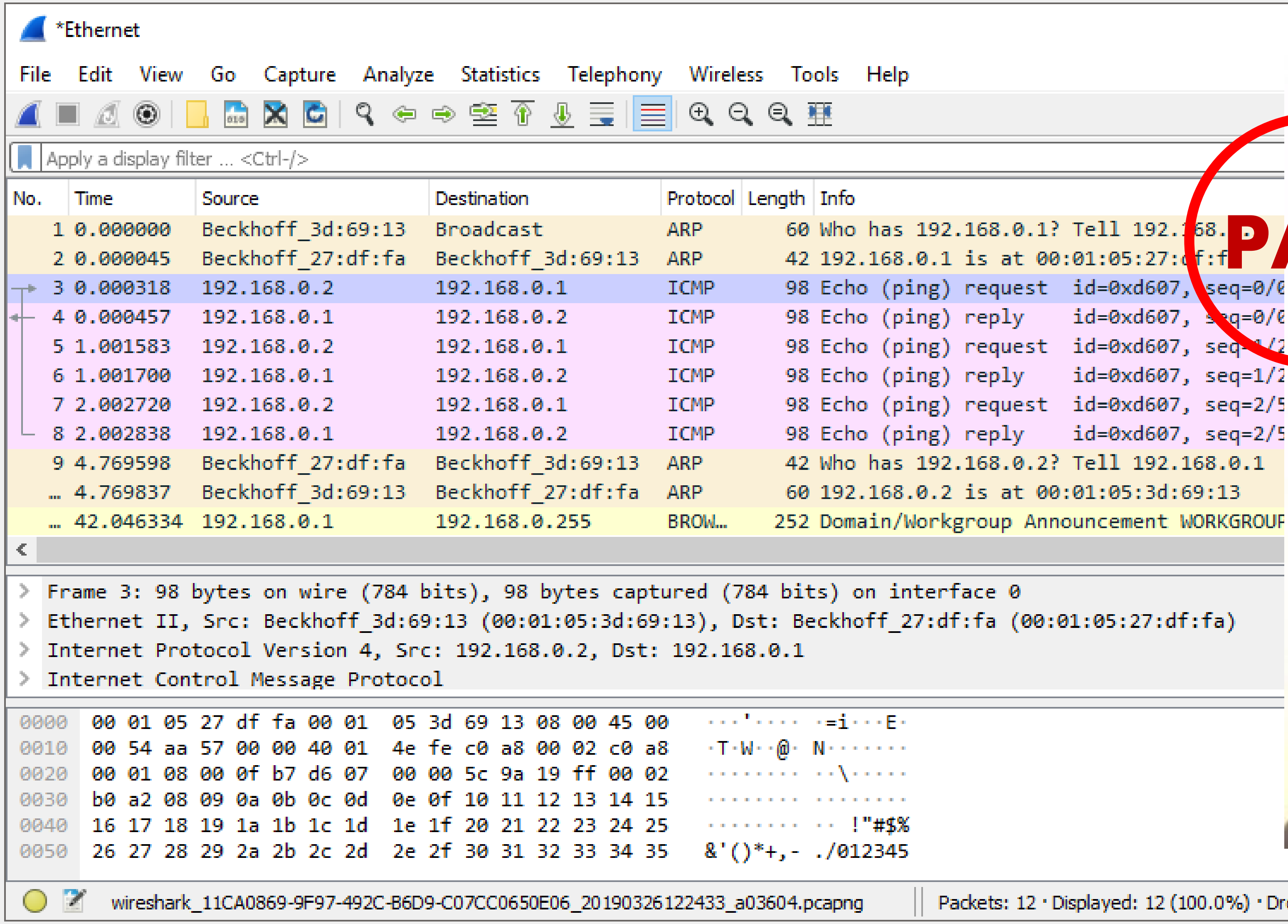
Fortinet 台灣區技術顧問

ljarvis@fortinet.com

What’s New in 7.2 GA

Graphical Diagnostics Tools

內嵌即時圖形化封包擷取分析工具



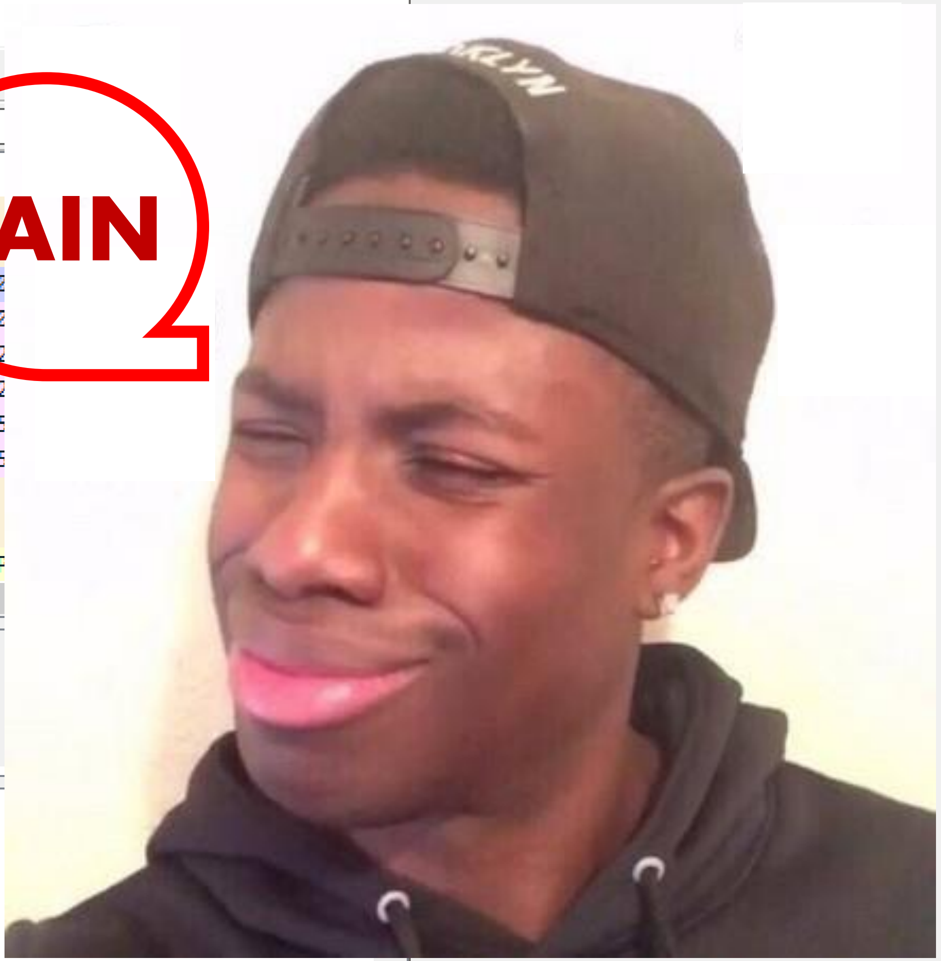
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No. Time        Source              Destination         Protocol Length Info
  1 0.000000    Beckhoff_3d:69:13   Broadcast           ARP        60 Who has 192.168.0.1? Tell 192.168.
  2 0.000045    Beckhoff_27:df:fa   Beckhoff_3d:69:13   ARP        42 192.168.0.1 is at 00:01:05:27:df:f
  3 0.000318    192.168.0.2         192.168.0.1         ICMP       98 Echo (ping) request  id=0xd607, seq=0/0
  4 0.000457    192.168.0.1         192.168.0.2         ICMP       98 Echo (ping) reply    id=0xd607, seq=0/0
  5 1.001583    192.168.0.2         192.168.0.1         ICMP       98 Echo (ping) request  id=0xd607, seq=1/2
  6 1.001700    192.168.0.1         192.168.0.2         ICMP       98 Echo (ping) reply    id=0xd607, seq=1/2
  7 2.002720    192.168.0.2         192.168.0.1         ICMP       98 Echo (ping) request  id=0xd607, seq=2/5
  8 2.002838    192.168.0.1         192.168.0.2         ICMP       98 Echo (ping) reply    id=0xd607, seq=2/5
  9 4.769598    Beckhoff_27:df:fa   Beckhoff_3d:69:13   ARP        42 Who has 192.168.0.2? Tell 192.168.0.1
  … 4.769837    Beckhoff_3d:69:13   Beckhoff_27:df:fa   ARP        60 192.168.0.2 is at 00:01:05:3d:69:13
  … 42.046334   192.168.0.1         192.168.0.255       BROW…     252 Domain/Workgroup Announcement WORKGROUP
```

```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: Beckhoff_3d:69:13 (00:01:05:3d:69:13), Dst: Beckhoff_27:df:fa (00:01:05:27:df:fa)
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
> Internet Control Message Protocol
```

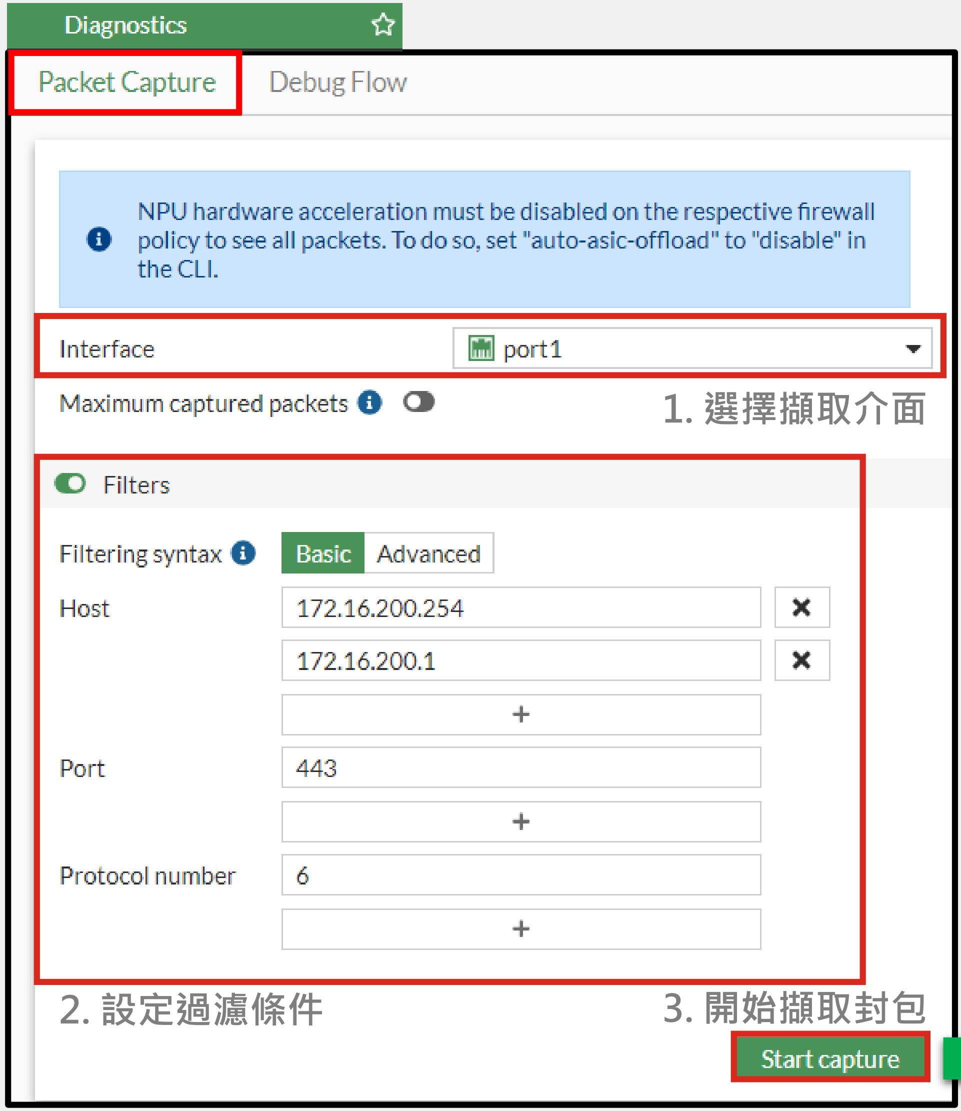
```
0000  00 01 05 27 df fa 00 01  05 3d 69 13 08 00 45 00   ···'···· ·=i···E·
0010  00 54 aa 57 00 00 40 01  4e fe c0 a8 00 02 c0 a8   ·T·W··@· N·······
0020  00 01 08 00 0f b7 d6 07  00 00 5c 9a 19 ff 00 02   ········ ··\·····
0030  b0 a2 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
```

wireshark_11CA0869-9F97-492C-B6D9-C07CC0650E06_20190326122433_a03604.pcapng | Packets: 12 · Displayed: 12 (100.0%) · Dropped: 0 (0.0%) | Profile: Default



Graphical Diagnostics Tools

內嵌即時圖形化封包擷取分析工具



NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Interface: port1

Maximum captured packets ○

1. 選擇擷取介面

● Filters

Filtering syntax: [✓ Basic] Advanced

Host: 172.16.200.254 ✖

172.16.200.1 ✖

+

Port: 443

+

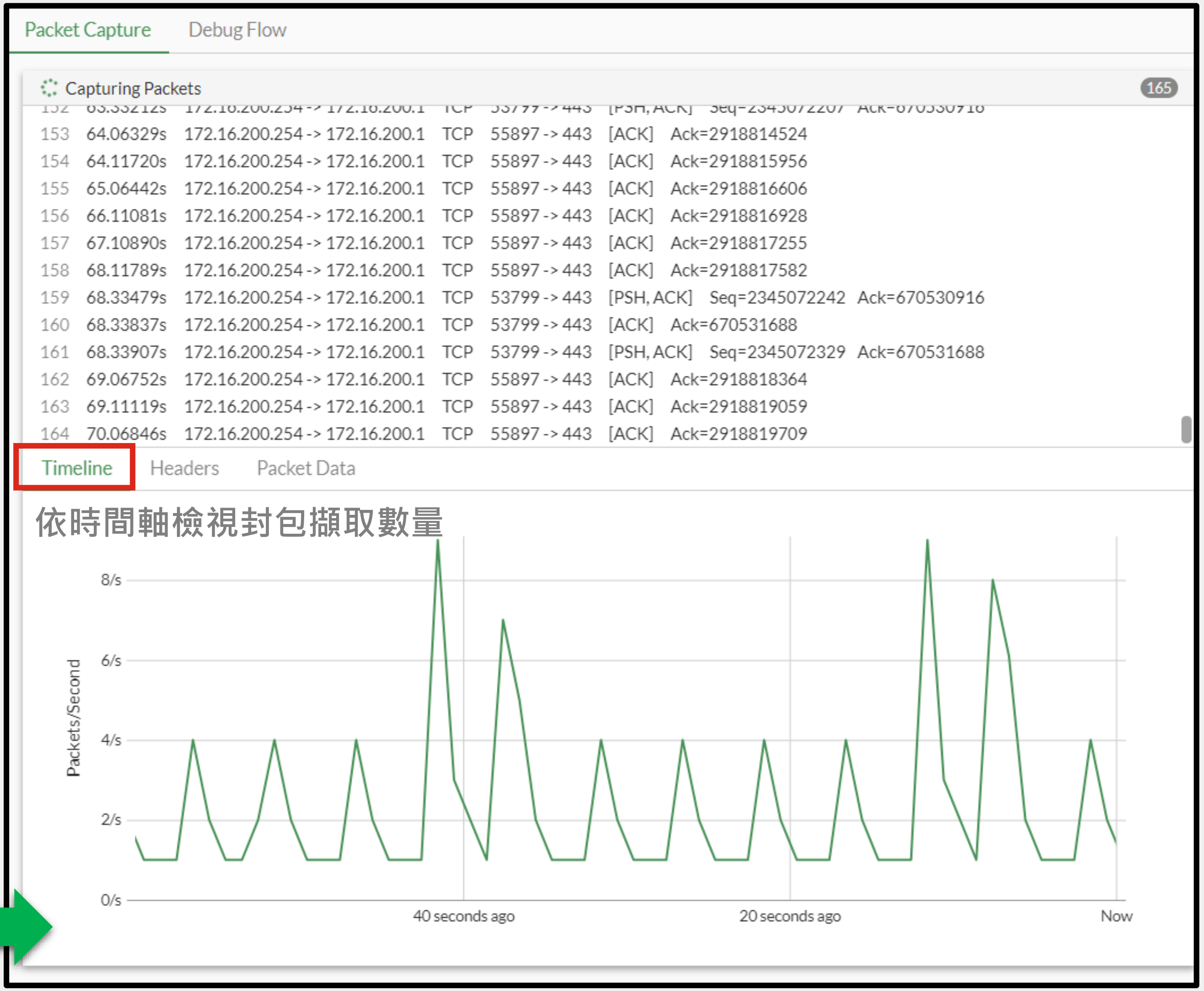
Protocol number: 6

+

2. 設定過濾條件

3. 開始擷取封包

Start capture



Capturing Packets 165

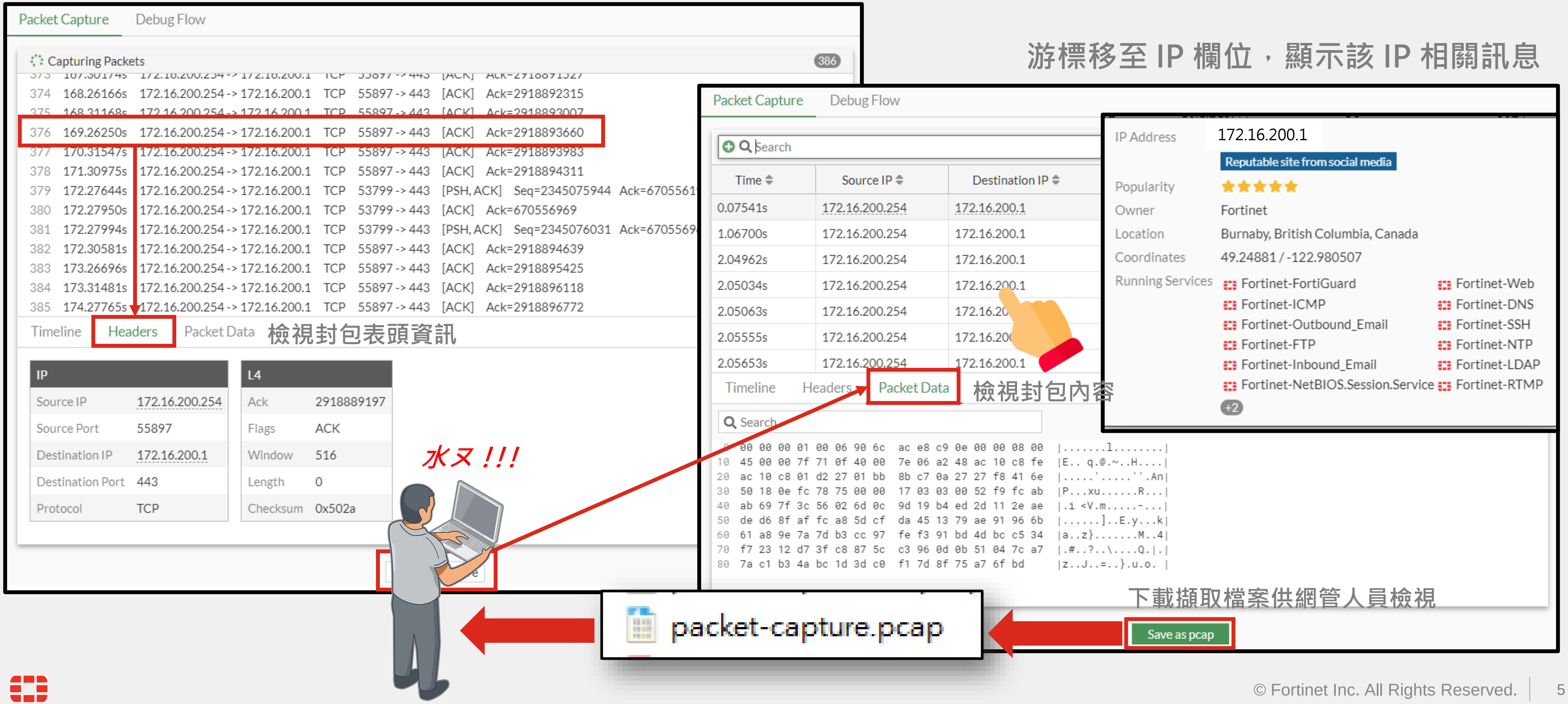
```
152  63.33212s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345072207  Ack=670530916
153  64.06329s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918814524
154  64.11720s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918815956
155  65.06442s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918816606
156  66.11081s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918816928
157  67.10890s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918817255
158  68.11789s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918817582
159  68.33479s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345072242  Ack=670530916
160  68.33837s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [ACK]  Ack=670531688
161  68.33907s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345072329  Ack=670531688
162  69.06752s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918818364
163  69.11119s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918819059
164  70.06846s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918819709
```

依時間軸檢視封包擷取數量

Click *Start capture*. The capture is visible in real-time.

Graphical Diagnostics Tools

“capture”運行時挑選欲檢視之封包點擊“*Headers*” or ” *Packet Data*”頁簽以查看更多封包訊息



游標移至 IP 欄位，顯示該 IP 相關訊息

```
373  167.30174s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918891527
374  168.26166s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918892315
375  168.31168s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918893007
376  169.26250s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918893660
377  170.31547s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918893983
378  171.30975s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918894311
379  172.27644s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345075944  Ack=6705561
380  172.27950s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [ACK]  Ack=670556969
381  172.27994s  172.16.200.254 -> 172.16.200.1  TCP  53799 -> 443  [PSH, ACK]  Seq=2345076031  Ack=6705569
382  172.30581s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918894639
383  173.26696s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918895425
384  173.31481s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918896118
385  174.27765s  172.16.200.254 -> 172.16.200.1  TCP  55897 -> 443  [ACK]  Ack=2918896772
```

檢視封包表頭資訊

IP	
Source IP	172.16.200.254
Source Port	55897
Destination IP	172.16.200.1
Destination Port	443
Protocol	TCP

L4	
Ack	2918889197
Flags	ACK
Window	516
Length	0
Checksum	0x502a

水ヌ !!!

Time	Source IP	Destination IP
0.07541s	172.16.200.254	172.16.200.1
1.06700s	172.16.200.254	172.16.200.1
2.04962s	172.16.200.254	172.16.200.1
2.05034s	172.16.200.254	172.16.200.1
2.05063s	172.16.200.254	172.16.20
2.05555s	172.16.200.254	172.16.20
2.05653s	172.16.200.254	172.16.200.1

IP Address	172.16.200.1
	Reputable site from social media
Popularity	★★★★★
Owner	Fortinet
Location	Burnaby, British Columbia, Canada
Coordinates	49.24881 / -122.980507
Running Services	Fortinet-FortiGuard Fortinet-ICMP Fortinet-Outbound_Email Fortinet-FTP Fortinet-Inbound_Email Fortinet-NetBIOS.Session.Service Fortinet-Web Fortinet-DNS Fortinet-SSH Fortinet-NTP Fortinet-LDAP Fortinet-RTMP +2

檢視封包內容

```
0   00 00 00 01 00 06 90 6c  ac e8 c9 0e 00 00 08 00  |.......l........|
10  45 00 00 7f 71 0f 40 00  7e 06 a2 48 ac 10 c8 fe  |E.. q.@.~..H....|
20  ac 10 c8 01 d2 27 01 bb  8b c7 0a 27 27 f8 41 6e  |.....'.....''.An|
30  50 18 0e fc 78 75 00 00  17 03 03 00 52 f9 fc ab  |P...xu......R...|
40  ab 69 7f 3c 56 02 6d 0c  9d 19 b4 ed 2d 11 2e ae  |.i <V.m.....-...|
50  de d6 8f af fc a8 5d cf  da 45 13 79 ae 91 96 6b  |......]..E.y...k|
60  61 a8 9e 7a 7d b3 cc 97  fe f3 91 bd 4d bc c5 34  |a..z}.......M..4|
70  f7 23 12 d7 3f c8 87 5c  c3 96 0d 0b 51 04 7c a7  |.#..?..\....Q.|.|
80  7a c1 b3 4a bc 1d 3d c0  f1 7d 8f 75 a7 6f bd     |z..J..=..}.u.o. |
```

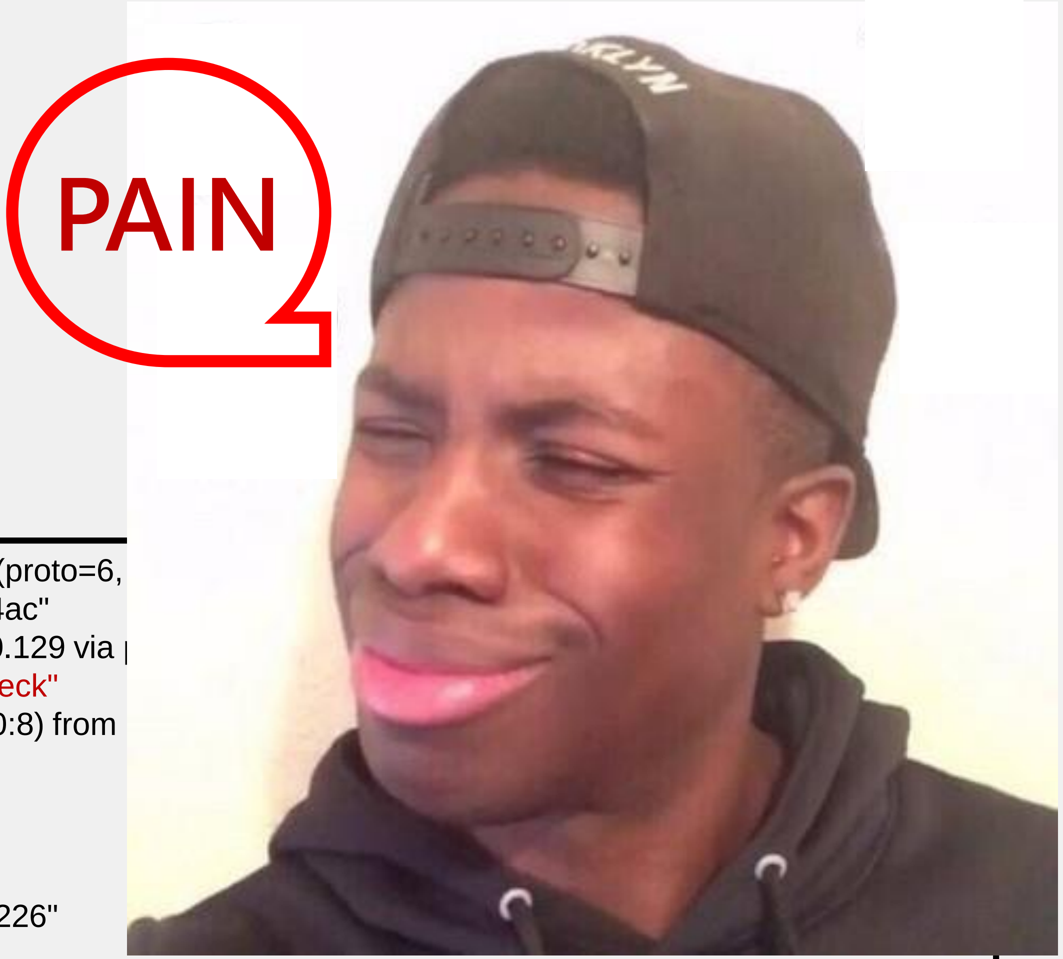
下載擷取檔案供網管人員檢視

Graphical Diagnostics Tools

內嵌即時圖形化 “diag debug flow” 除錯分析工具

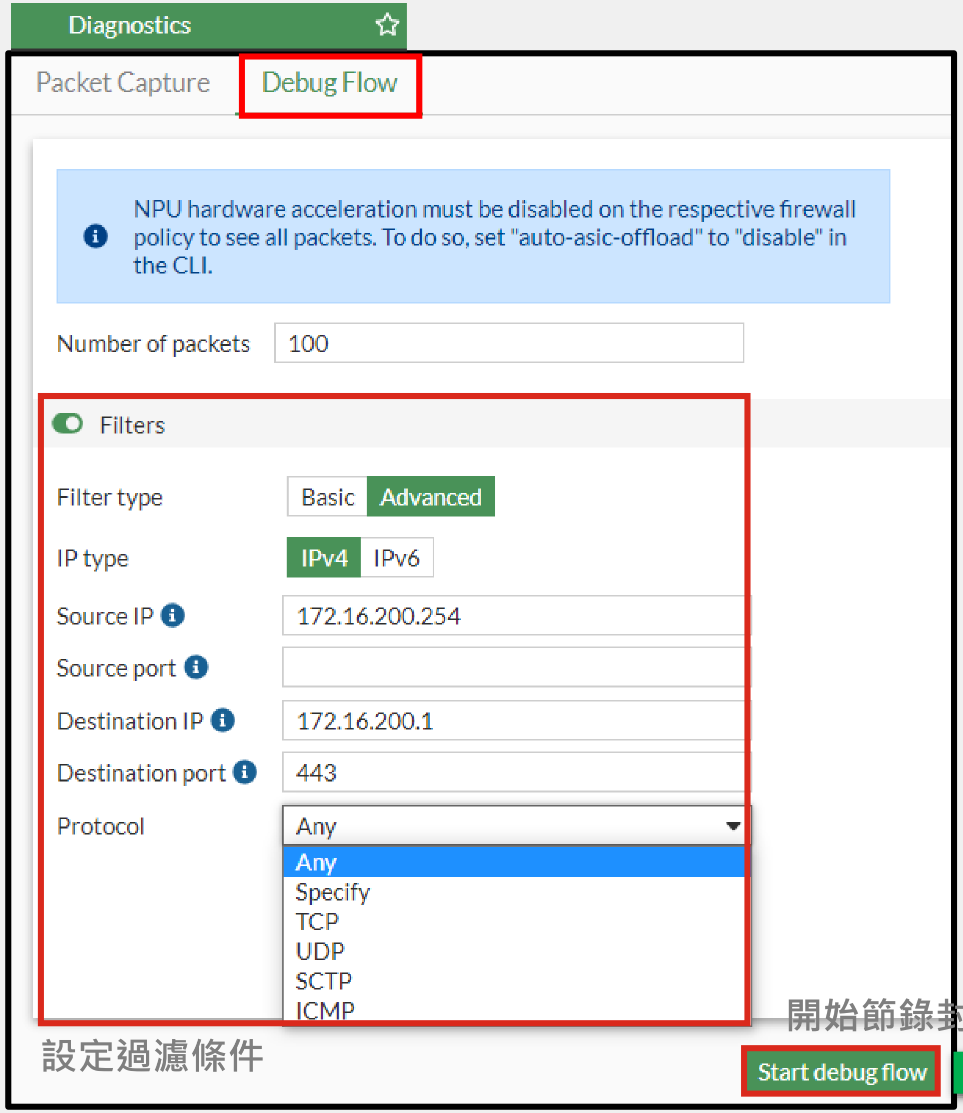
```
# diag debug reset
# diag debug flow show iprope enable
# diag debug flow sho function-name enable
# diagnose debug console timestamp enable
# diagnose debug flow filter saddr <addr/range>
# diagnose debug flow filter sport <port/range>
# diagnose debug flow filter daddr <addr/range>
# diagnose debug flow filter dport <port/range>
# diagnose debug flow filter proto <protocol>
# diag debug flow trace start 1000
# diag debug enable
```

```
id=20085 trace_id=319 func=resolve_ip_tuple_fast line=2825 msg="vd-root received a packet(proto=6,
id=20085 trace_id=319 func=resolve_ip_tuple line=2924 msg="allocate a new session-013004ac"
id=20085 trace_id=319 func=vf_ip4_route_input line=1597 msg="find a route: gw-192.168.150.129 via
id=20085 trace_id=319 func=fw_forward_handler line=248 msg=" Denied by forward policy check"
id=20085 trace_id-320 msg="vd-root received a packet (proto=1, 10.72.55.240:1->10.71.55.10:8) from
id=20085 trace_id-320 msg="allocate a new session-00001cd3"
id=20085 trace_id-320 msg="find a route: gw-192.168.56.230 via wan1"
id=20085 trace_id-320 msg="Allowed by Policy-2: encrypt"
id=20085 trace_id-320 msg="enter IPsec tunnel-RemotePhase1"
id=20085 trace_id-320 msg="encrypted, and send to 192.168.225.22 with source 192.168.56.226"
id=20085 trace_id-320 msg="send to 192.168.56.230 via intf-wan1 “
id=20085 trace_id=321 msg="vd-root received a packet (proto=1, 10.72.55.240:1-10.71.55.10:8) from internal."
id=20085 trace_id=321 msg="Find an existing session, id-00001cd3, original direction"
id=20085 trace_id=321 msg="enter IPsec ="encrypted, and send to 192.168.225.22 with source 192.168.56.226 ” tunnel-RemotePhase1"
id=20085 trace_id=321 msgid=20085 trace_id=2 msg="send to 192.168.56.230 via intf-wan1"
```



Graphical Diagnostics Tools

內嵌即時圖形化 “diag debug flow” 除錯分析工具



NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Number of packets: 100

Filters

Filter type: Basic [✓ Advanced]

IP type: [✓ IPv4] IPv6

Source IP: 172.16.200.254

Source port:

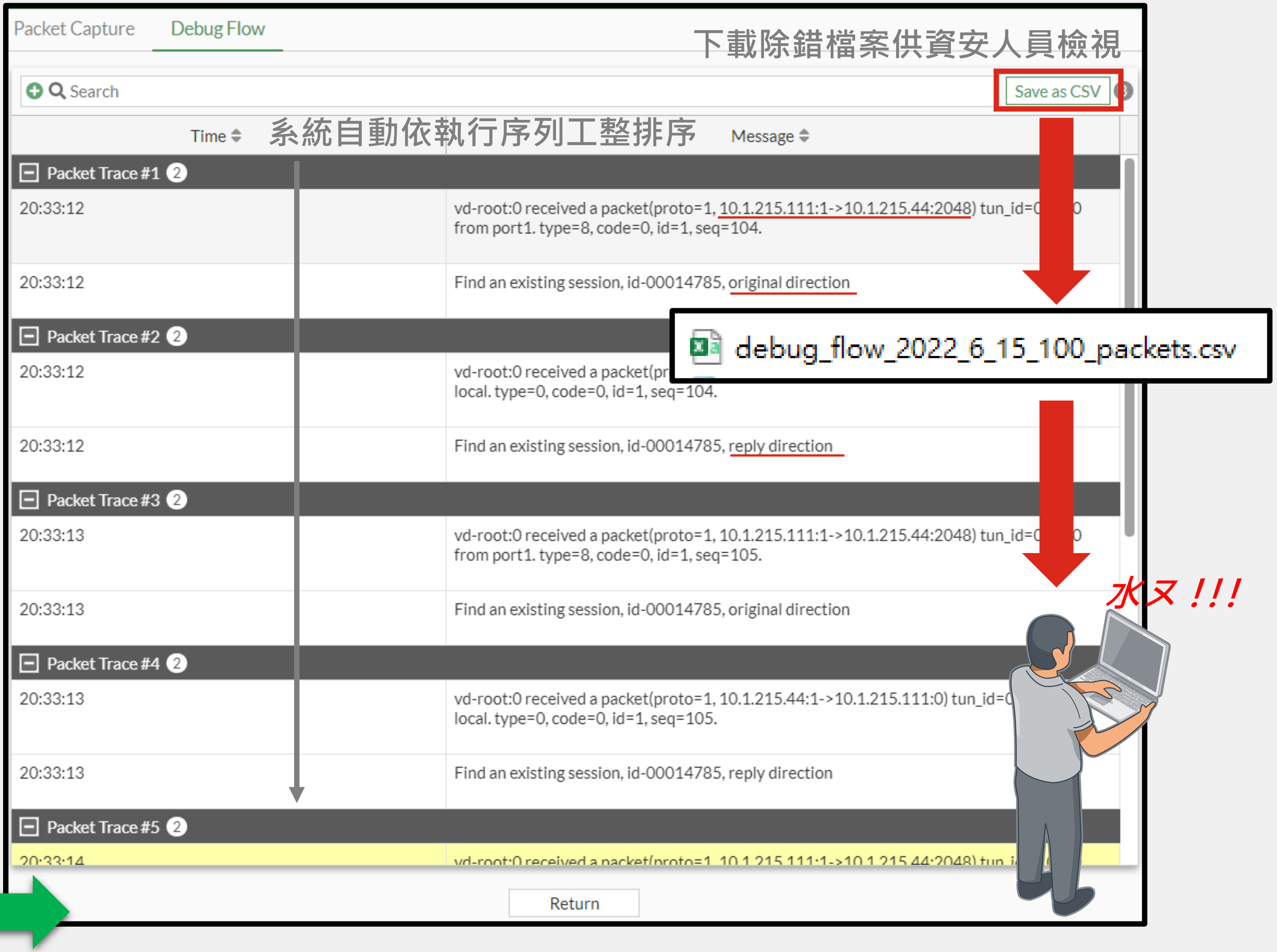
Destination IP: 172.16.200.1

Destination port: 443

Protocol: Any

設定過濾條件

開始節錄封包



下載除錯檔案供資安人員檢視

系統自動依執行序列工整排序

```
Packet Trace #1 (2)
20:33:12    vd-root:0 received a packet(proto=1, 10.1.215.111:1->10.1.215.44:2048) tun_id=0      0
            from port1. type=8, code=0, id=1, seq=104.
20:33:12    Find an existing session, id-00014785, original direction
Packet Trace #2 (2)
20:33:12    vd-root:0 received a packet(pr
            local. type=0, code=0, id=1, seq=104.
20:33:12    Find an existing session, id-00014785, reply direction
Packet Trace #3 (2)
20:33:13    vd-root:0 received a packet(proto=1, 10.1.215.111:1->10.1.215.44:2048) tun_id=0      0
            from port1. type=8, code=0, id=1, seq=105.
20:33:13    Find an existing session, id-00014785, original direction
Packet Trace #4 (2)
20:33:13    vd-root:0 received a packet(proto=1, 10.1.215.44:1->10.1.215.111:0) tun_id=0
            local. type=0, code=0, id=1, seq=105.
20:33:13    Find an existing session, id-00014785, reply direction
Packet Trace #5 (2)
20:33:14    vd-root:0 received a packet(proto=1, 10.1.215.111:1->10.1.215.44:2048) tun_i
```

debug_flow_2022_6_15_100_packets.csv

水ㄡ !!!

Click *Start capture*. The capture is visible in real-time.

Workflow Management

Policy change summary 摘要記錄

新增 Policy change summary 摘要記錄

Policy change summary 協助對防火牆政策異動的記錄與稽核追蹤

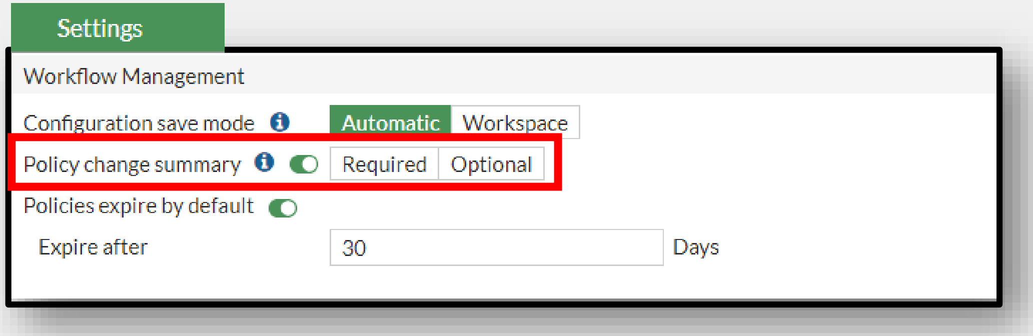
Policy change summary 協助對防火牆政策異動的記錄與稽核追蹤

Policy change summary 可依環境需求進行三種狀態配置

- *Disable: (關閉)* 防火牆政策異動時不執行摘要記錄
- *Required: (執行)* 防火牆政策異動時，強制要求管理者在編輯或創建防火牆策略時添加摘要記錄
- *Optional: (如果需要)* 防火牆政策異動時，管理者在編輯或創建防火牆策略時依需求自行決定是否添加摘要記錄

Workflow Management

新增 Policy change summary 摘要記錄



Settings

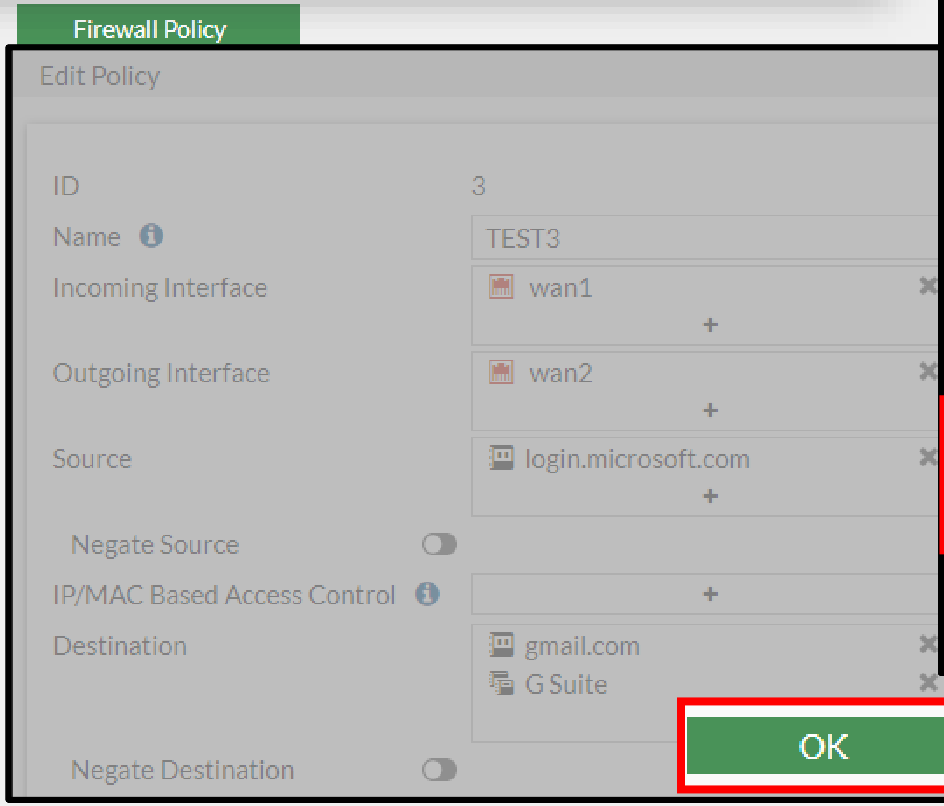
Workflow Management

Configuration save mode: [✓ Automatic] Workspace

Policy change summary: ● Required | Optional

Policies expire by default: ●

Expire after: 30 Days

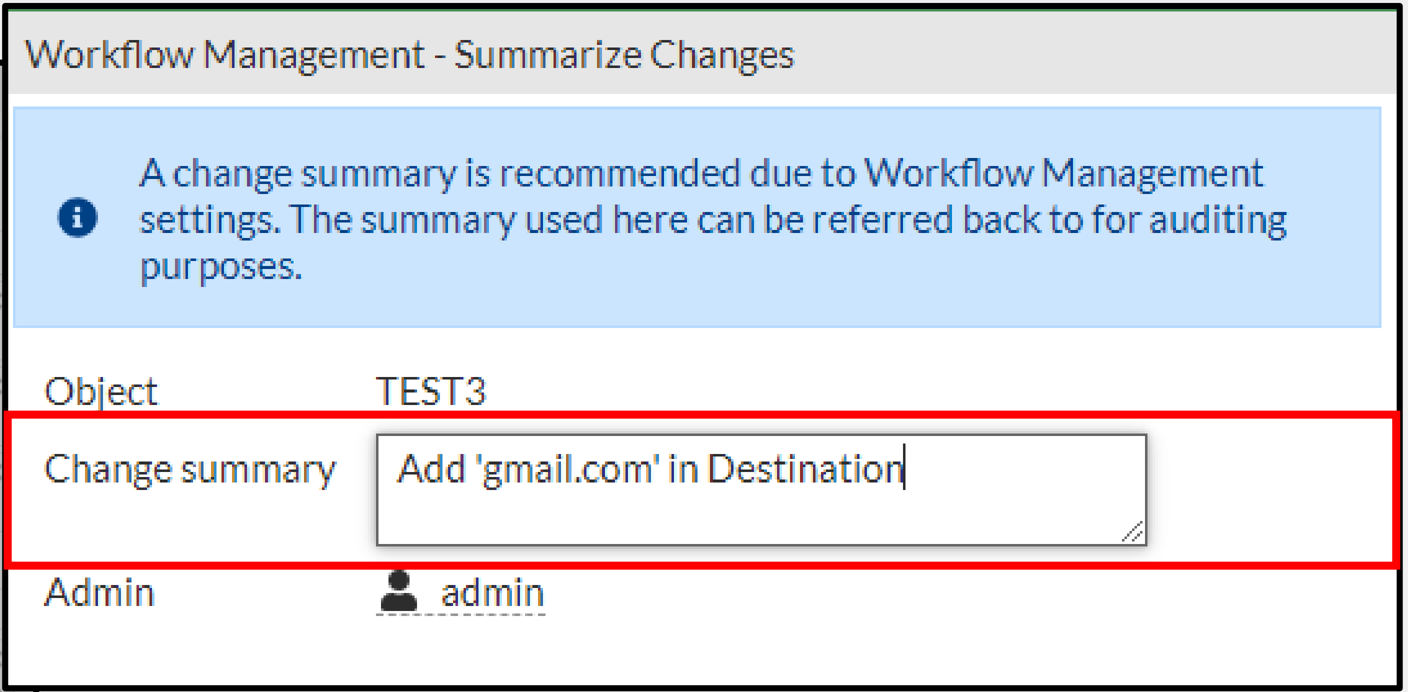


Firewall Policy

Edit Policy

ID	3
Name	TEST3
Incoming Interface	wan1
Outgoing Interface	wan2
Source	login.microsoft.com
Negate Source	○
IP/MAC Based Access Control	
Destination	gmail.com G Suite
Negate Destination	○

Default: 在創建或異動防火牆政策時，系統將**強制要求**使用者在添加異動摘要以供記錄與稽核追蹤



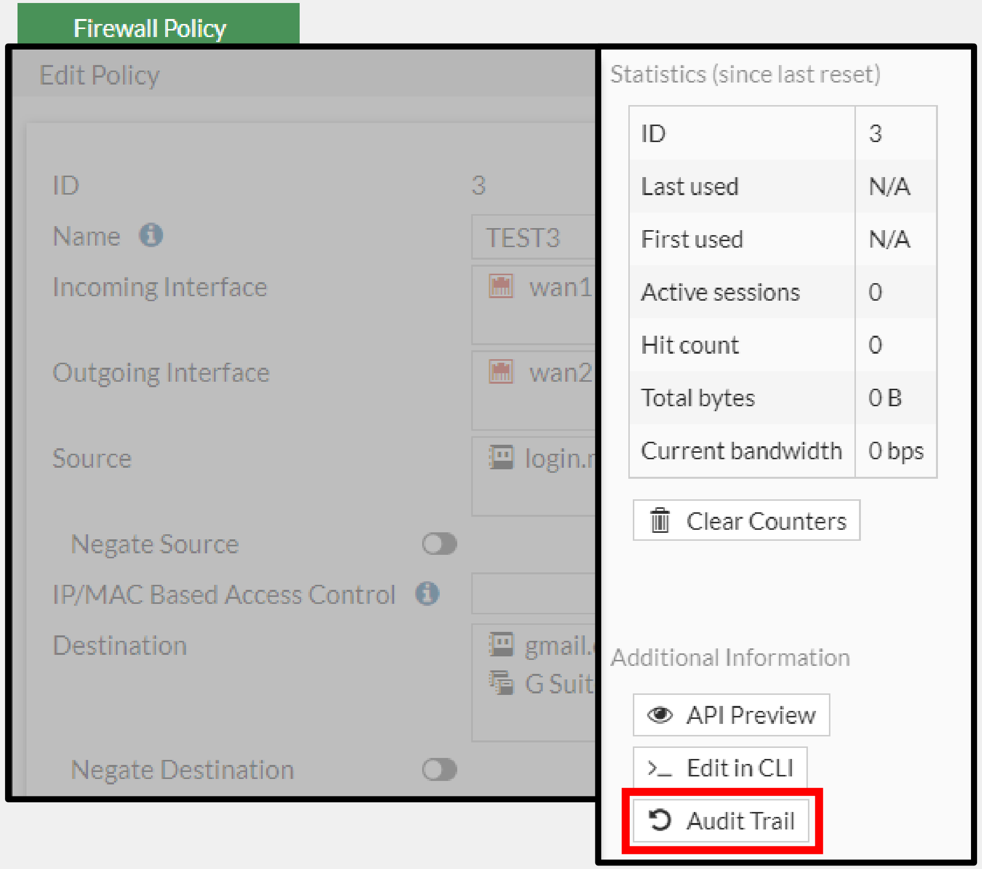
Workflow Management - Summarize Changes

A change summary is recommended due to Workflow Management settings. The summary used here can be referred back to for auditing purposes.

Object	TEST3
Change summary	Add 'gmail.com' in Destination
Admin	admin

Workflow Management

新增 Policy change summary 摘要記錄



Firewall Policy

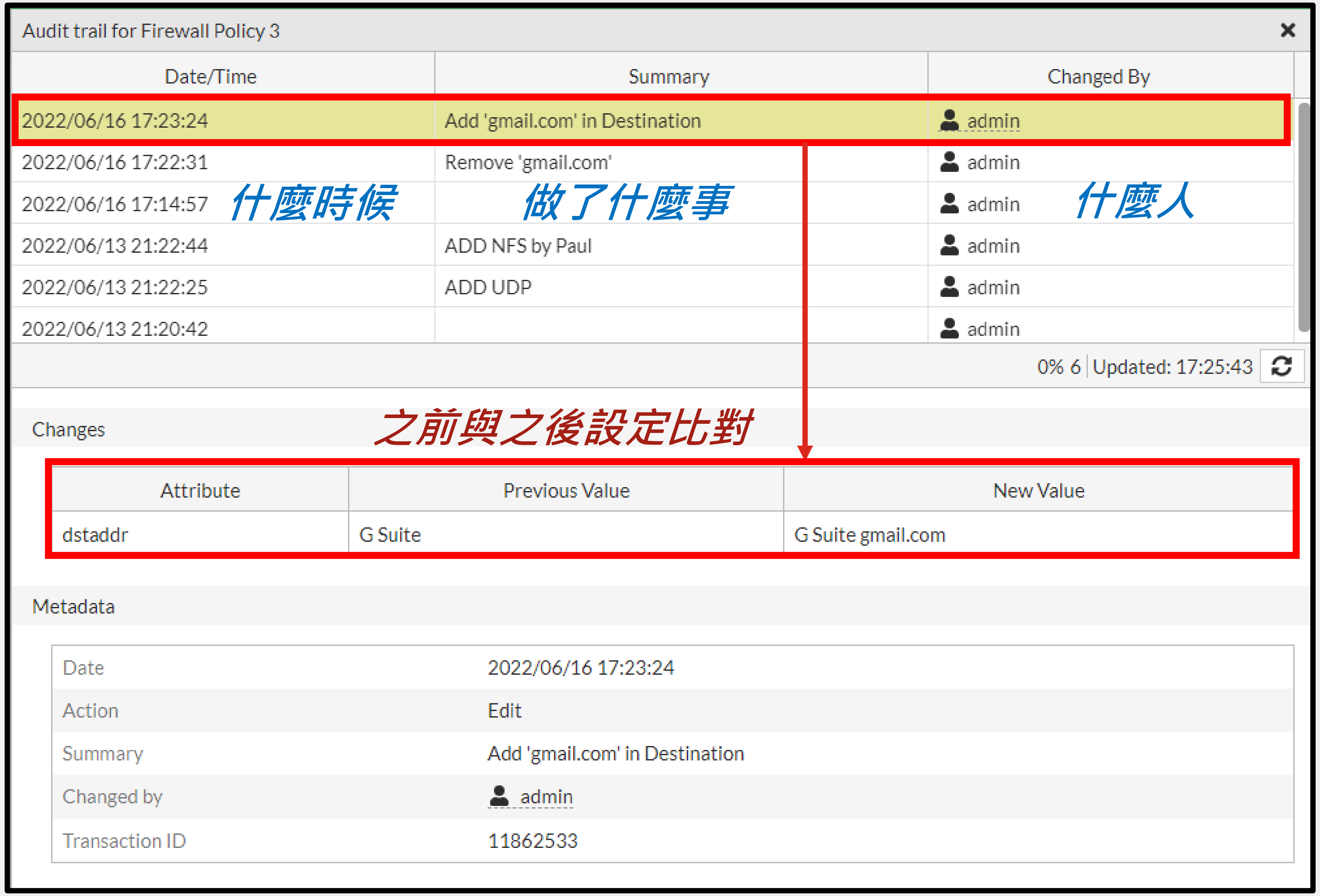
Edit Policy

ID	3
Name	TEST3
Incoming Interface	wan1
Outgoing Interface	wan2
Source	login.r
Negate Source	○
IP/MAC Based Access Control	
Destination	gmail. G Suit
Negate Destination	○

Statistics (since last reset)

ID	3
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B
Current bandwidth	0 bps

Additional Information



Audit trail for Firewall Policy 3

Date/Time	Summary	Changed By
2022/06/16 17:23:24	Add 'gmail.com' in Destination	admin
2022/06/16 17:22:31	Remove 'gmail.com'	admin
2022/06/16 17:14:57		admin
2022/06/13 21:22:44	ADD NFS by Paul	admin
2022/06/13 21:22:25	ADD UDP	admin
2022/06/13 21:20:42		admin

0% 6 Updated: 17:25:43

什麼時候

做了什麼事

什麼人

Changes

之前與之後設定比對

Attribute	Previous Value	New Value
dstaddr	G Suite	G Suite gmail.com

Metadata

Date	2022/06/16 17:23:24
Action	Edit
Summary	Add 'gmail.com' in Destination
Changed by	admin
Transaction ID	11862533

日後可點選 Audit Trail 檢視該防火牆政策異動記錄 (*“什麼人”* 在 *”什麼時候”* 做了 *” 什麼事”* ,*之前之後設定比對*)

Workflow Management

Policy expiration - 防火牆政策到期時間

新增 Policy expiration 快速設定防火牆政策到期時間

Policy expiration 協助管理者 快速定義防火牆政策到期時間

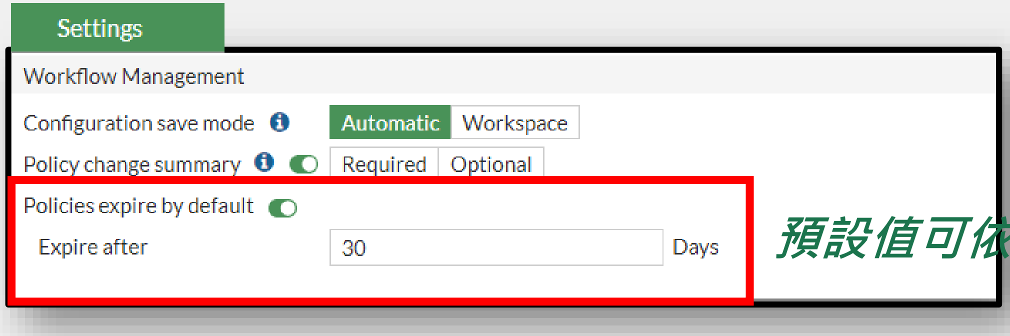
Policy expiration 協助管理者快速設定防火牆政策到期時間，不須額外套用 Schedule 物件

Policy expiration 可依環境需求進行三種狀態配置

- *Disable: (關閉)* 防火牆政策永久有效
- *Default: (預設值)* 防火牆政策將在設定 30 天後 (預設值) 到期關閉
- *Specify: (指定值)* 防火牆政策將在指定日期與時間後到期關閉

Workflow Management

新增 Policy expiration 快速設定防火牆政策到期時間



Settings

Workflow Management

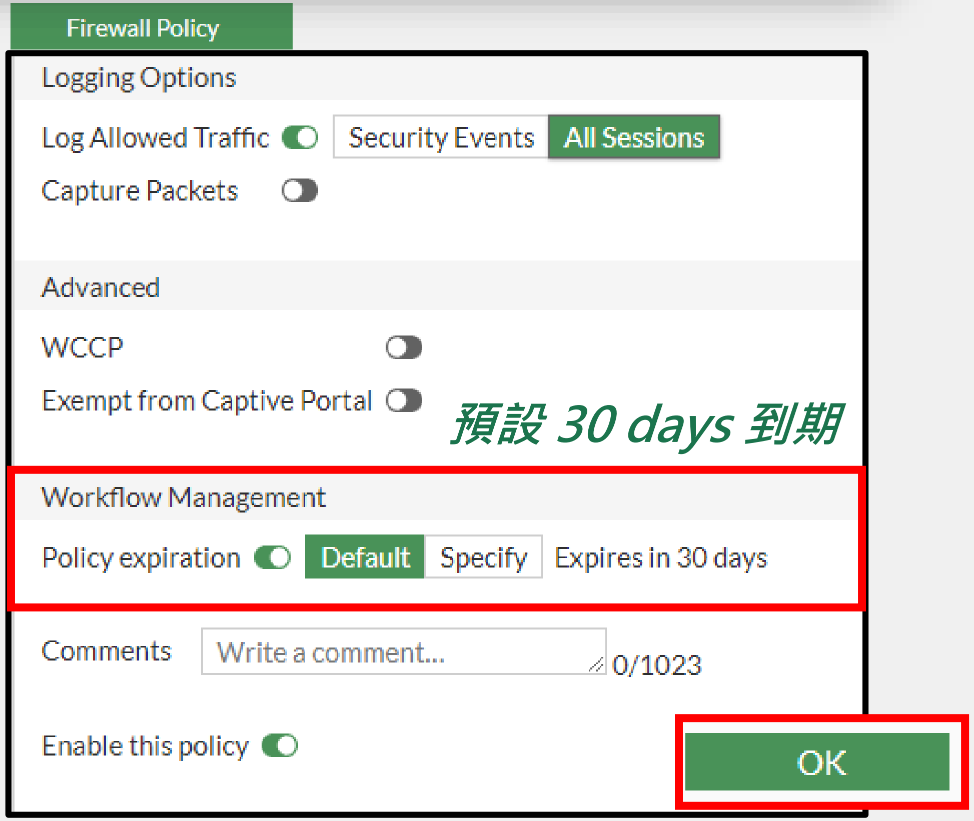
Configuration save mode ℹ [✓ Automatic] Workspace

Policy change summary ℹ ● Required Optional

Policies expire by default ●

Expire after 30 Days

預設值可依需求調整



Firewall Policy

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

Capture Packets ○

Advanced

WCCP ○

Exempt from Captive Portal ○

預設 30 days 到期

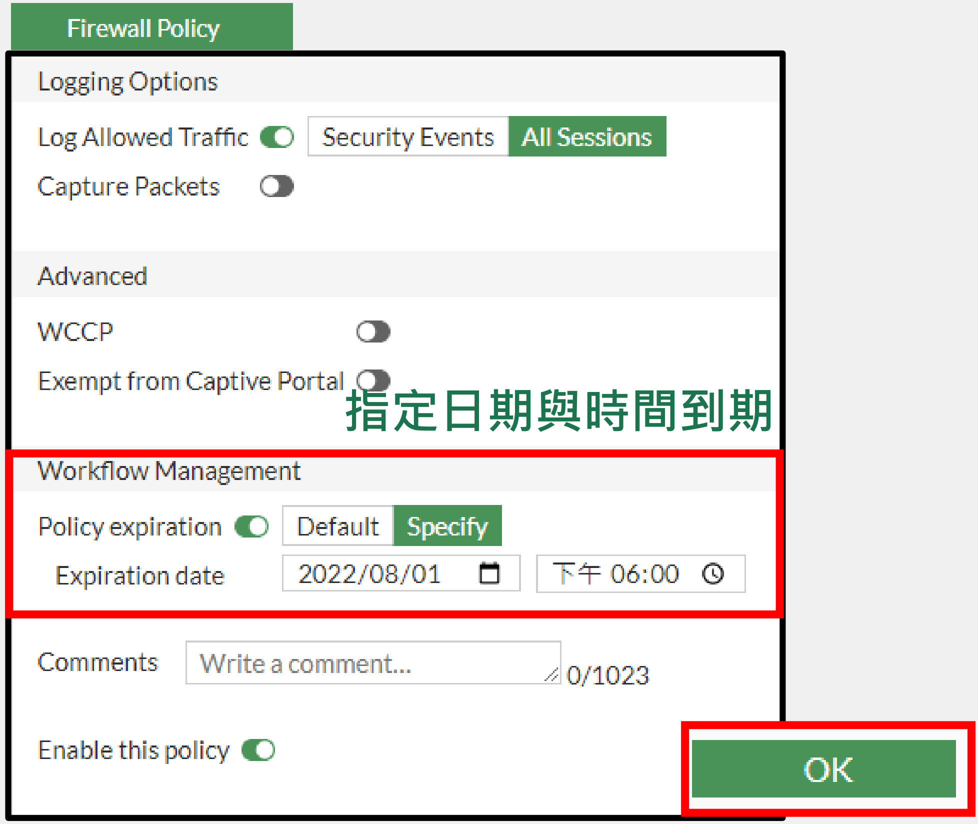
Workflow Management

Policy expiration ● [✓ Default] Specify Expires in 30 days

Comments Write a comment... 0/1023

Enable this policy ●

OK



Firewall Policy

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

Capture Packets ○

Advanced

WCCP ○

Exempt from Captive Portal ○

指定日期與時間到期

Workflow Management

Policy expiration ● Default [✓ Specify]

Expiration date 2022/08/01 下午 06:00

Comments Write a comment... 0/1023

Enable this policy ●

OK

Overlap VIPs

Allow Multiple VIPs with the Same External Interface

Overlap VIPs

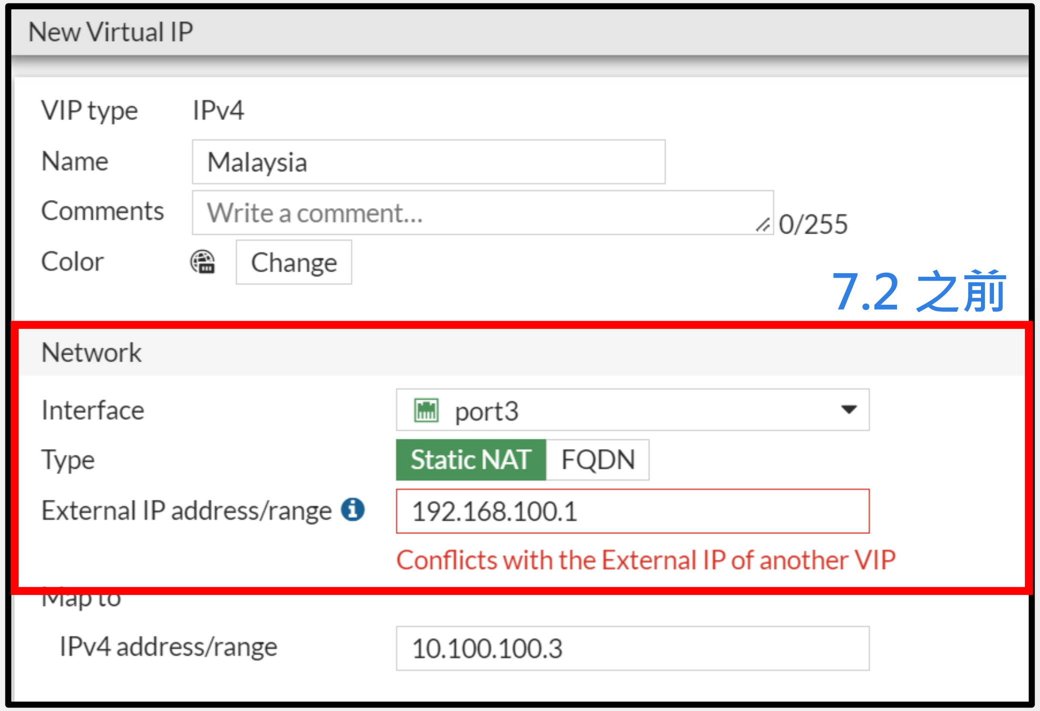
Allow Multiple VIPs with the Same External Interface

- 刪除了 VIP (外對內 Destination NAT) 的 overlapping 重複檢查限制，因此在使用相同的外部介面和外部 IP 配置多個 VIP 時沒有任何限制
- 可應用於一個外部 IP 套用不同的內部 Server IP，並定義存取來源位址，讓特定的來源透過相同的 IP 存取後端不同的服務

Overlap VIPs

Allow Multiple VIPs with the Same External Interface

FortiOS < 7.2



New Virtual IP

VIP type IPv4

Name: Malaysia

Comments: Write a comment... 0/255

Color: Change

7.2 之前

Network

Interface: port3

Type: Static NAT | FQDN

External IP address/range: 192.168.100.1

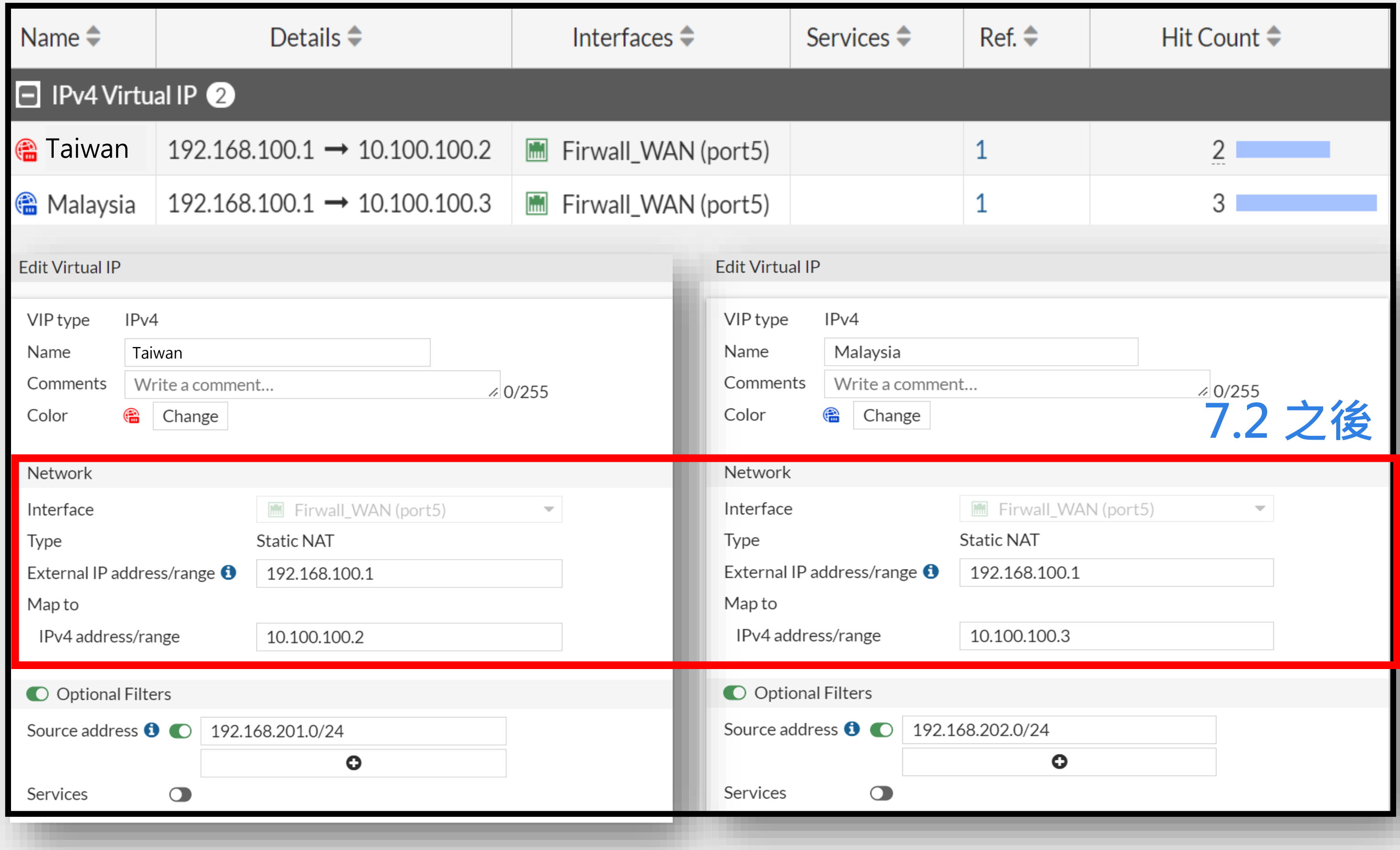
Conflicts with the External IP of another VIP

Map to

IPv4 address/range: 10.100.100.3

刪除了 VIP (外對內 Destination NAT) 的 overlapping 重疊檢查限制，因此在使用相同的外部介面和外部 IP 配置多個 VIP 時沒有任何限制

FortiOS >= 7.2



Name	Details	Interfaces	Services	Ref.	Hit Count
IPv4 Virtual IP 2					
Taiwan	192.168.100.1 → 10.100.100.2	Firwall_WAN (port5)		1	2
Malaysia	192.168.100.1 → 10.100.100.3	Firwall_WAN (port5)		1	3

Edit Virtual IP

VIP type IPv4

Name: Taiwan

Comments: Write a comment... 0/255

Color: Change

Network

Interface: Firwall_WAN (port5)

Type: Static NAT

External IP address/range: 192.168.100.1

Map to

IPv4 address/range: 10.100.100.2

Optional Filters

Source address: 192.168.201.0/24

Services

Edit Virtual IP

VIP type IPv4

Name: Malaysia

Comments: Write a comment... 0/255

Color: Change

7.2 之後

Network

Interface: Firwall_WAN (port5)

Type: Static NAT

External IP address/range: 192.168.100.1

Map to

IPv4 address/range: 10.100.100.3

Optional Filters

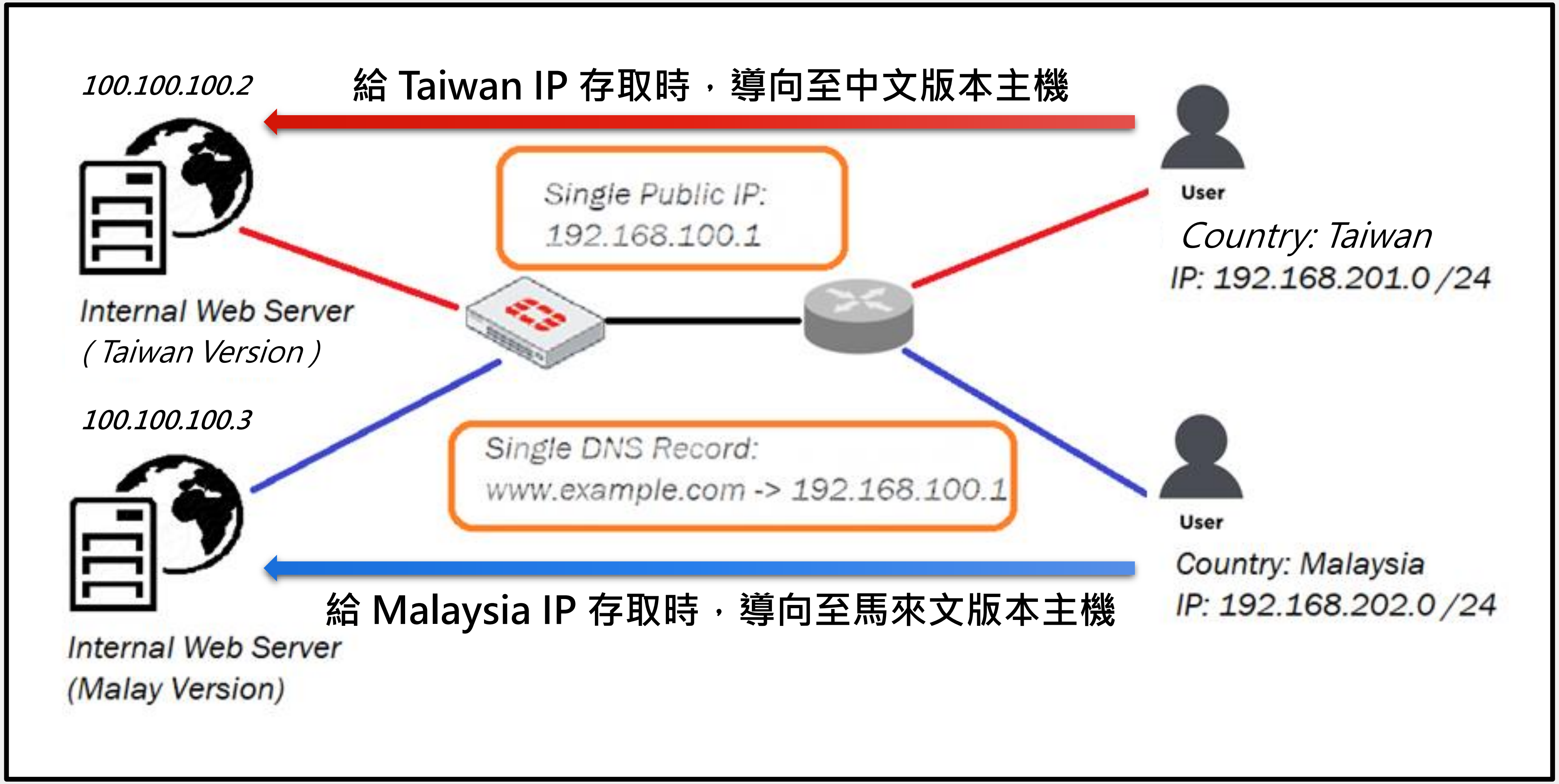
Source address: 192.168.202.0/24

Services

Overlap VIPs

Allow Multiple VIPs with the Same External Interface

Scenario: 同一個外部 IP (192.168.100.1) 提供服務



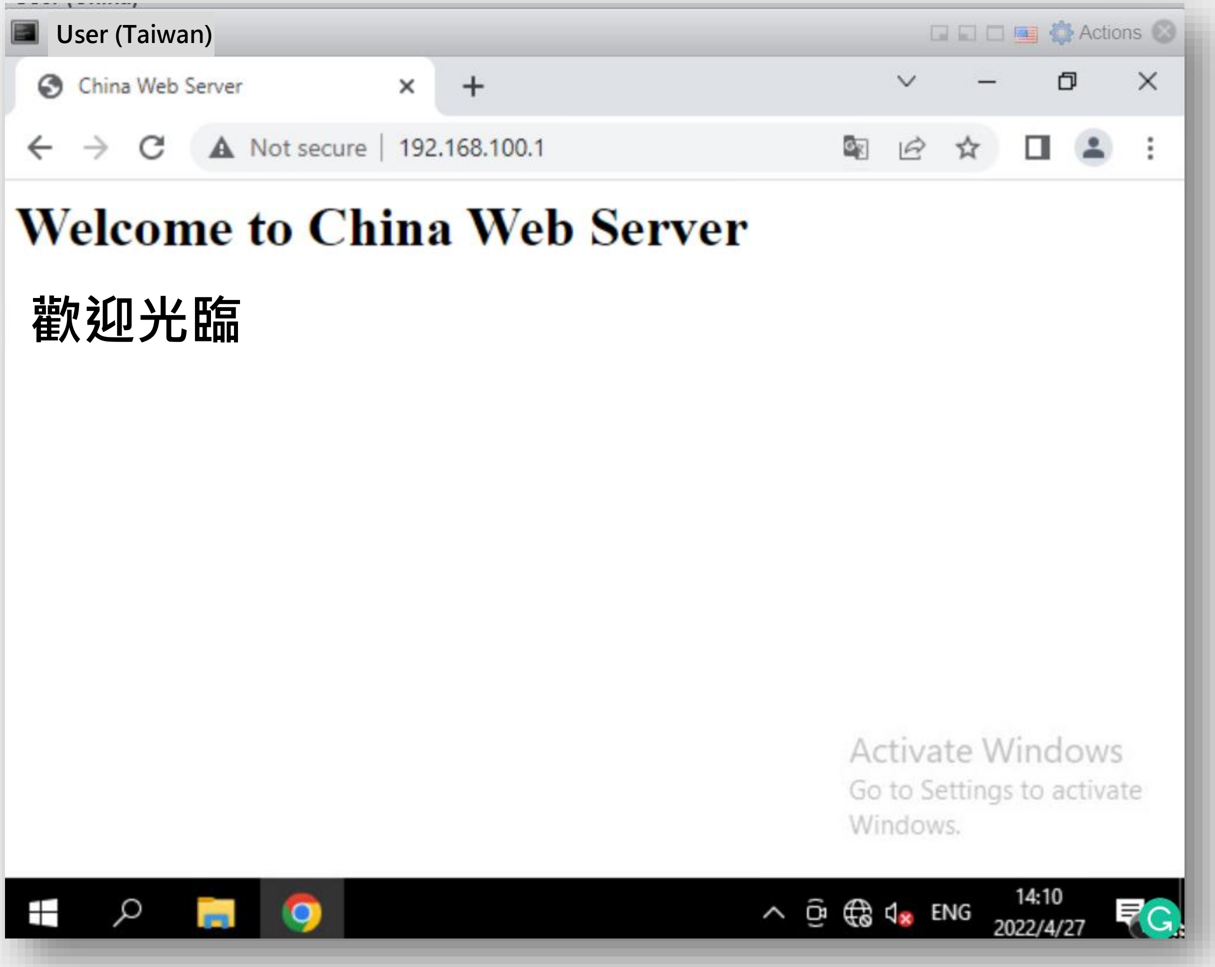
給 Taiwan IP 存取時，導向至中文版本主機

給 Malaysia IP 存取時，導向至馬來文版本主機

Overlap VIPs

Allow Multiple VIPs with the Same External Interface

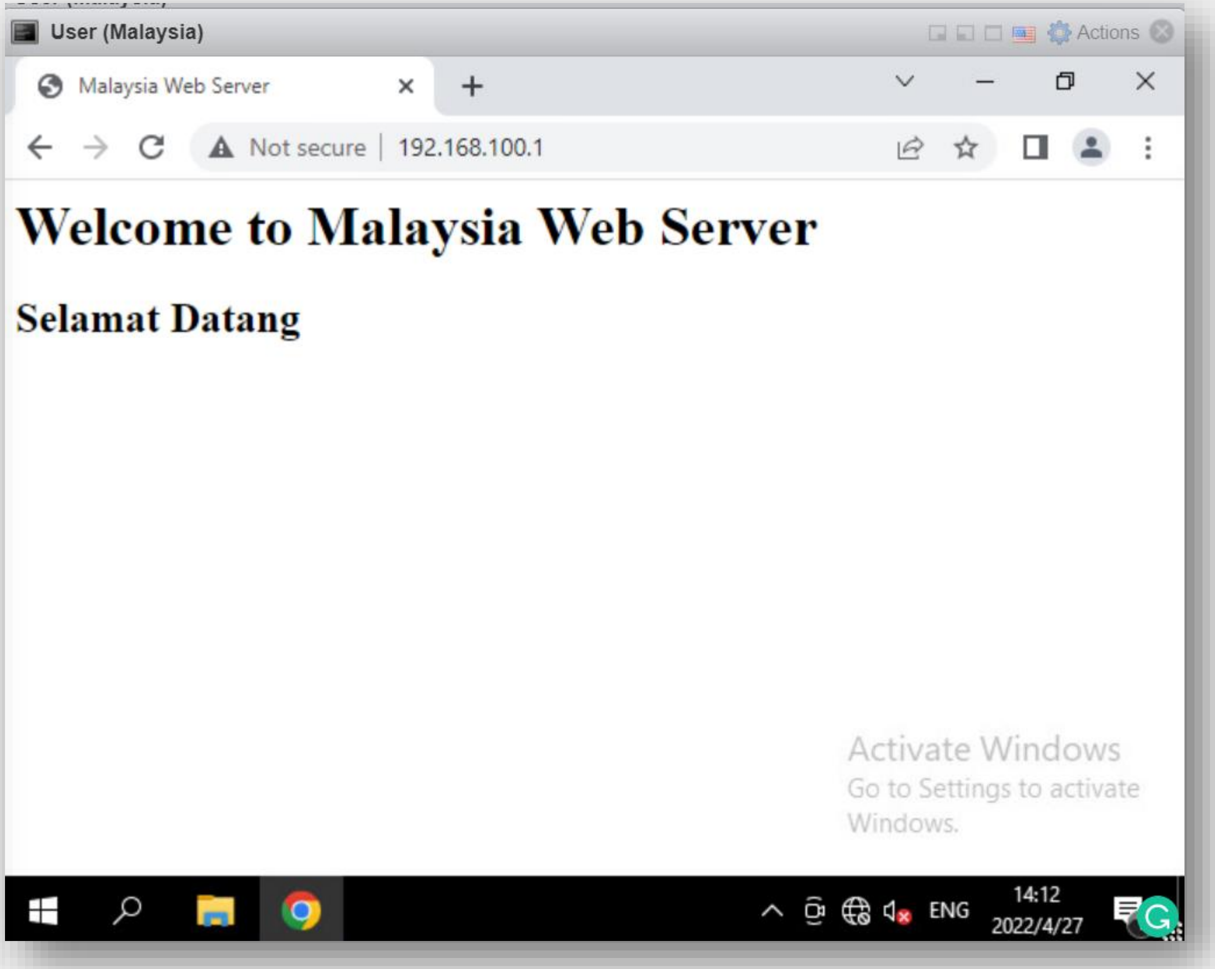
Test Results:



Welcome to China Web Server

歡迎光臨

Activate Windows
Go to Settings to activate Windows.



Welcome to Malaysia Web Server

Selamat Datang

Activate Windows
Go to Settings to activate Windows.

Fortinet Security Fabric 安全織網

全面性 (Broad)

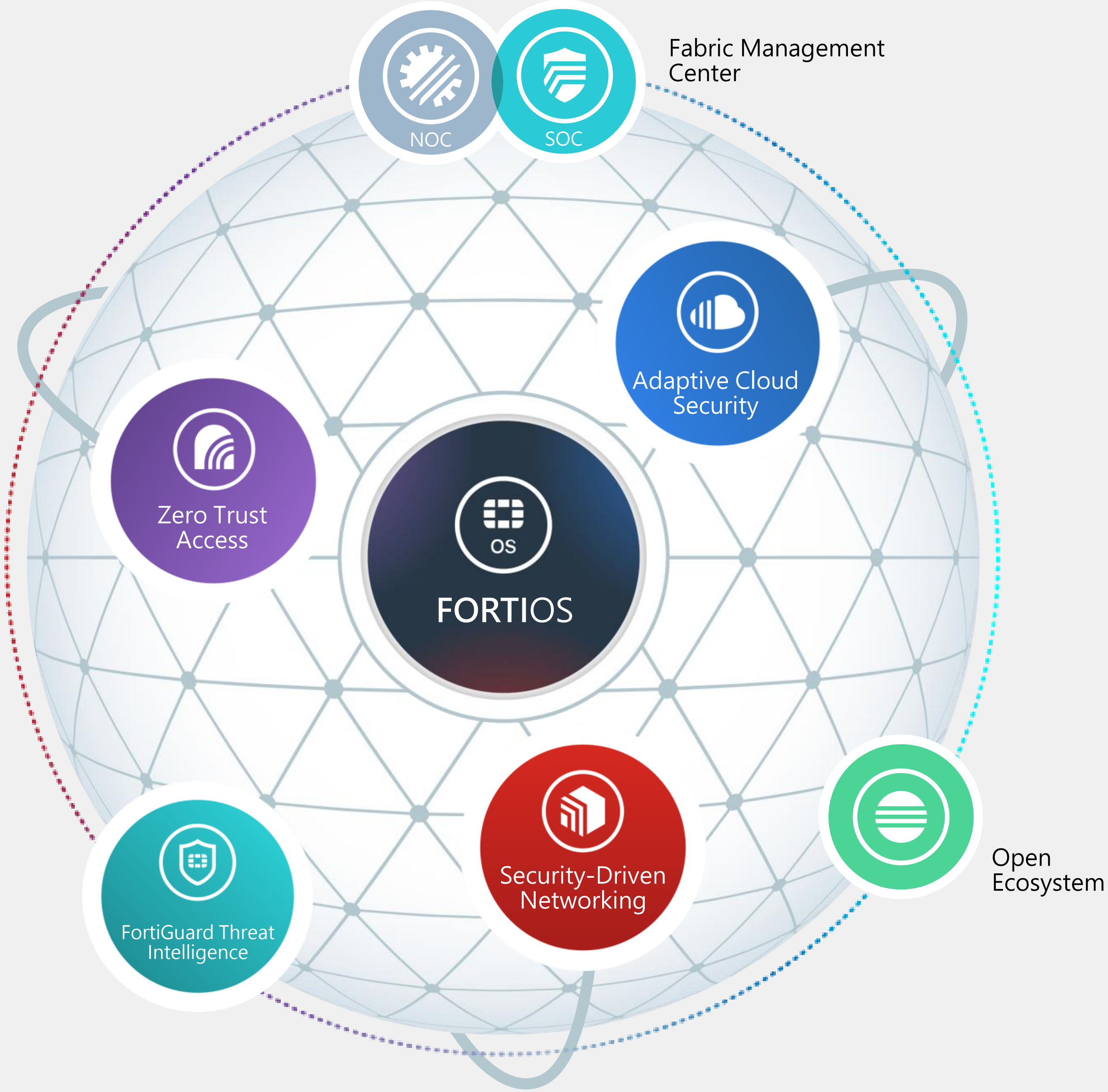
對全部數位化攻擊面提供更佳可視性與防護，以利更好的風險管理

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

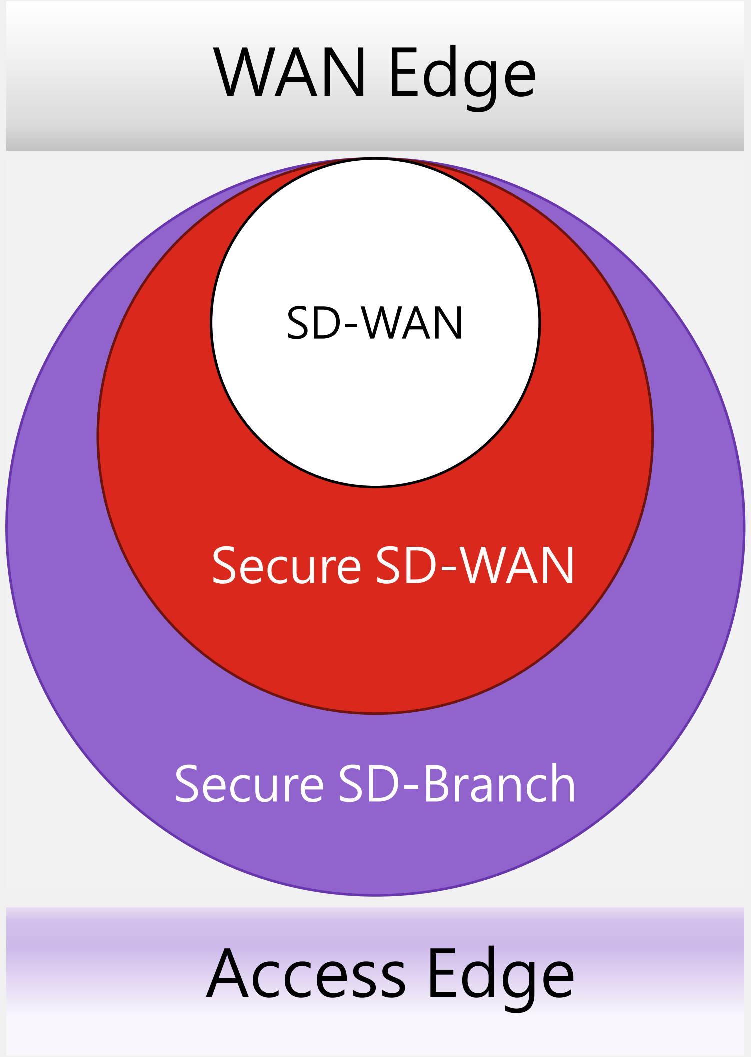
自動化 (Automated)

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



Secure SD-WAN

廣域網路架構的演進



- **需求增加**
  越來越多服務需要上雲造成WAM流量增加，降低了本來的網路性能並且增加了成本。
- **SD-WAN**
  提供線路負載均衡-增加性能並節約成本，但缺乏安全。
- **Secure SD-WAN**
  提供**卓越的應用程式線路負載均衡**和**安全性**-增加性能並節約成本，但隨著分支機構變多需要控管太多產品。
- **Secure SD-Branch**
  將**WAN和LAN統一平台控管**，減少人員成本。
  並**將完整的資訊安全擴展到網路環境中**。

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

65%
有效降低人力成本

99%
增加正常運行時間 降低風險

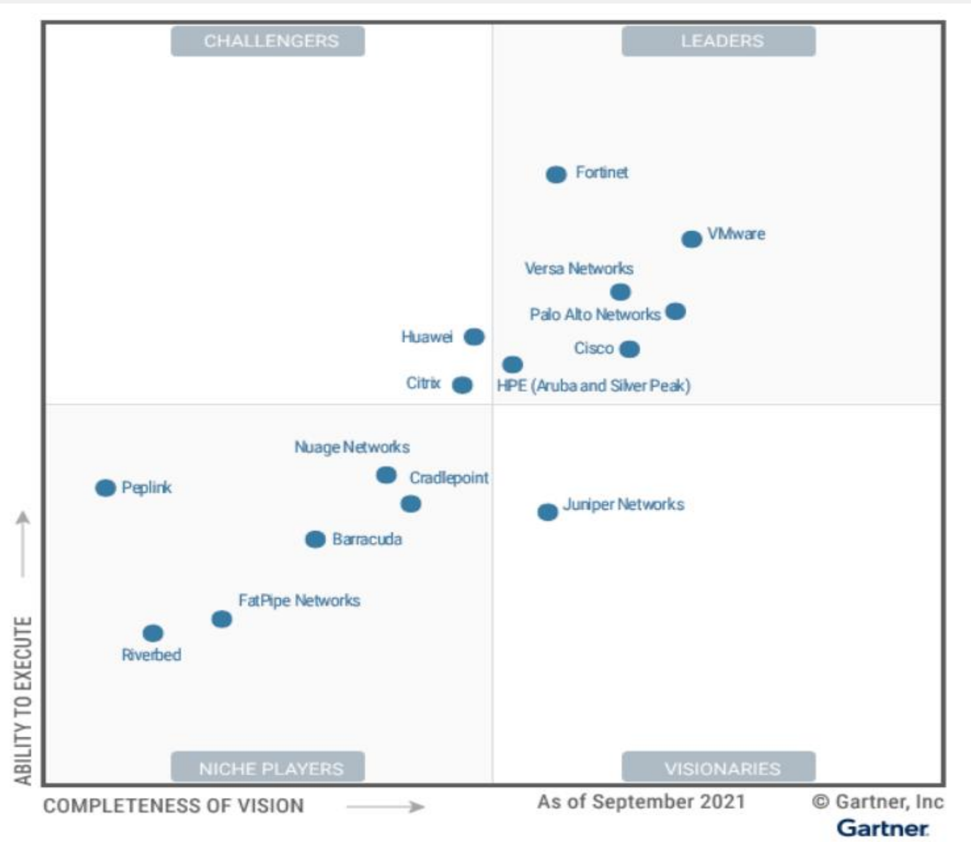
通過 Advanced WAN 實現準確的應用程序控制，以提供更好的用戶體驗

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

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

2021 年 Gartner WAN Edge 基礎設施魔力像限中的領導者和最高執行能力

2021 Gartner ® Magic Quadrant™ for WAN Edge Infrastructure



Gartner, Magic Quadrant for WAN Edge Infrastructure, Jonathan Forest, Naresh Singh, Andrew Lerner, Evan Zeng, 20 September 2021.

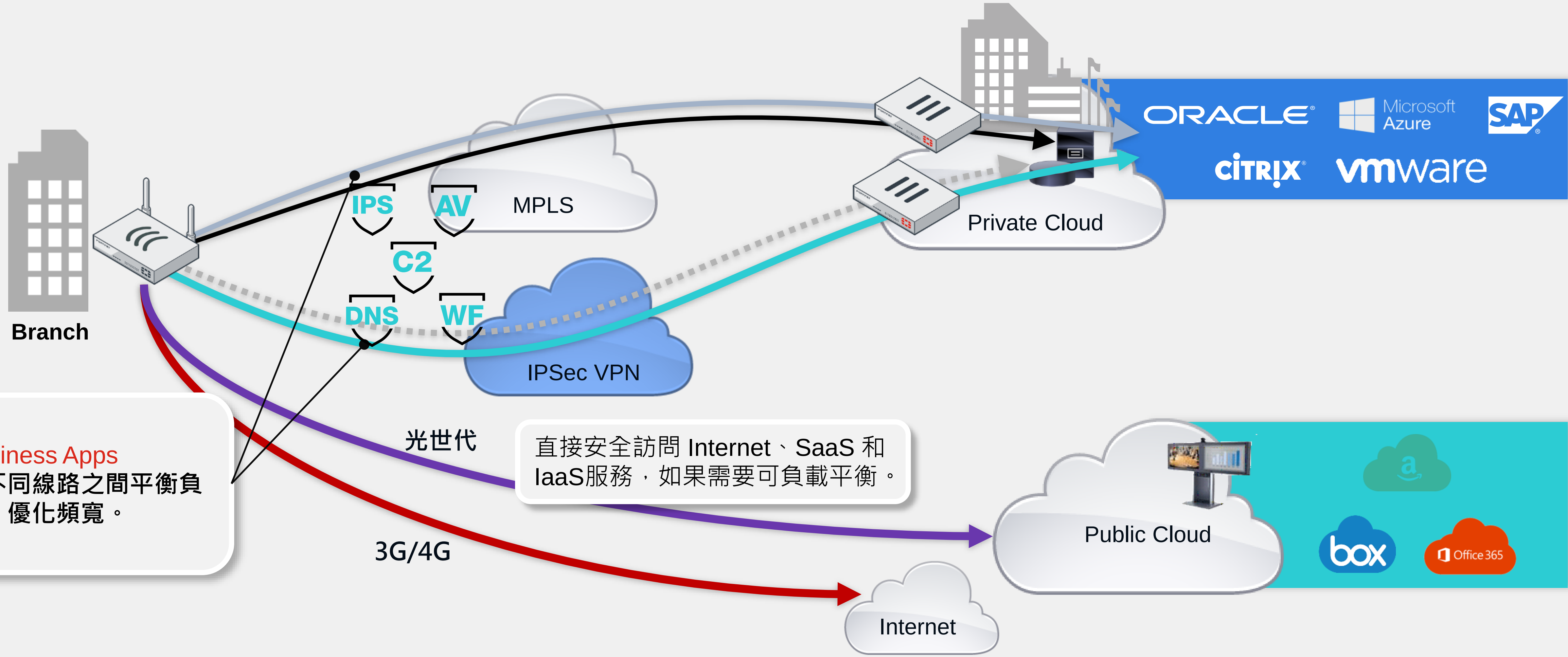
"Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner' s Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner and Magic Quadrant are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.

支援多樣化的線路整合

Secure SD-WAN

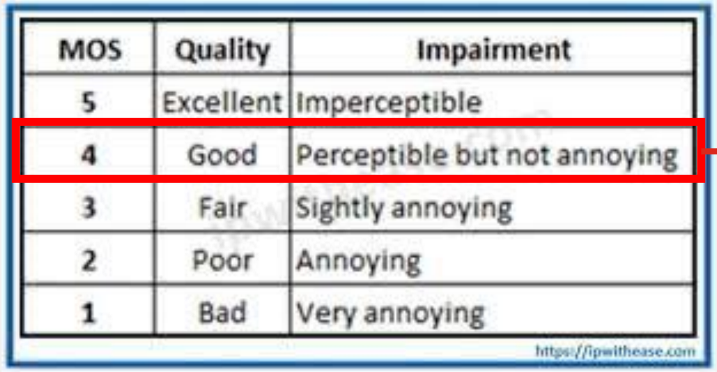


Business Apps
在不同線路之間平衡負載，優化頻寬。

直接安全訪問 Internet、SaaS 和 IaaS服務，如果需要可負載平衡。

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

https://ipwithease.com

(MOS) 是一種測量語音品質質量的方法，給予 0~5 的評估等級

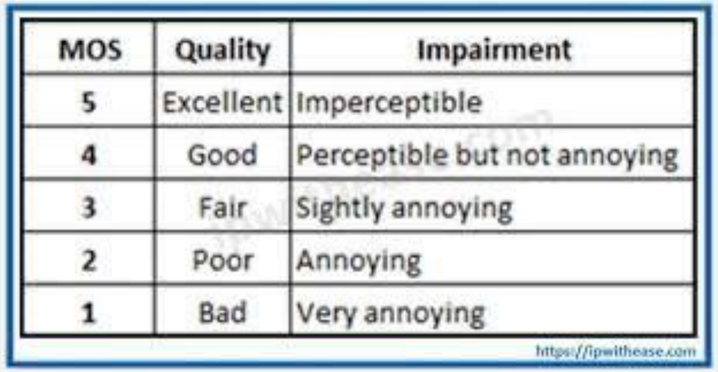
```
config health-check
    edit "Test_MOS"
        set server "2.2.2.2"
        set sla-fail-log-period 30
        set sla-pass-log-period 30
        set members 0
        set mos-codec {g711 | g729 | g722}
        config sla
            edit 1
                set link-cost-factor mos
             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

https://ipwithease.com

(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.
```

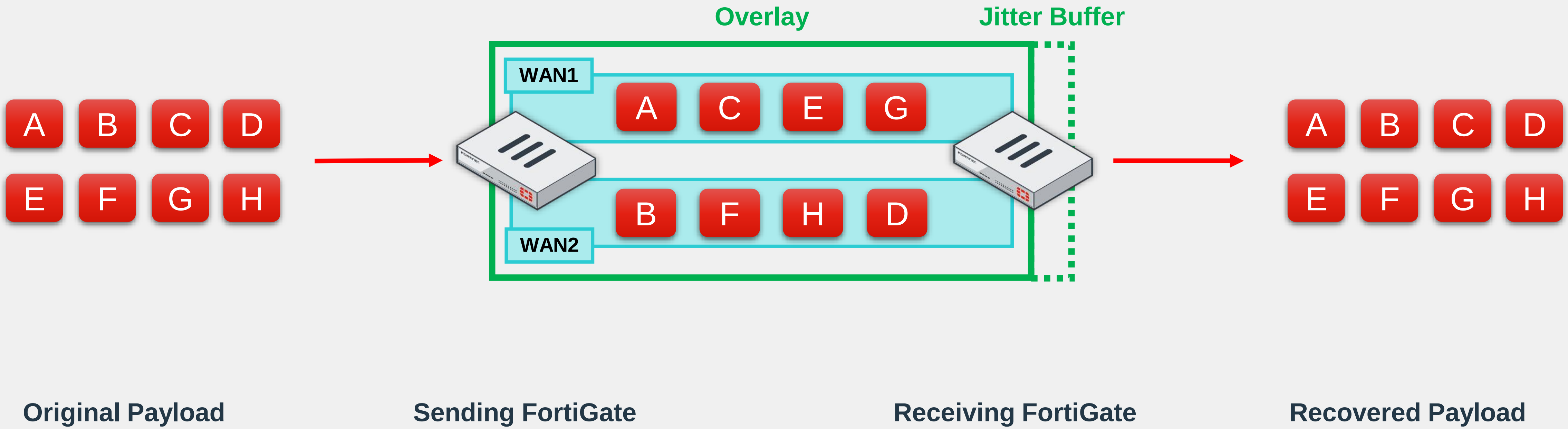
- 目前 (7.2)，MOS 值尚不能用作智能選徑條件來改變 SD-WAN 規則中的流量路徑

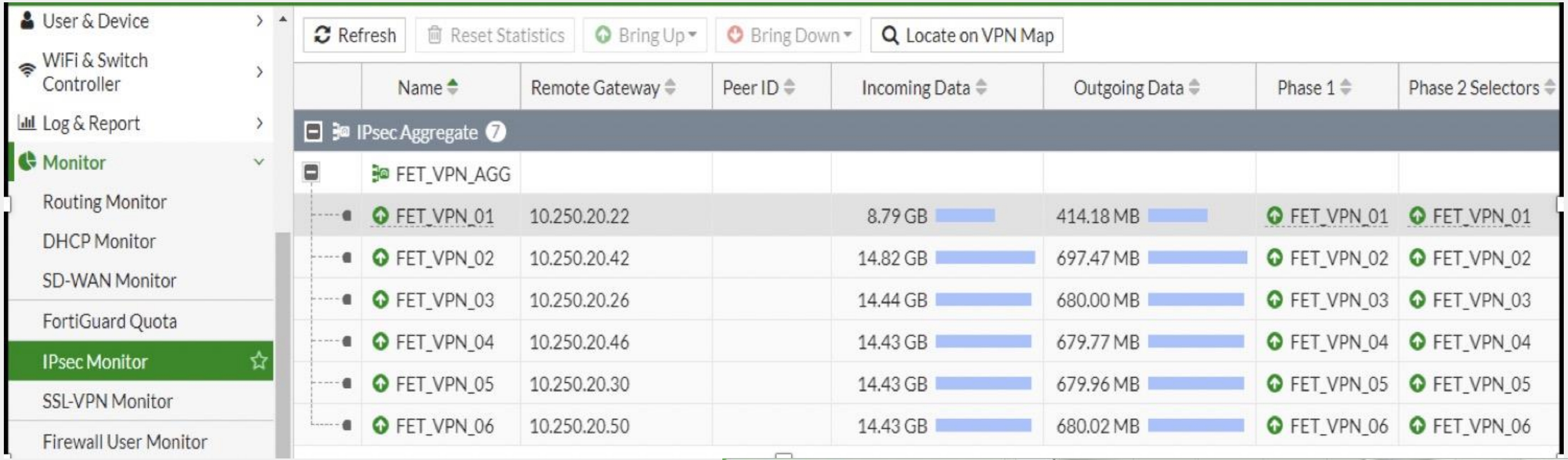
- 可以透過 Automation trigger SLA notification to do Action (CLI Script)

頻寬倍增合併技術

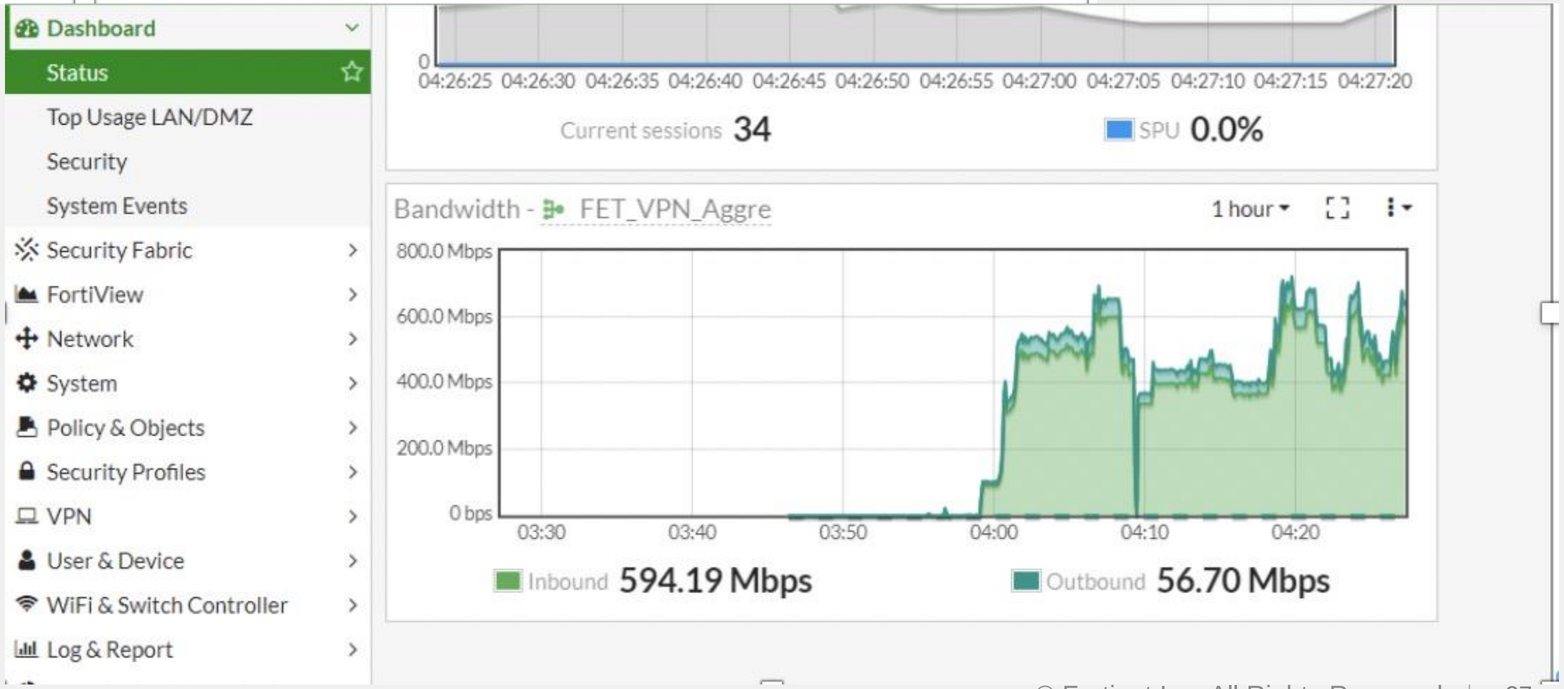
Secure SD-WAN

Per packet WAN Path Steering





Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
IPsec Aggregate 7						
FET_VPN_AGG						
FET_VPN_01	10.250.20.22		8.79 GB	414.18 MB	FET_VPN_01	FET_VPN_01
FET_VPN_02	10.250.20.42		14.82 GB	697.47 MB	FET_VPN_02	FET_VPN_02
FET_VPN_03	10.250.20.26		14.44 GB	680.00 MB	FET_VPN_03	FET_VPN_03
FET_VPN_04	10.250.20.46		14.43 GB	679.77 MB	FET_VPN_04	FET_VPN_04
FET_VPN_05	10.250.20.30		14.43 GB	679.96 MB	FET_VPN_05	FET_VPN_05
FET_VPN_06	10.250.20.50		14.43 GB	680.02 MB	FET_VPN_06	FET_VPN_06



Current sessions 34

SPU 0.0%

Bandwidth - FET_VPN_Aggre

Inbound 594.19 Mbps

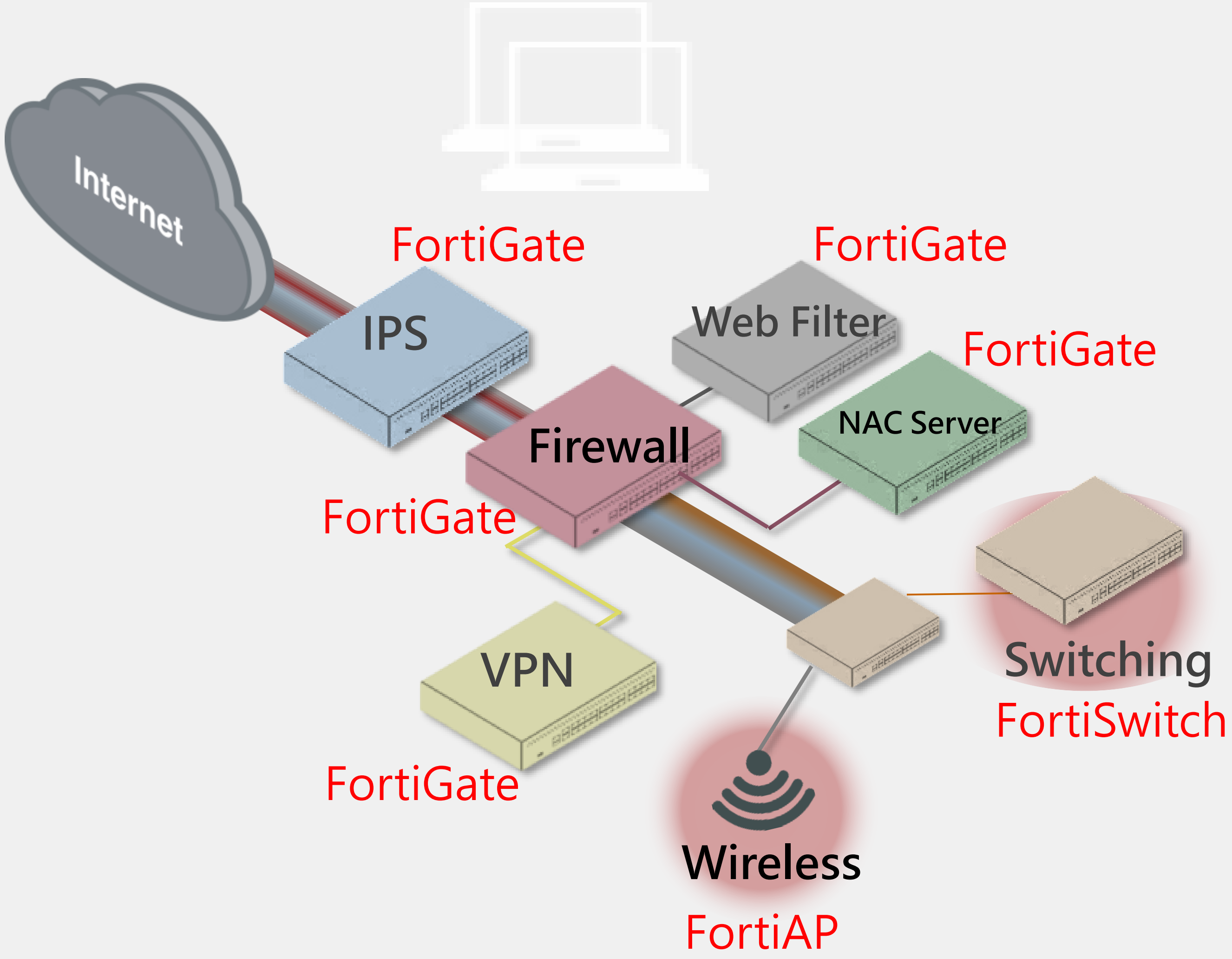
Outbound 56.70 Mbps

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

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

複雜的架構增加維運困難度

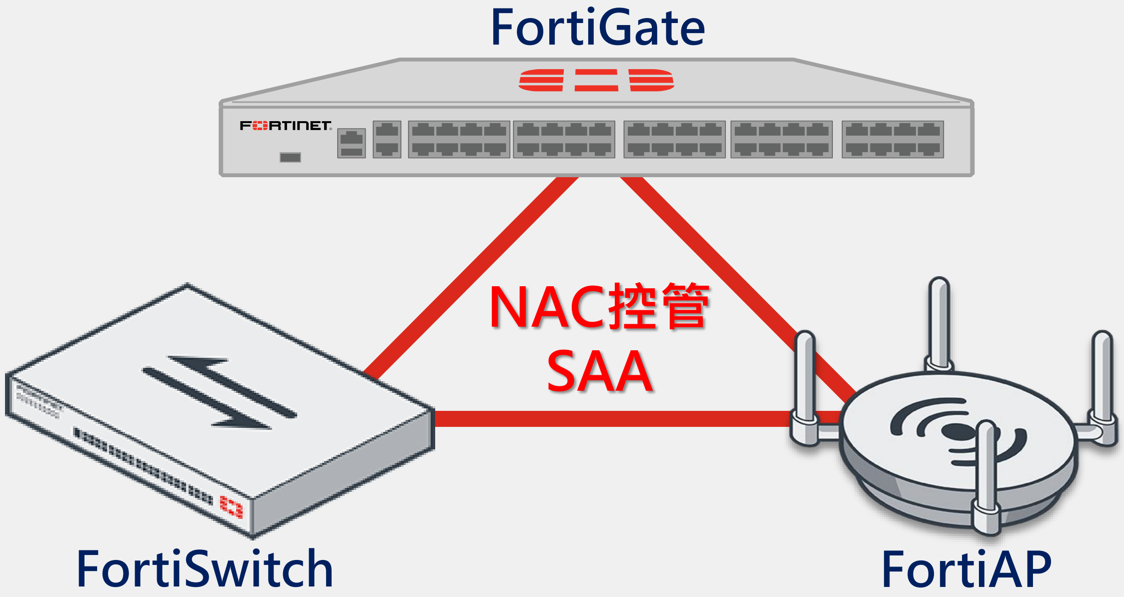
- ➢ 多品牌的解決方案佈署
- ➢ 各自獨立的管理系統
- ➢ 無法快速分辨與因應網路事件



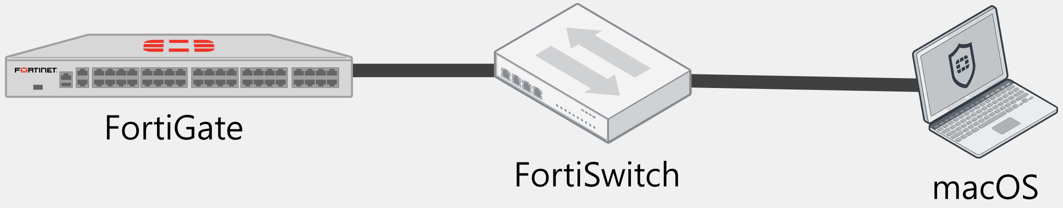
安全存取架構（Secure Access Architecture，SAA）

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 可以辨識千種設備)



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



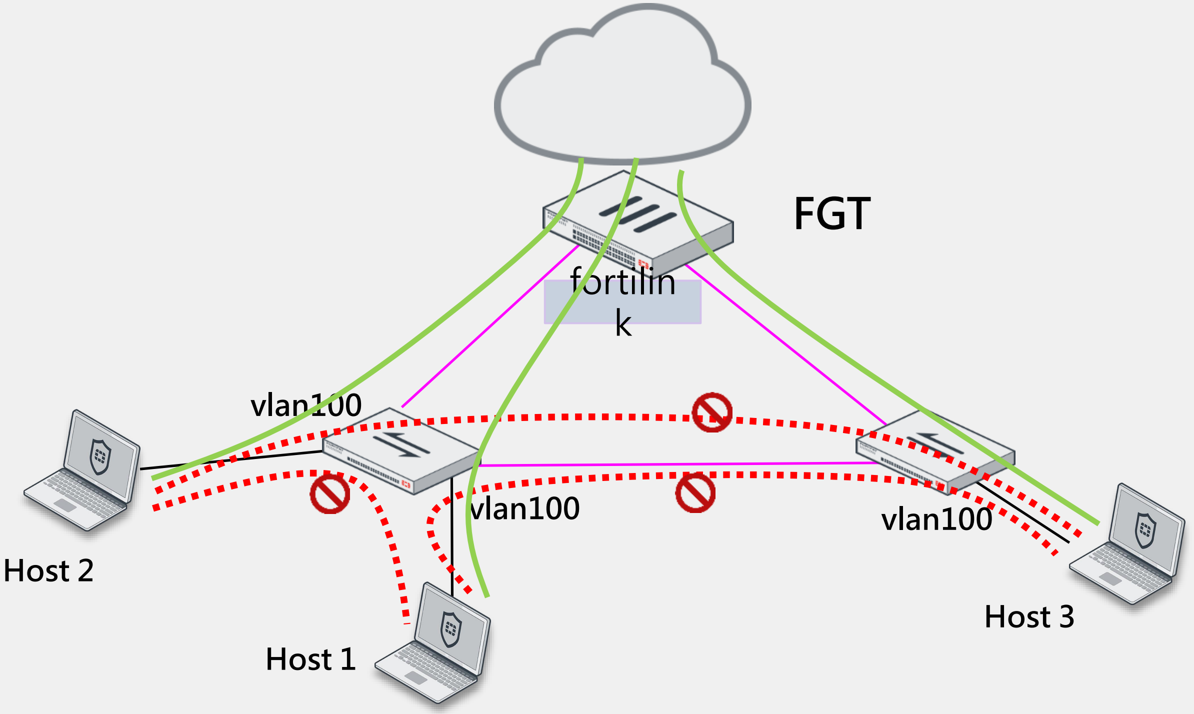
其餘功能：

- 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
- 自動產生拓墣圖/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

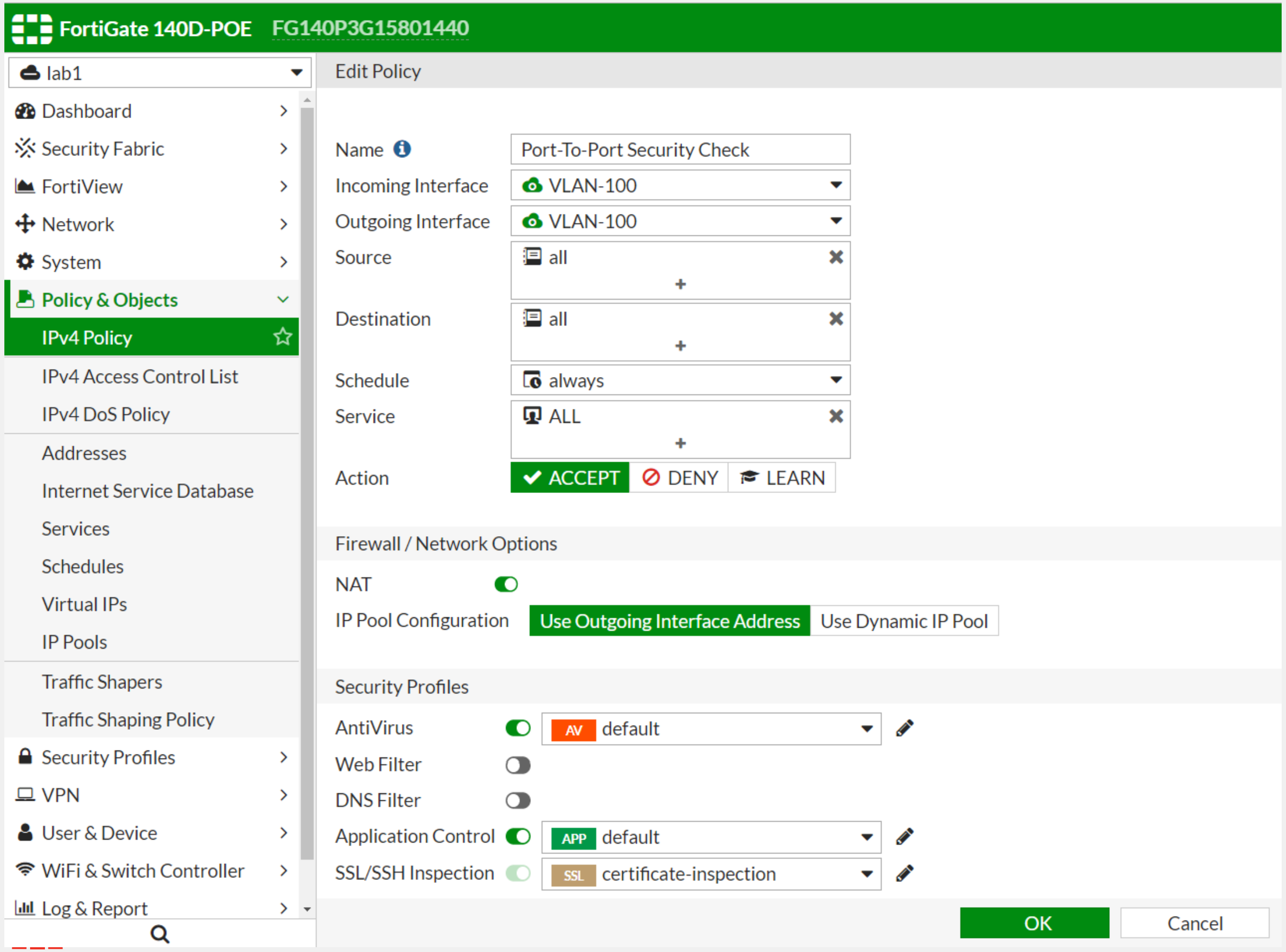
在FortiGate上設定防火牆政策允許同網段流量

```
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



Edit Policy

Name: Port-To-Port Security Check

Incoming Interface: VLAN-100

Outgoing Interface: VLAN-100

Source: all

Destination: all

Schedule: always

Service: ALL

Action: [✓ ACCEPT] DENY LEARN

Firewall / Network Options

NAT: ●

IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Security Profiles

AntiVirus: ● AV default

Web Filter: ○

DNS Filter: ○

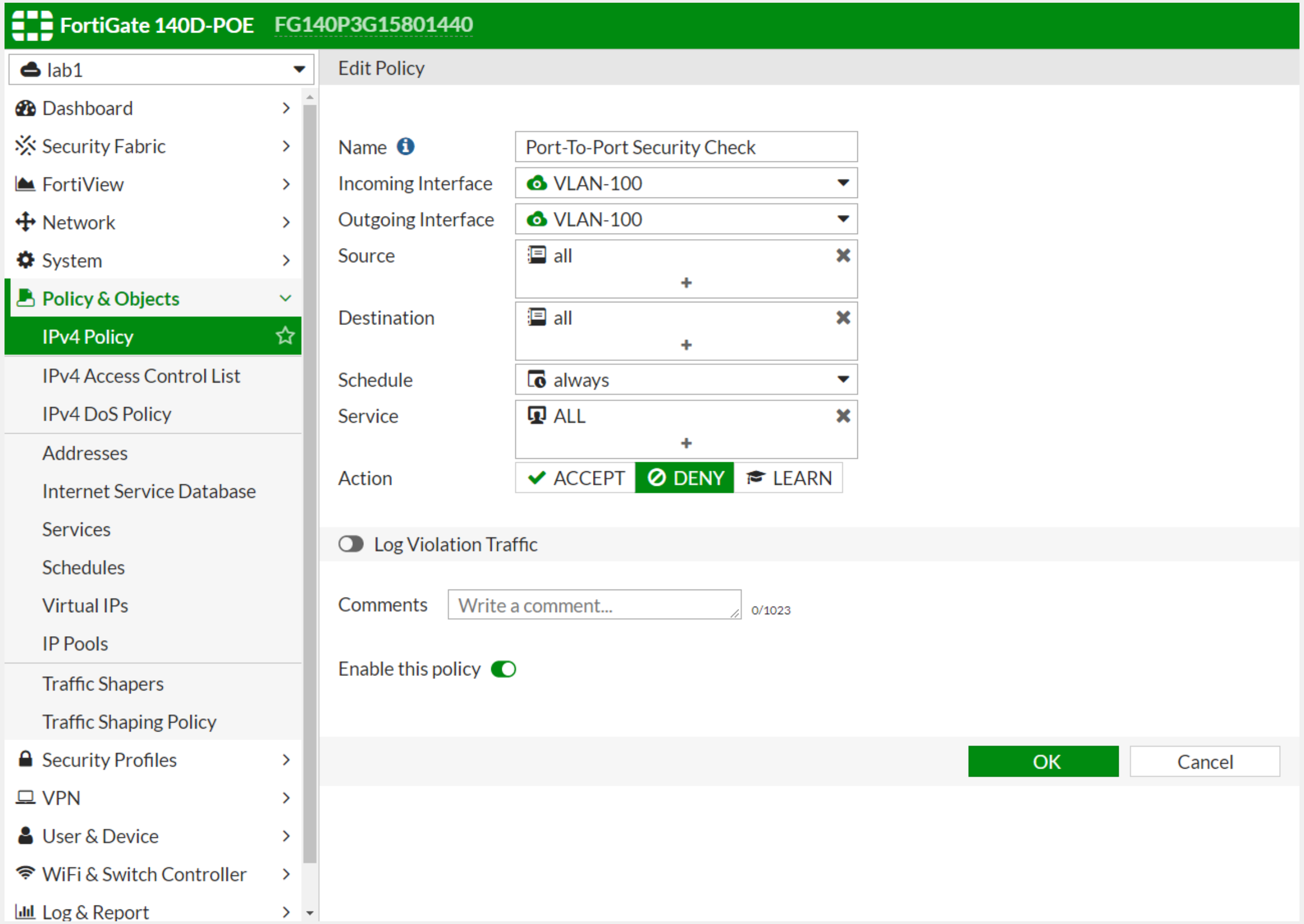
Application Control: ● APP default

SSL/SSH Inspection: ● SSL certificate-inspection

```
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



Edit Policy

Name: Port-To-Port Security Check
Incoming Interface: VLAN-100
Outgoing Interface: VLAN-100
Source: all
Destination: all
Schedule: always
Service: ALL
Action: ✓ ACCEPT [✓ DENY] LEARN
○ Log Violation Traffic
Comments: Write a comment... 0/1023
Enable this policy ●

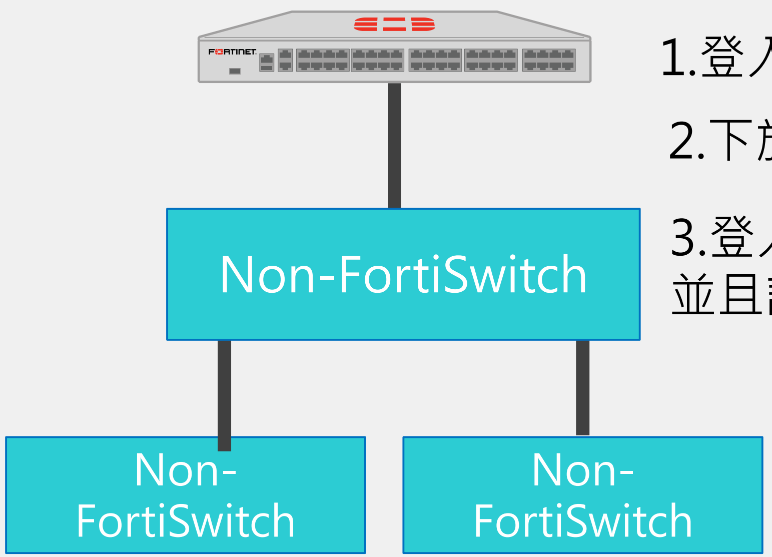
```
192.168.100.1 的 Ping 統計資料:
    封包: 已傳送 = 312，已收到 = 296, 已遺失 = 16 (5% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 0ms，最大值 = 166ms，平均 = 0ms
Control-C
^C
C:\Users\Jarvis>ping 192.168.100.1 -t

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 AP 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

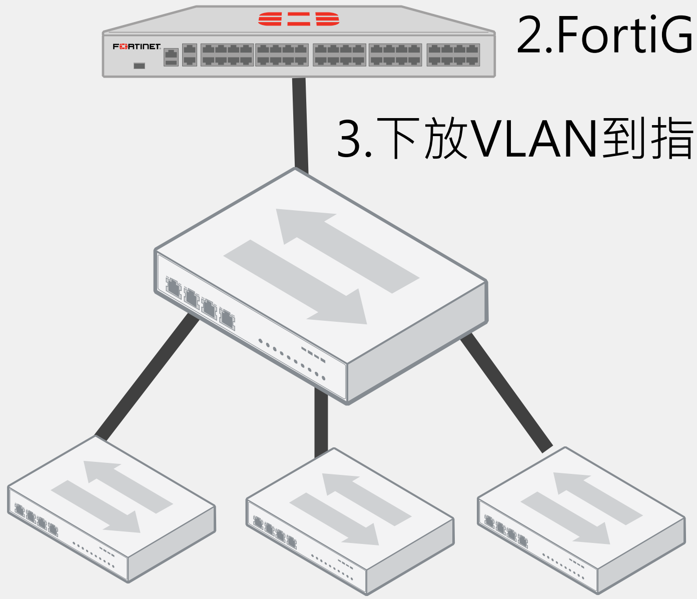
2.下放VLAN到指定的介面

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

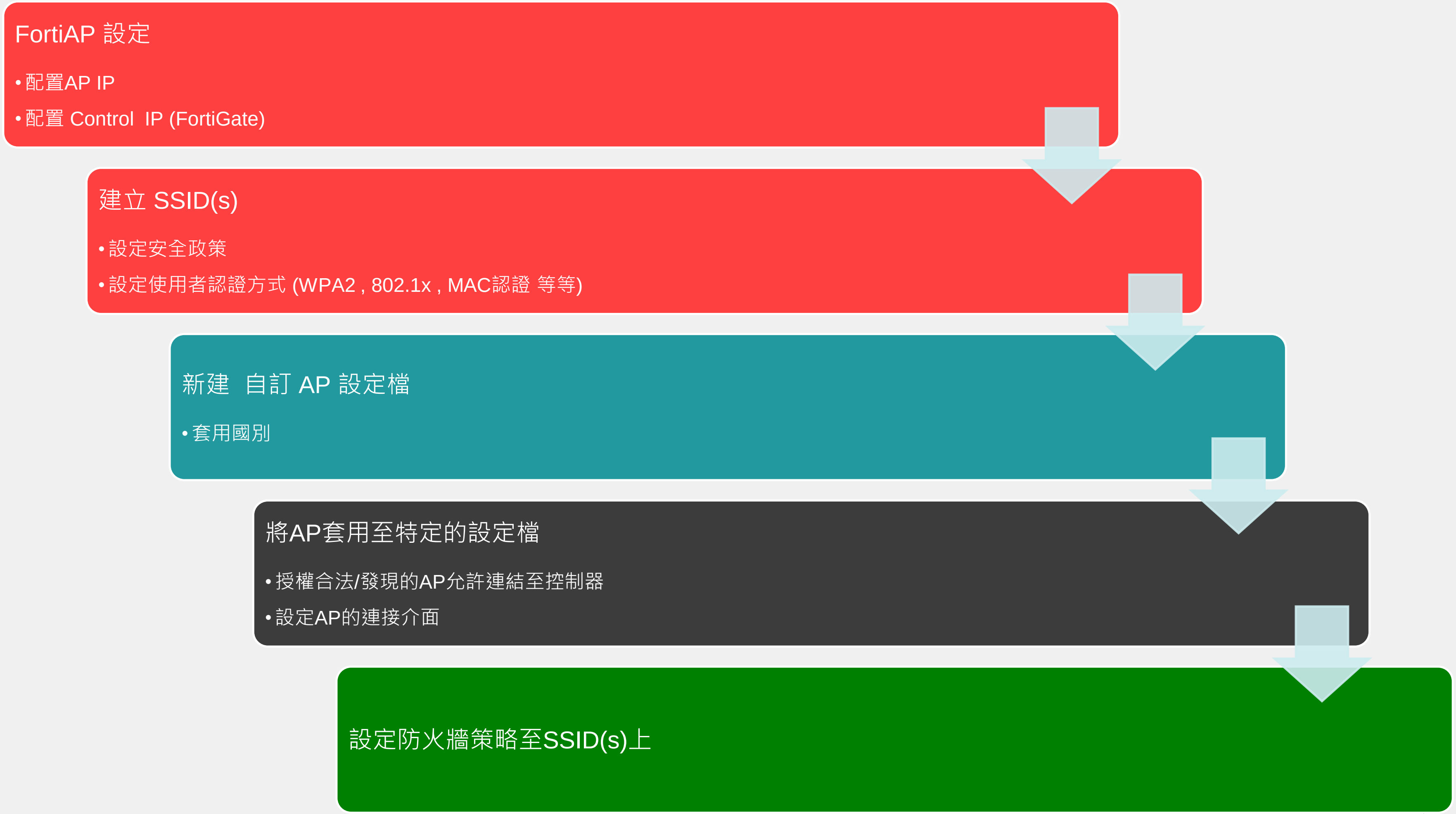
3.下放VLAN到指定的FSW介面

三步驟統一在FortiGate操作

關於新增SSID那件事

Switch AP Controller – 防火牆就是你的控制器

輕鬆建置無線環境 - FAP 五部曲



FortiAP 設定

- 配置AP IP
- 配置 Control IP (FortiGate)

建立 SSID(s)

- 設定安全政策
- 設定使用者認證方式 (WPA2 , 802.1x , MAC認證 等等)

新建 自訂 AP 設定檔

- 套用國別

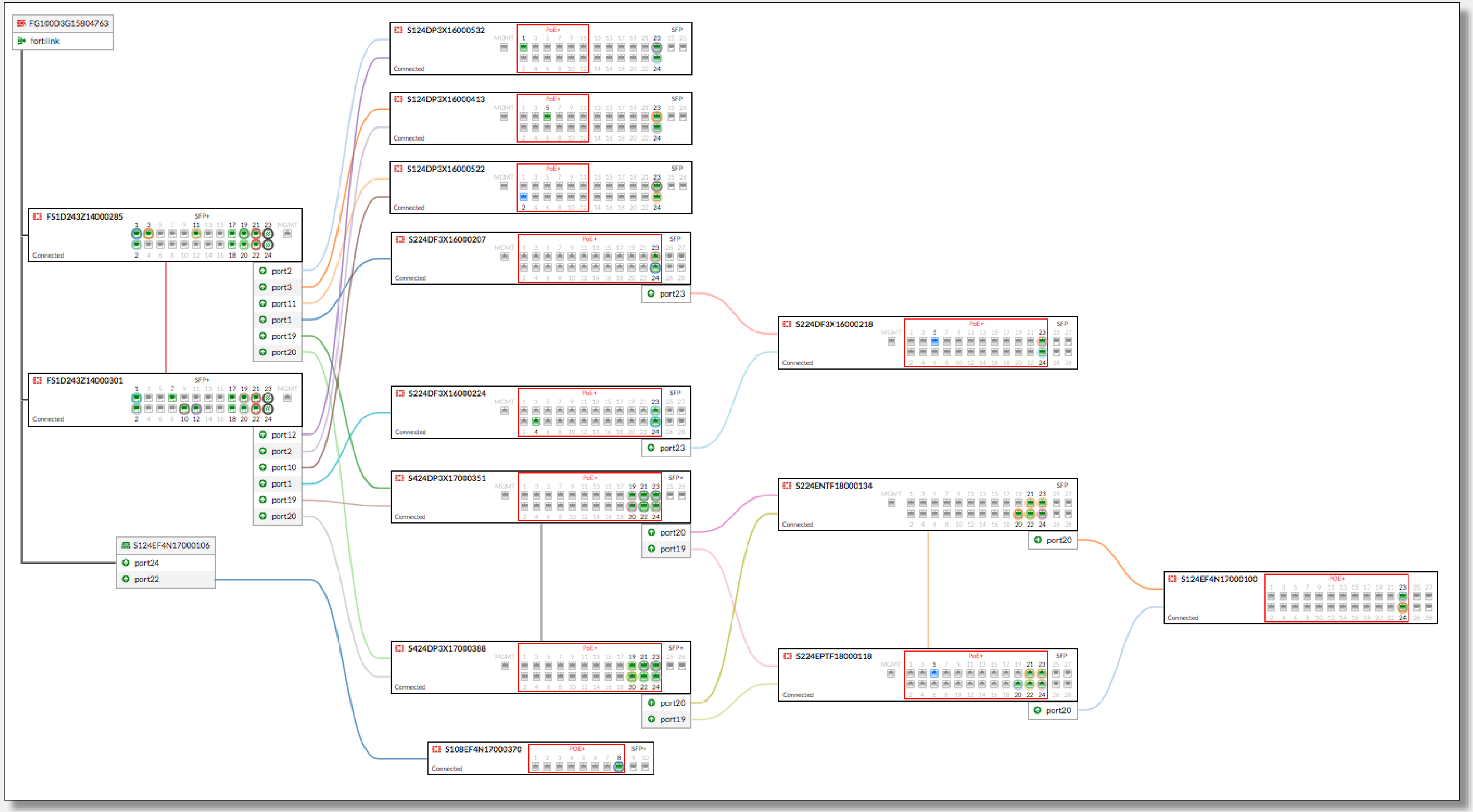
將AP套用至特定的設定檔

- 授權合法/發現的AP允許連結至控制器
- 設定AP的連接介面

設定防火牆策略至SSID(s)上

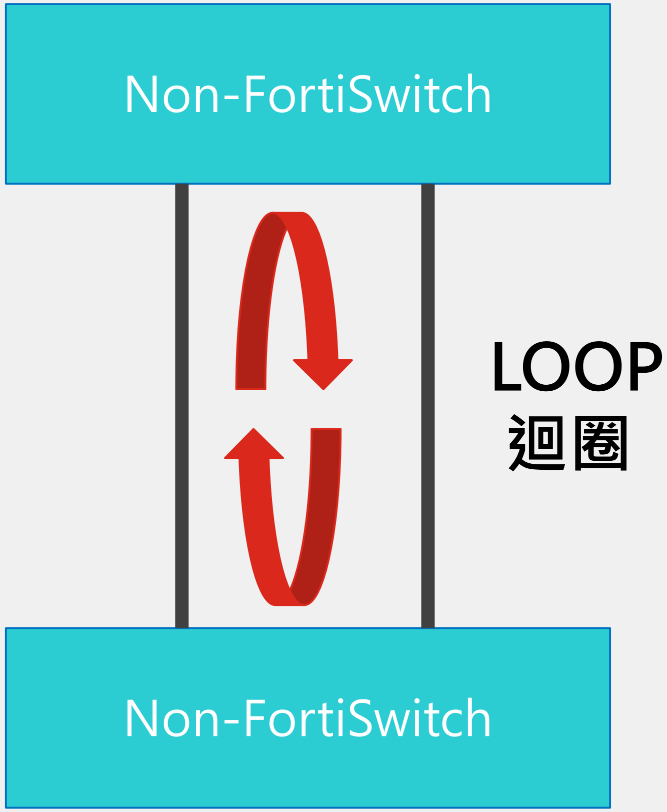
自動產生拓撲圖

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

傳統架構

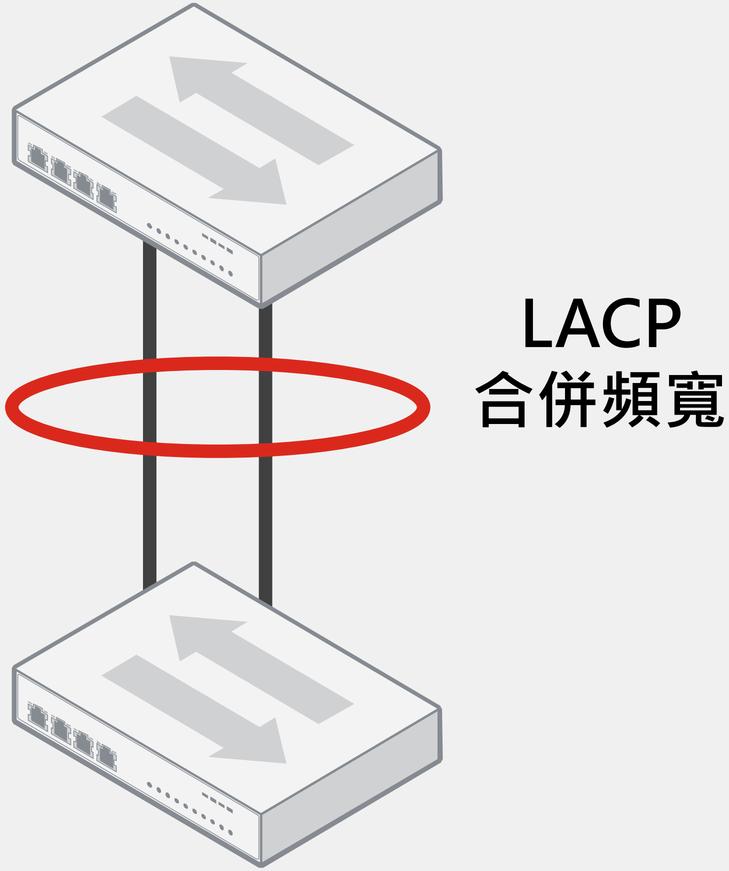


Non-FortiSwitch

LOOP
迴圈

Non-FortiSwitch

Fortinet資安鐵三角

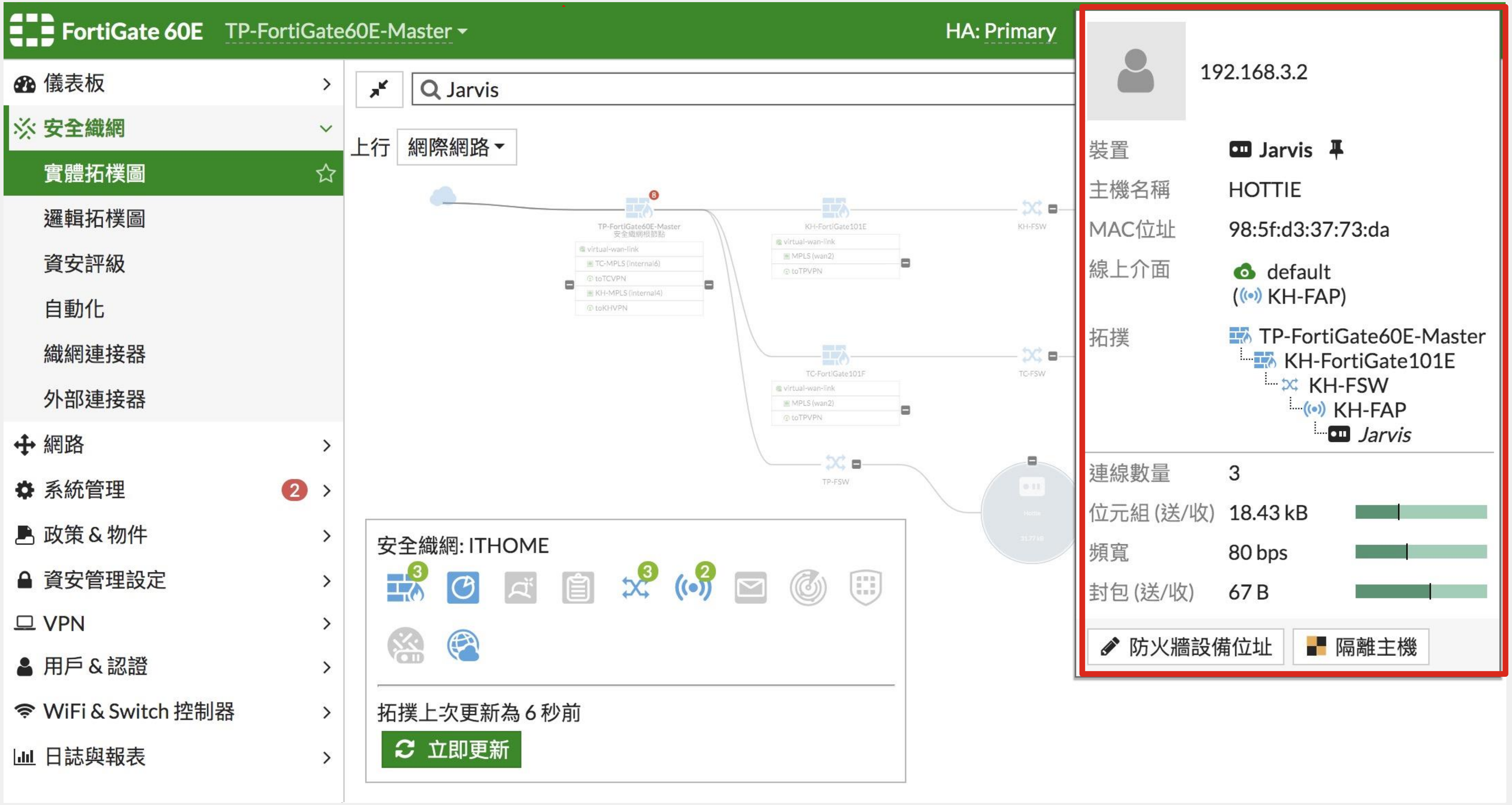


LACP
合併頻寬

安全織網

實體拓墣圖 - 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)



192.168.3.2

裝置 Jarvis

主機名稱 HOTTIE

MAC位址 98:5f:d3:37:73:da

線上介面 default (KH-FAP)

拓撲 TP-FortiGate60E-Master
- KH-FortiGate101E
  - KH-FSW
    - KH-FAP
      - *Jarvis*

連線數量 3

位元組 (送/收) 18.43 kB

頻寬 80 bps

封包 (送/收) 67 B

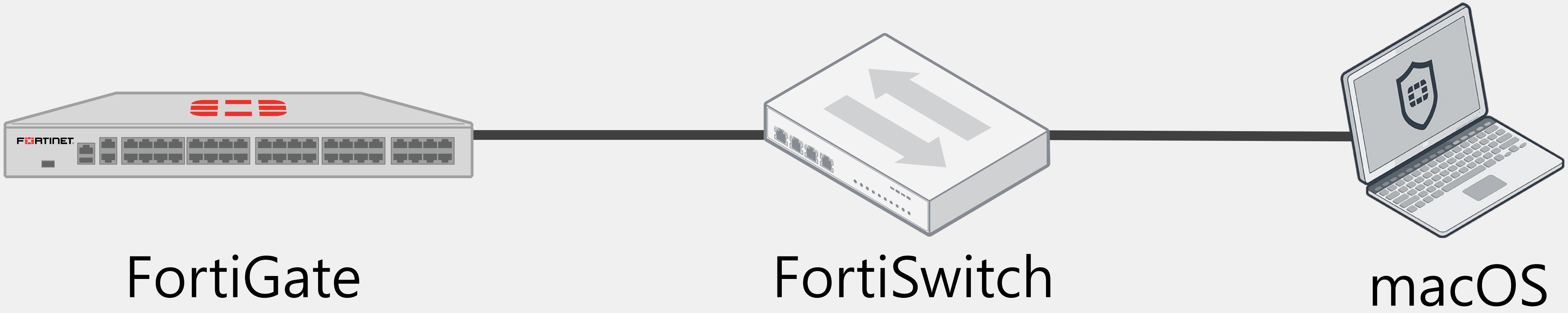
安全織網: ITHOME

拓撲上次更新為 6 秒前

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。(IOT License + FSW 可以辨識千種設備)

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。



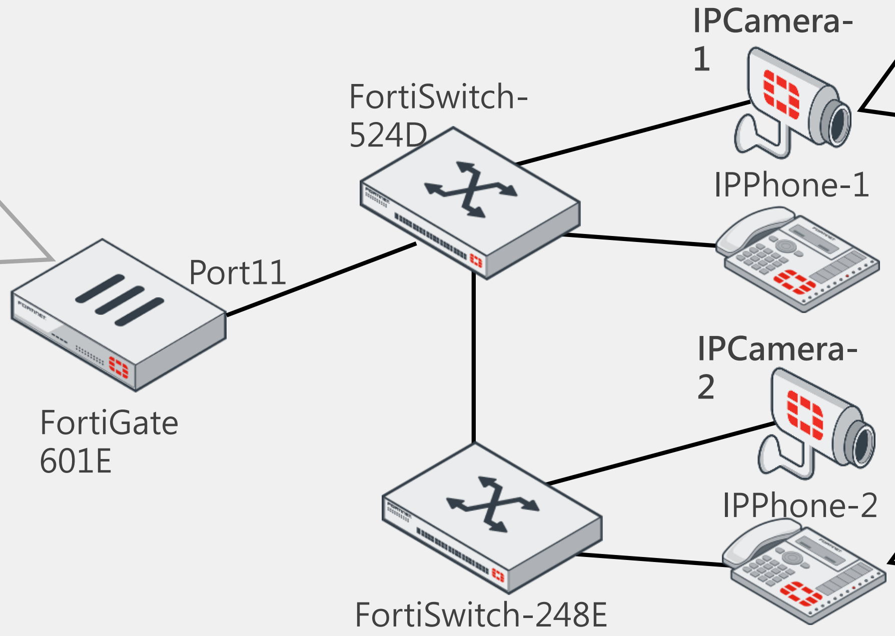
關於NAC那件事

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
```

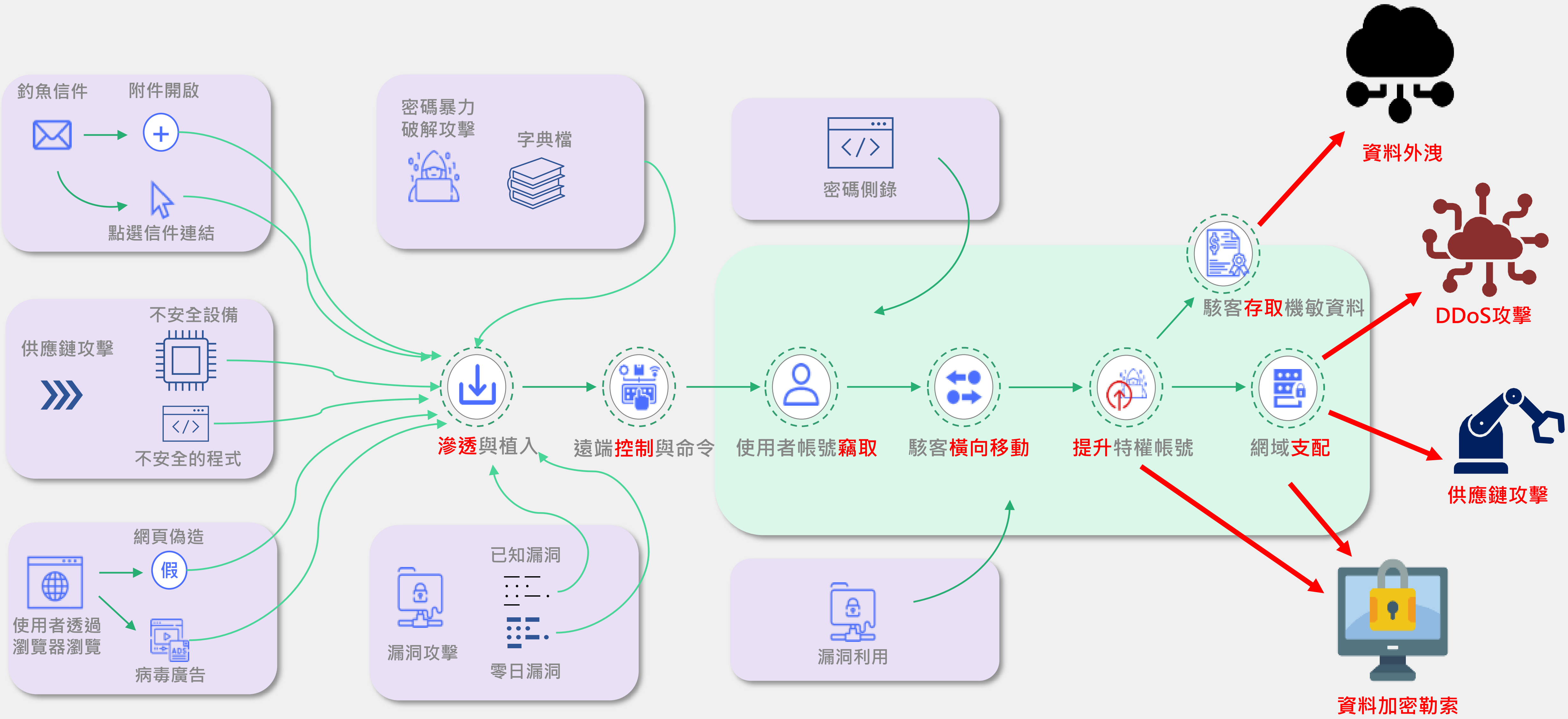


```
mac 08:5b:0e:d4:4f:3c
last-known-switch "S524DN4K16000116"
last-known-port "port6"
matched-nac-policy "Camera-Policy"
mac-policy "Camera-LAN"
```

```
mac 70:4c:a5:a8:0a:1c
last-known-switch "S248EPTF18001384"
last-known-port "port8"
matched-nac-policy   “Phone-Policy"
mac-policy   “Phone-LAN"
```

AI驅動次世代端點安全防護

防不勝防的駭客攻擊...


釣魚信件
附件開啟
點選信件連結
密碼暴力
破解攻擊
字典檔
密碼側錄
供應鏈攻擊
不安全設備
不安全的程式
網頁偽造
假
使用者透過
瀏覽器瀏覽
病毒廣告
已知漏洞
漏洞攻擊
零日漏洞
漏洞利用
滲透與植入
遠端控制與命令
使用者帳號竊取
駭客橫向移動
提升特權帳號
網域支配
駭客存取機敏資料
資料外洩
DDoS攻擊
供應鏈攻擊
資料加密勒索

端點防護需要強化偵測與事件回應
(EPPEndpoint Protection Platform + EDREndpoint Detection and Response)

01 即時阻斷

強化端點安全能力

透過NGAV機器學習強化端點安全防護能力以對抗未知、新型態惡意程式與攻擊手法。

02 自動隔離

保持營運不中斷

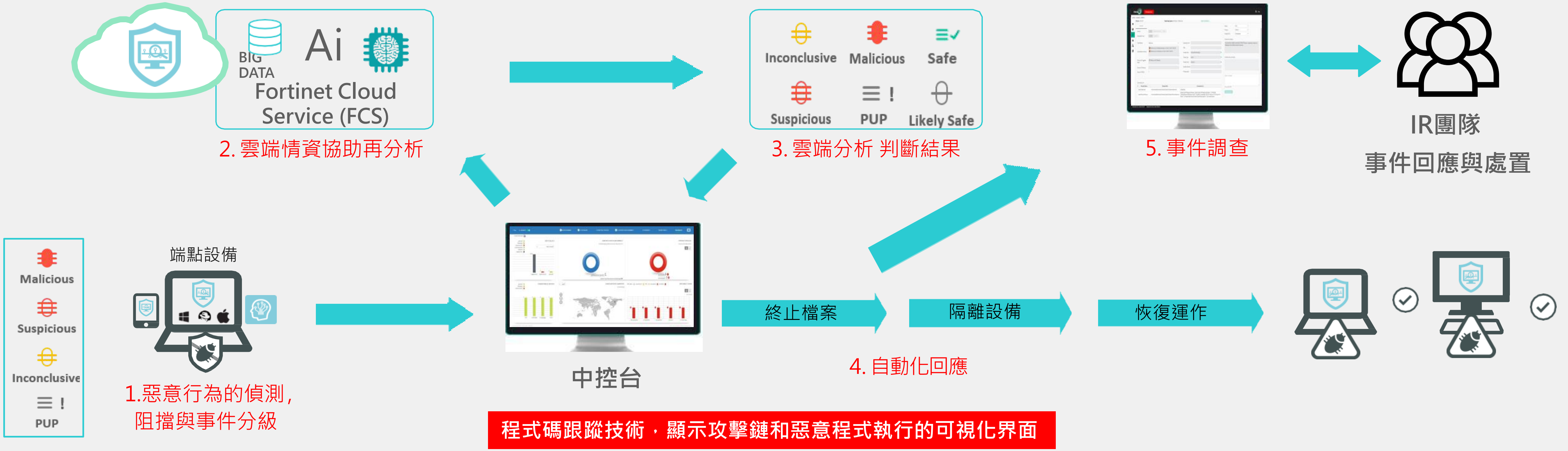
通過端點系統即時監控、快速回應與恢復以降低突破性感染攻擊事件帶來的衝擊。

03 安全聯防

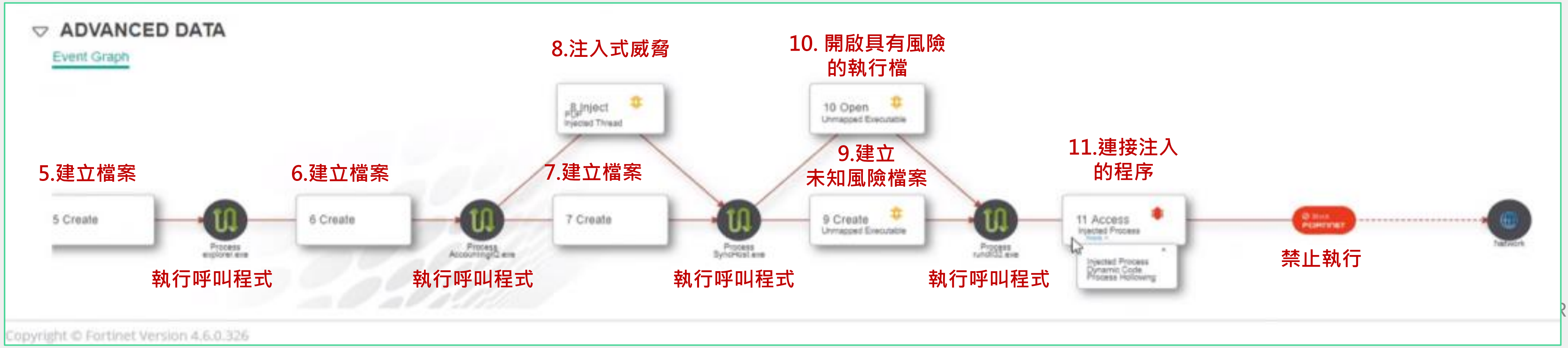
簡化安全維運

經由專業資安服務和安全設備自動化整合後，應對資安事件的調查與處理。

端點資安事件檢視與資訊分析



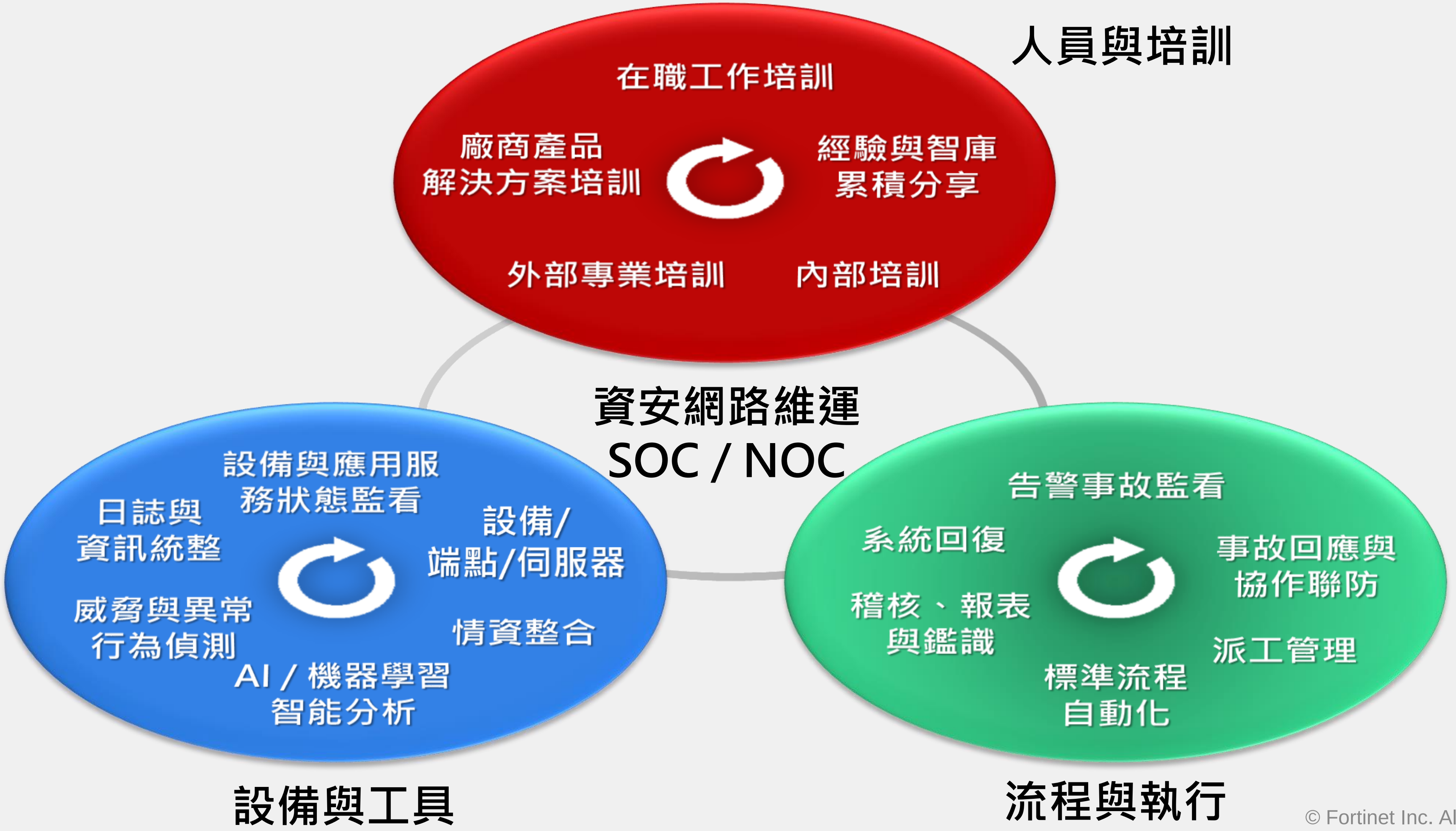
程式碼跟蹤技術，顯示攻擊鏈和惡意程式執行的可視化界面



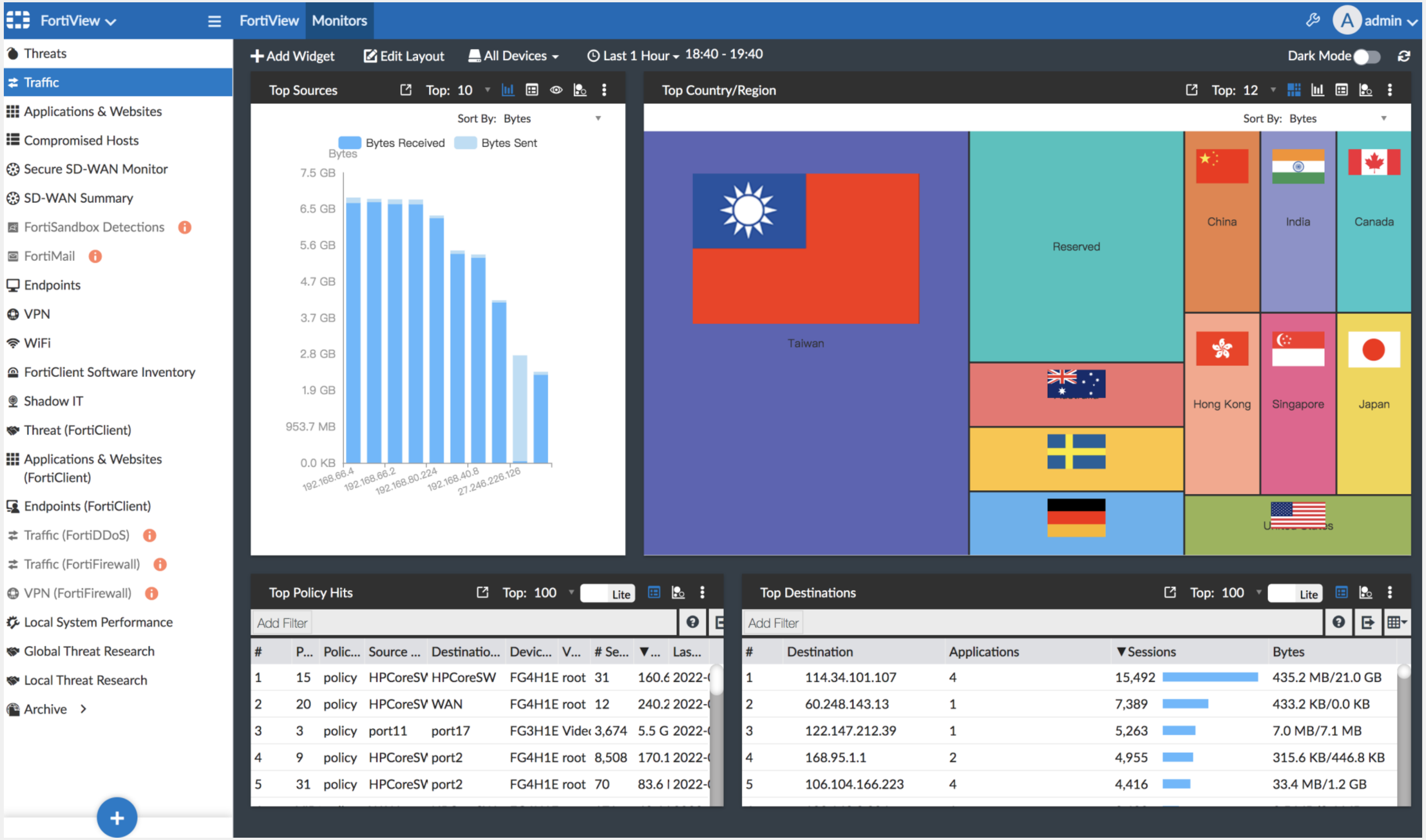
AI驅動高效率的安全營運

資安網維控管三重奏

導入好的設備與解決方案、簡單易用、標準化作業流程



FortiAnalyzer – Monitors



Top Policy Hits   Top: 100   Lite

Add Filter

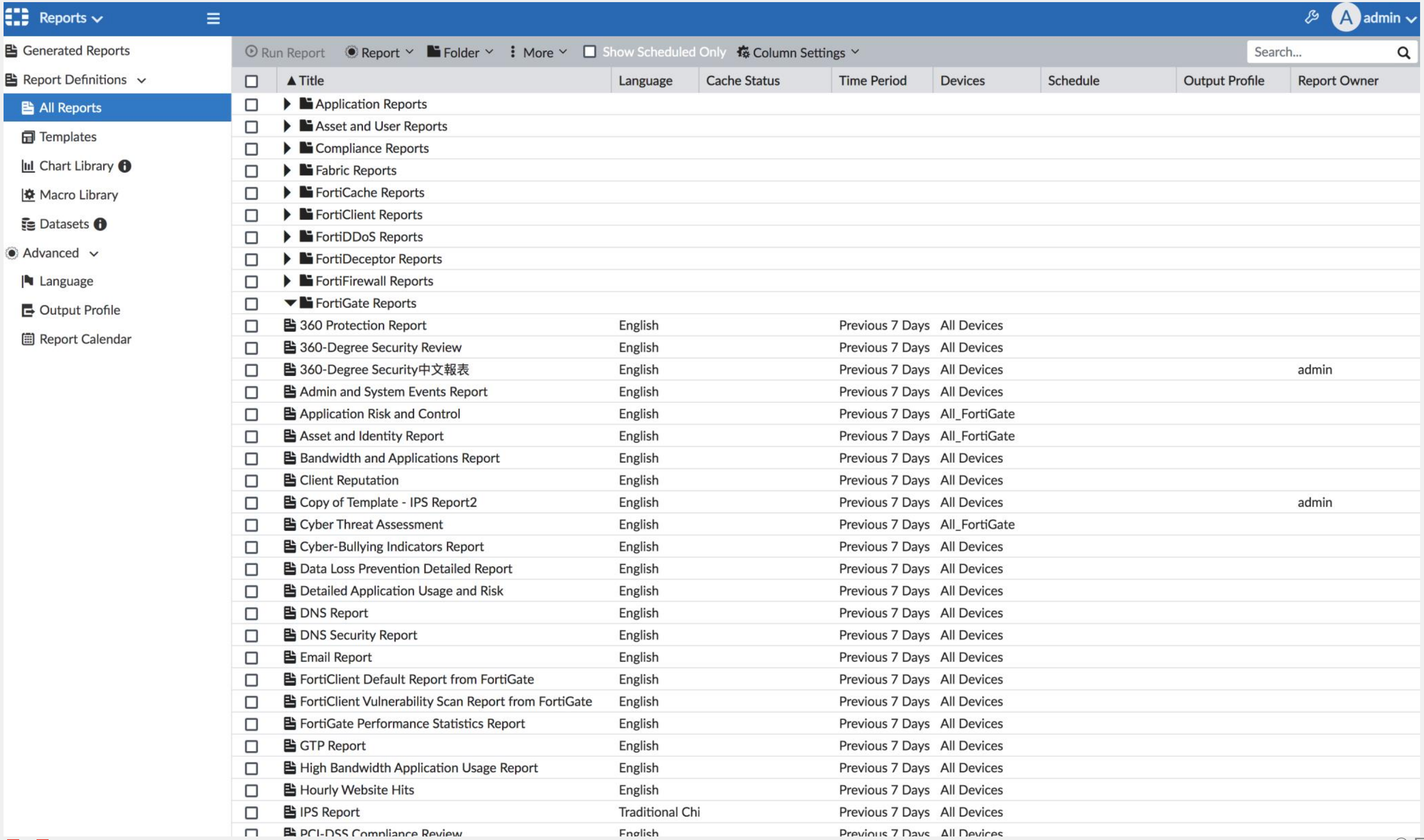
#	P...	Polic...	Source ...	Destinatio...	Devic...	V...	# Se...	▼...	Las...
1	15	policy	HPCoreSV	HPCoreSW	FG4H1E	root	31	160.6	2022-(
2	20	policy	HPCoreSV	WAN	FG4H1E	root	12	240.2	2022-(
3	3	policy	port11	port17	FG3H1E	Vide	3,674	5.5 G	2022-(
4	9	policy	HPCoreSV	port2	FG4H1E	root	8,508	170.1	2022-(
5	31	policy	HPCoreSV	port2	FG4H1E	root	70	83.6 I	2022-(

Top Destinations   Top: 100   Lite

Add Filter

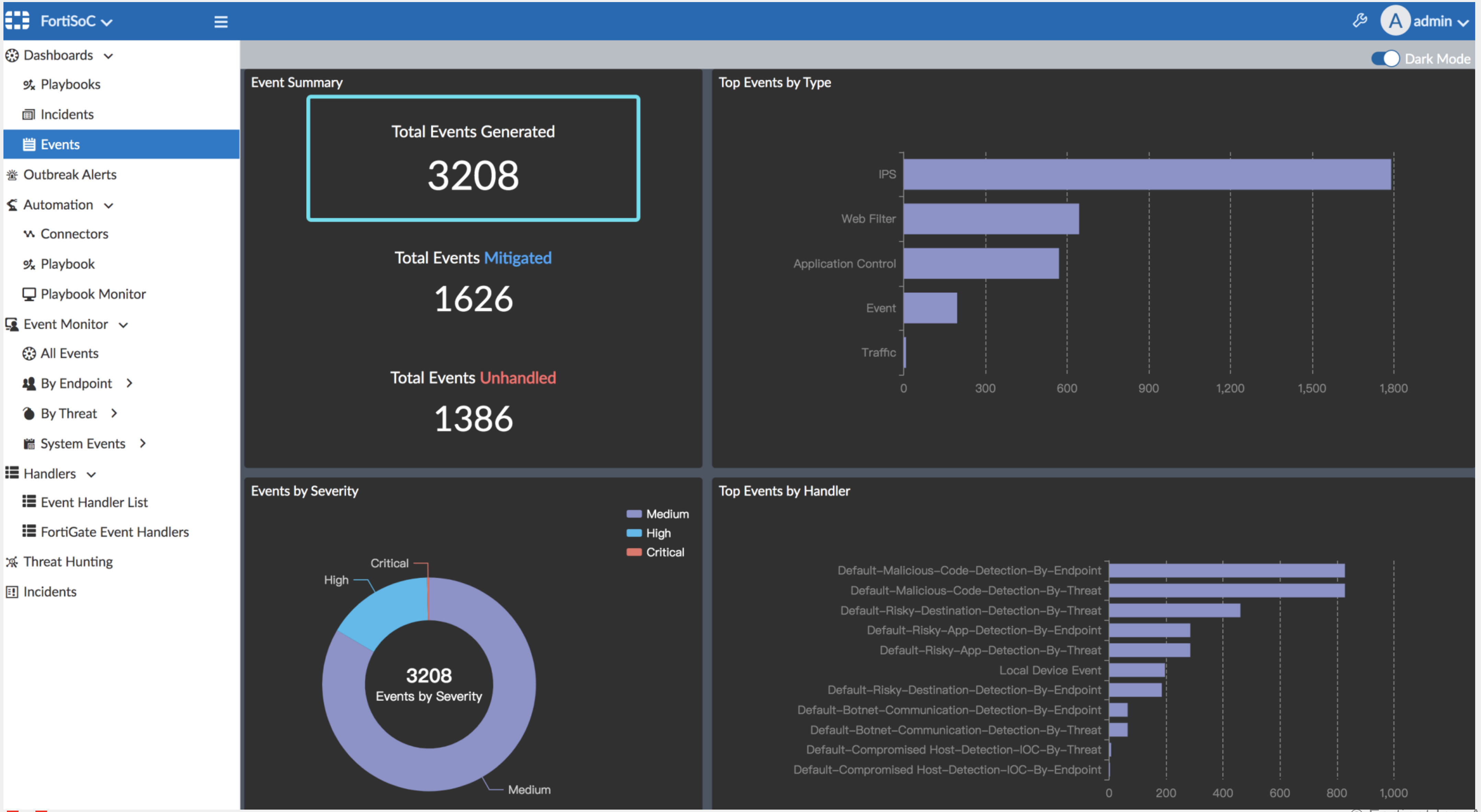
#	Destination	Applications	▼Sessions	Bytes
1	114.34.101.107	4	15,492	435.2 MB/21.0 GB
2	60.248.143.13	1	7,389	433.2 KB/0.0 KB
3	122.147.212.39	1	5,263	7.0 MB/7.1 MB
4	168.95.1.1	2	4,955	315.6 KB/446.8 KB
5	106.104.166.223	4	4,416	33.4 MB/1.2 GB

FortiAnalyzer – Reports (內建各種報表，可客製化)



☐	▲Title	Language	Cache Status	Time Period	Devices	Schedule	Output Profile	Report Owner
☐	▶ Application Reports							
☐	▶ Asset and User Reports							
☐	▶ Compliance Reports							
☐	▶ Fabric Reports							
☐	▶ FortiCache Reports							
☐	▶ FortiClient Reports							
☐	▶ FortiDDoS Reports							
☐	▶ FortiDeceptor Reports							
☐	▶ FortiFirewall Reports							
☐	▼ FortiGate Reports							
☐	360 Protection Report	English		Previous 7 Days	All Devices			
☐	360-Degree Security Review	English		Previous 7 Days	All Devices			
☐	360-Degree Security中文報表	English		Previous 7 Days	All Devices			admin
☐	Admin and System Events Report	English		Previous 7 Days	All Devices			
☐	Application Risk and Control	English		Previous 7 Days	All_FortiGate			
☐	Asset and Identity Report	English		Previous 7 Days	All_FortiGate			
☐	Bandwidth and Applications Report	English		Previous 7 Days	All Devices			
☐	Client Reputation	English		Previous 7 Days	All Devices			
☐	Copy of Template - IPS Report2	English		Previous 7 Days	All Devices			admin
☐	Cyber Threat Assessment	English		Previous 7 Days	All_FortiGate			
☐	Cyber-Bullying Indicators Report	English		Previous 7 Days	All Devices			
☐	Data Loss Prevention Detailed Report	English		Previous 7 Days	All Devices			
☐	Detailed Application Usage and Risk	English		Previous 7 Days	All Devices			
☐	DNS Report	English		Previous 7 Days	All Devices			
☐	DNS Security Report	English		Previous 7 Days	All Devices			
☐	Email Report	English		Previous 7 Days	All Devices			
☐	FortiClient Default Report from FortiGate	English		Previous 7 Days	All Devices			
☐	FortiClient Vulnerability Scan Report from FortiGate	English		Previous 7 Days	All Devices			
☐	FortiGate Performance Statistics Report	English		Previous 7 Days	All Devices			
☐	GTP Report	English		Previous 7 Days	All Devices			
☐	High Bandwidth Application Usage Report	English		Previous 7 Days	All Devices			
☐	Hourly Website Hits	English		Previous 7 Days	All Devices			
☐	IPS Report	Traditional Chi		Previous 7 Days	All Devices			
☐	PCI-DSS Compliance Review	English		Previous 7 Days	All Devices			

FortiAnalyzer – FortiSoC (事件檢視與分析)


FortiSoC
admin
Dark Mode
Dashboards
Playbooks
Incidents
Events
Outbreak Alerts
Automation
Connectors
Playbook
Playbook Monitor
Event Monitor
All Events
By Endpoint
By Threat
System Events
Handlers
Event Handler List
FortiGate Event Handlers
Threat Hunting
Incidents
Top Events by Type
IPS
Web Filter
Application Control
Event
Traffic
0
300
600
900
1,200
1,500
1,800
Events by Severity
Medium
High
Critical
3208
Events by Severity
Top Events by Handler
Default-Malicious-Code-Detection-By-Endpoint
Default-Malicious-Code-Detection-By-Threat
Default-Risky-Destination-Detection-By-Threat
Default-Risky-App-Detection-By-Endpoint
Default-Risky-App-Detection-By-Threat
Local Device Event
Default-Risky-Destination-Detection-By-Endpoint
Default-Botnet-Communication-Detection-By-Endpoint
Default-Botnet-Communication-Detection-By-Threat
Default-Compromised Host-Detection-IOC-By-Threat
Default-Compromised Host-Detection-IOC-By-Endpoint
0
200
400
600
800
1,000

Event Summary

Total Events Generated
3208

Total Events Mitigated
1626

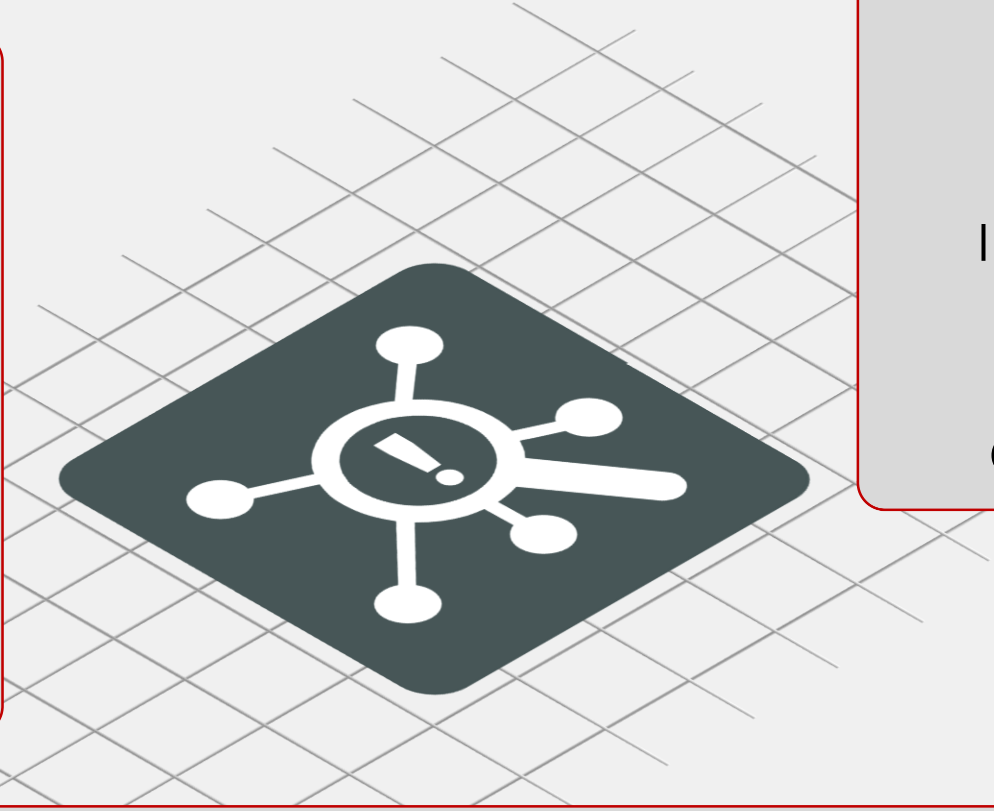
Total Events Unhandled
1386

FortiSIEM - 資安 (SOC) 與網維 (NOC) 融合式分析

完善您整體資安與網維的可視性

資安日誌與資訊

NGFW / IPS / VPN
EPP/EDR
Web Application
eMail System
AAA Server
Database
Traffic / Flows
Router / Switch / WLAN, etc.

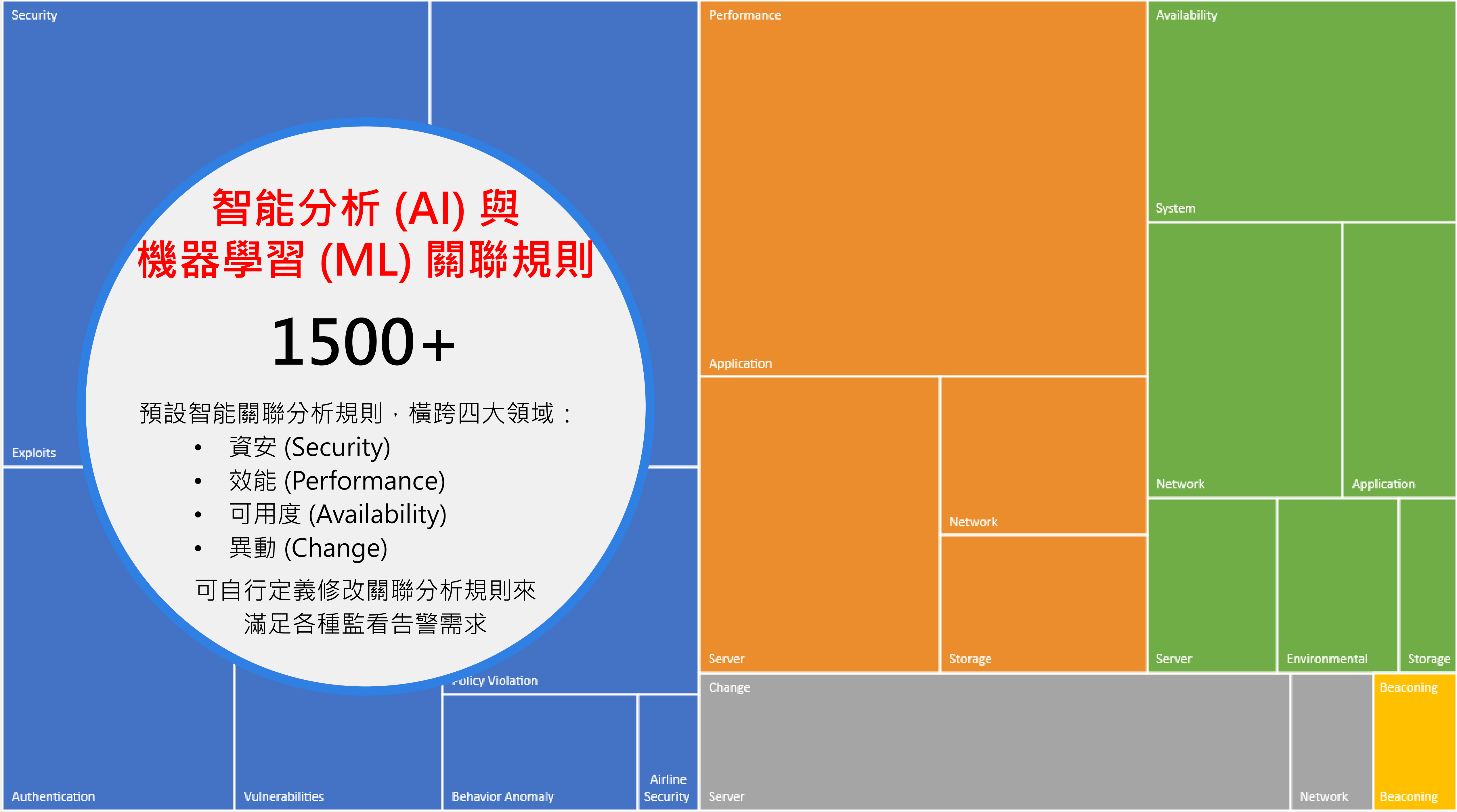


設備效能監看指標

CPU
Memory
Storage
Interface Utilization
Uptime
Process / Services
Configuration, etc.

融合式的資安與網維管理 (SOC & NOC)

更多豐富的功能 | 更好的可視性 | 加速事故回應時間



智能分析 (AI) 與 機器學習 (ML) 關聯規則

1500+

預設智能關聯分析規則，橫跨四大領域：

- 資安 (Security)
- 效能 (Performance)
- 可用度 (Availability)
- 異動 (Change)

可自行定義修改關聯分析規則來
滿足各種監看告警需求

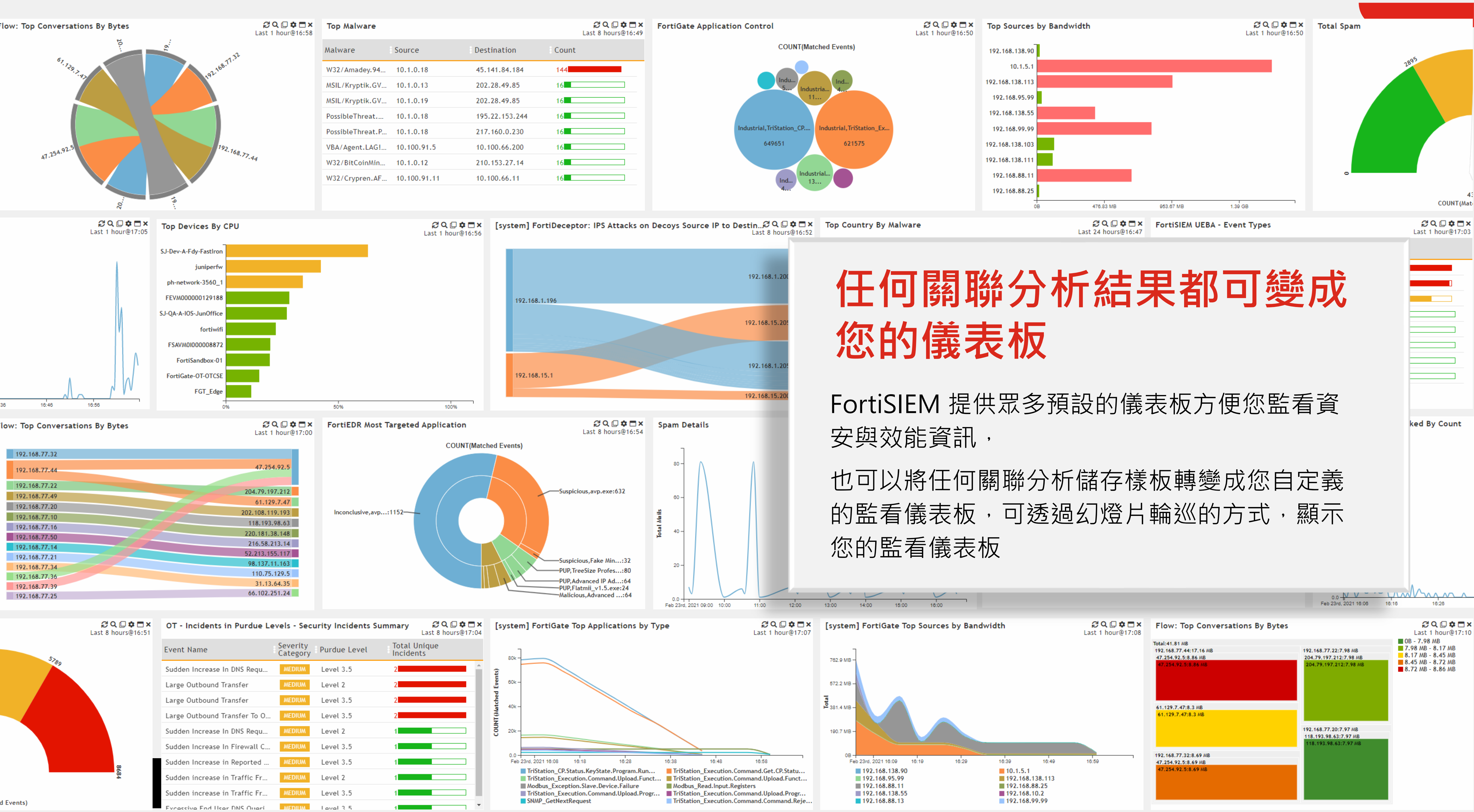
Security
Exploits
Vulnerabilities
Authentication
Vulnerabilities
Policy Violation
Behavior Anomaly
Airline Security
Performance
Application
Server
St
Availability
ication
Environmental
Storage
Change
Server
Network
Beaconing
Beaconing

內建豐富稽核與合規性報表

3000+

預設合規性報表 (Compliance Reports)：
包括 PCI, SOX, HIPAA, FISMA, NERC, COBIT, ITIL, NIST, ISO, GLBA, GPG13, CIS, SANS, Critical Controls

內建報表客製化建構器：
3,000+ 可客製化欄位，豐富的圖表資源庫，可穿插文字與附件


Flow: Top Conversations By Bytes
Top Malware
FortiGate Application Control
Top Sources by Bandwidth
Total Spam
Top Devices By CPU
[system] FortiDeceptor: IPS Attacks on Decoys Source IP to Destin...
Top Country By Malware
FortiSIEM UEBA - Event Types
FortiEDR Most Targeted Application
Spam Details
OT - Incidents in Purdue Levels - Security Incidents Summary
[system] FortiGate Top Applications by Type
[system] FortiGate Top Sources by Bandwidth
Flow: Top Conversations By Bytes

Malware	Source	Destination	Count
W32/Amadey.94...	10.1.0.18	45.141.84.184	144
MSIL/Kryptik.GV...	10.1.0.13	202.28.49.85	16
MSIL/Kryptik.GV...	10.1.0.19	202.28.49.85	16
PossibleThreat....	10.1.0.18	195.22.153.244	16
PossibleThreat.P...	10.1.0.18	217.160.0.230	16
VBA/Agent.LAG!...	10.100.91.5	10.100.66.200	16
W32/BitCoinMin...	10.1.0.12	210.153.27.14	16
W32/Crypren.AF...	10.100.91.11	10.100.66.11	16

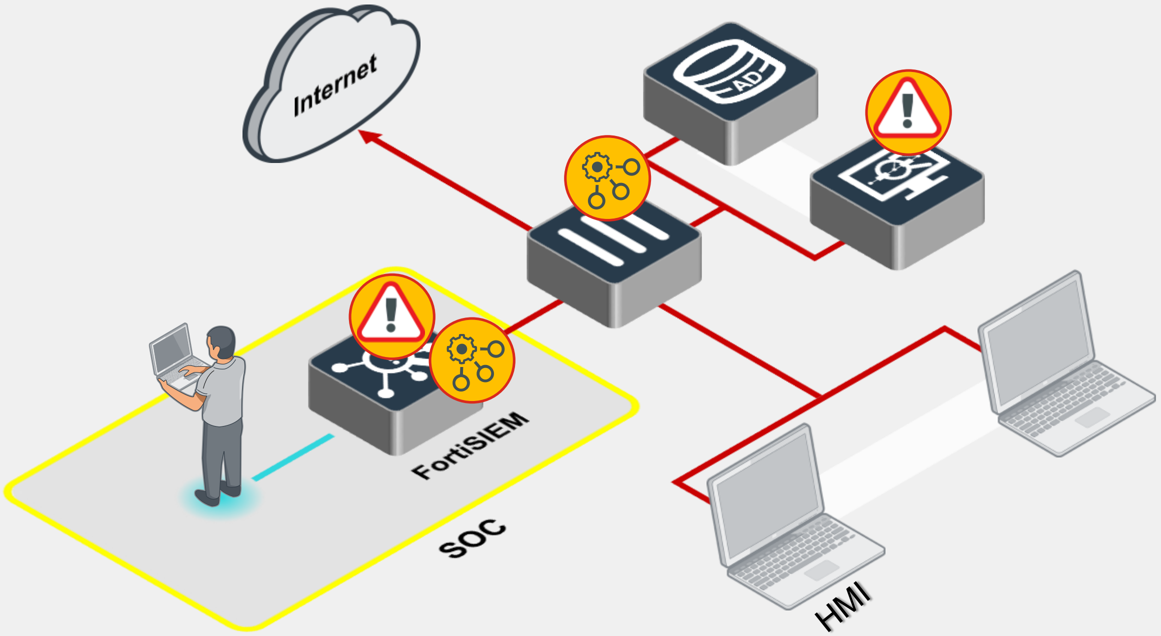
任何關聯分析結果都可變成您的儀表板

FortiSIEM 提供眾多預設的儀表板方便您監看資安與效能資訊，

也可以將任何關聯分析儲存樣板轉變成您自定義的監看儀表板，可透過幻燈片輪巡的方式，顯示您的監看儀表板

FortiSIEM - 標準化事故協作回應流程與自動化 (SOAR)

提供快速有效的告警事故聯防協作與自動化整合



① 部署 FortiSIEM 於您的環境

② FortiSIEM 集中彙整並關聯分析日誌與記錄

③ FortiSIEM 運用情資、智能分析與機器學習，自動產生告警事故

④ 資安分析師使用 FortiSIEM 調查告警事故與相關記錄

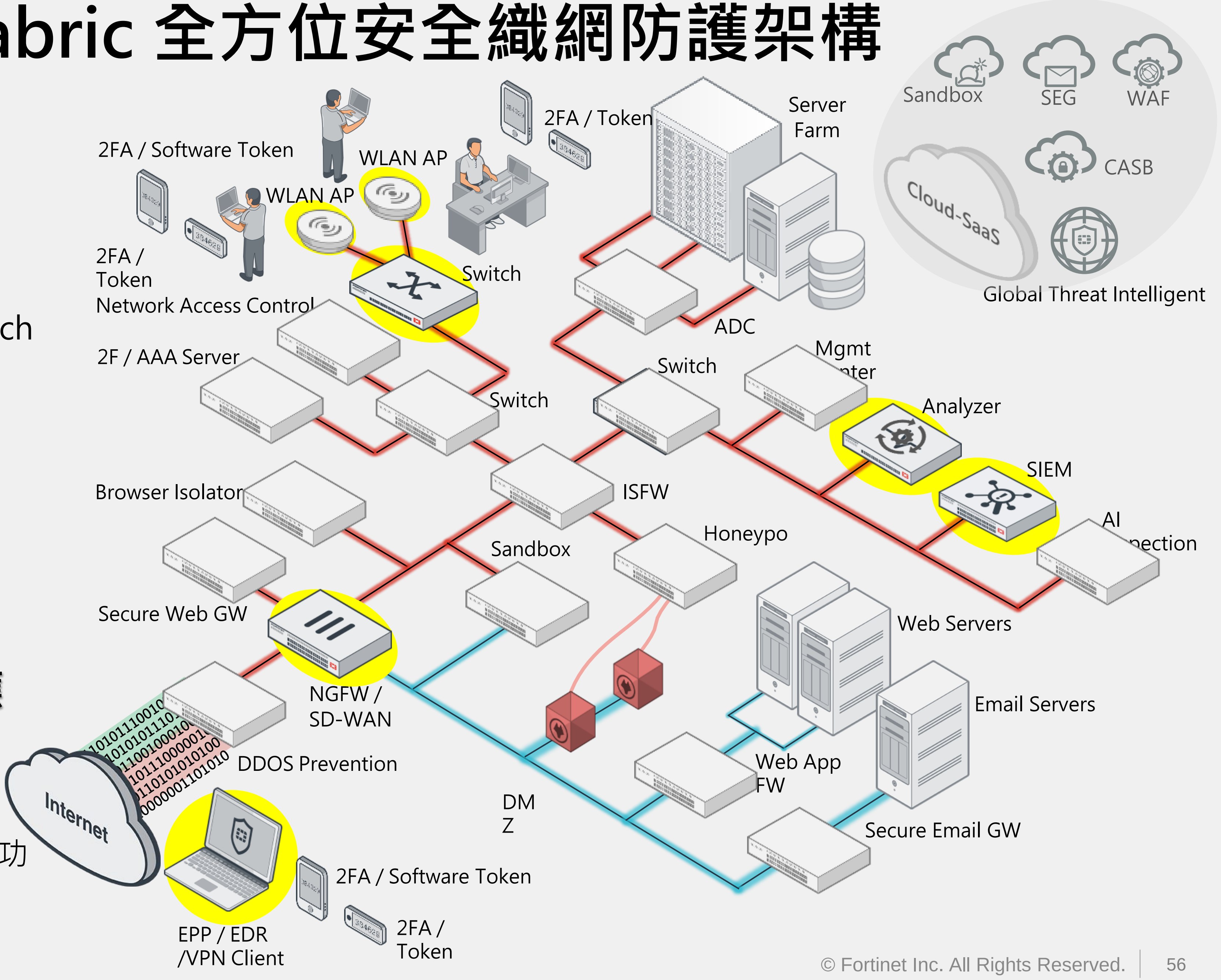
⑤ 資安分析師使用 FortiSIEM 執行告警事故緩解措施腳本

- 緩解措施腳本也可自動執行

Fortinet Security Fabric 全方位安全織網防護架構

讓校園擁有毫不妥協的安全防護

- **內網對外網防護**
  - 新世代防火牆 FortiGate NGFW
  - Secure SD-WAN / Secure SD-Branch
- **內網有線/無線安全存取**
  - 安全存取架構 FortiGate + FortiAP, FortiSwitch
- **強化進階威協偵測與防護**
  - AI驅動端點導向偵測 FortiEDR
- **資安事件告警、聯防、回應處理流程協作與自動化**
  - FortiAnalyzer (支援 Fortinet 產品)
  - FortiSIEM (跨品牌支援，內建SOAR功能)



FORTINET®